Dossier

Prévention et Sécurité

v 20071215

Sommaire

1- Prévention

1- Comment les menaces informatiques font-elles pour infecter système d'exploitation? Comment faire pour s'en prémunir ?

Des questions qui semblent évidentes, mais qui ne le sont pas forcément pour les nombreuses personnes débutantes dans le domaine de l'informatique.
De manière générale, ce qui semble évident pour les uns ne l'est pas forcément pour les autres.

Nous sommes un groupe de six internautes passionnés de sécurité informatique et chaque jour nous désinfectons bénévolement des dizaines d'ordinateurs sur plusieurs grands forums français d'entre-aide.

Aujourd'hui, les raisons qui nous poussent à vous interpeller dans votre quotidien sont issues d'un bien triste constat. En effet, 3/4 des infections rencontrées pourraient être évitées et malgré tous les efforts déployés pour sensibiliser, il reste un facteur immuable qui se doit de changer, de se responsabiliser et ce maillon c'est VOUS.

C'est pourquoi nous avons pris l'initiative de rédiger collectivement cet article afin de vous apporter des conseils et ainsi apprendre, par exemple, à éviter les pièges les plus répandus sur la toile. A ce jour, il n'existe pas de technologies capables de protéger efficacement un ordinateur si l'internaute n'est pas instruit sur les risques encourus sur la toile. Ce transfert de ces connaissances est indispensable pour construire l'Internet.

- La partie sur la prévention fait le point sur les principaux vecteurs d'infections aujourd'hui : du téléchargement aux vers par messagerie instantanée.
- La partie sur la protection vous donnera les meilleures pistes pour vous prémunir. Le texte est volontairement simple et épuré. Si vous souhaitez en connaître davantage, il vous suffira de cliquer sur les nombreux liens que nous présentons.

Angeldark (IDN, Informatruc)
Bibi26 (Zebulon)
JokuHech (abcdelasécurité)
Malekal_Morte(01.net, Malekal, Zebulon)
Sham_Rock (GNT, IDN)

Bonne lecture,

2- Pourquoi y a-t-il des infections informatiques ?

L'argent motive sans conteste les créateurs de programmes malveillants. Ce n'était pas le cas des premiers créateurs de virus dans le milieu des années **80**. À cette époque, c'était plutôt par défi, montrer qu'ils en étaient capables, ou provoquer tout simplement. Les infections **se contentaient** de se dupliquer d'elles-mêmes, d'afficher un message, et détruisaient parfois (rarement) des données.

De nos jours, ces programmes sont source de revenus et les **moyens** sont divers :

- Attaque en masse (*DDOS*) à partir d'ordinateurs détournés,
- Envois de publicités mails à partir d'ordinateurs détournés (*spam*),
- Affichage de publicités (*popup*),
- Arnaques avec de faux logiciels de sécurité (*rogues*),
- Vol de données, de mots de passe, de numéros de série de logiciels...
- Redirection vers des sites frauduleux (*phishing*),
- Chantage (*ransomware*),
- Etc.

Pour arriver à leur fin, la plupart des infections se doivent de **rester discrètes** afin de rester le plus longtemps chez leurs hôtes. On **pourra** suspecter une infection dans le cas d'affichage de popups, ou par une activité douteuse du système, voire de la connexion Internet.

Le nom virus s'appliquant à une famille bien précise d'infection on utilisera plutôt *malware*, un terme plus global. On parlera aussi de *crimeware* au vu des actions **frauduleuses** de ces applications.

3- Comment les infections sont arrivées dans le système ?

Dans la très grosse **majorité** des cas, c'est **l'utilisateur** lui-même qui invite sans le savoir ces compagnons indésirables par un excès de confiance. Simplement en **exécutant** des programmes téléchargés.

En outre, certains sites volontairement mal conçu permettent d'exploit les failles, les vulnérabilités de votre ordinateur ou de vos logiciels.

Les **principaux vecteurs** d'infections seront traités dans les parties suivantes :
I Les cracks et les keygens
II Les faux codecs
III Les logiciels gratuits
IV Les rogues, les faux logiciels de sécurité
V La navigation sur des sites à haut risque d'infections
VI Les pièces jointes et les vers par messagerie instantanée
VII Les Hoax et phishing, attention à ne pas vous faire abuser

1- Les cracks et les keygens

Pour utiliser des **logiciels payants** sans débourser le moindre centime, nombreux sont ceux qui **enlèvent** les protections à l'aide d'un programme appelé communément *crack* ou **inscrivent** un numéro de série généré par un *keygen*. Toutes ces applications facilitant le piratage ne sont pas forcément contaminées, mais les auteurs de *malwares* font maintenant passer leurs créations **malignes** comme étant ce type de programme.

Ainsi, en pensant faire sauter la protection d'un logiciel, l'utilisateur trop confiant exécute un programme malveillant avec ses **droits d'administrateur**, ce qui permettra l'infection du système.

Voici deux exemples issus d'un rapport d'un antivirus provenant d'un ordinateur infecté :

- C:\Documents and Settings\...\shared\ **Symantec.Norton.Ghost.10.patch.crack.zip** -> *Trojan-Downloader.Win32.Agent.bgy*
- C:\Program Files\eMule\Incoming\ **Camfrog_v3.72_PRO + CRACK.zip** -> *Trojan-Spy.Win32.KeyLogger.lu*

Sachez que les auteurs de malwares créent de **faux sites de cracks** où tous les cracks proposés sont infectieux, d'autres sites eux contiennent des exploits, si votre navigateur n'est pas à jour, c'est l'infection assurée.
En outre, certaines infections issues de cracks proposés sur les réseaux P2P, une fois installées mettent à disposition des cracks piégés sur le réseau **P2P** pour que d'autres internautes les téléchargent et s'infectent:

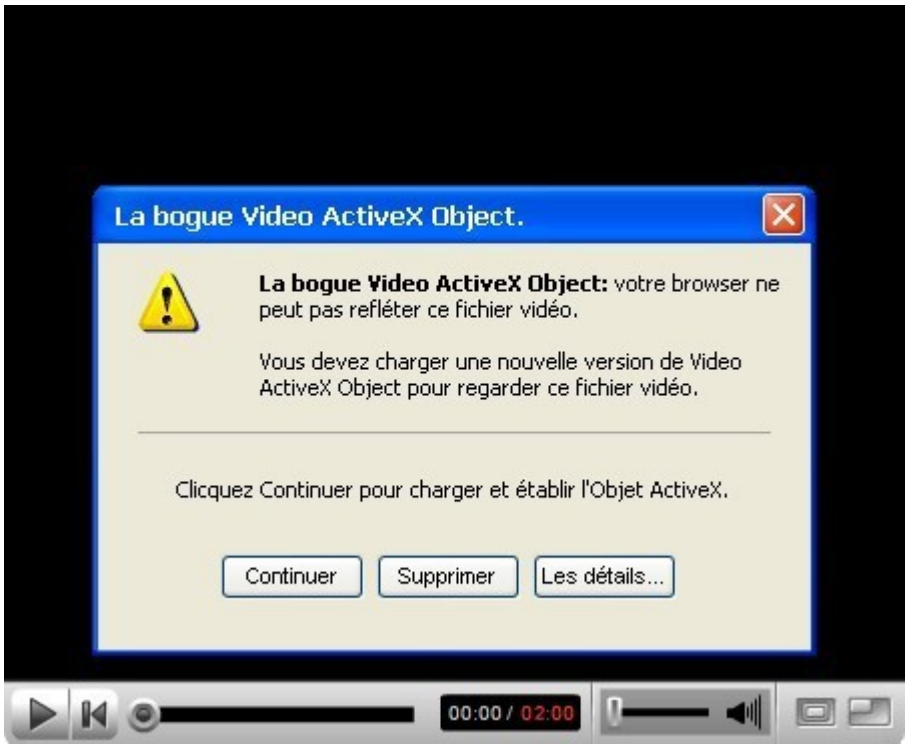
- **exemple avec l'infection Security Toolbar 7.1**
- **cracks/P2P**
- **Le Danger des cracks!**

2- Les faux codecs

La technique ne change pas, **l'utilisateur** est invité à exécuter un programme (**malsain** dans la réalité) pour laisser entrer l'infection dans le système.

