Visualizing Qakbot Infrastructure Part II: Uncharted Territory

By Team Cymru

Published: 2025-04-08 · Archived: 2026-04-05 15:51:59 UTC

A Data-Driven Approach Based on Analysis of Network Telemetry

In this blog post, we will provide an update on our high-level analysis of QakBot infrastructure, following on from our previous blog post. We will pick up the timeline from where we left it, basing our findings on data collected between 1 May and 20 July 2023.

We have continued to focus on elements and trends for which we do not observe in regular commentary; specifically the relationship between victim-facing command and control (C2) infrastructure and upstream servers, we previously referenced these as being geolocated in Russia.

As with our previous blog, this 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 welcome feedback and comment via our Twitter page on the hypotheses mentioned in this post; broadly our findings represent the benefits and challenges of working with NetFlow data - whilst we can form broad conclusions, these are sometimes open to interpretation. Confirmation and contradiction are both of value to us as we continue to understand this threat operation.

Key Findings

- C2 activity around both victim and upstream T2 communication slowed down before spamming ended around 22 June. After spamming ceased, C2 activity continued albeit at a lower volume.
- 15 new C2s set up after spamming ended have been identified so far. Additionally, the number of existing C2s communicating with the T2 layer significantly decreased with only 8 remaining past 22 June.
- We've observed interesting outbound activity from the T2 layer, targeting both publicly reported and suspected Qakbot C2s, as well as other undefined destinations.
    - The T2 C2s connect to the same list of ports used in the process for deploying the Qakbot proxy module, with usually only one or two ports observed in a day.
    - Although the volume of connections, variety of destinations, and port usage appear random, over time the destination ports are used with relatively equal frequency.
- During the first half of 2023, port 443 was assigned to approximately 48% of the C2s extracted from Qakbot campaigns. Among those C2s, only a subset engaged in communication with the T2 layer. Within this subset, 80% were assigned port 443, making it the predominant port for communication between victims and C2s.
- C2s are usually compromised hosts in residential IPs space, as are the other destination IPs identified from outbound T2 connections. Additional criteria like geolocation and AS organization may influence the

selection of these hosts, guiding the purchase from third parties and determining which Qakbot victims become bot C2s or used for other operator activity.

Summer Glow Up

Qakbot has a history of taking an extended break each summer before returning sometime in September, with this year's spamming activities ceasing around 22 June 2023. But are the QakBot operators actually on vacation when they aren't spamming, or is this "break" a time for them to refine and update their infrastructure and tools? It's worth considering that the summer months might offer a unique opportunity for operational work, especially when their main targets in the Northern Hemisphere are often on some form of holiday, leading to a potential decline in the success rate of their attacks during this time.

The line graph below shows the volume of connections from C2s over TCP/443 to the three Tier 2 (T2) IPs geolocated in Russia.

In our previous blog post, we referred to the three T2s as RU1, RU2, and RU3. Since then, the IPs have been made public so we have included them in some of the legends accompanying the charts below. However, for the sake of simplicity and continuity, we will continue to refer to them collectively as RU* within this post.

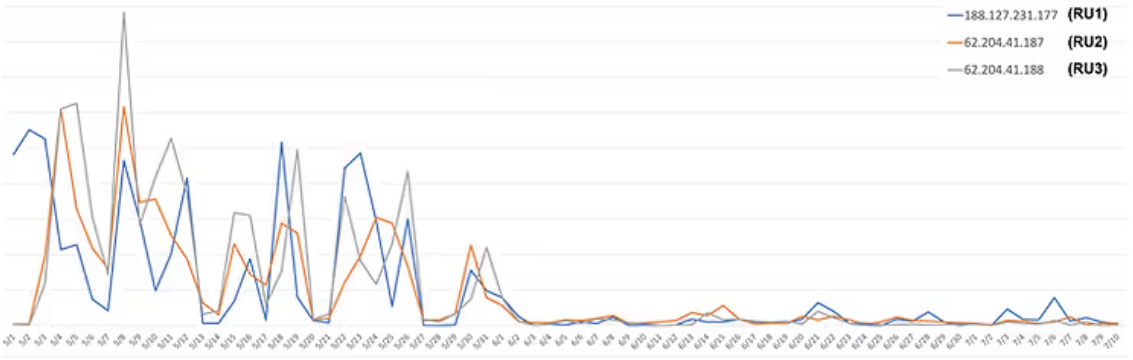


Figure 1: Volume of bot C2s connections with the T2 layer (RU1, RU2, RU3) over TCP/443

After a very busy May, things began to slowly wind down at the end of the month before a sudden drop in connections to the T2 in early June, even though spamming continued for three more weeks until around 22 June. We were unable to identify any new T2s after this decline in activity, though traffic from some C2s persisted, suggesting that the T2 infrastructure remained unchanged. However, it wouldn't be surprising if fresh IPs for the T2 layer are introduced before their anticipated return in late summer.

After this drop-off, a slight spike was observed on 21 and 22 June, the last day of pre-summer mass spamming (affiliate ID obama271). Interestingly, a few more spikes occurred after this period, which we will explore further.

The graph below represents the volume of bot C2 to T2 traffic according to C2 geolocation:

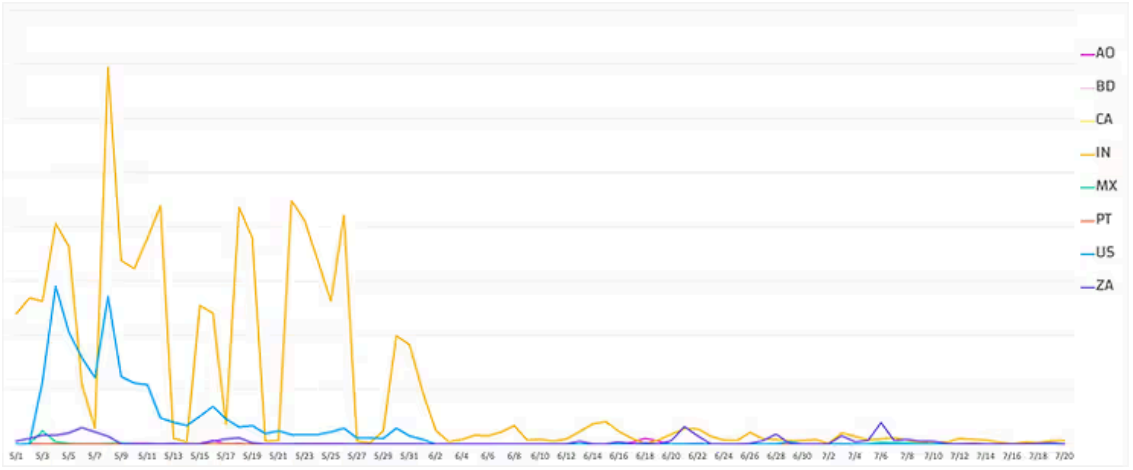


Figure 2: Volume of bot C2 to T2 traffic per geolocation (of C2s) for 1 May through 20 July

