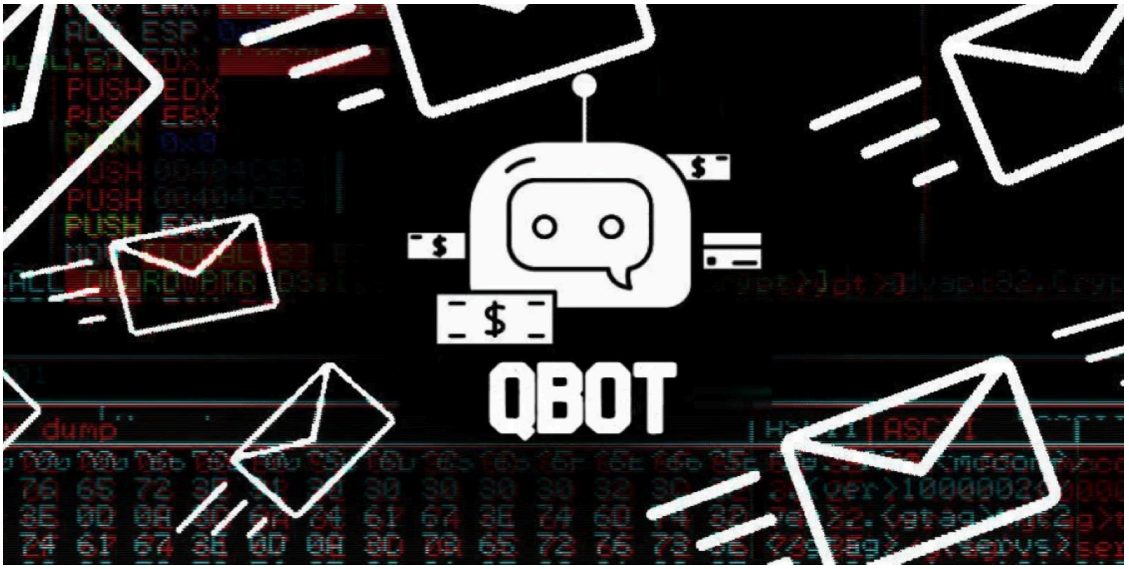
Qbot steals your email threads again to infect other victims

