Mylobot Continues Global Infections

November 15, 2018

BLACK LOTUS LABS Black Lotus Labs Posted On November 15, 2018

0

0

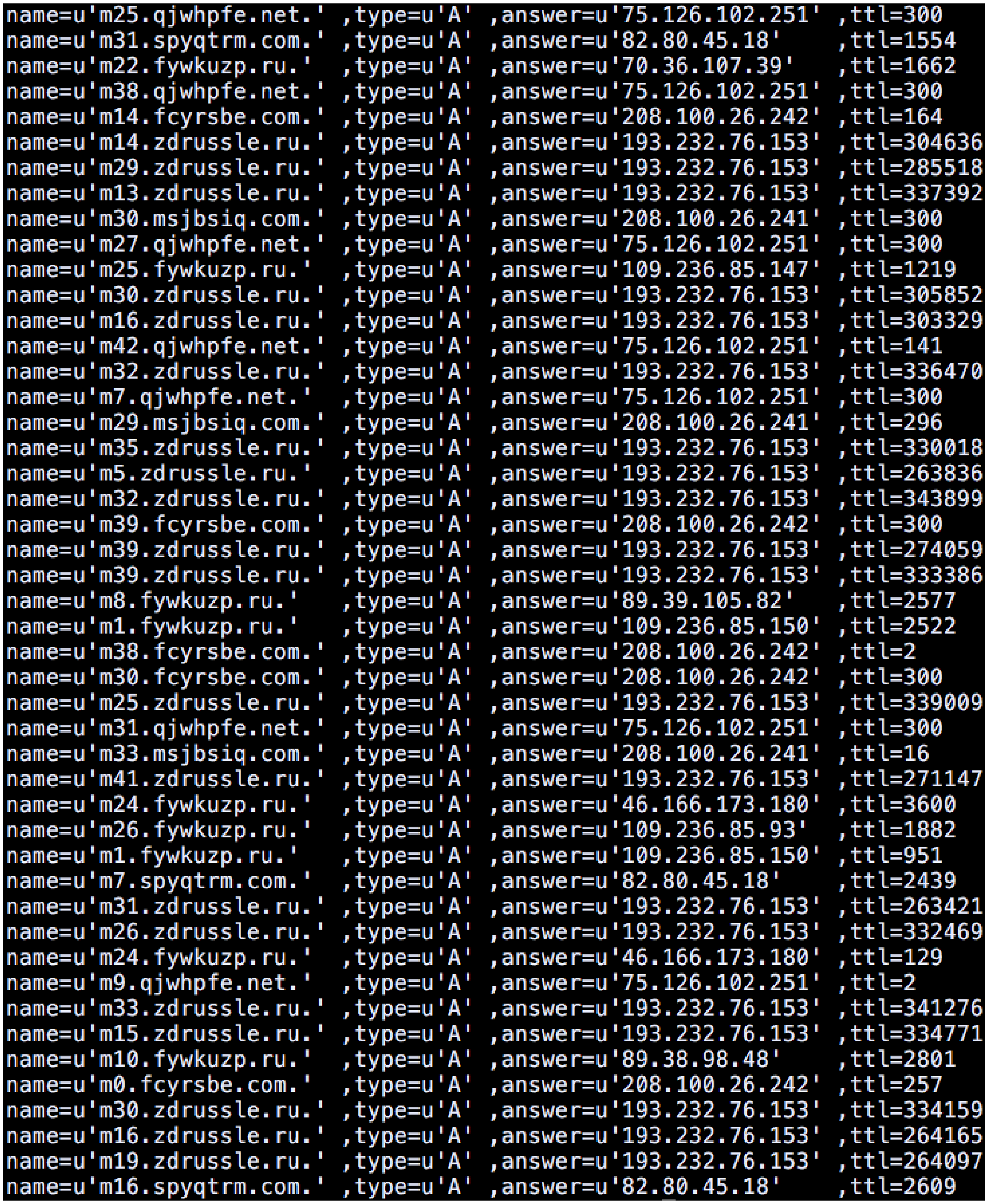
Shares

CenturyLink Threat Research Labs has been tracking the Mylobot botnet, a sophisticated malware family that is categorized as a downloader. What makes Mylobot dangerous is its ability to download and execute any type of payload after it infects a host. This means at any time it could download any other type of malware the attacker desires. A detailed walkthrough and reverse engineering analysis of Mylobot was first reported in June by Deep

Instinct. During the time we have been monitoring Mylobot we have observed it downloading the Khalesi malware as a second stage to infected hosts. Kaspersky Lab reports that the information stealing Khalesi malware is one of the top downloaded malware families in 2018.

