
DANGER
LE WEB EN PÉRIL
WWW
SYLVIE LAFLAMME
Trucs de Pros

AVIS

Cette publication est pour votre information seulement. L'auteure ou ses revendeurs ne sauraient être tenus responsables des résultats que vous obtiendrez en utilisant ce matériel.

Tous les liens présents dans ce document étaient valides au moment de publier ce livre. Parce qu'Internet change tous les jours, nous ne pouvons garantir qu'ils sont encore actifs au moment où vous lisez ces lignes.

ISBN – 978-2-923592-47-3
Dépôt légal - Bibliothèque et Archives nationales du Québec, 2009
Dépôt légal - Bibliothèque et Archives Canada, 2009

Ce rapport vous est offert gratuitement. Pour connaître nos autres publications, visitez

http://www.virtuelexpress.com

Table des matières

Introduction

Votre site est malade depuis quelques heures. Vous ne voyez plus votre page d'accueil mais que des trucs bizarres...

Vous accédez à votre espace pour remettre la nouvelle copie de votre page index et presqu'instantanément, elle devient identique à l'ancienne...

Cette petite histoire n'est peut-être pas encore la vôtre, mais il y a de fortes probabilités qu'elle le devienne très bientôt. Je ne vous le souhaite cependant pas car je sais ce que cela signifie, pour être passée par là durant l'été 2009.

C'est le monde à l'envers.

Hier on nous forçait presqu'à mettre une page index dans chaque répertoire d'un site web afin de cacher son contenu aux yeux trop curieux. Aujourd'hui c'est par ces pages index que nos sites deviennent fragiles et malades.

Pendant un peu plus de **SIX** semaines, mon équipe et moi-même avons littéralement COMBATTU le trojan Gumblar jours et nuits. Aussitôt que nous trouvions une faille de sécurité, que nous la bouchions et réparions le site, aussitôt il redevenait infecté.

Je ne compte plus le nombre de fois où nous avons fait réinstaller une copie de sauvegarde après avoir demandé aux techniciens de notre service d'hébergement de nettoyer tous les fichiers contenus dans le site infecté.

Mes plus proches amis vous diront qu'ils ont été inquiets pour mon moral et ma santé. En juillet il y a 31 jours et 31 nuits… mais je n'en ai dormi partiellement que 18… imaginez un peu la qualité de vie !

C'était à ce point déstabilisant et le sentiment d'impuissance si envahissant que je me souviens avoir même écrit à un ami très cher qui me prête oreille attentive quand la soupape veut sauter : « *J'aimerais m'évader de ma propre vie*. »

Ceci pour vous dire à quel point ce genre de problème peut devenir envahissant et intolérable.

Si votre gagne-pain est généré par votre entreprise sur le web, le risque encouru de tout perdre est majeur. Les utilisateurs de Mac ne peuvent plus se croire à l'abri. Dorénavant, plus aucun système d'exploitation, Mac, Unix/Linux inclus, n'est parfaitement invincible.

Nos pertes financières se comptent en plusieurs milliers de dollars sans compter le temps qu'il nous faudra pour nous en remettre car c'est réellement pénible pour le système nerveux et la planification de travail.

Ne voulant pas que d'autres personnes vivent le même enfer, l'idée d'écrire ce livre m'est apparue comme une évidence. Imprimez ce livre pour le conserver à portée de main. Il pourrait vous sauver ÉNORMÉMENT de temps et d'argent tout en vous permettant de conserver votre qualité de vie actuelle.

J’aurais pu facilement vendre ce livre mais il aurait été inaccessible aux personnes qui ont le plus besoin d’apprendre à se protéger et à sauvegarder leurs revenus en ligne.

C’est pourquoi j’ai opté pour préparer ce livre gratuit et un autre, plus élaboré pour ceux qui veulent vraiment aller à fond dans ce sujet, il est disponible sur le site mentionné en page 3.

Dans l’espoir que ce livre vous permettra de conserver la paix et l’harmonie dans votre vie.

