# Qbot - Red Canary Threat Detection Report

Archived: 2026-04-06 03:13:56 UTC

**Editor's note:** *While the detection opportunities and analysis on this page are still relevant, it has not been updated since 2024.*

Also known as "Qakbot," the Qbot banking trojan has been active since at least 2007. Initially focused on stealing user data and banking credentials, Qbot's functionality has expanded to incorporate features such as reconnaissance, follow-on payload delivery, command and control (C2) infrastructure, and anti-analysis capabilities. Qbot is typically delivered via an email-based distribution model.

Over the years, various groups have distributed Qbot. The Proofpoint-named groups TA570 and TA577 are historically two of the most active Qbot malware affiliates. TA570 is sometimes referred to as the "presidents" affiliate, because of the use of U.S. presidents' names in its malware configuration, for example, a campaign identifier like `obama225`. TA577 is also informally known as the "letters" affiliate based on the use of campaign IDs including letters such as `AA`, `BB`, or `TR`. While Red Canary can not validate with high confidence that a specific group is present in an environment without obtaining a copy of the malware containing the campaign identifier, we did observe threats with similar naming schemes to both TA570 and TA577 in our customers' environments in 2023.

Qbot is usually deployed as just one stage of an adversary's playbook, with follow-on activity tied to the objectives of the affiliate group deploying it. While Red Canary does not observe a lot of post-Qbot activity, we know various ransomware affiliates have used it as an initial access vector.

The story of Qbot in 2023 can be told in three acts: early-year activity, infrastructure takedown by the FBI, and finally, Qbot affiliates pivoting to deliver alternative malware.

### Act I: The year begins

Qbot began 2023 quietly, observing its traditional lull during the orthodox holidays, but by March it had quickly reasserted itself as the most prevalent threat facing Red Canary customers. In 2023, Qbot affiliates continued to experiment with a variety of file types to deliver malicious payloads during their campaigns, likely in an ongoing response to security controls implemented by Microsoft in 2022. Examples of different delivery approaches include:

- Early 2023 brought Qbot in the form of malicious OneNote files that tricked users into executing an embedded malicious HTML Application (HTA) file. OneNote files were, at the time, not protected by Microsoft's Mark-of-the-Web (MOTW) feature. Red Canary and other security researchers observed OneNote abuse until mid-February.
- In March 2023, multiple Red Canary customers received phishing emails with ZIP files containing malicious PDF, HTML, WSF, and JS files. Upon opening the files, victims unknowingly executed malicious JavaScript which led to further PowerShell commands that downloaded and executed the Qbot DLL payload.
- In May 2023, Qbot operators began modifying the file extensions of their malware. Red Canary observed attempted or successful execution of Qbot with filename extensions such as `directexaminationSuperarbitrary` and `englishedDuctal`, similar to some 2022 campaigns. Qbot also masqueraded as PNG, DAT, or JPG files.

Starting in July, Qbot detections decreased dramatically—in line with the extended summer vacation that Red Canary and other cybersecurity researchers have previously observed. In years past, Qbot would return after their two-to-three month hiatus with a new wave of infections in September. This year, however, would prove to be different.

**Act II: The takedown**

On August 29, 2023, the United States Justice Department announced their participation in an operation to take down Qbot C2 infrastructure and remove infections from victim endpoints. The "Operation Duck Hunt" team, made up of multinational law enforcement and industry professionals, reported that it uninstalled the malware from more than 700,000 systems comprising the Qbot botnet and seized extorted funds held as cryptocurrency by the operators. The takedown was successful. Not only did it thwart Qbot activity, it also delivered a significant blow to delivery affiliates that heavily leveraged Qbot, including TA577. Weeks passed with no signs of new Qbot or TA577 activity.

**Act III: Return of the affiliate**

On September 22, 2023, Deutsche Telekom CERT's CTI team shared details of a new TA577 phishing campaign delivering DarkGate as their new payload of choice. TA577 also elected to use IcedID and PikaBot to replace Qbot in this new campaign, which continued until the end of December 2023.

**DarkGate**

DarkGate is a loader offered on popular cybercrime forums as malware-as-a-service (MaaS). The DarkGate malware family has been active since at least 2018. It was historically delivered via email phishing campaigns, but as of August 2023 it has also been distributed via Microsoft Teams phishing messages. It includes built-in defense evasion, command & control (C2), and persistence capabilities. It also has the ability to download and execute additional payloads, making it an appealing replacement for Qbot.

TA577 was not the only threat to leverage DarkGate this year; Red Canary observed several different campaigns by different groups using DarkGate as their primary payload in 2023.

**PikaBot**

Pikabot is a malware family that was first discovered in early 2023. It is modular malware, consisting of loader and core module components. Pikabot enables unauthorized remote access to a system and it has been observed dropping malware like Cobalt Strike as a follow-on payload. The Pikabot code base is similar to another malware family named Matanbuchus.

**IcedID**

IcedID, also known as BokBot, is a crimeware-as-a-service banking trojan. You can learn more about IcedID here.

**Epilogue**

It remains to be seen what a Qbot return might look like. On December 15, 2023, Microsoft reported new Qbot activity, the first new infections publicly reported since the takedown in August. The campaign was low-volume and of limited scope, targeting the hospitality industry. As of late January 2024, Qbot's old affiliate networks are once again showing signs of life, following their old patterns of ramping up activities after a holiday break. While the takedown disrupted the Qbot malware, it is important to distinguish Qbot the tool from the adversaries who use it. You can think of the takedown like a government raid that seizes a warring faction's largest weapons cache; a blow to be sure, but while the adversaries are still at large you can bet they will retool and rearm themselves. Only time will tell what their new weapon of choice will be and how it will be used.

---