We were first alerted to the botnet's behavior by IPs interacting with our honeypot network. Our team is constantly monitoring attack patterns and looking for common behaviors in these attacks. In this case, we observed a common behavior to DNS lookups coming from a distinct group of these IPs. Each of the hosts performed DNS lookups for domains that we had flagged as likely to be algorithmically generated.

The common behavior was detected by combining the IPs extracted from our honeypot logs with DNS resolution data, and applying unsupervised clustering techniques to isolate large clusters of similarly-behaving devices. The resulting behavior appeared to be callbacks to Domain Generation Algorithm (DGA) generated domains. Our DGA domains list is generated by monitoring lookups to estimate the probability that a domain was generated using a variety of techniques. These techniques could include randomly choosing letters or numbers, or randomly choosing words from a dictionary to make up a domain. The domains being queried by this particular cluster of IPs appeared to be seven randomly-chosen letters with the TLDs .ru, .net and .com. The subdomains ranged from m0 to m42.

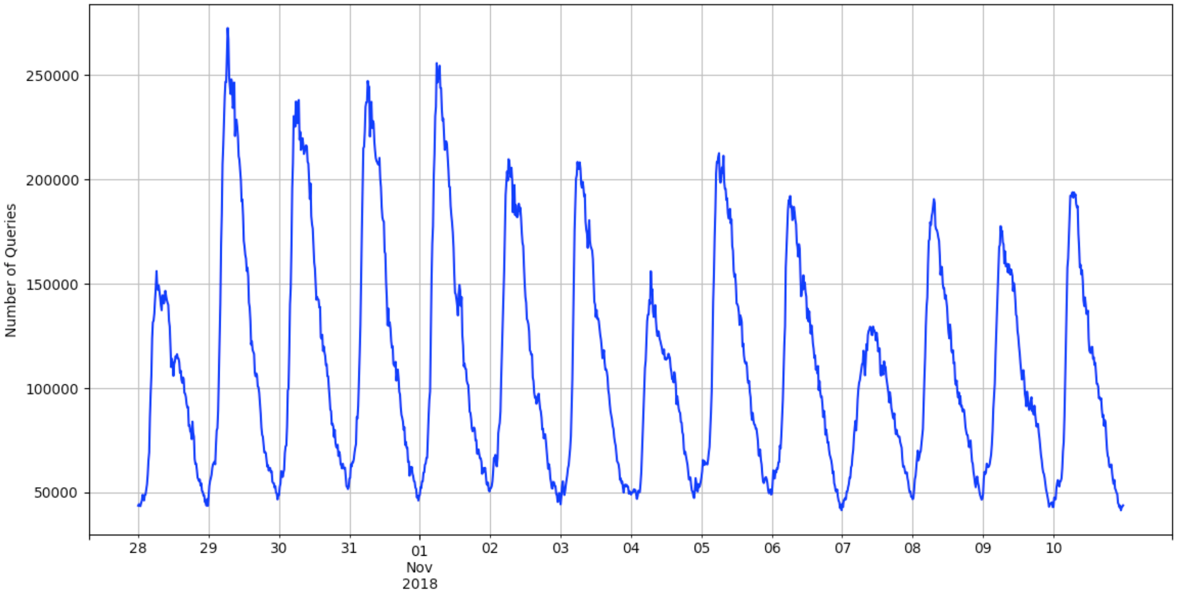


```
name=u'm25.qjwhpfe.net.' ,type=u'A' ,answer=u'75.126.102.251' ,ttl=300
name=u'm31.spyqtrm.com.' ,type=u'A' ,answer=u'82.80.45.18'    ,ttl=1554
name=u'm22.fywkuzp.ru.'  ,type=u'A' ,answer=u'70.36.107.39'   ,ttl=1662
name=u'm38.qjwhpfe.net.' ,type=u'A' ,answer=u'75.126.102.251' ,ttl=300
name=u'm14.fcyrsbe.com.' ,type=u'A' ,answer=u'208.100.26.242' ,ttl=164
name=u'm14.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=304636
name=u'm29.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=285518
name=u'm13.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=337392
name=u'm30.msjbsiq.com.' ,type=u'A' ,answer=u'208.100.26.241' ,ttl=300
name=u'm27.qjwhpfe.net.' ,type=u'A' ,answer=u'75.126.102.251' ,ttl=300
name=u'm25.fywkuzp.ru.'  ,type=u'A' ,answer=u'109.236.85.147' ,ttl=1219
name=u'm30.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=305852
name=u'm16.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=303329
name=u'm42.qjwhpfe.net.' ,type=u'A' ,answer=u'75.126.102.251' ,ttl=141
name=u'm32.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=336470
