

Have you taken the WordPress 2015 Survey yet?



WORDPRESS.ORG

Search WordPress.org



Forums

username or e

password



Log in

(forgot?)

Register

[WordPress › Support › Plugins and Hacks](#)

1 2 Next »

Wordfence Security

[closed] Virus not found in Wordfence (35 posts)



ewodrich

Member

Posted 4 weeks ago #

We've recently been dealing with several virus attacks. I encountered a virus that did not show up in the Wordfence scan, nor searching for it on Google or any other virus scans performed by myself or BlueHost.

I've since (hopefully) cleaned it up, but here's what I found. I could visually see something above my black header on <http://www.southwestballettheatre.org>, so I "inspected" the element. What came up was an inserted iframe linking to [http://c11n4.i.teaserguide.com/snitch?](http://c11n4.i.teaserguide.com/snitch?default_keyword=Southwest%20Ballet%20Theatre&referrer=http%3A%2F%2Fsouthwestballettheatre.org)

[default_keyword=Southwest%20Ballet%20Theatre&referrer=http%3A%2F%2Fsouthwestballettheatre.org](http://c11n4.i.teaserguide.com/snitch?default_keyword=Southwest%20Ballet%20Theatre&referrer=http%3A%2F%2Fsouthwestballettheatre.org)

The reference to "teaserguide.com" could be seen attempting a connection when the pages were loaded and was on all 3 of our sites theme header files. One was in a child header, the others in the main theme headers. I had just reinstalled the Divi theme on each website in the last week.

Thought you might be interested. Please let me know if you need any other info.

<https://wordpress.org/plugins/wordfence/>



ewodrich

Member

Posted 4 weeks ago #

I neglected to mention, I did have the Wordfence option checked to search theme and plugin files.



WFMattR

Member

Plugin Author

Posted 4 weeks ago #

Thanks for the report. Were you able to find code in any of the theme files before reinstalling the theme? If so, can you send a copy of the file to samples [at] wordfence.com and include a link to this post?

If not, there may still be other files outside of the theme that were causing the issue -- some hacks hide themselves using cookies, time of day, or other methods, so the links may come back again or may still be displayed to other visitors.

The Divi theme would be scanned for known malicious patterns (which are pretty extensive), since the theme's code is not available on wordpress.org for comparison to the original files.

You may want to try additional Wordfence scan options, such as high sensitivity scanning, mentioned in our guide to cleaning hacked sites, here -- this could help find any other files that would let the attacker back in, if there are any:

[Cleaning a hacked site with Wordfence](#)

Remember also to change any passwords related to the site -- sometimes hacks like this can be caused by a hosting account or FTP password being compromised.



ewodrich

Member

Posted 4 weeks ago #

Awesome - I'm grateful for the quick response. I've just emailed off the file (now called header.old) to the address you specified. I will definitely try the scan option you suggested. This being our 3rd attack in a short time, I am leary that we've gotten it all, but hopefully our comprehensive password changes will help.



WFMattR
Member
Plugin Author

Posted 3 weeks ago #

Great, thank you also for sending the file! Let us know if you have questions on anything that comes up in the scan. There can be false positives using the high sensitivity option, that you might need to investigate to see if they are actually malicious.



ewodrich
Member

Posted 3 weeks ago #

I must have not gotten to the root of the problem as it showed up again this morning. The problem was the same but the file size was different so I shot it over to your samples email.



WFMattR
Member
Plugin Author

Posted 3 weeks ago #

Sorry to hear that it hasn't been completely cleaned yet. Thanks for sending the new sample file. Let us know if you need help identifying any issues in different files with the high sensitivity option in Wordfence, too.



arsilveira
Member

Posted 3 weeks ago #

I'm facing the same problem with the site teaserguide.com. The Wordfence don't detected. I've found 12 instances of following code in header.php:

[Malware deleted]



WFMattR
Member
Plugin Author

Posted 3 weeks ago #

arsilveira: Thanks for the report -- if you can also send a copy of the header.php file to samples [at] wordfence.com, and include a link to this post, we will check it out.

