Sécuriser son ordinateur et connaître les menaces

Voici un article et dossier complet qui explique comment sécuriser votre ordinateur.

Cet article aborde aussi les menaces que l'on peut rencontrer sur internet qui sont à l'origine de programmes malveillants afin de les éviter.

Beaucoup de sites internet proposent de télécharger des utilitaires de sécurités mais abordent rarement ce qu'il ne faut pas faire sur internet.
Ainsi beaucoup d'internautes pensent que la sécurité de leur ordinateur se résume au choix de l'antivirus alors que pas du tout.

Voici comment sécuriser son ordinateur.

Pourquoi les virus existent ?

Pourquoi internet est-il dangereux?

Depuis l'explosion du nombre d'internautes (avènement du haut débit etc..), internet est devenu un média à part entière et comme tout média, il est de plus en plus submergé par la publicité, utilisation du marketing, etc.

Ces nouveaux internautes ont une connaissance minimale de l'informatique et des menaces. Il est donc assez facile de faire de beaucoup d'argent via ces menaces en trompant ces nouveaux internautes, cela a aussi provoqué une explosion du nombres de menaces par l'appât généré par le gain.
Des organisations structurées et professionnelles ont vu le jour qui ont pour simple but de se faire de l'argent sur le dos des internautes.

Plus d'exemples sur la page : Business malwares : le Pourquoi des infections informatique

Les trojan

Un trojan ou backdoor permet de contrôler l'ordinateur à distance. Ce dernier peut faire **tout ce qu'il désire** avec cet ordinateur même en étant à des milliers de kilomètres.
Vos données personnelles : mot de passe, documents Word & Excel ne sont plus à l'abri puisque ce dernier peut les modifier ou supprimer ou informations personnelles sont aussi

à sa portée.

Lorsque le PC est infecté et à la merci d'un pirate qui le contrôle à distance.
On dit alors que l'ordinateur est un PC zombi et rejoint un botnet, c'est à dire un réseau d'ordinateurs contrôlés par le pirate.
Plus d'informations : Les botnets : réseau de machines infectées

La vidéo suivante illustre un cheval de troie en action.

Les méthodes pour gagner de l'argent

Voici énuméré les diverses méthodes pour gagner de l'argent à travers les logiciels malveillants.

Les botnet

Les botnet sont des réseaux d'équipements (ordinateurs, routeur, etc) infectés et pilotés à distances par un pirate.

Pou rentabiliser ces derniers le botmaster a plusieurs codes à son arc comme :

- utiliser les ordinateurs infectés pour effectuer des attaques vers des sites PC zombies à sa disposition pour effectuer ses attaques. Imaginez 10 000 PC avec des connexions ADSL effectuant des requêtes en continu sur un site WEB !
- utiliser les ordinateurs infectés pour relayer des mails de spams pour des produits commerciaux. Votre ordinateur envoie des mails de spam à différentes adresses et ceci en continu. Le pirate ou organisme se rémunère aux nombres de spams envoyés pour promouvoir un produit commercial. Sur cette news, on peut lire qu'une infection est capable d'envoyer 12 000 spams images par heure

Une partie des botnet peuvent être sous-loués pour une certaine somme.
En d'autres termes votre PC et votre connexion internet est utilisé pour être sous-loués et se faire de l'argent sur votre dos.

Pour se faire un maximum d'argent, les pirates se doivent d'infecter un maximum d'ordinateurs. Plus le pirate a d'ordinateurs à sa disposition, plus la bande passante (la capacité du débit de connexion total) est grand. Il peut alors envoyer plus de spams, effectuer des attaques vers des sites plus « gros » ou plus nombreux. Il est aussi plus dangereux.

Adwares et publicités

Les adwares sont des logiciels publicitaires que l'on implante sur les ordinateurs des victimes.
Cela permet de gagner de l'argent via la publicité qui va

s’afficher sur l’écran.

Les pirates créent des adwares et programmes parasites qui affichent des popups de publicités. Le pirate gagne alors un certains nombres d’argent par popup de publicités ouverte donc plus le nombre d’ordinateur qui ouvre des popups est grand, plus le pirate se fera d’argent.

Ces adwares sont en général refourgués lors de l’installation de programmes gratuits ou en trompant les internautes via de fausses mises à jour Java/Flash ou du navigateur WEB.

Les arnaques sur internet

Il en existe beaucoup et de différentes.

Voici quelques pages présentes sur le site qui en détailles :

- Arnaque support téléphonique – PC Support et Arnaques aux désinfections / support par téléphone
- Arnaque : Gagner Iphone à 1 euro
- Les faux sites d’actualités
- Arnaque : fausse alerte de virus
- Les faux virus (scareware et rogues) et plus récemment TotalAv
- Arnaque africaine ou brouteur

La part de responsabilité des

internautes

Tout comme vous fermez la porte de votre domicile, il convient de verrouiller un minimum votre ordinateur afin que ce ne soit pas une porte ouverte à toute intrusion.

L'internaute est responsable de la bonne santé de son ordinateur, que ce soit pour l'intégrité de ses données mais aussi pour les autres internautes, l'internaute doit en conserver la maîtrise (ce qui demande un minimum de connaissance technique).
Lorsque vous prenez le volant d'une voiture, vous avez pris un minimum de leçon afin de ne pas causer d'accident pour vous et autrui. Il en va de même sur internet.

Voici une liste des erreurs commises généralement par les internautes.

Trop confiance en votre antivirus

Une trop grande confiance voire une confiance aveugle dans les outils de protection (antivirus et firewall).
Contrairement au discours marketing, un antivirus est loin d'être infaillible, je dirai même qu'actuellement les pirates ont pris une sérieuse avance sur les antivirus qui ont depuis quelques années peu évolué, notamment en ce qui concerne les rootkit.

Suite à une infection le seul réflexe de l'internaute est de demander « Quel est le meilleur antivirus » pensant que la

faute de son infection vient de son antivirus qui n'a pas fait le boulot. Il ne ne se pose pas la question : *pourquoi et comment j'ai été infecté ?* alors qu'en général l'infection vient d'un manque de connaissance des malwares et de mauvaises habitudes de surf.

Crack & Keygen

L'installation à tout va de logiciel sans en vérifier l'authenticité et la source et ceci généralement depuis des sources dangereuses : Réseau P2P , Site Web non vérifié, etc.. « Mon antivirus ne sonne pas ? OK le logiciel est pas dangereux ».

N'installez que des programmes depuis des sources sûres.

Les internautes ne sont pas assez méfiants : Lorsqu'ils arrivent sur un site WEB proposant des logiciels, ils ne se posent pas la question « ce logiciel peut-il être dangereux? ». Reportez-vous à l'article Prévention : Logiciels et sources de téléchargements

Quand le logiciel est non dangereux… On le crack alors que de nombreux faux sites de cracks vecteurs de logiciels malveillants sont mis en ligne.
Plus d'informations, reportez-vous à l'article Le danger des cracks !

Paranoïa et multiplication des protections

En général, la seule réponse pour sécuriser son ordinateur et soit de changer d'antivirus soit de multiplier les protections.
On retrouve alors plusieurs antispywares inutiles (SpyBot, Ad-aware, etc) sur une même machine croyant que cela les protègera mieux.

- Les résultats sont plutôt médiocres et mitigé, Reportez-vous à l'article Phénomène de sur-multiplication des logiciels de protection
- De plus, cela ralenti considérablement l'ordinateur, Reportez-vous à l'article Comprendre pourquoi votre ordinateur est ralenti

Vous allez voir dans la suite de cette page que les pièges mis en place par les pirates sont nombreux.
Ce que vous devez comprendre, c'est que votre antivirus ne détecte à peine 1/3 des programmes dangereux mentionnés ci-dessous, la seule parade est la **méfiance**.

N'installez pas le premier programme venu, n'exécutez pas le premier fichier venu même si votre antivirus ne dit rien.

Les différents menaces informatiques

Quels sont les pièges et dangers?

Lorsque vous naviguez sur internet, ou téléchargez et installez des programmes, vous devez être vigilant. En effet, des pièges ou arnaques sont monnaie courante sur la toile.

Pour infecter des ordinateurs, on utilisera les moyens de propagations qui pourront toucher le plus de monde possibles et qui touchent les activités que les internautes ont le plus souvent sur internet.
La page suivante donne un aperçu Comment les virus informatiques sont distribués

Abuser l'internaute

N'ouvrez pas n'importe quel fichier, faites attention à ce que vous téléchargez et d'où vous téléchargez : Prévention : Logiciels et sources de téléchargements

Pour infecter des ordinateurs, les pirates « sèment » internet de pièges, si possible à des endroits où ils risquent de toucher le plus d'internautes.
Les pirates surfent donc sur les modes.
Précédemment MSN et fichiers piégés sur les Réseau P2P étaient utilisées, de nos jours, ce sont plutôt de faux sites de cracks.

Les pièges reposent toujours sur le concept de social engineering et la crédulité de l'internaute. Le tout étant de déguiser l'infection dans des programmes ou des mails

attrayants et à la mode, l'internaute tellement intéressé ne pourra pas s'empêcher d'installer ce programme. C'est un peu comme lorsque vous recevez dans votre boîte aux lettres « Vous avez gagné 1 000 000 000 d'euros ».

N'installez que des programmes depuis des sources sûres.