name=u'm7.qjwhpfe.net.'  ,type=u'A' ,answer=u'75.126.102.251' ,ttl=300
name=u'm29.msjbsiq.com.' ,type=u'A' ,answer=u'208.100.26.241' ,ttl=296
name=u'm35.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=330018
name=u'm5.zdrussle.ru.'  ,type=u'A' ,answer=u'193.232.76.153' ,ttl=263836
name=u'm32.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=343899
name=u'm39.fcyrsbe.com.' ,type=u'A' ,answer=u'208.100.26.242' ,ttl=300
name=u'm39.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=274059
name=u'm39.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=333386
name=u'm8.fywkuzp.ru.'   ,type=u'A' ,answer=u'89.39.105.82'   ,ttl=2577
name=u'm1.fywkuzp.ru.'   ,type=u'A' ,answer=u'109.236.85.150' ,ttl=2522
name=u'm38.fcyrsbe.com.' ,type=u'A' ,answer=u'208.100.26.242' ,ttl=2
name=u'm30.fcyrsbe.com.' ,type=u'A' ,answer=u'208.100.26.242' ,ttl=300
name=u'm25.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=339009
name=u'm31.qjwhpfe.net.' ,type=u'A' ,answer=u'75.126.102.251' ,ttl=300
name=u'm33.msjbsiq.com.' ,type=u'A' ,answer=u'208.100.26.241' ,ttl=16
name=u'm41.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=271147
name=u'm24.fywkuzp.ru.'  ,type=u'A' ,answer=u'46.166.173.180' ,ttl=3600
name=u'm26.fywkuzp.ru.'  ,type=u'A' ,answer=u'109.236.85.93'  ,ttl=1882
name=u'm1.fywkuzp.ru.'   ,type=u'A' ,answer=u'109.236.85.150' ,ttl=951
name=u'm7.spyqtrm.com.'  ,type=u'A' ,answer=u'82.80.45.18'    ,ttl=2439
name=u'm31.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=263421
name=u'm26.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=332469
name=u'm24.fywkuzp.ru.'  ,type=u'A' ,answer=u'46.166.173.180' ,ttl=129
name=u'm9.qjwhpfe.net.'  ,type=u'A' ,answer=u'75.126.102.251' ,ttl=2
name=u'm33.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=341276
name=u'm15.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=334771
name=u'm10.fywkuzp.ru.'  ,type=u'A' ,answer=u'89.38.98.48'    ,ttl=2801
name=u'm0.fcyrsbe.com.'  ,type=u'A' ,answer=u'208.100.26.242' ,ttl=257
name=u'm30.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=334159
name=u'm16.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=264165
name=u'm19.zdrussle.ru.' ,type=u'A' ,answer=u'193.232.76.153' ,ttl=264097
name=u'm16.spyqtrm.com.' ,type=u'A' ,answer=u'82.80.45.18'    ,ttl=2609
```