By Lawrence Abrams

Published: 2020-08-27 · Archived: 2026-04-05 12:50:43 UTC

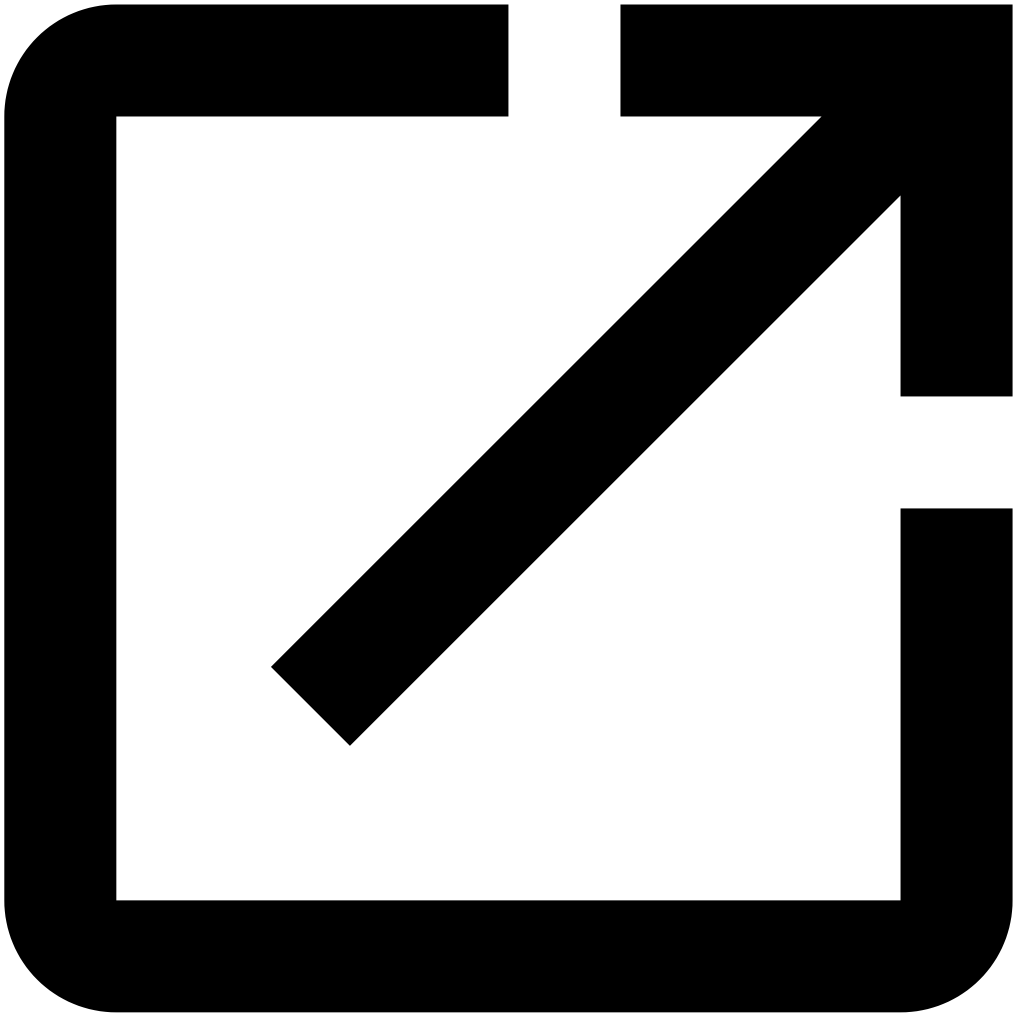


The Qbot trojan is again stealing reply-chain emails that can be used to camouflage malware-riddled emails as parts of previous conversations in future malicious spam campaigns.

Qbot (also known as QakBot) is a banking and information-stealing malware that has been actively infecting victims for more than ten years.

When installed, Qbot will attempt to steal its victims' stored passwords, cookies, credit cards, emails, and online banking credentials.


DIE LINKE.
0:00



This trojan is also known to download and install other malware onto compromised computers, including ProLock Ransomware payloads.

Since July 2020, Qbot has been a malware of choice for the notorious Emotet botnet and has seen a surge of new infections.

Qbot steals victim's emails for future malspam campaigns

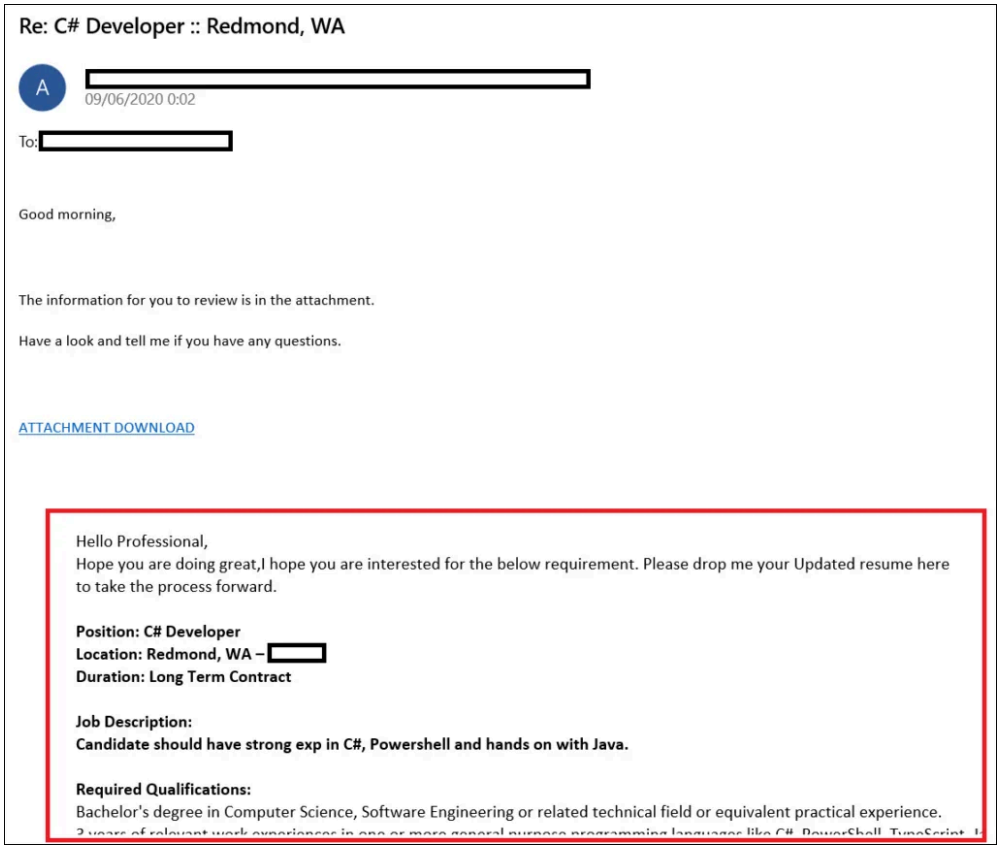
In 2019, we reported that QBot had started to steal victims' email threads, using them as part of a context-aware phishing campaign during late March 2019.

