Visualizing QakBot Infrastructure

team-cymru.com/post/visualizing-qakbot-infrastructure

S2 Research Team

May 16, 2023

A Data-Driven Approach based on Analysis of Network Telemetry

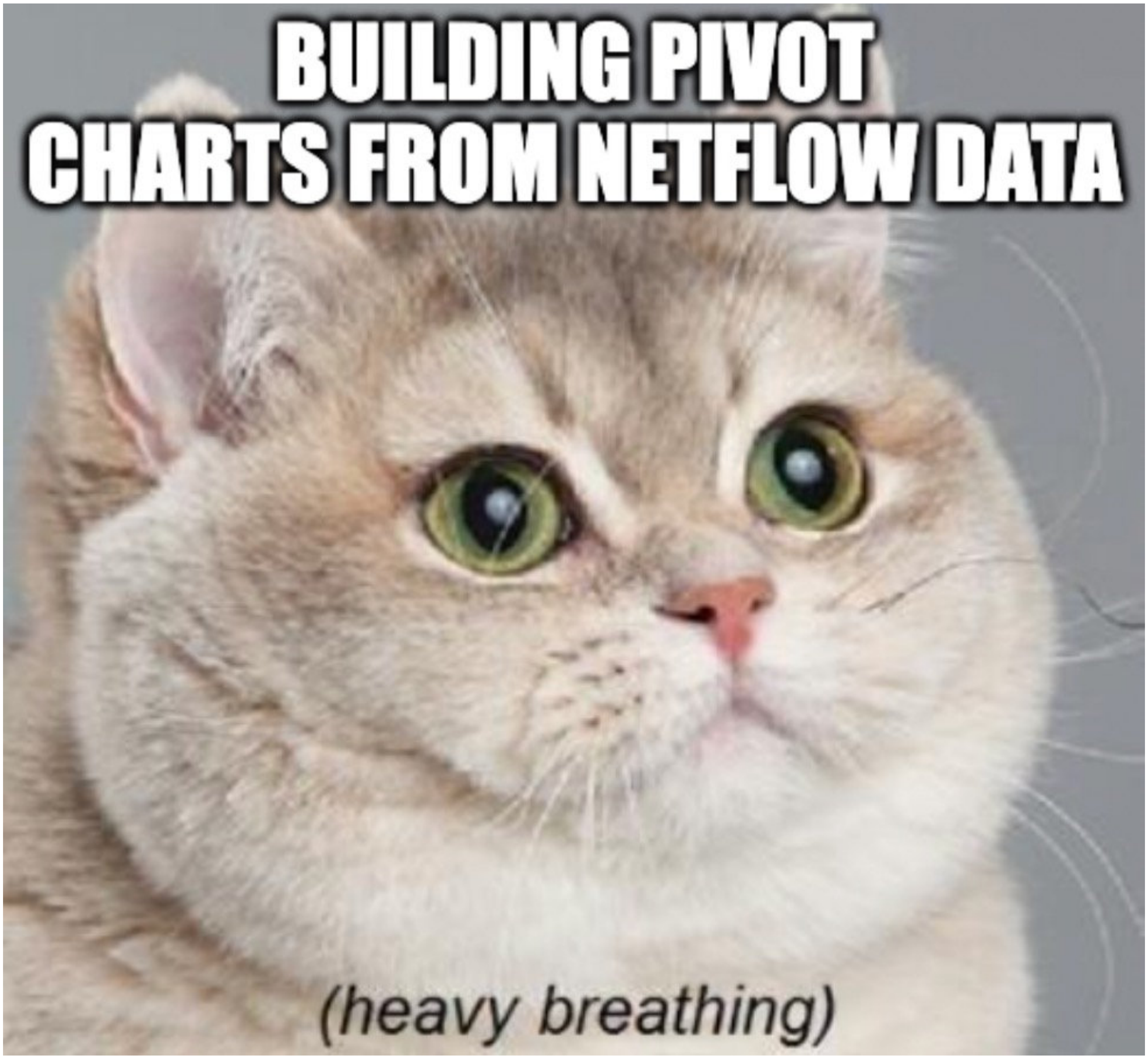
This blog post seeks to draw out some high-level trends and anomalies based on our ongoing tracking of QakBot command and control (C2) infrastructure. By looking at the data with a broader scope, we hope to supplement other research into this particular threat family, which in general focuses on specific infrastructure elements; e.g., daily alerting on active C2 servers.

