Malware Infection, Hacked Sites, Phishing, Spamming and...

Author:
Quadra Hosting

Created On: 30 Apr 2007 04:40 AM

Malware Infection, Hacked Sites, Phishing, Spamming

If your web site has been infected or hacked with malware, phishing or sending out spam, please read this article. Â

How to Clean Up Your SiteÂ AFTERÂ an Infection

Since you can never be sure that you have identified all the files that the hackers may have uploaded into your account, the only proper way to clean up is to re-upload all the files to a separate, clean directory, and then merge the media files that might have been uploaded through your web site.

The goal here is to clean things up and ensure that future repeat infections will not occur. Failing to follow the prescribed procedure below may result in future repeating malware infections.

For specific Joomla recovery / clean up steps, please see:Â
https://docs.joomla.org/Security_Checklist_7

The key to a proper clean up is that you must upload your clean site to a new directory as explained below.

» Take a backup of your current site and database.
» RenameÂ mysite.comÂ toÂ mysite.com-hackedÂ
» Create a new directory mysite.com on the same level as mysite.com-hackedÂ Â
» Obtain the clean / latest version of your site files (eg. Wordpress, Joomla, Magento, etc) from the source (e.g. www.wordpress.org for Wordpress) and upload them to this new subdirectory.
» Copy the media files from your mysite.com-hacked to mysite.com into the appropriate directories
» Check and verify that all your images / media files do not contain malware. Malware can disguise themselves as an innocent looking .jpg or .gif file. There should not be any php files inside your image directory.
» You can copy your configuration file (for Joomla it's configuration.php, for Wordpress: wp-config.php) after checking its content.
» Reinstall your themes and plugins/modules and use the latest versions.
» Delete (not just disable) all unused plugins and themes. Physically delete the actual files.
» Check for possible malware inside the databases. Make sure you aren't running any plugins that allow php code execution of your data.
» Check your database for the list of administrator level user to your site.
» Change the permissions of all configuration files (e.g. wp-config.php, configuration.php, etc.) to 600. Any php files that aren't directly accessed from the browser such as config files, should have chmod 600. This prevents anyone but you and your web sites to read it.
» Last but not least, do not have any directory permission set to 777. It is not necessary to have it set to 777 when you're running PHP under FastCGI (the recommended mode). phpinfo() will tell you

which mode you're running under. It's either FastCGI or Apache Module. You can change this in the control panel -> Web Options.

» As long as you have a vulnerability on your site, moving it to another server will not stop your site from being hacked.

What NOT to Do

» Simply deleting the files that have been identified as malware. Yes they do need to be deleted but deleting them alone doesn't stop any further hacks.

» Trying to figure out exactly how the malware got in. Most of the time the malware got injected via a vulnerability within Wordpress/Joomla or one of the plugins and their entry is untraceable. To implement a system to trace every single possible entry point for malware would be impractical if not impossible, considering that 100% malware detection itself is impossible. Doing the above steps under "How to Clean Up Your Site AFTER an Infection" would ensure that you've secured all possible entry points. Once you've got a malware injection, however they got in, your entire account will become suspect. For example, even if you can manage to figure out that their entry point is FTP, or a vulnerable script X for, simply closing that vulnerability AFTER a breach would be a fatal mistake because the malware would have opened other entry points that you will not be aware of.

» Reuploading your clean site over your existing site on the server. You must rename the existing directory on the server, and create a new empty directory prior to uploading your files. You only need to rename the domain directory e.g. mysite.com -> mysite.com-hacked and not every single one inside it. Renaming and creating a blank directory ensures a proper clean slate for your site.

Restoration from Backup

As an alternative to performing a complete reinstallation of your sites, Quadra Hosting can perform a restore of your site and database to a point in time before the hacking occurred.Â However, this is not a guarantee since there's no way to be certain that a malware has not already been uploaded. Therefore this method is not our recommended remedy.Â Our backups only go back to a month or two at most. Once this is done, you must immediately install the patches / upgrade all the applications, plugins and themes on your site to prevent a repeat attack.

Wordpress Malware Cleaning Service

If you would like assistance in cleaning up your site from malware infection, we can help. Quadra Hosting's security team can perform malware cleanupÂ on Wordpress based sites only. For more information see:Â http://www.quadrahosting.com.au/support/malware-cleaning.html

What to do to secure your siteÂ BEFOREÂ it is infected

» Keep your application (Wordpress/Joomla/Drupal/Magento, etc) up to date. Do a weekly check.

» Vulnerabilities may exist in the core application (e.g. wordpress, joomla) or in the themes, plugins / addons / modules that are either active or inactive.

