Emerging Threat – CryptoPHP

EXECUTIVE SUMMARY

Recent research details CryptoPHP; a backdoor delivered through a content management system (CMS) plug-in or theme (a method to modify the way a site is displayed without modifying the underlying software). This backdoor affects Joomla, WordPress and Drupal, the three largest CMS for web sites worldwide, comprising over 70% of all used CMS. Currently at version 1.0a, the CryptoPHP backdoor was first observed on November 12, 2014. Its command-and-control (C2) network is fairly robust, indicating an on-going attempt at targeting CMS systems resulting in almost 200 unique domains. This backdoor allows the attackers to perform content injection as well as search engine optimization (BlackhatSEO). Other features include unique capabilities such as encrypted C2 communication, the ability to update itself and an extensive C2 network, which makes it a threat of concern with very low detection rates seen from most anti-virus vendors.

THREAT TECHNICAL DETAILS

Targets

CryptoPHP is a web server compromise affecting Joomla, WordPress, and to a lesser extent, Drupal, and is delivered through theme packages and plug-ins. The backdoor-containing themes and plug-ins are pirated versions, advertised and distributed on a number of web sites. Social engineering is a primary method of enticement to acquire paid themes and plug-ins free of charge and without licenses.

This attack is targeted against the CMS user space; WordPress alone comprises over 60% of the CMS market, when combined with Joomla and Drupal, it captures over 70% of the market.

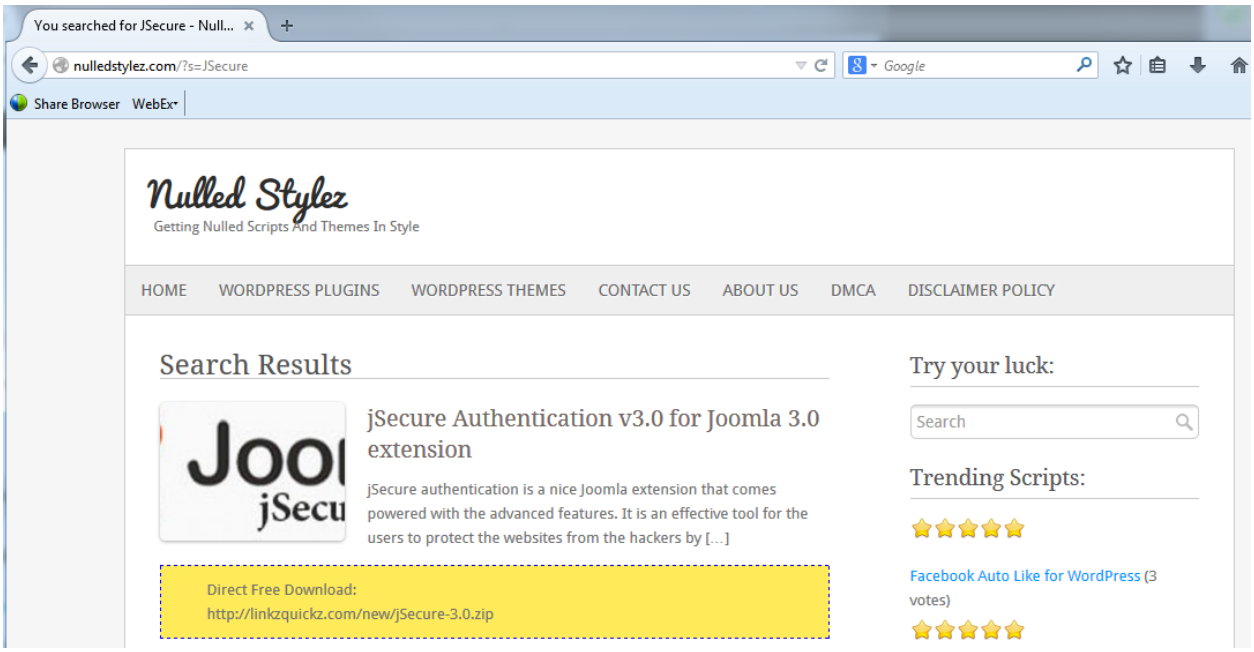
Domains and IPs Used

Over 20 different websites are being used to distribute the CryptoPHP backdoor (Fox IT Research Team):

