



Indiscrétions et discrétion sur Internet: les portes dérobées !!

Introduction

Puisqu'il devient très difficile de surfer tranquillement sans être atteint de toutes part par la pub,
Puisqu'il devient bientôt pénalisable d'exprimer notre opinion sur des blogs ou des sites,
Puisqu'il est devenu naïf de penser en laissant ses coordonnées, que nous n'entrons pas dans des fichiers échangés ensuite à prix d'or,
Puisque notre vie privée voit son espace se restreindre millimétriquement mais inexorablement,
Puisque bon nombre d'atteintes à votre système sont créées par des sociétés tout à fait respectables,
Puisque la pénétration de la publicité dans notre quotidien ne dérange personne mais que le moindre téléchargement de quelques morceaux de musique ou quelques films bien pourris, devient un crime d'état, relayé par les discours sirupeux de placebo d'artistes, babouins de foire qui ne sont ni à gauche, ni à droite mais là où on les pose,
... alors je vais tenter modestement de vous donner quelques clés pour vous protéger de ce monde intraitable ...

Plus elle est combattue, plus je trouve la critique nécessaire. Plus elle est médiocre dans nos médias, plus je trouve les analyses de l'information sur internet, vitales. Et ne venez pas me tancer avec cette sacro-sainte mise en garde sur le manque de rigueur de ces analyses ou le fait que l'on trouve tout et son contraire sur internet. Ce serait un argument si l'information habituelle était irréprochable... nous en sommes tellement loin...

Alors, amis virtuels des combats contre la renonciation, sachons protéger nos faibles moyens informatiques et nous cacher un peu lorsque cela est nécessaire....

A - Votre combat

C'est un combat perdu d'avance. Le but n'est pas de vous protéger de manière infaillible, c'est impossible, mais plutôt de faire en sorte de rendre ce combat extrêmement difficile pour vos adversaires et ainsi de les décourager. **SI VIS PACEM, PARA BELLUM**

Ce qui me fait enrager (entre autres):

- que des anti-virus et des protections de merde soient préinstallés sur tout ordinateur vendu. Ceux-ci sont gratuits pendant un certain temps puis il vous faudra payer pour les tenir à jour (sans mises à jour, ils sont tout bonnement inutiles). De plus ils sont très mauvais et enfin difficilement désinstallables ... bref un scandale !!
- qu'il suffise que j'aille sur un site pour me renseigner sur un short à fleur, par exemple et que vraiment bizarrement, j'ai l'incalculable chance de recevoir ensuite deux cents messages de publicité dans mon email portant sur des vêtements d'été.
- d'entendre des décérébrés nous répéter que le téléchargement illégal est responsable de tous les maux. Des gros connards pleins de pognon ont cru qu'ils pourraient maintenir les CD à un prix d'or et nous gaver avec des compil, remix et autres saloperies. Ce sont eux qui ont tué le CD, pas les téléchargeurs. Idem pour les places de cinéma. J'ajouterais qu'existe la même hypocrisie que pour le tabac, qui consiste à fournir l'intégralité des dispositifs en majorant les prix pour mieux nous dire ensuite que leur utilisation n'est pas légale (graveurs, homecinéma, vitesse ADSL en augmentation, taxes diverses sur CD et DVD vierges, etc...).
- que l'on ne cesse de vouloir agrandir mon penis alors que je m'y suis habitué comme il est...
- que l'on se paie notre gueule avec l'informatique. Votre pc est caduc en l'espace de deux ans maintenant. Pourquoi ? mais non ! pas parce que la technologie est géniale et qu'elle avance vite. La vraie raison est que les logiciels et les systèmes d'exploitation sont tellement mal développés que l'on a besoin de plus en plus de puissance pour cacher la merde aux chats. La qualité a été, comme dans bon nombre de domaines, sacrifiée sur l'autel de la productivité...
- que les systèmes d'exploitation soient payants (pour Microsoft) ou posés d'emblée sur un ordinateur neuf, sans laisser un quelconque choix pour l'acheteur.
- etc ...

Alors je vous propose de poser quelques grains de sable dans la machine, de tricher au détriment des tricheurs, de cambrioler des voleurs, de vous rendre furtifs aux yeux des espions, bref de foutre un peu la

merde pour retrouver un semblant de liberté ...

B – Palette des dangers et atteintes, terminologie en vrac

Je ne suis pas sûr que cette partie soit réellement nécessaire. Cependant, je crois que cette liste vous permettra éventuellement de mieux vous repérer si vous voulez aller plus loin dans vos recherches. Bon nombre de sites mélangent tout, des termes aux mécanismes, alors jetons un œil circulaire...

Malware

Terme générique (comme badware) pour qualifier différentes formes de logiciels ou code, hostiles, intrusifs et toutes autres formes d'atteinte, destructive ou non. Cela regroupe donc, selon les cas, les virus, les spywares, etc ...

Virus (virus ;-)

Au sens strict, un virus informatique est un programme informatique écrit dans le but de se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'internet, mais aussi les disquettes, les cd-roms, les clés USB, etc. Les virus informatiques ne doivent pas être confondus avec les vers qui sont des programmes capables de se propager et de se dupliquer par leurs propres moyens sans contaminer de programme hôte. On a tendance à utiliser souvent et abusivement le mot virus pour désigner toute forme de programme malveillant (malware). Le nombre de virus réellement en circulation ne serait pas supérieur à quelque milliers, chaque éditeur d'antivirus ayant intérêt à « gonfler » le nombre de virus qu'il détecte. Les virus font souvent l'objet de fausses alertes que la rumeur propage, encombrant les messageries. Certaines d'entre elles, jouant sur l'ignorance en informatique des utilisateurs, leur font parfois détruire des éléments de système d'exploitation totalement sains.

Spyware (logiciels espions)

Un logiciel espion est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur n'en ait connaissance. Un logiciel espion est composé de trois mécanismes distincts :

- Le mécanisme d'infection, qui installe le logiciel. Ces mécanismes sont identiques à ceux des virus, des vers ou des chevaux de troie. Par exemple, l'espionnage Cydoor utilise le logiciel grand public Kazaa ;

- Le mécanisme assurant la collecte d'information. Pour le même exemple, la collecte consiste à enregistrer tout ce que l'utilisateur recherche et télécharge via le logiciel Kazaa ;

- Le mécanisme assurant la transmission à un tiers. Ce mécanisme est généralement assuré via le réseau Internet. Le tiers peut être le concepteur du programme ou une entreprise.

Le logiciel espion peut afficher des offres publicitaires, télécharger un virus, installer un cheval de troie, capturer des mots de passe en enregistrant les touches pressées au clavier (keyloggers), espionner les programmes exécutés à telle ou telle heure, ou encore espionner les sites Internet visités.

Trojans (chevaux de troie)

Un cheval de Troie est un logiciel d'apparence légitime, mais conçu pour subrepticement détourner, diffuser ou détruire des informations. Le partage des programmes introduit la problématique des chevaux de Troie. Un cheval de Troie n'est pas un virus informatique dans le sens où il ne se duplique pas par lui-même, fonction essentielle pour qu'un logiciel puisse être considéré comme un virus. Un cheval de Troie est conçu pour être dupliqué par des utilisateurs naïfs, attirés par les fonctionnalités vantées. Les chevaux de Troie servent très fréquemment à introduire une porte dérobée sur un ordinateur. L'action nuisible à l'utilisateur est alors le fait qu'un pirate informatique peut à tout moment prendre à distance (par Internet) le contrôle de l'ordinateur. Il est difficile, voire impossible de définir exactement ce qu'est un cheval de Troie, car la légitimité d'un logiciel dépend aussi du contexte dans lequel il est employé. Les portes

dérobées par exemple peuvent s'avérer utiles pour un administrateur réseau ; en revanche, dans les mains d'un pirate elles sont clairement illégitimes.

Phishing (Hameçonnage)

La technique du phishing est une technique d'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique mais la « faille humaine ». Un mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc. Sur la quantité des messages envoyés il arrive que le destinataire soit effectivement client de la banque, si c'est l'objet de la tromperie. Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.). Devinez ce qu'ils font ensuite ...

Key-logger (traceur de frappe)

Un keylogger peut être assimilé à un matériel ou à un logiciel espion qui a la particularité d'enregistrer les touches frappées sur le clavier sous certaines conditions et de les transmettre via les réseaux (analyse des sites visités, enregistrement des codes secrets et mots de passe lors de la saisie, ...). Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur !

Dans la mesure où les keyloggers enregistrent toutes les frappes de clavier, ils peuvent servir à des personnes mal intentionnées pour récupérer les mots de passe des utilisateurs du poste de travail. Cela signifie que l'utilisateur doit être particulièrement vigilant lorsqu'il utilise un ordinateur accessible par d'autres utilisateurs (poste en libre accès dans une entreprise, une école ou un lieu public tel qu'un cybercafé). Les keyloggers peuvent être soit logiciels soit matériels. Dans le premier cas il s'agit d'un processus furtif, écrivant les informations captées dans un fichier caché. Dans le cas des keyloggers matériels il s'agit alors d'un dispositif (câble ou dongle) intercalé entre la prise clavier de l'ordinateur et le clavier.

RootKit

La fonction principale d'un programme de type « rootkit » est de camoufler la mise en place d'une ou plusieurs portes qui permettent au pirate de s'introduire à nouveau au cœur de la machine sans pour autant exploiter une nouvelle fois la faille avec laquelle il a pu obtenir l'accès frauduleux (donc pas de faille, pas de rootkit !!) initial, qui serait tôt ou tard comblée. Les « rootkit » opèrent une suite de modifications, notamment au niveau des commandes système, voire du noyau (kernel). À la différence d'un virus informatique ou un ver de nouvelle génération, un « rootkit » ne se réplique pas. L'installation d'un « rootkit » nécessite des droits administrateur sur la machine, notamment à cause des modifications profondes du système qu'il engendre. Un « rootkit » ne permet pas en tant que tel de s'introduire de manière frauduleuse sur une machine saine. En revanche, certains « rootkit » permettent la collecte des mots de passe qui transitent par la machine « corrompue ». Ainsi, un « rootkit » peut indirectement donner l'accès à d'autres machines. Certains « rootkit » sont également livrés avec des collections d'« exploits », ces petits bouts de code dédiés à l'exploitation d'une faille bien déterminée. Un « rootkit » opère au niveau du noyau (la plupart du temps chargé en tant que driver) et peut donc tromper à sa guise les programmes qui sont exécutés en mode utilisateur (antivirus, firewalls). Le rootkit est souvent couplé à d'autres programmes tel qu'un sniffeur de frappe, de paquets...

Worm (vers)

Un ver informatique est un logiciel malveillant qui se reproduit sur des ordinateurs à l'aide d'Internet. Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources afin d'assurer sa reproduction. La définition d'un ver s'arrête à la manière dont il se propage de machine en machine, mais le véritable but de tels programmes peut aller au delà du simple fait de se reproduire : espionner, offrir un point d'accès caché (porte dérobée), détruire des

données, faire des dégâts, envoi de multiples requêtes vers un site internet dans le but de le saturer, etc. Les effets secondaires peuvent être aussi un ralentissement de la machine infectée, ralentissement du réseau, plantage de services ou du système, etc. Des vers écrits sous forme de script peuvent être intégrés dans un courriel ou sur une page HTML sur internet. Ils sont activés par les actions de l'utilisateur qui croit accéder à des informations lui étant destinées.

Spam (pourriel)

Courrier ou message électronique non sollicité par les destinataires.

. contient généralement de la publicité. Les produits les plus vantés sont les services pornographiques, les médicaments, le crédit financier, les casinos en ligne, les montres de contrefaçon, les diplômes falsifiés et les logiciels craqués.

. envoient également des propositions prétendant pouvoir vous enrichir rapidement : travail à domicile, conseil d'achat de petites actions.

. Les lettres en chaînes peuvent aussi être qualifiées de pourriel.

. Il s'agit de messages d'entreprises ignorantes de la Netiquette qui y voient un moyen peu coûteux d'assurer leur promotion.

. Enfin la dernière forme de pourriel, l'hameçonnage

En France, 95 % des messages échangés courant décembre 2006 étaient des spams et a du atteindre 99 % courant 2007.

BackDoors (portes dérobées)

Une porte dérobée peut être introduite soit par le développeur du logiciel, soit par un tiers, typiquement un pirate informatique. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle (par contournement de l'authentification). Enfin, selon l'étendue des droits que le système d'exploitation donne au logiciel contenant la porte dérobée, le contrôle peut s'étendre à l'ensemble des opérations de l'ordinateur.

Wabbits

C'est un autre type de logiciels malveillants se reproduisant très rapidement. Contrairement aux virus, ils n'infectent pas les programmes ni les documents. Contrairement aux vers, ils ne se propagent pas par les réseaux. Un hijacker modifie les réglages du navigateur en utilisant une page web contenant un contrôle ActiveX ou du JavaScript pour rediriger les prochaines utilisations vers un site de son choix. Cet terme s'applique aussi aux programmes qui se multiplient à haute fréquence en local et finissent par rendre l'ordinateur inutilisable, car saturé. Ce type d'atteinte est appelé « Deny Of Services » ou DOS.

Exploits

Exploitation d'une faille de sécurité d'un système d'exploitation ou d'une application. Cette exploitation peut permettre la prise en main distante d'une machine.

Hoaks ou hoax

Canulars par email ou informations sur sites destinés à faire circuler un mail ou à faire faire des bêtises sur son ordinateur en croyant éliminer un virus, ou au contraire faire croire qu'un programme corrompu est sain. Le plus dramatique reste les fausses chaînes qui réduisent à néant les vrais messages de solidarité.

Traces diverses

Sans parler d'atteintes, cette fois-ci, tout ce que vous faites laisse des traces, soyez en sûrs. Chez vous comme dans votre entreprise, en regardant dans votre machine, il est possible de savoir vraiment beaucoup de choses. Puis lorsque vous sortez sur Internet, une fois encore il est possible de tout tracer.

C – Un peu de recul ...

Il ne faut pas tomber non plus dans la parano. Il existe beaucoup de sources de problèmes sur internet mais une sorte de « bonne pratique » permet de s'en sortir en général très bien. De plus, les plus grands dangers ne sont pas forcément des attaques volontaires mais un comportement normal de certains programmes qui doivent être corrigés par l'éducation technique, c'est tout.

Je parlerais des PC sous Windows, car malheureusement, ils sont encore majoritaires. Avec un pc sous Linux (Suse Linux Desktop ou Ubuntu sont parmi les plus évolués pour des utilisateurs standards) bien qu'il y ait des points communs, les traces et les dangers sont plus faibles.

Les bonnes habitudes données ci-dessous tentent d'être exhaustives (sans y parvenir, sans doutes) et seront développées plus précisément dans les chapitres suivants. Je continue sans doutes à faire des erreurs, aussi, ne voyez pas ce document comme une référence...

Traces laissées localement

Lorsque j'ouvre une application, je laisse une trace. Lorsque j'ouvre un document avec cette application, je laisse une trace. Lorsque je surf sur internet, certains sites récupèrent des données de mon ordinateur (essayez sur <http://www.anonymat.org/vostraces/index.php>). Ils utilisent ou pas ces données provenant simplement de mon navigateur. Ils peuvent aussi stocker ces données dans MON ordinateur grâce à un cookie. Ils tenteront à la prochaine visite de récupérer ce cookie pour me présenter des informations orientées vers mes préférences de surf (et les pubs qui vont avec). Certains sites peuvent aussi lancer des applications à distance par le biais du langage Java, des javascript ou des activeX. Si j'autorise mon navigateur à exécuter ces programmes, ceux-ci peuvent ramener plus d'informations, voir déposer un malware (si j'autorise l'installation de programmes ou d'utilitaires par les ActiveX par exemple: do you want to install and run ...).

Quand j'arrive sur un site, cookie ou pas, il est possible de récupérer l'adresse du site depuis lequel je viens (referer).