» Static HTML pages are impossible to hack and you can publish your site once and never ever had to "patch" them unless of course you need to actually change the contents.

» Consider using a commercial CMS that isn't open source. They are not completely secure either, but at least they are far less targeted and their vulnerabilities are less well known. If you must use Joomla / Wordpress / any dynamic web application, keep on reading.

» Completely uninstall and delete any unused plugins / modules / addons / files from the server. Do not just deactivate them.
» Make sure that all the third party stuff are up to date too.
» Do not use "admin" as the login name for your site.
» Use complex passwords with a combination of upper and lower case as well as numbers. Don't use consecutive numbers like "123" or simple dictionary words or part of your domain name. There are automated robots out there that will continually try to guess your passwords. Don't make it easy for them.
» Ensure that you have complex passwords for:
»

» Your website backend admin areaÂ
» Control panel
» FTP
» FTP sub-accounts (aka sub-ftp accounts)
» Database users (MySQL, PostgreSQL, MSSQL)
» Email accounts

» Do NOT use the same password for your FTP and Joomla/Wordpress.
» When you have multiple web sites in one account, ALL the web sites must be secured. Your sites / account is as secure as the weakest / least secure site. If you have 5 web sites in the same account for example, and you have been diligently keeping 4 of them up to date but neglected to update 1, the hackers can still get in and hack into ALL the 5 web sites that you have.
» Make sure that your PHP runs in FastCGI. You can check this using a phpinfo() page.
» Change the permissions of all configuration files (e.g. wp-config.php, configuration.php, etc.) to 600. Any php files that aren't directly accessed from the browser such as config files, should have chmod 600. This prevents anyone but you and your web sites to read it.
» Do not have any directory permission set to 777. It is not necessary to have it set to 777 when you're running PHP under FastCGI (the recommended mode). phpinfo() will tell you which mode you're running under. It's either FastCGI or Apache Module. You can change this in the control panel -> Web Options.
» Do not leave the "old version" of your site on the server. Having your old site in www.domain.com/old_site, or oldsite.domain.com or anything like that is a very bad idea. Old sites get neglected and forgotten and it becomes an easy target since nobody would keep it patched.

Background

How can my website get hacked?

A web site can get hacked through one of these methods:
» If your site has never been hacked before, the first time they got in would be through a known vulnerability in your application (wordpress/joomla/etc). After this, they can upload all sorts of backdoors to your site, it doesn't matter if you then update / patch your application later on, they'll be able to get back in through the backdoors that they've created initially.
» If there is justÂ oneÂ backdoor / malware in any of your web sites / subdomains that got left behind, the hackers can get back in even though you may have cleaned "everything" up.

» Brute force attempts to login to your web site back-end/administration area (such as wp-login or joomla's /administrator). This is why you shouldn't use "admin" as the login name and never use simple passwords.
» FTP Password brute force - hackers can attempt to guess your password if they are easy / english words. It is important to use non dictionary words and some non-consecutive numbers as well as a combination of upper and lower case.
» FTP Password discovery through spyware / malware that exists on your computer. These malware will steal your passwords from your computer and send it to the hackers. They can then use that information to go into your web site and upload malicious files.
» The server itself might have gotten hacked. This is the worst type of hacking because once they gained super user / administrator level access, they can do a lotÂ of damage. This article will discuss the first three types mentioned above, as this is related to you and what you can do to avoid being hacked.

What is a Vulnerability?

A vulnerability is a side effect, flaw or weakness that exists on an existing piece of software or web application, such as Wordpress, Joomla, Magento, ckeditor, etc. This flaw / weakness can be exploited by hackers. When a vulnerability is discovered, usually the application developers will be notified so that they have a chance to issue a patch to close the vulnerability and then announce this patch to their users. The legitimate users, upon learning that a patch is available, should update and patch their applications as soon as possible, in order to keep their web site from being hacked. After a period of time, the details of the vulnerability gets publicly revealed. At this point any hackers will be able to learn and use the knowledge to exploit the vulnerabilities.Â

Usually the hackers would exploit vulnerabilities by uploading files / scripts that will then allow them to use your account more easily to do what they want to do. These files / scripts that they upload are called malware, since they are not part of your web site and they are used to perform malicious tasks, such as sending spam, or adding unwanted pages to your web site to their benefit.

It is therefore extremely important for you to keep your web applications up to date at all time. The best policy would be to keep checking for updates every week or every day. This can sometimes be automated, depending on the web application itself. Beware that updates can sometimes break a perfectly working site, so before doing an update, backups should be taken to ensure an easy roll back.

