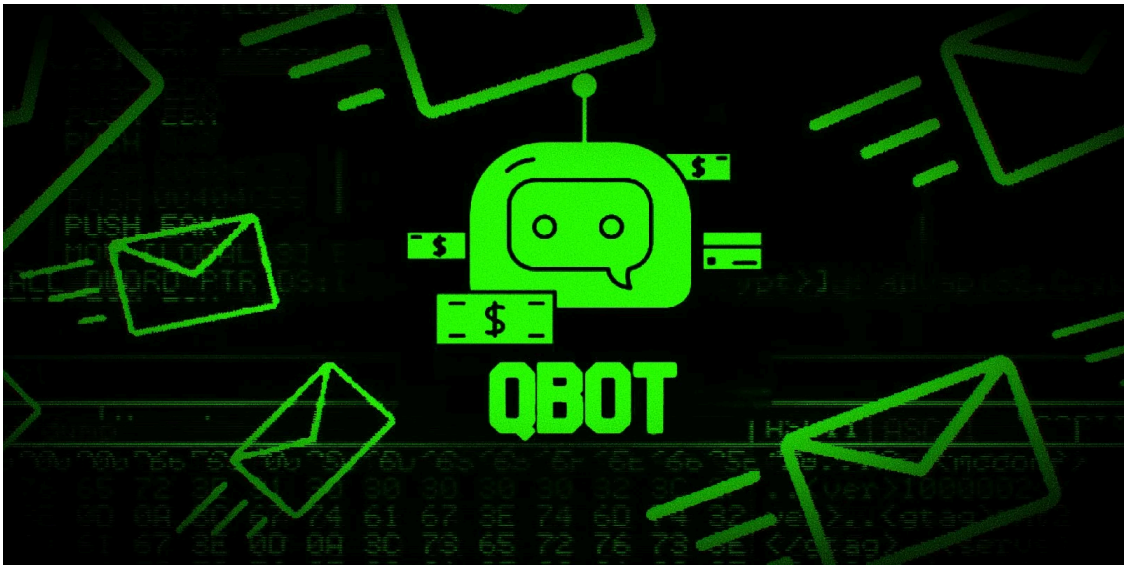
Qbot malware switched to stealthy new Windows autostart method

By Sergiu Gatlan

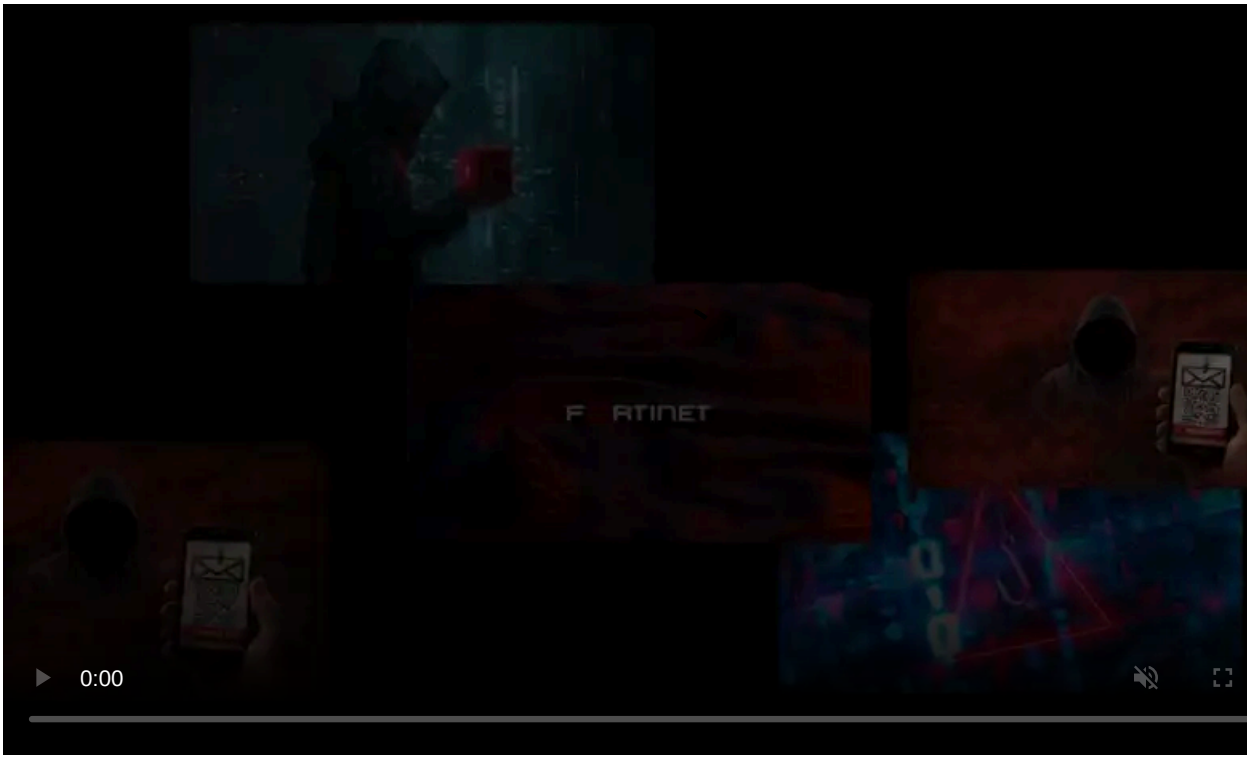
Published: 2020-12-09 · Archived: 2026-04-06 01:03:11 UTC