Mon navigateur garde traces des sites sur lesquels je suis allé, des pages que j'ai visitées, des fichiers que j'ai téléchargés, des champs de formulaires que j'ai remplis, des mots de passe que j'ai entrés et de ces fameux cookies.

Si je n'efface pas mes mots de passe ou mes cookies, un utilisateur suivant sur le même poste peut très bien utiliser mon email ou mes sites sans devoir s'authentifier si le navigateur est resté ouvert, et si j'ai enregistré mon mot de passe, il peut le faire même si le navigateur a été fermé.

Lorsque j'utilise ma messagerie pour ramener mes messages en local (messageries POP3 ou IMPA4, comme outlook express ou Thunderbird), ceux-ci passent en clair la plupart du temps, sur internet (mots de passe y compris) et sont stockés localement.

Lorsque j'utilise des outils de chat en ligne (messenger ou autres), des historiques de mes contacts ou de mes conversations sont stockés localement.

J'efface un fichier sur mon disque, il passe dans la poubelle. Je vide la poubelle, le fichier reste tout de même présent et exploitable .

Traces sur le net

A chaque fois que je surfe sur internet, quelque soit mon activité, j'ai besoin d'une adresse unique. Dans une entreprise cette adresse est contrôlée (fixe ou dynamique) et chez vous, en général, elle est attribuée temporairement par votre fournisseur d'accès (changement tous les un ou deux jours, cela dépend). Si vous voulez héberger un site qui doit être atteint depuis l'extérieur, alors vous devez avoir une adresse unique et stable (c'est plus cher).

Du pont de vue technique, il s'agit d'une adresse IP qui correspond à un nom de machine (host). Dans la plupart des cas, avec une liaison ADSL, cette adresse est allouée durant un ou deux jours par exemple et un nom de host lui est aussi donné (AMontpellier-104-1-4-220.w80-11.abo.wanadoo.fr par exemple).

Quoiqu'il en soit, cette adresse permet de retracer exactement votre parcours et éventuellement remonter jusqu'à vous (vous voyez déjà qu'en lisant simplement le nom de host, on peut savoir vers quel fournisseur d'accès vous êtes abonné et proche de quelle ville). Le fournisseur d'accès lui, garde toutes les traces de vos adresses (pendant deux ans je crois) et a les moyens techniques de savoir où vous allez et ce que

vous faites (ils n'ont pas le droit de le faire, ni le temps) mais peuvent sous commission rogatoire, fournir ces renseignements à la police.

Enfin en arrivant sur un site, ce site peut récupérer pas mal d'informations (voir plus haut).

Ne vous laissez pas abuser en utilisant votre ordinateur

Il y a un certain nombre de bonnes habitudes à prendre pour limiter les risques d'attaques ou de pollution:

- avoir un bon anti-virus et le tenir à jour
- avoir un bon anti-spyware
- avoir un firewall en mode apprentissage
- surveiller les programmes qui tournent sur votre machine
- ne jamais installer un programme depuis des sites "douteux" ou en tous cas passer le fichier d'installation à l'anti-virus immédiatement
- ne pas autoriser le javascript et les activeX sur votre navigateur
- favoriser une messagerie par web plutôt que par des clients de type POP3 (comme outlook express ou thunderbird).
- tenir votre système à jour
- configurer comme il faut votre routeur ADSL (firewall et routeur)

Il y a aussi un certain nombre de réflexes permettant d'augmenter votre anonymat et votre vie privée

- avoir un compte messagerie gratuit (yahoo mail, freesurf,...) avec un faux nom ou sans nom et sans aucune information. Utiliser ce compte pour tout ce qui sort du professionnel ou du relationnel avec des amis identifiés et proches.

- ne jamais répondre aux messages de personnes que vous n'arrivez pas identifier.
- ne jamais relayer des messages de chaîne (hoax).
- ne laisser pas un programme sortir sur internet pour aller sur le site du fournisseur pour soi disant vérifier des mises à jour (windows est aussi spécialisé là-dedans).
- ne pas laisser des outils de mises à jour automatiques démarrer automatiquement. Vous ferez vos mises à jour tout seul.
- si vous voulez essayer un programme, ne prenez pas des programmes d'essai soixante jours ou autres. Obtenez le d'une autre manière, testez le et décidez vous ensuite.
- installez des programmes d'anonymat pour ceux qui veulent aller plus loin
- préférer une adresse dynamique à une adresse fixe, même pour ceux qui hébergent un site
- protégez votre réseau wifi si vous habitez dans une zone habitée

Protection de la machine et de son fonctionnement

Comme pour le reste, la santé et le bon fonctionnement de votre ordinateur sont améliorés par de bonnes pratiques, comme :

- limiter les programmes qui démarrent automatiquement à leur minimum (normalement 4 ou 5)
- lancer des nettoyeurs de registres ou de fichiers temporaires
- désinstaller les programmes inutiles ou caducs
- défragmenter votre disque régulièrement
- vider votre poubelle
- faire des scans complets pour les anti-virus et les anti-spyware une fois par mois
- nettoyer les caches des navigateurs et des messageries instantanées
- achetez un disque dur USB et stockez-y tous vos fichiers de données précieux. Profitez en pour y mettre vos gros fichiers (vidéo, sons, programmes d'installation, etc...), cela permettra à votre ordinateur original de souffler
- si vous utilisez votre pc, de temps en temps, pour écouter de la musique ou voir des films, ou si vous laissez vos enfants l'utiliser comme cela, utilisez des programmes spécialisés pour ce rôle sans rien installer réellement...

D - Elimination des traces localement

Mettons nous pour simplifier dans la situation où nous avons aucune connexion à Internet

Les traces dans ce cadre ne sont pas à proprement parler des malware, mais plus d'effets de bord. Sous Windows (comme sous Linux partiellement d'ailleurs), chaque utilisation d'un programme va laisser des traces qu'il est aisé de retrouver (et ainsi de savoir ce que l'utilisateur a fait).

Traces des lancements

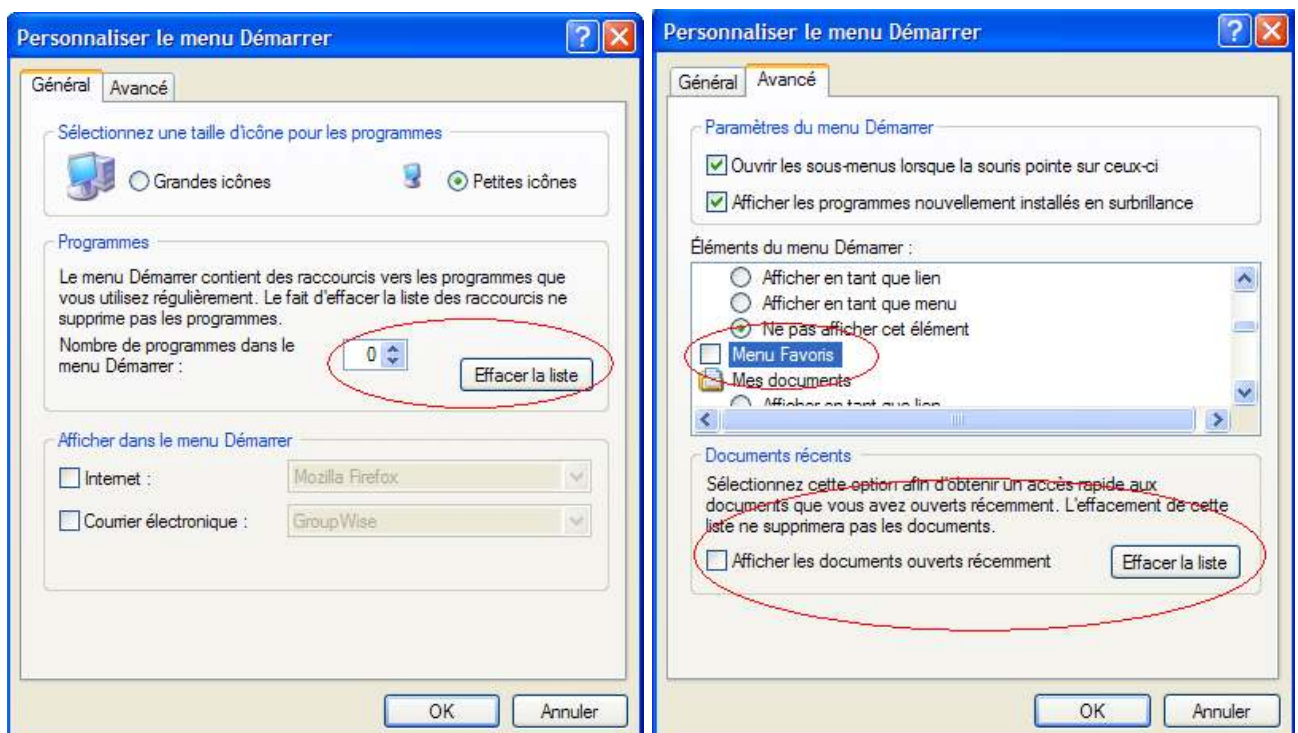
> Un programme laisse une trace de son utilisation (MFU : Most frequently Used)

- il la laisse dans le menu démarrer (dans le dossier des programmes les plus utilisés)

- il la laisse dans les registres

Pour éliminer ces traces, aller dans menu démarrer -> cliquer droit dans le bandeau du haut -> Propriétés -> onglet menu démarrer -> personnaliser -> onglet général -> dans Programmes, mettre le chiffre à 0 et effacer la liste.

Pendant que vous y êtes, cliquer sur l'onglet Avancé -> Décocher les boîtes indiquées sur a seconde figure ci-dessous + celle des Favoris Réseau dans le liste.



> Un programme laisse une trace car Windows garde les icones des programmes lancés (ShellNoramMUI).

Pour toutes ces traces, vous pouvez utiliser l'utilitaire **MRU-Blaster** (voir les liens en base de page)

Traces de fonctionnements

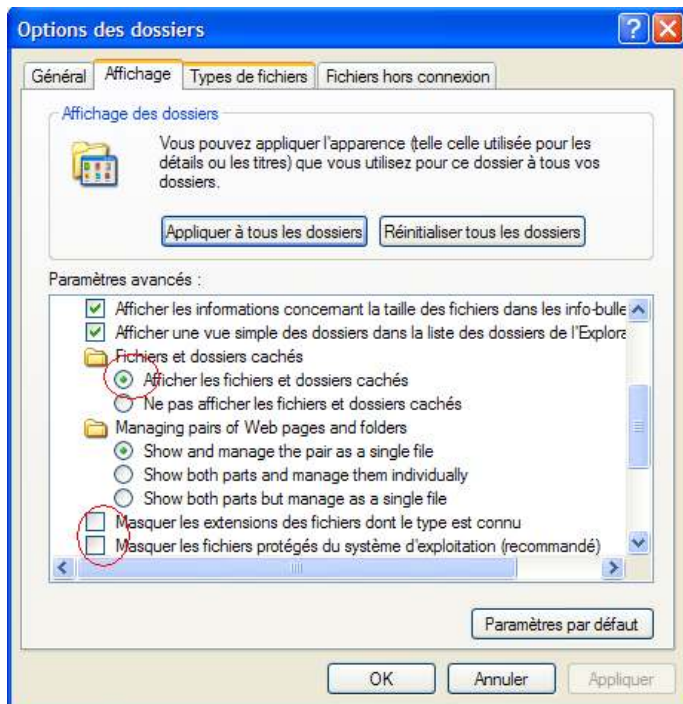
> Un programme laisse une trace des fichiers qu'il a manipulés (MRU Most Recently Used). Un simple lancement du programme et vous retrouverez cette liste. Elle est aussi dans les registres.

Pour ces traces, vous pouvez utiliser l'utilitaire **MRU-Blaster** (voir les liens en base de page)

> Un programme laisse un trace car windows garde les fichiers temporaires d'execution

Pour voir ces répertoires (en tous cas le premier) je vous conseille de configurer l'explorateur pour les

laisser apparaître. Lancer l'explorateur, aller sous Outils, Options et décocher comme sur l'image:



Faites gaffe car maintenant vous pourrez effacer des fichiers systèmes, donc tenez-vous en à ce que vous maîtrisez. Une fois cela fait, vous devez aller dans ces deux répertoires, en tous cas:

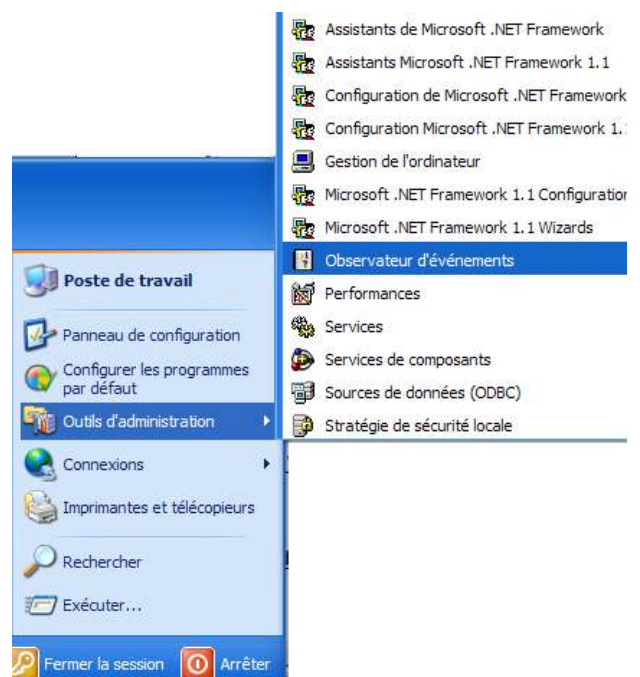
C:\Documents and Settings\C:\WINDOWS\Temp

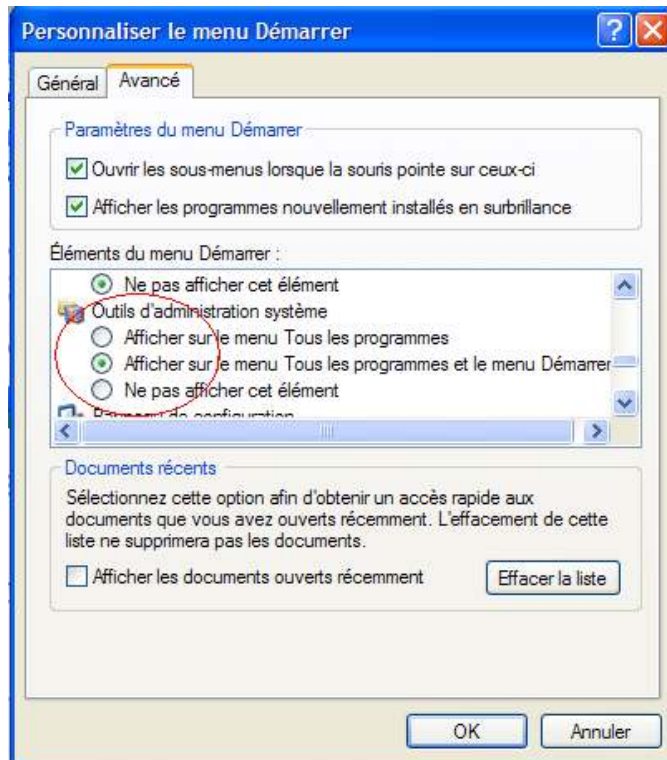
Vous fermez toutes les applications courantes et vous effacez définitivement TOUS les fichiers de ces répertoires. Il est possible que le système gueule en disant que certains de ces fichiers sont utilisés. Répondre ok.

Note: pour effacer définitivement (c'est à dire que rien n'ira dans la poubelle mais sera réellement effacé), vous pouvez taper <Shift><Delete>, ou <⇧><Supprimer> au lieu de Delete. Sinon effacer comme vous voulez et vider ensuite la Corbeille.

> Un programme peut laisser une trace dans les event logs (Evenements).