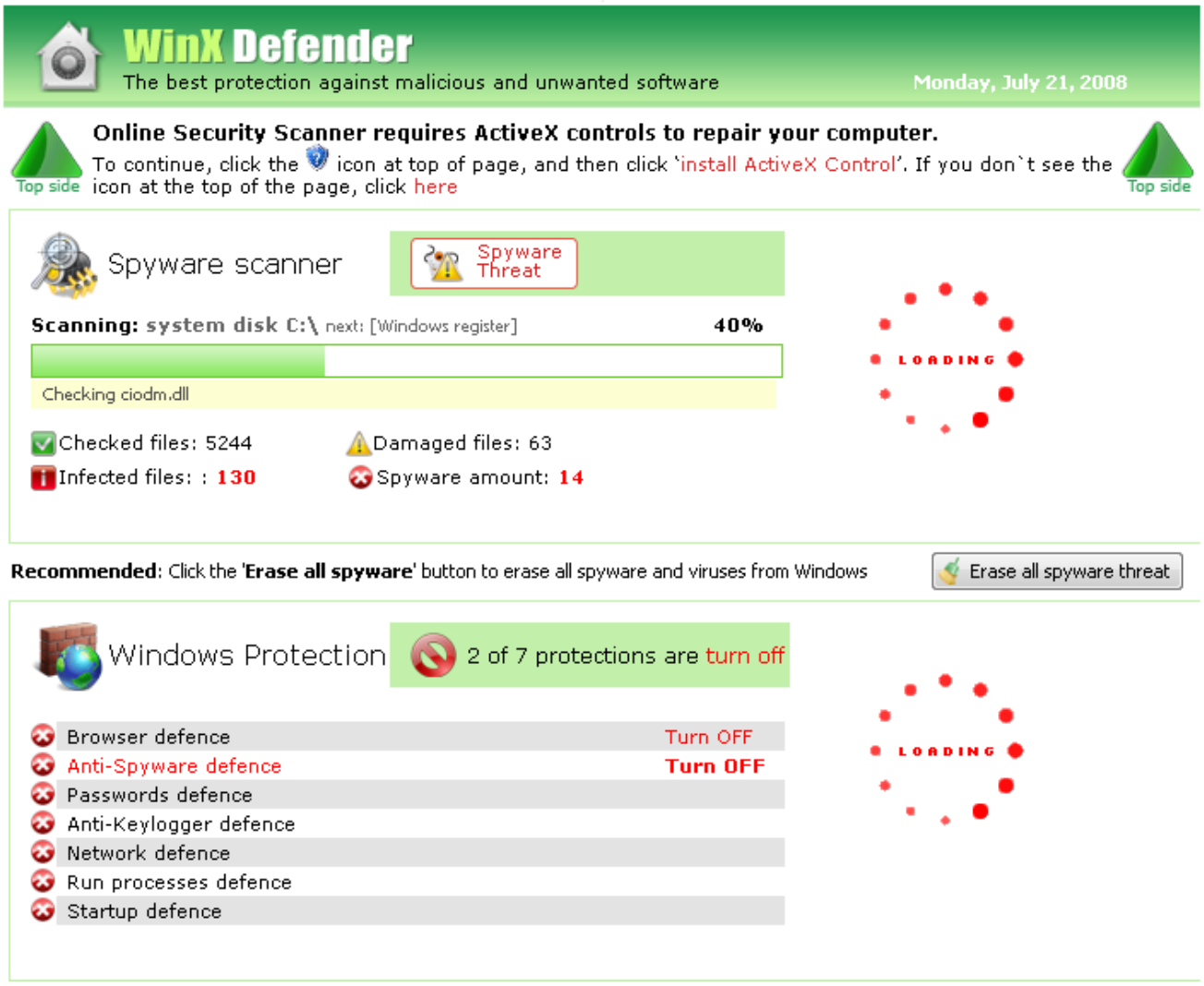
Les fausses alertes de sécurité

Les fausses alertes de sécurités et de virus consistent à afficher un faux messages de virus afin de faire croire à l'internaute que son ordinateur est infecté.
La plupart du temps, ces messages visent à bloquer l'ordinateur ou le navigateur WEB.
Le but est ensuite de faire effectuer une action par cet internaute, télécharger un fichier qui peut-être une vraie infection, téléphoner à une hotline ou payer une somme d'argent.

Plutôt courante de 2005 à 2011 pour pousser des rogues/scawares, elles ne sont aujourd'hui très peu courantes mais sont revenus sous une autre forme à travers les Arnaques aux désinfections / support par téléphone.

Par le passé, lorsque vous surfiez sur internet, surtout sur des sites douteux (cracks, pornographiques), il pouvait arriver que vous receviez des popups vous indiquant que votre ordinateur est infecté ou n'est pas sécurisé.
En règle général, ces sites vous invitent à télécharger et installer un antivirus ou un antispywares qui s'avéraient être un rogue.

Exemple sur la page : [Les Rogues et alertes de sécurité]



Les arnaques de support téléphoniques

Ces méthodes avaient disparus et sont revenus pour pousser des [Arnaques aux désinfections / support par téléphone.]

Le principe est le même, de faux messages vous indiquant que votre ordinateur est infecté ou a des problèmes s'affichent durant le surf, souvent à travers de faux messages [BSOD/Ecran bleus].

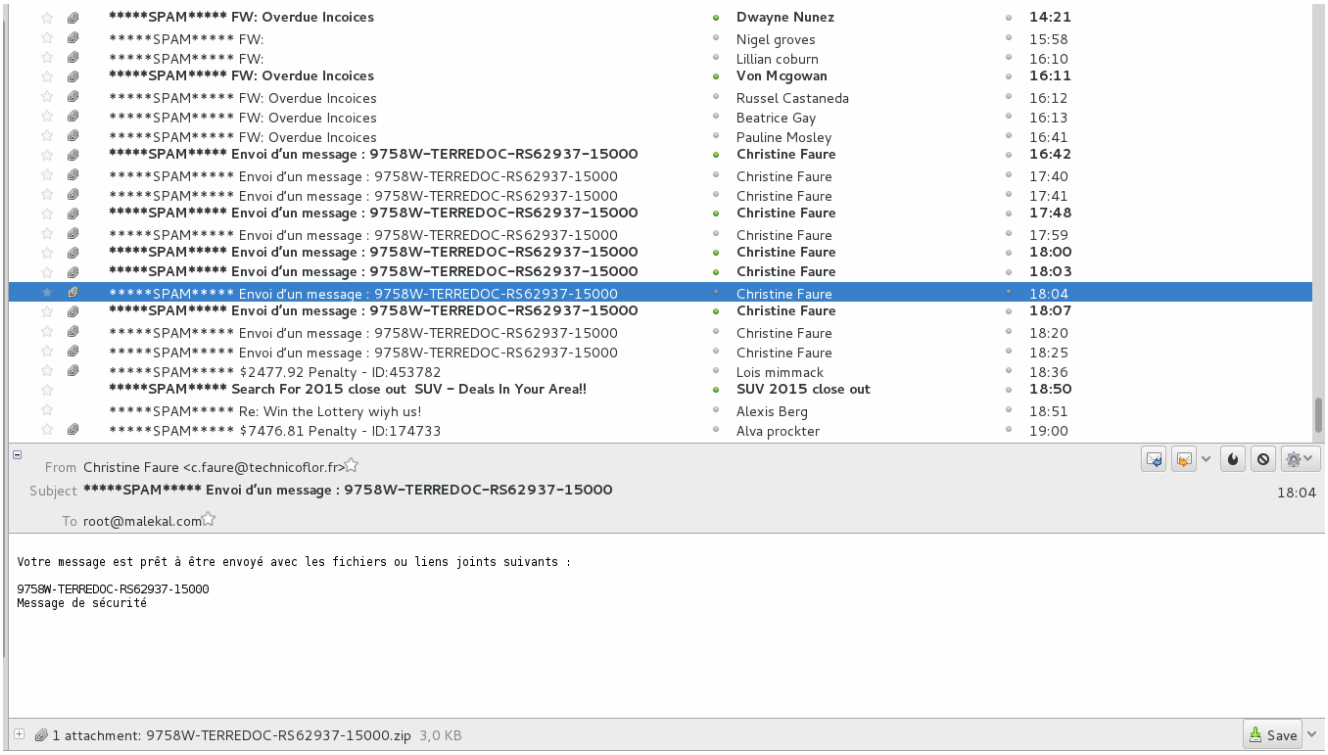
Le message vous recommande d'appeler un technicien qualifié, qui n'aura qu'un seul but, vous vendre une prestation et antivirus à des prix exorbitants.

Règle d'or : **NE JAMAIS** installer un programme qui vous est proposé par un popup, que ce soit un programme de smiley, des économiseurs d'écran, des antivirus, des antispywares. A coup sûr vous infectez votre machine.