Afin de visionner une séquence vidéo provenant des sites **pornographiques** ou parfois **humoristiques**, il vous est demandé d'installer un *codec* ou un *ActiveX*.

L'installation du logiciel demandé semble se dérouler normalement. Mais c'est bien l'infection que l'utilisateur **exécute** sur son système. Et les **effets** indésirables ne tardent pas à apparaitre:



- fausses alertes de sécurité,
- modification du fond d'écran,
- détournement de la page d'accueil du navigateur...
- installation non désirée de faux logiciels de sécurité (*rogue*) proposant leurs services payants pour nettoyer l'infection.

Plus d'informations sur les faux codecs

3- Les logiciels gratuits

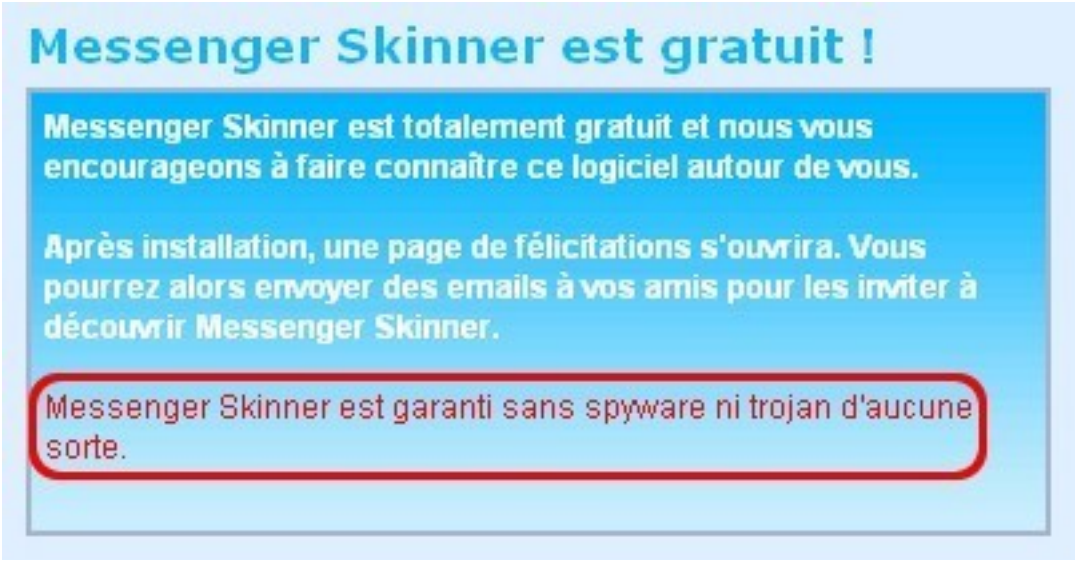
Faites-vous partie des personnes qui font confiance à tous les programmes ayant la mention "*gratuit*" ?
Lisez-vous les **conditions d'utilisation** (le texte immense écrit en tout petit pendant l'installation) ? Faites-vous partie des personnes qui cliquent sur *Suivant* jusqu'à lancer l'installation ?
C'est certainement le cas, il y a donc des réflexes à changer.

Une bonne initiative des éditeurs peut **cacher** des méthodes d'un tout autre genre.
En abusant de votre confiance grâce à la méthode du *social engineering* ces éditeurs infecteront votre machine afin de gagner de l'**argent** avec leurs logiciels gratuits.

Nous allons prendre l'exemple de l'adware **Magic.Control** qui s'installe avec les logiciels suivants :

- go- astro
- GoRecord
- HotTVPlayer
- MailSkinner
- Messenger Skinner
- Instant Access
- InternetGameBox
- sudoplanet
- Webmediaplayer

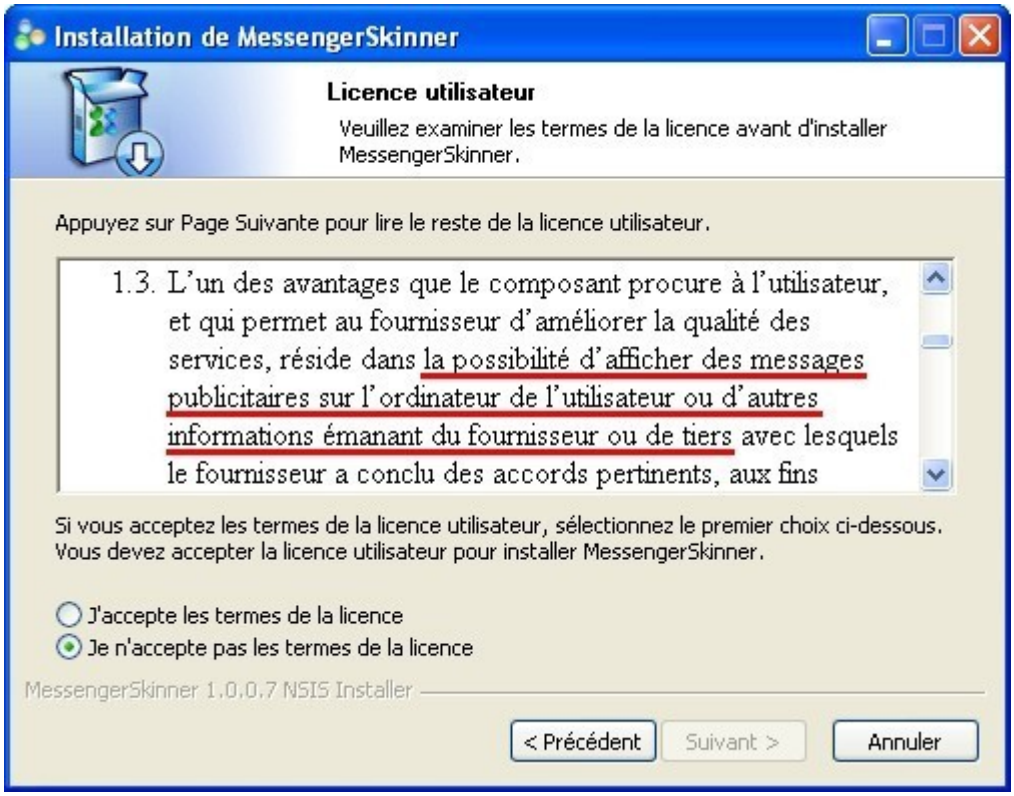
Une fois un de ces programmes installés, vous serez submergés sous les publicités.
Voici un exemple d'une page web :



