Qakbot Malware Now Exfiltrating Emails for Sophisticated Thread Hijacking Attacks

By Laurie Iacono, Cole Manaster

Published: 2020-06-04 · Archived: 2026-04-06 01:59:22 UTC

Kroll identified a growing trend in Qakbot (also known as Qbot) cases targeting and exfiltrating locally stored emails to commit a sophisticated phishing method known as email thread hijacking. This increase, merged with intelligence gathered by Kroll and analysts from the National Cyber-Forensics and Training Alliance (NCFTA) suggests the attacks are part of an ongoing campaign to steal financial data from multiple industries including media, education and academia.

This new tactic of exfiltrating emails opens Qakbot victims up to multiple issues:

- First, if the exfiltrated emails contain sensitive customer or patient data, there could be costly notice obligations to disclose the leaked data.
- Second, similar to how Emotet acts as a dropper for Ryuk ransomware, recent news indicates that Qakbot is being used as a point of entry by the operators of ProLock ransomware, meaning that users falling for these sophisticated phishing lures risk encrypting their entire networks.

Email thread hijacking occurs when cyber criminals respond to or forward legacy email threads with new phishing lures. Even though the threads may originate from a compromised user account or an actor-controlled system, by leveraging existing email threads and adding a malicious link or attachment, these messages help threat actors evade phishing detection software such as antivirus or spam filters. In addition, these threads appearing to come from a trusted sender increases the likelihood that others will click on the message, thereby exponentially spreading the infection.

In this flood of recent incidents, Kroll observed the attackers scraping and exfiltrating locally stored emails to an actor-controlled system where the actor can continue to hijack email threads even after leaving the compromised network.

In one instance, a company approached Kroll stating that they were receiving suspicious emails from one of their subsidiaries. Upon further inspection, Kroll learned that an employee using their work computer had clicked on a malicious link from their personal email account that downloaded a Qakbot dropper.

From that initial compromise, the malware scraped thousands of emails and contacts across multiple users.

The Evolution of Qakbot

Banking trojan Qakbot has been active for over a decade. Like other trojans, it is most well-known for targeting banking customer information. Its repertoire of malicious behavior includes:

- Online banking and website credential theft

- Windows account credential theft
- Keyloggers
- Authentication cookie grabber
- Brute force attacks
- Hooking onto running processes
- Worm-like behavior to propagate through and persist within an infected network

In the spring of 2019, multiple outlets reported on a massive Qakbot campaign which included the new tactic of email thread hijacking. After these public reports, the group appeared to go on a brief hiatus through late 2019. This new campaign shows efforts to strengthen the malware and cause even more damage by stealing emails and potentially sensitive data. Such tactics mean that Qakbot victims could now be subject to notification requirements around leaked data.

Kroll Observations: Anatomy of a Qakbot Email Hijack

Initial Compromise	Malicious attachment from a phishing email
Execution	Visual basic script execution which drops and executes a malicious file
Evasion	One of the tell-tale indicators of Qakbot: the original malicious executable is overwritten with the legitimate Microsoft calculator executable calc.exe.
Persistence	Series of automated installation and processes such as establishing folders within the infected user directory and persistent scheduled tasks within user and system registry hives

Collection	New folders are populated with individual email messages and aggregated text files containing additional contact details. • The naming convention for this maliciously created folder contains the host name of the infected system, the name of the infected user and a UNIX-formatted timestamp: C:\Users\<user>\EmailStorage_<hostname>_<username>_<timestamp> • Within the root of this new folder, the malware generates a text file named "collector_log.txt" which contains a record of the malware's enumeration and exfiltration process. • This file provides insight into the malicious process including the names of the email folders which it is enumerating as well as a purported total number of emails the malware was able to successfully collect and exfiltrate.

A review of recent Qakbot cases identified the following:

- Emails dating more than three years prior to malware execution have been included in the collected EmailStorage folder, meaning that there may not be a date limit for the email enumerator.
  There is a lack of keywords or other limiting pattern by which specific email messages in local mailboxes were targeted for exfiltration. Kroll has identified instances where specific email messages were deleted within the EmailStorage folder.
- In some instances, the entire EmailStorage folder is deleted once messages have all been exfiltrated.
- Based on observed cases, there was no evidence that attachments were included in the collected data.
- Kroll collaborators at the National Cyber Forensics Training Alliance (NCFTA) observed Qakbot samples sending SMTP traffic indicative of outbound spam thread hijackings.

Mitigating the Risks of Phishing via Email Thread Hijacking

As mentioned by Devon Ackerman, Managing Director in our Cyber Risk practice, in a previous article on banking trojans, employee education and awareness is still key for defense.

- **Update Phishing Training Materials**
  Standard phishing training should include steps to educate staff on email thread hijacking and build a healthy dose of skepticism to help minimize the chances of users clicking on links and attachments when they receive new replies to historical email threads.
- **Gauge the Effectiveness of Training Programs**
  Incorporate social engineering exercises, such as phishing attacks, as part of regularly scheduled security checks.

Additionally, it's important to highlight that traditional antivirus solutions have historically proved ineffective against trojans like Qakbot. It's crucial to implement a robust endpoint detection solution that can monitor suspicious activity and behaviors.