Pour jeter un œil sur ces événements, il faut activer le menu Outils d'Administration de windows. Cela se fait par la configuration du Menu Demarrer , comme sur la figure ci-dessous.





Dans cet outil, vous trouverez à gauche le type d'évènements et à droite les évènements pour cette catégorie. Pour effacer tous les évènements des applicatifs (impossible je crois d'en effacer que certains), allez dans une fenêtre de gauche et cliquez droit sur Applications. Sélectionner "*Effacer tous les évènements*" (vous pouvez aussi vous amuser à configurer cette partie en sélectionnant Propriétés).

Traces des fichiers effacés

Lorsque vous effacez des fichiers (avec <Delete>), ils passent dans la poubelle. Vous pouvez soit vider la poubelle, soit faire <Shift><Delete> pour ne pas les placer dans la Corbeille. Mais pire que cela, un fichier réellement effacé sur le disque reste en fait présent pour une question de rémanence magnétique des disques (en plus des systèmes de fichiers qui n'effacent que l'entrée

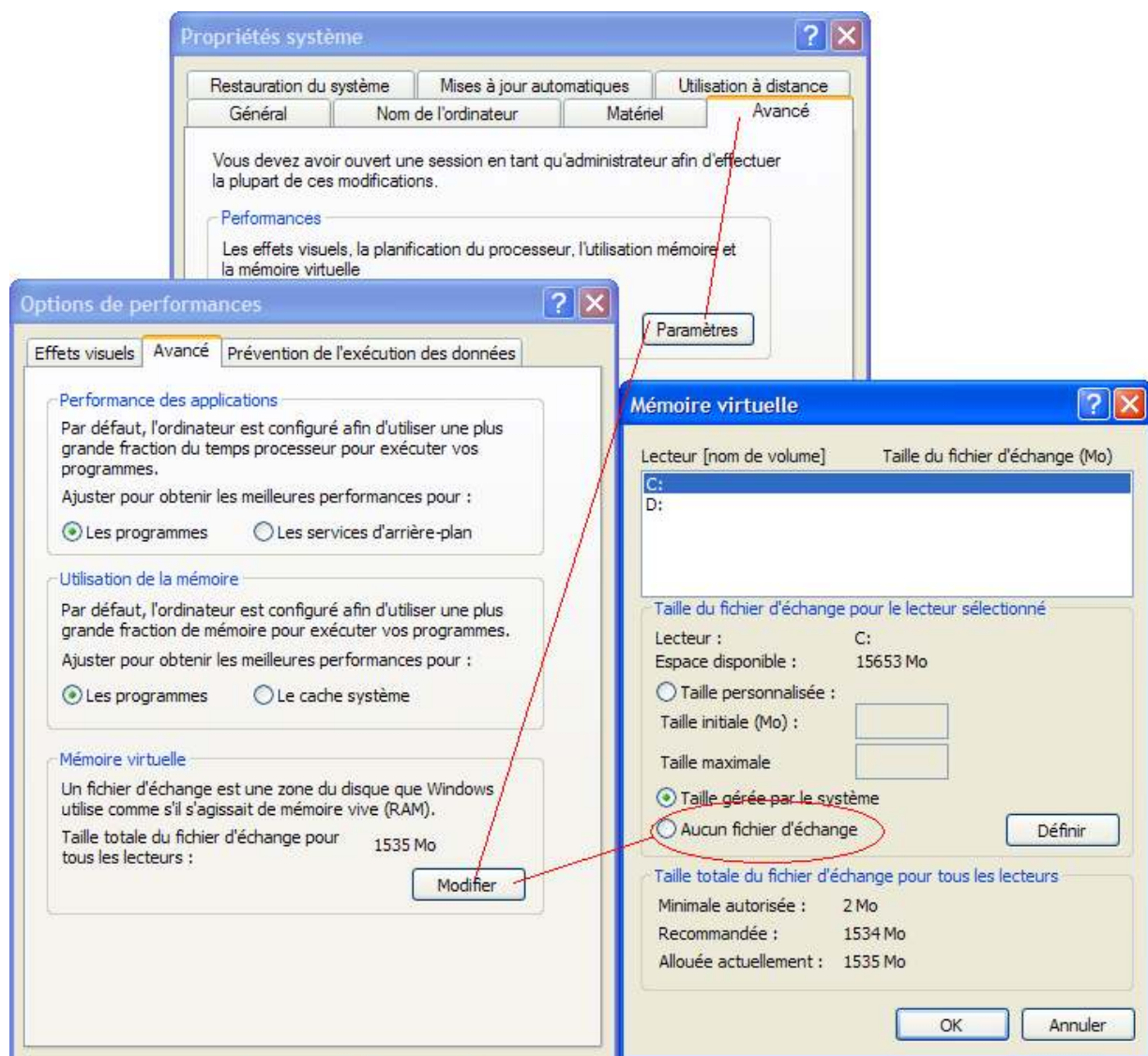
du fichier mais pas les données du fichier).

Pour ces traces, utiliser l'utilitaire **Eraser** (disponible dans les liens en bas de page).

Traces dans le fichier Swap

Il s'agit d'un fichier d'échange vital pour windows qui permet de soulager la mémoire vive (RAM). Ce fichier est réutilisé de démarrages en démarrages et finit donc pas contenir toutes sortes de traces d'utilisation. Certains utilitaires prétendent effacer le contenu de ce fichier mais ce n'est pas vrai. Windows le tient en accès exclusif et ne permet aucune manipulation. La seule manière de procéder est la suivante:

Désactiver le swap: aller dans menu démarrer -> bouton droit sur Poste de Travail puis suivez la figure ci-dessous pour désactiver le swap.



Une fois que cela est fait, redémarrer l'ordinateur.

Utilisez alors l'utilitaire **Eraser** (disponible dans les liens en bas de page) et choisissez d'effacer le "Unused Disk Space" (espace libre).

Une fois que cela est fait, reconfigurer le fichier d'échange (swap) sur "Taille gérée par le système" et redémarrer.

Envoi de données non demandées

Des mouchards envoient des données régulièrement sur Internet. Ne pas les autoriser à le faire. Voir plus bas "Les bonnes habitudes pour votre ordinateur".

Traces d'installation

La désinstallation des programmes est généralement pas tellement efficace, voire minable. Une opération manuelle est en générale nécessaire ensuite. Voir plus bas "les bonnes habitudes pour votre ordinateur".

L'utilitaire **EasyCleaner** est aussi un excellent moyen d'effectuer l'effacement de certaines de ces traces et d'autres. Voir plus bas "les bonnes habitudes pour votre ordinateur".

E - Elimination des traces en surfant

Soyons plus direct pour ce chapitre. Arrêter d'utiliser Internet Explorer et basculer sur FireFox (2.0.0.12 dans notre exemple, aller sous Outils -> Options). Il y a beaucoup plus d'options concernant la vie privée et d'options de configuration (cachées mais disponibles). Enfin il existe un grand nombre de plug-ins (ou greffons ou extensions) qui peuvent être utiles.

Traces des pages que vous allez visiter

Elles sont gardées et stockées dans le cache du navigateur. Le but est de limiter le trafic en retrouvant la page en local plutôt que sur le site distant. Certains champs de pages permettent de savoir si une mise à jour de la page a été faite depuis le moment où elle a été stockée en local. Aujourd'hui le caching local est bien moins intéressant et ceci pour deux raisons: la vitesse des lignes a augmenté, le plus grand nombre de site est maintenant dynamique et l'avènement du WEB 2.0 ou WEB 3.0 va amplifier ce phénomène.

Virez le cache !!



Traces sur l'historique de navigation et les téléchargements

L'historique des pages que vous visitez est conservé ainsi que les fichiers que vous avez téléchargés.

Virez l'historique !! (voir image plus bas)

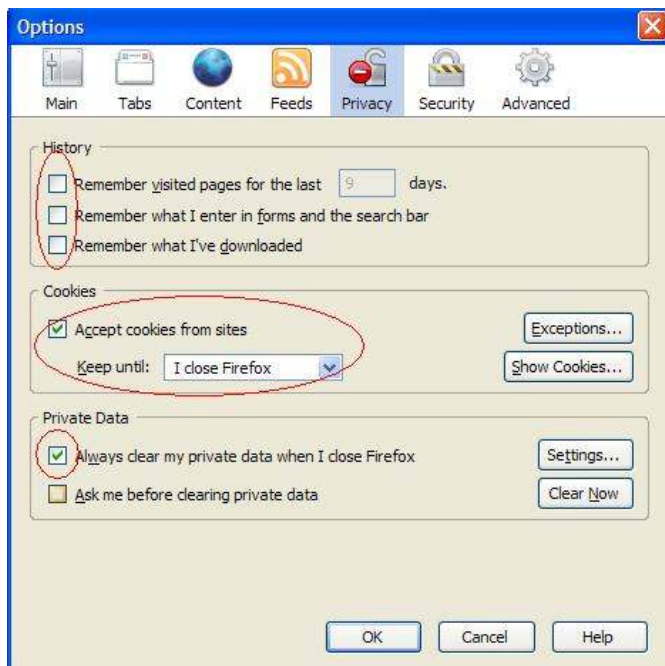
Traces sur les champs que vous avez remplis

Lorsque vous remplissez des champs de formulaire web, le navigateur garde les traces de ces données entrées pour vous permettre de faire une saisie semi-automatique par la suite.

Virez les entrées de formulaire !! (voir image plus bas)

Traces que les sites ont déposées dans votre navigateur

Ces fameux cookies expliqués plus haut dans l'article. Je vous conseille de les autoriser (sinon certains sites refusent de fonctionner) **mais de les virer en quittant FireFox** (voir image plus bas)



Traces sur les mots de passe que vous avez entrez

Est-ce nécessaire d'en dire plus ?

Virez les mots de passe !!

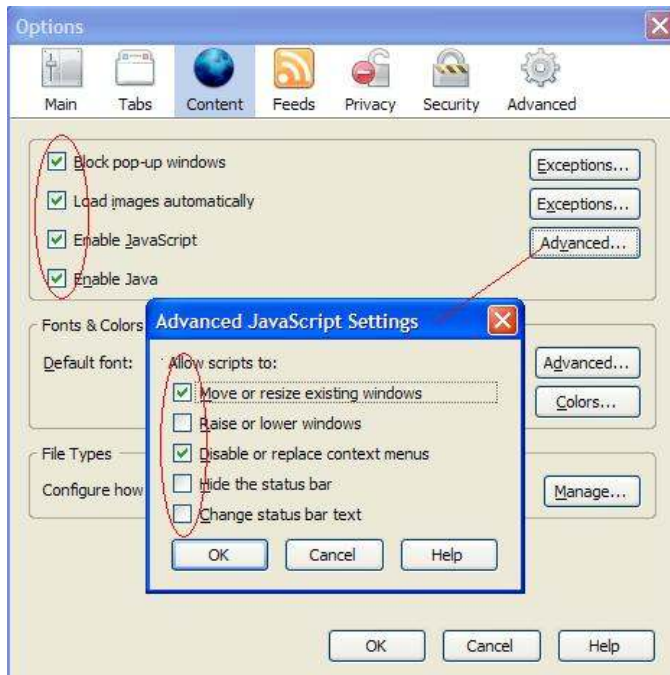


Malware déposés par certains sites

Certains vont dire que Firefox fonctionne encore mal avec certains sites. Ouais, sans doutes, mais d'une part ils deviennent vraiment très rares et d'autre part, quand c'est le cas, envoyez un message au WebMaster en lui demandant de se reveiller et de rendre son site compatible !!

Firefox accepte l'utilisation de modules qui étendent les fonctionnalités de base du navigateur (<https://addons.mozilla.org/fr/firefox/browse/type:7>). Du coup, Java et les javascripts sont utilisables, mais pas les activeX (il y a cependant un module qui le permet). Bon, ben tant mieux !! C'est pas de genre de procédés et par celui du jeu avec les fenêtres redimensionnables et les fenêtres popup que l'on se fait envahir de saletés.

L'exécution de certains type de fichier est configurable ici :



Bloquer les Popups, Permettre JavaScript mais en maîtrisant ce qui est permis, et autoriser ou pas Java (selon les sites que vous allez visiter).

Je vous conseille aussi l'utilisation du **module NoScript** (voir les liens en fin d'article)

Le Referer

Lorsque dans un site un lien pointe vers une page d'un autre site, le site cible en question peut récupérer l'URL du site original (hum... c'est clair ?). Il est possible de considérer cela comme une atteinte à la vie privée.

Faites un test et cliquez sur ce lien ici -> <http://www.stardrifter.org/cgi-bin/ref.cgi>

Vous avez vu ? Bon, supprimons cela même si certains sites ne vont pas être trop contents (des sites l'utilisent à des fins de sécurité et d'autres pour rembourser les sites d'origine !!)

Ouvrez un second onglet dans Firefox et tapez: **about:config**

Localisez la ligne **network.http.sendRefererHeader**

Double cliquez sur cette ligne et entrez la valeur **0** (mémorisez au cas où la valeur précédente, disons 2)

Refaites le même test plus haut... et voilà...

Certaines précautions pour votre sécurité

Une bonne configuration des plug-ins Java, du javascript et le blocage des ActiveX par un firewall est déjà

très bien concernant la sécurité.

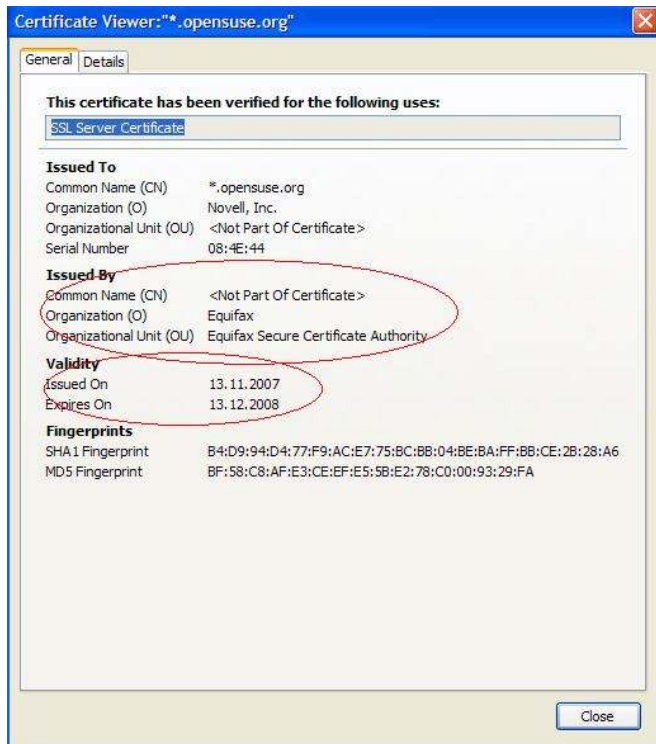
Cependant, il y a certaines précautions supplémentaires possibles surtout pour ceux qui veulent payer en ligne. Il faut absolument être vigilant et n'admettre aucune exception, sur les points suivants:

- si un mot de passe est demandé (ou numero de carte, etc...), la connexion doit être sécurisée (cadenas dans la barre du bas de FireFox)



- vous devez absolument renoncer si votre navigateur annonce un problème avec le certificat. Les certificats peuvent avoir plusieurs problèmes:

- 1) ils ne sont plus valides
- 2) ils ont été validés par le site émetteur lui-même et non par une autorité reconnue par votre navigateur
- 3) ils n'ont pas été faits pour le serveur sur lequel vous êtes connectés



Enfin, un module très sympa de FireFox vous permet de vérifier où est situé le serveur sur lequel vous connecté. Il s'agit du module **Shazou** (voir la liste des liens). Je l'utilise de temps en temps pour voir si le serveur est en France (on découvre des choses formidables, parfois , hé hé hé...). Tenez voici une localisation d'un site d'investissement français qui se trouve en fait en Allemagne. De plus vous avez des infos sur les personnes qui ont déposé le nom du site internet dans le bottin WhoIS.