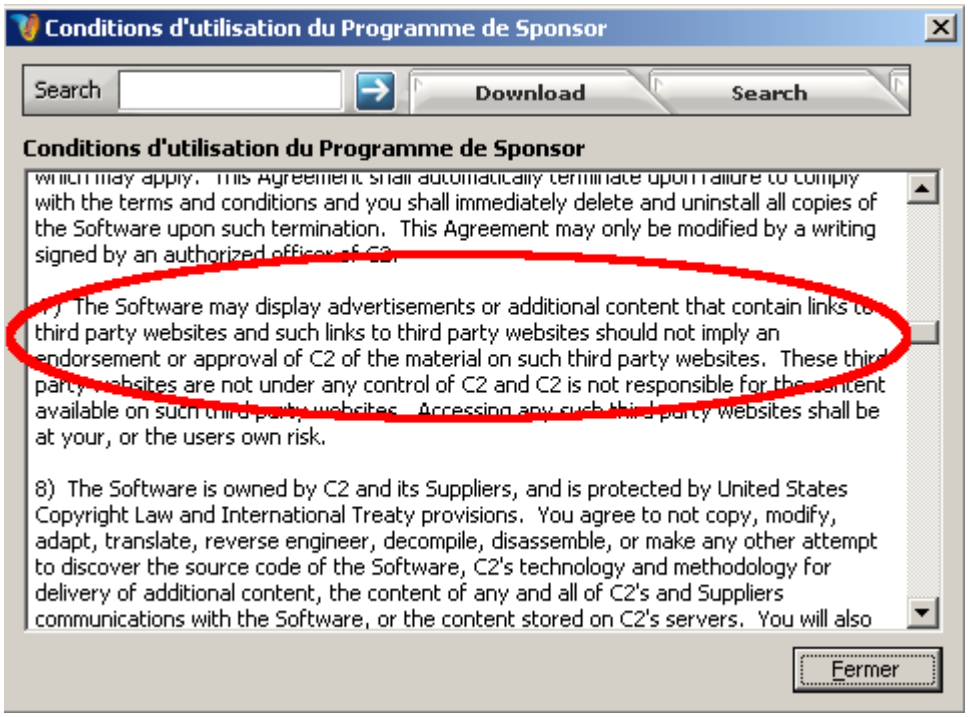
Regardez le bas de la page : *No Spyware*, *C'est gratuit*. Sans connaître l'éditeur, vous lancez l'installation et viendra avec elle l'**infection**.

Voici un exemple d'autres programmes installant l'adware lop.com/Swizzor, ce dernier est proposé sur l'add-on Messenger Plus! ou des programmes de P2P torrent (BitDownload, Bitroll, NetPumper etc.).

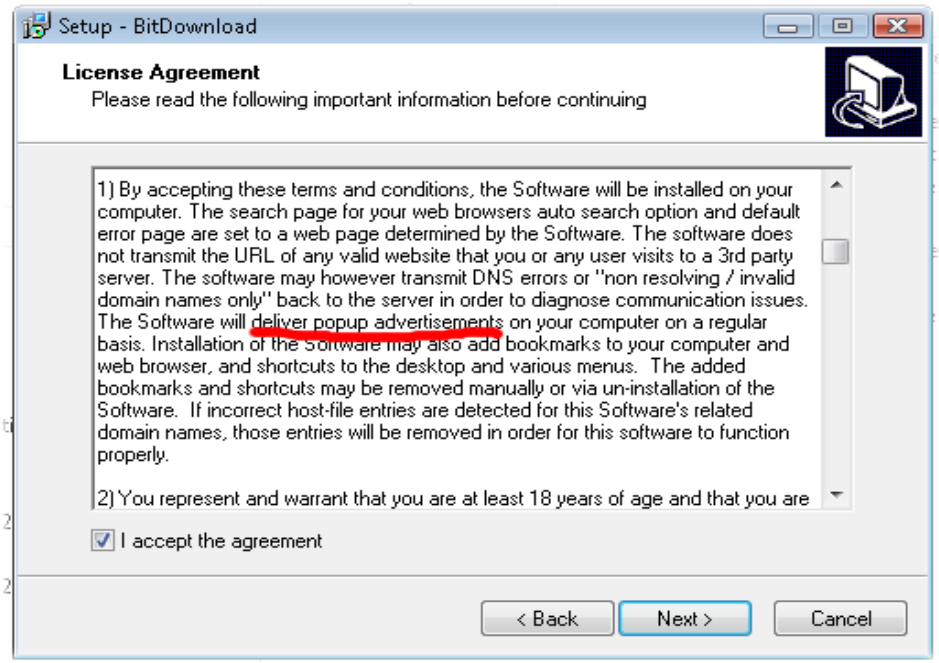
Encore une fois, dans l'EULA, il est clairement écrit que les dits programmes ouvriront des popups de publicités.



EULA de Messenger Plus!



EULA de BitDownload



Il ne faut donc pas télécharger tout et n'importe quoi sous prétexte que le logiciel est une nouveauté.

Par ailleurs, un logiciel présent sur un site de **téléchargement reconnu** ne doit pas être

installé sans se poser de question.
Prenez le temps pour **juger** de la fiabilité du programme, une simple recherche sur un moteur de recherches suffit généralement.

En outre, des services en ligne proposent le scan de fichier sur de multiples antivirus ce qui donner une idée sur comme :

- VirusTotal
- Virscan

Voici une liste de quelques programmes installant des adwares :

Logiciels	Domaine	Spyware/Adware installés	Commentaires
3wPlayer	3wplayer.com	CiD/Lop	
BitDownload	bitdownload.org	CiD/Lop	
BitGrabber	bitgrabber.com	CiD/Lop	
Bitroll	bitroll.com	CiD/Lop	
DivoPlayer	divoplayer.com	CiD/Lop	
eoClock	eorezo.com	eoRezo	
eoCPU	eorezo.com	eoRezo	
eoMail	eorezo.com	eoRezo	
eoMap	eorezo.com	eoRezo	
eoMeteo	eorezo.com	eoRezo	
eoNet	eorezo.com	eoRezo	
eoPhoto	eorezo.com	eoRezo	
eoRss	eorezo.com	eoRezo	
eoSudoku	eorezo.com	eoRezo	
eoTraduction	eorezo.com	eoRezo	
eoWikipedia	eorezo.com	eoRezo	
GoRecord	go-astro.com	Navipromo/Magic Control	
HotTVPlayer	mailskinner.com	Navipromo/Magic Control	
Instant Access		Navipromo/Magic Control	Dialer pour sites pornographiques
InternetGameBox	internetgamebox.com	Navipromo/Magic Control	Dialer pour sites pornographiques
Kazaa	kazaa.com	Cydoor, InstaFinder, RX Toolbar	
KitPlayer	kitplayer.com	CiD/Lop	
MailSkinner		Navipromo/Magic Control	
Messenger Plus! Live	msgpluslive.fr	CiD/Lop	A l'installation, choisir de ne pas installer le sponsor.
Messenger Skinner	messengerskinner.com	Navipromo/Magic Control	
NetPumper	netpumper.com	CiD/Lop	
sudoplanet	sudoplanet.com	Navipromo/Magic Control	Dialer pour sites pornographiques
Torrent101	torrent101.com	CiD/Lop	
Torrentq	torrent101.com	CiD/Lop	
Warez P2P	warez.com	CiD/Lop	
Warez P2P	warez.com	CiD/Lop	
Webmediaplayer	web-mediaplayer.com	Navipromo/Magic Control	Dialer pour sites pornographiques
Winzix	winzix.com	CiD/Lop	
Wowpapers	wowpapers.com	Hotbar	

4- Les rogues, les faux logiciels de sécurité

Le mot anglais *rogue* a pour signification **escroc**. Ce terme est aussi utilisé pour désigner un faux-logiciel de sécurité. Il en existe plusieurs catégories: anti-spyware, antivirus... Le but de ce faux logiciel est de **pousser** l'utilisateur à acheter une licence payante:

Soit via des **publicités** sur des sites WEB qui redirigent vers les sites qui fabriquent ces rogues.

Soit en installant des **infections** sur votre ordinateur :

- affichage de **bulles d'alertes** disant que votre ordinateur est infecté.
- modification de votre **fond d'écran** en disant que votre ordinateur est infecté.
- modification de la **page de démarrage** de votre ordinateur vers des sites affichant **de fausses alertes de sécurité**

A noter que les alertes sont en général en langue anglaise.

Chaque alerte propose de télécharger un de ces **rogues.** Une fois le scan (**totalement** mensonger) de l'ordinateur effectué par le programme, ce dernier affiche qu'il faut acheter la version commerciale pour nettoyer l'ordinateur.
Le but est donc de faire **peur** et forcer la main, via des alertes incessantes, d'acheter la version commerciale de ces boîtes vides.