Les infections par mails

Les mails sont un grand vecteur de propagation des malwares/virus qui se propagent sous forme de pièce jointes. La majorité des internautes à l'heure actuelle connaissent cette menace, même si les mails restent un gros vecteurs de malwares, il est en perte de vitesse, les antivirus offrant maintenant de bonnes protections. Nos dossiers sur les virus par email :

- Les virus par email
- Les virus par email



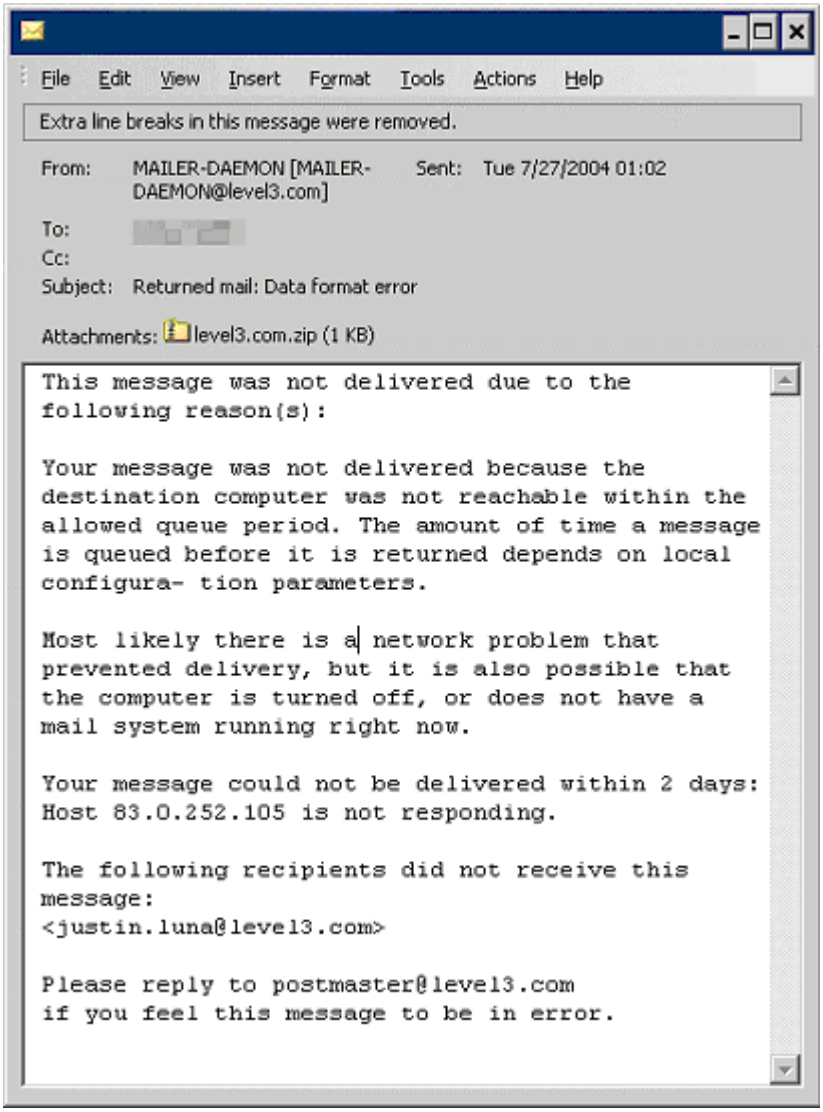
Les règles à suivre sont :

- Ne pas ouvrir les pièces jointes des mails anglophones
- Ne pas ouvrir les pièces jointes provenant d'un expéditeur que vous ne connaissez pas.

–> Supprimez le mail directement (évitez de le stocker dans les éléments supprimés)

Voici deux exemples de mails infectés, celui de gauche se fait passer pour un serveur de mails vous renvoyant une erreur.
Celui de droite vous explique que votre ordinateur est infecté et que vous devez suivre les instructions fournie dans la pièce jointe.

Comme vous pouvez le constater, les mails des virus sont de plus en plus ingénieux pour tromper l'utilisateur.



La propagation de malwares via des mails avait baissé depuis 2012 avec un retour fin 2015 jusqu'à 2017.
Ce retour de pièces jointes malveillants se base VBS et autres scripts pour pousser des crypto-ransomwares.

N'ouvrez pas n'importe quel mail – Phishing

Le phishing ou hameçonnage consiste à se faire passer pour une société (banque, société de jeux, société de paiement en ligne etc..) afin de récolter des informations, généralement votre numéro de CB.

Soit les informations sont en remplir directement dans le mail, soit la personne est redirigée vers un site qui peut être une copie **très proche** d'un site de Banque.

Règle d'or : Ne jamais communiquer des informations suite à un mail, surtout quand il s'agit de votre numéro de CB, de compte etc.. Vous pouvez aussi protéger vos comptes en ligne : Comment protéger ses comptes internet

Plusieurs exemples de mail de phishing sont donnés sur la page suivante : Exemple de mail phising


LCL
LE CRÉDIT LYONNAIS
DEMANDEZ PLUS À VOTRE ARGENT

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.

Exemple de mail de phishing

N’ouvrez pas n’importe quel lien – *Le SPAM*

Le SPAM (ou pourriel en français) consiste à envoyer des messages non sollicités à une personne souvent dans un but commercial, ils ne sont pas dangereux en soi. Les SPAM sont envoyés par mail mais aussi en commentaire sur des blogs, forum et notamment sur des sites sociaux comme facebook, myspace etc.

Les liens utilisent le social engineering pour tromper l’internaute, ce dernier clic sur le lien amenant à l’infection, quelques exemples :

- Net-Worm.Win32.Koobface sur FaceBook et MySpace
- Zhelatin/Storm/Waledac Worm par mail
- Trojan-Downloader.Win32.Exchanger : faux-codecs et mails

Certaines infections ne sont plus d’actualité mais c’est le principe qui compte qui repris par d’autres campagnes.

Pour plus d’informations sur le SPAM par mail, n’hésitez pas à consulter la page du site : Le SPAM / Pourriel

Les vers par messagerie instantanée ou Facebook

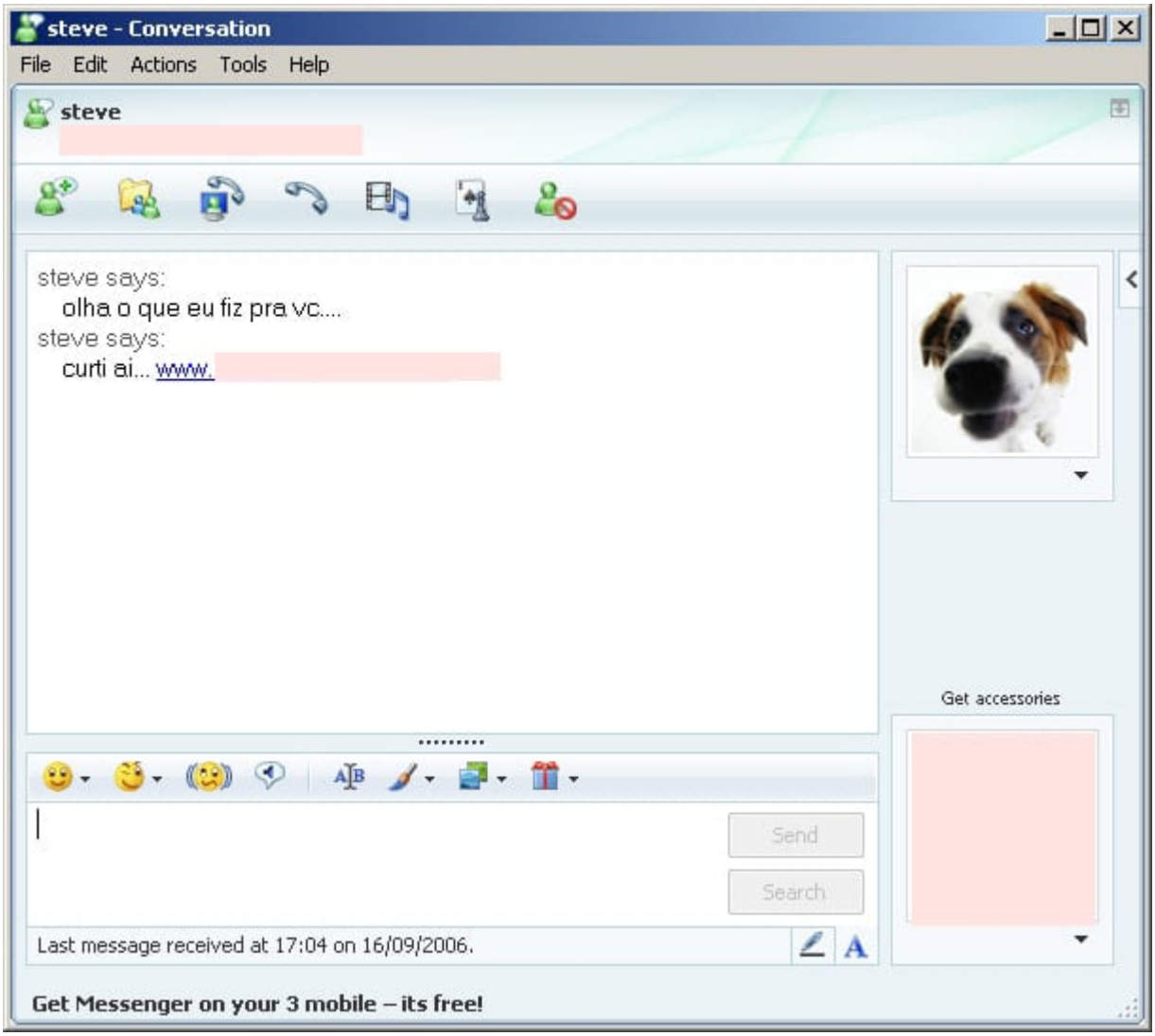
Les messageries instannées (MSN Messenger, Yahoo Messenger etc..) sont aussi des vecteurs de malwares bien que l’âge d’or

fut de 2007 à 2010.
Ces infections utilisent le social engineering en tirant partie du masquage des extensions de fichiers.

