RECOVERING FROM / AND PREVENTING AN IFRAME VIRUS ATTACK ON YOUR WEBSITE

Version 1.0 Patrick Brunswyck

a manual by

all2all

Moving Art Studio a.s.b.l.

all2all .beagent RIPE NCC Member

Table of Contents

Recovering from / and preventing an iframe virus/Trojan attack on your website

What is an iframe

IFRAMES (Inline Frames) are an easy way to include one html page in another. They are used to embed some content on a page. The content is separated either because it's big, and you want to be able to scroll it independently, or because it's dynamically generated and you want to embed it easily. the tags used for an iframe are <iframe> </iframe>.

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

What is the impact of an iframe virus/Trojan

When you browse to a website (e.g. in IE), that is infected with malicious code, the browser will download that code (this is a trojan horse / spyware) from the URL situated in the iframe container. (sometimes your browser might open an Acrobat Reader document). Most anti-virus programs don't detect this Trojan horse, some will give you a warning but won't prevent the execution of the script. As soon your PC is infected, the trojan will hide itself and steal your FTP passwords whenever you type them into your FTP program and it will report your passwords to a central server. This server will then use your FTP-logins, download your site files, manipulate them, to then upload them to your site again. This trojan will recursively run through all of your directories on the FTP server and hunt down the most vulnerable files for this kind of attack, files with names like:

- main
- default
- index
- home

The trojan horse will inject the malicious code into these and other files. It may inject an iframe container into any page it can. It changes the iframe targetpage. All .php, .html, .js,.... files can be infected, especially when they contain the </body> tag. This iframe virus infects your PC via PHP, java (including javascripts in .pdf or .swf files) and HTML scripts. The virus nests itself on the **end user's** PC in 99% of the cases. The code overwrites the **iframe targetpage**, in the example above this is ***yourinitialsite.htm***, this will be changed into something like **<iframe src="http://c9u.at:8080/ts/in.cgi?pepsi147"**, to then redirect you to another website that your visitors will view and end up being infected themselves, where the virus will lurk again on their PC's waiting to steal and collect more FTP passwords to access servers...

How to remove the virus

To get rid of the virus you need to remove all the **iframe code** out of your infected php files. You have to check all the PHP, HTML, JS, ... files on your server. Also, the virus can modify the **.htaccess** file, **hosts** files and create **images.php** files in the **images** directory. The virus could also have infected your CMS themes and templates of your CMS. This is not a system wide server infection because the virus only exploits the ftp accounts it knows the passwords of.

On the server:

Check the files on your server for the following code: **<iframe .... style="visibility: hidden;"></iframe>** A good tool to help you locate the iframe code quickly is TextCrawler. Once you have removed all these corrupted iframe tags, proceed as follows:

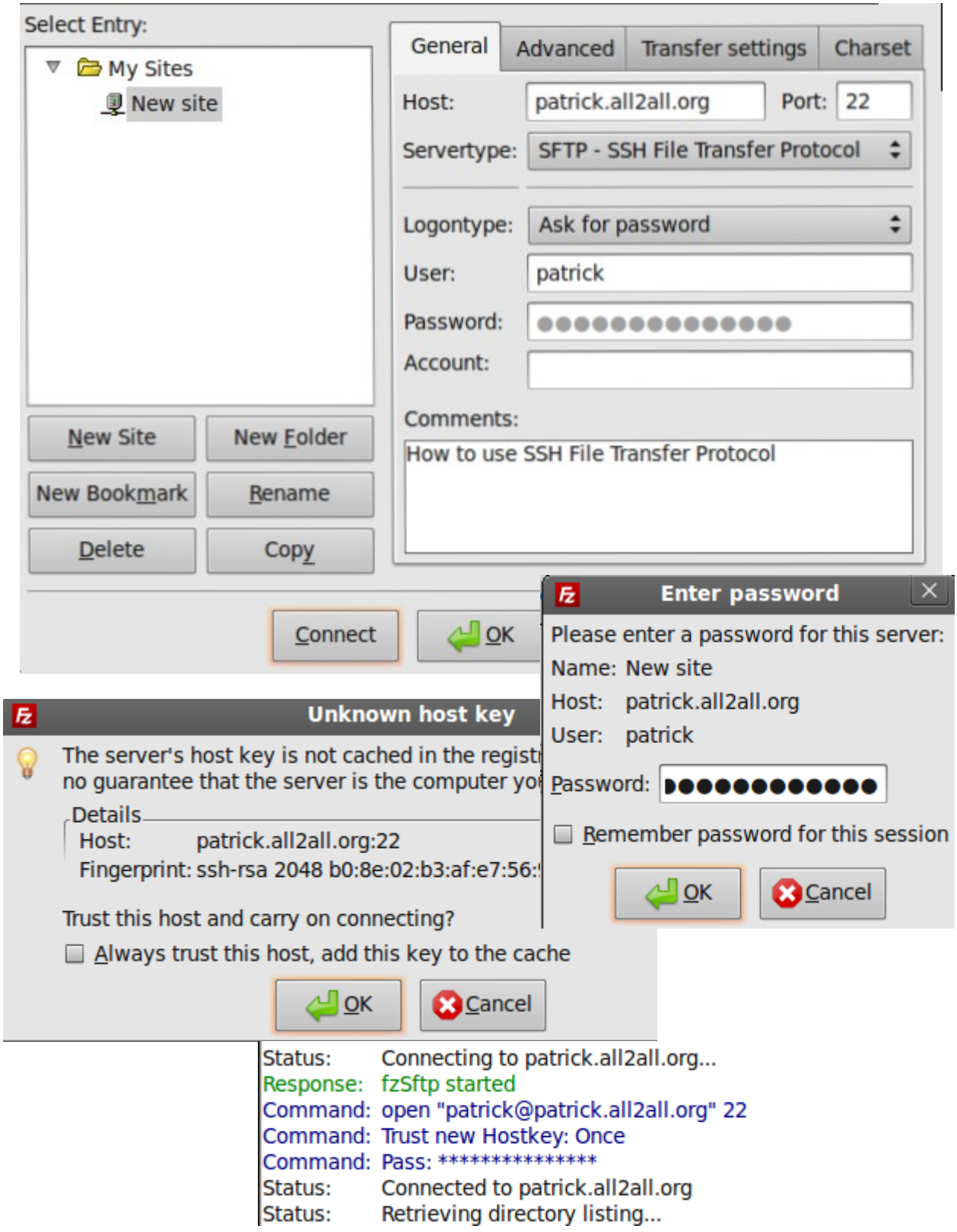
- clear your CMS's cache (clear cache: Drupal – Joomla! – SPIP – WordPress)
- your website is currently infecting other PCs so you need to temporarily block access to your website by uploading an index.htm file explaining why the server is down
- don't remove the files on your server but replace the infected files on your server with the files of your last virus free site backup. If this happens to be impossible then download the infected PHP, HTML, JS, etc. files to a location under quarantine to clean them
- recheck your files to see if there are no more occurrences of corrupted iframe containers on the server (<iframe .... style="visibility: hidden;"></iframe>)
- clear your CMS's cache once more
- make sure you continue to monitor the situation the first couple of days to make sure the files don't get infected again, so keep a close eye on the files.
- always make sure you have a **virus free backup** of your site!

On the PC:
(note: Linux PCs are not affected)

- install a good and **up to date** antivirus program / internet security suite on the pc and execute a full scan (For WordPress install the antivirus plugin as well)
- once your PC is totally clean you can change your **FTP passwords** (use a secure password!)
- update Adobe Acrobat Reader and Shockwave
- change all passwords you have used while your PCs were infected
- now uninstall your FTP program including the registry keys. You can achieve this with a freeware program called Revo Uninstaller. Install FileZilla (recommended)
- try to use alternative software like FileZilla as your FTP client and Mozilla Firefox as your browser (Internet Explorer is very vulnerable). Make sure your Operating System and your software is up to date!
- don't save passwords on your PC. Try to memorize them

Attention! The virus may be listening in (eavesdropping) on bypassing network traffic originating from other computers on the local network (packet sniffing) to steal FTP passwords! This means that you can clean up your PC but if another PC is infected located in the same network segment, the virus can still intercept the passwords you have entered on the clean PC!
Also, be careful with FTP passwords you have saved in the past. The virus may have the potential to extract those saved passwords. Considering the dangers involved it is advisable to login to your FTP server using the SSH over FTP protocol.
Source: http://soyouwillfindit.blogspot.com/2009/08/virus-steals-ftp-passwords-and-insert.html

Configure FileZilla with FTP over SSH



Versions

Version number	Modifications	Author
1.0 EN	Original version	Patrick Brunswyck
1.0 NL	Original version	Patrick Brunswyck

page	**Modifications**