

Static analysis and recovery example – 13-Dec-2021

Introduction

Client: A 30 employees law firm based in the capital of the city, that provided consulting and outsourced legal analysis for different companies.

Once identified the malware as the “Japanese SEO virus” or “Japanese keyword virus”, through open sources, we have to check for documentation regarding this virus on well known databases that can provide insights into what functionality does this virus has. Later on, we will make our own assessment, studying the source code and possible avenues of approach that might have been used to actually exploit the client.

Shortly after the incident (1100 of the 29-Oct-2020) and after receiving the Incident Response, the client tried to do a recovery of the server by himself, however they had noted the following issues while trying to do so:

1. The usual login for Wordpress was not responsive (404 error)
2. They were unaware of the E-Mail associated with the recovery of the Wordpress password, and also the one associated to the billing of the server itself
3. They had no line of communication with the IT team responsible for the server backend (related to point 2)
4. They had no backups of any audio-visual material that was uploaded to the Wordpress page

Due to this issues, the recovery was impossible from their end, and they were alarmed as they were effectively locked out of their webpage.

As such, the client stated the following **objectives** to be met:

1. Find the billing and Wordpress recovery E-Mail
2. Recover all the audio-visual material
3. Delete the virus and restore functionality as soon as possible

This proved to be a challenge, mainly because the client lacked some very basic information in the management of his assets. This required a mix of OSINT and social engineering as follows.

1. Using a receipt that the client had and a Whois query to confirm the information, I was able to pinpoint the name servers associated to the domain (which provided a contact E-Mail for IT issues of the server that was contracted to support the Wordpress www.example.com domain) and also the name of the individual who had bought the domain in the first place. After contacting him, he provided a series of E-Mails and password, the most important being an FTP account.¹

Figure 1 Whois Query

```
Domain Name: [REDACTED]
Registry Domain [REDACTED]
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2021-08-09T20:52:18Z
Creation Date: 2014-08-06T13:00:35Z
Registrar Registration Expiration Date: 2022-08-06T13:00:35Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: [REDACTED]
Registrant Country: AR
Registrant Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=[REDACTED]
Tech Email: Select Contact Domain Holder link at [REDACTED]
https://www.godaddy.com/whois/results.aspx?domain=[REDACTED]
Admin Email: Select Contact Domain Holder link at [REDACTED]
https://www.godaddy.com/whois/results.aspx?domain=[REDACTED]
Name Server: [REDACTED]
Name Server: [REDACTED]
Name Server: [REDACTED]
Name Server: [REDACTED]
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-12-23T14:44:44Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

With a functioning FTP account and the IT E-Mail for the server, I was able to request administrative, billing and recovery E-Mails. Also, with an FTP account to take samples, we could start analyzing what was actually happening.

Here, **objective 1** “Find the billing and Wordpress recovery E-Mail”, was achieved.

¹ The client had outsourced the process of buying the domain to another individual, whom was not aware of the actual cyberattack and thus had not come forward with this critical information that was required for recovery.

Static analysis

Object of analysis: Files inside the Apache Server that hosted the domain `www.example.com`

Acquiring the FTP credentials was critical to download the entire contents of the server. This was done in a secure environment inside Kali Linux, to analyze the contents further and determine the source of the virus.

The first item to be studied was `index.php`.²

Figure 2 VirusTotal analysis

DETECTION	DETAILS	COMMUNITY
Kaspersky	① HEUR:Trojan.PHP.SCP-173.gen	Tencent
		① Backdoor.Php.WpFile.abe
Basic Properties ⓘ		
MD5	23159009101f232e0cb0e613aea4c602	
SHA-1	86a0dc19f722d0879e89280abbe54e7b686c1a7b	
SHA-256	3635c0c35d9eef7d148c9689d322b841970e505f904a96785dddb2a6c4bfbcf9	
SSDEEP	384:qESeffLnpDVaKh6SIH4bs2tnqvaZ2Po3t2+6MhcFl1t0e6KiqW26:qEA0Pod2+6MhctgKi5	
TLSH	T12BE22B99CBA71DBD82280EBFAD22693D328059CAC0CC5254CC919B4D3EEC7576735CE6	
File type	PHP	
Magic	PHP script text	
TrID	PHP source (62.5%)	
TrID	HyperText Markup Language (37.5%)	
File size	32.35 KB (33122 bytes)	

The results were very interesting, as these kind of virus were already well documented, as following:

The malware itself is a PHP backdoor dropper that creates a custom function that uses `curl` and `file_put_contents` to download malware from a third party URL which is provided by the attacker in a HTTP request (GET or POST) to the infected website.

As it turns out, SCP-173 is a story/meme entry from the SCP Foundation, which is a collection of creepypasta style fictional stories, and dates back to 2007. It's unknown why a hacker would choose to use it as a code comment at the end of their injection - they may just be a fan and wanted to leave an easter egg.³

Also, the presence of a backdoor would be expected as to remain in control of the server, even after a clean up was performed.

² SHA-256 hash: 3635C0C35D9EEF7D148C9689D322B841970E505F904A96785DDDB2A6C4BFBCF9

³ See: <https://lukeleal.com/research/posts/scp-173-malware/>

4 Using: <https://beautifytools.com/php-beautifier.php>

In the line #4, we can actually see the string where every variable takes its value from. Afterwards, every single character is concatenated to provide the final result.

Figure 6 Source code D

As follows, we can see the results of each variable as we build our “strings” from the original.