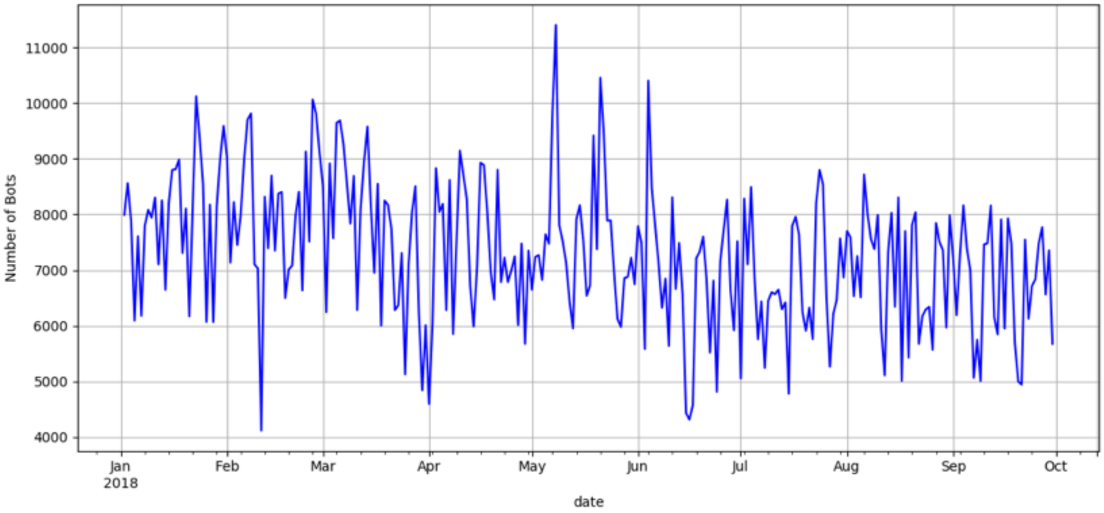
Our investigation in to these domains found that they are hardcoded into samples of the Mylobot malware. Mylobot contains sophisticated anti-VM and anti-sandboxing techniques. For example, it sits idle for 14 days before attempting to contact the C2.[1] This delaying technique is used to wait out the sandbox environment to avoid detection. When it attempts to contact the C2, the malware uses a set of 1,404 hard-coded domain name and port pairs.

For each domain-port pair, the malware first attempts to resolve 43 subdomains, which are the same as those we saw in passive DNS (m0 through m42). If one of the FQDNs resolves to an IP, the malware tries to connect to the IP on the port that was hard-coded with that domain. With 1,404 domains and 43 subdomains, this results in 60,372 DNS queries from each bot.

The large volume of queries from an individual host can be used as an indication of an infection by this malware. The internet-wide impact of this behavior can be seen when looking at a two-week period. As each region of infected hosts is powered on to begin the day, a large volume of queries occurs, slowly dropping off as each host finds the C2. Below is a graph showing the total number of queries to these domains we see in our DNS traffic over this period.



Through our analysis it was important to understand if the botnet had shown any noticeable variation in size. We found, that while day-to-day sizes may vary due to normal botnet maintenance and data sampling, the botnet’s total size has remained relatively consistent throughout the year. The below graph displays the number of IPs we see in passive DNS traffic querying the domains in question for the current year.



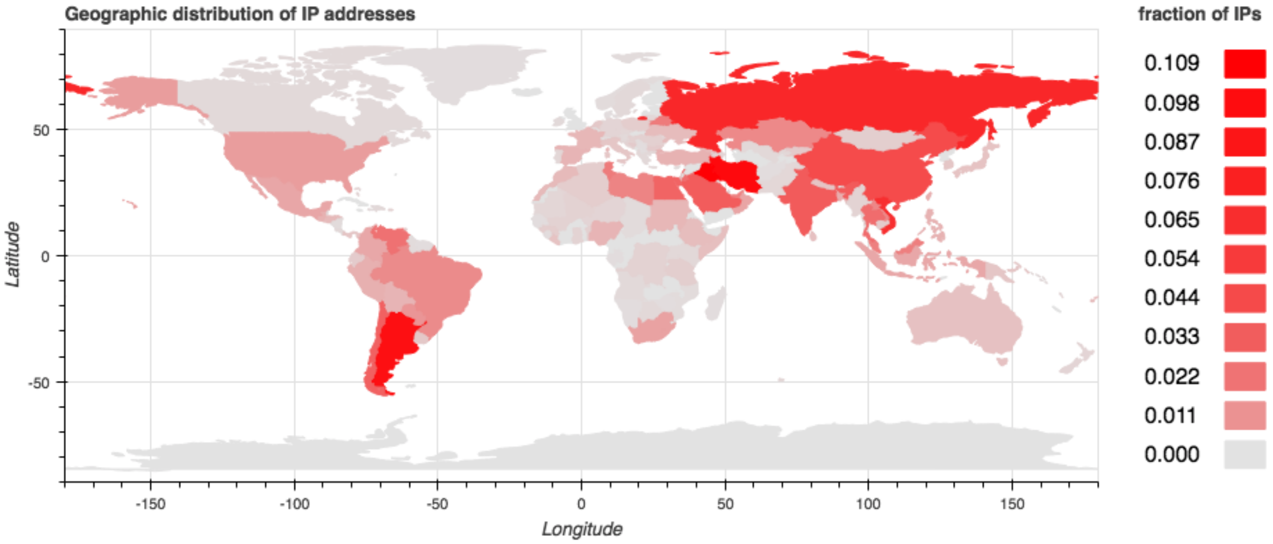
At CenturyLink Threat Research Labs, we leverage our global visibility to identify botnet infrastructure. Analyzing DNS response data allowed us to generate a list of potential C2s from the FQDNs that resolved to IP addresses. Searching our sampled Netflow for traffic from these IPs, we can identify the active C2s and their ports. Below are the active C2s from November and the number of IPs the C2 sent responses to on the C2 port.