Voici un exemple de bulles d'alertes :

Le site **Malekal.com** propose une liste de rogues **ici**. Vous pouvez également consulter la **crapthèque** d'Assiste.
En Anglais, **Spyware Warrior** publie aussi une liste de **rogues**.

Encore une fois, effectuez une simple **recherche** sur google est plus que recommandé. Cette simple recherche peut permettre de **déterminer** si le logiciel est nuisible ou pas !

5- La navigation sur des sites à haut risque d'infections

Les **failles de sécurités** permettent d'infecter votre ordinateur automatiquement et à votre insu.
A l'heure actuelle, les failles sur les navigateurs WEB sont très exploitées, ces failles permettent via la consultation d'un site WEB *malicieux* d'infecter votre ordinateur de manière automatique. Le seul rempart si votre navigateur WEB est vulnérable reste votre antivirus, ces

infections sont très souvent mises à jour afin de s'assurer que les antivirus ne puissent pas suivre la cadence.
Les chances d'infections si votre navigateur WEB est vulnérable restent très élevées.

Certains sites WEB sont *hackés* afin d'y déposer le code malicieux permettant l'infection, d'autres sites (notamment pornographiques) sont payés par les auteurs de malwares (ce sont des formes de sponsors) pour y ajouter le code malicieux.

Pour être **infecté via un site WEB**, il faut donc remplir les conditions suivantes :

- avoir un navigateur WEB vulnérable (*donc pas à jour*).
- surfer avec les droits administrateurs
- consulter un site WEB avec du contenu malicieux
- antivirus qui laisse passer l'infection.

Le projet **honeynet.org** a effectué une étude sur ce type d'infection, il en ressort le tableau suivant :

source: honeynet.org *(Table 2 %u2013 Identified malicious URLs/ hosts by category)*

Cette étude montre que les trois premiers sites WEB vecteurs de malwares exploitants des failles de sécurité ont un contenu pour adultes, warez (cracks, issus de liens de Spam, téléchargements illégaux.).

Les habitudes de surfs sont alors très importantes, on comprend très bien qu'un internaute qui va sur des **sites pour adultes ou qui télécharge des cracks** a beaucoup plus de chances de se faire infecter qu'un internaute qui va sur des sites de musiques ou lire les actualités en ligne!

Les mauvaises habitudes de surf sont un vecteur important d'infection !

Il convient ensuite de maintenir son système à jour, éviter d'utiliser le compte administrateur, etc. Tout ceci est abordé plus longuement dans la seconde partie.

Plus d'informations sur les failles de sécurités :

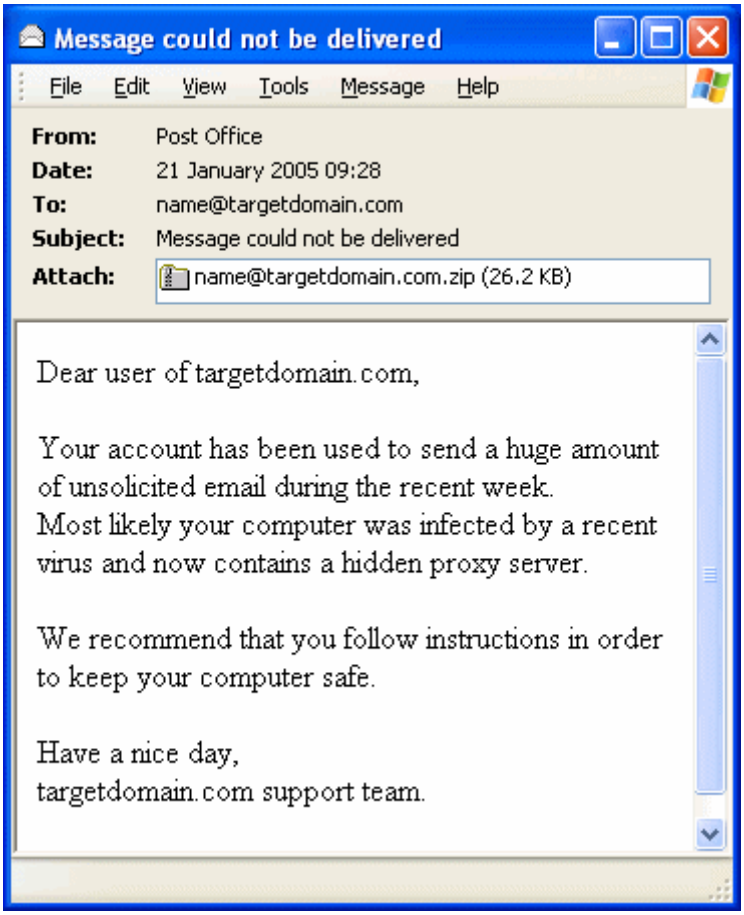
Category	Malicious Hosts	Malicious URLs	% Malicious URLs
Adult	102	195	0.5735
Spam	17	19	0.1658
Warez	19	27	0.0602
Typo	13	13	0.0567
News	15	20	0.0424
User Content	12	13	0.0284
Music	10	11	0.0223
Sponsored Links	4	7	0.0166
Defacement/Vuln	1	1	0.0002

- **Exploitation des failles**
- **Web : du problème à la solution**
- **Exploits sur les sites WEB**
- **Know Your Enemy: Malicious Web Servers**

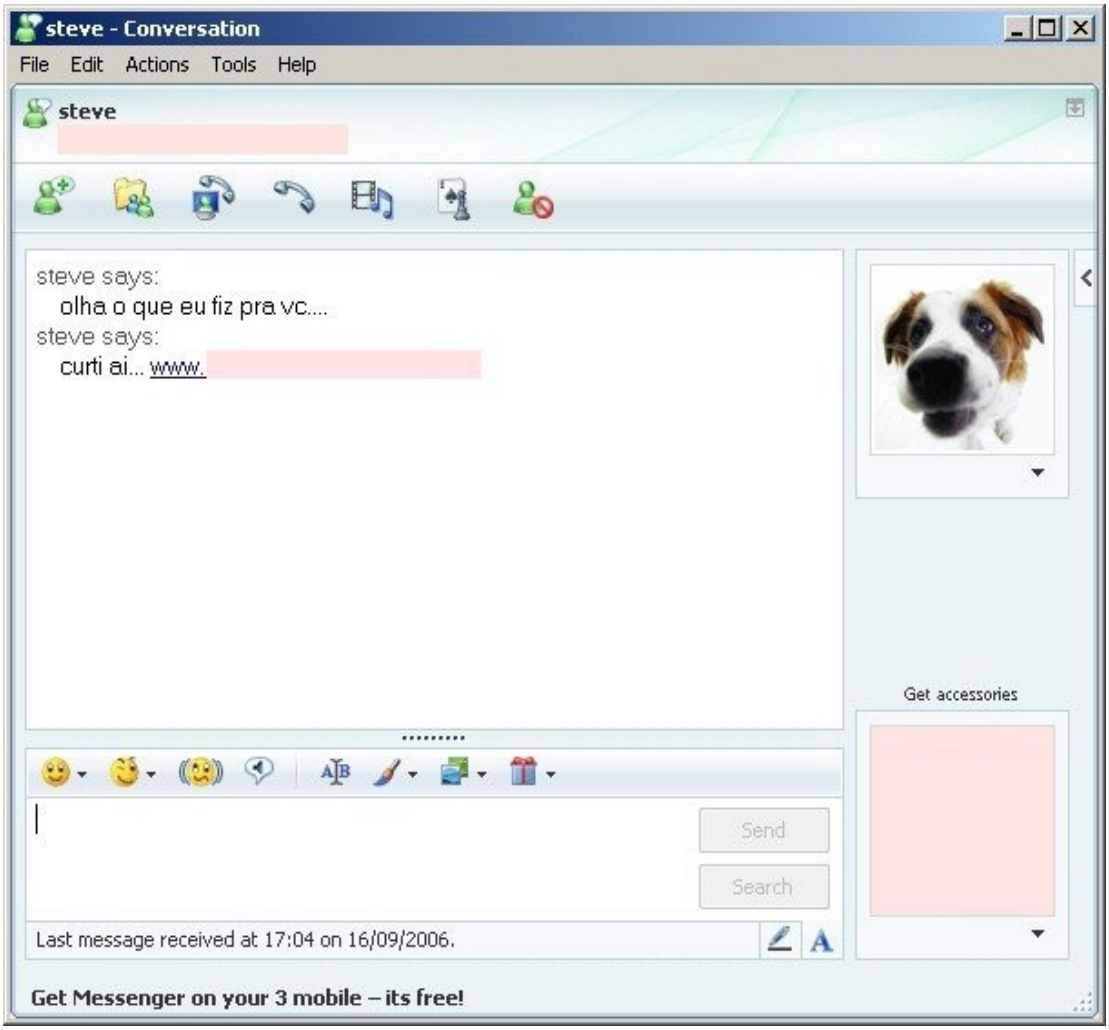
6- Les pièces jointes et les vers par messagerie instantanée