From this perspective, we observe that on 2 June, US C2s all but disappeared, and traffic from Indian C2s significantly decreased. We suspect the lack of US activity is at least partially attributable to Lumen's Black Lotus Labs null-routing the T2 layer in their networks, as noted in their recent blog post.

For curiosity's sake, let's quickly examine data for traffic volume and timing from the perspective of likely QakBot victim to C2 communications during the same time frame:

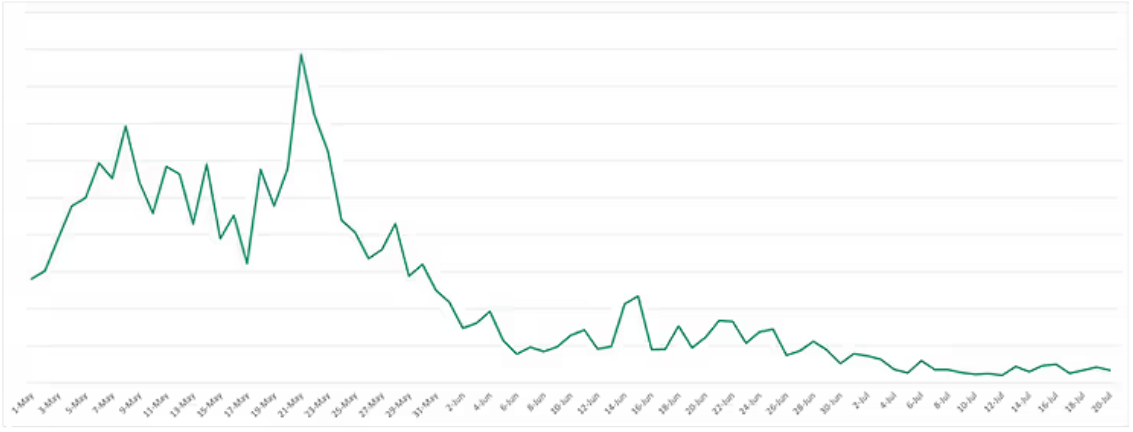


Figure 3: Volume of inbound connections to C2s from hosts that are likely infected with Qakbot

As was the case with C2 to T2 communications, we can see a winding down of activity at the end of May, however this does not drop off as suddenly at the beginning of June. Instead, victim to C2 communications appear to gradually reduce in volume up to and beyond the date QakBot ceased spamming operations (22 June).

Turning back to C2 to T2 activity, the following graph is a zoomed-in view of June onward, highlighting the start of a considerable drop in activity that persists through July.

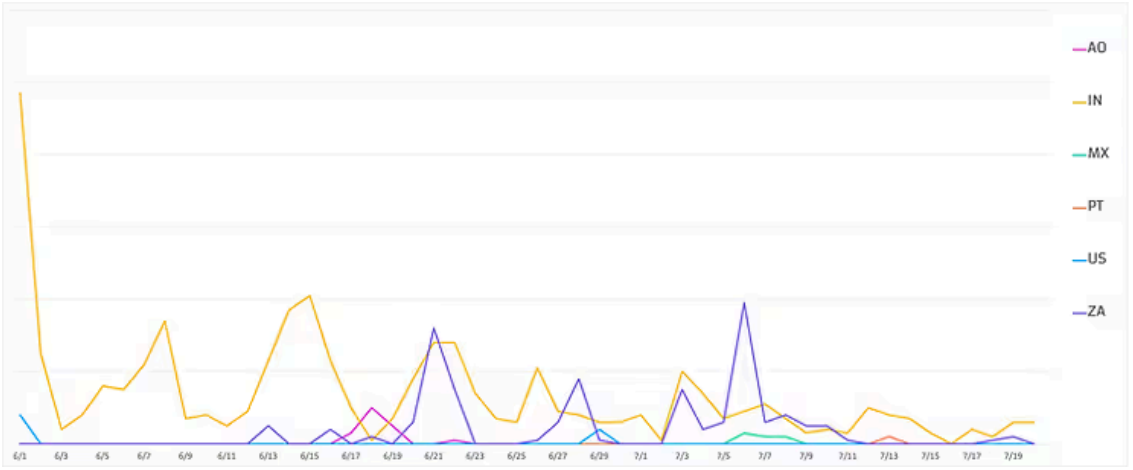


Figure 4: Volume of bot C2 to T2 traffic per geolocation (of C2s) for 1 June through 20 July

According to our data, a lull lasted from 2 June to 12 June, during which only Indian C2s communicated upstream, albeit at a drastically reduced volume compared to May. We also noted some spikes in traffic from South African C2s.

We examined the IPs from the geolocations present during this timeframe to determine whether these were legacy C2s with sporadic bursts of activity, or new C2s being incorporated into their infrastructure.

Our analysis revealed:

- Fifteen new C2s were set up since Qakbot ceased spamming, indicated by a green box in the timeline below.
- Six additional C2s, active since before June (some dating back to October and December 2022), that continued to exhibit upstream activity after spamming concluded, indicated by a blue box in the timeline below.
- Two C2s, new in June, that also maintained activity after spamming concluded, indicated by an orange box in the timeline below.

