VOORKOMEN / HERSTELLEN VAN EEN IFRAME VIRUS AANVAL OP UW WEBSITE

Versie 1.0 Patrick Brunswyck

een handleiding door

all2all

Moving Art Studio v.z.w.

all2all .beagent RIPE NCC Member

Inhoudsopgave

Voorkomen/herstellen van een iframe virus/Trojaans paard aanval op uw website

Wat is een iframe

Een IFRAME staat voor Inline Frame. Door deze definitie is het mogelijk om een andere html-pagina weer te geven in een bepaald gedeelte van een tabel. De tag die voor een iframe gebruikt wordt is <iframe> </iframe>

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

Wat doet een iframe virus/Trojaans paard

Wanneer u een website opent (bvb in IE), die geïnfecteerd is met kwaadaardige code, dan zal uw browser deze code downloaden (dit is een Trojaans paard/spyware) van de URL die zich in de iframe container bevindt. (soms opent uw browser een Adobe Acrobat Reader document). De meeste anti-virus programma's detecteren dit Trojaans paard niet, sommige geven enkel een waarschuwing maar blokkeren de uitvoering van dit script niet. Zodra uw computer geïnfecteerd is zal een Trojaans paard zich nestelen op uw computer en uw FTP paswoorden stelen wanneer je deze in uw FTP programma intypt en deze rapporteren aan een centrale server. Deze server maakt dan gebruik van uw FTP-logins, download uw bestanden, manipuleert deze, om ze dan weer naar uw site te uploaden. Dit Trojaans paard zal al de mappen op uw FTP server aflopen en op zoek gaan naar bestanden die het meest vatbaar zijn voor deze aanval, bestanden met b.v.b. de volgende namen:

- main
- default
- index
- home

Het Trojaans paard injecteert de kwaadaardige iframe code in deze én andere bestanden. Het wijzigt de iframe doelpagina. Alle .php, .html, .js, ... bestanden kunnen geïnfecteerd zijn, zeker als die een </body> tag bevatten. Dit iframe virus infecteert uw pc via PHP, java (ook javascript in .pdf of .swf bestanden) en HTML scripts. Het virus nestelt zich in 99% van de gevallen op de **eindgebruiker** zijn PC. Deze code overschrijft de **iframe doelpagina**, in het voorbeeld hierboven is dat ***jebeginsite.htm*** dit wordt bijvoorbeeld **<iframe src="http://c9u.at:8080/ts/in.cgi?pepsi147"**, om dan naar een andere webpagina te verwijzen waar uiteindelijk uw website bezoekers op terecht komen om vervolgens zelf geïnfecteerd te worden door dit virus, waar het vervolgens wacht om opnieuw FTP paswoorden te verzamelen van een server...

Hoe dit virus verwijderen

Om dit virus te verwijderen dien je de **iframe code** te verwijderen uit de geïnfecteerde php bestanden. Je moet alle PHP, HTML, JS, ... bestanden nakijken op uw server. Ook kan het virus het **.htaccess** bestand, **hosts** bestanden gewijzigd hebben en **images.php** bestanden aanmaken in de folder **images**. Het virus kan mogelijks ook via uw themes en templates uw CMS infecteren. Dit is geen wijdverspreide server infectie daar het enkel servers uitbuit waar het de paswoorden van kent.

Op de server:

Controleer op het volgende in de bestanden op uw server: **<iframe .... style="visibility: hidden;"></iframe>** Een hulpmiddel om alle iframe code te lokaliseren en tijd kan besparen is TextCrawler. Eens u al deze iframe tags hebt verwijderd, neem de volgende maatregelen:

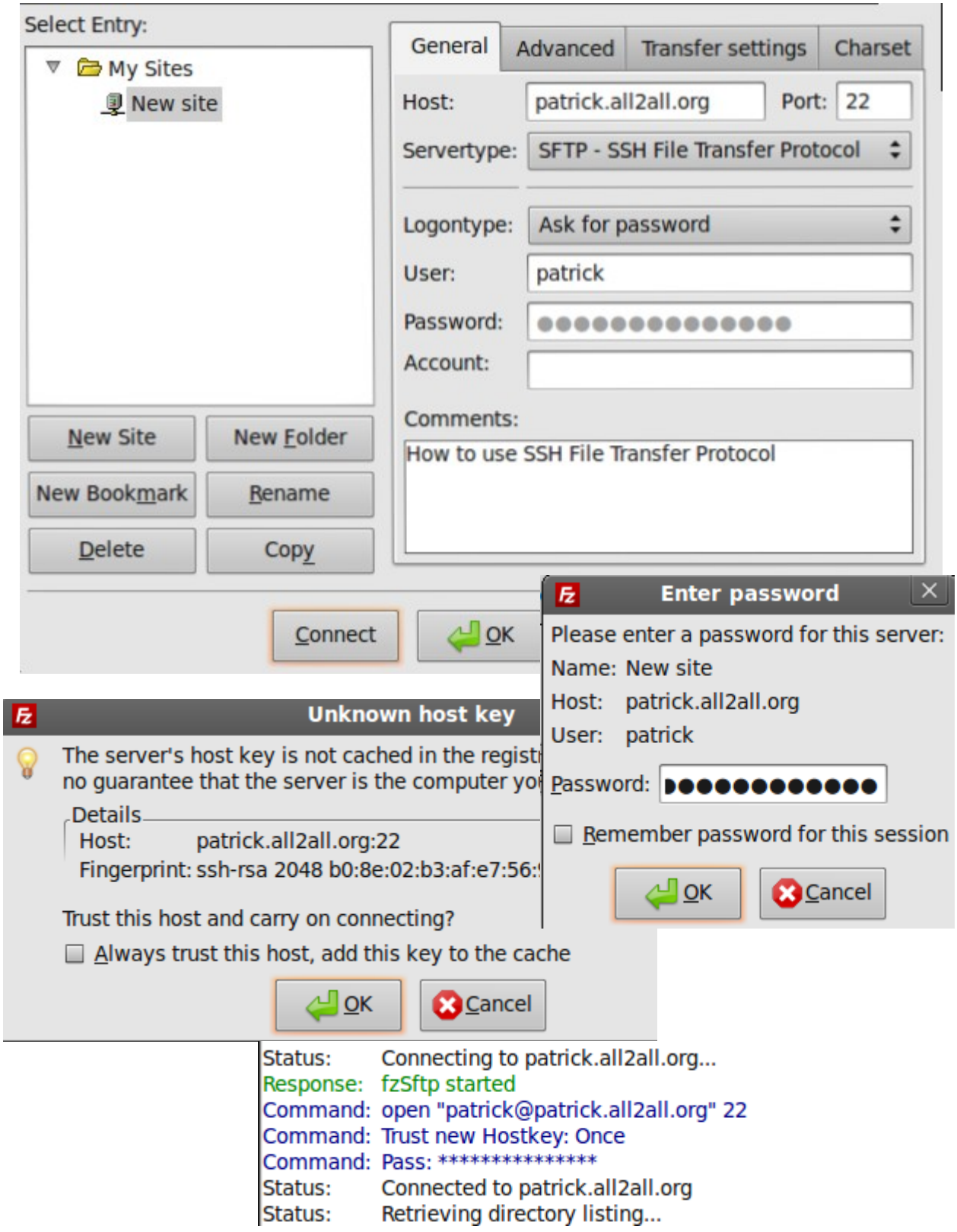
- ledig de cache van uw CMS (clear cache: Drupal – Joomla! – SPIP – WordPress)
- uw website infecteert momenteel andere pc's dus blokkeer tijdelijk de toegang tot uw website door een index.htm te uploaden waarin u uitlegt waarom de server down is.
- verwijder geen bestanden op uw server maar vervang de geïnfecteerde bestanden met de bestanden van uw laatste backup die virus vrij is. Indien dit niet mogelijk is download dan de geïnfecteerde bestanden PHP, HTML, JS, enz. naar een locatie onder quarantaine om ze schoon te maken.
- controleer opnieuw of er geen verschijningen meer zijn van malafide iframe containers op de server. (<iframe .... style="visibility: hidden;"></iframe>)
- ledig nogmaals de cache van uw CMS
- blijf zeker de eerste dagen de situatie op de voet volgen door op regelmatige tijdstippen uw bestanden te controleren.
- zorg ervoor dat u altijd een **virus vrije back up** heeft van uw site!

Op de PC:
(nota: Linux PCs zijn niet kwetsbaar voor dit virus)

- installeer een goed en **up to date** antivirusprogramma / internet security suite op uw pc en doe een volledige scan.(Voor WordPress installeer ook het antivirus plugin)
- na een volledige schoonmaak, **verander uw FTP paswoord(en)**. Gebruik een veilig paswoord!
- update Adobe Acrobat Reader en Shockwave
- verander alle paswoorden die u sinds de infectie mogelijks gebruikt heeft.
- deinstalleer nu uw FTP-programma samen met alle register sleutels. U kan dit doen met het gratis programma Revo Uninstaller. Installeer FileZilla (wordt aanbevolen).
- tracht alternatieve software zoals FileZilla als FTP client en Mozilla Firefox als uw browser te gebruiken (Internet Explorer is erg kwetsbaar). Zorg ervoor dat uw besturingssysteem en software over de laatste updates beschikt!
- sla géén paswoorden op, probeer ze te memoriseren.

Opgelet! Het virus kan mogelijks het netwerkverkeer afluisteren op andere computers in het netwerk (packet sniffing) om FTP paswoorden te onderscheppen! U kan dus één pc clean hebben als een andere pc in hetzelfde netwerk segment geïnfecteerd is, kan deze opnieuw de paswoorden onderscheppen die ingetypt worden via de cleane PC!
Let ook op met FTP paswoorden die u opgeslaan heeft. Dit virus is mogelijks in staat deze te achterhalen! In dit licht strikt het tot de aanbeveling SSH over FTP te gebruiken.
Bron: http://soyouwillfindit.blogspot.com/2009/08/virus-steals-ftp-passwords-and-insert.html

Configureren FileZilla met FTP over SSH



Versions

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

page	**Modifications**