Comme beaucoup de gens, vous recevez peut-être plusieurs emails **dont vous ne connaissez pas le destinataire** qui vous incite à cliquer sur un lien ou à ouvrir une pièce jointe. La règle est plutôt simple : si vous ne connaissez pas le destinataire, supprimez le message. Même si le message paraît venir de Microsoft ou de votre meilleur ami, vous devez faire attention, car

l'**adresse** peut très bien avoir été **falsifiée** ou votre meilleur ami peut être très bien infecté sans le savoir.



Ce qui est bien, c'est que la plupart des internautes ont compris qu'il ne fallait pas ouvrir des pièces jointes venant d'un inconnu. Malheureusement, la méthode d'infection a évolué et il n'est pas rare de voir des **vers par messagerie instantanée** (comme MSN). Ces vers utilisent une méthode plutôt ingénieuse en se propageant par le biais de vos propres contacts et en vous incitant à cliquer sur un lien ou à ouvrir une pièce jointe. Le mieux est encore de **ne pas cliquer bêtement**.



7- Les Hoax et phishing, attention à ne pas vous faire abuser

Nous sommes tous confrontés à des **Hoax**: Ce sont des **canulars** qui circulent sur le net et qui sont véhiculés par mails. Vos proches souhaitent vous faire partager une information qu'ils jugent importante alors qu'en fait, ce n'est qu'un leurre destiné à engorger le réseau Internet. Ce sont le plus souvent de *fausses alertes de virus* ou, ce qui est bien plus pervers, de *fausses chaînes de solidarités*.

Tout mail se terminant par des phrases du type « envoyez ce mail à tous vos contacts pour ... » demandant à propager l'information est certainement un hoax, **vérifiez la véracité du contenu du mail.**

Le site **hoaxbuster.com** mène une véritable lutte contre ces fausses informations. Vous pouvez utiliser leur formulaire de recherche pour y vérifier le "scoop" que vous venez de recevoir.

Depuis quelques années, les pirates du web s'attaquent à une nouvelle forme d'escroquerie en masse via **le phishing**: Ils spamment des milliers d'internautes avec des messages dans le but de leur **voler des informations bancaires**. Leur procédé est très astucieux: ils envoient un mail avec un lien vers un site qui ressemble "*presque*" parfaitement au portail de votre banque. "*Presque*" car l'adresse n'est pas la même et **jamais** une banque ne vous demanderait des informations confidentielles en ligne. L'internaute trop confiant enverra ainsi des informations bancaires à ces pirates et le résultat ne se fera pas attendre: les pirates n'ont plus qu'à se servir de ces informations pour ponctionner de l'argent sur son compte en banque.

La règle est donc simple: Ne jamais fournir d'informations confidentielles même si c'est votre banque qui en fait la demande. Les organismes bancaires connaissent suffisamment ces questions de sécurité bancaire pour ne pas faire ce genre de choses.

Voici deux captures de phishing provenant de banques françaises. Comme vous pouvez le constater le mail semble réaliste, n'importe quel prétexte est utilisé pour vous demander des informations :

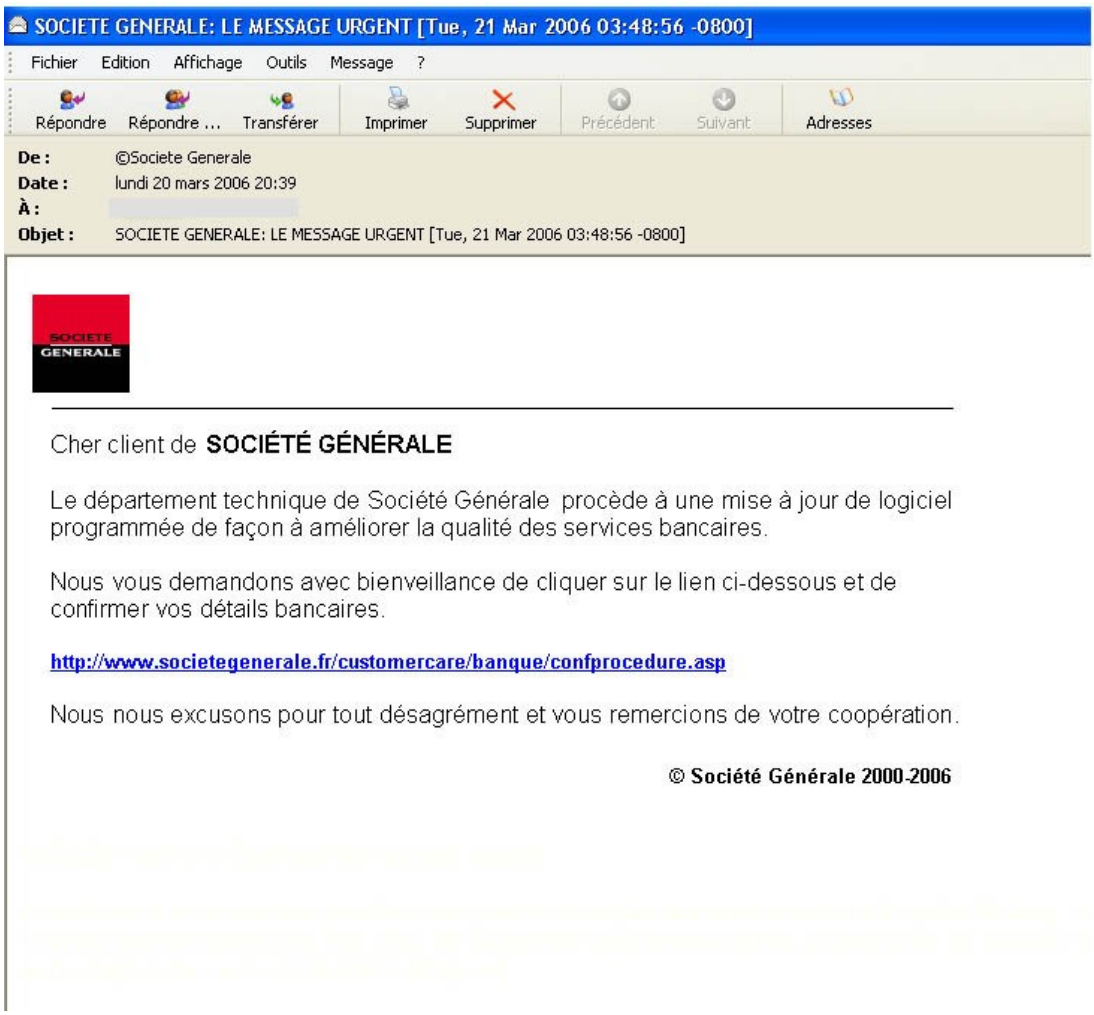
Le test du nouveau systeme de securite. Notre devise: Banking sans fraude.