Sylvie Laflamme

L'infection

Les internautes actifs savent depuis longtemps qu'il est nécessaire d'utiliser un bon antivirus et qu'il faut surtout très souvent le mettre à jour. L'habitude peut nous porter à devenir trop confiants et c'est alors que les failles apparaissent dans notre armure.

Vous reconnaissez-vous dans l'une ou l'autre de ces situations ?

- L'heure de la mise à jour de votre antivirus est planifiée à 8h du matin mais vous n'êtes pas devant votre ordinateur à cette heure matinale et il est fermé.

- Vous avez téléchargé votre antivirus sur un site qui en faisait l'éloge, sans être le site du fabricant ni celui d'un portail qui vous aurait dirigé vers le site de la compagnie qui offre ce produit sur le marché.

- Vous utilisez un pare-feu chaudement recommandé par un ami mais vous n'avez pas désactivé le pare-feu de Windows qui est déjà là.

- Votre antivirus est gratuit et les mises à jour se font automatiquement sans vous donner la possibilité de vous rendre sur le site de la compagnie pour télécharger manuellement le fichier de mise à jour ou du moins pour vérifier le nom du fichier ainsi que son « poids » et le comparer à celui que vous avez sur votre ordinateur.

- Vous possédez un antivirus et un pare-feu et vous vous sentez totalement protégé puisque vos mises à jour sont quotidiennes et que vous vous assurez qu'elles ont bel et bien été faites.

- Vous laissez votre antivirus faire les scans quand bon lui semble car vous ignorez comment programmer les scans vous-même.

- Vous utilisez un antivirus démonstrateur et quand il arrive à expiration, vous le désinstallez puis vous en utilisez un autre.

- Vous préférez n'utiliser que les antivirus en ligne pour ne pas devoir les mettre à jour vous-même.

Tout ceci est intéressant mais hélas, vous n'êtes pas protégé si vous vous en tenez qu'à une ou l'autre de ces situations ou même à la liste entière.

Il y a quelques années, les spécialistes ne parlaient que de virus puis est arrivé le temps des fichiers espions, des chevaux de Troie, des spams, des Trojan, des fishing et j'en passe…

Sauriez-vous faire la différence ?

L'infection d'un ordinateur ne nécessite même plus que vous téléchargiez un fichier en provenance d'un site douteux ni même que quelqu'un vous l'envoie par courriel.

En effet, de nos jours il suffit de visiter un site infecté pour que l'infection s'accroche à votre ordinateur. Les vidéos et les fichiers audio ne sont pas toujours « propres ».

Même une belle image toute simple du chaton sur le bord de la fenêtre de la cuisine, reçue d'une personne de confiance, pourrait être porteuse d'une faille de sécurité insérée dans son code.

Tous ces beaux fichiers qui circulent librement sur le web et qui sont si touchants… sont-ils inoffensifs ?

Peut-être vous souvenez-vous de ce magnifique feu d'artifice qui était attaché à de nombreux courriels et qui nous invitait à ouvrir le fichier pour regarder l'image? Il était porteur de bien mauvaises nouvelles…

Aujourd'hui il est possible d'ouvrir un courriel en refusant que les images et attachements s'ouvrent en même temps. Configurez votre logiciel de gestion de courriels de manière à ne pas ouvrir les images en ouvrant le message. Ne téléchargez pas les attachements et s'il est trop tard, ne les ouvrez pas avant d'avoir fait quelques mises à jour de vos outils de protection.

Une bonne habitude à prendre serait de n'ouvrir les attachements que plusieurs jours après leur arrivée. Ainsi vous donnerez la chance à vos outils de protection de pouvoir vous protéger.

Dans le monde médical il est impossible de créer un vaccin contre un virus avant même la naissance du dit virus. Il en va de même dans le monde informatique.

Un super antivirus accompagné d'aussi formidables outils de sécurité ne peut rien pour vous s'il fait face à ce fichier malsain pour la toute première fois. Certains antivirus sont conçus pour déceler un code sortant de l'ordinaire mais selon la configuration que vous leur aurez attribuée, ils placeront le code en quarantaine, l'ignoreront ou le détruiront.