N’ouvrez jamais de liens provenant de discussions surtout

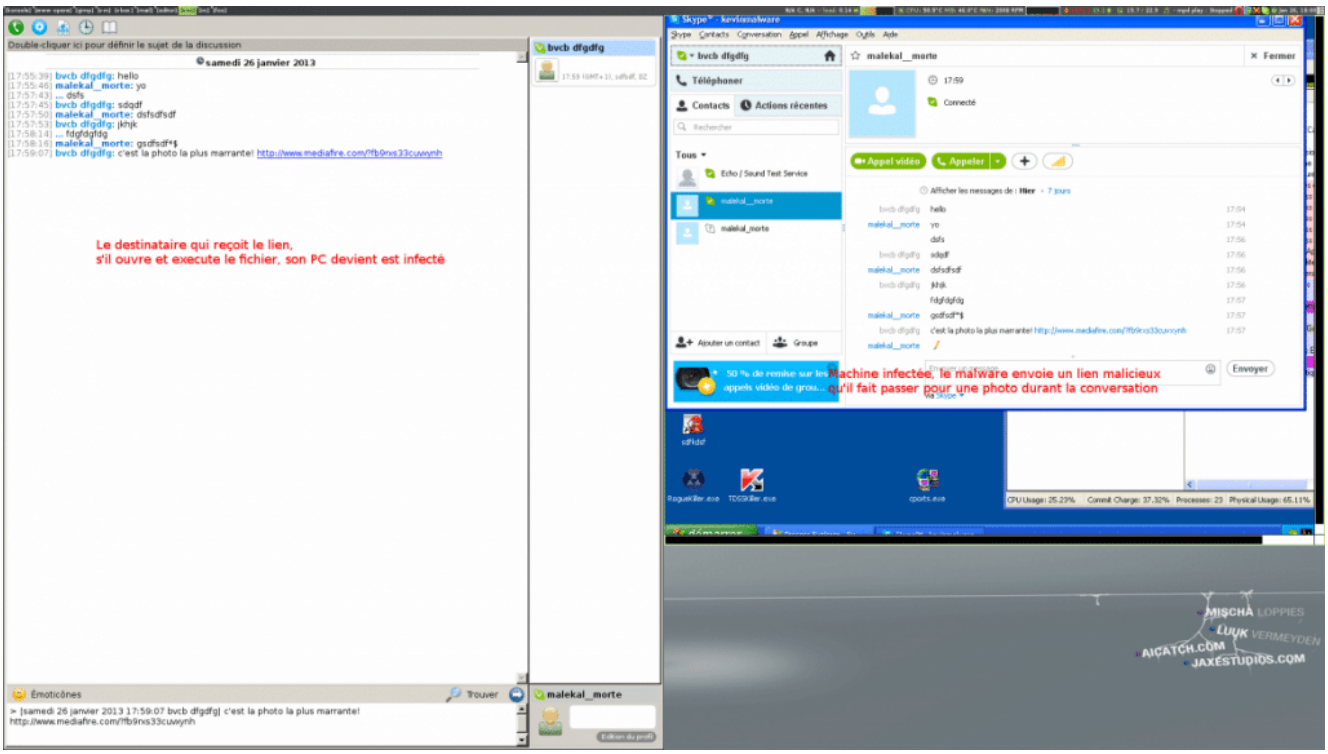
- Évitez de télécharger des fichiers Zips proposés en discussions (en général, pour des photos, album, emoticons etc..).
- Si les propositions de téléchargement ou d’envoi pour des zips se multiplient, méfiez-vous!

Pour plus d’informations, sur les vers de messageries instantanées, voir : Vers de messageries ne sont plus vecteur 1er des infections
Voici quelques exemples de messages vecteurs d’infections :



Virus par MSN

Par le passé, Skype avait été aussi touché par ces infections instantanées comme par exemple : [Win32.Phorpiex par Skype]



Win32.Phorpiex par Skype

Facebook peut aussi être touché par ce type de vers ou des Trojans capables de diffuser des messages.
A lire : [Spam/Virus Facebook]

Les virus sur Facebook

Les infections par disques amovibles

Les infections par disques amovibles ou virus par clé USB sont de plus en plus fréquentes.
On entend par disques amovibles, les périphériques de masses que l'on peut insérer et retirer de l'ordinateur comme les clefs USB, disques dur externe ou cartes Flash

Ces infections se propagent beaucoup dans les lycées, fac, université, cyber café où les postes sont à la disposition de beaucoup de monde qui viennent avec leurs clefs USB et

infectent les ordinateurs. Dès lors les nouveaux étudiants qui viennent avec leurs clefs les infectent qui à leur tour infectent leurs ordinateurs personnels etc.. etc..

Cette page décrit le fonctionne et la manière dont ces infections se propagent ainsi que des conseils de préventions :

- virus par clé USB
- infection sur disques amovibles
- infection par disques amovibles 2
- Sécurité : Maitriser ses médias amovibles

Ces infections utilisent des scripts VBS et tirent partie de Windows Script Hosting, nous vous conseillons vivement de désactiver ce dernier : Malware par VBS / WSH.
Pour se protéger : Comment se protéger des scripts malicieux sur Windows

Les faux codecs et mise à jour

Les faux codecs étaient des méthodes d'infections très utilisées de 2005 à 2011. Ces méthodes ont un peu disparus de nos jours. Ces faux codecs se propagent installant des infections de type Zlob/VideoAccess/Trojan.Win32.DNSChanger :

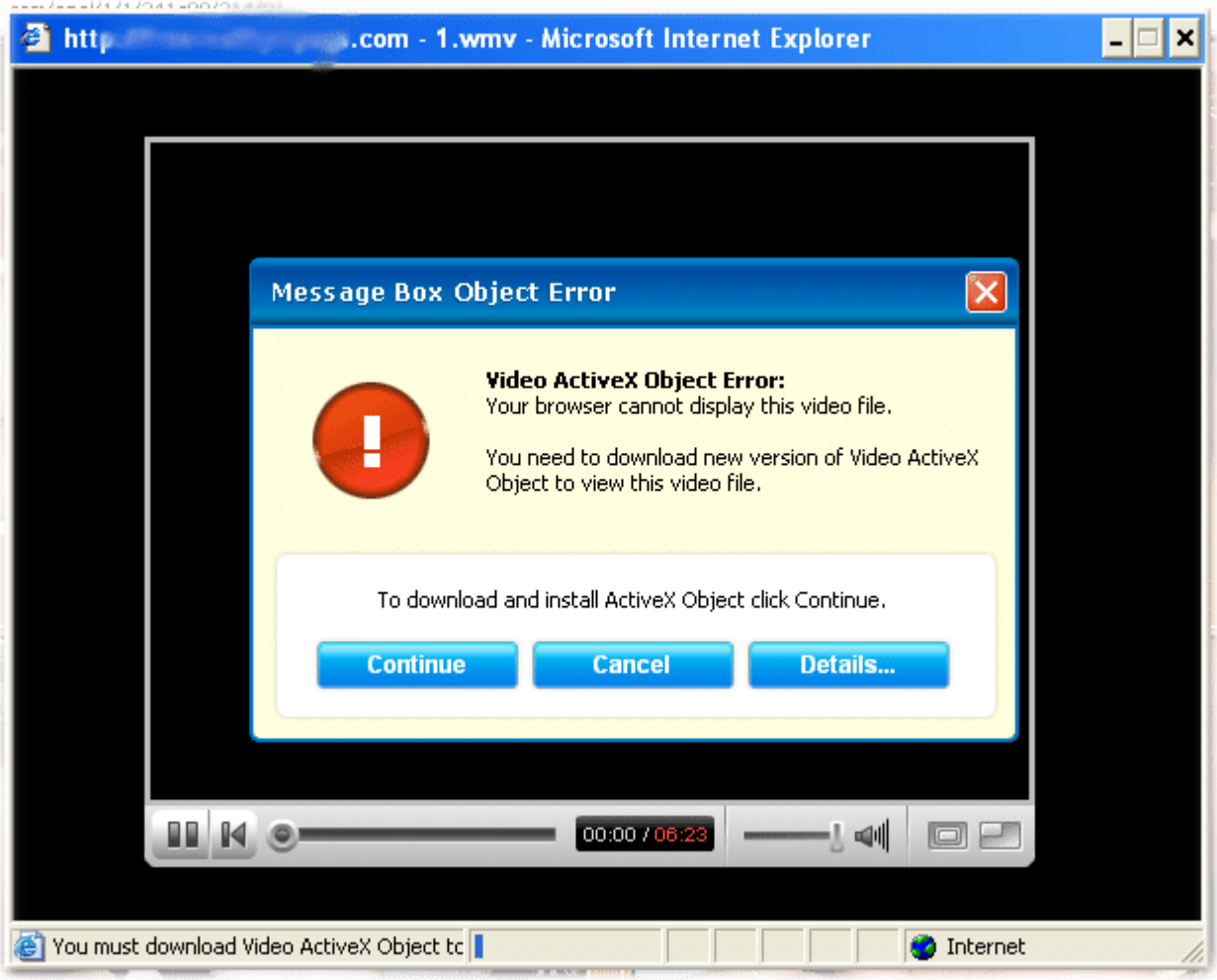
- sur des **sites pornographiques**. L'internaute clic sur un lien pour visualiser des vidéos pornographiques.. Un message lui indique qu'il doit installer un nouveau codec pour visualiser la vidéo. Exemple aussi avec

WebMediaPlayer.

