Incident Response - Website Cleanup

Table of Contents

About

It may happen that your website got hacked - spreads malicious files or was defaced or is suddenly blacklisted. This guide tells you the steps what you should do to get your systems up and running again and also support investigations.

Step 1 - Backup

Backup your files - with timestamps. This makes it a lot easier afterwards to find out what happened. Everything saved in the `archive` can be shared for further investigations.

```
# archive everything
tar -zcvf /PATH/TO/WEBSPACE/ARCHIVE.tar.gz /PATH/TO/WEBSPACE
```

Step 2 - Find infected

If one malicious file is found, the chance is high that more files were affected at the same time. They often hide, but it is not impossible to find them following the next few abstracts.

By Date

To find all modified files in a specific timeframe you can use `find` command. Choose a time surrounding the hacked file modified/created time.

```
# find files modified at a specific date
find . -type f -newermt 2015-02-26 ! -newermt 2015-02-27
```

By Originals

Check the files against their original counterparts. Injections are placed in random files of your webspace. In `Step 1` you have created a file with MD5s of your files. Now it is about comparison:

- Download or locate the files of the original CMS
- Change into the directory of the CMS
- Use for example `md5deep` to create md5 hashes
  - `md5deep -r -l * > ~/cms-versions/<cmsname>-<version>.md5`
- Now change to your webspace directory
- Compare it with `md5sum`
  - `md5sum -c --quiet ~/cms-versions/<cmsname>-<version>.md5`

You will receive the modified files and new ones which don't match. It will be good to have a look at the modified ones and replace them with the originals if needed.

Access Logs

If you have logfiles of your webserver, have a look at them. Filter the webspace/website requests and have a look at the time when the hacked file(s) were first detected.

What is of interest there: POST requests to your website, or specific files on your webspace can give you a hint where executable code is hidden.

Step 3 - Clean

There are at least 3 approaches to finally clean successfully a webspace.

Total Zen: This is most likely the hardest step, but possibly the most effective. Start from scratch, wipe the whole webspace directory and copy over only:

- Install a new CMS (use the most current version)
- Add additional files required to run your website (e.g. images, css styles, javascripts)
- Only install needed Plugins

Classic Cleanup: This approach makes use of the information you gathered before. Delete or replace all files that you encountered as malicious previously. If the file was injected with malware, and it is needed by the CMS you use, replace it with its original.

Backup: Simple and fast, yet effective. Restore your webspace with a backup you know that it is clean.

!!! Be warned for the last 2 approaches: The cause of the hack is probably not fixed with the removal of malicious files. To get a little on the secure side try at least the following:

- If possibly update your CMS
- Also consider plugins and themes
- Remove plugins and themes you don't use (anymore)
- Update your server infrastructure if possible
  - Database
  - PHP, Java, ...
  - Webserver (Apache, nginx, ...)
- Change passwords for FTP, DB, CMS-Logins

Step 4 - Monitor

When your website is clean again, keep an eye on it for the next few days to a week. You will maybe want to watch the request/access logs. Especially

- POST requests to your website
- File count
- Modified files

Revision #3
Created 4 August 2021 09:07:05 by Patrick Wall
Updated 7 June 2023 09:40:44 by Lena