

Rebecca the Webmaster - A StopBadWare Case Study: Practical Guide for Webmasters (1 of 3)

Don't panic!!! - Rebecca the Webmaster - A StopBadWare Case Study: Practical Guide for Webmasters– descriptions of tools we used. (Part 1 of 3) - In-depth analysis of problems and issues (Part 2 of 3), - Avoiding problems in > the future (Part 3 of 3)

This is the requested follow up from “Rebecca the Webmaster - this is my story, no tears, no glory.” Here we describe the problem solving methodology, analysis, tools used, web code issues, and steps taken to avoid problems in the future. The “we” are Rebecca a newbie webmaster with the guidance of El Jart, also we made sure that although Jart started with his “geek” tools (which I could not even understand the names of), we made sure anything we used was available to all and “free” – no commercials. Remember if I can learn to do this anyone can.

Introduction

First of all let us stress the obvious; regular checks of the tools available to virtually all webmasters are the way to avoid being flagged by Google in the first place, see how to avoid problems below. However, remember even the best web sites get hacked or compromised, for example AOL or MSN, so the most important advice from The Hitchhiker’s Guide to the Galaxy “Don’t Panic!!!”

The Tools

Just a word of caution, the tools below worked for us, however do get the help of your web host and only do this work if you have a PC with a really good anti-virus, anti-spyware etc. The stuff you are trying to clean up can bite; also make sure your PC is clean in the first place!

1. Server access – I know it sounds obvious but to start with as the site webmaster I realized I did not have full access or know what tools were available. So check this first, if you use CPanel or similar many of the tools to clean up and check are there e.g. <http://www.cpanel.net/docs/cpanel/>

2. Firefox and add ons – As the webmaster you have to be able to look at the site and check what is called. What we mean by this is the “scripts”; for example you may use a simple Ad or banner, what is actually called by your web site, e.g. the “inline scripts”;, “cookies”; etc. Just a note for end users if you surf with Firefox and these add ons <https://addons.mozilla.org/en-US/firefox/browse/type:1> your surfing is a lot safer, it is then up to you if you want to accept scripts, cookies or other downloads.
 - a. Firefox – ensure latest version (set for no-popups and cookies to manually accept)
 - b. Google toolbar (add on) – this helps to search the web for any terms or third party web addresses, but for me if you search “define:sql injection”; you can get any description to help you or use “site:anywebsite.com”; “inurl:anywebsite.com”; “cache:anywebsite.com”; you see a lot more about any web site, including your own.
 - c. McAfee Site Advisor (add on)– Just to check out any web address you come across, especially on any spam or script.
 - d. No-Script (add on) – this is great because when used you can look at a web sites but any script on the web site is disabled.
 - e. PhProxy (add on) – Using this you can go to any website without using your real IP address, however this is for the first safe look, you have to switch this off when you look at “inline scripts”;

- f. Edit Cookies (add on) – Now you can see any cookies, before you accept them
- g. DOM Inspector (add on) – Lets you inspect a web window and its contents.
- h. Safe cache (add on) – Prevents any cache based privacy attacks.
- i. Key scrambler (add on) – This encrypts any passwords you type on your PC for websites; just in case there are keyloggers in action.
- j. Web developer (add on) – This lets you check the actual scripts called, in other words not what you think is on your website, but what the user actually gets.

3. Notepad ++ - This is an Open Source text editor, using this you can capture or download text, HTML, scripts, server log files, SQL, and save for later examination.

4. SmartFTP – There are several around this is the one we used, simply because you can use it in a secure mode and set / reset file permissions, so you help being attacked again.

5. Windiff – A free utility so you can compare directories that you FTP as a backup from your website to your PC and even individual files.

6. On the server (assumes PHP & MySQL);

a. Server Log files – just use your secure FTP to download and check in your text editor

b. PHPmyAdmin – now this is daunting at first but a bit of reading http://www.phpmyadmin.net/home_page/docs.php soon help to master this, in our case this was vital to down load and backup the website databases. This is where we found most of the problems that could have re-infected / re-hijacked us.

c. PhpBB – forum tools <http://www.phpbb.com/community/> lots of help here.

7. Common sense – Maybe the most important webmaster tool as Jart kept on stressing, what should be within the website; its scripts, files, on the forums, within the SQL databases, etc. If you see a call to some website you do not recognize check it out. If some script is calling to download a special multi-media application, is it the real one? If some website / bot is coming to your site (on the server log files) every 10 seconds, why is it coming? What is its purpose or even more important what is calling it? Simple really.