SHAZOU
we know WHERE...
your server is

Plan Satellite Mixte

Your Shazou is up to date Submit as a potential Phishing Site

Geop Data: Server Location	Whois Lookup: Domain Owner
Server: www.cortalconsors.fr IP Address: 194.150.80.23 Organization: CortalConsorts SA, Zweigniederlassung Deutschland Country: Germany City, State: Benzenhof, 02	Organization Name: RIPE Network Coordination Centre Address: P.O. Box 10096 City, State: Amsterdam, Postal Code: 1001EB Country: NL

Plot Whois

Notes:

- mettez à jour régulièrement votre navigateur FireFox et les modules de sécurité que vous avez installé
- pour Internet Explorer, le logiciel EasyCleaner vide aussi les données privées
- pour les ActiveX, les popups et autres saloperies, un bon firewall comporte souvent ce genre de fonctionnalités qu'il est intéressant de laisser en plus du reste.

Pour tester si vous êtes protégés contre les Popups, vous pouvez aller sur:

<http://www.proxomitron.info/tests/index.html>

Pour tester la sécurité de votre navigateur, vous pouvez aller sur le site :

<http://www.jasons-toolbox.com/BrowserSecurity/>

F - Messagerie

Les attaques par les messageries sont sans doutes les plus répandues. Elles sont de trois sortes principalement, les virus, le spam et le phishing.

Pour les virus, le but est de poser un malware sur le disque qui va perturber le système, le crasher ou utiliser le carnet d'adresses pour envoyer des messages sous le nom du propriétaire aux destinataires, propageant ainsi le virus. Ces virus sont transmis par des pièces jointes mais aussi dans le corps du message lui-même (html, etc...). Les pièces jointes infectées peuvent être de n'importe quel type (exécutable, html, etc ... même un format d'image). Ces virus infectent votre machine par des trous de sécurité de votre système de messagerie ou en abusant de votre curiosité (on se rapproche du spam).

Pour le spam, il s'agit de courrier non sollicité qui va contenir toute sorte d'informations, allant de la publicité aux virus en passant par des hoax.

Enfin le phishing va tenter de vous demandez de vous connecter quelque part en prétendant être votre banque, etc...

Que l'on soit d'accord tout de suite, si vous voulez éviter la plupart des ennuis avec votre messagerie, en étant puriste, il y a **quatre règles d'or** que vous pouvez suivre:

Règle 1 - utiliser une messagerie web (freesurf, yahoo mail ou autres) et pas un client de messagerie comme outlook, outlook express ou thunderbird. Il est alors plus difficile qu'un virus s'exécute sur votre poste si votre navigateur est bien protégé (vois chapitre précédent). Le vol du carnet d'adresse est dans ce cas pratiquement impossible.

Règle 2 - n'ouvrez jamais un message qui vient de quelqu'un que vous n'arrivez pas à formellement identifier. Cette technique ne fait que limiter les dégâts car comme dit plus haut, certains virus utilisent le carnet d'adresses et l'identité de vos correspondants pour se déployer.

Règle 3 - gardez une adresse email privée que vous n'utilisez absolument jamais pour recevoir des renseignements ou vous inscrire sur des forums, etc... Cette adresse ne doit servir qu'à des messages privés à des personnes bien ciblées.

Règle 4 - lorsque vous donnez votre email public dans des forums ou autre, donnez la sous une forme volontairement fausse. Exemple: votre adresse réelle est jean.dupont@monmail.fr, donnez alors votre adresse sous : jean<point>dupount<AT>monmail<point>fr. DE cette manière les robots et les aspirateurs à email des spammeurs, vont avaler une adresse qui ne sera pas utilisable, alors qu'un humain va comprendre le truc. Si vraiment le site n'accepte pas cela (il attend un vrai signe @) alors vous pouvez aussi décaler l'adresse, comme par exemple: jean.dupont.monmail@fr .

Si malgré tout vous utilisez une messagerie locale, favorisez ThunderBird par rapport à Outlook et tenez cette messagerie à jour.

Il n'empêche que tout cela ne vous abstiendra pas d'avoir un très bon anti-virus et anti-spam sur votre machine pour vous protéger. **Voir chapitre "Protégez votre ordinateur gratuitement"**.

Enfin, pour certains messages que nous qualifierons de privés ou secrets, il est nécessaire de se rendre compte qu'avec la plupart des messageries disponibles, hors messageries professionnelles dans l'entreprise (et encore...), le contenu des messages transite en clair. Si vous voulez crypter le contenu d'un message, vous pouvez alors utiliser des outils GPG (Gnu Privacy Guard) qui permettent l'utilisation de clés (de type PGP - Pretty Good Privacy) nécessaires à l'encryption des messages.

En admettant que vous utilisiez Thunderbird (bravo !) sur Windows (tant pis !), alors il vous faut:

- le portage de GPG sous Windows : Winpt - <http://winpt.sourceforge.net/fr/download.php>

- le plug-in PGP pour Thunderbird : Enigmail - <http://enigmail.mozdev.org/download/index.php>

Et un petit tutoriel pour ceux qui sont paumés :

http://cd.eitic.net/logiciels/winpt/tuto_enigmail.pdf

Vous aurez alors des fonctionnalités supplémentaires dans Thunderbird qui vous permettront d'encrypter des messages pour les envoyer à certains de vos contacts.

G – Les bonnes habitudes pour votre ordinateur

Quand je parle de bonnes habitudes, cela concerne la "**santé**" de votre ordinateur. Je ne parle plus de sécurité (voir plus bas "**Protégez votre ordinateur efficacement**").

Il y a quelque chose de totalement évident avec les ordinateurs sous Windows (je vous conseille sérieusement d'envisager le passage sous Linux mais je n'y reviendrais plus). Au bout de un ou deux ans, il devient plus lent, moins stable et ce sans même avoir jamais installé quoique ce soit.

Je ne suis pas un expert Microsoft, mais je crois que tout simplement que la taille du registre augmente irrémédiablement, le nombre de fichiers aussi, le nombre de répertoires aussi, l'organisation du système de fichiers sur votre disque devient bordélique, vous êtes envahis par des spywares, des programmes qui se lancent au démarrage, etc ...

Si vous êtes sérieux et que vous pratiquez le genre de séances de revitalisation qui suit, je peux vous assurer que ce ne sera plus le cas.

Disques USB

Très intéressants pour y sauvegarder des gros fichiers (films, musique, programmes d'installation, fichiers de données, etc...). Facilement transportables, ils peuvent passer d'un ordinateur à un autre.

Dans notre discussion, leur intérêt est de permettre de soulager le système de fichiers de notre pc principal. Windows et le système de fichier NTFS aiment garder suffisamment d'espace disque libre et un nombre restreint de fichiers et de répertoires. De plus, avec un espace disque utilisé réduit, cela vous permet de désactiver deux fonctionnalités qui pénalisent les performances: l'indexation et la compression.

Pour cela depuis l'explorateur, faites bouton droit sur votre lecteur (C: en général) et **décocher** les deux cases:

Compresser le lecteur ...

Autoriser l'indexation -> appliquer cela à tous les dossiers et sous-dossiers

Programmes, Fichiers et services inutiles

Programmes inutiles

Au bout de quelques mois, vous ne vous souviendrez plus de tout ce que vous avez installé. Aussi, de temps en temps, c'est intéressant d'aller dans la liste des programmes installés et de faire du ménage.

Allez dans: *Menu Démarrer -> Panneau de Configuration -> Ajout/Suppression de Programmes*

Tout devrait bien se passer, mais il arrive que :

- le système doit redémarrer (il doit nettoyer des fichiers tenus par Windows)
- il est mal désinstallé. Il faut alors intervenir manuellement (voir plus bas)
- il ne s'efface pas de la liste : **je vous conseille d'utiliser EasyCleaner - Ajout/Suppression (disponible dans les liens en bas de page).**
- il dit qu'il ne peut pas désinstaller (le fichier uninstall.exe a été effacé). Il faut alors intervenir manuellement (voir plus bas)

Programmes qui se chargent au démarrage

C'est la mode. La moindre merde d'imprimante vient avec une ribambelle de trucs qui se chargent. Adobe vient aussi avec un tas de trucs qui démarrent tout seul. Tous les logiciels de mise à jour sont chargés continuellement en mémoire. Toutes les saloperies Office, companions, quick time, real player, etc...

s'installent avec un cortège de bouts de programmes lancés automatiquement. Vous les voyez pour la plupart dans la liste d'icônes en bas à droite de votre écran. Bon, faut faire du ménage...

En étant psychorigide, je dirais que seul l'anti-virus devrait apparaître au démarrage, rien d'autre. Mais bon

...

Ces programmes sont soit présents dans le dossier Démarrage du menu Démarrer mais le plus souvent dans les clés de registre. Le meilleur truc est de passer la souris sur chacune de ces icônes et

normalement une info bulle apparaît vous disant à quoi cela sert. Une fois cela fait, **je vous conseille d'utiliser EasyCleaner -> Démarrage (disponible dans les liens en bas de page).**

Services inutiles

Et oui, sous Windows, il y a beaucoup de choses qui ne servent à rien et qui tournent sans arrêt sur votre machine. En général cela ne consomme pas trop de ressources (CPU ou RAM) mais avec le nombre...ben ...

Il faut donc arrêter ces services. Pour cela, il faut d'abord faire apparaître le menu Outils d'Administration (pour la marche à suivre, aller chapitre D -> Traces de Fonctionnement -> Event log).

Dans ce menu Outils d'Administration, choisissez Services. Dans cette liste vous voyez tout ce qui est démarré automatiquement sur votre machine. Pour chaque service que vous voulez modifier, double cliquer dessus et de là vous pourrez (il faut faire les deux):

- L'arrêter là maintenant.
- Ne pas le démarrer Automatiquement, mais manuellement ou le désactivé complètement, pour le prochain démarrage de votre machine.

Reste à savoir ce que vous pouvez arrêter... aie moins drôle ...

Sur ce site, vous avez tous les renseignements en Français sur chaque processus :
<http://www.gsiteg.com/processus.php>

Ici quelques idées pour arrêter certains services peuvent être inutiles pour vous :
<http://www.pcastuces.com/pratique/windows/services/page4.htm>
<http://www.coolxp.fr/tutorial/services/services.htm>

Soulagement de la mémoire:

Deux petits trucs:

<http://www.zonewindows.com/astuce36.php>

<http://www.zonewindows.com/astuce15.php>

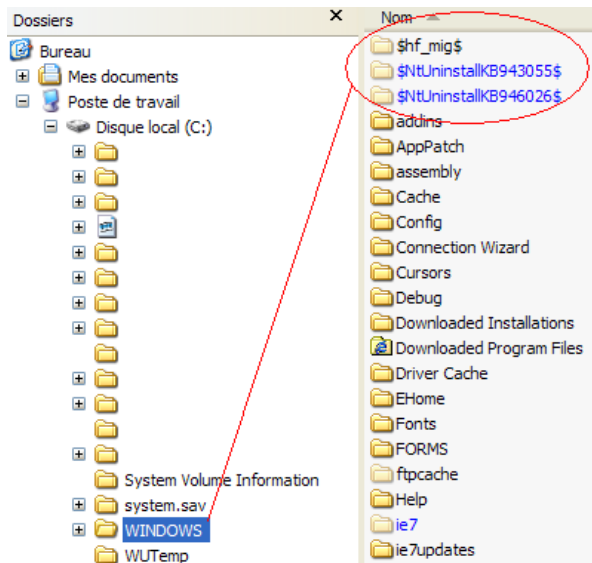
Optimisation plus complète de Windows :

<http://www.tuto-underground.net/tutorial-225-optimiser-son-systeme-windows-tutoriels-tutoriaux-tuto-tutorial-didacticiel-gratuit.html>

Fichiers inutiles

Je vous conseille d'utiliser **EasyCleaner - Inutiles** (disponible dans les liens en bas de page).
Ou plus efficace encore mais plus dangereux dans les options **CCleaner** (disponible dans les liens en bas de page).

a) Lorsque vous faites des mises à jour (services pack, patch, etc...) le système garde des traces de ces fichiers. Après une petite semaine, vous pouvez les éliminer. Ils se trouvent comme indiqué dans l'image ci-dessous:



b) Quelques autres pour gratter un peu plus (certains sont déjà inclus dans les outils précédents)

Fichier **C:\WINDOWS\0** (le chiffre)

Fichier **C:\WINDOWS\clock.avi**

Aller : Menu Démarrer/rechercher/fichiers ou dossiers et rechercher les fichiers :

***.tmp**

***.bak**

pour ces extensions là, ne prenez que les fichiers plus vieux que 1 jour (pour éviter de supprimer des

fichiers utilisés actuellement)

*.chk (fichiers scandisk) supprimer les fichiers + de 5 jours

*.log (fichiers journaux) supprimer les plus anciens

*.old (anciennes versions de fichier remplacées par de nouvelles)

*.gid (générés pour les aides en ligne)

*.bad (fichiers défaillants)

*.prv (fichiers journaux créés par des initialisations de windows antérieures)

*.wbk (fichiers de sauvegarde word)

~\$.doc (fichier word temporaire) : supprimer tout

*.obj, *.pch, *.pdb, *.ilk, *.exp, *.idb, *.ncb (fichiers intermédiaires de compilateur)

.td\$. (*.tda, *.tdb, etc.) sauf si on utilise un gestionnaire de base de données (agenda, etc.)

~.*

~\$.* (fichiers d'installation provisoires)

*.dmp (fichiers memory.dmp et parfois user.dmp), Créés lors des plantages sérieux (écrans bleus) ils ne servent que pour l'envoi d'analyses chez Microsoft

c) Tous les fichiers contenus dans le dossier **C:\WINDOWS\PREFETCH**

d) Tous les fichiers contenus dans le dossier **C:\WINDOWS\HelpTours** (présentation Windows)

e) **C:\MSOCache** aussi

Ce répertoire contient des fichiers d'installation de MSOffice qui permettent de ne pas réintroduire les CD d'installation quand on enlève ou ajoute des options de Office. Si vous avez les CD, vous pouvez très bien virer tout ce répertoire:

f) Fichier hibernation

Un gros fichier peut exister sous **C:\Hiberfil.sys**. Ce fichier est créé par le système en cas de passage en mode veille prolongée. Si vous ne souhaitez pas passer en mode veille prolongée (cas d'ordinateurs de bureau par exemple) car vous n'avez pas de portable avec batterie, alors vous pouvez désactiver cette fonction et ainsi le fichier (*Menu Démarrer -> Paramètres de configuration*)



Raccourcis et clés de registre caduques

Lorsque vous déplacez ou effacez des programmes, les fichiers disparaissent (nous avons vu que pas totalement d'ailleurs) mais pas forcément tout le cortège de paramètres qui les accompagne. De la même manière, lorsque vous désinstallez un programme, les programmes de désinstallation ne font pas leur travail à fond. Il reste très souvent trois types de traces principalement:

- des raccourcis caducs dans le menu démarrer
- des DLLs (bibliothèques dynamiques) orphelines
- des clés de registre

Imaginez tout ce qui va rester d'inutile au bout d'une année de vie d'une machine. Une somme considérable. Selon moi, les registres sont sans doute le plus pénalisant. Windows passe le clair de son temps à fouiller et refouiller ces registres (il existe d'ailleurs des outils qui vous permettent de visualiser l'utilisation des registres... c'est édifiant !!).

Je vous conseille donc de nettoyer ces traces. Pour cela, des outils excellents font le travail à votre place:

Je vous conseille d'utiliser **EasyCleaner - Raccourcis et Registres** (disponible dans les liens en bas de page).

Ou plus efficace encore mais plus dangereux dans les options **CCleaner - Registres et Nettoyeur** (disponible dans les liens en bas de page).

