# Qakbot: retool, reinfect, recycle

blog.lumen.com/qakbot-retool-reinfect-recycle/

June 1, 2023

## Executive Summary

Qakbot (aka Pinkslipbot, Qbot) has persisted as a banking trojan – then a potent malware/ransomware distribution network – for well over a decade, its origins going back as far as 2007. As a ransomware botnet, Qakbot is usually spread through email hijacking and social engineering, dropping malicious files that infect Windows hosts. This botnet has adapted techniques to conceal its infrastructure in residential IP space and infected web servers, as opposed to hiding in a network of hosted virtual private servers (VPSs). Qakbot alternates its means of initial entry to stay ahead of tightening security policies and evolving defenses. Using Black Lotus Labs' global visibility, we have tracked Qakbot's more recent campaigns to observe the network structure, and gained key insights into the methods that support Qakbot's reputation as an evasive and tenacious threat.

## Introduction

In 2023, Qakbot exhibited dynamic operational techniques – including new malware delivery mechanisms and an adaptable Command and Control (C2) infrastructure – to account for tightening security practices, the speed at which defenders adapt to new variations, and the challenges inherent to hiding C2s in residential proxies. For example, Black Lotus Labs detected that 25% of Qakbot's C2s are only active for a single day. We observed that Qakbot operators tend to reduce or stop their spamming attacks for long periods of time on a seasonal basis, returning to activity with a modified suite of tools. This is similar to what was documented in the last half of 2022, where the summer months were noticeably quiet, and, as the year closed out, the activity picked up.

Several researchers cited throughout this blog have since discussed Qakbot's evolution from initial access and endpoint detection perspectives. While Black Lotus Labs has tracked Qakbot for years, in this blog we demonstrate—through the lens of Lumen's proprietary telemetry – how recent evolution of the botnet finds success, and we identify key features of the actor's network.

## Technical Details

We began our analysis by charting Qakbot's success in the spamming campaigns that began in late December 2022. The threat actors relied on macro-based exploitation in Microsoft Office documents through the beginning of 2022, then shifted in response to Microsoft's announcement that it would block XL4 and VBA macros by default for Office users. This year, the botnet gained initial access by rapidly changing the types of files delivered in socially engineered email-hijacking campaigns. It maintained the attacker's advantage by leveraging a wide range of malicious OneNote files, Mark of the Web evasion and HTML smuggling techniques. Accessing telemetry from the Lumen global IP backbone, the chart below illustrates Black Lotus Labs' visibility into Qakbot's bot volume over time, correlated with the entry techniques that were notable for each.