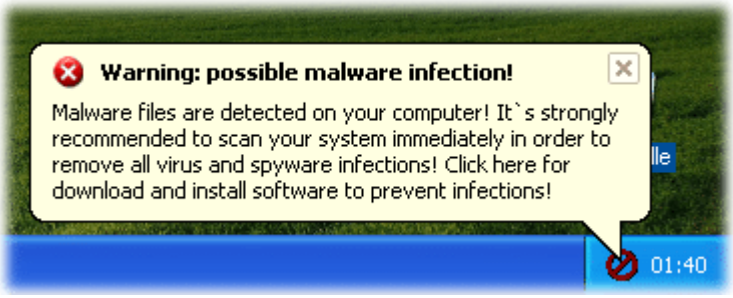
- via de faux sites de **cracks** : faux codecs & cracks
- Sur des sites WEB **piégés**:
    - ex avec MySpace : faux codecs et pages piégées (MySpace)
    - ou faux codecs et pages piégées (site WEB FR)

Le but de ces faux codecs est l'installation d'infection qui entraîne l'affichage de fausses alertes de sécurité afin de vous faire télécharger mais surtout acheter de faux antispywares que l'on nomme rogue.

Lorsque vous surfez sur des sites pornographiques, on vous incite à installer ce codec en indiquant qu'il est nécessaire pour visualiser les vidéos.



L’installation du codec n’est qu’un prétexte pour vous faire charger un trojan.
Ce dernier affiche de fausses alertes de sécurité et charger un faux antivirus.



Fausse alerte de virus

Le but de ces infections est très simple, elle consiste à faire peur à l’internaute, via des alertes, modifications du

fond d’écran (en rouge ou avec des panneaux rouges) tout en proposant de télécharger de faux antispywares rogues.
Ces rogues une fois installé vont scanner l’ordinateur, ils afficheront eux aussi des alertes disant que l’ordinateur est infecté, mais il faudra acheter la version commerciale pour nettoyer l’ordinateur.
Le but est donc de vous arnaquer en vous faisant acheter un faux-antispyware.

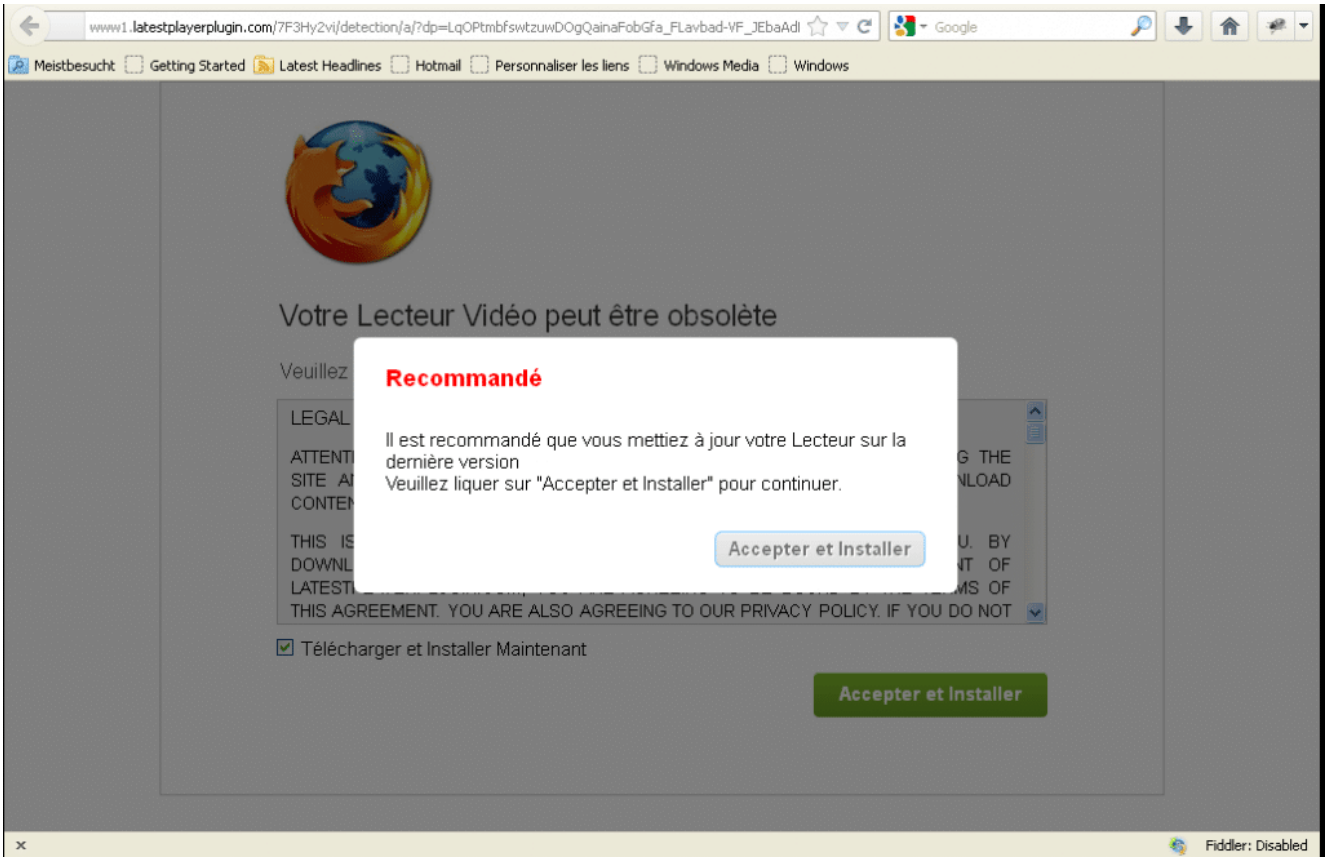
Plus d’infos, voir :

- Alertes faux codecs
- Exemple d’une infection affichant des alertes

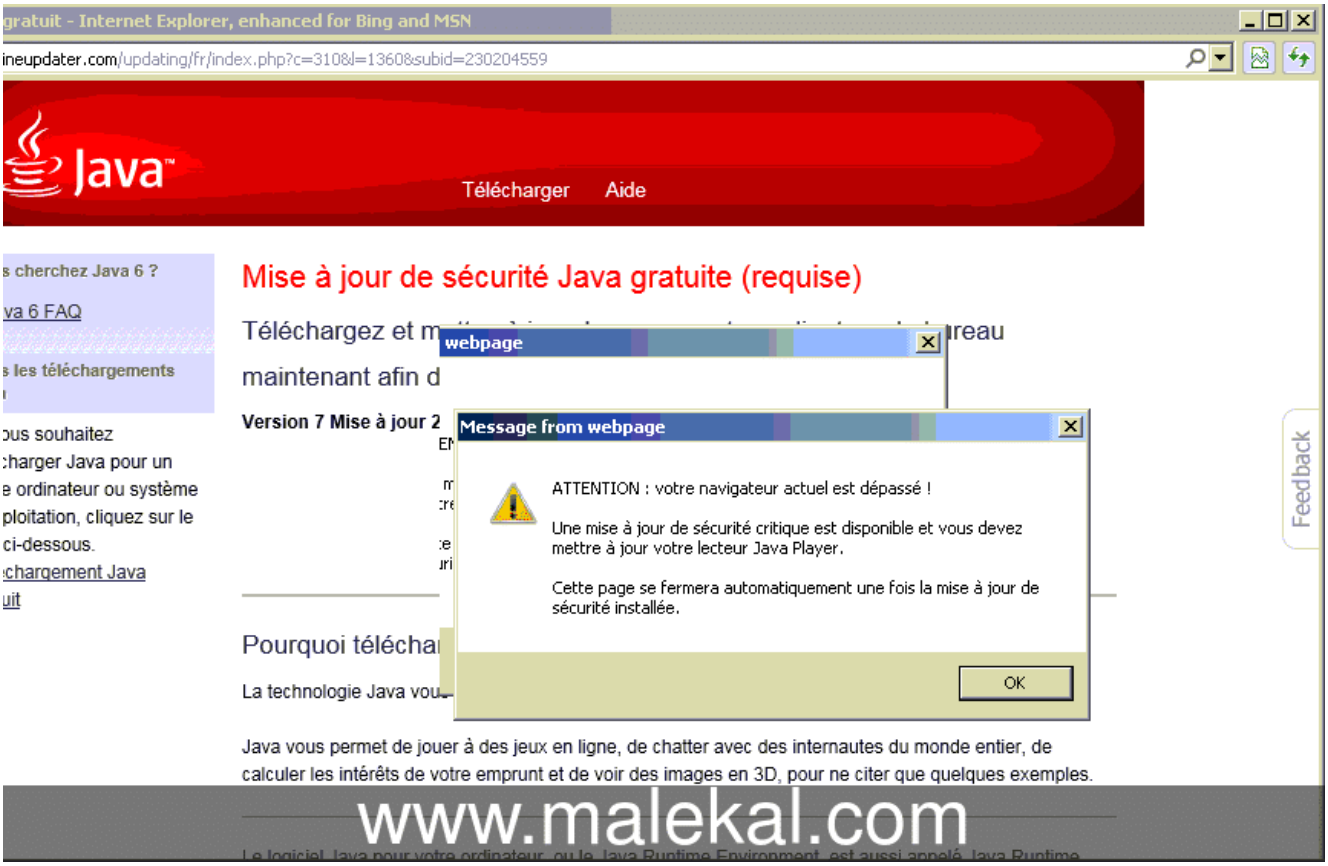
Fausse mise à jour Java ou Flash

Dans le même style et autre prétexte pour vous faire exécuter un fichier malicieux sur votre ordinateur : les mises à jour Flash ou Java.
Exemple sur la page : Nation Zoom et fausses mises à jour Java (PUP.DomaIQ)

re exécuter un fichier malicieux sur votre ordinateur : les mises à jour Flash ou Java.
Exemple sur la page : Nation Zoom et fausses mises à jour Java (PUP.DomaIQ)


www1.latestplayerplugin.com/7F3Hy2vi/detection/a/?dp=LqOPtmbfswtzuwDOgQainaFobGfa_FLavbad-VF_JEbaAdl
Google
Meistbesucht
Getting Started
Latest Headlines
Hotmail
Personnaliser les liens
Windows Media
Windows
Votre Lecteur Vidéo peut être obsolète
Veuillez
Recommandé
Il est recommandé que vous mettiez à jour votre Lecteur sur la dernière version
Veuillez liquer sur "Accepter et Installer" pour continuer.
Accepter et Installer
LEGAL
THIS AGREEMENT. YOU ARE ALSO AGREEING TO OUR PRIVACY POLICY. IF YOU DO NOT
Télécharger et Installer Maintenant
Accepter et Installer
Fiddler: Disabled