A new Qbot malware version now activates its persistence mechanism right before infected Windows devices shutdown and it automatically removes any traces when the system restarts or wakes up from sleep.

Qbot (also known as Qakbot, Quakbot, and Pinkslipbot) is a Windows banking trojan with worm features active since at least 2009 and used to steal banking credentials, personal information, and financial data.

The malware has also been used for logging user keystrokes, for dropping backdoors on compromised computers, and to deploy Cobalt Strike beacons used by ransomware operators to deliver ProLock and Egregor ransomware payloads.


F RTINET
0:00

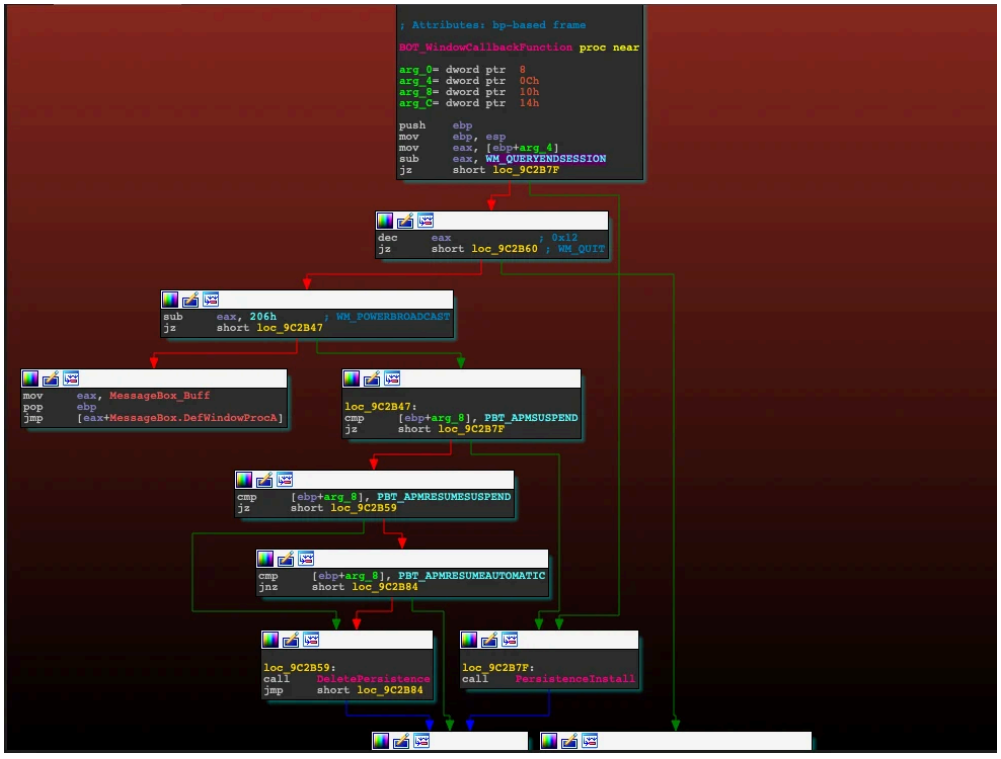
In recent campaigns, Qbot victims have been infected using phishing emails featuring Excel document attachments pretending to be DocuSign documents.

