Hackers exploit gaping Windows loophole to give their malware kernel access



Getty Images

reader comments

38 with

Hackers are using open source software that’s popular with video game cheaters to allow their Windows-based malware to bypass restrictions Microsoft put in place to prevent such infections from occurring.

The software comes in the form of two software tools that are available on GitHub. Cheaters use them to digitally sign malicious system drivers so they can modify video games in

ways that give the player an unfair advantage. The drivers clear the considerable hurdle required for the cheat code to run inside the Windows kernel, the fortified layer of the operating system reserved for the most critical and sensitive functions.

Researchers from Cisco's Talos security team said Tuesday that multiple Chinese-speaking threat groups have repurposed the tools—one called HookSignTool and the other FuckCertVerifyTimeValidity. Instead of using the kernel access for cheating, the threat actors use it to give their malware capabilities it wouldn't otherwise have.

A new way to bypass Windows driver restrictions

"During our research we identified threat actors leveraging HookSignTool and FuckCertVerifyTimeValidity, signature timestamp forging tools that have been publicly available since 2019 and 2018 respectively, to deploy these malicious drivers," the researchers wrote. "While they have gained popularity within the game cheat development community, we have observed the use of these tools on malicious Windows drivers unrelated to game cheats."

With the debut of Windows Vista, Microsoft enacted strict new restrictions on the loading of system drivers that can run in kernel mode. The drivers are critical for devices to work with antivirus software, printers, and other kinds of software and peripherals, but they have long been a convenient inroad for hackers to run malware in kernel mode. These inroads are available to hackers post-exploit, meaning once they've already gained administrative privileges on a targeted machine.

Advertisement
While attackers who gain such privileges can steal passwords

and take other liberties, their malware typically must run in the Windows kernel to perform a large number of more advanced tasks. Under the policy put in place with Vista, all such drivers can be loaded only after they've been approved in advance by Microsoft and then digitally signed by a trusted certificate authority to verify they are safe.

Malware developers with admin privileges already had one well-known way to easily bypass the driver restrictions. The technique is known as "bring your own vulnerable driver." It works by loading a publicly available third-party driver that has already been signed and later is found to contain a vulnerability allowing system takeover. The hackers install the driver post exploit and then exploit the driver vulnerability to inject their malware into the Windows kernel.

Although the technique has existed for more than a decade, Microsoft has yet to devise working defenses and has yet to provide any actionable guidance on mitigating the threat despite one of its executives publicly lauding the efficacy of Windows to defend against it.

The technique Talos has discovered represents a new way to bypass Windows driver restrictions. It exploits a loophole that has existed since the start of the policy that grandfathers in older drivers even when they haven't been reviewed for safety by Microsoft. The exception, designed to ensure older software was still able to run on Windows systems, is triggered when a driver is signed by a Windows-trusted certificate authority prior to July 29, 2015.

"If a driver is successfully signed this way, it will not be prevented from being installed and started as a service," Tuesday's Talos post explained. "As a result, multiple open source tools have been developed to exploit this loophole. This is a known technique though often overlooked despite posing a serious threat to Windows systems and being relatively easy to perform due in part to the tooling being

publicly available.”

https://arstechnica.com/?p=1952993