Sandeep Verma

January 30, 2011

admin

How to clean malware from website?

Malware, short for malicious software, is a software designed to secretly access a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

You have seen above warning many times when you want to browse website using web browsers. This is the warning from search engine bots like Google for website is affected from malwares or viruses. If you still want to access website, it can affect your system or system resources.

Most of times websites are hacked or unauthorized accessed from hackers or cross-site scripting (XSS) or cross-site request forgeries (CSRF).

There may be lot of "holes" in website security that invite hackers to play their game.

The possible HOLES may be:
1. File/Folder permissions
2. Poor authentication for application
3. Cross-Site Scripting
4. Cross-Site Request Forgeries
5. Anti-Virus Software
6. File formats
7. Network "Firewalls/Filters"
8. Shell access & Logs

Please check some link to make web application secure and safe
* http://advosys.ca/papers/web/61-web-security.html
* http://www.claymania.com/safe-hex.html
* http://shiflett.org/articles/foiling-cross-site-attacks

* http://www.ehow.com/how_6804695_remove-malware-website.html
*http://smackdown.blogsblogsblogs.com/2008/06/24/how-to-completely-clean-your-hacked-wordpress-installation/

You can review online **Virus & Threat Scanner** for cleaning malwares & viruses. These softwares are designed to run on your web server and scan your public web files for malicious code.

Google Safe Browsing Tool
http://www.google.com/safebrowsing/diagnostic?site=yoursite.com

Norton Safe Web
http://safeweb.norton.com/

You can search for more tools like...
"**Security Pro** | **SiteMonitor** | **IP trap** | **htaccess** | **AntiXSS** | **Check Permissions** | **KISS FileSafe**"

If you are running PHP website under Apache & MySQL, make sure file and folder should not be

Printed with jolliprint

How to clean malware from website?

access public. You have to check PHP function's security for more secure access.

PHP Functions may be used in hacking:
1. file_get_contents()
2. base64_decode()
3. eval()
4. exec()
5. preg_match()
6. gzuncompress()
7. urldecode()
8. error_reporting()
9. shell_exec()
10. setcookie()
11. chmod()
12. is_writable()
13. move_uploaded_file() and copy()

The above functions can be used by hackers to write malicious code to your files. The malicious code executed using eval() that will execute every run of website. So, disable eval(), file_put_contents(), file_get_contents(), exec() etc. You can check safe_mode in php.ini for disabling shell access

Most of the time websites are hacked using file_get_contents(), **eval(base64_decode())**, urldecode(), include() or iframes.

You can search infected file on web server "/var/www/" using below command:

```
# grep -iR 'eval(base64_decode(' /web-root
# grep -iR ' # grep -iR 'urldecode(' /web-root
# grep -iR 'file_get_contents(' /web-root
# grep -iR 'exec(' /web-root
```

As soon as infection found, you have to backup all application running on web server, now you have to remove infected files manually or using scanner. Now all up to you how you can manage your web server more securely…

I've found that luck is quite predictable. If you want more luck, take more chances. Be more active. Show up more often.

Printed with jolliprint