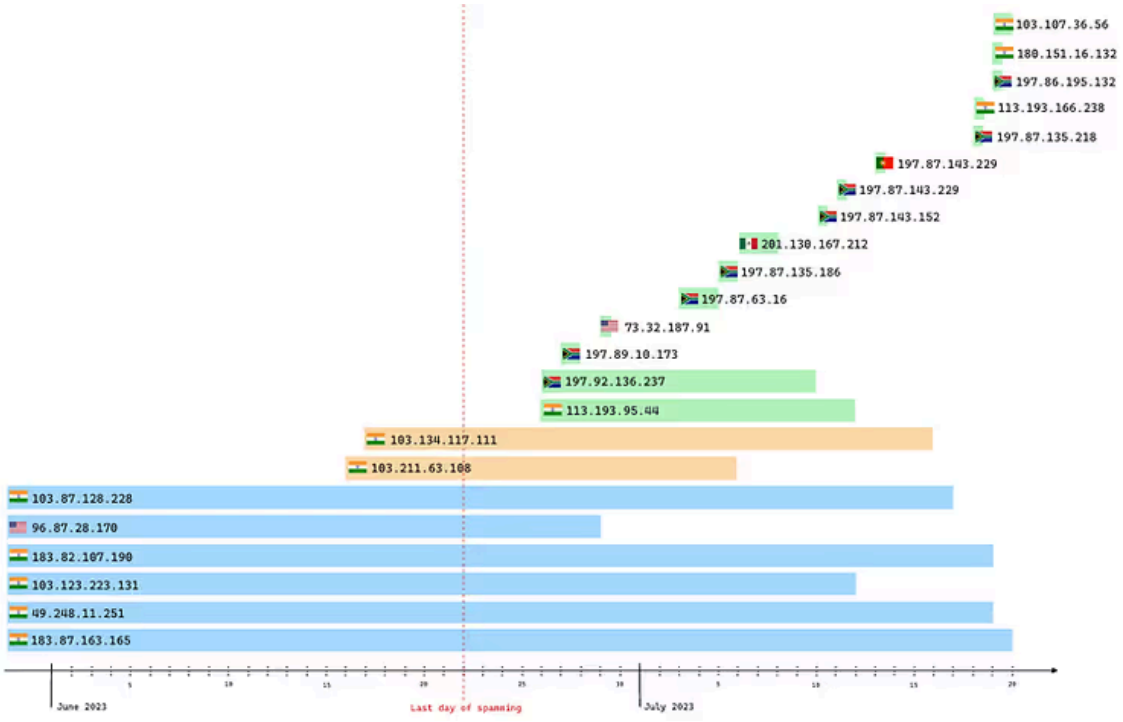


Figure 5: Timeline of most recent reported and suspected Qakbot C2s

We suspect that the IPs in the above timeline represent new and existing C2s intended for use upon Qakbot's return post-summer glow up break. Most of the C2s established after spamming ceased have only a few connections to the T2 and for brief durations, possibly indicative of C2s that are not currently active but were prepared or primed for future spamming.

We will continue monitoring Qakbot during their summer break for any signs of changes in their infrastructure or how they operate.

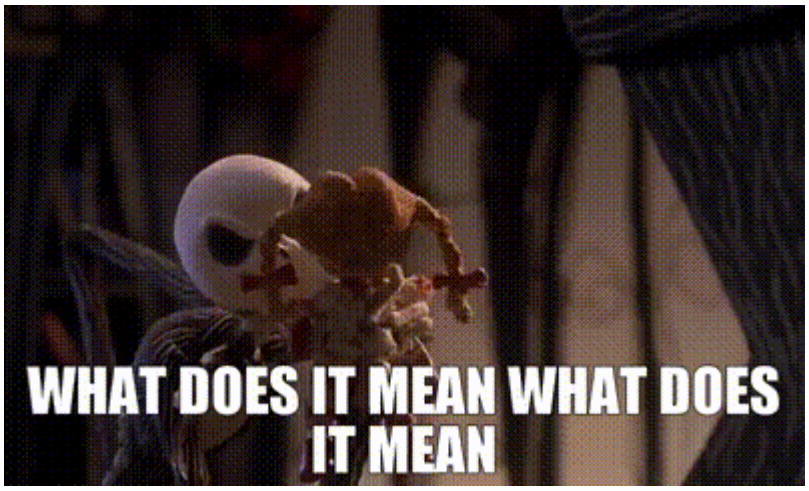
The Mystery of the Outbound Tier 2 Connections

Whilst examining NetFlow data for the C2 to T2 communications from which we derived the findings described above, we kept making the same unexpected observation. A clear pattern of communications sourced from the T2s, where QakBot C2s were the destination, i.e., the reverse of the traffic we were examining. These communications occurred over the same 32 ports: 20, 21, 22, 53, 80, 443, 465, 990, 993, 995, 1194, 2078, 2083, 2087, 2222, 3389, 6881, 6882, 6883, 8443, 32100, 32101, 32102, 32103, 50000, 50001, 50002, 50003, 50010, 61200, 61201, and 61202.

Malware such as Qakbot, IcedID, and Emotet leverage tiered infrastructure. This consists of victim hosts communicating with bot C2s, which comprise the Tier 1 layer of the bot infrastructure, which then communicate upstream with the T2 layer. The traffic typically continues to be proxied through additional tiers of infrastructure before it reaches the pane, which is accessed by the threat actors. Aside from subtle differences, for example the ports used, this process is essentially the same for the many malware families we track.

The traffic we have observed sourced from QakBot T2s to the C2 / Tier 1 layer is atypical. When we expand our dataset to look at all outbound traffic from the T2s, we establish a larger pool of 'T2 destination IPs'. As

mentioned, some of these T2 destination IPs are publicly reported QakBot C2s. However, in the majority of cases the T2 destination IPs have not previously been identified as malicious, although many share common host characteristics associated with QakBot C2s.



Let's begin by examining what we already know. Qakbot C2s utilize various ports as defined in their malware configurations. These are the ports that an infected host would use to communicate with the bot C2. Bot C2s are generally compromised machines, often including previous Qakbot victims that have been elevated to C2 status. Our findings for 2023 reveal that 52 different ports were employed for C2s within the Qakbot configurations, including many of the ports listed above. Based on this, it is possible that the T2s are conducting a form of check-in with the C2s, utilizing the ports designated for victim traffic.