Anythingforwp[.]com

awesome4wp[.]com
bestnulledscripts[.]com
dailynulled[.]com
freeforwp[.]com
freemiumscripts[.]com
getnulledscripts[.]com
izplace[.]com
mightywordpress[.]com
nulleddirectory[.]com
nulledlistings[.]com
nullednet[.]com
nulledstylez[.]com
nulledwp[.]com
nullit[.]net
topnulledownload[.]com
websitesdesignaffordable[.]com
wp-nulled[.]com
yoctotemplates[.]com

The initial plug-in discovered was JSecure. This plug-in was downloaded from nulledstylez[.]com, purported to be a source for "nulled" scripts or pirated plugins with no licensing checks.



Still available as a download, the malicious JSecure plug-in has an MD5 signature of 8bb834dfc442d1f96b1c7fd13b1bac7f. Many of the plug-ins available on this site contains the same backdoor. The MD5 hashes are, however, of limited use because the original .zip file is removed shortly after installation.

A link to the user-agent chishijen12 (identified as a Moldavian-based IP address) has been in use since December 2013. The IP is located in Chisinau, making the user-agent string geographically relevant.

The C2 servers include a domain to publish backdoored content, and a server to store published content, most hidden behind CloudFlare. Forty-five unique IPs, and almost two hundred unique domains have been identified, with a pattern of three to six domains pointing to each IP address, with very little overlap.

The geographic breakdown of the C2 server' s shows they are in the Netherlands (18), Germany (18), the U.S. (8) and Poland (1). Many of the discovered domains have been sinkholed.

Attack Vectors

- Social Engineering enticement to acquire expensive plug-ins and themes for free
- Backdoored themes and plug-ins available from many "nulled" script websites, where many themes and plug-ins contain the same backdoor

- Installation of infected scripts or themes provide website compromise and backdoor access for content injection and remote code execution
- Insertion of illicit search engine optimization strings and links in web content when the requesting user-agent appears to be a crawler or bot

Incursion and Expansion

Original detection of the backdoor was via an unusual request, namely one with no referrer, no user agent and performing an HTTP POST to a .biz domain:
[08/May/2014:12:44:10+0100] "POST http://worldcute[.]biz/ HTTP/1.1" - - "-" "-"
The request was further suspicious in that it was a multi-part MIME with some information about the compromised server contained within. The only event prior to the request was a Joomla plug-in installation.
The installation package includes an image in the images directory called "social.png" that is actually a PHP script backdoor. The first visitor to the site (after the plug-in or theme is installed) activates the backdoor and begins the external connection to the C2 network. An echo array is available for inserting content into web pages. Redirections to a Justin Bieber YouTube video and hijacking of SEO meta-data have been observed in the wild. The injection appears to only occur when the visitor resembles a web crawler, based on its user-agent or hostname. This behavior is known as "BlackhatSEO" or illegally performing search engine optimization. The backdoor uses the CMS framework and database to function and to store encrypted content for injection in web pages.

Exfiltration and Communication

C2 communication is performed using RSA public key encryption to an extensive infrastructure of domains and IPs with backup against takedowns using email. The backdoor is also capable of remotely updating its C2 list.
Email, when used as a backup for unavailable C2 servers, has always been seen with the subject of 'Phone Home'. Manual control of the backdoor via a crafted URL is also possible. Manual commands can be used to check in to a new C2 server or connect to a new C2 server:
http://infected.host/index.php?<server_key>=reset and optionally &url=<new_C2>

Version information for the backdoor is sent as a part of the POST data: *$post_data['ver'] = '1.0a'*;. Additional statistics sent to the C2 server include install date, last connected date, version number and visitor count to the infected web site.
C2 communication is encrypted with an embedded public RSA key using PHP' s openssl_seal command. Originally a 1024-bit RSA key was used, but that has been upgraded to a 2048-bit RSA key.
When the backdoor is first run, it generates a random 10-character key for the server and an RSA key pair. The public key is sent to C2 servers. It is used for encrypting communications along with the server key used to send commands to the backdoor. Commands currently supported are *update* and *reset*.
Curl_exec is used to send the encrypted data with newer versions supporting fsockopen if curl_exec is not available.