Firefox
Adobe - Install Adobe Flash Player
adobe.leeshow.net/FlashPlayer6/FR/update.php?installer=Flash_Player_11_for_Other_Browsers&browser_type=KHTML&dt
Google
Adobe
Adobe Flash Player
Version 11.9.900.152
Configuration requise
votre système:
Windows, française
Vous êtes un responsable informatique ou OEM?
À propos de :
Adobe® Flash® Player est un module externe de navigation léger et une application d'exécution sur Internet riche qui offre des expériences cohérentes et engageante pour l'utilisateur, la lecture audio/vidéo et un principe de jeu étonnant.
Installé sur plus de 1,3 milliard d'ordinateurs, Flash Player est la norme de référence pour afficher un contenu Web riche avec un fort impact.
Conditions :
En cliquant sur le bouton « Télécharger maintenant », vous reconnaissez que vous avez lu et accepté le Contrat de licence d'Adobe.
Remarque : votre antivirus doit vous permettre d'installer le logiciel.
Télécharger dès maintenant
France (modifier)
Copyright © 2013 Adobe Systems Incorporated. All rights reserved.
Conditions d'utilisatione | Politique de confidentialité | Cookies
www.malekal.com

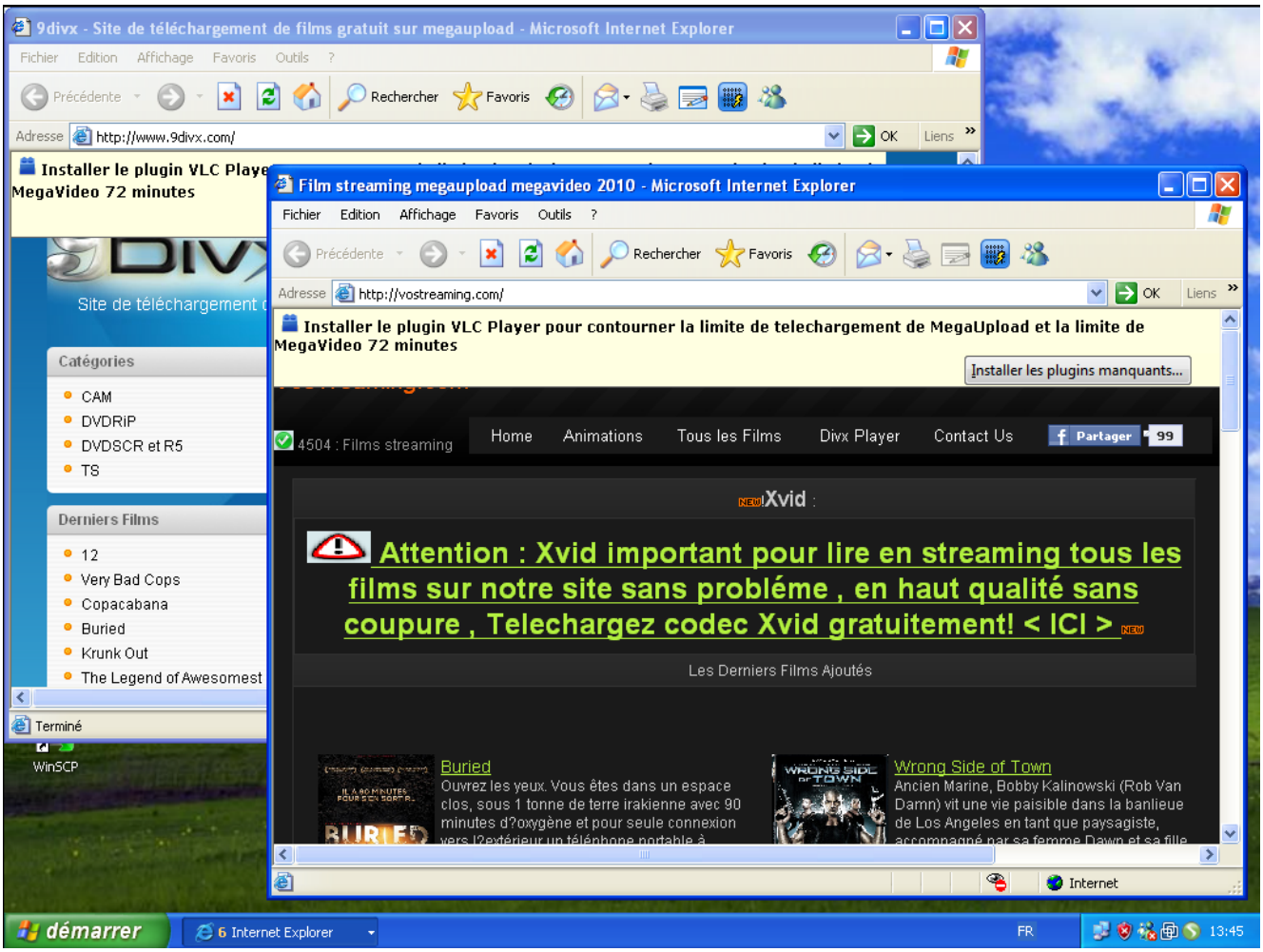


Des programmes pièges : PUPs et Adwares

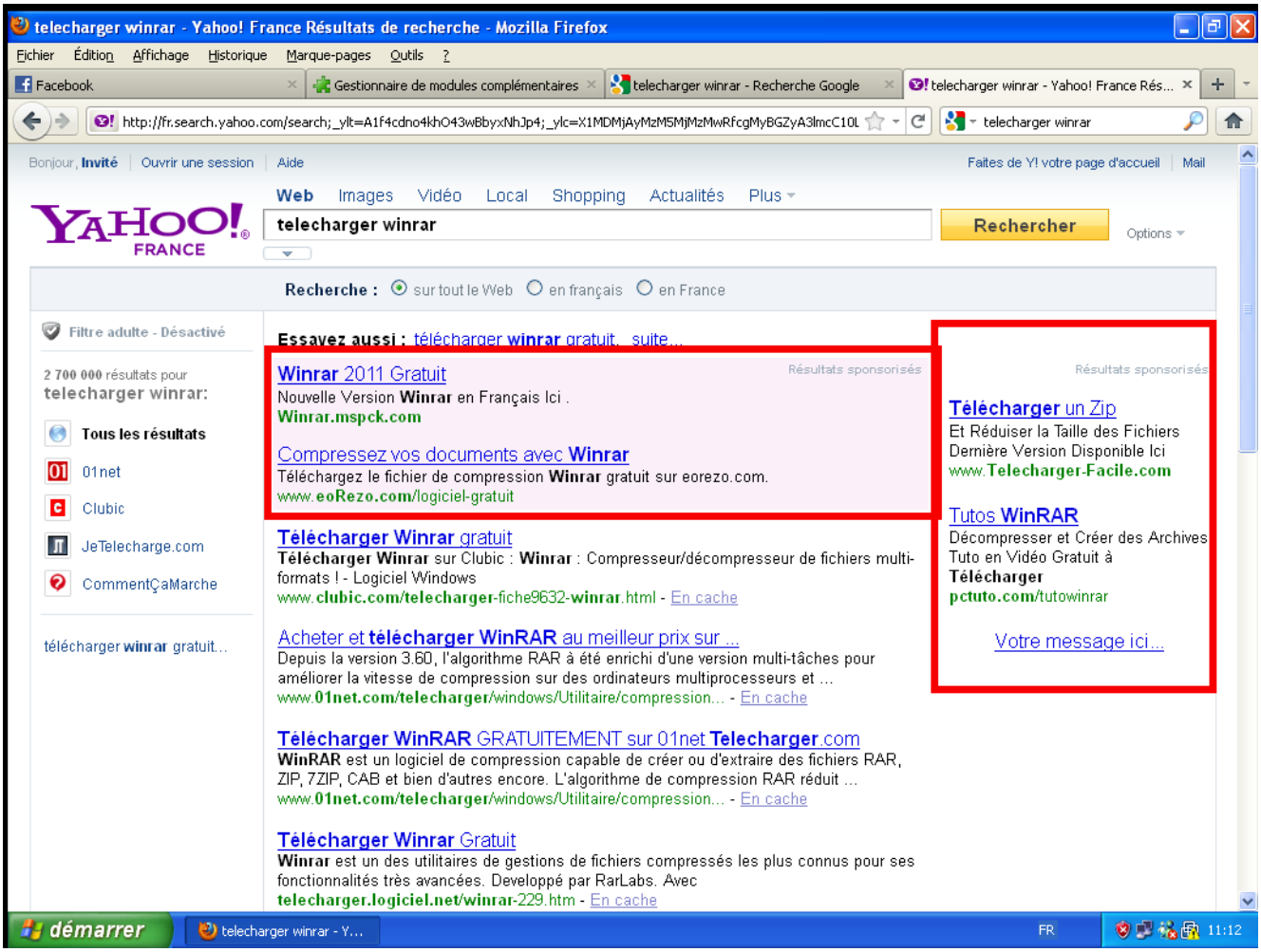
Tout comme il existe des codecs piégés, il existe aussi des sites proposant des logiciels contenant soit des adwares soit des des programmes non essentiels comme les barres d'outils : PUPs / LPIs : Logiciels potentiellements indésirables
Ces logiciels piégés sont très peu détectés par les antivirus, ce qui vous rend très vulnérable.