We developed a second theory based on information provided in a fantastic writeup published a few years ago by Check Point Research, where they explored how a Qakbot-infected victim ultimately receives the proxy module. After the malware ensures incoming connections are allowed in the host firewall and port forwarding is enabled, it verifies incoming connections by sending a message to a bot, with confirmation based upon the response. The payload in this message contains a list of ports that match the same destination ports the T2s are using for the mysterious outbound connections, as shown in the excerpt below.

Figure 6: "An Old Bot's Nasty New Tricks: Exploring Qbot's Latest Attack Methods", Check Point Research, 2020

Mystery solved? Unfortunately no, it wasn't so simple. The activity that Check Point describes would appear differently in NetFlow data from what we are currently observing with respect to outbound T2 communications. Our investigation encompasses repeated connections over an extended time frame, interspersed with periods of inactivity. Usually, one to three of the T2s will sporadically reach out to the same destination IPs for months, and not in a manner that implies verification of a fixed list of available ports.

However, this information offers another possible explanation for the activity; the mysterious outbound connections from the T2s might be related in some way to the proxy module, given the identical port list. Spoiler alert, we believe this the most likely theory based on our analysis of the NetFlow data and information currently available to us, into which we will now delve deeper.

“You know my method. It is founded upon the observation of trifles.”

Sherlock Holmes

NetFlow Observations I: Reported vs Unidentified C2s

Examining the T2 destination IPs identified over a seven-month period, we discovered that only **29%** of all destination IPs were reported Qakbot C2s. Of these, **79%** also demonstrated typical upstream C2 to T2 bot communication over TCP/443. The remaining **71%** of destination IPs were not known as malicious, although **17%** of them did exhibit standard upstream C2 communication with the T2 over TCP/443.

To provide additional context for these and other data points discussed in this blog post, we compared the findings against both reported and unreported C2s. The unreported C2s were identified by monitoring communications to the T2s over TCP/443 during the same time period.

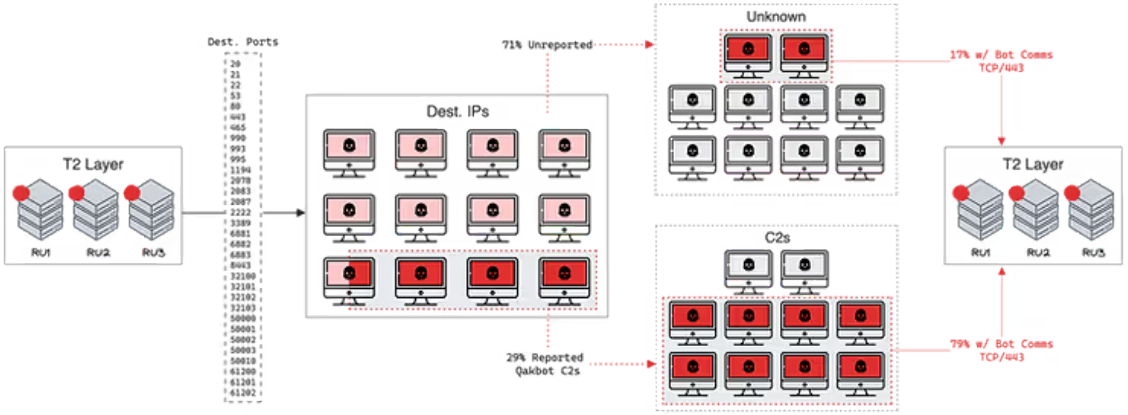


Figure 7: Percentages of T2 destination IPs that are Qakbot C2s, and of IPs with upstream T2 bot communication

Repeating the same process for analyzing bot C2 to T2 NetFlow data, we found that **76%** of all source IPs were recognized as Qakbot C2s. Of all the C2s, only **17%** had inbound connections from the T2, and within this subset, **65%** were publicly reported as Qakbot C2s.

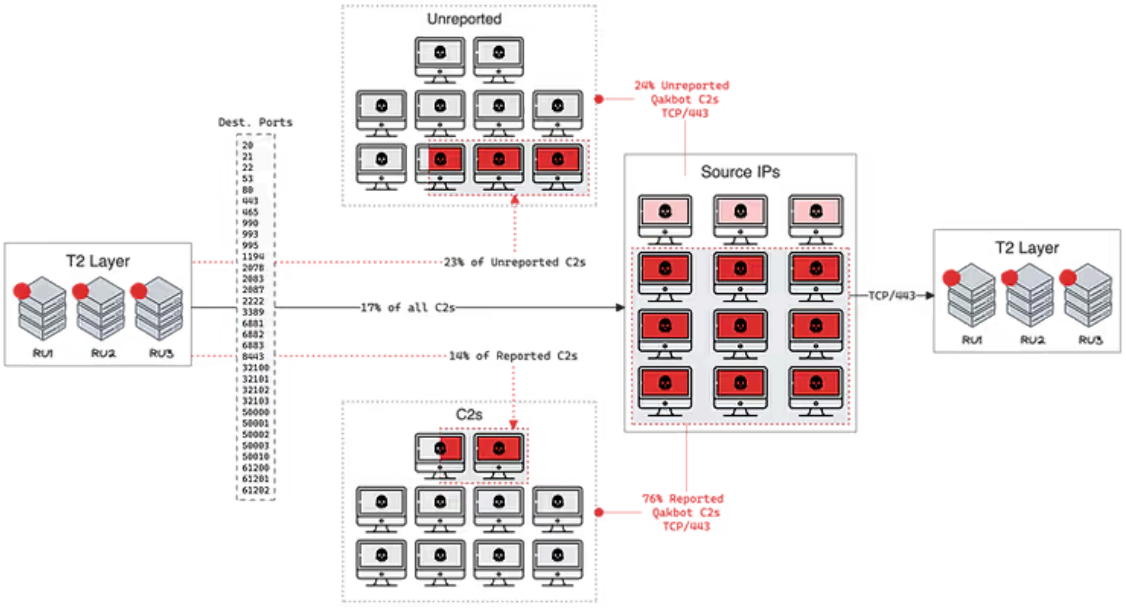


Figure 8: Percentages of reported and unreported C2s with typical upstream bot traffic, and of those that are also T2 destination IPs

In summary, only **29%** of the T2 destination IPs were verified as Qakbot C2s, as opposed to **76%** of the C2s exhibiting upstream T2 traffic. Consequently, over **70%** of the T2 destination IPs have *not* been observed in the wild as malicious. Furthermore, only **12%** of the T2 destination IPs displayed upstream T2 bot traffic typical of a normal C2 but were not identified in the wild as Qakbot C2s.