It would be a good idea to follow the guide mentioned above:

[Cleaning a hacked site with Wordfence](#)

Make sure especially that all themes and plugins are up to date, and to change all passwords that are associated with the site.



rolyv
Member

Posted 3 weeks ago #

the same problem here, a week ago I deleted the script from the header.php, but last night showed again, maybe we can compare the plugin we are using? the weird is that que header.php don't even change the modification time.



ewodrich
Member

Posted 3 weeks ago #

rolyv - I noticed that with mine too, but thought the virus might have been there and not done anything for a few days. The header files in our 3 instances (we run 3 sites) were each changed but the last modified time was the same as the other files in the directory - all of which I'd recently updated. I've been going through FTP and checking file size each day to make sure it hasn't changed as a precaution. So far we've been clean for 3 days.



rolyv
Member

Posted 3 weeks ago #

I did the same... another thing is that "image.php" file appeared in the root of theme with code like a content-image.php, but I'm pretty sure don't belong there (compared with my localhost), I hope this get a solution soon!



WFMattR
Member
Plugin Author

Posted 3 weeks ago #

Can you tell me the themes and plugins you are all running, and if you are on the current version of WordPress core, or an older version? If you don't want to post the lists here, you can email me the list at: matt [at] wordfence.com

To help in cleaning your site, make sure WordPress is up to date, and that all of your plugins and themes are up to date (even inactive plugins and themes). If you have old themes or plugins that you don't plan to use again, it is best to remove them. If you didn't already do that before using the "cleaning a hacked site" link above, it would be best to go through the process again.

Our dev team also identified that there may be two related files -- if you run another Wordfence scan without finding new issues, and can find these in your folders, please also send these to samples (at) wordfence.com

```
/wp-content/languages/plugins/ajax.php  
/wp-content/languages/themes/start92.php
```

If you are on shared hosting, you may also want to check your file permissions, to make sure that other sites cannot write to your site's folders. Your hosting company

can help, if you are not sure how to do that yourself.



ewodrich

Member

Posted 3 weeks ago #

Matt, I'm so grateful you are looking into this. It's reassuring.

I've emailed you the details, but for the sake of anyone who might be following along, we have 3 websites, 2 using DIVI (child) and one using twenty-thirteen (child). Only the site using twenty-thirteen had a wp-content languages directory and I've sent the 2 files in question as requested.

Between the 3 sites we use the following plugins:

WooCommerce
Meteor Slides
Meta Slides
Wordfence
Akismet
Our Team Enhanced



WFMattR

Member

Plugin Author

Posted 3 weeks ago #

ewodrich: Thanks so much -- I will see if I can find out anything more in the meantime.

arsilveira and rolyv, if you can post (or email) your list of plugins as well, we can see if there is anything common, especially since this list is pretty small.



rolyv

Member

Posted 3 weeks ago #

Hello Matt, thank you for care about this, like ewodrich I'm using the Twenty Thirteen theme customized (v 1.5) I know there's a new version (1.6), but personalize so much the current version I'm afraid the mess it to update

The plugin are I'm using are:

Advanced Text Widget
Akismet
Categories Images
Custom fields display
Facebook Open Graph, Google+ and Twitter Card Tags
Flexible Posts Widget
NextGEN Gallery by Photocrati
NS Featured Posts
Post Types Order
WordPress Popular Posts
WordPress Related Posts
WP-PageNavi
WP-PostRatings
WP No Category Base
WP Super Cache

I did not find the languages files in question.



WFMattR

Member

Plugin Author

Posted 3 weeks ago #

rolyv: Thanks for the list of plugins. For the Twenty Thirteen theme -- there was a security fix between 1.5 and 1.6. If you haven't done this already, go to the folder /wp-content/themes/twentythirteen/genericons/ and remove the file "example.html" -- it's a sample file that is not necessary for the theme to work, and it has a flaw in it. I don't know if that was the way they got in or not.

I'd recommend looking into child themes for customization -- that will let you use the current version of twentythirteen, with your customizations in a separate folder, so that you can update the main theme when there are changes, with less chance of anything breaking. (It may take some effort to convert from your current format though.) WordPress has a good explanation here: [Child Themes](#)



rolyv

Member

Posted 3 weeks ago #

Thanks Matt!, I will check it out.



oliverrealize

Member

Posted 3 weeks ago #

I'm having the same issue. Just submitted a ticket.



nicjansma

Member

Posted 3 weeks ago #

Seeing the same issue as well.



DebraCuming

Member

Posted 2 weeks ago #

I also have this code inserted in my header.php of all themes and child themes. The only common plugin I have is Akismet. I am running 4.3 and everything is up to date.

If you do a google search for a partial match on the script tag you get back 100s of results of sites with this in the header :(



WFMattR

Member

Plugin Author

Posted 2 weeks ago #

Thanks, everyone for the additional details. Patterns have been added to Wordfence to scan for these files. If anyone has additional unusual files showing up that are not mentioned above, please let us know.