C2 IP	Port	FQDN	Number of IPs
74.222.19.103	7432	m20.fywkuzp.ru	2,675
74.222.19.63	7432	m19.fywkuzp.ru	2,511
217.23.13.62	7432	m7.fywkuzp.ru	2,420
89.39.107.19	7432	m12.fywkuzp.ru	2,289
70.36.107.38	7432	m21.fywkuzp.ru	2,259
89.39.105.82	7432	m8.fywkuzp.ru	2,133
89.38.98.48	7432	m10.fywkuzp.ru	2,128
109.236.85.147	7432	m25.fywkuzp.ru	2,108
217.23.6.62	7432	m11.fywkuzp.ru	2,082
89.38.98.165	7432	m6.fywkuzp.ru	1,632
109.236.85.21	7432	m4.fywkuzp.ru	1,532
217.23.3.15	7432	m13.fywkuzp.ru	1,119
109.236.85.150	7432	m1.fywkuzp.ru	986

109.236.85.154	7432	m5.fywkuzp.ru	971
46.166.173.180	7432	m24.fywkuzp.ru	943
109.236.85.153	7432	m3.fywkuzp.ru	917
109.236.85.135	7432	m2.fywkuzp.ru	840
109.236.87.49	7432	m9.fywkuzp.ru	683
70.36.107.39	7432	m22.fywkuzp.ru	666
75.126.102.251	9529	m9.qjwhpfe.net	344
109.236.85.93	7432	m26.fywkuzp.ru	184
70.36.107.154	7432	m0.fywkuzp.ru	135

In total, there were 9,874 unique IPs that received responses from the C2s on the C2 port for this particular day. Comparing this with other time intervals, we have observed the total number of unique IPs reach as high as 17,979.

There was speculation in the Deep Instinct analysis that a GeoIP filter was being used by the C2s, since researchers were unable to get a response from C2s in certain geographic areas. We were able to get a response from one of the C2s, 70.36.107.154, from an IP located in a different geographic region. Therefore, it is unclear to us if there is any GeoIP filtering taking place. Below is a heatmap showing the concentration of IPs that communicated with the C2s on the C2 port.



Below are the top 10 countries we observed communicating with the C2 on the C2 port on November 10.

Country	Number of IPs
Iraq	3,014
Iran	2,788
Argentina	2,602
Russia	1,919
Vietnam	1,786
China	1,202
India	926
Saudi Arabia	914
Chile	844
Egypt	798

When the malware receives a response from the C2, it XORs it with the byte 0xDE. The resulting string contains up to two URLs. Each URL contains an IP and a file ending in .gif. Below is the decoded response we received from the C2.

```
'\xde\xde\xde\xde\xd6http://138.128.150.133/winme.gif\x00\xde\xde\xde\xde\xd9http://13
```