Défragmentation

Voici encore une fragilité de Windows. Elle provient du système de fichiers. Après être passé de FAT32 à NTFS, le problème ne s'est guère amélioré (Linux est beaucoup moins sensible avec ReiserFS). Je vous explique. Lorsque vous stockez un fichier sur le disque, il est possible que le système tente de le poser par morceaux à différents endroits du disque. Ce phénomène est voulu pour permettre en fonction des effacements et ajouts de garder la plus grande partie du disque inutilisée en cas de stockage d'un très gros fichier. Le problème vient du fait qu'à la lecture de ce fichier morcelé, par la suite, la tête sur le disque dur va devoir se positionner, puis lire, puis se repositionner, puis lire, puis se repositionner, puis lire, etc... L'accès disque va être plus long du fait des allers venus continus de la tête. C'est la fragmentation. Il est nécessaire de défragmenter une fois par mois d'utilisation. Ce la peut prendre du temps pour un gros disque. Windows propose un outil pour le faire (Explorateur -> bouton droit sur la lettre du disque -> propriétés -> outils). Franchement, il n'est pas terrible.

Je vous conseille l'outil **OO-Defrag**: <http://www.oo-software.com/home/fr/products/oodefrag/>

Je vous conseille la défragmentation de type SPACE. Malheureusement, cet outil est payant.

Un autre outil un peu moins performant mais gratuit, se trouve sous:

<http://www.kessels.com/JkDefrag/>

Désinstallation

Enfin, les désinstallations ne sont pas totalement correctes la plupart du temps (assez rare cependant). Je vous conseille d'être organisé lors de l'installation. Suivez autant que possible la procédure suivante pour un programme que nous appellerons *laiguillon*:

- a) télécharger le fichier d'installation dans un répertoire que vous créez *c:\Program Files\laiguillon*
- b) lancer l'installation et demander une installation spéciale
- c) spécifier *c:\Program Files\laiguillon* comme lieu d'installation
- d) aller dans la configuration du programme et placer autant que possible tous les éléments sous *c:\Program Files\laiguillon*

De cette manière à la désinstallation, lorsque la procédure sera terminée (avec éventuellement un redémarrage, supprimer totalement *c:\Program Files\laiguillon* (regardez si vous n'avez pas de répertoire *C:\Documents and Settings\<user>\Application Data\laiguillon* (il s'agit des options, des parties sauveées dans un jeu, etc...)). Si vous avez un tel répertoire et que vous ne voulez plus conserver ces données, effacez le répertoire aussi. Finalement, lancer les nettoyeurs pour finir le ménage.

H - Protégez votre ordinateur efficacement

Routeur ADSL

Les modems/routeurs ADSL sont livrés avec un mot de passe par défaut et une adresse par défaut.
Exemple: *Sur une LiveBox, l'utilisateur est "admin", le mot de passe "admin" et l'adresse de base 192.168.1.1*

Si moi je le sais, je ne suis pas le seul. Vous avez sacrément intérêt à :

- mettre un mot de passe complexe (12 caractères minimum avec mélange chiffres, majuscules, minuscules, signes)
- changer l'adresse pas défaut et la passer à, par exemple, 192.168.4.156

D'autre part, faites en sorte de :

- ne pas laisser d'administration à distance
- bien configurer le firewall et le NAT (souvent intégrés dans l'appareil)

Note: Il est souvent difficile de comprendre exactement ce que l'on fait:

- Pour le trafic sortant, c'est le firewall qui va faire foi (configurez le de manière personnalisée)
- Pour le trafic entrant, c'est le routeur qui va vous permettre de ne laisser que certains types de trafic et vers des machines internes très précises (appelé aussi NAT)

Enfin faite une sauvegarde de la configuration sur votre disque dur et sur une clé USB. Nommez ces configurations par date.

Wifi

Beaucoup de foyers disposent aujourd'hui d'un réseau WiFi. Implémenté dans les routeurs ADSL, un réseau Wifi domestique permet une plus grande mobilité des ordinateurs. Installés par défaut, ceux-ci dans un environnement citadin offrent des possibilités de piratage extrêmement aisé. Il serait ici difficile d'expliquer en détail toutes les possibilités et les failles,

Pour résumer je dirais en utilisant des termes techniques cabalistiques:

- Changer le mot de passe du routeur ou AP (Access Point ou Point d'accès Wifi). Voir point précédent.
- Filtrer les adresses MAC
- Ne pas utiliser de DHCP
- Favoriser une cryptographie forte WPA2
- Changer le SSID

Je vous laisse suivre ce lien pour mieux comprendre:

http://www.securiteinfo.com/attaques/phreaking/securite_reseaux_wifi_wardriving.shtml

FireWall (pare-feu)

Un firewall est un système qui filtre les paquets réseau en entrée et/ou en sortie et ne laisse passer que ceux qui sont autorisés. En dehors de ce comportement trivial, ils sont aussi aptes à bloquer des trafics qu'ils jugent dangereux, Ils ont des règles qui leur permettent aussi de bloquer les attaques en entrée par reconnaissance de comportement (détection d'intrusions).

Certains d'entre eux ont des fonctions web et permettent de bloquer les publicités, empêcher les fenêtres popups de s'ouvrir, etc...

La mise en place d'un firewall ou pare-feu est obligatoire si vous voulez assurer un minimum de sécurité. Il se trouve que Microsoft fournit un tel système mais de qualité très moyenne et avec peu de fonctionnalités.

Je vous conseille, si vous le pouvez, de mettre un firewall en mode comportemental (ou apprentissage). C'est un peu plus pénible au début (le temps qu'il apprenne les règles) mais par la suite ceci s'avère un grand avantage et pour tout dire vous vous rendrez vite compte que beaucoup de programmes tentent de sortir sur Internet (mises à jour, vérifications, enregistrements, statistiques,...) à votre insu. Lors de l'apprentissage, le système vous présentera qui essaie de faire quoi et vous demandera ce qu'il doit faire (accepter ou refuser, et écrire une règle pour accepter ou refuser la prochaine fois que cela se produit).

Les produits que je vous propose de tester sont (dans l'ordre de mes préférences):

Sunbelt Personal Firewall 4 (anciennement Kerio) :

Lien : <http://www.sunbelt-software.com/Home-Home-Office/Sunbelt-Personal-Firewall/Download/>
document pour la configuration de Sunbelt : <http://www.vulgarisation-informatique.com/kerio.php>
Une version complète que devient moins complète au bout de la période de test mais reste très intéressante. Je vous conseille d'activer le blocage comportemental...

Jetico version 1 ou 2 :

Lien : <http://www.jetico.com/download.htm>

Sans doutes le meilleur mais payant pour sa version 2. Je vous conseille de rester en version 1...

ZoneAlarm:

Lien : <http://www.zonealarm.com/store/content/company/products/znalm/freeDownload.jsp>

Une version gratuite et une version Pro payante

Comodo :

Lien : http://www.personalfirewall.comodo.com/download_firewall.html

Gratuit dans la mesure de ce que je sais.

Vous allez trouver beaucoup de comparatifs et aucun ne vous donnera le même résultat, alors je ne vais pas en rajouter une couche. Il y a tout de même quelque chose que vous devez garder en tête. Dans le cas courant d'un raccordement, vous disposez d'un modem/routeur ADSL. Celui-ci, dans le meilleur des cas, comporte aussi un pare-feu. Il faut absolument prendre du soin pour le configurer. C'est le point d'entrée de votre réseau de toutes manières. Si vous ne disposez pas d'un tel matériel, je vous conseille d'aller jeter un œil sur des boîtiers qui sauront vous satisfaire. Par exemple (ce n'est qu'un exemple et je ne dis pas que ce sont les meilleurs):

<http://www.netgear.fr/produits/index.php?cat=10>

AntiVirus

Autant vous dire tout de suite, je déteste McAfee et Norton. Ces saloperies sont installées par défaut sur des ordinateurs neufs, sont payants, et sont très difficiles à désinstaller. Je vous conseille de virer ces merdes dès que possible et je me fous de savoir s'ils sont efficaces ou pas !!

Nous devons donc trouver d'autres anti-virus. Comme pour les pare-feu, il existe beaucoup de comparatifs qui ne sont pas forcément d'accord entre eux. En voici un : <http://www.clubic.com/article-77079-1-guide-comparatif-meilleur-antivirus.html>

En ce qui me concerne, j'utilise avec succès Avira AntiVir PersonalEdition classic avec beaucoup de réussite, mais cela ne veut pas dire pour autant que ce soit le meilleur. Vous devez décider si vous voulez protéger aussi votre messagerie thunderbird (*dites moi pas que vous utilisez Outlook !!*), ce qui n'est pas mon cas (uniquement de la messagerie par le web).

Je vous laisse donc la référence de deux produits gratuits et vous verrez.

Avast

Lien : <http://www.avast.com/fre/download-avast-home.html>

Compatible avec Thunderbird.

Avira AntiVir

Lien : http://www.free-av.de/en/download/1/avira_antivir_personal_free_antivirus.html

Si votre souci est la compatibilité avec Thunderbird, deux documents pour faire votre choix:

Sur le site Mozilla : http://kb.mozillazine.org/Thunderbird:_FAQs:_Anti-virus_Software

Sur un autre site : <http://www.geckozone.org/forum/viewtopic.php?t=22467>

AntiSpyware

Autant la notion d'anti-virus et de pare-feu paraît évidente, autant celle d'élimination des Spyware et spam l'est beaucoup moins.

Vous pouvez très bien récupérer des mouchards en surfant. Ces programmes ne sont pas des virus et ne sont pas détectés alors par vos anti-virus. Arrivant par le surf, les pare-feux n'ont pas de raisons non plus, de les bloquer.

Vous avez affaire aussi à des petits logiciels faisant partie de programmes légitimes qui s'amusent à stocker et/ou à transférer des informations personnelles vers l'extérieur.

Vous avez des informations sur l'utilisation de votre ordinateur qui restent aussi dans les registres.

Vous avez des mouchards qui transmettent des informations quand ils sont appelés, d'une manière ou d'une autre (keylogger, etc...).

Il vous donc trouver un programme qui vous fait un peu de nettoyage. Je vous propose l'outil gratuit, SpyBot:

Lien : <http://www.spybot.info/fr/spybotsd/index.html>

Cet outil vous permet de bloquer des mouchards connus (vaccination) et se met à jour régulièrement.

De plus, il peut scanner l'intégralité de votre machine pour découvrir des espions qui seraient déjà présents sur votre disque (Search & Destroy). Enfin il comprend des outils qui le font se rapprocher de CCleaner pour le nettoyage.

En plus de ce type de programme, il faut que vous appreniez à ne pas autoriser certains programmes à sortir, sous couvert de vous rendre service. Ceci concerne principalement les outils de :

- mises à jour (hormis l'anti-virus, bien sûr). Vous ferez cela de temps en temps manuellement.
- rapporteurs d'erreurs. Dr Watson et autres saletés qui ne vous apportent rien du tout (faut pas déconner, ce n'est à charge de l'utilisateur de corriger les programmes).

Testeurs de Ports et de Services ouverts

Pour finir le tour d'horizon, sachez que les plus techniques et précis, il existe des outils assez sympas qui vous permettent de regarder le comportement en live de votre machine.

Ces outils sont gratuits et sont disponibles sur le site de MicroSoft (et oui ...!!).

Ils sont là: <http://technet.microsoft.com/en-us/sysinternals/default.aspx>

I - Manipulations régulières pour tenir votre machine en bonne forme

Bon, en résumant, pour ceux qui ont eu du mal à faire un résumer, essayons de donner les bonnes actions entreprendre régulièrement pour garder une machine propre, sécurisée et en bonne forme. Tous ces points ont été vus en détails ci avant.

D'une manière générale:

- utiliser une messagerie Web
- configurer le navigateur FireFox pour tout éliminer en sortant
- surveiller votre façon de surfer
- effacer les fichiers importants avec Eraser
- quand vous avez installé un programme, supprimer les saloperies en démarrage automatique
- quand vous désinstallez, faites-le proprement

1 fois par jour:

Mettre à jour l'antivirus. (Avira par exemple)
Faire du nettoyage des fichiers et du registre (EasyCleaner ou CCleaner)
Lancer RootKitRevealer et MRUBlaster

1 fois par semaine (après avoir fait les opérations avant):

Déplacer les gros fichiers vers un disque USB
Vérifier et supprimer les programmes, fichiers et services inutiles
Lancer une défragmentation (OOdefrag par exemple)
Faire une mise à jour de SpyBot puis le lancer
Regarder les logs de votre modem/routeur ADSL et votre FireWall pour voir s'il y a eu des attaques

1 fois par mois (après avoir fait les opérations journalières et hebdomadaires)

Lancer un Scan AntiVirus complet de la machine
Vérifier le fonctionnement de la machine avec les outils SysInterNals
Vérifier les mises à jour du FireWall
Vérifiez la configuration de votre WiFi

Et puis.... surtout ... commencez à vous intéresser à des systèmes d'exploitation un peu plus sécurisés (Ubuntu, Suse Linux Enterprise Desktop, etc...).

Si vous avez des enfants adolescents, vous pouvez aussi leur laisser votre machine en les faisant démarrer avec un LiveCD qui leur permettra de surfer, d'utiliser MSN, d'écouter de la musique ou voir des films sans risque pour votre PC (LiveCD de gOS, LiveCD de Mandriva, GeexBox, DreamLinux, etc...).

J – Téléchargements discrets

Nous parlerons ici des méthodes de téléchargement de fichiers. Ces fichiers peuvent être des données, de la vidéo, de l'audio, bref tout ce que vous voulez.

Je vais présenter quelques alternatives pour les personnes qui aimeraient pouvoir bénéficier de ce que d'autres personnes partagent mais qui sont un peu effrayés ou attristés par l'ambiance délétère et de suspicion qui règne aujourd'hui. Cette ambiance générale est abîmée chaque jour un peu plus par des déclarations récurrentes dans lesquelles apparaissent fréquemment les termes "piratage", "droits d'auteur", "vol" mais aussi "surveillance", "répression", "saisie", "amende". Tout cela conduit des personnes modestes qui ne veulent que très épisodiquement partager un contenu, à hésiter de se lancer. Malgré le fait que l'on ne puisse rester insensible aux cris de détresse des majors dont l'embarras financier est aussi évident que la sincérité des artistes en mal de succès, et que l'on accepte ainsi, tellement volontiers, que les fournisseurs d'accès soient contraints par l'état à faire acte de surveillance et de répression, on aimerait, un tant soit peu, pouvoir profiter d'une parcelle de liberté dans un réseau dont c'est la vocation.

D'autre part, cet article n'a pas pour ambition d'être une référence en la matière. En effet, techniquement, les réseaux de partage sont complexes et les technologies émergentes sont nombreuses. Grosso modo, il y a trois systèmes qui permettent de "partager" des données. J'exclue les protocoles internes aux entreprises (nfs, cifs, ncp, etc ...) et les protocoles spécialisés dans un service (messagerie avec smtp, imap, pop, les protocoles des messageries instantanées comme irc, etc...).

- http/ftp : http c'est le protocole qui vous permet de naviguer sur internet mais il est possible aussi de partager des données avec (bouton droit, Sauvegarder sous ...) ou simplement cliquer sur une ressource (video, audio, image, fichier, etc...).

- p2p ou peer to peer : ensemble des techniques de partages mutuels. J'en parle comme d'un protocole mais pour être plus exact, il s'agit d'un concept de partage qui peut utiliser plusieurs protocoles.

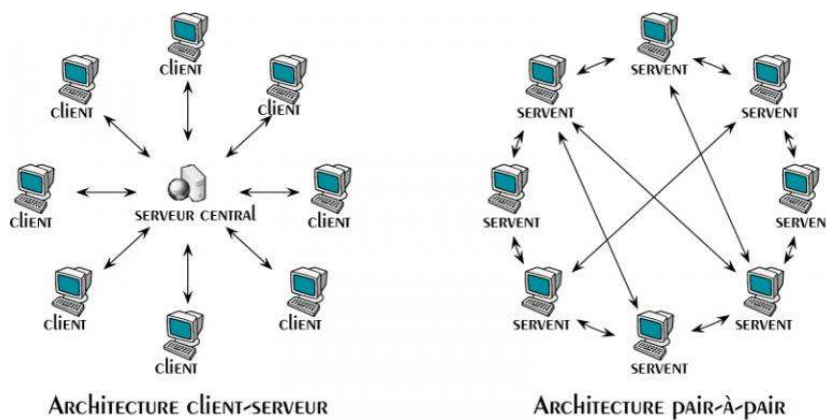
- nntp ou usenet : protocole et technique très ancienne de partage d'articles.