Switching to a stealthier persistence mechanism

Starting with November 24, when Binary Defense threat researcher James Quinn says that the new Qbot version was spotted, the malware is using a newer and stealthier persistence mechanism that takes advantage of system shutdown and resume messages to toggle persistence on infected devices.

This tactic is so successful that some researchers have previously thought that the Qbot trojan has removed this persistence mechanism altogether.

"While initial reports by other researchers had stated that the Run key persistence mechanism was removed in the new version of Qakbot, it has instead been added to a more stealthy and interesting persistence mechanism that listens for System Shutdown Messages, along with PowerBroadcast Suspend/Resume messages," Quinn explains.



Qbot Window message listener (*Binary Defense*)

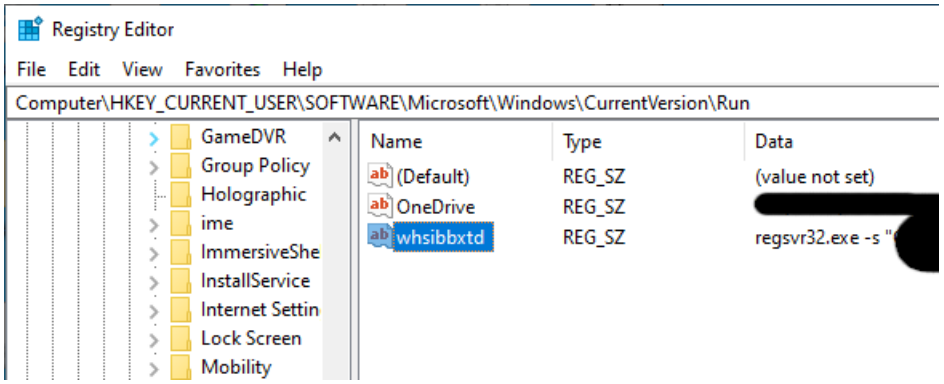
The trojan will add a registry Run key on the infected systems that allows it to automatically start on system login and will try to immediately remove it once the user powers up or wakes up the computer from sleep to evade detection by anti-malware solutions or security researchers.

What makes this technique stealthy is the perfect timing used by Qbot's developers to inject the key in the Windows registry.

The malware will only add the Run key before the system goes into sleep or shuts down but it will do it so close to it happening that "security products don’t have a chance to detect and report on the new run key."

Qbot will then try to delete the persistence key several times once it's launched again on system wake up or login.

However, because the key's value name is randomly generated on each infected system, Qbot will attempt "to delete any run keys with value data matching" its path.



Qbot Run key persistence mechanism (*Binary Defense*)

While this method for gaining persistence is new for Qbot, other malware has used similar techniques to evade detection in the past, including the Gozi and Dridex banking trojans.

"It looks like the two malware families have a similar mechanism in that they are both listening for the WM_QUERYENDSESSION and WM_ENDSESSION messages to detect when the user logs off, but the new version of Qakbot is going further by also looking for power events such as WM_POWERBROADCAST and PBT_APMSUSPEND to install its hooks when the system is suspended, too," Binary Defense threat team senior director Randy Pargman told BleepingComputer.

Installation and config changes

Qbot's installation technique has also been updated in this new version as it uses a new DLL architecture which combines the malware loader and the bot within a single DLL.

Previously the loader evaded detection by automated malware sandbox systems by storing all the malicious code in a separate DllRegisterServer component and only calling it via *regsvr32.exe* or *rundll32.exe* when using certain command-line arguments.

The new version simplifies this technique by removing the command-line arguments from the process and switching injecting the bot code into newly created processes.

"Removing the command line switches and analysis checks through new process creation (while still keeping many of the anti-analysis/anti-sandbox checks), the new loader's installation mechanism only occurs after the bot has been injected into explorer.exe," Quinn adds.

Qbot has also switched to a new in-registry encrypted config from the .dat configuration and log files previously stored on victims' compromised computers.

Source: https://www.bleepingcomputer.com/news/security/qbot-malware-switched-to-stealthy-new-windows-autostart-method/