JASK

THREAT ADVISORY

CMS exploitation frameworks driving botnet creation

AUTHOR
ROD SOTO

JASKLABS
TA-0009

TLP
WHITE

RISK FACTOR
HIGH

THREAT ADVISORY

CMS exploitation frameworks driving botnet creation

AUTHOR
ROD SOTO

JASKLABS
TA-0009

TLP
WHITE

RISK FACTOR

HIGH

Overview

The proliferation of Content Management System (CMS) frameworks has provided many end users and companies with the ability to create, collaborate and publish content in an effective, simple and straightforward manner. These frameworks also have "plugins" that can connect to any other application that can interact, manage or push content. CMS frameworks allow many companies to have a "front store" without having to develop or build their own technology. And many of them are already hosted by cloud providers, making them easier to be deployed in a matter of minutes.

These frameworks are also based on the LAMP software bundle. A large portion of the internet runs on the LAMP model and its variations like LEMP and MEAN. All these software bundle frameworks represent an operating system, a web server, a backend database and a web/scripting language code.

There are several popular CMS frameworks which are calculated in the millions. Below is a graphic that shows the approximate population and ranking of such frameworks.

Figure 1. Shows most popular CMS frameworks *

#	WEBSITES USING	MARKET SHARE %	ACTIVE SITES	# OF WEBSITES IN MILLION
1	WordPress	59.9 %	26,701,222	239,139
2	Joomla	6.6 %	2,009,717	13,480
3	Drupal	4.6 %	964,820	23,330
4	Magento	2.4 %	372,915	12,095
5	Blogger	1.9 %	758,571	15,779
6	Shopify	1.8 %	605,506	11,587
7	Bitrix	1.5 %	200,210	3,925
8	TYPO3	1.5 %	582,629	3,568
9	Squarespace	1.5 %	1,390,307	9,799
10	PrestaShop	1.3 %	262,342	2,099

As seen above, the popularity of these frameworks means they influence a large part of the internet - and more importantly, these sites receive and interact with a lot of traffic, many of them storing personal and sensitive information, as well as financial transactions.

Indicators

Logically, the proliferation of these frameworks presents malicious actors with numerous targets of opportunity that can subsequently be used for botnet creation and monetization. It is really not difficult to find these frameworks, as many vulnerability scanners, either commercial or open source, are available on the internet. Or malicious actors can simply use a vulnerability search engine such as Shodan.io. The following figure shows the results of a simple search on Shodan.io using the keyword "wordpress."