Persistence

WordPress infections add an additional administrator account called 'system' or with appended numbers if 'system' is already used. The email set for the administrator account is 'afjiaa@asfuhus.cc.c' and again with numbers inserted before the @ if that email is already in use.
While a C2 can return a JSON update to configuration, manual configuration updates do not appear possible at this time.
There is a list of hard-coded domains that are randomized based on the infected host domain name.

SYMANTEC MSS SOC DETECTION CAPABILITIES

For customers with our IDS/IPS Security Management services, vendor-based signatures will be automatically deployed, as per the vendor's recommendation. If you would like further information regarding the signature states on your devices, or would like to request the activation of a signature, we can be reached by requesting help via phone, e-mail, chat, or by visiting the MSS portal at https://mss.symantec.com.

For customers with monitor-only IDS/IPS devices, Symantec MSS stands ready to provide security monitoring once your IDS/IPS vendor releases signatures and those signatures are enabled on your monitored devices.

MSS SOC Analytics Detection

We are actively working on adding detection for indicators associated with CryptoPHP.

Vendor Detection

- **Symantec AV:**
- PHP.Phocrypt

- **Snort/Emerging Threat:**
- SID 2019748 - ET WEB SERVER FOX SRT Backdoor CryptoPHP Shell C2 POST
- SID 2019749 - ET WEB SERVER FOX SRT Backdoor CryptoPHP Shell C2 POST (fsockopen)

This list represents a snapshot of current detection. As threats evolve, detection for those threats can and will evolve as well.

MITIGATION STRATEGIES, BEST PRACTICES AND RECOMMENDATIONS

- Only acquire plug-ins and themes for content management systems from legitimate sources.
- For technologies not monitored/managed by MSS, ensure all signatures are up to date, including endpoint technologies.
- Ensure all operating systems and public-facing machines have the latest security patches and that anti-virus software and definitions are up to date.
- Ensure that Content Management Systems (CMS) are configured properly and that the following recommendations are observed:
    - Never run a CMS in its default configuration state.

- Upgrade whenever newer versions become available.
- Change the administrator folder. Sometimes this is enough to deceive your average script kiddy and also prevents your systems from becoming the low-hanging fruit (targeted first by automated scanners).
- Symantec also recommends that you integrate CMS systems into your patch processes and subscribe to vulnerability warnings for the corresponding vendor.

REFERENCES

- **"Market share trends for content management systems for websites"**, w3techs http://w3techs.com/technologies/history_overview/content_management
- **"CryptoPHP: Analysis of a hidden threat inside popular content management systems", Fox IT Security** https://foxitsecurity.files.wordpress.com/2014/11/cryptophp-whitepaper-foxsrt-v4.pdf
- **"CryptoPHP a week later: more than 23.000 sites affected,"** Fox IT Blog http://blog.fox-it.com/2014/11/26/cryptophp-a-week-later-more-than-23-000-sites-affected/

Thank you for choosing Symantec as your managed Security Services Provider. Should you have any questions or feedback, please contact your Services Manager or the Analysis Team. Both can be reached by requesting help via phone, e-mail, chat or by visiting the MSS portal at https://mss.symantec.com.

Global Client Services Team
Symantec Managed Security Services
MSS Portal: https://mss.symantec.com
MSS Blog: http://www.symantec.com/connect/symantec-blogs/cyber-security-group