This blog represents an ongoing piece of research, our analysis of QakBot is fluid with various hypotheses being identified and tested. As and when we uncover new insights into QakBot campaigns we will seek to provide further written updates.

We are not going to go over the entire history and functionality of Qakbot, for which there are numerous, well written reports on the subject. However, there are a couple of details relevant for this analysis worth mentioning.

1. Qakbot campaigns are tracked by the threat actors via affiliate IDs that are included in the malware configurations, at present the most active are “Obama” and “BB”.
2. Whilst each malware configuration includes a list of around 100 to 150 potential C2s, only a fraction are actually used for bot communications.

Refill your coffee and get comfortable, things are about to get data heavy.



Key Findings

- QakBot C2 servers are not separated by affiliate ID.
- QakBot C2 servers from older configurations continue to communicate with upstream C2 servers months after being used in campaigns.
- Identification of three upstream C2 servers located in Russia, two of which behave similarly based on network telemetry patterns and the geolocations of the bot C2s communicating with them.
- When one upstream C2 server goes down for a period of time, other upstream C2 servers see a spike in C2 traffic volume.
- The majority of Qakbot bot C2 servers are likely compromised hosts that were purchased from a third-party. Based on our data, most of these compromised hosts are located in India.

Active C2 Servers

By analyzing outbound connections from known victim-facing C2 servers, we are able to determine upstream management (Tier 2) infrastructure based on communications with common peers. In most cases a particular management port is utilized and generally communications are 'ongoing' for extended periods.

Once this Tier 2 (T2) management layer is identified, we are able to further determine which victim-facing C2 servers are currently active, based on the observation of connections to this T2 layer.

This is a family agnostic process, not limited to QakBot C2 infrastructure.

In the case of Qakbot, C2 servers from campaigns associated with the affiliate IDs "Obama" and "BB" have been communicating with the same three upstream Russian T2 servers over TCP/443 for months.

Russian IP space is often used in higher tiers of botnet infrastructure due to the protection it offers against (non-Russian) LEA activity and researcher visibility. It is a bit of a catch-22, however, since repeated outbound connections to Russian IP space from source IPs located in various random countries tend to stand out as anomalous, or at least, of interest.

Using C2 configuration data from April 2023 QakBot campaigns, we confirmed that the upstream Russian T2 servers remained unchanged. We then sifted through all of the C2 servers to identify those that connected to them over TCP/443. Interestingly, most of the C2 servers with this upstream traffic were listed in configurations from both Obama and BB campaigns. Five IPs were unique to Obama campaigns, and only one was unique to BB within this timeframe (specifically BB23 with campaign ID 1681114726).

