Angler EK: More Obfuscation, Fake Extensions, and Other Nonsense

Talos Group | June 5, 2015 at 5:05 am PST

(0 Comments)

This post was authored by Nick Biasini

Late last week Talos researchers noticed a drastic uptick in Angler Exploit Kit activity. We have covered Angler previously, such as the discussion of domain shadowing. This exploit kit evolves on an almost constant basis. However, the recent activity caught our attention due to a change to the URL structure of the landing pages. This type of change doesn't occur often and was coupled with some other interesting tidbits including how the HTTP 302 cushioning has evolved and the payload of another ransomware has changed.

During research Talos identified several active Angler campaigns delivering different payloads via different methods. The first campaign was delivering Cryptowall, which will be covered in detail here. The second delivered Bedep with click fraud and illustrates the variety with which Angler can be used to deliver different payloads. The details of Bedep with click fraud has been covered thoroughly and will not be specifically discussed in this article.

Angler Updates

Before we discuss the changes let's cover how the Angler Exploit Kit typically operates. Historically, users have been primarily exposed to the Angler exploit kit via malvertising. When a user encounters an exploit kit, users are typically sent through a redirect chain before winding up on the exploit kits landing page. The gate where users redirected to typically has a has structure similar to the following:

/some_random_words_here/154920479320

This is where the final redirection occurs to the landing page that is serving the exploits that compromise the system. This landing page normally looks something like this:

/L8Vz9fnAJQ-NIIEeBal7h7QTEL5YpvcKfrOMuBGcE7sOA4Xt

Which would then serve an exploit, usually Adobe Flash related, and then finally a payload, which has historically been Bedep mostly. At a high level, this is how Angler operated and the basic functionality remains the same. One thing that has been discussed previously is the use of 302 cushioning during the redirection chain. Basically, the initial redirection leads to a page that uses a HTTP code of 302, which is the HTTP return code for "Moved Temporarily". This adds more layers to the redirection which continues with this campaign. This particular campaign falls back to an older methodology of utilizing compromised websites with scripts that are redirecting the user to the malicious site. This particular sample was being hosted on one such compromised site. Note the malicious iframe found in the code below:

```
angler_iframe
```

This malicious iframe is indicative of most iframes used in conjunction with exploit kits. However, there was a subtle change, instead of using the typical domain shadowing the use of a dynamic DNS provider was substituted. This again adds another small wrinkle and level of customization. The use of dynamic DNS in exploit kits isn't new and is still widely used with Fiesta exploit kit.

The addition of dynamic DNS was the first change. The second more significant change is related to the actual URL of the landing page. When the spike in our telemetry data was seen that's when the change became obvious, although very subtle. The URL changed from what was shown above to one of the following URLs:

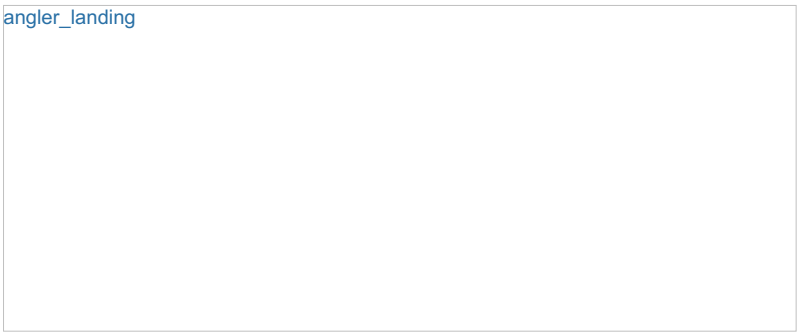
/L8Vz9fnAJQ-NIIEeBal7h7QTEL5YpvcKfrOMuBGcE7sOA4Xt.php
/w1smRNTBDuMu9mMm2EFsj-B_a8VpjJMEpo98-m4MezJhSsNS.play
/F-4C7nrgQ1DuqCPXKC7e9ruFQmqVv-d5tYyK4xVtDMPy6Ywh.vbscript
/pYRIH5ApZdFL4gLDzx8_VcaemFmBymXY0EQXrIM8RwAzISSo.pycharm
/bcxo-513WCIhyfbChTj0JEsDjdfozPC0SDYufo-SEV2yU0TP.aspnet

