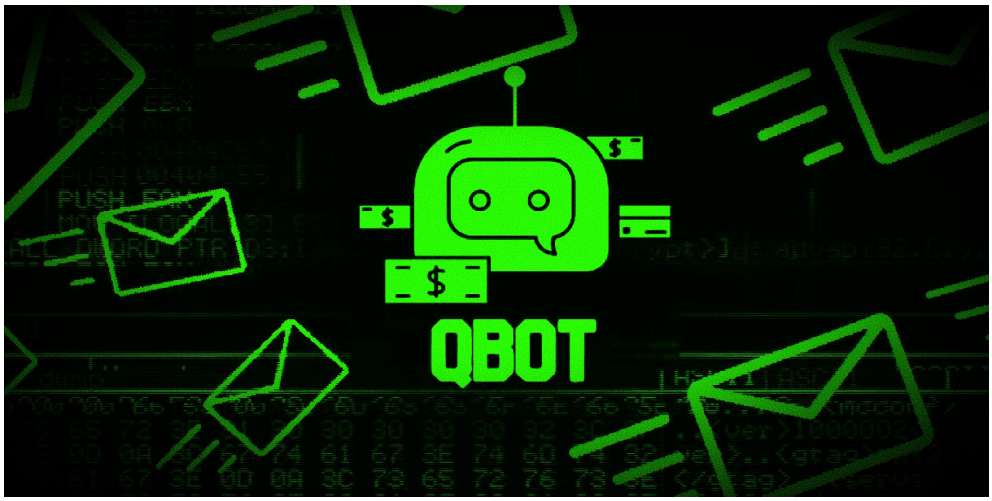
Qbot needs only 30 minutes to steal your credentials, emails

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

February 8, 2022 03:12 AM **0**



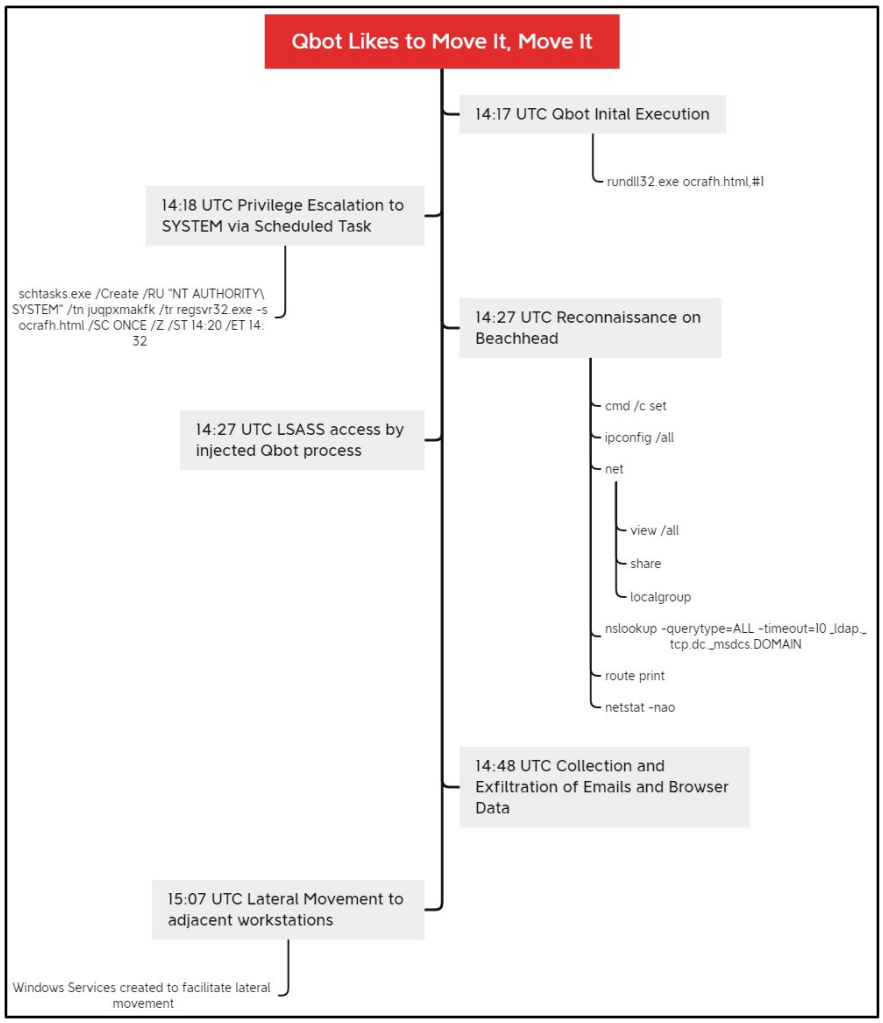
The widespread malware known as Qbot (aka Qakbot or QuakBot) has recently returned to light-speed attacks, and according to analysts, it only takes around 30 minutes to steal sensitive data after the initial infection.