Based on these discrepancies, it seems improbable that the T2s are conducting any sort of management-related check-in for the bot C2s.

NetFlow Observations II: Traffic Volume

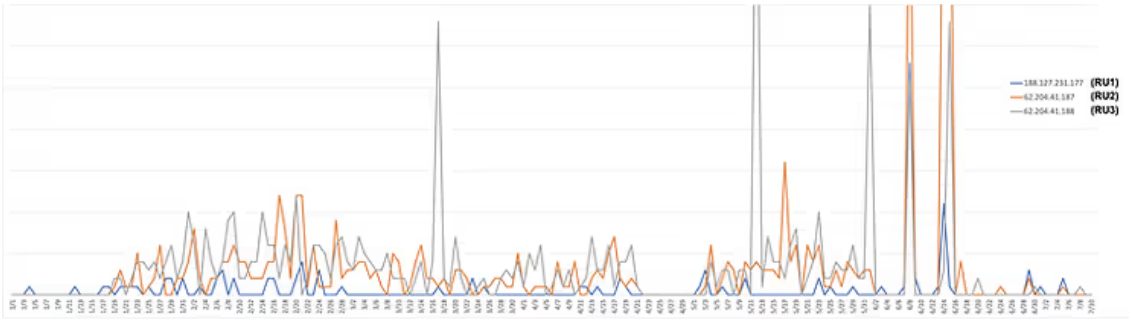


Figure 9: Line chart of traffic volume for outbound communication per T2 C2, spike outliers are cut off for legibility

Similar to the upstream bot C2 traffic we analyzed in our previous blog post, there are notable resemblances between **RU2** and **RU3** in terms of traffic volume and timing, and are also adjacent IP addresses associated with Horizon LLC (ASN 59425). In contrast, **RU1** belongs to IP space assigned to SmartApe (ASN 56694), and exhibits a lower overall traffic volume compared to the other two IPs. The timing of **RU1** activity generally occurs

independently of **RU2** and **RU3**, although there are occasions when all three simultaneously experience spikes in volume.

Next, we will present a comparison of all T2 outbound communication juxtaposed with typical C2 to T2 bot communication, irrespective of the T2 host.

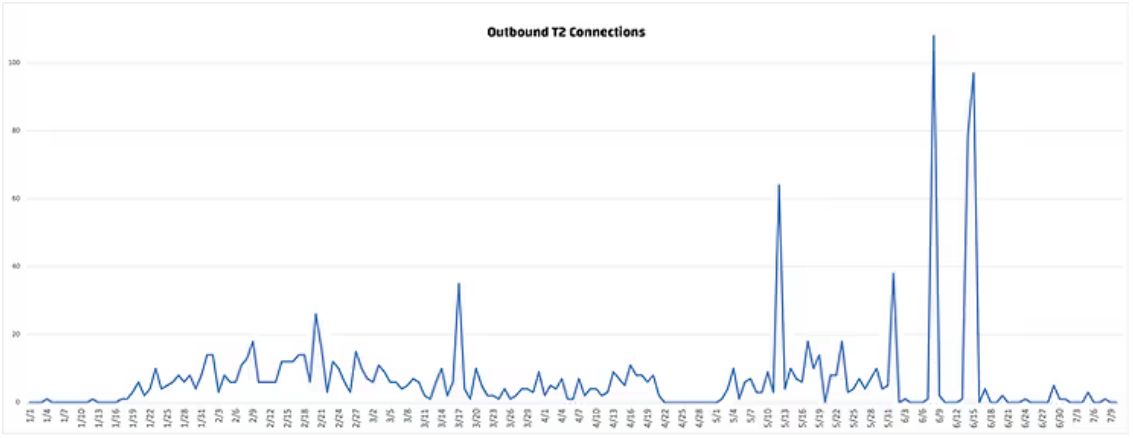


Figure 10: Volume of outbound connections from the T2 layer

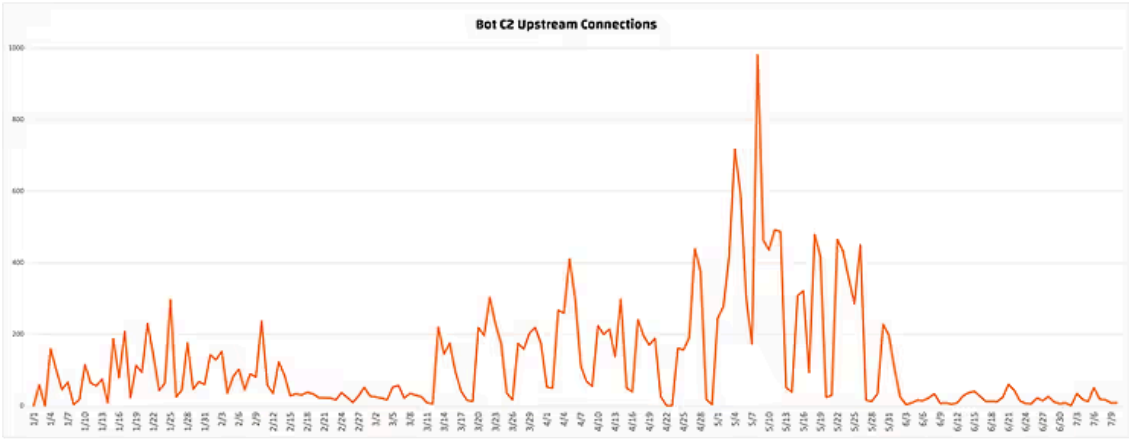


Figure 11: Volume of inbound connections to the T2 layer, from Qakbot bot C2s, over TCP/443

There are a few notable observations:

- The traffic volume for outbound T2 connections (blue) is markedly smaller than that of standard inbound bot C2 connections (orange). If they appeared on the same chart, the outbound T2 traffic would be virtually indiscernible when compared to the bot C2 traffic.
- Outbound T2 activity functions independently of inbound communication from C2s, meaning they do not happen concurrently.
- Instances of increased outbound T2 connections often occur following spikes in activity for inbound bot C2 connections
    - Spikes in outbound T2 connections frequently correspond with a decline in bot C2 activity.