Compte tenu d'accidents tres frequents provoques par des activites frauduleuses sur Internet, notre banque a introduit le nouveau systeme de securite de nos clients. Conformement a celui-la chaque mois vous serez le destinataire d'une lettre confirmante vos donnee secretes. Nous esperons votre comprehension a l'egard de cet innovation. Les mesures entreprises nous permettront de reduire les risques d'acces non sanctionne de tierces personnes a votre compte personnel, ainsi que controler l'activite de votre compte en comparant l'adresse IP et version de votre navigateur de votre session presente et celle precedente. A l'avis de l'organisation mondiale bancaire ces mesures permettront de diminuer au maximum les voles d'argent des clients.

Log in: lecreditlyonnais

Si vous n'etes pas d'accord ou mecontent de cet innovation veuillez nous ecrire a lecreditlyonnais@banksecurity.fr
votre opinion sera prise en compte.

Nous vous remercions de nous avoir accorde vote temps et prions d'accepter nos salutations distinguees.



Pour en savoir plus: **Phishing : les moyens de lutter**

4- *Conclusion*

Internet est un média de plus en plus démocratisé, le nombre d'internautes grandissant, il s'avère être une mine d'or pour des groupes sans scrupules qui s'enrichissent sur le dos des internautes.

Les pièges et menaces sont maintenant omniprésents, si une protection est recommandée, **une attitude sensée fera la différence**. Il conviendra d'éviter:

- l'utilisation de cracks, il existe des **logiciels libres** qui évitent de prendre des risques et de se mettre dans l'illégalité en piratant.
- le surf sur les sites pornographiques.
- l'installation de tout logiciel/plugin sans une recherche sur sa provenance et ses effets indésirables.

- les logiciels proposés via des publicités contenues sur les sites WEB.
- les logiciels dit gratuits (une recherche Google sur le nom du logiciel permet d'avoir des renseignements sur les effets indésirables).
- l'exécution des fichiers reçus depuis MSN ou par email. Même si l'antivirus ne détecte rien.

Si vous avez un doute sur un fichier, **VirusTotal** permet de le scanner avec plusieurs antivirus.

2- Comment se protéger?

La règle de base est la **méfiance**. Même en étant protégé, l'exécution d'un fichier inconnu peut s'avérer risquée.

- Utiliser un compte utilisateur limité : utilisation identique des programmes, mais l'installation de logiciels et indirectement de malwares est limitée.
- Tenir son système à jour (Failles OS et Logiciels)
- Utiliser **un** antivirus et **un** antispyware et les tenir à jour. Il ne faut pas donner une confiance absolue dans son antivirus.

1- Utiliser un compte utilisateur limité

Windows 2000, XP et Vista utilisent le système de fichiers **NTFS** (New Technology File System).

NTFS permet de gérer les autorisations et restrictions sur les dossiers et fichiers, mais aussi les utilisateurs inscrits (ou non) sur votre ordinateur.
Il est aussi intéressant de noter que NTFS nous arrive avec la section Serveurs sous Windows.

Pour savoir si vous utilisez ce système de fichiers :

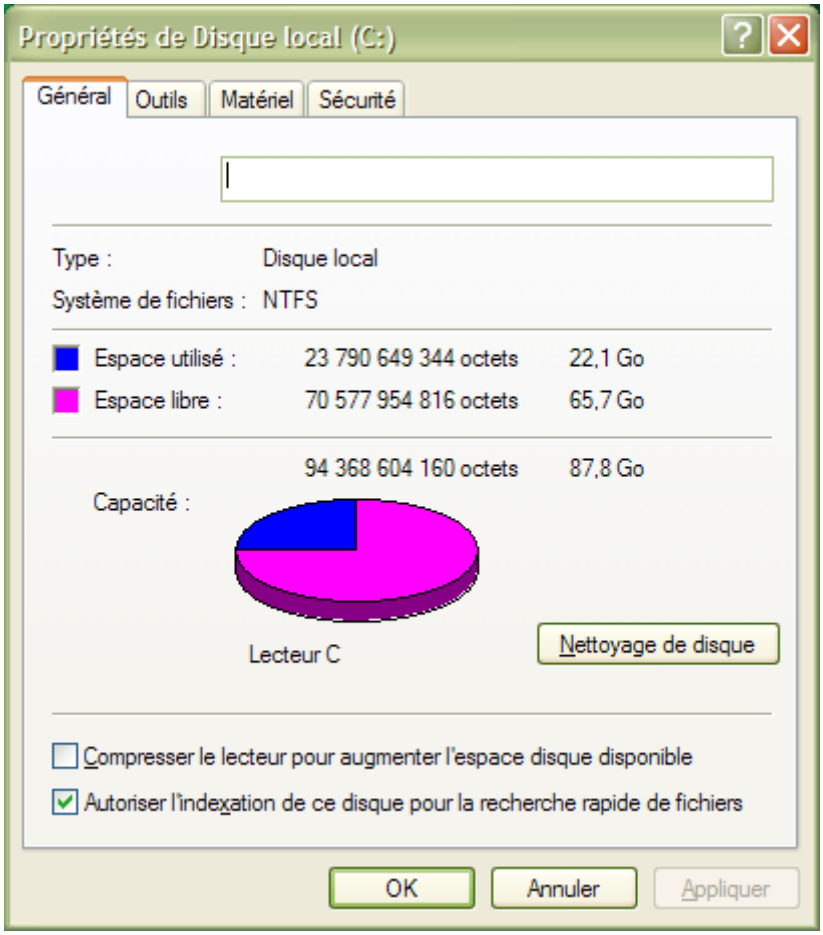
Cliquer sur **Démarrer** puis **Poste de travail**. Poursuivez avec un clic bouton droit de souris sur le **Disque local C:**

Dans le menu contextuel qui s'affiche, choisissez **Propriétés**.

Qu'est ce qu'un compte limité ?

En fait, le terme est assez mal choisi. Le mot "limité" est une erreur de traduction. En établissant un parallèle avec les systèmes Unix, il s'agit d'un simple compte d'utilisateur usuel.

Sous Windows, ce compte disposera de tout ce qu'il faut pour permettre un usage **confortable**



de l'ensemble du système, et pour peu que vous sachiez comment faire, vous pourrez même **administrer Windows, à partir d'un compte de ce type**.

Choisir l'utilisation de comptes limités ou standards est déjà une "stratégie de sécurité à part entière".
Vous trouverez cette dénomination sur Windows 2000 et Windows XP. Windows Vista appellera ce compte: "standard", vous en conviendrez, c'est déjà un progrès appréciable.
Ces comptes feront partie d'un groupe appelé: Tous les utilisateurs.

Ce groupe est soumis à des restrictions (restrictions qui seront toujours prioritaires contrairement aux autorisations accordées). Parmi ces restrictions, celle qui fera **la** différence.

Vous pourrez lancer une application (droit d'exécution) qui elle-même aura des droits en lecture seule, afin de fonctionner correctement. Cependant, vous n'aurez pas le droit à l'écriture (droit de modification) sur les composants de cette application. Ceci est une explication théorique et schématisée à l'extrême; dans les faits, c'est nettement plus complexe.

- Toute règle apporte ses exceptions.

Tout utilisateur dispose de son propre répertoire, et à ce titre, il en est détenteur de tous les droits. Ceci lui permet de créer, modifier, exécuter et supprimer des documents, fichiers et dossiers. Ce qui veut donc aussi dire que si vous disposez d'une application qui installe des composants dans votre propre répertoire, vous en devenez propriétaire, mais uniquement de la partie dans votre répertoire. Vous pourrez en user comme bon vous semble. Un exemple concret, le navigateur Web Mozilla Firefox. Sous votre propre compte d'utilisateur, vous installerez tous les modules complémentaires que vous désirez avoir, et bien évidemment, les paramétrer.