AUTHOR
ROD SOTO

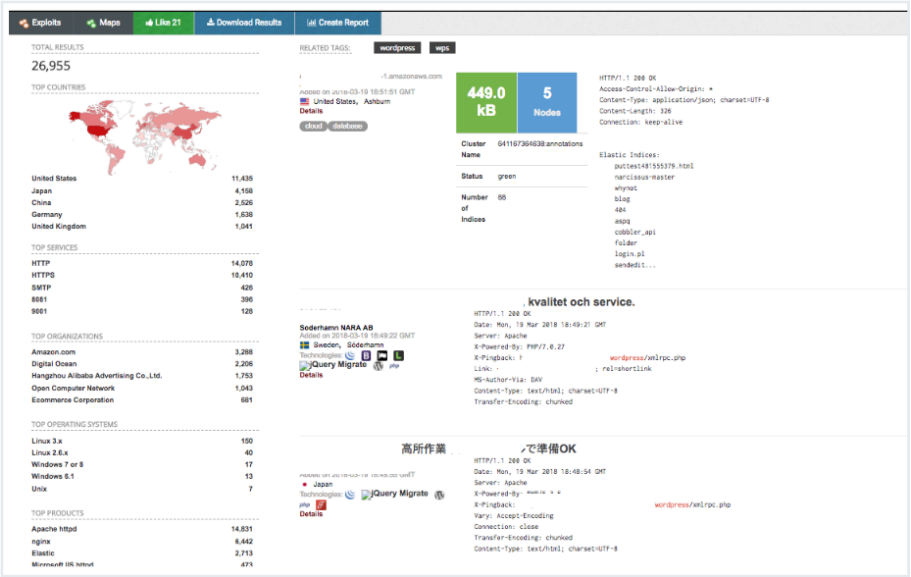
JASKLABS
TA-0009

TLP
WHITE

RISK FACTOR

HIGH

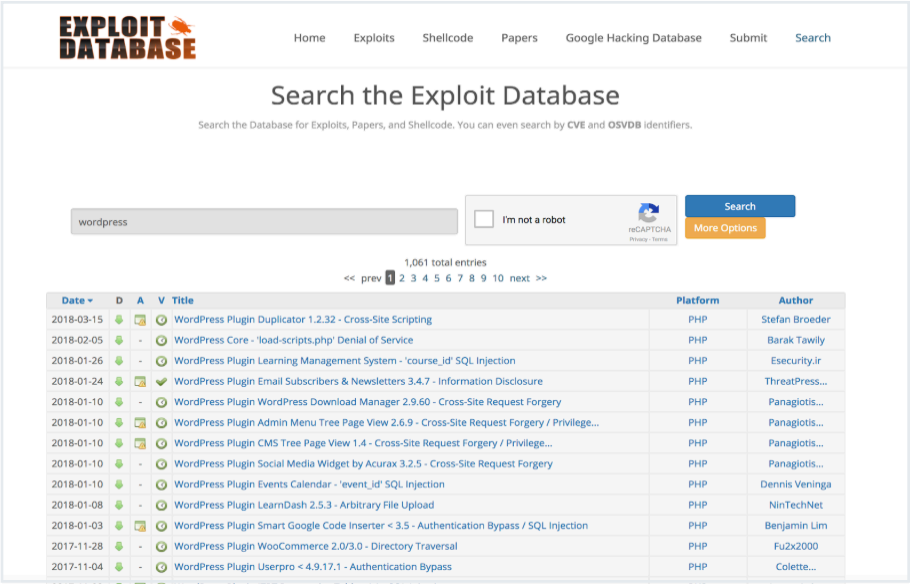
Fig 2. Shows simple Wordpress search result on vulnerability search engine Shodan.io



With an internet population of about 2 billion websites, Wordpress is said to have 5 percent of the total population. There are other many ways of discovering CMS frameworks on the web, such as using popular open source scanning like as Nmap or MassScan. There are also specific CMS vulnerable scan frameworks such WPScan.

Once the targets have been identified, malicious actors can proceed to exploit them and then entrench with a public or customized botnet code. Exploits are abundant for these type of CMS frameworks. A simple example of how to find available exploits is the website exploit-db.com.

Fig 3. Shows a query with keyword 'wordpress' on exploit-db website



AUTHOR
ROD SOTO

JASKLABS
TA-0009

TLP
WHITE

RISK FACTOR

HIGH

As seen in the above figures, it can be trivial even for a low-skilled attacker to find targets and matching exploits in order to start building a botnet. These botnets will likely be used for malicious purposes such as DDoS attacks, traffic distribution, spam, torrent storage, drive-by-downloads and the recently popular cryptomining attack vectors.

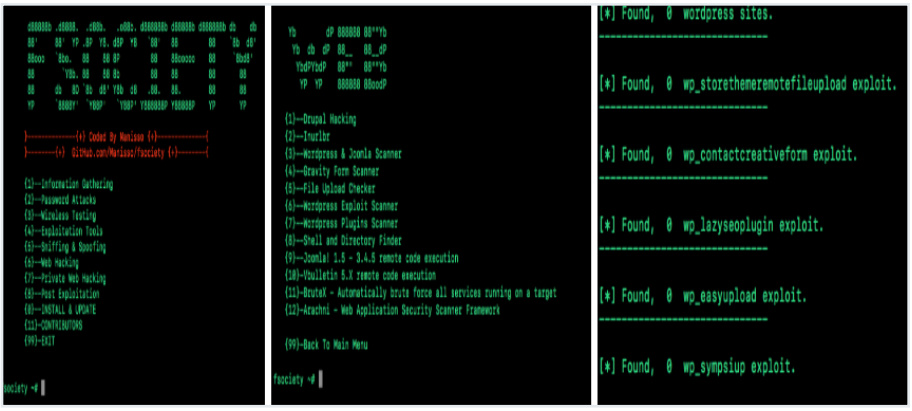
A more recent example on how CMS exploitation can drive botnet creation is the vulnerability known as Drupalgeddon2, which is said to affect over 1 million websites. As soon as proof of concept exploits were developed, mass exploitation of affected websites ensued.