Si vous êtes dans le premier lot d'Internautes ayant reçu ce tout nouveau fichier malsain, vos outils ne pourront guère vous aider.

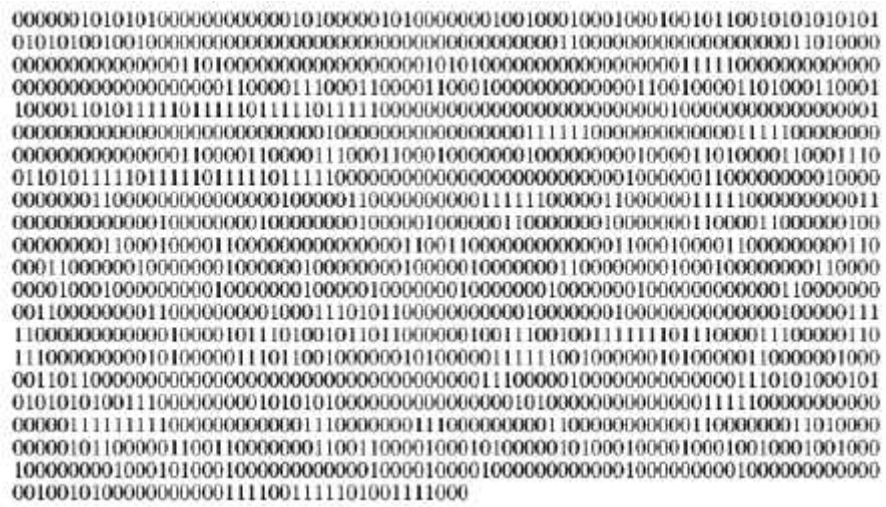
Mais si vous attendez 4 ou 5 jours avant d'ouvrir les fichiers, vous donnez plus de chances à vos outils d'être mis à jour et de pouvoir conjurer le mauvais sort et vous protéger adéquatement.

Comment est-ce possible ?

Il faut comprendre un peu le fonctionnement de votre ordinateur, de l'informatique et d'Internet. Sans vous donner une formation approfondie qui prendrait des mois à assimiler, sachez que tout ce qui touche à l'informatique, du moins dans sa portion utilisée actuellement par les Internautes, est constitué de deux impulsions électriques (en fait une impulsion et son absence) représentées graphiquement par les chiffres 1 et 0.

Le nombre de répétitions et la disposition de chacune des impulsions fera en sorte que l'ordinateur, du moins la composante qui en a la capacité, pourra traduire le signal en image, en son, en couleur etc.

Une image, une vidéo, une lettre, un chiffre, bref tout ce qui passe par l'informatique est donc constitué d'un code ressemblant à ceci :



*source de l'image : http://frenzy.chez.com/images/code_binaire.jpg

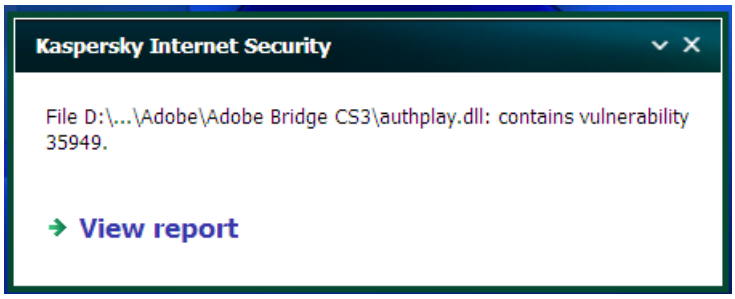
Afin de rendre l'image « dangereuse » (ou n'importe quel autre fichier), la personne mal intentionnée n'a qu'à insérer un code en transparence. Je n'entrerai pas dans les détails techniques car il faut quand même connaître la programmation et être en mesure d'écrire un code bien spécial.

Mais sachez qu'un fichier malsain peut porter une extension tout à fait anodine, tel que les .jpg, .gif, mpeg, .scr, .flv ou bien d'autres et pourtant ne pas du tout être un fichier de cette catégorie. Il faut avoir des doutes lorsque vous tentez de voir un fichier portant une extension habituelle et que votre ordinateur vous indique qu'il ne sait pas avec quel outil ouvrir ce fichier.