Nous allons éliminer http/ftp du fait qu'il ne s'agit pas totalement d'un réseau multi nœuds mais plus d'un système central dont les clients (ceux qui veulent récupérer quelque chose) se connectent en grappe. http est le protocole sur le plus utilisé sur Internet, mais pas à des fins de transfert ou de partage de données. A ce sujet, la part approximative de ces protocoles est: http 46%, p2p 37%, nntp 9%. (à noter que les transferts vidéo par YouTube efface encore un peu plus les autres).

Bref, nous avons donc le choix entre Peer-to-Peer et UseNet (même si UseNet pourrait finalement être considéré comme une sorte de p2p, mais ne compliquons pas).

P2P

Le Peer-To-Peer est un concept qui permet de partager des ressources, non pas de manière standard avec un serveur centralisé, mais en permettant des liens plus variés à la manière d'un réseau distribué.

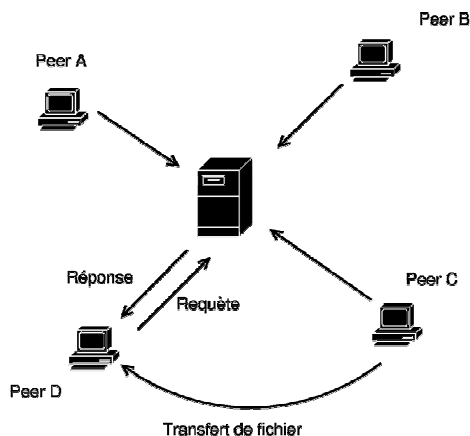


Chaque machine est à la fois Serveur et Client (Servent). C'est à dire que si vous télécharger un fichier, vous le rendez aussi disponible pour les autres personnes du réseau. Ce type de réseau maillé est intéressant car la disparition d'une machine ne le rend pas non fonctionnel. Par contre, le nombre de discussions entre les machines est grand et les recherches ainsi lentes.

Voici pour le concept. Dans ce concept, il y a cependant plusieurs techniques qui ont été adoptées par les différents types de réseaux P2P. A noter que quel que soit le type, il faut absolument que vous possédiez un "Client", c'est à dire un programme qui vous permet, depuis votre machine, d'entrer dans le réseau tel ou tel. Ces clients ne sont généralement pas compatibles entre eux.

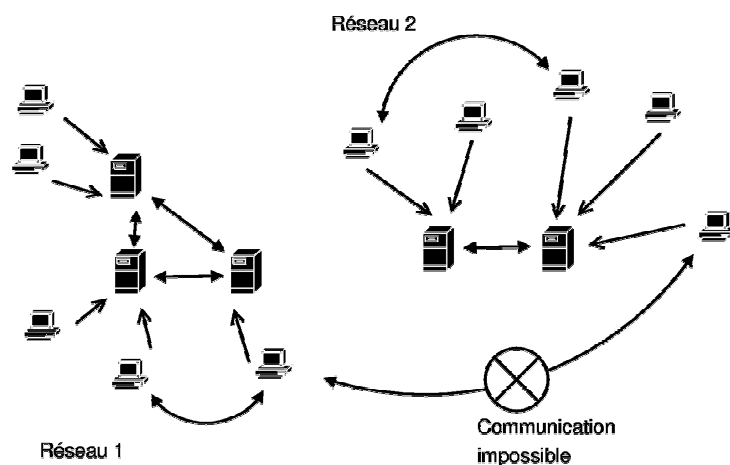
Les principaux acteurs

Le vieux: Napster



C'était un serveur qui ne faisait que mettre en relation des clients entre eux selon ce qu'ils voulaient récupérer. Je dis c'était, car Napster a presque disparu même si Napster2 continue de répondre.

eDonKey / eMule :

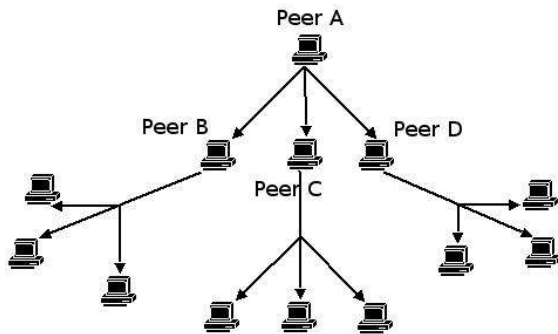


Il s'agit de plusieurs serveurs centralisés. Le client doit d'abord se connecter sur un serveur. Pour trouver un fichier à télécharger, un client s'adresse à son serveur, puis son serveur contacte les autres pour trouver la ressource. Quand les ressources sont trouvées, le client se connecte directement chez les autres clients qui dispose des morceaux de cette ressource, pour pouvoir récupérer l'ensemble du fichier. Durant la récupération, le serveur du client de départ, met à disposition le fichier pour d'autres clients... etc...

Les clients:

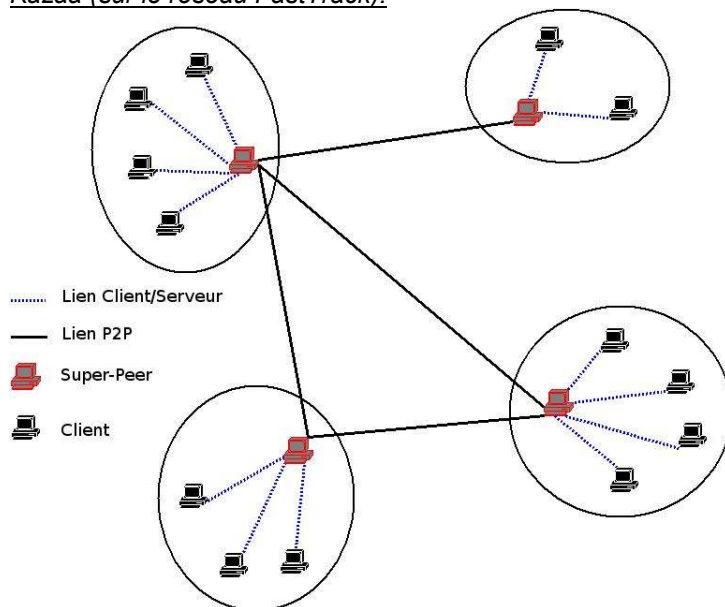
- emule : <http://www.emule-project.net/home/perl/general.cgi?l=13>
- edonkey: <http://www.edonkey2000-france.com/index.php?pagetype=downloads&flash=>
- amule: <http://www.amule.org/>
- xmule: <http://sourceforge.net/projects/xmule>

Gnutella/Limewire:



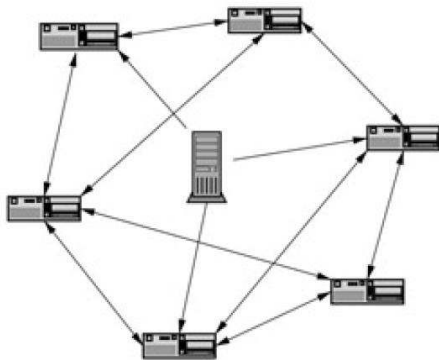
A peu près identique au précédent mais chaque machine est en fait un client et un serveur. C'est une architecture décentralisée. Des avantages par rapport au précédent, toujours (taille du réseau infinie, impossible de repérer quelqu'un volontairement, etc...) mais aussi des inconvénients (free-riding, grosse bande passante, pas de sécurité, etc...)

Kazaa (sur le réseau FastTrack):



Il s'agit d'une organisation en super-peer (hybride en fait, centralisée + décentralisée)

BitTorrent:



BitTorrent est en fait un protocole et non un réseau à proprement parler. Il y a des différences majeures

par rapport aux autres systèmes de partage des réseaux p2p.

- Dans un traditionnel réseau P2P, plus un fichier est demandé, moins il est accessible, car le serveur sature. Sur BitTorrent on partage seulement le fichier que l'on est en train de télécharger. Sur les autres réseaux on partage généralement une partie du disque dur.

- Sur les réseaux traditionnels, dès que plusieurs utilisateurs veulent récupérer le même fichier, une file d'attente se crée. Sur BitTorrent on parle de Torrent (fichier de faible poids indiquant au client les adresses des autres clients téléchargeant ce même fichier). Ce fichier Torrent possède les informations relatives au fichier que l'on décide de télécharger. Il permet de mettre en relation le client et le tracker. On le trouve sur Internet, et c'est le point de départ de tout téléchargement BitTorrent. Un fichier torrent ne contient donc aucune donnée du fichier qu'il sert à télécharger. On trouve les fichiers torrent un peu partout sur Internet, via le protocole HTTP.

- Régulièrement le client met à jour le tracker (Le Tracker est celui qui met les clients téléchargeant un même fichier en relation), en l'informant où il en est dans le téléchargement du fichier, dans l'envoi de ce fichier etc. Inversement le tracker envoie au client une mise à jour de la liste des personnes téléchargeant ce fichier.

- Lorsque vous téléchargez un fichier en tant que client, vous êtes, soit un "peer" (ceux qui téléchargent et envoient des parties de fichiers à d'autres clients), soit un "seed" (ceux qui possèdent la totalité du fichier).

Avantages: La vitesse de téléchargement est extrêmement rapide, grâce à ses protocoles légers et à son principe de fonctionnement : plus on télécharge le fichier, plus il est accessible en débit. Des fichiers très récents mais aussi des fichiers très volumineux sont disponibles sur les sites Internet. En effet il n'est pas rare de trouver des fichiers de plusieurs giga. Avec la grande vitesse de téléchargement disponible pour le client, il est désormais possible de télécharger ce type de fichier (à condition que suffisamment de clients soient intéressés).

Inconvénients: Il n'y a pas de mécanisme de recherches intégrés aux logiciels BitTorrent (peut être dans le futur...) En effet les .Torrents sont disponibles directement sur Internet, par le biais du protocole HTTP. Il est parfois très difficile de trouver un fichier précis, avec un torrent toujours actif. Les fichiers .Torrent meurent rapidement. En effet au départ beaucoup de personnes téléchargent le fichier. Mais au fur et à mesure, le nombre de client recherchant le fichier diminue et le torrent devient inactif.

D'autres réseaux :

Shareaza, Ares Galaxy, etc...

Jetez un œil sur la plupart des réseaux/clients P2P :

<http://www.commentcamarche.net/telecharger/logiciel-34-telechargement>

A noter un multi client : mldonkey: http://mldonkey.sourceforge.net/Main_Page

Le P4P:

Idée pour améliorer la vitesse des réseaux actuels en P2P:

<http://www.numerama.com/magazine/8968-P4P-le-P2P-plus-rapide-que-le-P2P.html>

Protection et sécurisation de emule/edonkey.

Nous avons donc affaire à un réseau p2p centralisé. Un client de ce type de réseau est, par exemple: emule :<http://www.emule-project.net/home/perl/general.cgi?!=13>

Quelques principes généraux:

- les clients free-riding (ceux qui ne font que télécharger mais ne partagent rien) ne sont pas bien appréciés mais tolérés. Des mécanismes vont tout de même les pénaliser.
- vous partager une zone de votre disque dur (dossier Incoming, en général). Plus vous partagez, plus vos téléchargements sont rapides.
- vos communications ne sont pas cryptées
- on peut tracer assez facilement votre connexion

Actuellement, la chasse aux pirates, rend l'exercice de téléchargements, un peu périlleux et dangereux. Les mesures sont les suivantes, dans la plupart des cas:

- Les FAI (fournisseurs d'accès) contrôlent les protocoles P2P
- De faux serveurs apparaissent dans la liste et ceux-ci vont surveiller les clients qui s'y connectent en observant le taux de chargements et le nombre de fichiers en partage (dossier Incoming)
- Des statistiques sont faites sur les connexions des utilisateurs.

Bon, je vous propose donc de faire plusieurs choses dans le cadre de la protection et du respect de la vie privée (bien sûr ...)

a) éviter au maximum les faux serveurs

Suivez la procédure : http://divxplanetv2.free.fr/?cat=securisation_emule

Ceci vous permettra d'éviter les connexions pirates par un filtre, en plus de ne pas vous connecter sur des faux serveurs.

b) brouiller le protocole d'emule

Ceci pur permettra d'éviter dans la mesure du possible que le protocole P2P soit bridé ou bloqué par votre fournisseur d'accès. Attention cependant à ne pas penser que cela vous rendra anonyme ou crypté...

Suivez la procédure: <http://www.numerama.com/magazine/3259-eMule-se-dote-d-un-brouillage-pour-eviter-le-bridage.html>

c) respectez un comportement discret avec votre mule

Ne pas laisser trop de fichiers dans votre dossier Incoming (mais un peu quand même car c'est le principe d'échange qui fait que cela fonctionne). Disons une vingtaine de fichiers. Virez les autres sur CD ou sur votre disque USB (effacez les avec **eraser** par exemple...;-)

Ne pas rester connecté constamment. Par exemple laisser votre mule tourner toute la nuit, mais uniquement une ou deux nuits par semaine, sinon déconnectez la.

Ceci vous permettra de ne pas entrer dans le hit parade des trackers de pirates

d) Concernant les traces laissées d'une utilisation à l'autre, il vous suffit de suivre la procédure sur le site: <http://www.article12.fr/nf/traces-de-certains-logiciels-sous-xp/emule-0.48a-effacer-ses-traces-2.html>

Enfin, si vous voulez encrypter vos téléchargements et le contenu de votre disque, pour vos téléchargements, vous pouvez prendre le logiciel Steganos P2P (malheureusement un shareware). Ce logiciel vous permet de :

- La musique et les films provenant de bourses d'échange telles que Kazaa sont tous automatiquement cryptés sur le disque dur et enregistrés dans le coffre-fort multimédia.
- Sans le mot de passe approprié, personne ne peut accéder à votre coffre-fort multimédia.
- Steganos P2P Sécurisé crypte vos téléchargements en temps réel en utilisant le procédé AES (Advanced Encryption Standard) en 128 bits.
- Reconnaissance automatique des programmes de partage de fichiers pris en charge.
- Destruction automatique des traces sur demande. A l'issue du partage de fichiers, les données d'historique et les requêtes de recherche sont automatiquement effacées de votre PC.
- Un dictionnaire intégré stoppe les mots de passe mal choisis - pour que vous jouiez toujours la carte de la sécurité avec votre mot de passe.
- Le coffre-fort multimédia contient jusqu'à 32 Go (voir Configuration minimale).
- Prends en charge : Kazaa, Kazaa Lite, Morpheus, iMesh, eMule et Souseek.

P2P sécurisés

Attention, que l'on soit clair. Il est impossible d'être totalement anonyme. A partir du moment où vous vous connectez chez votre FAI, vous êtes dès lors connu. Maintenant, le but du jeu est le suivant: faire en sorte que vous retrouvez soit suffisamment difficile pour que cela devienne cher et ainsi que le jeu n'en vaille pas la chandelle. C'est le cas pour les téléchargements... Nous allons parler ici de réseaux qui promettent d'être anonymes (difficile de vous tracer) et sécurisés (difficile de savoir ce que vous faites).

De plus, cette confidentialité, cet anonymat a un coût. Pas financier mais un coût en performances. Il est malheureusement incontournable d'utiliser de la bande passante pour l'anonymat, de ce fait les performances de téléchargements s'en trouvent affectées. Gageons, pour finir, que les vitesses de connexion de vos abonnements vont combler petit à petit ce handicap.

