Qbot Botnet Deploys Malware Payloads Through Malicious Windows Installers

techtimes.com/articles/274190/20220412/qbot-botnet-deploys-malware-payloads-through-malicious-windows-installers.htm

April 12, 2022

Joseph Henry, Tech Times 12 April 2022, 02:04 am
Qbot operators are now relying on infecting systems by installing malware payloads on emails. These files reportedly have malware-ridden Windows Installers.

According to cybersecurity researchers, the threat actors have done this technique for the first time. It's different from their previous tactic which is spreading malware through a document from Microsoft Office.

What the Experts Think About Qbot Malware

(Photo : Philipp Katzenberger from Unsplash)
Cybersecurity researchers have recently discovered that the Qbot operators are compromising systems by infecting Windows installers.

Per Bleeping Computer's report, the experts thought that the cybercriminals have finally responded to what the Microsoft office did earlier this year.

The Redmond firm said back in February that it will now make it tougher to activate VBA macros in Microsoft Office applications. It has reportedly kicked off this month.

In late 2021, the tech titan noted that the presence of many "malicious macros" in the Office documents (pertaining to the Excel 4.0 macros) had been evident among the attackers.

To evade further security detection systems, the threat actors make use of Excel 4.0 macros. However, to properly execute them, they will be required to manually activate them because Microsoft disabled it by default.

As such, Microsoft had done a great job in preventing hackers from gaining access to its apps. The widespread phishing schemes have been hitting Office applications. The tactic will also prevent the cybercriminals from being invaded by various malware including TrickBot, Emotet, and Qbot to name a few.

Related Article: How to Troubleshoot Windows 10 Boot Issues [2022] [To be Published on February 22]

The History of Qbot

For those unfamiliar with Qbot, it is a notorious malware known to be hitting Windows since 2007. When it infiltrates the system, it could gain access to the user's financial information, as well as some confidential details including password and email address.

The actors rely on compromising a particular network through an exploit. Previously, it has been seen to be "aggressively" attacking the Active Directory admin accounts.

A myriad of dangerous cyberhacking groups have used it already including REvil, MegaCortex, PwndLocker, ProLock, and more ransomware gangs.

Over the past years, IT admins and security analysts have learned to effectively suppress the Qbot botnet. Since it's known to launch disruptive attacks on its victims, the professionals have gotten used to its signs and what preventive measures can best stop it.

In other news, ZDNet reported that attackers are now taking advantage of the Spring4Shell flaw to spread botnet malware on their targets.

Particularly, cybersecurity firms such as Qihoo 360 and Trend Micro discovered this incident in late March.

Per Trend Micro analysts, the findings concluded that the Spring4Shell exploitation was clearly seen in the most vulnerable servers. The hackers have exploited the Mirai botnet malware to hit several systems in Singapore.

Another group of researchers from Unit 42 (Palo Alto Network) noted that the hackers made use of this flaw as their weapon. With that being said, cybercriminals have already abused it on a wide scale.

Read Also: Windows Users Beware: 95% of Ransomware Attacks Target Microsoft's OS [Google Report]

This article is owned by Tech Times

Written by Joseph Henry

Tags: Qbot Botnet Malware Malware Payload Windows Installer Security phishing