How can I be a Target?

You may be running a third party application / scripts such as Joomla, Wordpress, osCommerce, vBulletin, etc., hackers can easily find out what product you are running and then look into what specific vulnerabilities exist in the product and then exploit those vulnerabilities.

Most of the time these vulnerabilities are fixed by the developer as soon as they are made aware of it, and often before they became widely known. However it does rely on the fact that you as the site owner make the effort of upgrading your product code to the latest version and keeping up with the security patches as they are issued.

This is one of the biggest problems that hackers abuse though because they know that people tend to install/build their sites and once it runs fine they don't touch it again. Â It's in our human nature to not fix it if it isn't broken and we worry about the potential of the site being broken should we upgrade, hackers are very aware of this.

Why are They Hacking My Web Site?

Most of the time, hackers don't have any personal agenda against you or your web site in

particular. They simply scan the internet using google searches for anyÂ web sites that may be vulnerable, or even simply known to run popular applications such as Wordpress or Joomla. Once they've found one, they would attempt to hack the vulnerable site. If your site has a vulnerability, they will be successful. If it's not vulnerable, they'd move on just as quickly. They don't care a bit. The purpose of the hack varies, from:

» Simply wanting to deface and gloat / boast to their friends, to prove that they can
» Upload scripts to your site that enables them to send spam out from your site to their victims

» Upload scripts to your site that they can use to perform Denial of Service attacks (these are often called zombies or bots)
» Upload scripts to your site that they can use to infect other web sites, thus making their job easier and easier
» Upload scripts to your site to infect your web site visitorsÂ

In some rare cases, they will also see if they can steal your data / customers list, but most of the time, this isn't their intention. It's too much of a targeted thing and they would not bother, unless of course if you are a bank or a high profiled online shop. Once again it is rare that they would specifically choose you as a victim. The only thing they are looking for is a vulnerable site and if yours happen to be one, they'd hack your site. Nothing personal!

Spyware / Malware on Your Computer

There is a small possibility that the malware came from your computer whether directly or indirectly. Scan your computer with an anti virus / anti malware program. If it discovered traces of a virus or malware, please contact a professional who is experienced in virus / malware clean up.

Do not rely on your anti virus / anti malware to properly clean the infection on your computer!

Beware of the Backdoors!

Once a hacker managed to hack into your web site, they would typically set up a backdoor that will give them easy access in the future. Once a backdoor exists, they can continue to gain access to your account even after the original vulnerabilities have been patched.Â

What does a backdoor look like?

Some backdoors may be very easy to spot, but some others camouflage themselves so well, it is very hard to spot them. They may use innocently named files, such as footer.php, data.php or whatever they may fancy. Unless you know every single file in your site and know what they are for, and actually verify the checksums of those files, you can very easily miss these backdoors, thinking that they are legitimate files.

A vulnerability or a backdoor in any one of the web sites inside your account will give the hacker the same level of access that you as the account owner have. They can see all the files that you can see, and consequently they can write, infect, delete, overwrite, upload any file, create a new directory, edit existing files, etc just as you can.

Since most modern applications nowadays allow for third party plugins/modules/add-ons and themes to be installed, vulnerabilities may not only exist within the main application core, but also in one of the installed third party plugins or themes.

The only sure fire way to remove all backdoors is akin to reformatting: delete everythingÂ (i.e. all your web sites on the server) and upload a clean fresh directory for your entire site instead of uploading into the existing site / directory. If you have multiple web sites / subdomains

in one account, this must be done onÂ allÂ of them at the same time.

Quadra Hosting's Malware Scanner

Quadra Hosting has developed its own malware scanner tool to detect common malware patterns. While 100% detection is impossible to achieve, our malware scanner can at least eliminate most of the common exploits / backdoors. However, 100% eradication of the backdoors isÂ absolutely required. The easiestÂ way to achieve 100% clean up is by re-uploading a fresh copy of your site into a separate directory.Â

Our malware scanner can find the malware that hackers had uploaded, however, the main reason why they were able to upload them, is because there is a vulnerability in your own web site. Our malware scanner does not patch this vulnerability as it is actually a legitimate part of your web site. You need to patch this vulnerability in order to stop future hacks.

Caveat

Beware that hackers most often upload their backdoors in the media file directories, so really they need to be scrutinised with a fine tooth comb. If you know that all the media files are only image files, it might be easier as you can delete anything that don't end with "jpg" or "gif" or "png". However, hackers have also uploaded their backdoors with these extensions and disguise them. You must verify that all the image files are indeed images, and not some php or perl scripts.