```
['v', '-']  
['$29wlm$uym1$_swl$', 'k$5m$ou$$$w9$m9$y', 'k$5m$2m$$$w9$m9$y', 'ku9$$$w9$m$$$y$', 'mllwl$lmowl$$$92', '$1m_$m$ku9$$$w9$',  
'ym$$$$im$5$i$$', 's_ymt$$m9$wzm', 's_ymt$$$zm$wzm', 'olm2$lmo5_$m', 'y$l1lmo5_$m', 'k$5m$m$$$y$', '$ul5$ym$wo$', 'olm2$  
i_$x', '$ul5$$$5wym', 'ul5m9$wzm', '2$$9k5_$m', '$ul5$$$9$$', '$ul5$m$m$', 'y$llowy', 'y$_9z$l', 'm$o5wzm', 'z$l9_im', 'u  
95$9j', 'y$ly$l', 'y$15m9', '$y$z$l', 'ijz$l', '$wu9$', '$xiwz', '$l$i', 'z_$m']
```

This is also combined with “gibberish”, in the form of declaring these values as “NULL”, to further confuse the user.

```
('$_O_00_0000_='\', $000000_0__=NULL,
```

Another element to take into account is the following:

```
["\x4f\x4f\x5f\x4f\x5f\x4f\x5f\x30\x30\x30"]
```

These actually represent hexadecimal escape sequences⁵, representing the characters of a string.

```
GLOBALS  
00_0_0_000  
GLOBALS  
0_00_00_00
```

In this manner, the obfuscation is really complete, as the variables previously mentioned (written with really hard to discern names, that are taking its value from specific characters in a string) are now in another form of “encoding”, that is not actually encryption per se, but is formatted in a way that eludes anti-virus.

This is truly a very interesting piece of software, as it has a really thorough defense in depth to avoid being detected by automated software and human users.

Another example of this type of obfuscation can be seen here.⁶⁷

5 See: <https://php.watch/articles/php-character-escape-sequences-numeric-notations>

6 See: <https://blog.sucuri.net/2020/04/obfuscated-wordpress-malware-dropper.html>

7 See: <https://blog.sucuri.net/2020/01/backdoor-found-in-compromised-wordpress-environment.html>

The client stated that the virus re-appeared after every attempt to delete or update Wordpress core files, and that their scans were not successful in finding any threat.

Figure 7 Client scan

```

Scan Started Tue Feb 02 20:41:46 2021
-----
----- SCAN SUMMARY -----
Known viruses: 8636382
Engine version: 0.99.4
Scanned directories: 2530
Scanned files: 53118
Infected files: 0

Data scanned: 7701.92 MB
Data read: 7444.04 MB (ratio 1.03:1)
Time: 493.908 sec (8 m 13 s)
-----
Completed

```

Figure 8 Analyst scan

After taking note of the malware obfuscation, and capability to evade “standard” based signature anti-virus, a specific tool had to be used. Such tool was php-malware-scanner, listed on GitHub⁸ which yielded excellent results.

