

## Forum:[Hack Forums](#)

Thread: [My Wordpress Site Got Malware/Spam code in Every PHP File. Content Inside](#)

**n31ght0** - May 31, 2018, 6:22 pm

Please help guys my wordpress site got hacked and the attacker inject malware code in every PHP file. it seem the purpose for google ads booster.

the decode base64 is here <https://malwaredecoder.com/result/5578cf43059b45ff525742f2e525f75c>

the original file is here <https://pastebin.com/raw/RFvCDsYm>

i don't know how they do that. Any idea how to find the security hole? i was deleted all the malware in every file before but in a couple of day it back again. i need to know the security hole first before restoring my file. If anyone have experience before with the same issues like me please share guys.

**Geatzo** - May 31, 2018, 6:56 pm

Maybe google php shells?

The original file is encoded so i would never ever use a encoded file.

**newQuery** - June 1, 2018, 5:24 am

Hello, first of all, you should check if all your plugins/modules are up to date and maintained.

It seems like a user was able to upload some sort of shell, probably using a form upload somewhere on your site.

**Squito** - June 1, 2018, 5:43 am

Also make a phpinfo file and check if open\_basedir set up properly. If not, then demand your money back and get the hell out of there.

**n31ght0** - June 4, 2018, 7:15 pm

(Jun 1, 2018 05:24 AM)TheZdo Wrote: [\[CITE\]](#) Hello, first of all, you should check if all your plugins/modules are up to date and maintained.

It seems like a user was able to upload some sort of shell, probably using a form upload somewhere on your site.

(Jun 1, 2018 05:43 AM)Squito Wrote: [\[CITE\]](#) Also make a phpinfo file and check if open\_basedir set up properly. If not, then demand your money back and get the hell out of there.

Hi, is it possible to track from where the file is modified? i mean i want to know who/which inserting base64 code to every PHP file on my site

**Zher0** - June 4, 2018, 7:19 pm

Also make sure you wordpress theme is patched/safe. If you're are using any nulled plugins/themes always check them.

**darksh33p** - June 4, 2018, 8:20 pm

this very common. i would get a security company to clean ur site and then make sure you change FTP an ssh password. most of time it is FTP that gets brute especially on cpanel style services can also always do clean migration to new wp site but move your db, not php files. only thing is you need to check db to make sure no malicious stuff there either

**zxyl** - June 13, 2018, 1:03 pm

WP Protect Admin

[Download & Install it...](#)