Also, for anyone who hasn't listed their plugins/themes let me know which ones you have, even if they are not active. If you don't want to post it in the forum, you can send me the list at mattR (at) wordfence.com

For fixing your header.php file, it is best to replace it with a backup copy, or click the link to have Wordfence replace it with the original (if it is a theme from wordpress.org).



DebraCuming

Member

Posted 2 weeks ago #

So, turned out all sites I was running have been infected and one of those had a really old version of WP running. Is it possible for this to have come in via that site and infected the others? They all run as sub directories under a parent.



DebraCuming

Member

Posted 2 weeks ago #

I installed WordFence on the old site and it found 3 malicious files. Do you want me to send those over or they unlikely to be related?

Critical Problems:

* File appears to be malicious: backup/wp-content/themes/neonsential/functions/required/template-bot.php

* File appears to be malicious: backup/wp-content/themes/neonsential/functions/required/template-top.php

* File appears to be malicious: backup/wp-content/themes/neonsential-reloaded/includes/prelude.php



WFMattR

Member

Plugin Author

Posted 2 weeks ago #

DebraCuming: Yes, if all of the sites are running under a single hosting account (or as the same linux user, if you're on a VPS or dedicated hosting), then the infection can easily spread among the various sites.

If the files above were found in a regular Wordfence scan without the "high sensitivity" option enabled, then we do not need copies of them. Thanks for checking! You might also want to do a thorough cleaning, using the guide that I linked to in my first post, in case anything else remains.



snthorv

Member

Posted 2 weeks ago #

I don't have this plugin but I have been having this problem. I have done all the normal things, such as making sure everything is up to date, changing passwords and so on. I still have no idea how they are actually getting into my sites. However, I did notice something that no one mentioned here, so I'll mention it now:

they were also adding a line in the .htaccess file. This line caused a redirect. The htaccess change and the change in the header seemed to work in conjunction, so that after I deleted the line, even though the 'teaserguide' bit still showed, users were not actually moved away from my site.

Also, I had one site that I had restored like 5 times that is presently uninfected, and the thing that I did this time was go through and carefully made sure that all of the permissions for every file in the WP directory and sub-directories were correct. I have a hunch that they are exploiting permissions somehow.

Anyway, I have been able to instantly repair my sites by uploading completely fresh copies of the latest WP as well as a backed up copy of .htaccess. So, even though I can't figure out how they're getting in, at least I can fix it now in about 5 mins.

I'm presently working on another site that was infected, and focusing on the permissions. If that seems to solve this site as well, I'll let ya'll know.

What was the offending .htaccess line so I can search for it? Thanks :)



DebraCuming
Member
Posted 2 weeks ago #



snthorv
Member
Posted 2 weeks ago #

It was a little different each time. Here was one:

```
RewriteRule ^oe/(.*)$r/openx-adm.php?$1 [L]
```

So you can tell from this that there was also a file added to the directory r/ with the addition of the evil script. I deleted that and used a virus scanner to check for some others. They seem to have 'salted' the site with several, with variations on the word openx and -adm.

This line was right underneath the WordPress rewrite rules in my htaccess file.



DebraCuming
Member
Posted 2 weeks ago #

Thanks!



PhilaPhans
Member
Posted 2 weeks ago #

MattR, thanks for your help with this issue.

I'm concerned about infection other than in WordPress files, will WordFence also look in the entire file structure, as well? We also run a message board off our WP site. I've also got concerns over database infection.

Thoughts?

Thanks.

Topic Closed


This topic has been closed to new replies.

About this Plugin



- Wordfence Security
- Frequently Asked Questions
- Support Threads
- Reviews

About this Topic

 [RSS feed for this topic](#)

Started 4 weeks ago
by ewodrich

Latest reply from
roncruickshank

This topic is not
resolved

WordPress version: 4.3

Tags

- [iframe](#)
- [teaserguide](#)
- [virus](#)


[About](#)
[Blog](#)
[Hosting](#)
[Jobs](#)


[Support](#)
[Developers](#)
[Get Involved](#)
[Learn](#)


[Showcase](#)
[Plugins](#)
[Themes](#)
[Ideas](#)

[WordCamp](#)
[WordPress.TV](#)
[BuddyPress](#)
[bbPress](#)

[WordPress.com](#)
[Matt](#)
[Privacy](#)
[License / GPLv2](#)

 **Follow @WordPress**

 **Like** 954k

 **+1** 108k

CODE IS POETRY