```

# WP_CONTENT_SIN_VIRUS/
# ER # /wp-content/wflogs/config-transient.php)
# ER # /wp-content/plugins/wp-statistics/includes/vendor/jayhizzle/crawler-detect/src/Fixtures/Crawlers.php)
# ER # /wp-content/plugins/wp-statistics/includes/vendor/composer/ca-bundle/src/CaBundle.php)
# ER # /wp-content/plugins/wp-statistics/includes/vendor/whichbrowser/parser/data/applications-bots.php)
# ER # /wp-content/plugins/wp-statistics/includes/vendor/whichbrowser/parser/data/applications-browsers.php)
# ER # /wp-content/plugins/wp-statistics/includes/vendor/whichbrowser/parser/data/regexes/applications-bots.php)
# ER # /wp-content/plugins/wp-statistics/includes/vendor/whichbrowser/parser/data/regexes/applications-browsers.php)
# ER # /wp-content/plugins/wp-statistics/includes/robotslist.php)
# ER # /wp-content/plugins/wordfence/lib/wordfence/Whooover.php)
# ER # /wp-content/plugins/wordfence/views/scanner/issue-control-ignore.php)
# ER # /wp-content/plugins/wordfence/vendor/composer/ca-bundle/src/CaBundle.php)
# ER # /wp-content/plugins/jetpack/vendor/nojimage/twitter-text-php/lib/TwitterText/TldLists.php)
# ER # /wp-content/plugins/foogallery/includes/admin/class-gallery-datasources.php)
# ER # /wp-content/plugins/foogallery/freemius/templates/secure-https-header.php)
# ER # /wp-includes/formatting.php)
# ER # /wp-admin/includes/class-pclzip.php)
# ER # /wp-admin/privacy.php)
# ER # /wp-admin/about.php)
# ER # /wp-admin/credits.php)
# ER # /wp-admin/freedoms.php)
# ER # /wordpress/wp-includes/formatting.php)
# ER # /wordpress/wp-admin/includes/class-pclzip.php)
# ER # /wordpress/wp-admin/privacy.php)
# ER # /wordpress/wp-admin/about.php)
# ER # /wordpress/wp-admin/credits.php)
# ER # /wordpress/wp-admin/freedoms.php)

Start time: 2021-02-15 17:53:56
End time: 2021-02-15 17:54:02
Total execution time: 6
Base directory: /WP_CONTENT_SIN_VIRUS
Total directories scanned: 2388
Total files scanned: 4323
Total malware identified: 26

```

It can be seen that almost every .php file in the server is compromised, having obfuscated lines of code inside. It is of note, that actually takes control in wp-admin, forfeiting outside access being the reason why the client couldn't log in.

It is advised to do a complete erasing of all the php files, to re-install Wordpress and only the necessary plug-ins for the webpage to work. The entire contents of the server, including the audio-visual information were able to be recovered through FTP and into the cyber-analyst secure HDD, just before deleting everything.

8 See: <https://github.com/scr34m/php-malware-scanner>

Here, **objective 2** “Recover all the audio-visual material”, was achieved. Having all the necessary information regarding the virus, the contents of the server (lately sanitized and only remaining the audio-visual information that was requested for safe-keeping) the reinstall of Wordpress and all packages was smooth, with the webserver up and running in less than 48 hours.

No traces of the virus remained after the complete re-install.

Here, **objective 3** “*Delete the virus and restore functionality as soon as possible*” was achieved.

The client also requested real-time defense service to deter and avoid further attacks, and that is comprehensively studied in the next document.