/2UQV9IGkBXFC2QCgiR6K96J94PqCOTf6kuIdm0VoZkfM21_N.cppfile
/nM89-qFt1Dl3YUmj-OS3sqr-1J0fVPxbHf46FHklvmYCkWZJ.javabin
/C9nRrUnG8wsks480kqIDBVw_Rrr7hmapSuqBmNAW0ZIgDMrL.jsscript
/0qIbGTXEKgTKX-N8Cg8TOwQ4M49pH6FHKxPrcKq3CaY_06Vy.playme
/b8WPbgZJNEPngVAz2Zq7PlHkS1T_N4TGrQzLZWJaGuRAON_0.cpp3
/6GAyyn99jAscOPNNN9VxCUH403etgcntIDdvwB0bs9RuYZtl.js8
/ee3m7b8DD1MfeRQp3NLByWQFlv6mRIUnlHKtxMKiV3fmugce.java1
/Grdelu0G6OwIxkOqjlRuoaIxa80ioqx-5_Ki2gQtBzeD7Kie.js
/d4FDOgD1Mzck36MKTp6tdUTrq_jNHwqDuSgmgf5M0L7M1tSn.java
/9XJUs2Vu29QnBDAQHH_QU0JeoVE__dtrZGovrxg3wdPZ1EWE.cpp
/1Rk4kgr_OzlNhQxKBDbP_GmbYHiBJq5027gO83vayAeFXk4c.py
/I1PiQRtfNiMqZHSFWu1JbMqFCCuJcVEWs9SDMhzNQibvFi_P.vb

Obviously, the first portion of the string involves a randomly generated string. The part to focus on is the extensions. This is a significant change to the URL structure, by adding a varied list of extensions Angler authors are creating significantly more variation. The reason for the change has everything to do with detection. Most Angler landing page detection is done off of the URL structure and by making this change and adding a list of varying extensions, exploit kit authors bypass a huge amount of the detection technologies. This type of a change would be expected especially if there are other major changes underway. Much the same way that domain shadowing was unveiled at roughly the same time the Adobe Flash 0-day was dropped into this exploit kit.

This isn't the first time that the URL has evolved for Angler which previously made use of simple .php paths in the past before changing to the recent random string of text shown above. The actual content displayed to the user has remained largely static. Presenting the user with a series of quotes from *Sense and Sensibility* as shown below:

angler_landing



Payload

cryptowall_3_banner

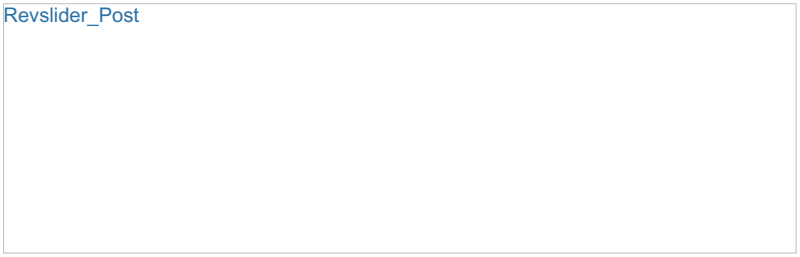
After compromising the user with a malicious Flash file or other exploit, the user is served a variant of Cryptowall. This isn't uncommon behavior as we have seen an explosion in the delivery of various types of ransomware via exploit kits. This is a cheap and efficient way to make sure threat actors are able to compromise users for monetary gain.

This specific variation of Cryptowall did have some interesting characteristics. First is the use of WordPress sites to store information. Talos observed a significant amount of potentially compromised WordPress sites being used to house information about the compromised systems including IP information as well as other key identifiers. One interesting thing was the amount of different domains contacted. Normally malware will contact several domains for different purposes (i.e C2, Dropped Files, Exfil, etc.). Its not uncommon to see a host contact ten different domains during an infection chain. This particular sample contacted almost 40 different domains and attempted to post data on 30 different WordPress sites. These posts were made to

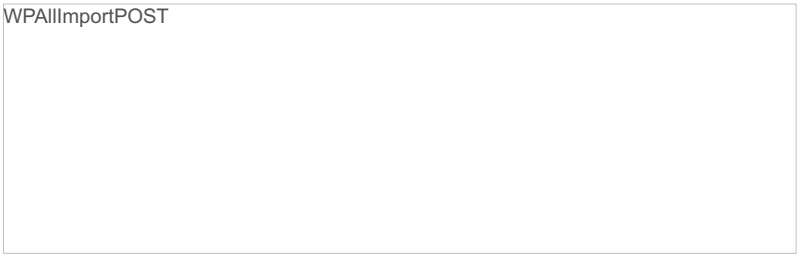
look like image files being posted and were seen posting to wordpress plugins that have been in the news over the last several months for being exploitable. Below are some sample images associated with the data that was posted:

Portion of string uploaded to compromised WordPress Site

These posts were done to two specific paths both associated with specific WordPress plugins. The first was revslider and the POST would look similar to what is shown below:



The second is WP All Import and the POST would look similar to this:



Both Revslider and WP All Import had recent severe vulnerabilities that resulted in a large amount of WordPress sites being exploited and eventually compromised. This is likely the method that the threat actors used to gain access to the sites and leverage them as locations for hosts to send data. This allows the threat actor to still be able to gather information regarding infected hosts without having the liability of an associated domain or server. Additionally, since the large majority of these sites utilize shared hosting it makes IP blacklisting far more challenging without impacting thousands of other legitimate websites.

