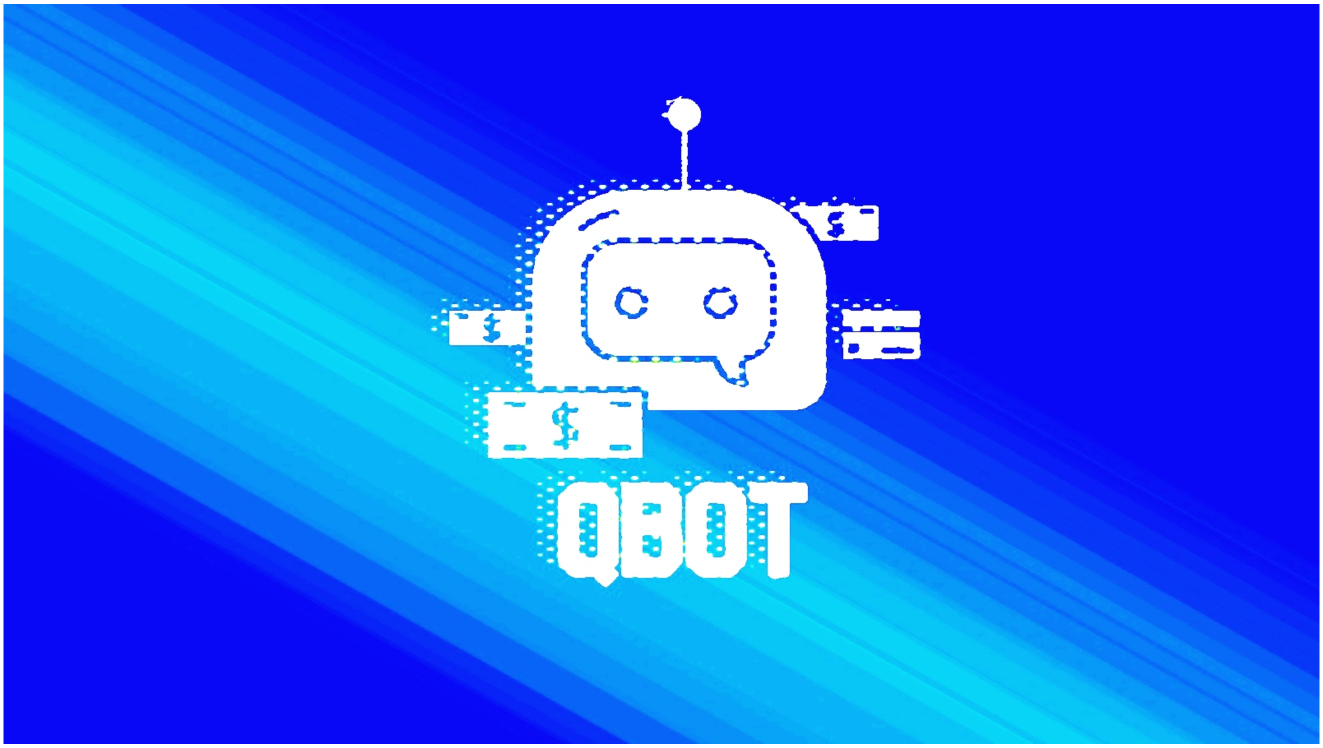
# Qbot malware switches to new Windows Installer infection vector

bleepingcomputer.com/news/security/qbot-malware-switches-to-new-windows-installer-infection-vector/

Sergiu Gatlan

By
Sergiu Gatlan

- April 11, 2022
- 04:58 PM
- 0



The Qbot botnet is now pushing malware payloads via phishing emails with password-protected ZIP archive attachments containing malicious MSI Windows Installer packages.

This is the first time the Qbot operators are using this tactic, switching from their standard way of delivering the malware via phishing emails dropping Microsoft Office documents with malicious macros on targets' devices.