According to a new report by The DFIR Report (https://thedfirreport.com/2022/02/07/qbot-likes-to-move-it-move-it/), Qbot was performing these quick data-snatching strikes back in October 2021, and it now appears that the threat actors behind it have returned to similar tactics.

More specifically, the analysts report that it takes half an hour for the adversaries to steal browser data and emails from Outlook and 50 minutes before they jump to an adjacent workstation.

The timeline of an attack

As shown in the following diagram from the researcher's report, Qbot moves quickly to perform privilege escalation immediately following an infection, while a full-fledged reconnaissance scan takes place within ten minutes.

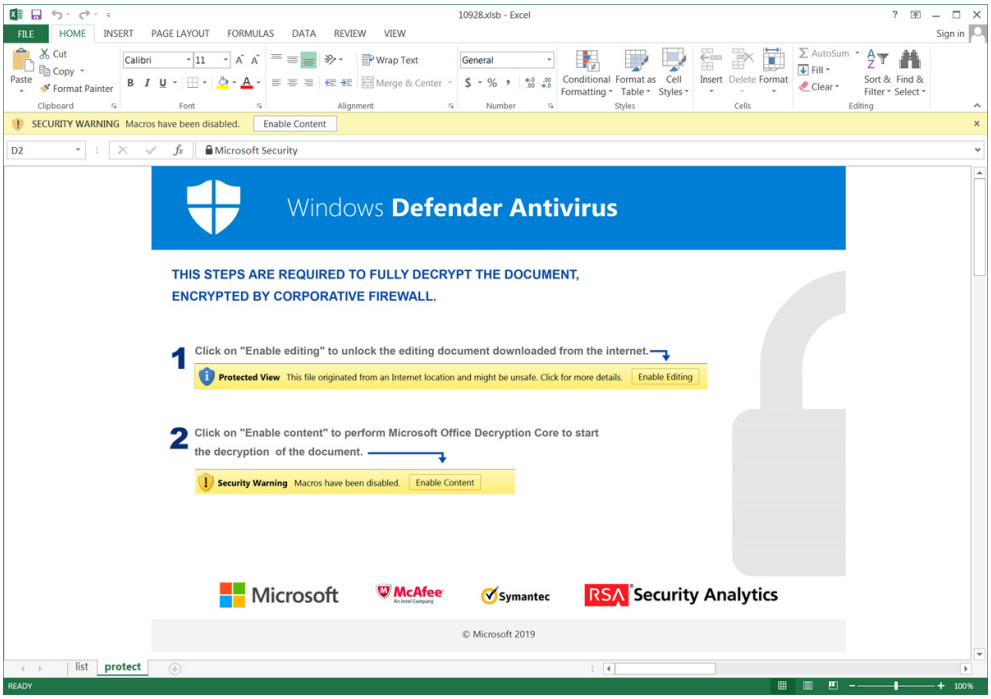


Timeline of a typical Qbot attack

Source: The DFIR Report

Initial access for Qbot infections is typically achieved via phishing emails (https://www.bleepingcomputer.com/news/security/microsoft-these-are-the-building-blocks-of-qbot-malware-attacks/) with malicious attacks, such as Excel (XLS) documents that use a macro to drop the DLL loader on the target machine.

Historically, BleepingComputer has seen Qbot phishing campaigns use various malicious document templates. For example, one document template pretends to be a warning from "Windows Defender Antivirus," (https://www.bleepingcomputer.com/news/security/qbot-uses-windows-defender-antivirus-phishing-bait-to-infect-pcs/) providing instructions on enabling macros.