- Exceptions, oui mais...

Si vous avez tous les droits sur votre répertoire, vous ne disposerez pas de celui vous permettant d'écrire et modifier des fichiers et dossiers sur le système. **C'est pour cette raison que vous serez nettement mieux sécurisé**.

Mieux Sécuriser dans la mesure où toute installation de logiciel, ou programme, a besoin d'une autorisation d'écriture et modification sur les fichiers et dossiers du **système**. N'oubliez pas qu'un malware est un programme; il a besoin des autorisations nécessaires à sa bonne mise en place. Si vous ne lui donnez pas ces autorisations, il ne pourra pas vous infecter.

- **Pourquoi ne pas surfer avec les droits administrateurs?**
- **Migrer vers un compte limité sous Windows XP Home**
- **Migrer vers un compte limité sous Windows XP Pro**

2- Tenir son système à jour

Pour infecter votre ordinateur, les auteurs de malwares peuvent s'appuyer sur des failles de sécurité.
Une faille de sécurité est un comportement non prévu par une application qui peut permettre de compromettre le système.
Il existe deux types de failles :

- Les failles **distantes** : celles-ci sont exploitables à distance, c'est à dire via un accès distant de l'ordinateur et sans interaction de l'utilisateur. Ce sont bien entendu, les plus dangereuses puisqu'elles peuvent permettre la compromission du système à tout instant.
- Les failles **locales** : celles-ci sont exploitables seulement par l'interaction de l'utilisateur, par exemple lors de la consultation d'un site WEB qui exploite une faille

sur le navigateur ou lors de l'ouverture d'un fichier vidéo ou audio prévu pour exploiter une faille sur le lecteur audio/vidéo.

A l'heure actuelle, les failles de sécurités les plus exploitées sont celles contenues sur les navigateurs WEB (surtout Internet Explorer 6), **des milliers de sites WEB sont hackés en permanence**. L'internaute qui tombe dessus et dont le navigateur WEB est vulnérable exécute alors automatiquement et à son insu le code malicieux, l'infection s'installe alors.
Bien sûr certains sites comme les sites pornographiques ou ceux de cracks contiennent plus souvent des failles ce qui fait qu'il est risqué de s'y aventurer...

Pour pallier à cela, vous devez maintenir votre système d'exploitation à jour, ainsi que toutes les composantes (navigateur WEB, logiciels installés etc.).

- Utilisez Windows Update régulièrement :**Windows Updates**
  - Vous pouvez configurer Windows pour télécharger automatiquement les mises à jours :
    Maintenir Windows à jour avec Windows Update
- Maintenez tous vos logiciels à jour en particulier les composants de vos navigateurs, ainsi que vos lecteurs vidéos/audio : Java, Flash, QuickTime etc. Certains logiciels critiques sont pourvus de programmes de mises à jour, utilisez-les ! Vous pouvez aussi effectuer un Scan de vulnérabilités
- **Bannissez Internet Explorer dans sa version 6** Mettez à jour vers la version 7, vous pouvez aussi utiliser un navigateur alternatif comme **Firefox** en le sécurisant, vous échapperez aussi aux publicités sur les sites WEB.
- **Utilisez Firefox sécurisé** et **Sécuriser un peu plus Firefox sur Zebulon.fr**

3- *Antivirus et Antispyware*

L'antivirus est le **dernier rempart** du système pour prévenir l'infection. Malheureusement, les éditeurs de logiciels de sécurité ont de plus en plus de mal à détecter toutes les infections, et particulièrement les plus récentes.

Un **malware** doit exister avant de pouvoir être classé comme étant un programme malveillant. Tous les antivirus sont soumis à cette contrainte. L'infection fait des **dégâts** avant de pouvoir être détectée.

Il existe des techniques permettant aux antivirus de déterminer si un fichier est potentiellement à risque. Mais ces techniques sont *contournables* et s'accompagnent souvent de résultats *erronés*, un programme légitime pouvant être détecté comme étant une infection (Ce qu'on appelle un *''faux positif''*).

Si un antivirus est recommandé, il ne sera **jamais** totalement fiable, même si sa base virale est mise à jour plusieurs fois par jour. Le sentiment de sécurité que procure un antivirus fait oublier qu'il **ne** faut **pas** faire confiance aux programmes téléchargés sur Internet.

Enfin un antivirus est destiné à la détection **des virus, des trojans, des vers et backdoor**.
Les antivirus ne détectent ni les spywares, ni les adwares et ni les rogues.

Les **antispywares** sont les programmes qui protègent contre les spywares et adwares (et parfois les rogues). Les antispywares ont un fonctionnement assez similaire aux antivirus puisqu'ils intègrent une définition **virale**. Cependant, les antispywares intègrent souvent une protection (minimale) contre les modifications du système, par exemple l'ajout de programmes au démarrage de Windows, la protection contre les modifications du navigateur WEB etc.

Tout comme les antivirus, les antispywares sont à l'heure actuelle une protection indispensable mais ne sont pas infaillibles contre les menaces grandissantes que sont les adwares et les rogues.

4- *Limites des antivirus & antispyware*

Les limites des antivirus & antispywares se font de plus en plus sentir...
S'il y a quelques années, les auteurs de virus étaient des ados qui envoyaient des vers de messageries, les auteurs de malwares sont maintenant des bandes organisées motivées par l'appât du gain.
Les technologies utilisées par les auteurs de malwares sont de plus en plus pointues, le nombre de nouvelles menaces augmente chaque jour afin que les éditeurs de logiciels de sécurité ne puissent suivre la cadence. Le but des auteurs de malwares à l'heure actuelle est d'asphyxier de nouvelles menaces les éditeurs de sécurité pour toucher l'internaute.
Les voies de propagation pour toucher l'internaute étant de plus en plus facile (Emule, pages MySpace infectées, MSN etc.).

Les antivirus/antispywares étant le dernier rempart entre les menaces et votre ordinateur, la réaction des internautes perdus est en général de "blinder son ordinateur de logiciels de protections", on voit parfois deux antivirus, ou 3-4 antispywares sur un même PC. Accompagnés de 3-4 barres d'outils qui ont les mêmes fonctions, on constate alors de plus en plus de sujets sur les forums: "*mon ordinateur est lent*", "*je rame*".

Quelle est la bonne réaction face aux menaces grandissantes?

La différence se fera sur **de bonnes habitudes et un minimum de méfiance**. Il est clair qu'avec un antivirus équivalent, une personne qui télécharge sur emule, ouvre sans réfléchir les fichiers qu'on lui propose sur MSN ou sur des publicités sera infectée contrairement à une personne qui se contente de lire ses mails.

Pour beaucoup, sécurité rime avec installation du "meilleur" antivirus & antispyware, cinq minutes chrono on installe les plus répandus/connus et en avant: On va piller Emule, installer pour essayer n'importe quel logiciel, ou ouvrir tous fichiers qui se présentent sous la main en pensant *"bah mon antivirus va détecter si problème"*.
La sécurité est en amont, se tenir au courant, faire attention à ce que vous faites sur la toile, un utilisateur averti vaut tous les antivirus.