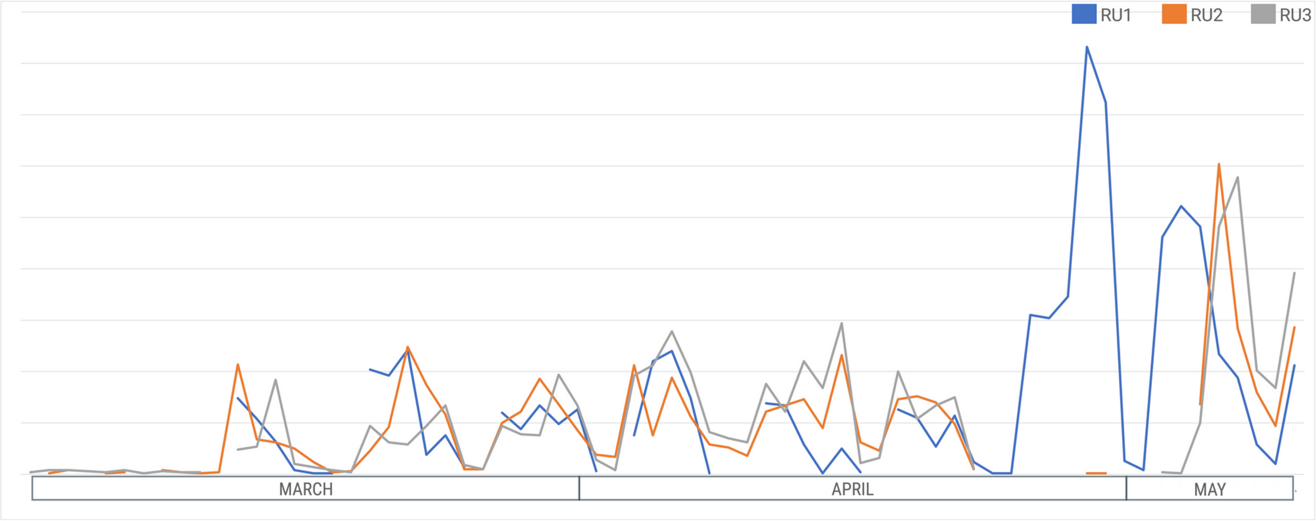
Obama & BB Obama BB

23.30.22.225	59.153.96.4	174.171.130.96
23.30.173.133	73.22.121.210	
27.0.48.233	119.82.121.251	
27.109.19.90	189.151.95.176	
43.243.215.206	197.94.95.20	
43.243.215.210		
69.242.31.249		
73.36.196.11		
73.161.176.218		
74.92.243.115		
75.149.21.157		
76.16.49.134		
96.87.28.170		
98.37.25.99		
103.42.86.42		
103.111.70.66		
103.113.68.33		
103.123.223.130		
103.123.223.141		
103.212.19.254		
114.143.176.235		
119.82.120.15		
119.82.123.160		
157.119.85.203		
183.87.163.165		
197.94.78.32		
202.142.98.62		

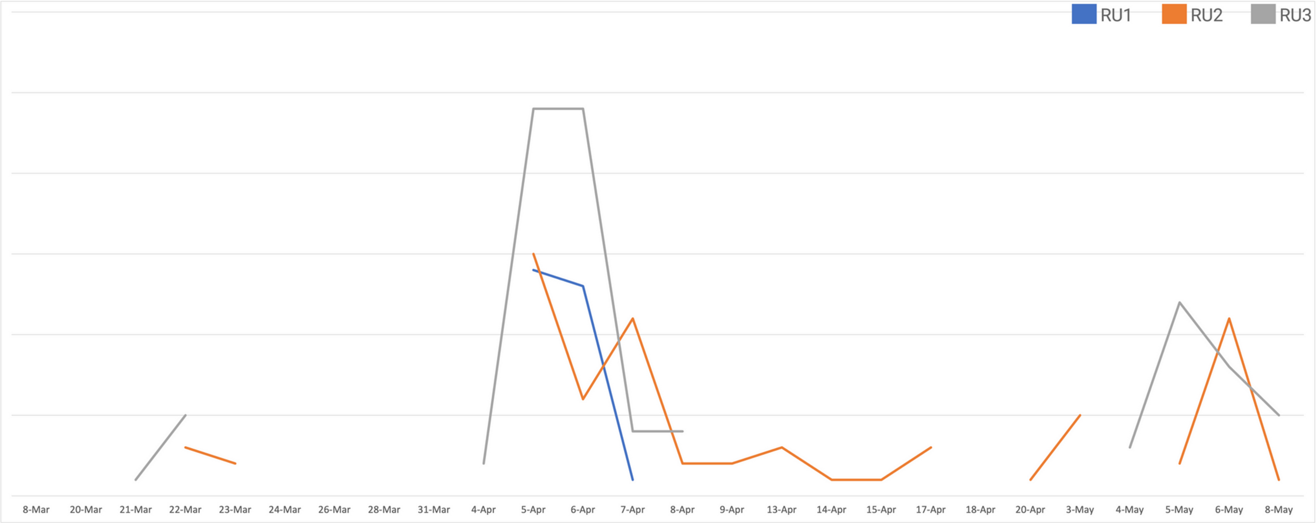
Bot C2s to Upstream T2s

The graphs below display the volume of traffic flows from 1 March to 8 May 2023 for the active C2 servers identified above, categorized by the affiliate configurations they appeared in. Each color represents one of the upstream Russian IPs, referred to as RU1, RU2, and RU3.

