

Virus Iframe Illiframe infecting websites

I have been badly infected by those trojan / viruses. They show up under couple of different names. (Ifram, Iframe-JS, Iframe-Tri, Illiframe...etc)

I have been searching on the web for a while until I could really get rid of these infections. It's why I make here a small pdf file that might give you informations on how to remove them completely.

These trojans have infected all my websites I'm administrating. So, it actually infected my computer at first and then scanned all my ftp accounts and mofified the the files named Index, home or news.

Also the member_news.php or such variant files would be infected.

It basically insert script lines in your source codes and replace the original files directly on your ftp account. Also htaccess files would be infected and another file would be added (something like .heder, same type as .htaccess). Sorry, I don't remember the exact name by heart, as I removed all of them both in my computer and in my ftp accounts.

Not all antivirus softwares or anti-spywares would detect it.

Here is the best solution I've found :

Install Avast home edition (free)

Make full scan of your machine.

I've used both Avast and Malwarebytes (Shareware). Both together seem to be very strong.

If I scan my computer with Malwarebytes, it would make Avast detecting more threats that actually Malwarebytes or Avast alone wouldn't detect.

But for the first time, free version of Avast should work fine to clean your computer.

After you finished cleaning your machine and think you've removed all trojans, if your website is infected by Illiframe or Iframe trojan, Avast would detect it as soon as you try to display the website.

If you try to copy the infected files from your FTP to your computer, It would also alarm you about the virus.

Change your FTP password ! Or infection will happen again on the website.

Re-upload a clean version of your website. (I know it might be a hard job if you haven't well saved different versions of your website, but that's the best solution).

If you don't have a backup, you'll have to look in every Index, News, Home named files of your website and remove the Iframe added extra line. Also check the FTP for the .heder files. (Don't forget to look in subfolders too!)

Then keep running Avast on your computer, it seems to be a very powerfull tool against trojan attacks.

That's it. Hope this could help you.

Vince – www.electrynose.com