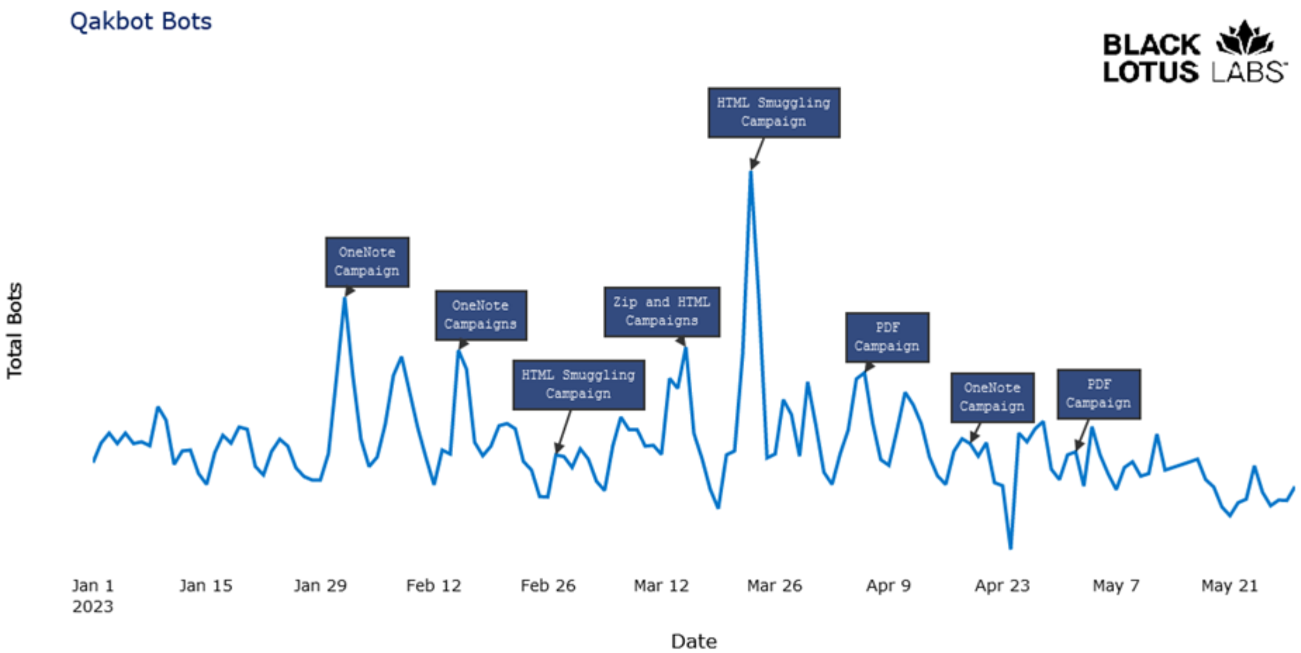

Figure 1: Daily active Qakbot bots January 2023- May 2023

We see the highest peaks of bot recruitment, indicating likely successful spamming campaigns, during the January and February 2023 OneNote campaigns, then in the March HTML Smuggling campaign. It’s likely that OneNote-based exploitation became less effective at obtaining new bots because of the ease with which defenders can block OneNote on mail servers.

The threat actors elect to hide their C2s in compromised web servers and hosts existing in the residential IP space – essentially those addresses in the ISP-issued dynamic IP range- instead of using a hosted VPS. Persistence in these C2s can be difficult to maintain over time, and we noticed that the lifespan of C2s was brief; however, they continually replenished their numbers. Over a given seven-day period, we could see between 70-90 new C2s emerge during the botnet spamming cycle, shown in the chart below:

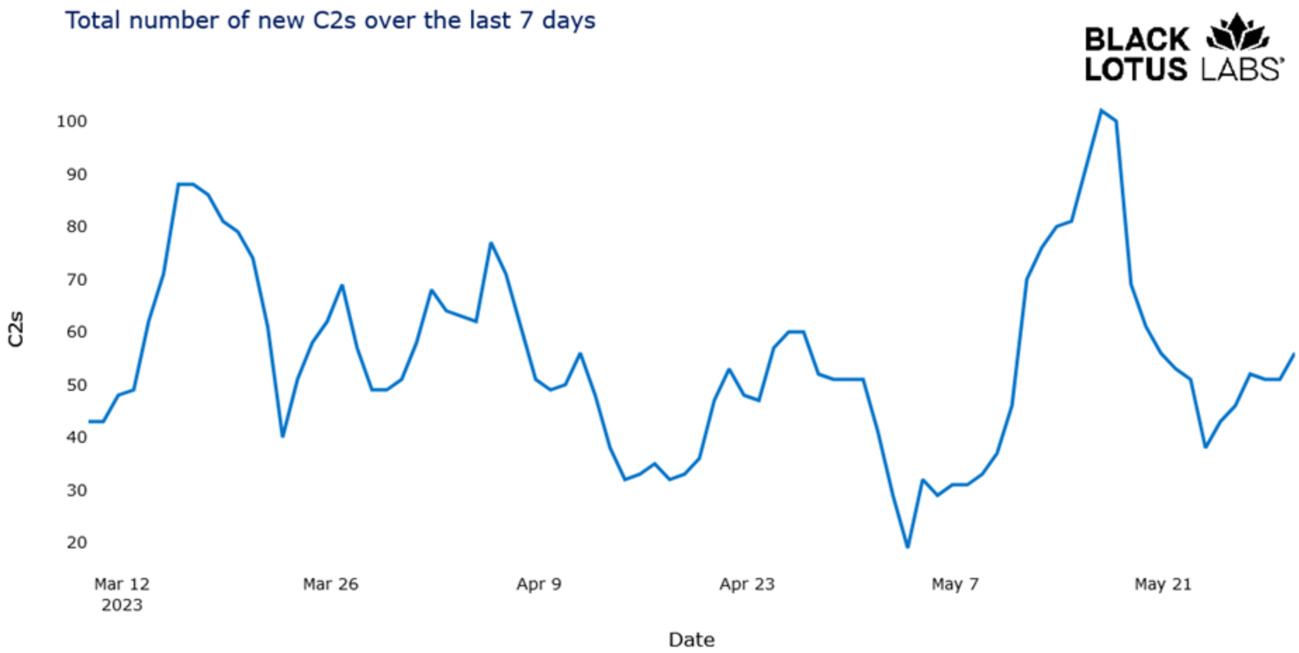

Figure 2: Total number of new Qakbot C2s over seven days, March 2023-May 2023

As we studied the lifespan of individual bots and C2s, our telemetry revealed the botnet operators were able to maintain their numbers. After the first day of an infection, a bot transmits about half of all the data it will ever send to a C2. By day seven, the number gets close to 90%. This indicates that, once a victim is infected, the operators get what they need posthaste, loading additional malware at will. The actors can then use the bot for other nefarious purposes or sell it off to other actors.