Based on these findings, we hypothesize a connection between the volume and timing of bot C2 upstream activity and the outbound T2 activity we are investigating. Although there is minimal overlap between the groups of bot

C2s and T2 destination IPs, it seems that both forms of T2 activity occur in a sequential manner, contingent on traffic volume.

NetFlow Observations III: Port Usage Frequency

In Qakbot C2 configurations, many C2s (often exceeding 100) are present, but only a small subset have been observed communicating with the T2 layer in our data. Taking into account all C2s, regardless of T2 communication, we found that approximately 48% were assigned port 443, 29% port 2222, and 16% port 995. All other ports were allocated to fewer than 3% of C2s.

It's worth noting that for C2s we've identified communicating upstream over TCP/443, these percentages change; around 80% of C2s are assigned port 443, 9% port 995, 5% port 2078, and 4% port 2222. The remaining ports were associated with less than 1% of C2s.

In comparison, the chart below illustrates the frequency of destination ports utilized for outbound connections from the T2:

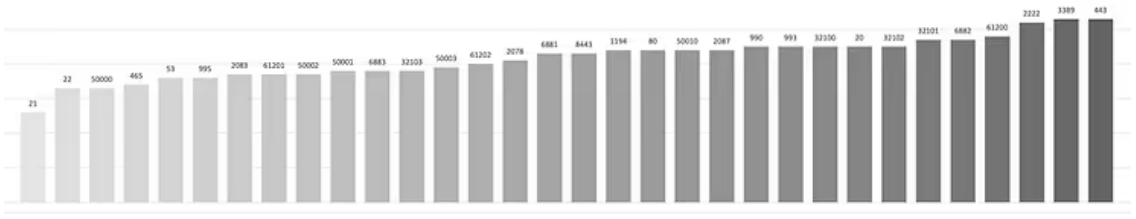


Figure 12: Frequency of ports used as destination ports in outbound T2 connections, since November 2022

Upon examination, it's immediately evident that there is no correlation between the two datasets regarding port usage frequency. Although port 443 was technically the most frequently utilized destination port for outbound T2 connections, its usage is far from the 48% seen with all reported bot C2s (regardless of T2 communication), and port 3389 was observed just as often. In fact, all of the 32 ports we identified with this type of communication were seen at roughly equivalent rates, with port 21 being the least common.

On its own, this data point might suggest some form of automation governing which ports are accessed. However, this inference alone is not sufficient. Incorporating the timing of when the ports are used in these connections could provide further insights into whether the process appears automated.

Our analysis focused on the period from May through 16 June, when activity gradually diminished to become almost nonexistent.

RU1

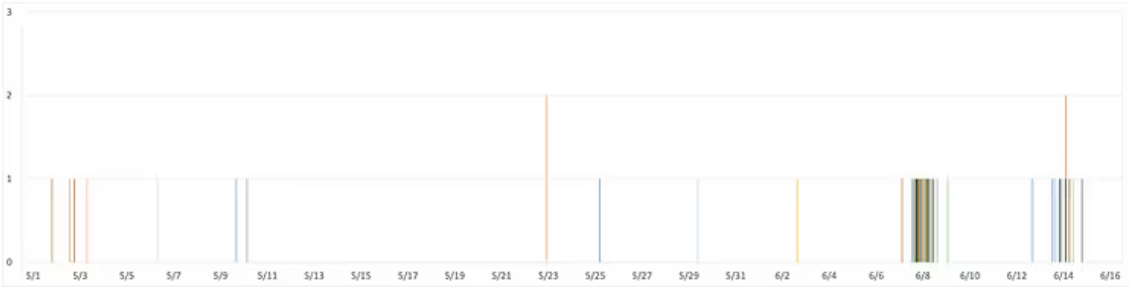


Figure 13: Destination ports identified in outbound connections per day from T2 188.127.231.177

RU2

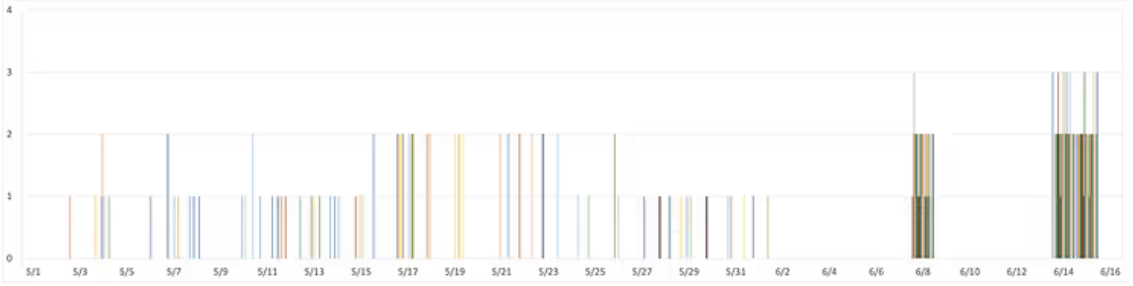


Figure 14: Destination ports identified in outbound connections per day from T2 62.204.41.187

RU3

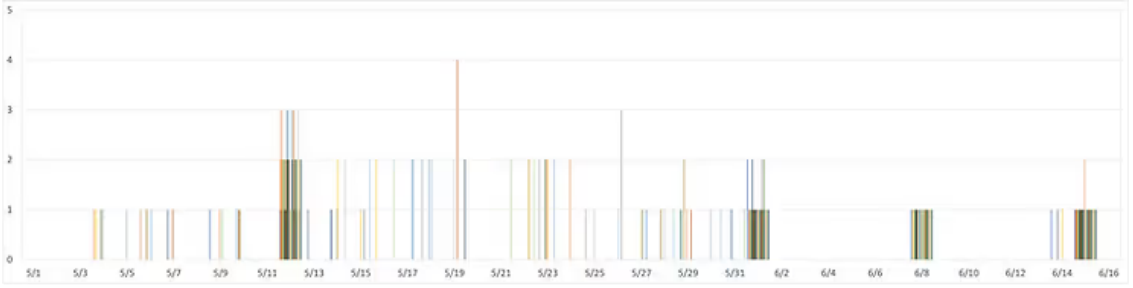


Figure 15: Destination ports identified in outbound connections per day from T2 62.204.41.188

This data may not be pretty, but fortunately, a detailed examination of the individual colored bars representing each port isn't essential to grasp the overarching trends of what's occurring. By viewing the visuals collectively, it's apparent that typically only a small number of ports are accessed in a single day, with usually just one or two destination IPs accessed via each port (y-axis). Interestingly, all of the T2 IPs have visually different patterns from this perspective, a finding that contradicts the general similarities observed between **RU2** and **RU3**. However, **RU2** and **RU3** do share a similar volume of ports seen per day compared to **RU1**.