Toujours via du social engineering, il vous est proposé des programmes gratuits, ces programmes peu installer un adware qui ouvre des popups de publicités afin de rémunérer les auteurs.
Il n'est pas clairement dit sur ces sites que le programme installe un adware, en règle général, seulement dans les conditions d'utilisation.

Le fait que le programme soit gratuit fait que beaucoup d'internautes vont l'installer et se faire piéger, ayant du mal à désinstaller l'adware ou des programmes non essentiels comme les barres d'outils.
C'est donc une bonne stratégie pour gagner plus d'argent que d'offrir un programme payant qui sera certainement moins installer par les internautes.



ou ici en résultat de liens commerciaux depuis les moteurs de recherches :



La page suivant récapitule quelques un des PUPs/LPIS : [Détection Adwares PUA/PUP/PUP.Optional/LPI : Potentially Unwanted Program]

Les cracks et keygen

Un des gros vecteurs : les cracks et keygen.
Pourquoi ?
Car beaucoup d'internautes en téléchargent. Dès lors les auteurs de malwares proposent de faux cracks qui sont des installeurs de malwares. On créé des faux sites de cracks, les internautes les téléchargent et voila.
De plus, pour la majorité des internautes, faire la différence entre un vrai crack et un faux est difficile. Il n'y a qu'au

moment de l’exécution que l’internaute saura si c’est un vrai crack ou si cela va installer un malware.

Beaucoup d’exemples de malwares propagés des cracks sont donnés sur l’article : Le danger des cracks !

Ci-dessous un faux site de cracks pour distribuer des malwares: Faux site de crack : ça marche encore bien

Les auteurs de [RAT, Bifrose, Cybergate, Spynet : Botnet pour les nuls] utilisent beaucoup les forums Warez pour distribuer ces faux cracks.

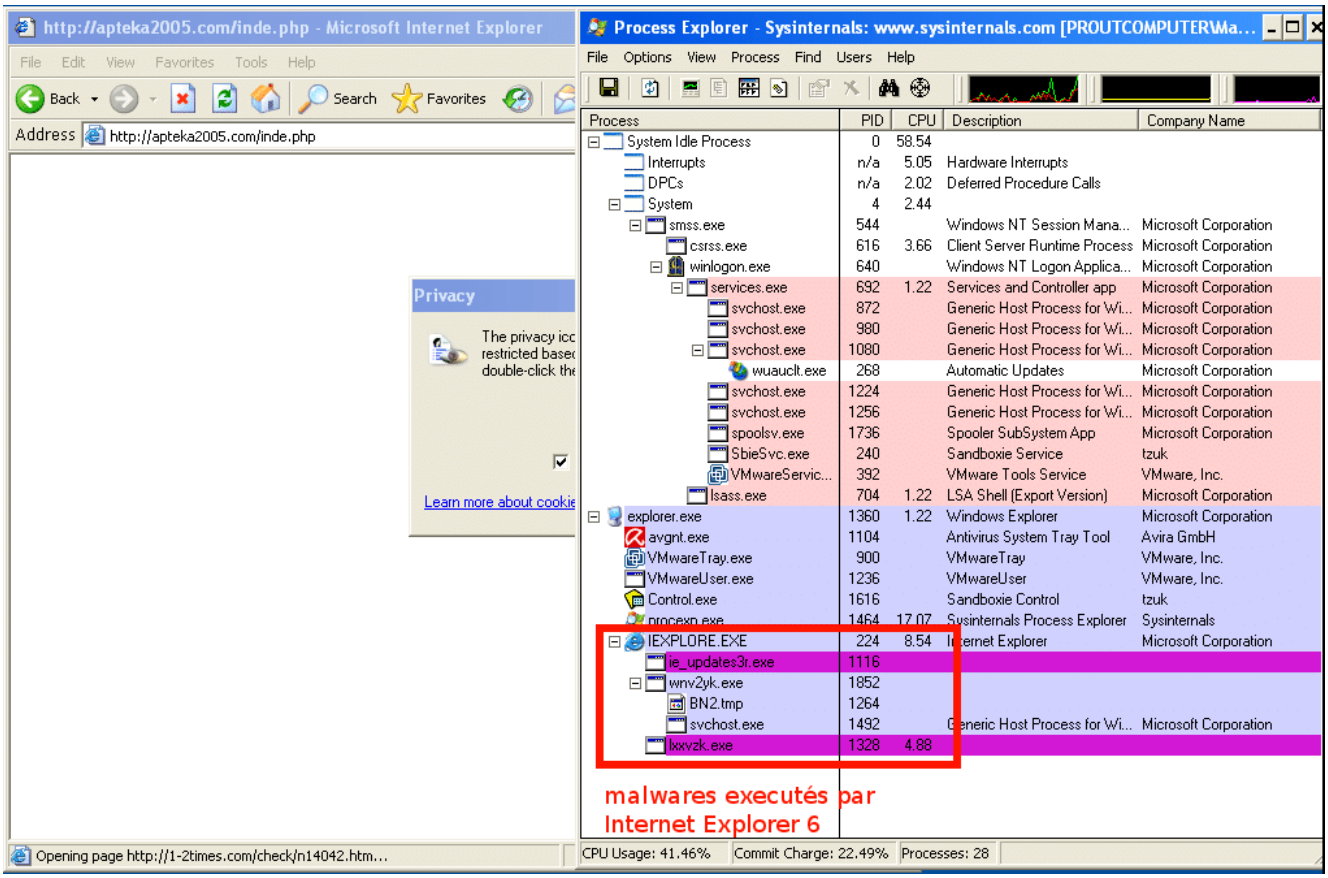
Ici un stealer pas très évolué qui vole les mots de passe des navigateurs WEB, cela permet de voir la porté de ces malwares : [Stealer pour les nuls : exemple de vol de mot de passe]

Driver Download et Web Exploit

Même si vous faites attention à ce que vous téléchargez etc… vous pouvez infecter votre ordinateur en consultant des [sites WEB hackés].

Certains groupes d'auteurs de malwares hackent des sites WEB afin de rediriger automatiquement les internautes vers des sites contenants des malwares, ceci se fait de manière invisible.
Vous pouvez donc être infecté en consultant des sites anodins..

Ces infections reposent sur des vulnérabilités, en maintenant votre ordinateur à jour (voir conseils plus bas), en utilisant un navigateur alternatif et en le sécurisant (voir Sécuriser le navigateur WEB Firefox), vous pouvez éviter ces infections.
Vous pouvez aussi consulter la page Surfer de manière sécurisée! qui permet de surfer à partir d'un OS virtuel et donc ne pas infecter son système d'exploitation.