Lab Study

As described above there are many tools for discovery and also sites where public exploits are available - though some are even more streamlined to exploit targeted CMS frameworks. For the purposes of this threat advisory, several recently released tools were selected. This selection is not exhaustive but aims to show how these tools can be used in the wild. Some of them allow malicious actors to target the most popular CMS frameworks in one single tool.

Fig 4. Shows CMS Brute Force tool in action *

Fig 5. Shows FSociety exploitation kit in action *



AUTHOR
ROD SOTO

JASKLABS
TA-0009

TLP
WHITE

RISK FACTOR

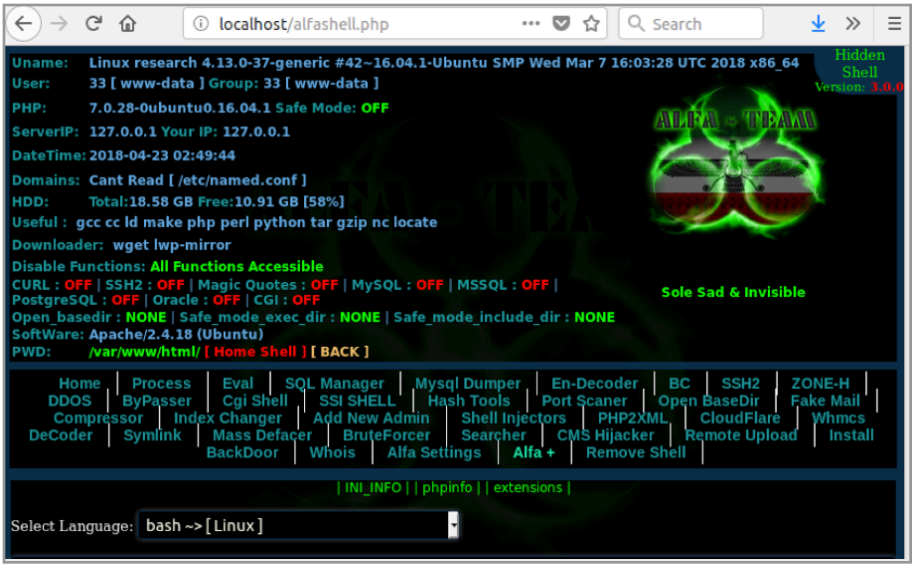
HIGH

The above tools are a sample of publicly available tools that can be downloaded from the internet. There are more sophisticated and customizable commercial tools that can provide a wider range of attack vectors.

Once the exploitation is successful, malicious actors proceed to entrench in those hosts by installing persistence/remote administration tools like webshells or installing botnet-type software that allows monitoring and the execution of commands from a command and control host.

One popular method of entrenching into a compromised website is the use of a webshell. Webshells are pieces of code functionality embedded in a website like interface. Webshells are widely available and are usually used by above-average skilled criminals or nation states. Some known nation state groups have their own webshells, as was recently revealed by Fireyee on a APT33 report where the use of an specific webshell (Alfashell) was observed during their campaigns.

Figure Shows APTE33 - alfashell (webshell)



Webshells can streamline post-exploitation operations by allowing command execution on compromised hosts. These commands usually pursue malicious activities such as DDoS attacks, spam, drive-by-downloads, exploit kits, cryptomining and crytpojacking.Cryptojacking is the use of cryptocoin commands embedded in a webpage that can use the CPU of a browsing computer in order to mine cryptocoin. Some cryptocoins like Monero (XMR) can be mined using CPUs.

There are actual Wordpress plugins that can be installed directly into a Wordpress site, as shown in the following graphic. This also allows malicious users to abuse free 'blogging' platform providers by opening multiple sites and installing plugins like the one below.