Despite these variations, there are common patterns that all three hosts exhibit. For example, they all display consistent periods of inactivity, such as those occurring from May 1-2, June 4-6, and June 9-13. They also share some spikes related to the variety of different ports used for outbound connections within specific time frames, as seen on 8 June and the period around 14/15 June.

So far, we've determined that the T2 makes outbound connections over different ports at relatively the same frequency, with no one or two ports used far more or less than others. However, usually, only a few of the ports are seen in connections per day, and they seem to be chosen sporadically, with the exception of certain days when almost all of the ports are utilized. Regardless, over time, the T2s communicate across each of the 32 ports with a generally equal frequency.

What remains unclear is the rhythm or cadence of how often a T2 connects to each destination IP using these ports, and whether this process is automated. If blatant automation is involved, we would anticipate a pattern of repeated connections with consistent timing and volume. Behavior attributed to human intervention wouldn't be so orderly; instead, it would appear more random and unpredictable. While automation can be configured to mimic this, we can at least rule out the more evident instances.

To delve deeper, we chose a small sample of IPs that showed inbound T2 connections over an extended period and mapped out a timeline. In this illustration, each line color symbolizes a different T2 destination IP from the sample. A spike in a line indicates that at least one of the T2 C2s connected to that IP on that day, with the Y axis representing how many of the 32 destination ports were observed in those communications.

Figure 16: Volume and timing of inbound connections from the T2 for a sample of nine destination IPs

Examining the timing and volume of connections for each destination IP, there appears to be no evident pattern suggesting the use of automation. The T2 C2s communicate with these IPs erratically and in inconsistent volumes. While it's conceivable that the activity is directly linked to operator actions, considering the observations previously discussed, it may actually be a hybrid of both systematic automation and random activity.

We hypothesize that the selection of ports used in connections may be determined by an automated process, yet the connections themselves seem to be responsive to the unpredictable nature of C2 bot communications that outbound T2 connections appear to follow.

NetFlow Observations IV: Characteristics of Destination IPs

To enrich our analysis, we examined and compared characteristics such as AS and geolocation to those of hosts identified from typical upstream bot communication. Some T2 destination IPs were confirmed as proxies and subsequently removed from the data to prevent skewing observations based on specific host details.

We first compared geolocations between T2 destination IPs and bot C2s identified from November to July 2023. We identified geolocations that were unique to bot C2s and not present among T2 destination IPs. Geolocations that were shared between the two datasets appeared in differing quantities. For instance, while only 31% of bot C2s were situated in the US, this figure increased to 60% of T2 destination IPs.

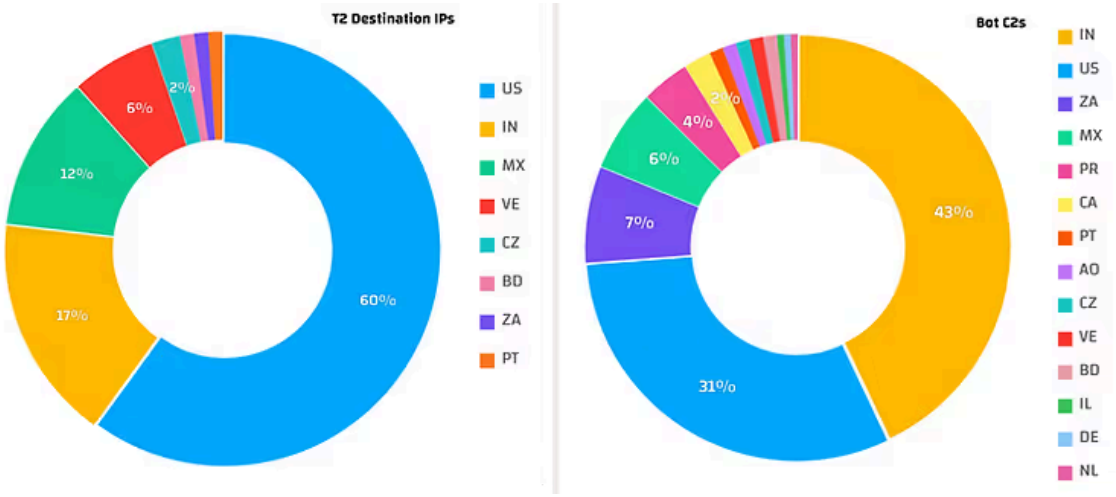


Figure 17: Side-by-side comparison of the geolocations that are associated bot C2s and T2 destination IPs

Next, we made a similar comparison of AS designations, filtered by geolocations with more than one IP. As pointed out by Black Lotus Labs, Qakbot seems to favor compromised hosts located in residential IP space, and our findings align with this observation. We found that Comcast is the predominant AS organization for both bot C2s and T2 destination IPs. According to our NetFlow data, the vast majority of US-based T2 destination IPs and (high confidence) bot C2s with upstream T2 connections are located within Comcast's IP space.