Il y a quelques années on nous mettait en garde contre les fichiers .exe (exécutables), très souvent porteurs de fichiers malsains. De nos jours, presque toutes les sortes de fichiers peuvent transporter un code malsain.

Le dernier à ma connaissance est le fichier .pdf. Depuis février 2009, la compagnie Adobe a été informée de la faille de sécurité de ses produits, principalement dans son lecteur Adobe Acrobat mais ce n'est qu'à la fin de juillet de cette même année, que la compagnie s'est décidée à agir et à créer une mise à jour plus sécuritaire.

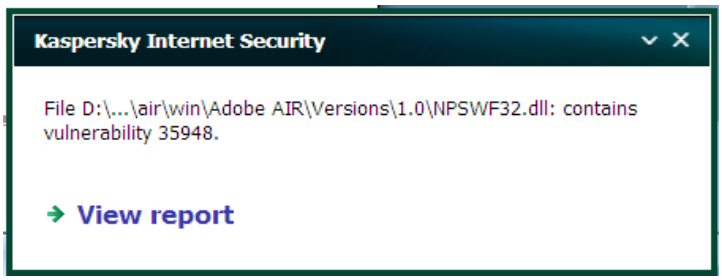
Mais il n'y a pas que ce produit qui soit fautif chez Adobe. La collection presque complète a été soumise à une inspection et malgré tout il demeure quand même des failles de sécurité comme en fait foi cette image prise sur mon portable il y a quelques minutes à peine :



Dans cette image vous remarquez que je possède la version CS3 D'Adobe. L'idéal serait d'acheter la version CS4 afin d'avoir les produits les plus performants et les plus sécuritaires et c'est probablement la meilleure solution.

Adobe offre plusieurs utilitaires gratuits dont son Acrobat Reader mais aussi son très populaire Adobe Air.

Kaspersky m'a informée d'une faille de sécurité dans la version que j'utilise :



Une façon assez simple d'améliorer la sécurité de mon ordinateur sera de visiter le site d'Adobe pour récupérer la version la plus récente. Au moment d'écrire ces lignes, la version Adobe Air la plus récente est la 1.5.2. Je dois donc la télécharger immédiatement pour éviter une faille de sécurité.

Adobe offre d'autres utilitaires gratuits tel que Flash player et Shockwave Player. Il me faudra aussi les mettre à jour avec les versions les plus récentes. Nous devrions tous faire ces mises à jour fréquemment.

Pendant ce temps, les éditeurs de fichiers .pdf, les acheteurs et lecteurs de ces mêmes fichiers, ont fait partie de la grande famille des hackers, sans le savoir. Eh oui ! Chacun a fait sa petite part pour que l'infection se propage partout sur le réseau Internet.

Vous connaissez certainement ce logo  c'est celui du lecteur Acrobat. Faites votre mise à niveau très fréquemment et inscrivez-vous sur leur liste pour être informé lorsque de nouvelles versions sortiront. C'est gratuit et ne vous engage à rien du tout.

Gumblar

Dans le cas de Gumblar, un petit code inséré dans la page index du site malade, vient s'installer dans votre ordinateur dès que vous accédez à la page infectée.

Comment y parvient-il ?

Simplement parce que, pour s'afficher à l'écran, le site que vous regardez doit être téléchargé sur votre ordinateur dans la cache du navigateur utilisé.

Une fois sur votre ordinateur, parce qu'il contient aussi un bout de code qui empêche de le désinstaller ou même d'effacer le fichier porteur, il se balade dans votre disque dur à la recherche d'un logiciel FTP. Si sa recherche est fructueuse, il récupère tous les codes d'accès et les envoi à son concepteur ou les utilise lui-même pour accéder, à votre insu, à tous les sites auxquels vous avez accès.

Qu'y fera-t-il ?

Il viendra infecter toutes les pages index, visibles en ligne ou non.

Si vous ne gérez pas de sites web, vous participerez à la propagation de l'infection si vous publiez un lien menant vers un site infecté.

