My site was hacked, why must it be deleted?

2024/05/03 08:57:56

FAQ Article Print

Category:	Abuse Issues	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	en	**Last update:**	14:29:04 - 2015/01/26

Keywords

abuse compromised

Symptom (public)

Problem (public)

You received a notice that your site was hacked and you do not agree with the requirement for the site to be deleted and recreated or a clean copy re-uploaded.

Solution (public)

This is correct and this is the policy of our independent abuse team.

Many hackers do not only modify one or two files, and they certainly do not make ALL their changes easy to detect.

When they compromise sites, they leave noticeable pieces which trick people into thinking it can be "cleaned". The other portions of the hack or compromisation can be stored in the database, deeply embedded in other files (including images) and encrypted with combinations of rot13, base64, gzip and randomization techniques. This makes it almost impossible to "clean" a site. And no ... you cannot use the "last modified" date of files as this can very easily be changed, even in PHP (ref: http://php.net/manual/en/function.touch.php).

Furthermore, if a cPanel site has been compromised the hacker had access to ALL email stored for that site and the encrypted passwords of all email accounts, directory protections, the database username and password (stored in the CMS software configuration file) and any other sensitive information in the account.

The hacker also would of had access to ALL email stored in the account at that time and a very popular activity is to run a PHP script to scan over this email and divulge anything containing the words "password" , "pin" or similar keywords.

The abuse departments focus is system security. The policy for any compromised site or account is thus deletion and removal.

Should you have been a victim of an attack, your account can be backed up. You are not permitted to upload this "dirty" copy of the site and you will need to upload a previous backup of the site from when it was in a clean state. Apon doing so you will need to immediately take action to secure the site, update the site software and take reasonable steps to ensure this does not happen again.

We provide daily, weekly and monthly offsite backup services to mitigate the impact of such an event and we encourage all clients to take advantage of this.

Please refer to our [1]Abuse Department 3 step process FAQ to have service re-instated.

[1] https://servicedesk.iitsp.com/faq/7