red canary

HOMEPAGE

TRENDS

THREATS

- All threats
- Charcoal Stork
- Impacket
- Mimikatz
- Yellow Cockatoo
- SocGholish
- ChromeLoader
- Gamarue
- Qbot
- Raspberry Robin
- SmashJacker

TECHNIQUES

THREAT SOUNDS

MIDYEAR UPDATE

ARCHIVE

DOWNLOAD

SEARCH

THREAT

Qbot

#8

OVERALL RANK

2.9%

CUSTOMERS AFFECTED

After a government takedown in August, Qbot affiliates resumed activity in late 2023 after adopting new malware and infrastructure.

PAIRS WITH THIS SONG

ANALYSIS

Analysis

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

red canary

HOMEPAGE

TRENDS

THREATS

All threats
Charcoal Stork
Impacket
Mimikatz
Yellow Cockatoo
SocGholish
ChromeLoader
Gamarue
Qbot
Raspberry Robin
SmashJacker

TECHNIQUES

THREAT SOUNDS

MIDYEAR UPDATE

ARCHIVE

DOWNLOAD

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.

red canary

HOMEPAGE

TRENDS

THREATS

All threats
Charcoal Stork
Impacket
Mimikatz
Yellow Cockatoo
SocGholish
ChromeLoader
Gamarue
Qbot
Raspberry Robin
SmashJacker

TECHNIQUES

THREAT SOUNDS

MIDYEAR UPDATE

ARCHIVE

DOWNLOAD

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

red canary

HOMEPAGE

TRENDS

THREATS

All threats
Charcoal Stork
Impacket
Mimikatz
Yellow Cockatoo
SocGholish
ChromeLoader
Gamarue
Qbot
Raspberry Robin
SmashJacker

TECHNIQUES

THREAT SOUNDS

MIDYEAR UPDATE

ARCHIVE

DOWNLOAD

TAKE ACTION

The best way to remedy the risk of any threat is to prevent your users from having the opportunity to become a victim. Qbot, DarkGate, and PikaBot are adaptive threats that are reliant on email for distribution, so if you want to stop threats like these, start in the inbox. Implementing an email gateway filtering solution is one way of minimizing infections within your environment.

To inhibit users from infecting themselves via mountable virtual drives, consider disabling disk image (ISO, IMG, VHD, VHDX) mounting functionality via **registry hive modifications,** which also has the benefit of inhibiting **additional threats**.

Detection opportunities

Phishing emails related to Qbot may contain a variety of attachment types. One tactic used is for the attachments to download a ZIP archive containing a disk image such as an ISO, IMG, or VHD. Contained within these virtual disks is a script file that is subsequently executed, followed by activity that is consistent with successful Qbot execution.

Focusing on the activity from this early-to-intermediary stage TTP, we've provided a detection opportunity that focuses on Windows Scripting Hosts (`wscript.exe` and `cscript.exe`) that are invoking the execution of common scripting formats that Red Canary has observed being used by Qbot—such as `.js`, `.vbs`, and `.wsf`—that are from a logical mounted drive using the drive letters D: through Z: and that have a child process.

```
parent_process == 'explorer.exe'
&&
process == ('wscript' || 'cscript')
&&
command_includes ('[d-z]:\\[^\\]+\.(?:js|vbs|wsf)')
&&
has_child_process
```

HOMEPAGE
TRENDS
THREATS
All threats
Charcoal Stork
Impacket
Mimikatz
Yellow Cockatoo
SocGholish
ChromeLoader
Gamarue
Qbot
Raspberry Robin
SmashJacker
TECHNIQUES
THREAT SOUNDS
MIDYEAR UPDATE
ARCHIVE
DOWNLOAD

Testing

Start testing your defenses against Qbot using **Atomic Red Team**—an open source testing framework of small, highly portable detection tests mapped to MITRE ATT&CK.

Getting started

Atomic test #2 for T1553.005: Subvert Trust Controls: **Mark-of-the-Web Bypass** mounts an ISO image and runs an executable from the ISO. As noted above, using a disk image file allows Qbot to bypass the MOTW feature because extracted or mounted files do not reliably inherit MOTW.

Further, **many of the tests for T1218.011: Rundll32** execute `rundll32.exe` without a command line containing the file formats mentioned in the final detection opportunity of the previous section.

Review and repeat

Now that you have executed one or several common tests and checked for the expected results, it's useful to answer some immediate questions:

- Were any of your actions detected?
- Were any of your actions blocked or prevented?
- Were your actions visible in logs or other defensive telemetry?

Repeat this process, performing additional tests related to this technique. You can also **create and contribute** tests of your own.

HOMEPAGE
TRENDS
THREATS
All threats
Charcoal Stork
Impacket
Mimikatz
Yellow Cockatoo
SocGholish
ChromeLoader
Gamarue
Qbot
Raspberry Robin
SmashJacker
TECHNIQUES
THREAT
Search
MIDYEAR UPDATE
ARCHIVE
DOWNLOAD

PRODUCTS
Managed Detection and Response (MDR)
Readiness Exercises
Linux EDR
Atomic Red Team™
Mac Monitor
What's New?
Plans

SOLUTIONS
Deliver Enterprise Security Across Your IT Environment
Get a 24×7 SOC Instantly
Protect Your Corporate Endpoints and Network
Protect Your Users' Email, Identities, and SaaS Apps
Protect Your Cloud
Protect Critical Production Linux and Kubernetes
Stop Business Email Compromise
Replace Your MSSP or MDR
Run More Effective Tabletops
Train Continuously for Real-World Scenarios
Operationalize Your Microsoft Security Stack
Minimize Downtime with After-Hours Support

RESOURCES
View all Resources
Blog
Integrations
Guides & Overviews
Cybersecurity 101
Case Studies
Videos
Webinars
Events
Customer Help Center
Newsletter

PARTNERS
Overview
Incident Response
Insurance & Risk
Managed Service Providers
Solution Providers
Technology Partners
Apply to Become a Partner

COMPANY
About Us
The Red Canary Difference
News & Press
Careers – We're Hiring!
Contact Us
Trust Center and Security

info@redcanary.com +1 855-977-0686 Privacy Policy Trust Center and Security