An analysis of our telemetry data has tracked this change back to earlier in 2015 continuing for several months. Depending on the data sent via POST from the compromised host a different response was returned. In some cases encoded commands and in others the image presented to the user for ransom purposes was downloaded. Also, included was additional 302 cushioning that pointed to specific sites being hosted from a hard coded IP address (194.6.233.7) or to a payment information site. Additionally, Talos found multiple occasions where a formerly compromised wordpress site had appeared to have been patched or at least had the malicious content removed.

Sample 302 Response from WordPress site

IOC

Hashes:
28f6b5f344f7d2bef75b30ba2e286ddff3d3a2009da1d01d7e30e21feecfde34 (Flash Exploit)
023de93e9d686bf6a1f80ad68bde4f94c5100b534f95285c1582fb8b8be8d31f (Cryptowall 3.0 Sample)

Domains:
schapershonden-yhteenliittymin.inspirefilms.us
capsteads-tmenupopup.mercuryoutboardnc.com
mfrzdzjjpi.myftp.biz
traditionetgourmandises.fr
convenzioni.ording.roma.it

99mkb.com
hostyoursitehere.com
alpha.akesha.com
andreiprundeanu.eu
4042shopping.com
redstarfuochicinesi.it
alebehr.com
alchemyofpresence.com
blationmedia.com
jeanrey.fr
awynnejoinery.co.uk
americanfamilyenergy.com
bezpiecznaswinka.pl
redstarfuochicinesi.it
buroroebers.nl
bebeamor.co.uk
jandchousecleaning.com
asambleadedios.org
buhtime.by
asadiag.com
beijerlandsekelnerrace.nl
atlantacustomwork.com
braingame.biz
doggonesigns.com
ancientvoyages.com
gonavarro.com
sweetthangzdesserts.com
traditionetgourmandises.fr
brandgriffin.com
tarifair.fr
alsblueshelpt.nl
7d2.c27.myftpupload.com
autorijschoolconsistent.nl

IP Addresses:
78.46.250.103
194.6.233.7
94.131.14.23
94.242.198.221
173.227.247.35
**Note: The large majority of the domains are residing on shared IP address space. To prevent affecting non-malicious domains hosted on these servers the IPs have been excluded.*

Conclusion

Exploit kits are always going to evolve to improve efficiencies, increase evasion, maximize ability to compromise users, and create detection and prevention challenges. This is another example of how specifically the Angler Exploit Kit continues to change. This doesn't always involve using new or novel techniques. In this example the EK went from being distributed via the newer technique of malvertising to reverting to malicious iframes on compromised websites. Also, it seems that a hybrid approach to URL's has been undertaken by Angler. The old usage of .php files has been merged with the more recent randomized string to create a third variant of URL structure. Finally, the removal of domain shadowing for the 302 cushioning and the addition of dynamic DNS instead. This technique may be a relatively new feature to Angler, but has been in use by other Exploit Kits for some time.

The payloads are another example of how exploit kits continue to evolve. The threat actors behind exploit kits are, like most people making money from hacking, jumping on the ransomware bandwagon. Ransomware works and makes reliable money. Threat actors realize this and are using whatever means necessary to get users infected. Exploit kits provide the perfect platform to infect large amounts of users and get lots of monetary gain.

Angler related Snort Rules: 28612-28616, 29066, 29411-29414, 30852, 30920, 31046, 31129-31332, 31370-31372, 31694-31695, 31898-31901, 32390, 32399, 33182-33188, 33271-33274, 33286, 33292, 33663, 34348, 34719-34720

For the most up to date list, please refer to Defense Center or FireSIGHT Management Center.

Coverage

image09

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites, including the downloading of the malware downloaded during these attacks.

The Network Security protection of IPS and NGFW have up-to-date rules to detect malicious network activity by threat actors.

Tags: angler, Cryptowall, exploit kit, Talos, Threat Research

We'd love to hear from you! To earn points and badges for participating in the conversation, joinCisco Social Rewards. Your comment(s) will appear instantly on the live site. Spam, promotional and derogatory comments will be removed.

All comments in this blog are held for moderation. Your comment will not display until it has been approved

Leave a Reply

Name

Website (please include "http://")

Switch To Mobile Version