Hackers using Follina Windows zero-day to spread Qbot malware

By Jonathan Greig

Published: 2023-01-13 · Archived: 2026-04-02 11:13:53 UTC

Hackers are using a recently disclosed Windows zero-day vulnerability named Follina to spread a widely-used banking trojan with ties to several ransomware groups.

The vulnerability — CVE-2022-30190 — is in the Microsoft Support Diagnostic Tool (MSDT) in Windows and is already being exploited by several state-backed threat actors, according to reports from multiple security companies.

Follina, which was given its name by cybersecurity expert Kevin Beaumont because the sample references 0438 — the area code of Follina, Italy — currently doesn't have a patch and allows attackers to "install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights."

Almost immediately after the vulnerability was highlighted, cybersecurity firm Proofpoint said that Chinese state-sponsored hacking groups were seen exploiting the zero-day in attacks on organizations associated with the Tibetan Government in Exile. The campaigns impersonate the "Women Empowerments Desk" of the Central Tibetan Administration, the firm said.

On Tuesday, Proofpoint shared evidence that a threat actor they've named "TA570" – who they've been tracking since 2018 and is heavily associated with the Qbot malware – is now using CVE-2022-30190 to deliver the popular malware used to steal banking information.

"Actor uses thread hijacked messages with HTML attachments which, if opened, drop a zip archive," the company explained on Twitter.

"Archive contains an IMG with a Word doc, shortcut file, and DLL. The LNK will execute the DLL to start Qbot. The doc will load and execute a HTML file containing PowerShell abusing CVE-2022-30190 used to download and execute Qbot."

> Archive contains an IMG with a Word doc, shortcut file, and DLL. The LNK will execute the DLL to start Qbot. The doc will load and execute a HTML file containing PowerShell abusing CVE-2022-30190 used to download and execute Qbot.
>
> — Threat Insight (@threatinsight) June 7, 2022

Several other cybersecurity experts corroborated Proofpoint's findings this week. Nicole Hoffman, senior cyber threat intelligence analyst at Digital Shadows, told The Record that Qbot, also known as QakBot, has been identified in attacks where the Follina vulnerability was exploited.

Both Hoffman and Recorded Future ransomware expert Allan Liska noted that Qbot has a long history of coordinating with ransomware groups.

“QakBot is associated with several ransomware variants, including Conti and Black Basta, given its ability to establish a persistent foothold in target networks. It is likely only a matter of time before a ransomware group takes advantage of this,” Hoffman said.

Andrew Brandt, principal researcher at Sophos, said his team has seen Follina being used to deliver other kinds of payloads, but some of them — notably Cobalt Strike — can be used to deliver other malware, or to give ransomware actors a foothold into the network.

"But so far there doesn't seem to be any direct connection between a Follina-type attack and a subsequent ransomware incident," Brandt said.

Liska echoed those remarks, adding that while it appears QBot is using Follina, he has not seen any ransomware attacks yet exploiting the bug.

“But QBot works with a couple of different ransomware groups, so it is likely just a matter of time,” Liska said.

> New TTPs from #qakbot #qbot discovered by @k3dg3
>
> In case you haven't seen it yet, here's the top and bottom of the res.123 file downloaded by the .docx file.
>
> From the top of the file, it seems like the threat actor is feeling pretty cocky right now. Bottom shows #follina use. pic.twitter.com/dMXOTF1te7
>
> — ExecuteMalware (@executemalware) June 7, 2022

Proofpoint previously said Qbot’s operators had been seen delivering several different kinds of ransomware including ProLock and Egregor.

France’s Computer Emergency Response Team (CERT-FR), a division of ANSSI, the country’s national cybersecurity agency, released a lengthy report in November that found the Lockean ransomware affiliate group would deploy the QakBot malware during attacks.

Qbot has seen a resurgence in activity since the takedown of Emotet, with multiple companies reporting a surge in activity since January 2021. Group-IB researchers found that Qbot has also been used by Prometheus, a cybercrime service that helps malware gangs distribute malicious payloads.

Microsoft previously told The Record that it did not know when a patch will be released for CVE-2022-30190 but pointed to the documents they published about ways the issue can be mitigated.

Several security researchers tested the issue and found it affects Office 2013, 2016, 2019, 2021, Office ProPlus and Office 365.

Researchers published suggestions for security teams of things they can do to limit exposure, including removing the ms-msdt URI schema registry key.

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