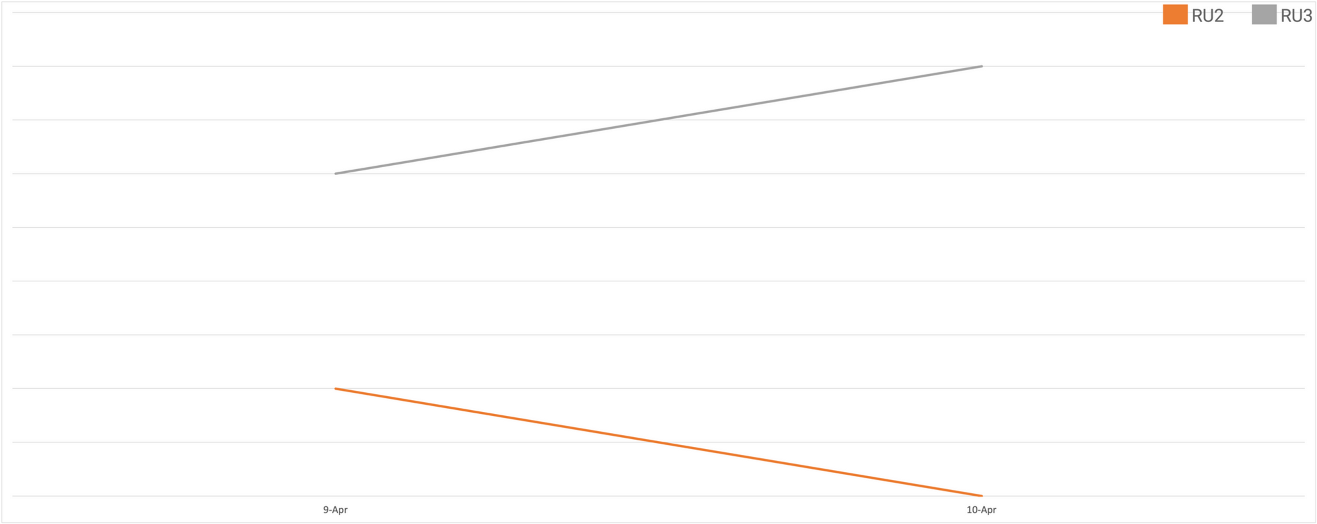
April C2 servers present in both Obama and BB campaigns