AUTHOR
ROD SOTO

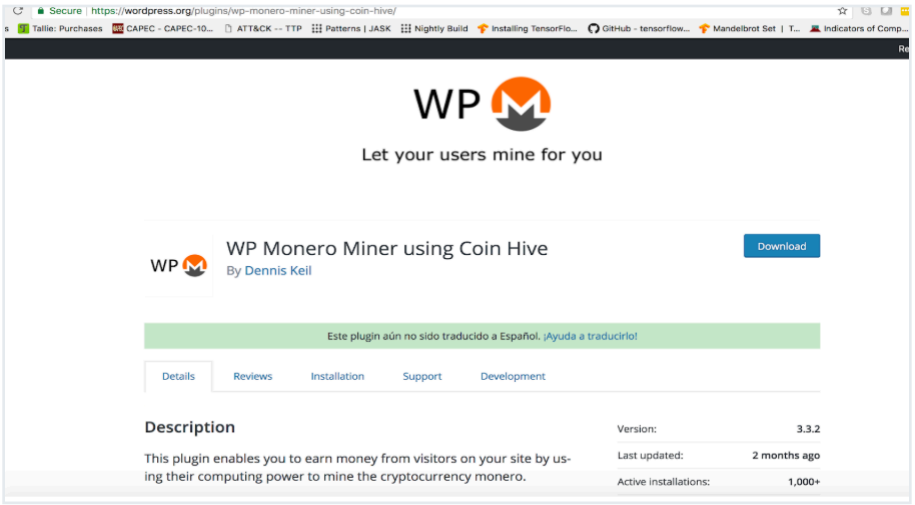
JASKLABS
TA-0009

TLP
WHITE

RISK FACTOR

HIGH

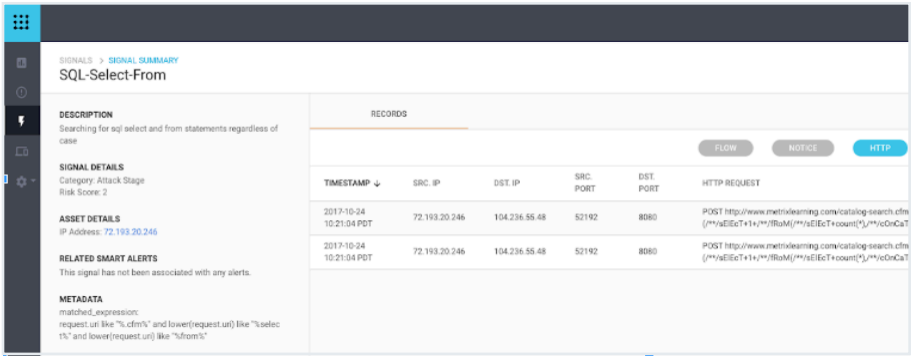
Fig 6. Shows WP Monero miner coinhive plugin



JASK Detection

The JASK ASOC platform provides several methods to detect these types of attacks, which are, for the most par t, web-based. JASK ASOC automatically detects for well-known OWASP TOP 10 attack vectors and offers the ability to customize and create patterns for specific user agents, or command strings in URLs. The following figure shows a signal from JASK ASOC detecting a SQL injection attack.

Fig 7. Shows SQL injection signal



AUTHOR
ROD SOTO

JASKLABS
TA-0009

TLP
WHITE

RISK FACTOR

HIGH

Mitigation

The following mitigation techniques will work for the most common CMS frameworks. More specific mitigation checks should be applied per use case and per customization level of such frameworks.

- Stay up to date on CMS versions.
- When possible, do not install third party plugins. Plugins are usually very insecure and provide a wider attack surface.
- Perform assessments against your site. Make sure things such as install directories, web directories and sensitive files are not accessible.
- Use complex passwords and multi-actor authentication.
- Use system firewalls and web application firewalls to protect against some attacks.
- Use DDoS defense providers.
- Do not use default credentials.
- Monitor your server for unusual files (webshells, binaries).
- Monitor your server for unusual traffic (Spikes in traffic to a specific file may indicate the presence of a webshell).