Nous prendrons quatre réseaux exemples, pour se rendre compte que "ça bouge !!!" :

Freenet

Site: <http://www.freenet-doc.info/index.php/Accueil>

Doc: <http://fr.wikipedia.org/wiki/Freenet>

Les données ne sont pas téléchargées directement d'un pair à un autre, mais peuvent transiter par un ou plusieurs pairs. Il est ainsi quasiment impossible de déterminer l'origine exacte d'un message. Afin de protéger les hébergeurs, tous les fichiers sont cryptés. Le possesseur d'un nœud ne peut donc pas connaître le contenu des fichiers stockés sur son nœud. Si le nœud 1 cherche une information, il demandera à son voisin (appelons-le 2) qui, s'il ne dispose pas de la ressource, transmettra la requête à 3, et ainsi de suite.

Certaines faiblesses de ce réseau ont été évoquées, comme par exemple:

- Temps de récupération d'un fichier Le temps nécessaire pour trouver un fichier dans Freenet reste très honorable. En revanche, le temps de récupération est beaucoup plus long, à cause des problèmes d'anonymat : afin de ne pas connaître la source du fichier, celui-ci sera copié sur tous les nœuds intermédiaires de la requête.
- Diffusion des clefs Freenet utilise des clefs, notamment pour permettre d'identifier les fichiers. Une recherche de fichier sans cette clef étant quasiment impossible, il faut que la personne disposant d'un fichier dispose d'un moyen de diffuser la clef. Or si on envisage un site web, cela implique un serveur centralisant les données, ce qui va à l'encontre de l'esprit de freenet, à savoir la décentralisation totale. Il est actuellement possible d'héberger un site web sur freenet (donc sans offrir de serveur fixe), mais dans ce cas là, on revient au premier problème (temps de récupération) pour chaque page...

Omemo

Site: <http://www.omemo.com/>

Doc: <http://fr.wikipedia.org/wiki/Omemo>

Sur Omemo, tous les contenus multimédias (musique, films, logiciels, documents, images...) partagés par l'ensemble des utilisateurs sont ainsi accessibles directement, comme avec n'importe quel réseau P2P, mais en plus parfaitement classés dans des dossiers comme vous le feriez sur votre propre disque dur. Les utilisateurs participent collectivement à l'organisation des contenus qu'ils envoient, à la manière d'un wiki. Vous pouvez ajouter un dossier ou même en supprimer un (en expliquant pourquoi), et uploader les fichiers que vous souhaitez y glisser. Les contenus ainsi uploadés sont ensuite classés ou écartés en fonction des votes des utilisateurs, qui s'assurent que les contenus sont bien pertinents et de qualité. Omemo pourrait devenir le plus grand disque dur virtuel du monde, dans lequel il sera facile de trouver n'importe quel contenu. Le réseau est structuré de telle manière qu'il est très difficile de retracer qui a envoyé un fichier sur le réseau, et de savoir qui le télécharge.

Mute

Site : <http://mute-net.sourceforge.net/index.fr.shtml>

Doc: http://fr.wikipedia.org/wiki/Mute_%28logiciel%29

Idée très astucieuse et très prometteuse. La base est vraiment de contourner la surveillance de la RIAA (Notre SACEM = Recording Industry Association of America) - voir <http://www.downhillbattle.org/>

- Les connexions ne sont pas possibles entre téléchargeur et échangeur. Vous faites une demande et cette demande progresse sur le réseau de proche en proche. Aucun nœud ne connaît le chemin global entre vous et la source (issu de l'étude des fourmis ...).
- les connexions sont chiffrées à un degré militaire
- le système remplace les adresses IP par des codes complexes

GNUNet

Site: <http://gnunet.org/index.php?xlang=French>

Doc: <http://fr.wikipedia.org/wiki/GNUNet>

Assez proche de FreeNet. La philosophie est de garantir anonymat et empêcher la censure. Des détails, ici : <http://gnunet.org/philosophy.php3?xlang=French>

Remarque: disponible sous Unix et Linux uniquement, il semble que ce soit désormais disponible sous Windows.

UseNet ou NNTP ou les newsgroups

Qu'est que c'est ?

Nous avons vu que pour que les réseaux de P2P fonctionnent (quels qu'ils soient), il faut que tout le monde partage (sinon plus de sources, plus de téléchargements). La plupart des clients (logiciels utilisés pour accéder aux réseaux) ne permettent même pas de désactiver l'envoi. Dans la loi Française, le téléchargement est légal, ce qui ne l'est pas est le partage des fichiers (le *download* est légal mais pas le *upload*).

Il existe un réseau très ancien maintenant (1979) qui risque bien de devenir de plus en plus populaire. Si nous lisons la définition donnée dans wikipedia, voici ce que nous avons : " *Usenet est un ensemble de protocoles servant à générer, stocker et récupérer des « articles » (des messages qui sont proches, dans leur structure, des courriels), et permet l'échange de ces articles entre les membres d'une communauté qui peut être répartie sur une zone potentiellement très étendue. Usenet est organisé autour du principe de groupes de discussion ou groupes de nouvelles (en anglais newsgroups), qui rassemblent chacun des articles (contributions) sur un sujet précis. Les sujets des groupes de discussion sont organisés selon une hiérarchie. Une fois connectés à un serveur informatique fournissant un service Usenet, les utilisateurs peuvent choisir les groupes mis à disposition par ce serveur auxquels ils désirent « s'abonner ». Pour chaque groupe auquel il est abonné, l'utilisateur peut alors voir tous les nouveaux articles mis à disposition sur ce groupe et tous les articles reçus par le serveur depuis un certain temps. Lorsqu'un utilisateur envoie un article sur un serveur Usenet, celui-ci le propage à tous les autres serveurs avec qui il a conclu des accords d'échange d'articles (feeding, littéralement, « alimentation »), et ainsi de suite. Chaque serveur conserve une copie de cet article, et peut ensuite le mettre à disposition des utilisateurs ayant accès à ce serveur. Les utilisateurs emploient généralement un logiciel client appelé lecteur de nouvelles (parfois aussi appelé client de news, en référence au modèle client-serveur) pour lire et composer des articles Usenet.* "

Derrière cette utilisation toujours active mais délaissée de plus en plus (les lectures de *news*), se cache aussi la mise à disposition de contenus binaires. Le protocole utilisé est resté l'historique NNTP.

Les newsgroups présentent 2 avantages majeurs: 1) leur utilisation est légale, 2) la vitesse de téléchargement est constante et égale au maximum de votre bande passante.

Le seul point noir est que l'accès à Usenet n'est pas gratuit, pour les contenus binaires. Les prétendants devront souscrire un abonnement auprès d'une société tierce offrant un accès aux newsgroups.

Comment ça marche ?

Les fichiers binaires déposés sur les newsgroups étant découpés en plusieurs parties (multi-parties), il faut les réassembler une fois tous les téléchargements terminés. Des logiciels sont apparus afin de faciliter et d'accélérer le téléchargement mais aussi de l'interrompre pour le reprendre plus tard. Beaucoup d'autres options sont disponibles et varient selon les programmes.

Le principe d'Usenet est le suivant: une personne envoie un fichier à son serveur d'accès Usenet. Le serveur transfère ce fichier à tous les autres serveurs dans le monde. Il devient possible de télécharger le

fichier directement depuis le serveur. Usenet met en relation le client directement avec son serveur et ***cela explique les vitesses de téléchargement très grandes***. Là où le P2P fait d'utilisateur à utilisateur (les fournisseurs d'accès limitent bien évidemment le vitesse d'upload au maximum),.

Il est important d'expliquer à ce propos le principe de rétention. Puisque les fichiers sont stockés sur les serveurs et que l'espace disque de ces serveurs n'est pas illimité, tous les fichiers vieux de plus de X jours sont effacés. Le X représente le taux de rétention. Plus le taux de rétention est élevé plus vous aurez accès à des vieux fichiers. Le taux de rétention moyen se situe entre 1 et 2 semaines. Ne choisissez pas un fournisseur d'accès aux newsgroups qui offre un taux de rétention inférieur à une semaine.

Comment s'y mettre ?

Il faut d'abord choisir un fournisseur d'accès aux newsgroups. Pour cela vous pouvez aller jeter un œil, ici: <http://www.usenetforyou.com/>

Ensuite, il faut télécharger un client qui vous permet de faire des recherches, de se connecter sur votre fournisseur et de récupérer du contenu. Je vous conseille le plus répandu, GrabIT. Vous le trouverez ici : <http://www.shemes.com/index.php?p=download> et vous trouverez des explications, ici : <http://www.usenetforyou.com/grabit.html>

Sécurité et anonymat

Vous pensez bien que les autorités (ou plutôt les majors et leurs copains) s'intéressent de près depuis quelques temps aux newsgroups. Le fournisseur d'accès FREE est d'ailleurs connu pour brider cet accès (brider le protocole nntp). Mais manque de chances pour eux, il existe certaines façons de contourner ces bridages et d'assurer plus d'anonymat ou plutôt plus de confidentialité dans les échanges. Il existe deux formes :

- votre fournisseur vous permet de vous connecter en SSL (système d'encryption basé sur des clés asymétriques)
 - vous encapsulez le protocole NNTP dans un Secure Tunnel pour atteindre une passerelle.
- Lire cet article : <http://www.usenetforyou.com/bridage-newsgroups-free.html>

Quand je dis qu'il ne faut pas confondre confidentialité et anonymat, je veux dire que dans le cas de téléchargement en mode encrypté, votre fournisseur saura qui (vous), où (sur quel serveur) et comment (par quel protocole) mais ne saura pas quoi (ce que vous téléchargez). Même quelqu'un qui porterait plainte contre vous, devra au moins savoir pourquoi (contenu illicite ?) et avec l'encryption, il a du boulot !!

Vous me direz, oui mais le fournisseur de newsgroup, lui, il sait !! C'est vrai, lui il sait tout !! Mais pour cela, trois remarques:

- si il donne ces infos aux autorités, il perd tous ses clients
- les fournisseurs de contenu newsgroups ne gardent pas leurs logs
- les fichiers ne sont disponibles que pour un temps donné, puis éliminés ensuite (on appelle cela le temps de rétention).

Et puis, n'oubliez pas qu'avec les newsgroups, vous ne partagez rien, vous ne faites que télécharger !!

Voici donc une très jolie alternative au p2p !!

Politique

Un cours très instructif concernant l'intoxication actuelle sur le piratage, histoire de replacer les éléments à leur juste échelle et recadrer le débat d'un point de vue historique: <http://www.slideshare.net/guest5e4ebf/cours-1-introductif/>

Des articles sur la guerre entre piratage, état et infra-structures techniques: <http://www.numerama.com/magazine/8837-Brider-les-rseaux-P2P-ne-payé-plus.html>

<http://www.01net.com/editorial/359963/le-piegeur-de-pirates-accuse-de-piratage/>
<http://news.p2pfr.com/?558>
<http://news.p2pfr.com/?561>

K - Surfez en tout anonymat

Que l'on soit d'accord tout de suite. Vous n'êtes jamais TOTALEMENT anonymes !! Le deal n'est pas de vous rendre 100% anonymes mais de faire en sorte que vous retrouvez devienne un terrible casse-tête et que seules de très bonnes raisons le justifient (et il y en a, parfois, qui me paraissent être de bonnes raisons).

LiveCD

Si votre but est simplement de surfer, une solution élégante est de démarrer votre PC avec une version d'un système d'exploitation en LiveCD (c'est à dire bootable tel quel sans que le contenu réel de votre machine soit affecté d'une quelconque manière). Vous disposerez alors d'outils généralement suffisant pour surfer tranquillement sur le net.

Cette solution pourrait tout à fait être aussi envisagée pour permettre à vos enfants de surfer sans pour cela récupérer un virus, ni stocker des données, ni mettre en péril votre ordinateur de bureau, par exemple.

La plupart des distributions de ce type sont basées sur Linux et il vous faudra peut-être en essayer plus d'une avant de trouver celle qui vous convient (si vous n'êtes pas un habitué de Linux).

Il est aussi à remarquer que comme ces distributions tournent en mémoire vive, il est souvent conseillé d'avoir une machine disposant d'une taille mémoire correct (minimum 512 Mo) pour ne pas souffrir d'un manque cruel de confort.

Parmi ces distributions (allez jeter un œil sur : http://fr.wikipedia.org/wiki/Liste_des_LiveCD), nous en remarquerons une orientée sécurité et anonymat: Anonym OS

En effet cette distribution base ses outils sur une couche d'encryption pour limiter au maximum l'empreinte des surfs.

Article sur Anonym OS: <http://www.infododos.com/guides/view-guide-19.html>

Proxy

Ah, les proxies... capables du meilleur comme du pire...

Un proxy est une machine intermédiaire par laquelle vous allez vous faire vos requêtes sur internet.

Dans l'entreprise:

Dans une entreprise, c'est en général le moyen par lequel vous avez le droit de sortir sur Internet. Généralement, votre machine n'est pas autorisée à sortir directement sur internet. Une raison est que son adresse IP est une adresse pure interne (elle n'est pas acceptée par les routeurs sur Internet. rappel: un routeur est une machine qui relie deux réseaux différents. En allant surfer vous passez par une grande quantité de routeurs dont le premier est sans doute celui de votre fournisseur d'accès). Une autre raison est que si vous passez par une machine de ce genre, les requêtes que vous allez faire, seront apparemment faites par le proxy, et ceci permettra de "masquer" votre véritable adresse. Enfin, les personnes qui s'occupent du réseau de l'entreprise vont pouvoir effectuer toutes sortes de sélections sur cette machine (comme il s'agit d'une machine par laquelle vous êtes obligés de passer). Ils vont mettre des filtres (vous bloquant certains sites), ils vont logguer ce que vous faites (garder des traces de vos pérégrinations sur internet) et vont éventuellement vous demander de vous authentifier (au moins une fois) avant de vous laisser surfer.

Chez soi:

Depuis chez nous, nous avons deux possibilités. Soit nous avons notre propre proxy (voir les avantages plus bas), soit nous pouvons passer par le proxy de notre fournisseur d'accès. Quels peuvent être les intérêts ?

En premier lieu, comme toutes les requêtes vont passer par cette machine, votre machine sera quelque peu dissimulée derrière. En passant par le proxy de mon FAI, je vais "faire croire" que c'est lui qui fait les demandes, espérant ainsi ne pas être emmerdé par les sites qui tentent de loguer ce que vous faites. En plus, celui-ci aura sans doute un "cache". Un cache est un stockage local qui va garder les pages que vous visitez. Ainsi, dans une connexion ultérieure, la même page sera récupérée sur cette zone, sans être obligé de retourner sur internet. Bon, très honnêtement, je ne suis pas fan du tout et vous déconseille de la faire. Pour deux raisons: la première est que le cache ne sert plus à grand chose car la plupart des contenus des sites aujourd'hui est dynamique (change en fonction de paramètres particuliers). La seconde est que les vitesses de connexion sont suffisantes pour ne pas sentir vraiment l'intérêt comparé au problème que votre FAI va vraiment récupérer l'intégralité de vos actions sur internet.

Si j'installe mon propre proxy, je vais avoir deux avantages: le premier est que je pourrais m'amuser à mettre un tas de filtres sur cette machine pour tenter de bloquer un maximum de saloperies. D'autre part, c'est cette machine qui sera sujette aux attaques et autres puisque que c'est elle qui apparaîtra comme l'origine de mes actions.

En quoi cela m'apporte quelque chose au niveau anonymat ?:

Imaginez la situation suivante. J'ouvre mon navigateur. Celui-ci, au lieu de se connecter directement sur les sites que je veux visiter, va passer par l'intermédiaire d'un proxy quelque part sur internet (un proxy public). Du coup, les sites visités vont penser que c'est le proxy public qui fait la démarche (au niveau de l'adresse IP aussi)... gagné!!

Euh, non ... qu'et-ce qui me dit que mon proxy public sera assez gentil pour ne pas retenir ce que je fais et transmettre mes infos à qui veut bien les connaître ? et puis les connections depuis chez moi jusqu'au proxy public, seront quant à elles totalement visibles... oui, bonnes remarques.