April C2 servers only present in Obama campaigns



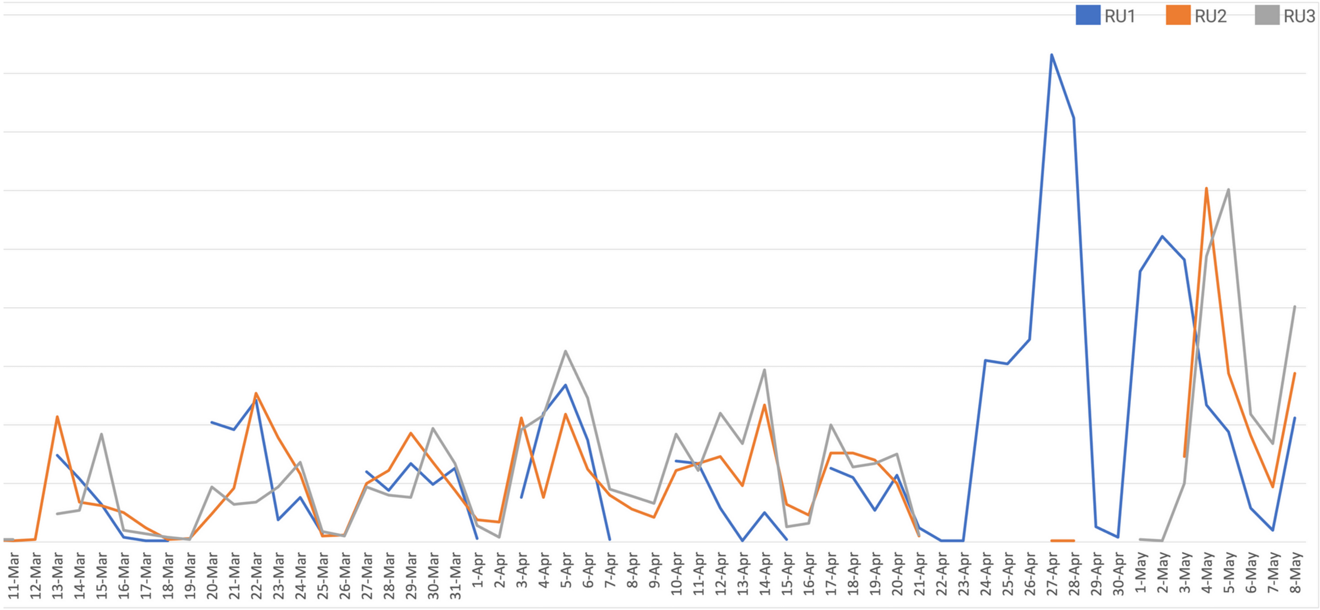
April C2 servers only present in BB campaigns



In general, the affiliates do not seem to be separated by the upstream infrastructure with which their C2 servers communicate. However, there are some exceptions. For instance, a single unique BB C2 was live for two days and mostly communicated with RU3, with one connection to RU2 on the first day. C2s from the Obama campaigns primarily communicated with RU2 and RU3, although there were a few interactions with RU1 in early April.

In April, there seems to be a gap in activity for RU2 and RU3. To gain a clearer understanding of the overall C2 to T2 traffic volumes, it is necessary to combine all active C2s from April, regardless of affiliation.