5- *Configuration conseillée*

Voici la configuration que nous conseillons. Celle-ci est entièrement gratuite et offrira une protection plus qu'acceptable :

- Utiliser un compte limité pour les tâches courantes. **Ne surfez pas avec les droits administrateurs.**
  - **Pourquoi ne pas surfer avec les droits administrateurs?**
  - **Gestion des utilisateurs (jokuhech.free.fr)**
  - **Gestion des utilisateurs sous Windows (malekal.com)**
- L'Antivirus **AntiVir** :**Tutorial Antivir (libellules.ch)**
  - **Pourquoi nous recommandons plutôt AntiVir**
- L'AntiSpyware **SpyBot Search & Destroy**
  - **Tutorial SpyBot Search & Destroy (Zebulon.fr)**
  - **Tutorial animé SpyBot Search & Destroy (balltrap 34)**
- Le navigateur WEB Firefox Sécurisé
  - **Utilisez Firefox sécurisé**
  - **Sécuriser un peu plus Firefox sur Zebulon.fr**
- Filtrer les ActiveX et ajouts de sites sensibles pour Internet Explorer
  - **SpywareBlaster**
- Un fichier HOSTS Filtrant
  - **Utiliser HOSTS Manager**

- **B.I.S.S Hosts manager** (Libellules.ch)

Encore une fois rien d'exceptionnel, pas besoin d'alourdir son PC de logiciels de protection qui vont ralentir l'ordinateur, **une bonne attitude sur la toile fera la différence**.

Voici quelques sites traitants de la sécurité si vous désirez approfondir le sujet :

- http://www.malekal.com
- http://assiste.com.free.fr
- http://abcdelasecurite.free.fr
- http://mickael.barroux.free.fr/securite/index.php
- http://pagesperso- orange.fr/jesses/Docs/Nuisibles/IndexNuisibles.htm

Ces sites peuvent aussi vous aider à être informé des menaces constamment en évolution sur la toile.

6- *Conclusion*

La sécurité est un tout et ne se résume pas aux choix des programmes de protection que vous installez sur votre ordinateur. La sécurité c'est avant tout **être vigilant** et éviter certaines mauvaises habitudes qui conduisent à l'infection à coup sûr, et bien sûr , **maintenir ses logiciels à jour**.

La sécurité de votre ordinateur sur internet se résume en :

- Réduire les chances d'infections
- Avoir une bonne habitude de surf (bannir certaines catégories de site WEB).
- Bannir certaines sources & téléchargements : P2P, cracks etc.
- Se méfier des fichiers que vous ouvrez, toujours se poser la question "peut-il infecter mon PC?"
- Eviter d'utiliser son ordinateur avec les droits administrateur
- Maintenir son système et ses logiciels constamment à jour pour éviter les failles.
- Etre un utilisateur averti : se tenir informer des derniers virus et dernières méthodes d'infection pour ne pas tomber dans les pièges.
- Ne jamais trop faire confiance aux logiciels de protection.

3- Désinfecter son ordinateur

Vous êtes infecté, vous avez besoin d'aide.
Voici une liste de forums sur lesquels vous trouverez de l'aide pour désinfecter votre ordinateur **gratuitement**.

Connectez-vous puis créez un sujet dans les parties Virus et attendez que l'on vous réponde!

- **Forum désinfection malekal.com**
- **Forum désinfection Generation-NT**
- **Forum désinfection -infos-du-net.com/Tom's Guide**
- **forum désinfection telecharger.com**

4- Participer à la lutte

Vous souhaitez aider à participer à la lutte contre les malwares?
La simple diffusion de ce PDF peut aider des internautes à ne pas infecter leurs machines, les connaissances et le savoir contre ces menaces sont très importants.

Pour participer rien de plus simple, envoyez ce PDF à vos amis, si vous avez un site ou blog, vous pouvez mettre le PDF librement en téléchargement!

Sachez qu'une version pour les forums (bbcode) est disponible si vous administrez un forum. Vous avez alors la liberté d'effectuer un copier/coller sur votre forum pour informer vos membres des menaces.

Le code html :

```
<a href="http://www.malekal.com/ProjetAntiMalwares.php"><img style="border: 0px solid ; width: 262px; height: 150px;"  alt="Projet AntiMalware"
 src="http:///www.malekal.com/fichiers/projetantimalwares/campagne_fightantimalware.gif"></a>
<br>
```

Si vous êtes simple membre d'un forum, vous pouvez mettre cette bannière en signature!

bbcode pour signature :

```
[url=http://www.malekal.com/ProjetAntiMalwares.php]
[img]http://www.malekal.com/fichiers/projetantimalwares/reagir_miniban.gif[/img][/url]
```

Pour plus d'informations, reportez-vous à la page : Lutte contre les malwares

5- Glossaire

- **Adware** : Composant destiné à ouvrir des publicités sur votre ordinateur. Beaucoup de logiciels dits gratuits se font rémunérer en ouvrant des popups de publicités. Dans L'eula, il est écrit généralement en anglais que le logiciel est susceptible d'ouvrir des publicités. Les utilisateurs ne lisant jamais l'EULA se retrouvent alors piégés. En France, l'adware le plus répandu est NaviPromo/Magic.Control Agent qui s'installe via des logiciels gratuits comme MailSkinner; MessengerSKinner; WebMediaPlayer etc.
- **Backdoor** : ou porte dérobée. Famille de trojans qui a pour but de permettre l'accès ou le contrôle de votre système d'exploitation à un pirate.
- **Keylogger** : ou enregistreur claviers. Keylogger désigne un programme qui a pour but d'enregistrer les frappes claviers. Certains Keylogger sont capables d'envoyer automatiquement les saisies claviers par mail. Le but du Keylogger est de récupérer les mots de passe, numéro de carte bancaire etc.
- **Malware** : Le malware désigne l'ensemble des menaces toutes catégories/familles confondues (Virus, Spywares, Adwares etc.). Malware est la contraction de "Malicious Software" qui signifie *Logiciel Malicieux* en français.
- **Spyware** : Le Spyware est un logiciel espion qui enregistre certaines informations personnelles pour les transmettre à un ou des serveurs tiers. En général, ce sont vos habitudes de surf (sites WEB consultés etc.) afin de mieux pouvoir cibler le contenu en rapport à vos loisirs, goûts etc.. Beaucoup de Spywares sont sous forme de barres d'outils pour votre navigateur WEB (MyWebSearch, HotBar etc.).
- **Rogue** : Le mot anglais "*rogue*" a pour signification "*escroc*". Un **rogue** désigne dans le monde de l'informatique un faux-logiciel de sécurité. Il existe plusieurs catégories de **rogues** : un rogue anti-spyware, rogue antivirus... Le site Spyware Warrior a répertorié ces nombreux logiciels dans sa Rogue List.
- **Ver Informatique** : Le ver informatique est une infection se propageant sur des ordinateurs à l'aide d'un réseau informatique comme l'Internet. Les vers les plus actifs utilisent MSN Messenger comme moyen de propagation.
- **Virus** : Les virus dans leurs définitions d'origine désignés les malwares infectants des fichiers et se propageant sur un système sain lors de l'exécution de ce fichier infecté. A l'heure actuelle et par abus, virus tent à devenir toute forme de malwares.
- **Trojans** : Les parasites non viraux sont appelés, d'une manière générique, "Trojans", ce qui recouvre un vaste éventail de classes très différentes de parasites. Il y a une confusion actuelle complète entre le terme de trojan (Cheval de Troie) qui n'est qu'un vecteur, une méthode de transport des parasites, et les parasites eux-mêmes, contenus dans ces chevaux de Troie. On devrait se limiter à appeler "Cheval de Troie" ou "Trojan" l'organisme (le programme) ayant une finalité autre que le transport de parasites et qui est squatté pour servir de vecteur à l'introduction de parasites dans un autre organisme (le système d'exploitation d'un ordinateur), les parasites appartenant, eux, à des classes de parasites comme les Virus, les RATs, les Backdoors, les Keyloggers, les Dialers, les Spywares, les Adwares etc. Le trojan est et reste la méthode d'infection utilisée et uniquement cela. Le trojan n'est pas le parasite ! Il le transporte ! Si, et seulement "si", le moyen de transport a été développé exclusivement pour permettre la diffusion d'un parasite et n'a pas d'autre activité et finalité que celle-là, le cheval de Troie se confond avec le parasite.

6- Remerciements

Nous tenons à remercier **les équipes** de Génération-NT et Infos-du-net (nouvellement Tom'Guide) ainsi que PC-Entraide pour leur soutien.