According to a new report by Check Point, QBot continues to employ a tactic previously used by the Gozi ISFB banking trojan, the URSNIF information-stealing trojan, and the Emotet trojan [1, 2, 3]: the stealing of full email threads to use in reply-chain, or 'hijacked email thread' attacks.

A reply-chain phishing attack is when threat actors use a stolen email thread and then reply to it with their own message and an attached malicious document.

After infecting victims, one of the malicious activities conducted by Qbot is to steal emails from a user's Outlook client.

These stolen emails are then uploaded to the Qbot threat actors servers to be used in future spam campaigns targeting other potential victims.



Reply-chain phishing email (*Check Point*)

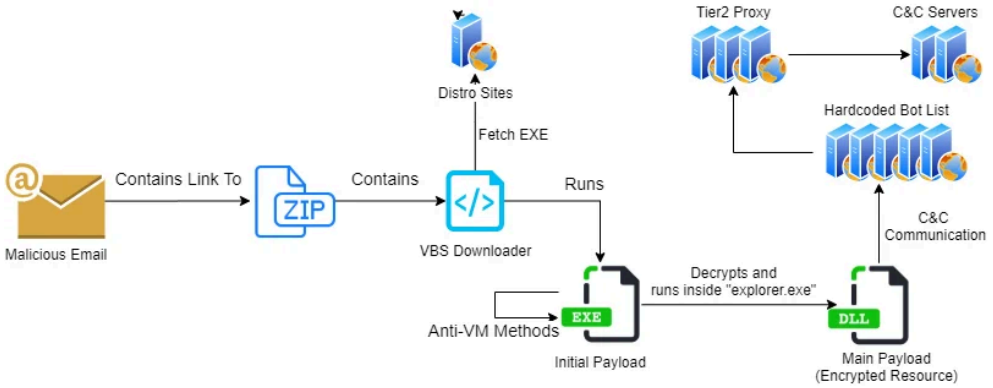
This type of attack makes the phishing campaign more believable, especially when it is used against those in the original thread.

Check Point has observed that these reply-chain attacks contain ZIP attachments with malicious VBS scripts enclosed. When executed, these VBS scripts will download the Qbot malware on the system and infect the user.

"During our tracking of the malspam campaign, we have seen hundreds of different URLs for malicious ZIP dropping when most of them were compromised WordPress sites," Check Point researchers explain.

Using a victim's stolen email against other recipients creates a perpetuating cycle of new victims being used against others to spread the malware.

Since this email thread stealing module has been added, Check Point's researchers have spotted targeted, hijacked email threads being used in ongoing campaigns with subjects related to tax payment reminders, the Covid-19 pandemic, and job offers.



Infection chain (*Check Point*)

Malware used in highly-targeted campaigns

Qbot's authors have also added unusual capabilities at one point or another, as well as a clever way for the malware to assemble itself from two encrypted halves to evade detection when being delivered onto a target's system.

The malware is also known for infecting other devices on the same network using network share exploits and as well as highly aggressive brute-force attacks that target Active Directory admin accounts.

Even though it has been active for over a decade, this banking trojan was mostly used in highly targeted attacks on enterprise entities that could provide a higher return on investment.

As proof of this, Qbot attacks have been quite infrequent over time, with researchers spotting one in October 2014, one in April 2016, as well as another one during mid-May 2017. Qbot came back last year, being dropped as a first stage or as a second stage payload by the Emotet gang.

Source: https://www.bleepingcomputer.com/news/security/qbot-steals-your-email-threads-again-to-infect-other-victims/