Vous avez aimé un site web, une vidéo, avez effectué une recherche via un moteur de recherche dont le site a été infecté ? Si votre ordinateur n'est pas suffisamment protégé et que vous l'ignorez, vous infecterez votre disque dur à coup sûr.

Cette infection est invisible sauf si vous utilisez un outil de protection qui est en mesure de la déceler et de vous en aviser.

Vous pensez faire plaisir à vos amis en les invitant à visiter un site amusant ou pour visionner une vidéo particulière mais vous les avez poussés vers une source de problèmes potentiels.

Vous ne gérez probablement pas de sites web, mais eux peut-être que oui.

Avant de partager vos bonnes trouvailles, assurez-vous que votre ordinateur est réellement bien protégé avec PLUSIEURS outils de sécurité. Un antivirus mis à jour NE SUFFIT PLUS !

Quel outil peut m'aider ?

Il existe plusieurs bons outils, mais celui qui nous a sortis de la tempête est la suite Kaspersky. Pas uniquement l'antivirus mais LA SUITE COMPLÈTE du nom de Internet Security.

Une remarque cependant, vous devez désactiver le pare-feu Windows pour qu'il soit réellement efficace car il vous est fourni avec son propre pare-feu entièrement compatible avec tous les autres outils faisant partie de cette suite complète.

Il y a possibilité de tester leur produit avant de l'acheter.

Si vous pensez avoir un problème avec votre ordinateur, Kaspersky offre aussi la possibilité d'une vérification en ligne avec leur outil. Il faut télécharger une petite application qui sert à confirmer à leurs serveurs que c'est bel et bien votre ordinateur et qu'il peut y chercher des fichiers malsains.

Notez que l'outil en ligne est inutile si vous ne désinstallez pas vos logiciels de protection déjà installés sur votre disque dur. Assurez-vous donc de pouvoir installer à nouveau vos outils ou de nouveaux outils ensuite.

Si vous préférez utiliser des outils gratuits, vous aurez besoin de PLUSIEURS d'entre eux et assurez-vous de prendre garde qu'ils ne soient pas incompatibles entre eux.

Il vous faudra un :
. antivirus
. anti fichier espion
. anti spam
. anti hameçonnage
. anti trojan
. anti cheval de Troie
. etc.

Vous devrez les télécharger DIRECTEMENT à partir du site de la compagnie qui l'a conçu pour éviter de vous faire prendre par des versions déjà contaminées et mises en ligne pour mieux répandre l'infection.

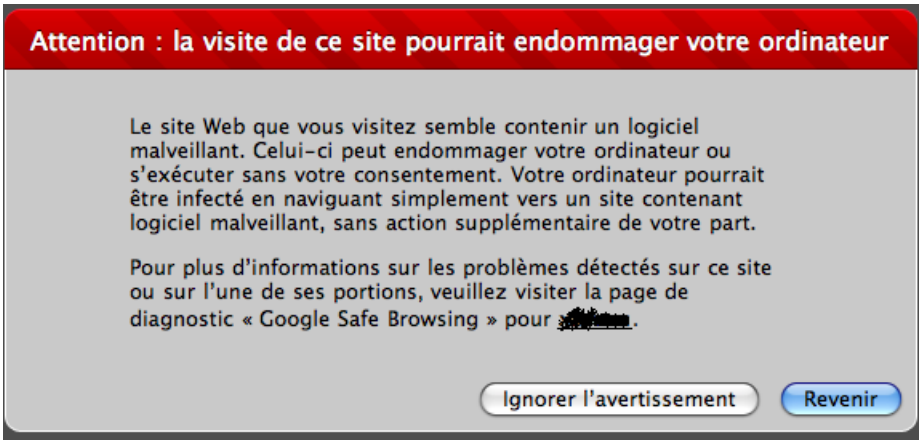
Plusieurs de ces outils gratuits sont conçus de manière à ne pas fonctionner si un autre logiciel entre en compétition avec un autre des logiciels de sécurité offert par la compagnie d'origine.