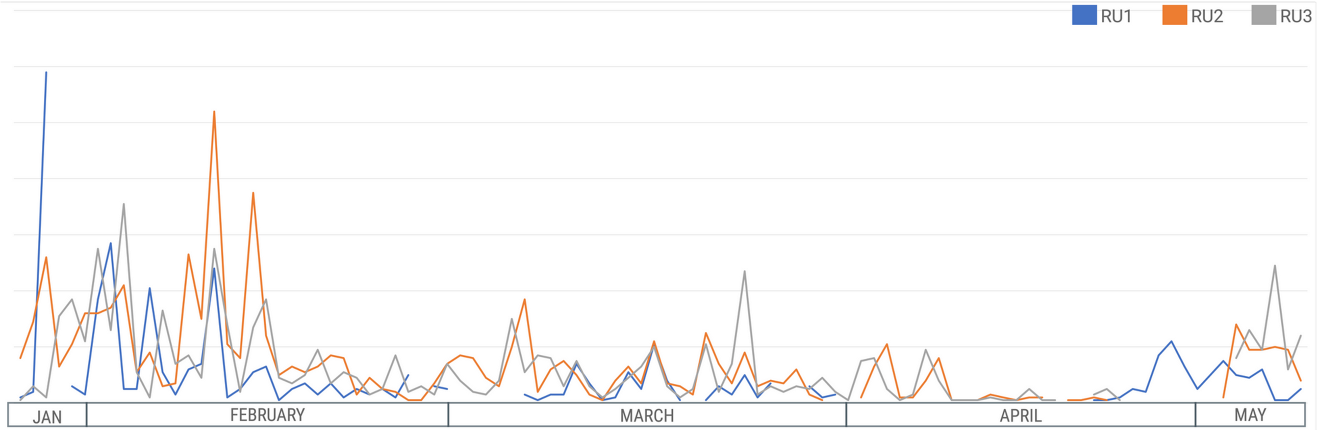
All April C2 Servers



RU2 and RU3 exhibit similar patterns to each other, while RU1 follows a separate pattern. Traffic volumes consistently decrease over weekends for all three, a trend commonly observed in e-crime infrastructure. Interestingly, RU2 and RU3 were nearly inactive from 21 April until 1 May 2023. Upon resuming activity, C2 communication over TCP/443 spiked to levels twice as high as before the period of inactivity. During the inactivity period, there was a significant surge in traffic volume to RU1. However, just before the return of RU2 and RU3 in early May, the traffic volume to RU1 reduced to roughly match their volume patterns.

Many C2 servers from this timeframe became active around mid-March and increased their activity beyond April. For comparison, the graph below includes all other confirmed or high confidence C2 servers that communicated with the Russian IPs over TCP/443 since 26 January 2023 (but were not included in April campaigns).

C2 Servers First Active Prior to April 2023



These previous C2 servers experienced spikes in activity, presumably when they were included in malware configurations, as observed with the C2 servers identified as active during April 2023. Subsequently, the traffic volume of these previous C2 servers significantly decreased but remained active.

In a future blog post, we will revisit this topic and explore the timelines of C2 servers and the relationships between affiliates.

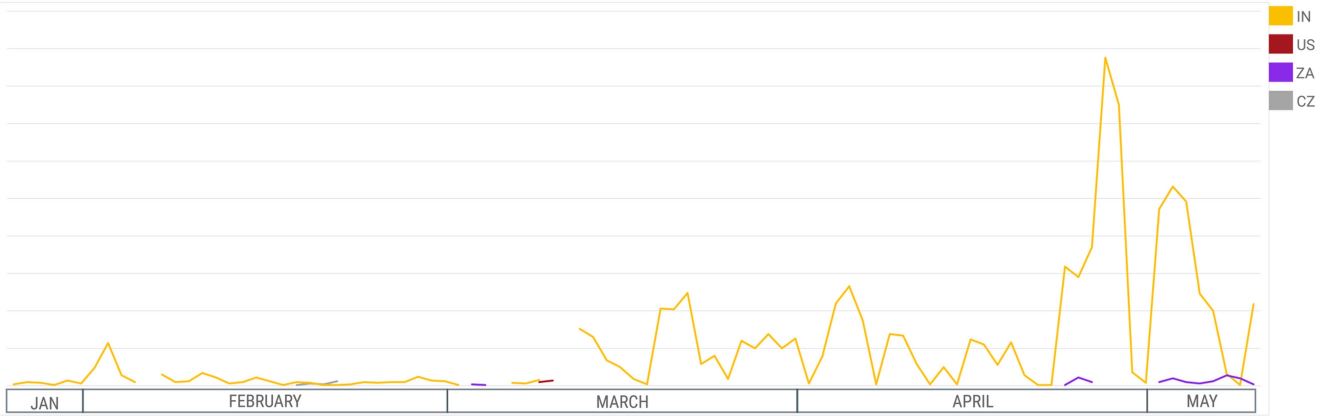
From this perspective, there are fewer similarities between RU2 and RU3, although they still share more alignment than with RU1. It also appears there have been previous periods of inactivity when C2 servers ceased communicating with an upstream Russian IP, as observed with RU1 from 25 February to 6 March 2023. These older C2 servers also stopped communicating with RU1 for approximately three weeks from the end of March through April, but they resumed connections on 19 April 2023. C2 servers included in April campaigns continued to communicate with RU1 during this period.