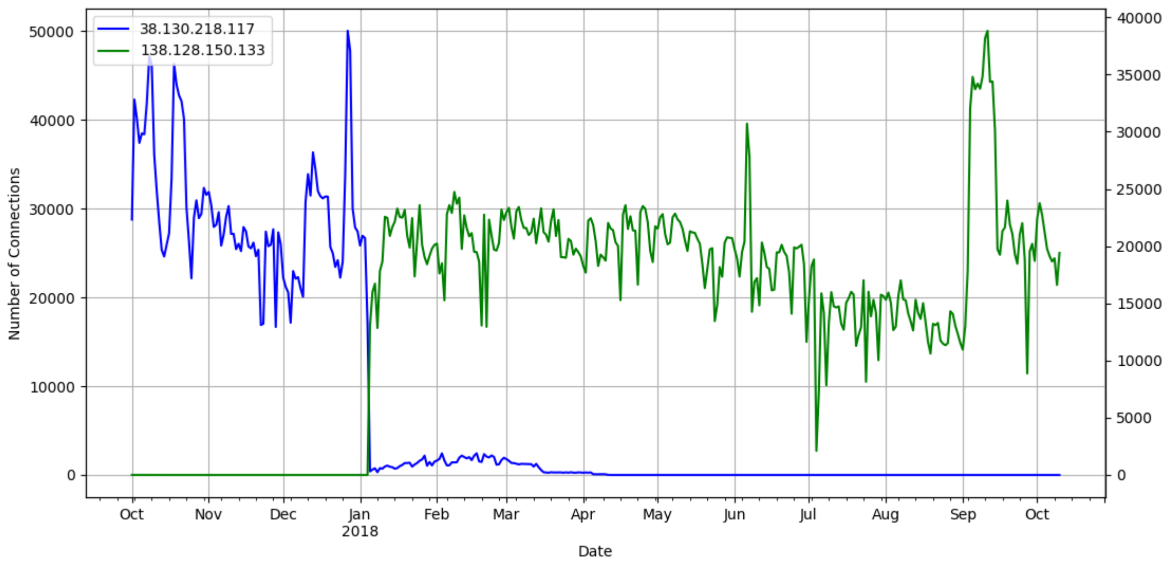
The malware connects to this downloader IP and executes the downloaded file. The two files we saw in the C2 response were PE32 executables. These downloaded files appear to be modified quite frequently. While the sizes are always the same, we observed that the file hashes change approximately every 30 minutes. We have included the below hashes as examples for further industry analysis.

```
winme.gif (267776 bytes)
4ca8ef5d00bde49659ca97faf2a2a47445e6a3e82c151f18f0923392826d5af0

winext.gif (180224 bytes)
b7245ed896cd4199b410a326e1295aafb3e23c3311d301b1cdaf964cf7c008d9
```

Through collaboration with Kurt Baumgartner at Kaspersky Lab, we believe we can positively identify the second stage payload as the information stealing Khalesi malware. Using a graph analysis technique to find IPs of interest that communicated with a large number of bots, we were able to identify two downloaders. One of the downloaders, 138.128.150.133, is currently very active and was also the one contained in the response we decoded from the C2. VirusTotal confirms this IP as a malware distribution host. All the URLs associated to this IP have similar names to the ones above ending in .gif and are flagged as Khalesi or Zusy malware. This behavior appears as far back as April.

The other downloader, 38.130.218.117, was active until the beginning of the year. The plot below shows the number of connections to both, with a clear transition of infrastructure occurring at the beginning of the year.



By combining different data sources, such as DNS and Netflow, and using unsupervised clustering and graph analysis techniques, CenturyLink Threat Research Labs has been able to track the bots, C2s and downloaders for the Mylobot botnet. This analysis, performed without access to specific malware samples shows the power that network forensics can play in tracking malicious infrastructure. CenturyLink has blocked this infrastructure on our network to mitigate risk to our customers and notified the owners of any components operating within their environments to clean up and protect the global internet.

For a full list of IOCs such as the C2 domains and IPs, the downloader IP and the file hashes, please visit our GitHub page.

CybersecurityLumen

BLACK LOTUS LABS®

Author

Black Lotus Labs

The mission of Black Lotus Labs is to leverage our network visibility to help protect customers and keep the internet clean.

Trending Now

You may also like

Services not available everywhere. ©2022 Lumen Technologies. All Rights Reserved.