Hackers Tricked Microsoft Into Certifying Malware That Could Spy on Users

vice.com/en/article/pkbzxv/hackers-tricked-microsoft-into-certifying-malware-that-could-spy-on-users

Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

See More →

Hackers were able to trick Microsoft into certifying a malicious driver that, if installed, would be able to decrypt internet traffic on an infected computer and send it to a third party.

On June 17, a security researcher found that Microsoft had signed a rootkit, a dangerous type of malware that has the ability to be persistent and capture practically all data on an infected computer. Whoever is behind this attack was able to make their malware look like a legitimate driver approved by Microsoft, giving them the ability to bypass most computers' protections.

On Friday, Microsoft published a blog post revealing that the hackers behind the malware were "distributing malicious drivers within gaming environments."

"The actor's activity is limited to the gaming sector specifically in China and does not appear to target enterprise environments," Microsoft wrote. "The actor's goal is to use the driver to spoof their geo-location to cheat the system and play from anywhere. The malware enables them to gain an advantage in games and possibly exploit other players by compromising their accounts through common tools like keyloggers."

Microsoft published a more in-depth analysis of the hack in a report that is only for customers and not available to the public. A Microsoft spokesperson declined to provide more details about the incident.

> **Do you have more information about this malware? We'd love to hear from you. Using a non-work phone or computer, you can contact Lorenzo Franceschi-Bicchierai securely on Signal at +1 917 257 1382, lorenzofb on Wickr and Wire, or email lorenzofb@vice.com**

Karsten Hahn, the security researcher who first found the malware and works for antivirus firm G Data, wrote in a blog post published last week that he and his colleagues were able to find older samples of the malware, dating back to March 2021.

"What really unsettles me is that this malware was undetected for many months," Hahn told Motherboard. "The worst is the demonstration that this incident shows you can still create kernel mode rootkits for Windows 10 by slipping through the [Microsoft] driver signing process. And that may in turn lead to more threat actors trying this."

In a blog post published last week, Hahn wrote that he and his colleagues were able to find older samples of the malware, dating back to March 2021. Hahn said he called the malware Netfilter because that word appears repeatedly in the code. Netfilter is also a Linux open source framework to filter network traffic. Microsoft called the malware Retliften, the reverse of Netfilter.

Kevin Beaumont, a security researcher and former Microsoft employee, said that the hack "impacts thousands of Chinese made games," according to the paywalled report. The malware was designed to install certificates on the victims' computers in order to decrypt their internet traffic, Beaumont wrote on Twitter. Johann Aydinbas, another security researcher who has analyzed the malware, also found that "the core functionality seems to be eavesdropping on SSL connections," meaning encrypted internet traffic.

Modern Windows PCs are designed to only run signed drivers, meaning Microsoft reviewed them and certified they are safe In this case, the hackers tried to hide their malware in a Netfilter driver that has the ability to intercept internet traffic, according to Sherrod DeGrippo, the senior director of threat research and detection at cybersecurity firm Proofpoint.

"Given these drivers have the ability to operate on packet-level network communications, intercepting existing traffic is trivial, allowing the author of the malicious code the ability to do whatever they want with said traffic," DeGrippo told Motherboard in an email.

Microsoft wrote in the blog post that hackers would only be able to use the malware after getting access to a victim's computer, meaning the signed rootkit was designed to be part of a second or further step in an hypothetical attack, which needed the hackers to "either have already gained administrative privileges in order to be able to run the installer to update the registry and install the malicious driver the next time the system boots or convince the user to do it on their behalf."

Microsoft didn't say who exactly was targeted or actually hacked, nor who is behind the attack, only that the hackers were not "a nation-state actor."

"The malware itself is not wide-spread," Hahn said, arguing that if it was, G Data would have "seen telemetry," the industry lingo for data on actual attacks.

Microsoft also did not share many details about how exactly the hackers tricked the company into certifying their malware, saying only that they "submitted drivers for certification through the Windows Hardware Compatibility Program."

"The drivers were built by a third party," Microsoft added. "We have suspended the account and reviewed their submissions for additional signs of malware."

Users who have Windows Defender are now protected against this malware, and so should be people who use other antivirus software, according to Microsoft.

Subscribe to our cybersecurity podcast, CYBER.