En plus tu parles toujours de surfer mais si je veux utiliser mon email au lieu de surfer, je peux ?

Bon, ok... alors il faut compliquer un peu le tableau et introduire d'autres pièces... imaginons que je dispose d'un système qui va automatiquement entourer les requêtes de mes applications, et les rediriger de manière transparente vers un proxy public ?

Bien, je viens de décrire un client SOCKS et un serveur SOCKS public. SOCKS est un protocole qui permet d'embarquer les communications d'une application pour les diriger vers un serveur SOCKS ou plus exactement un proxy socks.

D'autre part, imaginons que parallèlement à cela, j'ai un système qui essaie de se connecter à toute une liste de proxies, s'amuse à les détecter automatiquement et même à basculer de temps en temps de l'un vers l'autre...

Ah oui, là, j'ai un système qui commence à être pas mal du tout. Si j'ajoute maintenant un truc qui peut m'encrypter les communications de mon pc ou mon proxy vers le prochain proxy public, on touche au divin les p'tits gars !!!

Et bien tout cela existe...

Pour les proxy HTTP

a) on obtient la liste des proxies publics

Liste de proxies publiques : <http://www.free-proxy.fr/>

b) on vérifie que cette liste est correcte (n peut cumuler des listes)

Un testeur de proxies qui valide les bons : <http://www.project2025.com/charon.php>

c) on installe dans firefox, une extension qui bascule régulièrement d'un proxy de votre liste vers un autre
Extension switchproxy pour FireFox : <https://addons.mozilla.org/fr/firefox/addon/125>

Pour le socks (vos emails, etc...)

a) Client SOCKS

humminbgbird : <http://connectivity.hummingbird.com/products/nc/cpsecurity.html>

sockscap : <http://soft.softoogle.com/ap/sockscap-download-5157.shtml>

freecap: <http://www.freecap.ru/eng/?p=download>

b) Liste des proxy socks dispo : <http://www.samair.ru/proxy/socks.htm>

c) une petite aide au cas où

<http://websecurite.free.fr/anonymat.htm>

on finit par vérifier notre anonymat

<http://privacy.net/>

Comme vous avez pu vous en rendre compte, cela commence à devenir complexe et souvent mal aisé à mettre en place correctement (la discrétion se paie ...!). Il faut aussi remarquer que les performances de vitesse pour surfer seront forcément moins bonnes ... pas de bras, pas de chocolat !!

Tor

En fait Tor a un rapport direct avec les proxies. Mais avec ce je ne sais quoi qui me plait, de participation et de transparence... mais aussi, moins plaisant, une part de doutes sur les raisons de certains à utiliser un réseau comme Tor. Je vous conseille un très bon article sur le sujet :

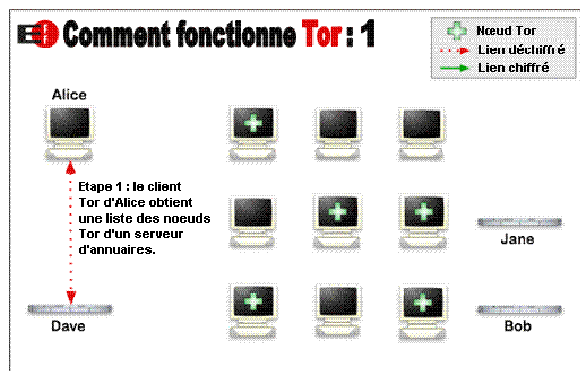
<http://www.framasoft.net/article4338.html>

Mécanique

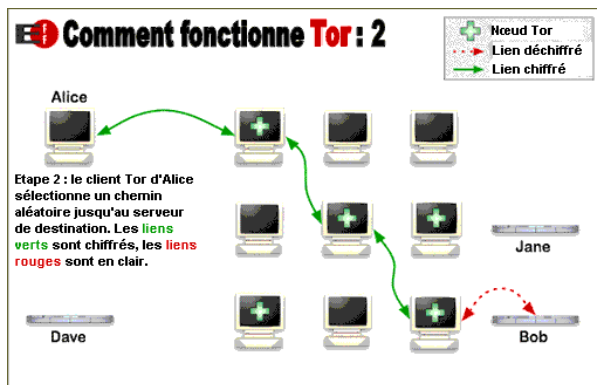
TOR et les routeurs Oignons !!!

Je reprends en résumé la doc du site qui est très bonne: <http://www.torproject.org/overview.html.fr>

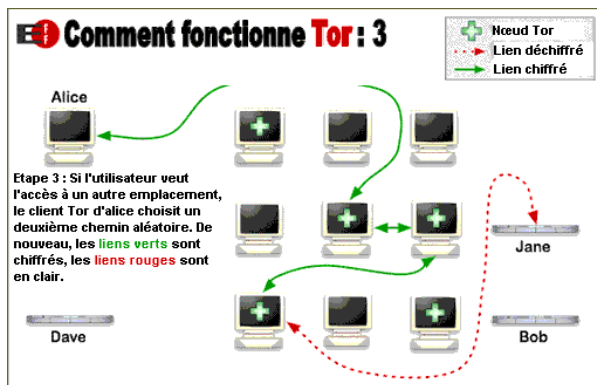
Le but du jeu est faire transiter vos communications de manière cryptée à travers une forêt de routeurs qui tiennent plus de proxies. Par exemple, la très célèbre Alice veut se connecter chez Bob...



Alice possède Tor (client Tor), Vidalia (une interface de gestion de Tor) et PrivProxy (Proxy privé qui fait du filtrage). Le client Tor s'adresse à un serveur d'annuaire qui va lui donner la liste des serveurs Tor (ou routeurs). Le client va ensuite calculer de manière aléatoire le chemin que la communication va prendre tout au long de ce dédale jusque chez Bob.



Notez que tout est crypté depuis Alice jusqu'au routeur avant bob, mais n'est pas crypté de ce dernier routeur vers Bob.



Si Alice décide d'aller ailleurs, alors un circuit est recalculé. Passer de sites en sites, va brouiller la possibilité de remonter jusqu'à Alice.

Ce qui est intéressant, c'est que pour retrouver l'origine (Alice) c'est pas coton, autant que le contenu est encryté (jusqu'avant le site final). L'anonymat et la confidentialité sont donc parfaitement gérés. Au niveau technique, chaque nœud va ajouter une couche d'encryption qui ne sera décryptable que par le nœud suivant (comme des couches, d'où le terme routeurs oignons). Un nœud ne pourra pas connaître le chemin global. Comme il s'agit d'un système de proxy SOCKS, en gros, ce système fonctionne non seulement pour un navigateur mais pour plusieurs applications.

Faiblesses

Ben oui... il est attaquable. Par une reconnaissance d'empreinte temporelle, il serait possible de vous retrouver, de même qu'il serait possible de coucher un nœud par une attaque ciblée. Mais les efforts techniques demandés dans ce cas sont loin d'être négligeables...

De plus, une certaine lenteur peut être observée (ralying, encapsulation, cheminement complexe, etc..). Comme SOCKS toutes les applications ne sont pas possibles avec Tor mais suffisamment pour que cela reste très intéressant.

Enfin, le fondement de ce système repose sur la disponibilité des routeurs oignons. Ces routeurs sont assurés par vous et moi, en tant que volontaires pour laisser une petite partie de notre bande passante pour assurer le bon fonctionnement de l'ensemble.

Mise en place

Télécharger : <http://www.torproject.org/download.html.fr>
Installer: <http://www.torproject.org/docs/tor-doc-windows.html.fr>

Note: ce n'est pas parce que vous avez installé la partie client de Tor que tout va passer dans ce tube de manière magique. Pour FireFox, par exemple, vous avez besoin du plugin TorButton :
<https://addons.mozilla.org/firefox/2275/>

N'oubliez pas non, si vous voulez devenir un relay Tor, n'hésitez surtout pas :
<http://www.torproject.org/docs/tor-doc-relay.html.fr>

Conclusion

Ben voilà... j'espère que vous êtes un peu plus armés maintenant pour ne plus vous laisser faire !!

Bye

Laiguillon - Mars 2008

Liens :

Définition des termes (WikiPedia)

Malware : http://fr.wikipedia.org/wiki/Logiciel_malveillant
Virus : http://fr.wikipedia.org/wiki/Virus_informatique
Logiciels espion : http://fr.wikipedia.org/wiki/Logiciel_espion
Chevaux de Troie : http://fr.wikipedia.org/wiki/Cheval_de_Troie_%28informatique%29
Hameçonnage : <http://fr.wikipedia.org/wiki/Hame%C3%A7onnage>
Traceurs de frappe : http://fr.wikipedia.org/wiki/Enregistreur_de_frappe
Rootkit : <http://fr.wikipedia.org/wiki/Rootkit>
Vers : http://fr.wikipedia.org/wiki/Ver_informatique
Spam : <http://fr.wikipedia.org/wiki/Pourriel>
Porte dérobée : <http://fr.wikipedia.org/wiki/Backdoor>

Se renseigner si c'est un Hoax : <http://www.hoaxbuster.com/>

Outils de détection (tous gratuits et testés au moins un minimum par mes soins...of course)

RootKits : RootkitRevealer [http://technet.microsoft.com/fr-fr/sysinternals/bb897445\(en-us\).aspx](http://technet.microsoft.com/fr-fr/sysinternals/bb897445(en-us).aspx)
Malware and spyware : Ad-aware <http://www.lavasoftusa.com/single/trialpay.php>
Spywares : Spybot Search & Destroy <http://www.spybot.info/fr/index.html>
Anti-virus, worms et tojans : Avira Antivirus <http://www.free-av.fr/>

Effaceurs de traces

EasyCleaner : <http://personal.inet.fi/business/toniarts/ecleane.htm>
MRU-Blaster : <http://www.snapfiles.com/get/mrublaster.html>
Eraser : <http://www.bugbrother.com/eraser/>

Protections de FireFox et modules intéressants

Module NoScript : <https://addons.mozilla.org/fr/firefox/addon/722>
Module Shazou (géolocateur) : <https://addons.mozilla.org/en-US/firefox/search?q=shazou&status=4>
Testeur de sécurité du navigateur: <http://www.jasons-toolbox.com/BrowserSecurity/>
Testeur de Popups de publicité pour navigateur: <http://www.proxomitron.info/tests/index.html>

Encryption de messages: windows + winpt + thunderbird + enigmail

Le portage de GPG sous Windows : Winpt - <http://winpt.sourceforge.net/fr/download.php>
Le plug-in PGP pour Thunderbird : Enigmail - <http://enigmail.mozdev.org/download/index.php>
Un petit tutoriel : http://cd.eitic.net/logiciels/winpt/tuto_enigmail.pdf

Nettoyage des Processus Inutiles Microsoft:

Renseignements en Français sur chaque processus : <http://www.gsiteg.com/processus.php>

Astuces pour les processus inutiles: <http://www.pcastuces.com/pratique/windows/services/page4.htm>

Astuces 2 pour les processus inutiles: <http://www.coolxp.fr/tutorial/services/services.htm>

Nettoyage des Fichiers Inutiles Microsoft:

Outil CCleaner : <http://www.libellules.ch/desinstal.php>

Soulagement de la mémoire Windows:

<http://www.zonewindows.com/astuce36.php>

<http://www.zonewindows.com/astuce15.php>

<http://www.tuto-underground.net/tutorial-225-optimiser-son-systeme-windows-tutoriels-tutoriaux-tutorial-didacticiel-gratuit.html>

Protéger son ordinateur et réseau à la maison

Protections WiFi : http://www.securiteinfo.com/attaques/phreaking/securite_reseaux_wifi_wardriving.shtml

Pare-Feu ou Firewall:

Subelt Personal Firewall 4 : <http://www.sunbelt-software.com/Home-Home-Office/Sunbelt-Personal-Firewall/Download/>

Jetico version 1 ou 2 : <http://www.jetico.com/download.htm>

ZoneAlarm: <http://www.zonealarm.com/store/content/company/products/znalm/freeDownload.jsp>

Comodo : http://www.personalfirewall.comodo.com/download_firewall.html

Antivirus:

Un comparatif parmi d'autres : <http://www.clubic.com/article-77079-1-guide-comparatif-meilleur-antivirus.html>

Avast <http://www.avast.com/fre/download-avast-home.html>

Avira AntiVir http://www.free-av.de/en/download/1/avira_antivir_personal_free_antivirus.html

Pour Thunderbird, lisez: <http://www.geckozone.org/forum/viewtopic.php?t=22467>

AntiSpyware:

SpyBot Search & Destroy: <http://www.spybot.info/fr/spybotsd/index.html>

Outils d'analyse de votre machine Microsoft: <http://technet.microsoft.com/en-us/sysinternals/default.aspx>

Téléchargements P2P

Choix: <http://www.commentcamarche.net/telecharger/logiciel-34-telechargement>

Clients:

emule : <http://www.emule-project.net/home/perl/general.cgi?l=13>

edonkey: <http://www.edonkey2000-france.com/index.php?pagetype=downloads&flash=>

amule: <http://www.amule.org/>

xmule: <http://sourceforge.net/projects/xmule>

mildonkey: http://mildonkey.sourceforge.net/Main_Page

brouillage et securite emule:

http://divxplanetv2.free.fr/?cat=securisation_emule

<http://www.numerama.com/magazine/3259-eMule-se-dote-d-un-brouillage-pour-eviter-le-bridage.html>

effacement des traces emule: <http://www.article12.fr.nf/traces-de-certains-logiciels-sous-xp/emule-0.48a-effacer-ses-traces-2.html>

Téléchargements P2P sécurisés

Freenet : Site: <http://www.freenet-doc.info/index.php/Accueil>

Doc: <http://fr.wikipedia.org/wiki/Freenet>

Omemo : Site: <http://www.omemo.com/>

Doc: <http://fr.wikipedia.org/wiki/Omemo>

Mute : Site : http://mute-net.sourceforge.net/index_fr.shtml

Doc: http://fr.wikipedia.org/wiki/Mute_%28logiciel%29

GNUNet : Site: <http://gnunet.org/index.php?xlang=French>

Doc: <http://fr.wikipedia.org/wiki/GNUNet>

Téléchargements NNTP

Choisir un fournisseur: <http://www.usenetforyou.com/>

Télécharger GrabiT (client newsgroup) : <http://www.shemes.com/index.php?p=download>

Utiliser GrabiT: <http://www.usenetforyou.com/grabit.html>

Sécurisation : <http://www.usenetforyou.com/bridage-newsgroups-free.html>

Surf Anonyme

LiveCD - Liste : http://fr.wikipedia.org/wiki/Liste_des_LiveCD

AnonymOS: <http://www.infododos.com/guides/view-guide-19.html>

Proxy:

Pour les proxy HTTP

Liste de proxies publiques : <http://www.free-proxy.fr/>

Un testeur de proxies qui valide les bons : <http://www.project2025.com/charon.php>

Extension switchproxy pour FireFox : <https://addons.mozilla.org/fr/firefox/addon/125>

Pour le socks (vos emails, etc...)

Clients SOCKS

humminbgbird : <http://connectivity.hummingbird.com/products/nc/cpsecurity.html>

sockscap : <http://soft.softoogle.com/ap/sockscap-download-5157.shtml>

freecap: <http://www.freecap.ru/eng/?p=download>

Liste des proxy socks dispo : <http://www.samair.ru/proxy/socks.htm>

Aide sockscap: <http://websecurite.free.fr/anonymat.htm>

Vérification anonymat: <http://privacy.net/>

Tor:

article Framasoft: <http://www.framasoft.net/article4338.html>

Documentation et site de Tor: <http://www.torproject.org/overview.html.fr>

Sites de références pour la dénonciation du manque de transparence d'internet

CNIL Commission Nationale de l'Informatique et des Libertés : <http://www.cnil.fr/>

Anonymat.org : <http://www.anonymat.org/>