This includes, but is not limited to, conversion into use as a C2 in the botnet, enabling a key factor in Qakbot's ability to elude network defenses and maintain resiliency. Qakbot's use of bot C2s reduces the efficacy of static, IOC-based blocking by continually turning over the addresses of these control points. This wouldn't be the first time a large botnet was converting bots to C2s, as we noted here in our reporting on Emotet.

## C2 supply

While leveraging residential IP ranges enables Qakbot to resist mitigation action by VPS providers and evade some behavior-based firewall blocking, infections on residential IPs are inherently more vulnerable to bandwidth issues and to being wiped out by defenders and system updates. Qakbot retains resiliency by repurposing victim machines into C2s. Access to a large pool of bots to convert into C2s is essential – Black Lotus Labs observes that more than 25% of C2s don't remain active for more than a day, and 50% don't remain active for more than a week. We see Qakbot continue to replenish the supply of C2s through bots that subsequently turn to C2s.

As noted by Team Cymru, C2 nodes communicate with upstream Tier 2 C2 nodes hosted on VPS providers, often out of reach of non-Russian law enforcement. In addition to the C2s and the Tier 2 C2s, Black Lotus Labs observes a separate server – likely a backconnect server – in the Qakbot architecture.

We discovered that several hours after a bot became infected, a significant number of them began reaching out to this backconnect server. This server only interacts with the bots and not the higher-tier architecture. While its complete functionality is currently unknown, it is often seen turning bots into proxies that can be used or sold for different purposes.

We see other interesting behavior after bots interact with this server. It is not uncommon to see a bot connect to the backconnect server, then a day or two later reach out to a Tier 2 C2. There are bots in contact with multiple different Tier 1 C2s while simultaneously talking to one or more of the Tier 2 C2s. In both cases, we believe we are looking at bots that have been converted into C2s and can still maintain bot functionality. Below demonstrates the relationships between the bots and servers.

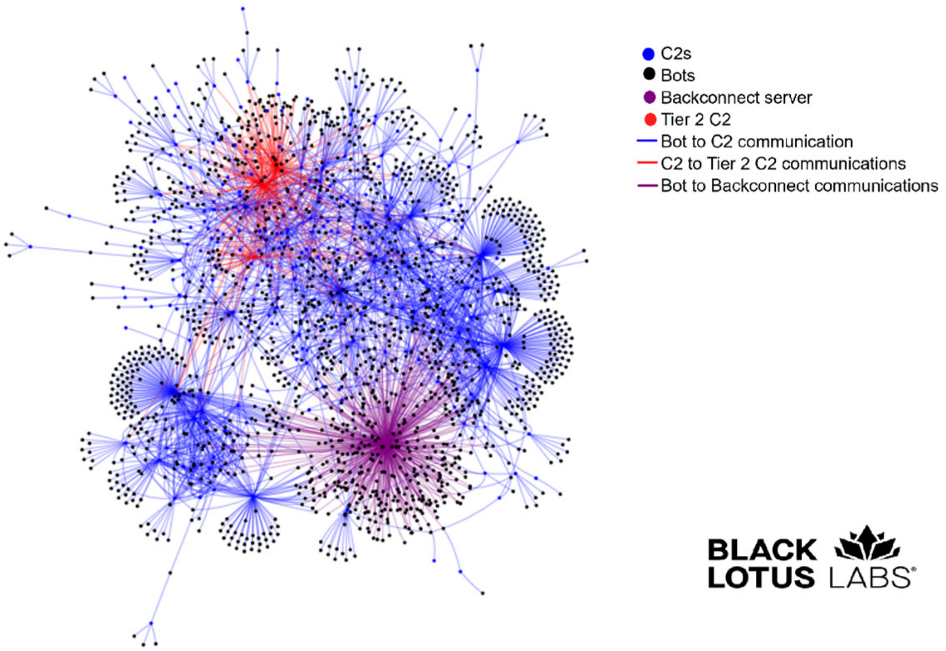
● C2s
● Bots
● Backconnect server
● Tier 2 C2
— Bot to C2 communication
— C2 to Tier 2 C2 communications
— Bot to Backconnect communications
BLACK LOTUS LABS

Figure 3: Qakbot infrastructure, May 2023

Black Lotus Labs leverages this visibility to discover and track new Qakbot C2 nodes often before they are used in campaigns and potentially alerted on by endpoint detection tools. When Qakbot breaks from spamming, it often doesn't stop converting bots to C2s, meaning that Black Lotus Labs can have advanced knowledge of as many as 35% of confirmed Qakbot C2s. For example, we noted an absence of spam from March 24 – 30. Even when bots are not spamming, Black Lotus Labs telemetry allows us to look for underlying behavioral characteristics of the known C2s. We are then able to chart what percentage of emerging C2s are exhibiting these characteristics but are not yet associated with any previous campaign activity.