web exploit ou drive download : vecteur de malware

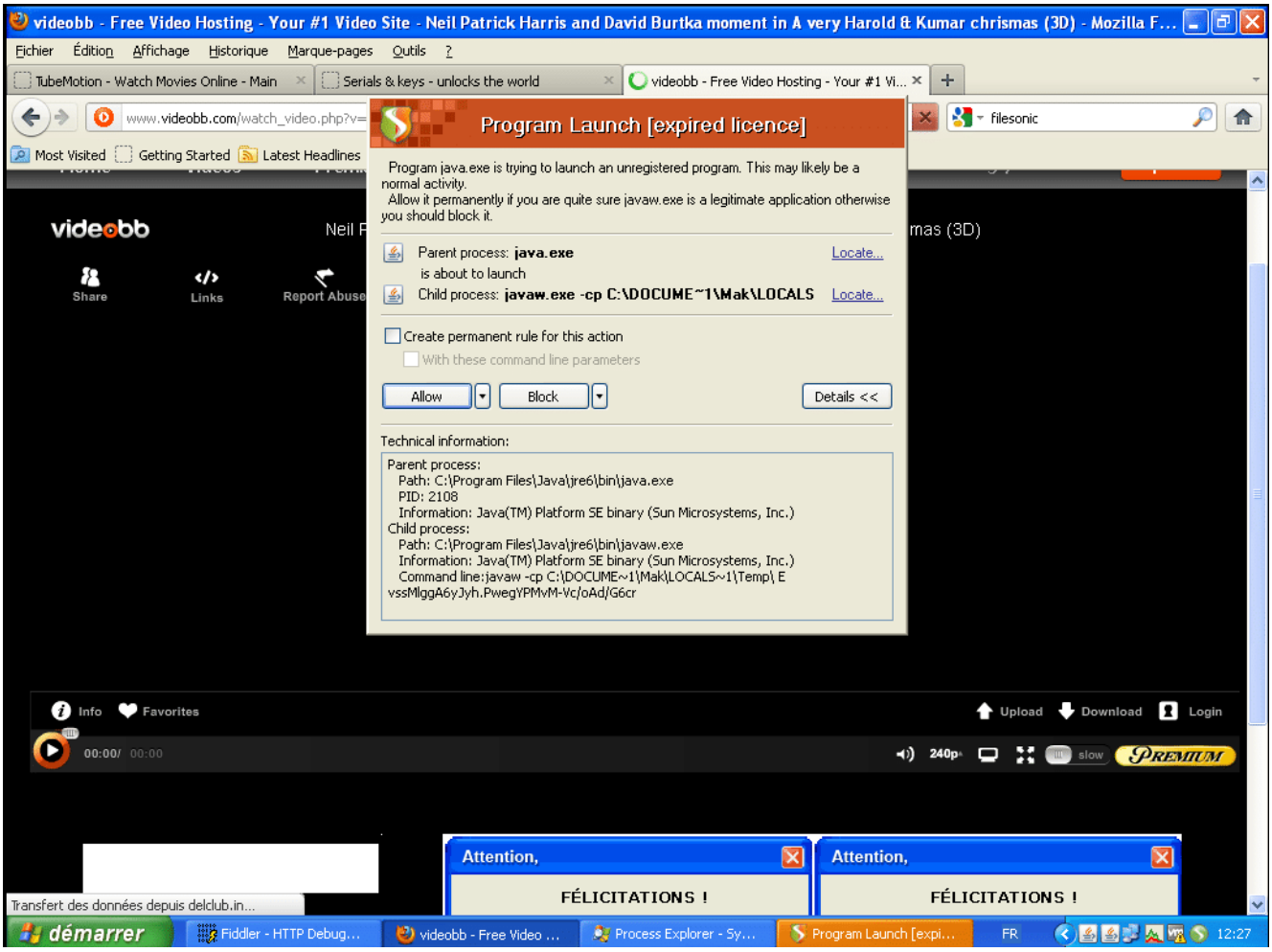
En vidéo :

Les malvertising

Les menaces ne concernent pas forcément des sites hackés mais aussi aussi être transmis via des « malvertising« , c'est à dire des publicités malicieuses.
Des publicités malicieuses qui conduisent aux exploits. Cela permet de toucher plusieurs sites à forte audience.

Fin Novembre 2011 de grosses campagnes de malvertising (publicités malicieuses) ont lieu pour transmettre des ransomwares type Fake Police.
Des sites de téléchargements sont touchés mais aussi videobb :

- Malvertising : asrvstatsmanager.com droppe malware via videobb et adserve.com
- dl-protect.com : Malvertising sur dl-protect.com via hooqy.com et clicksor



Mais aussi, par la suite, des sites pornographiques : pornerbros.com conduit à des infections via des exploits ou Malvertising : delivery.trafficbroker.com délivre ransomware « Activite illicite demelée »

Les arnaques sur internet

Parfois, de simples arnaques sont aussi diffusées, notamment à travers des publicités malicieuses sur les sites de cracks, streaming illégaux ou pornographiques.
Parmi ces arnaques, on trouve :

- Arnaque support téléphonique – PC Support et Arnaques

aux désinfections / support par téléphone
- Arnaque : Gagner Iphone à 1 euro
- Les faux sites d'actualités

A lire : Les sites de streaming et les virus

Sécuriser son ordinateur

Vous trouverez ici les règles de bases pour sécuriser votre ordinateur et Windows. Il est **fortement conseillé** de graver ces programmes afin d'être en mesure de les installer, avant toute connexion à internet, lorsque vous venez de formater.

Les bonnes bases

Vous trouverez énuméré ici quelques conseils à suivre afin de sécuriser Windows et votre ordinateur.
On voit de plus en plus de personnes installer deux, voir trois antispywares croyant être bien protégé, or il n'en est rien. Prenez soin de votre ordinateur, évitez d'installer tout et n'importe quoi, déjà car vous risquez de l'infecter mais surtout empiler les programmes tant à ralentir l'ordinateur et occasionner des plantages.

Multiplier les programmes augmente les chances de plantages et ralentit votre ordinateur mais ne procure pas une meilleur protection surtout si vous délaissez le reste des conseils (mises à jour, télécharger des cracks etc..).

Pour sécuriser Windows et votre ordinateur, suivez le guide :**Comment sécuriser son ordinateur ?**

Effectuer les mises à jour régulières

Vous devez ensuite effectuer les mises à jour Windows, afin de télécharger et installer les derniers correctifs disponibles. Les mises à jour se font à partir de Windows Update et Maintenez Windows et vos logiciels à jour !!!

Cette partie est très importante pour ne pas être à la merci des infections qui reposent sur des des failles de sécurités,

Maintenir votre machine à jour va augmenter vos chances de protection contre les malwares

Conclusion

Les auteurs de programmes malicieux utilisent beaucoup de méthodes différentes, parfois subtiles pour infecter les internautes. Pour s'assurer une prolifération importante de leurs œuvre, ils utilisent les vecteurs de propagation qui vont toucher le plus de monde possible :

- pièces jointes par mail
- fichiers piégés sur les Réseau P2P
- cracks piégés sur des sites de cracks ou tout simplement de faux sites de cracks : Un exemple des dangers du crack à travers Le danger des cracks!

- popup invitant à télécharger de faux anti-spyware

=> Comment les virus informatiques sont distribués

Résumé des recommandations de préventions

Si vous ne voulez plus être infecté :

- ne cherchez pas l'ultime programme de protection, EVITEZ simplement les cracks, faites attention aux fichiers que vous téléchargez et ouvrez.
- N'installez pas les programmes proposés par des publicités sur des site WEB ou via des popups
- Maintenez Windows à jour **et aussi** les composants WEB de votre navigateur (Java, Flash etc..)
- Gardez à jour votre antivirus
- Dans le cas où vous vous connectez depuis un modem, installez un firewall.
- Évitez d'installer le premier logiciel venu même si le site vous en donne l'envie, dans la mesure du possible installez des logiciels depuis des sites reconnus et sûres.

Il faut bien respecter **l'intégralité** de ces recommandations sinon cela ne sert à rien même avec un antivirus.

Un antivirus n'est pas infaillible, la sécurité de votre ordinateur sur internet ne se résume pas à l'installation d'un antivirus. La sécurité de votre ordinateur est au quotidien et c'est vous qui la faite :

- Connaître un minimum sur la propagation des menaces. Si pour vous sécurité, c'est installer un antivirus pour vous débarrasser du problème de malwares/virus pour courir sur P2P ou n'importe quel site, ce sera l'infection à coup sûr.
- Être vigilant.
    - Faire attention à ce que vous téléchargez, fichiers que vous ouvrez. N'importe quel fichier que vous téléchargez peut-être un virus informatique. C'est pas parce qu'un site est joli ou qu'il y a écrit « gratuit » qu'il faut foncer télécharger sans réfléchir.
- Maintenir son système à jour et ses logiciels tiers. Les vulnérabilités Windows, logiciels sont utilisés pour installer des infections automatiquement et à votre insu via la simple visite de page WEB => WEB Exploit. Voir les pages : Infections : exploitation SWF/PDF et Java

Autres conseils et liens

En plus de ce dossier, vous pouvez lire en parallèle la page suivante qui donne toutes les les méthodes utilisées pour distribuer des malwares/virus sur la page :

- Comment les virus informatiques sont distribués
- Pourquoi et comment je me fais infecter?

Ces deux pages démontrent en autre la faiblesse des antivirus :

- Un point sur les antivirus
- Adwares/Spywares : Comment NE PAS désinfecter son PC ?

Toutes les personnes qui viennent se faire désinfecter et qui ont un antivirus et un antispyware installés le démontrent aussi.

Quelque soit l'utilitaire que vous choisirez, si vous avez de mauvaises habitudes sur internet, vous serez infecté, ne posez donc plus la question « quel est le meilleur antivirus? », « ma protection est bonne? » cela revient à demander si on ne risque rien à sortir avec un gilet par-balles en pleine fusillade.

Pas de panique, venez demander de l'aide sur le forum dans la partie : VIRUS : Aide Malwares (vers, trojans, spywares, hijack)

Liens connexes

Voici quelques articles annexes sur la sécurité informatique :

- Pourquoi et comment je me fais infecter?
- Business malwares : le Pourquoi des infections informatique
- Comment les virus informatiques sont distribués.
- La sécurité de son PC, c'est quoi ?

- Pourquoi et comment je me fais infecter?

- N’ouvrez pas n’importe quel fichier, faites attention à ce que vous téléchargez et d’où vous téléchargez : Prévention : Logiciels et sources de téléchargements
- Les Bannières/popups de publicités dangereuses sur la toile
- Surfer de manière sécurisée!

Je vous invite si vous avez des enfants à lire cette page :

- Sur le forum sont recensées les arnaques et pièges de l’internet

Participez au projet Antimalware (pour plus d’informations, cliquez sur la bannière)

Si vous avez des questions ou rencontrez des problèmes, n’hésitez pas à venir poser vos questions sur le forum du site