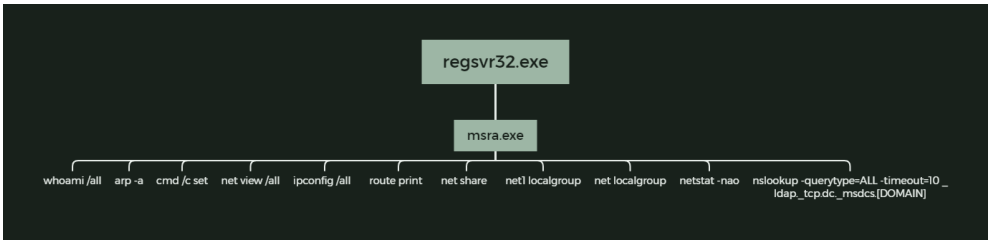


Qbot phishing document

Source: BleepingComputer

When launched, the Qbot DLL payload will be injected and launched into legitimate Windows applications to evade detection, such as MSRA.exe and Mobsync.exe. For example, in The DFIR Report's analysis, Qbot injected into MSRA.exe and then created a scheduled task for privilege elevation.

Additionally, the malware adds the Qbot DLL to Microsoft Defender's exclusion list, so it won't be detected when injection into msra.exe happens.



Discovery commands injected into msra.exe

Source: The DFIR Report

The malware steals emails in half an hour after the initial execution, which are then commonly used for future replay-chain phishing attacks (https://www.bleepingcomputer.com/news/security/qbot-steals-your-email-threads-again-to-infect-other-victims/).

The researchers note that Qbot will also steal Windows credentials by dumping the memory of the LSASS (Local Security Authority Server Service) process and by stealing from web browsers. These credentials can then be used to spread to other devices on the network laterally.

The DFIR Report states that it only took on average fifty minutes for credentials to be dumped after the malware was first executed.

The lateral movement takes place rapidly, so if there's no network segmentation to protect the workstations, the situation becomes very challenging for defense teams.

The impact of these expeditious attacks isn't limited to data loss, as Qbot has also been observed in the past to drop ransomware payloads onto compromised corporate networks.

Ransomware gangs known to have partnered with Qbot for initial access to corporate networks include REvil, Egregor (https://www.bleepingcomputer.com/news/security/qbot-partners-with-egregor-ransomware-in-bot-fueled-attacks/), ProLock (https://www.bleepingcomputer.com/news/security/prolock-ransomware-teams-up-with-qakbot-trojan-for-network-access/), and MegaCortex (https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-found-targeting-business-networks/).

A versatile infection

A Microsoft report from December 2021 captured the versatility of Qbot attacks (https://www.bleepingcomputer.com/news/security/microsoft-these-are-the-building-blocks-of-qbot-malware-attacks/), making it harder to evaluate the scope of its infections accurately.

However, no matter how a Qbot infection unfolds precisely, it is essential to keep in mind that almost all begin with an email, so this is the main access point that organizations need to strengthen.

Today's announcement by Microsoft that they will be blocking macros in downloaded documents by default (https://www.bleepingcomputer.com/news/microsoft/microsoft-plans-to-kill-malware-delivery-via-office-macros/) by removing the 'Enable Content' and 'Enable Editing' buttons will go a long way to protecting users from Qbot phishing attacks.

Related Articles:

Qbot malware returns in campaign targeting hospitality industry (https://www.bleepingcomputer.com/news/security/qbot-malware-returns-in-campaign-targeting-hospitality-industry/)

Malware abuses Google OAuth endpoint to 'revive' cookies, hijack accounts (https://www.bleepingcomputer.com/news/security/malware-abuses-google-oauth-endpoint-to-revive-cookies-hijack-accounts/)

Steam game mod breached to push password-stealing malware (https://www.bleepingcomputer.com/news/security/steam-game-mod-breached-to-push-password-stealing-malware/)

Microsoft disables MSIX protocol handler abused in malware attacks (https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-msix-protocol-handler-abused-in-malware-attacks/)

New Xamalicious Android malware installed 330k times on Google Play (https://www.bleepingcomputer.com/news/security/new-xamalicious-android-malware-installed-330k-times-on-google-play/)

CREDENTIALS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CREDENTIALS/)

EMAIL (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/EMAIL/)

LATERAL MOVEMENT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/LATERAL-MOVEMENT/)

MALWARE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MALWARE/)

QBOT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/QBOT/)