Telemetry by IP Geolocation

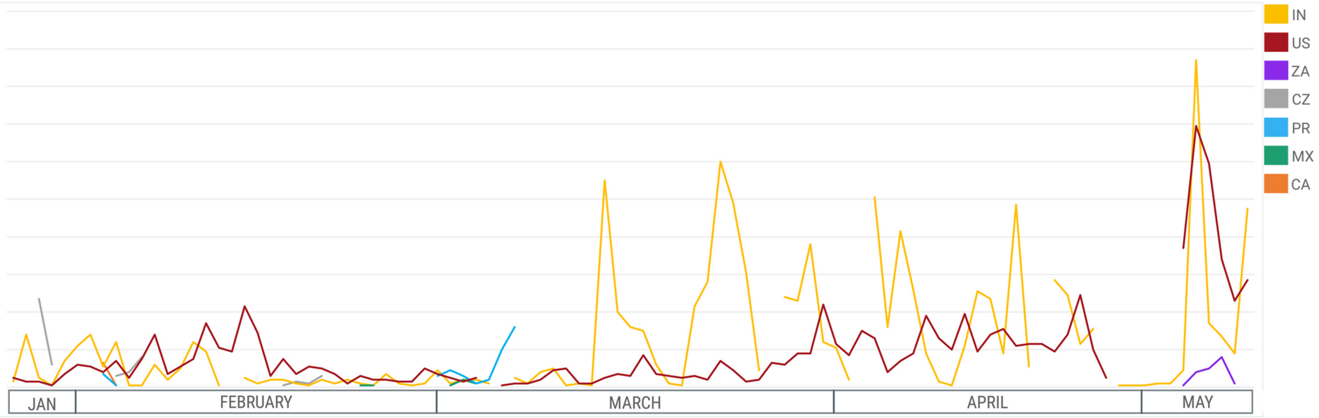
There appears to be a potential relationship between RU2 and RU3 based on the April C2 traffic volume patterns. Hypothesizing from Qakbot's intermittent use of geofencing payloads, perhaps this relationship is influenced by geolocation. The following comparison shows confirmed and high confidence C2s, active between 26 January and 8 May 2023, categorized by geolocation for each of the three Russian T2s.

This section is caveated by the potential for observation bias. Team Cymru's global coverage varies from region to region, and from day to day based on sampling rates and data volumes.

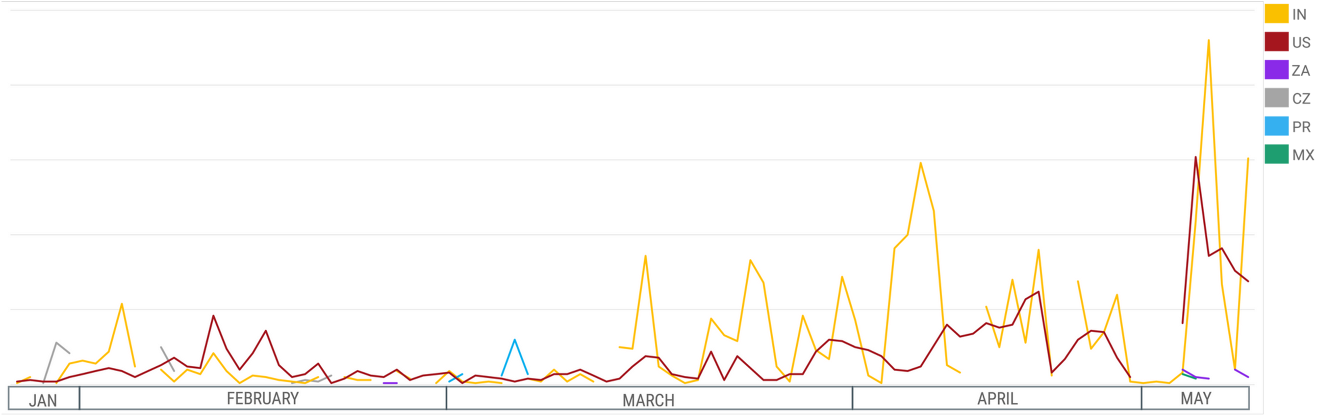
RU1



RU2



RU3



The volume and diversity of C2s for all three Russian T2s changed their patterns around the second week of March, with increased activity for India (IN) and United States (US) located IPs, and a decrease in the number of different GEOs with active C2 servers. RU2 and RU3 once again exhibit similar patterns and receive traffic from all US-based C2 servers, as well as C2s from other North American locations not observed with RU1.