Par exemple, l'antivirus xyz ne fonctionnera pas efficacement si un autre antivirus est déjà installé. De plus, en voulant le désinstaller, vous aurez à retirer manuellement un fichier pour permettre l'installation d'un autre antivirus. Cependant, cet antivirus concerné est très réputé. Ceci n'est qu'une stratégie marketing, rien de bien méchant mais passablement désagréable pour qui désire ne plus utiliser leurs produits.

Si vous gérez un ou des sites web, les connaissances à posséder pour vous protéger, protéger votre site et par le fait même tous vos visiteurs, sont trop imposantes. Procurez-vous le livre « La Toile se fissure : comblez vos brèches » Afin d'en savoir plus et dormir en paix.

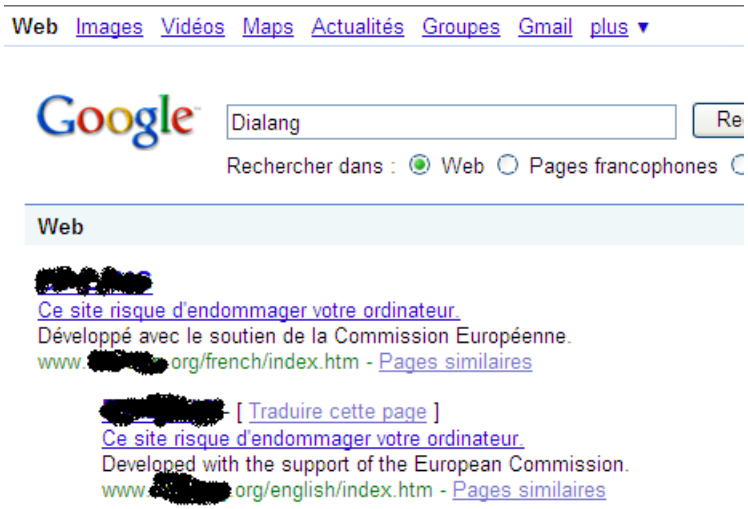
Vous devez comprendre que Gumblar est très agressif. Il détruit vos sites web, il vole vos informations, il peut même détruire votre entreprise en ligne. Mais son cousin qui arrive à grands pas, semble bien plus néfaste.

Ne permettez pas que vos visiteurs reçoivent ce genre d'alerte en visitant votre site web :



IL FAUT AGIR MAINTENANT !

Google et d'autres moteurs de recherche ont opté pour bannir temporairement les sites infectés tout en indiquant un avis dans les résultats de recherche. Voici ce qu'on pouvait lire à propos d'un site qui semble avoir été détruit par Gumblar :



Lorsqu'un client potentiel voit « Ce site risque d'endommager votre ordinateur », vous venez de perdre une vente.

Chaque jour il se perd des milliers, voir des centaines de milliers de commandes. Faites en sorte de ne pas faire partie des perdants.

Conclusion

Vous en savez suffisamment pour ne plus prétendre ignorer les risques. Soyez responsable de votre ordinateur, même si vos enfants l'utilisent. Ne vous fiez pas à eux pour que vos outils de protection soient mis à jour. Faites-le vous-même.

Souvenez-vous de cette phrase :

Si je ne fais pas partie de la solution,

je fais partie du problème !

Affichez-la partout ! Faites en sorte que tous les utilisateurs de l'ordinateur de la maison soient conscients de leurs responsabilités et s'ils ignorent comment se protéger, qu'ils se donnent la peine de vous informer lorsqu'ils rencontrent des situations particulières.

Au printemps 2009, il n'y avait que quelques dizaines de milliers de sites infectés, en juin ils étaient plusieurs centaines de milliers, en juillet ils dépassaient largement le million et au moment d'écrire ces lignes, ils sont maintenant plusieurs millions.

Dites-vous que vous avez plus de probabilités d'en rencontrer un que de tous les éviter. N'hésitez pas à commander le livre qui explore le sujet beaucoup plus profondément. Il est disponible sur le site mentionné à la page 3 de ce livre gratuit.

Tous ensembles nous réussirons à ralentir l'infection si nous nous y appliquons sérieusement.

Sylvie