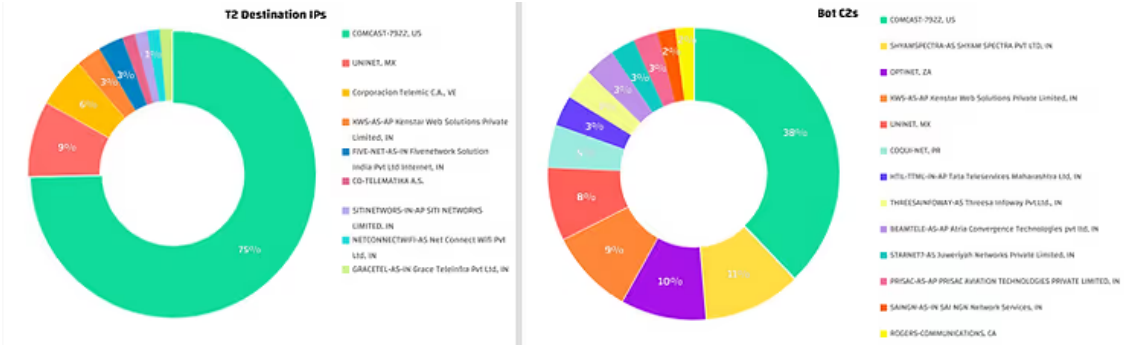


Figure 18: Side-by-side comparison of AS organizations associated with bot C2s and T2 destination IPs. Click the image to view it in full screen for better legibility.

These characteristics lead us to develop a theory that additional criteria, such as geolocation and AS organization, may influence the selection of compromised hosts. These factors could determine which hosts are purchased from third parties, or decide which Qakbot victims are escalated to the status of bot C2s or become T2 destination IPs, at least in some cases.

Conclusion

In this post, we have sought to continue our understanding of the relationship between the various tiers of infrastructure associated with the QakBot operation. Our data illustrates the winding down of operations leading up to QakBot's seasonal 'lull' in operations, which appears in part to have been accelerated by good work from Lumen's Black Lotus Labs. However, we also demonstrate that there is not a total cessation in operations, new infrastructure continues to be stood up albeit at a reduced cadence - likely for future use once spamming recommences.

We have also sought to illuminate interesting communications sourced from QakBot's upstream infrastructure, with outbound traffic occurring to both reported and unreported QakBot C2s, as well as currently undefined servers. We have demonstrated possible relationships between this activity and inbound communications to the same upstream infrastructure, noting that activity does not overlap, but one may precede the other.

We have established an interest in 32 specific ports, which the upstream infrastructure seeks to communicate with, potentially associated with QakBot's proxy module. We have also shown that this activity is, at least in part, possibly human-generated, with some reliance on automation for certain elements of the activity (specifying ports).

Finally, we hypothesized that certain factors may be considered when elevating a victim / compromised host to C2 status; including geolocation and who the host is assigned to from a hosting perspective.

Drawing this all together, we hope to have provided some interesting leads into further investigation of the QakBot operation, as well as providing opportunities for identification and mitigation of its threat. In elevating victims to be used as C2 infrastructure with T2 communication, QakBot effectively punishes users twice, first in the initial compromise, and second in the potential risk to reputation of a host being identified publicly as malicious.

We believe cutting off communications to the upstream servers is an effective remedy to the second part of this process; meaning that victim machines are cut off from further C2 instructions and in doing so protecting current and future users from compromise.

Recommendations

- Users of Pure Signal Recon and Scout are able to follow this activity by querying for the three Russian T2 IPs.
- Cyber defenders should monitor for inbound connections from the three Russian T2 IPs over the ports listed below.
- In addition, to identify any compromised hosts that were elevated to Qakbot C2 status, monitor for outbound connections from the host to any of the T2 IPs over TCP/443.

Indicators of Compromise

Ports

20

21

22

53

80

443

465

990

993

995

1194

2078

2083

2087

2222

3389

6881

6882

6883

8443

32100

32101

32102

32103

50000

50001

50002

50003

50010

61200

61201

61202

RU T2

188.127.231.177

62.204.41.187

62.204.41.188

New Bot C2s (Figure 5)

73.32.187.91

81.20.248.72

103.107.36.56

113.193.95.44

113.193.166.238

180.151.16.132

197.86.195.132

197.87.63.16

197.87.135.186

197.87.135.218

197.87.143.152

197.87.143.229

197.89.10.173

197.92.136.237

201.130.167.212

Other C2s Observed Active January - July 2023

High Confidence

23.30.22.225

23.30.22.230

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

49.248.11.251

50.248.58.241

59.153.96.4

64.237.207.9

64.237.212.162

64.237.221.254

64.237.245.195

64.237.251.199

67.177.41.245

67.177.42.38

67.187.130.101

68.59.64.105

68.62.199.70

69.242.31.249

73.0.34.177

73.1.85.92

73.22.121.210

73.29.92.128

73.36.196.11

73.41.215.237

73.60.227.230

73.78.215.104

73.88.173.113

73.127.53.140

73.155.10.79

73.161.176.218

73.161.178.173

73.165.119.20

73.197.85.237

73.207.160.219

73.215.22.78

73.223.248.31

73.226.175.11

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

79.168.224.165

89.203.252.238

96.87.28.170

98.37.25.99

98.222.212.149

99.251.67.229

99.252.190.205

99.254.167.145

102.130.200.134

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

103.123.223.124

103.123.223.125

103.123.223.130

103.123.223.131

103.123.223.132

103.123.223.133

103.123.223.141

103.123.223.144

103.123.223.153

103.123.223.168

103.123.223.171

103.134.117.111

103.176.239.98

103.195.16.175

103.211.63.108

103.212.19.254

103.221.68.250

103.231.216.238

103.252.7.228

103.252.7.231

103.252.7.238

109.49.47.10

113.11.92.30

114.143.176.234

114.143.176.235

114.143.176.236

114.143.176.237

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

125.63.121.38

157.119.85.203

174.58.146.57

174.171.10.179

174.171.129.247

174.171.130.96

180.151.13.23

180.151.19.13

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

195.146.105.72

197.83.246.187

197.83.246.199

197.90.177.242

197.92.136.122

197.92.141.173

197.94.78.32

197.94.95.20

197.148.17.17

200.8.245.72

201.130.116.138

201.130.119.176

201.142.207.183

202.142.98.62

203.109.44.236

Medium Confidence

49.205.181.242

64.237.188.252

64.237.213.86

69.255.128.224

73.14.226.243

73.45.247.179

76.149.184.246

96.85.69.170

96.85.69.171

96.92.67.169

98.244.148.34

103.204.192.220

138.68.166.127

138.197.95.196

175.100.177.171

180.151.18.235

180.151.107.118

180.151.118.243

183.82.122.136

187.199.135.157

187.211.104.152

187.211.105.137

189.248.64.238

197.92.131.106

201.142.195.172

201.142.197.29

201.142.213.13