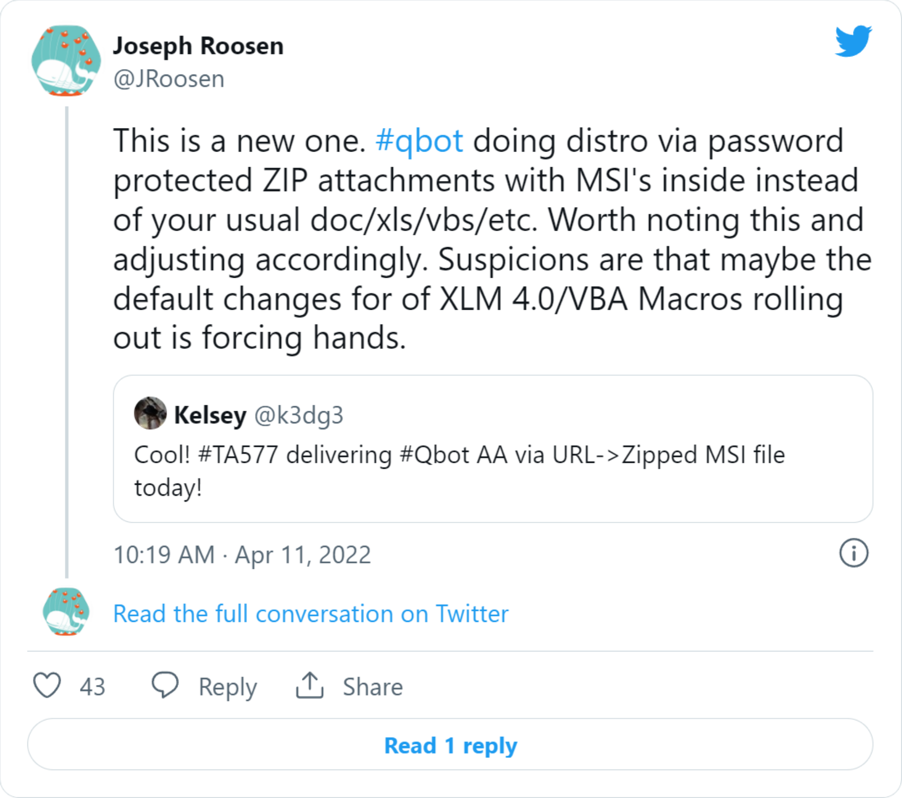
Security researchers suspect this move might be a direct reaction to Microsoft announcing plans to kill malware delivery via VBA Office macros in February after disabling Excel 4.0 (XLM) macros by default in January.

Microsoft has begun rolling out the VBA macro autoblock feature to Office for Windows users in early April 2022, starting with Version 2203 in the Current Channel (Preview) and to other release channels and older versions later.

"Despite the varying email methods attackers are using to deliver Qakbot, these campaigns have in common their use of malicious macros in Office documents, specifically Excel 4.0 macros," Microsoft said in December.

"It should be noted that while threats use Excel 4.0 macros as an attempt to evade detection, this feature is now disabled by default and thus requires users to enable it manually for such threats to execute properly."

This is a significant security improvement towards protecting Office customers since using malicious VBA macros embedded in Office documents is a prevalent method to push a large assortment of malware strains in phishing attacks, including Qbot, Emotet, TrickBot, and Dridex.



**Joseph Roosen**
@JRoosen

This is a new one. #qbot doing distro via password protected ZIP attachments with MSI's inside instead of your usual doc/xls/vbs/etc. Worth noting this and adjusting accordingly. Suspicions are that maybe the default changes for of XLM 4.0/VBA Macros rolling out is forcing hands.

**Kelsey** @k3dg3
Cool! #TA577 delivering #Qbot AA via URL->Zipped MSI file today!

10:19 AM · Apr 11, 2022

## What is Qbot?

Qbot (also known as Qakbot, Quakbot, and Pinkslipbot) is a modular Windows banking trojan with worm features used since at least 2007 to steal banking credentials, personal information, and financial data, as well as to drop backdoors on compromised computers and deploy Cobalt Strike beacons.

This malware is also known for infecting other devices on a compromised network using network share exploits and highly aggressive brute-force attacks targeting Active Directory admin accounts.

Although active for over a decade, the Qbot malware has been primarily used in highly targeted attacks against corporate entities since they provide a higher return on investment.

Multiple ransomware gangs, including REvil, Egregor, ProLock, PwndLocker, and MegaCortex, have also used Qbot to breach corporate networks.

Since Qbot infections can lead to dangerous infections and highly disruptive attacks, IT admins and security professionals need to become familiar with this malware, the tactics it's using to spread throughout a network, and those used by the botnet operators to deliver it to new targets.

A Microsoft report from December 2021 captured the versatility of Qbot attacks, making it harder to evaluate the scope of its infections accurately.

## Related Articles:

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Microsoft detects massive surge in Linux XorDDoS malware activity

New Raspberry Robin worm uses Windows Installer to drop malware

Emotet botnet switches to 64-bit modules, increases activity