During this timeframe, RU1 showed less diversity compared to RU2 and RU3, predominantly utilizing hosts located in India. There were only two short periods in February and March when US and Czech Republic (CZ) C2 servers connected to RU1.

The CZ hosts were seen communicating with all three T2s around the same time period in February. More recently, hosts geo-tagged as South African (ZA) have started communicating with all three T2s, but most consistently connect to RU1.

One last thing to note: Qakbot C2 servers are historically compromised machines, either purchased from third parties or infected and turned into bots (although the latter is less common). Combining the above information into one graph reveals that starting in March, India is by far the most prevalent country for active Qakbot C2s. These compromised machines are most likely purchased from a broker serving the e-crime community.

Conclusion

This analysis provides a recent snapshot of the Qakbot infrastructure, highlighting observed trends and anomalies. By visualizing this data through line charts, we have uncovered intriguing insights into the inner workings of Qakbot's infrastructure. While the data can be utilized to identify potential threats and implement proactive measures, the primary focus of this post is to highlight the interesting data points that can be uncovered through network telemetry analysis. By leveraging these insights, readers can gain a deeper understanding of the tactics and strategies employed by cybercriminals to carry out their attacks.

Recommendations

- We recommend that the IOCs listed at the end of this blog post are used by cyber defenders to hunt for existing QakBot infections, as well as in blocking future attacks.
- For users of Pure Signal™ Recon and Scout, the aforementioned Russian T2 servers are identifiable by querying against the IOC list; filtering on outbound connections to remote TCP/443.
- Pivoting on inbound connections to the Russian T2 servers will illuminate new QakBot C2 infrastructure over time.

Indicators of Compromise

Below are the confirmed Qakbot bot C2 servers that we have identified communicating with upstream T2 infrastructure over TCP/443 this year.

23.30.22.225

23.30.173.133

24.9.220.167

27.0.48.205

27.0.48.233

27.109.19.90

43.243.215.206

43.243.215.210

59.153.96.4

64.237.207.9

64.237.212.162

64.237.221.254

64.237.245.195

64.237.251.199

67.187.130.101

68.62.199.70

69.242.31.249

73.22.121.210

73.29.92.128

73.36.196.11

73.60.227.230

73.78.215.104

73.88.173.113

73.155.10.79

73.161.176.218

73.161.178.173

73.165.119.20

73.215.22.78

73.223.248.31

73.228.158.175

73.230.28.7

74.92.243.113

74.92.243.115

74.93.148.97

75.149.21.157

76.16.49.134

76.27.40.189

89.203.252.238

96.87.28.170

98.37.25.99

98.159.33.25

98.222.212.149

99.251.67.229

99.252.190.205

99.254.167.145

103.11.80.148

103.12.133.134

103.42.86.42

103.42.86.110

103.42.86.238

103.42.86.246

103.71.20.249

103.71.21.107

103.87.128.228

103.111.70.66

103.111.70.115

103.113.68.33

103.123.221.16

103.123.223.76

103.123.223.121

103.123.223.130

103.123.223.131

103.123.223.132

103.123.223.141

103.123.223.144

103.123.223.168

103.123.223.171

103.212.19.254

103.231.216.238

103.252.7.228

103.252.7.231

103.252.7.238

109.49.47.10

114.143.176.234

114.143.176.235

117.248.109.38

119.82.120.15

119.82.120.175

119.82.121.87

119.82.121.251

119.82.122.226

119.82.123.160

157.119.85.203

174.58.146.57

174.171.10.179

174.171.130.96

180.151.104.240

180.151.108.14

183.82.107.190

183.82.112.209

183.87.163.165

183.87.192.196

189.151.95.176

197.92.136.122

197.94.78.32

197.94.95.20

201.130.119.176

201.142.195.172

201.142.207.183

201.142.213.13

202.142.98.62