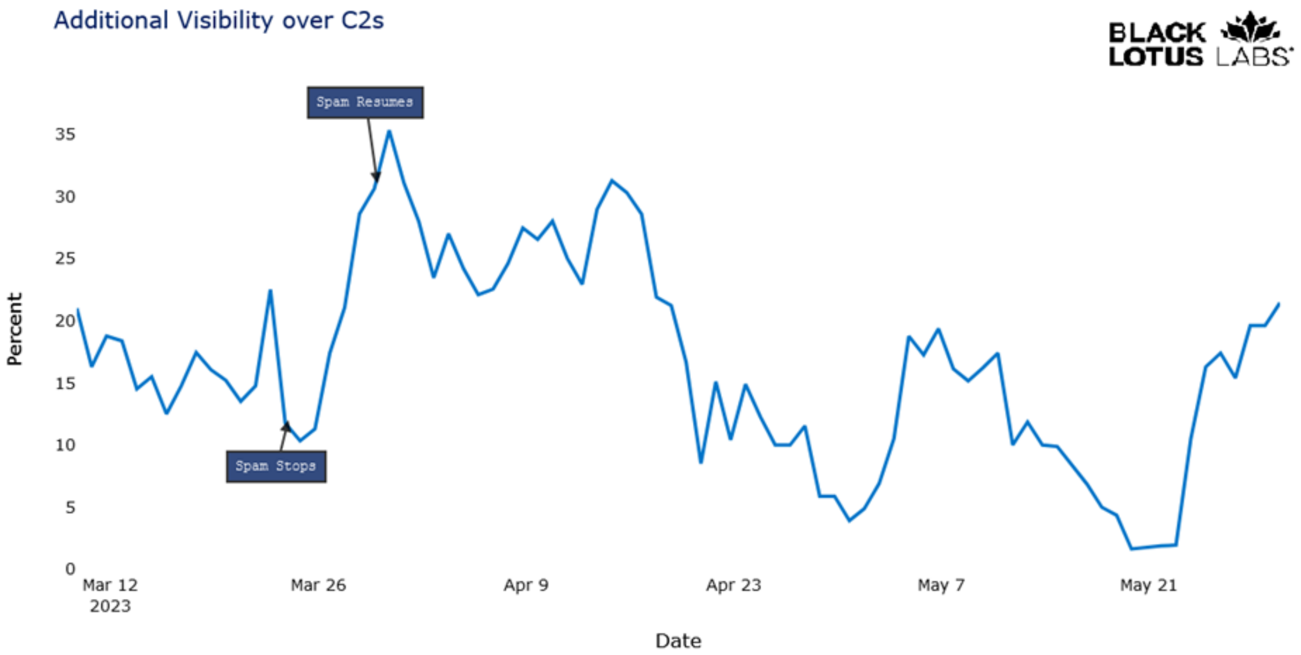

Figure 4: Black Lotus Labs additional visibility over new Qakbot C2s

## Conclusion

Qakbot has persevered by adopting a field-expedient approach to build and develop its architecture. While it may not rely on sheer numbers like Emotet, it demonstrates technical craft by varying initial access methods and maintaining a resilient yet evasive residential C2 architecture.

Because Qakbot is primarily spread through email hijacking and spamming malicious email attachments and embedded URLs, we advise Lumen customers to bolster defenses against phishing as an initial access vector by fully monitoring network resources, ensuring proper patch management and conducting ongoing phishing and social engineering training for employees.

As there are currently no signs of Qakbot slowing down, Black Lotus Labs null-routed all higher-tier infrastructure prior to publication of this report. We will continue to collaborate with the community to detect and disrupt Qakbot, as this and other botnets rise and fall in activity. We encourage other organizations to alert on these and similar indicators in their environments.

We would like to thank the many researchers who track and share information to help defend against this and many other botnets, including Cryptolaemus, malware_traffic_analysis, and pr0xylife.

For a list of higher-tier infrastructure, please visit our Github page.

This analysis was performed by Chris Formosa and Steve Rudd. Technical editing by Ryan English.

This information is provided “as is” without any warranty or condition of any kind, either express or implied. Use of this information is at the end user’s own risk.