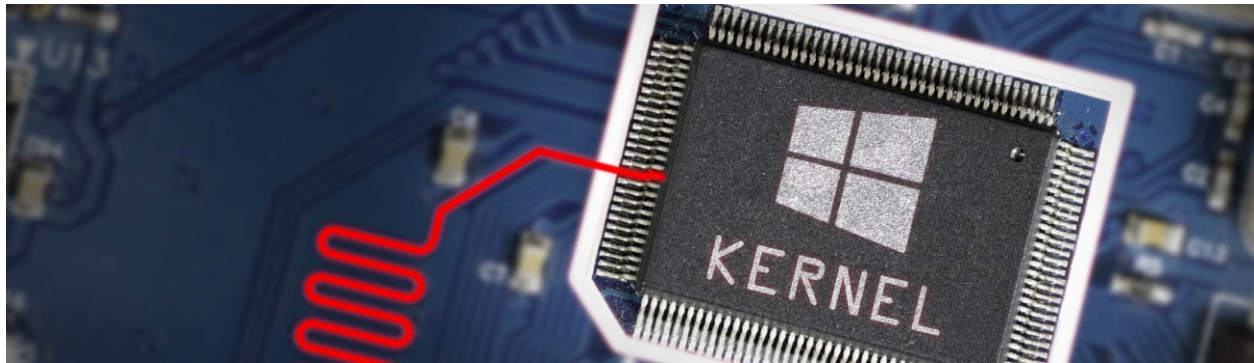


## Microsoft signed a driver called Netfilter, turns out it contained malware



Microsoft acknowledged the incident and currently investigating the issue but at the same time downplaying its impact.

In recent news, it has been found that Microsoft signed off a third-party driver, Netfilter, for Windows that contains rootkit malware and has been circulating mainly amongst the gaming community.

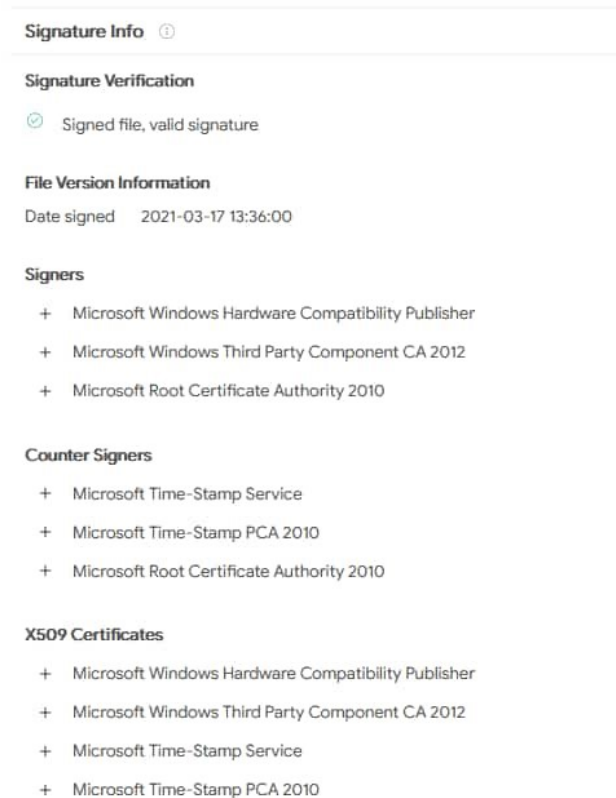
This was first found out by Karsten Hahn, a G Data malware analyst, who tweeted about this after noticing the “Netfilter” which he later traced, analyzed, and identified as bearing Microsoft’s seal.

When Microsoft observed the rootkit, it was found out that it communicated with Chinese command-and-control IPs (C2) and as it turns out, these belong to one of the companies that the United States Department of Defense labeled as “Community Chinese Military”.

The driver maker, Ningbo Zhuo Zhi Innovation Network Technology, was working with Microsoft to study and patch any known security holes, including for affected hardware. Users will get clean drivers through Windows Update.

Although Microsoft admitted its mistake and started investigating the incident, they did downplay the impact of the driver. They focused on the idea that since the driver was aimed at gamers and only circulated in the gaming community, it isn’t known to have compromised any enterprise users.

Moreover, they added that the rootkit only works if a user authorizes the driver and it obtains administrator-level access on a PC to install the driver. The idea is that Netfilter won't pose a threat to your PC unless you go out of your way to install it.



The screenshot displays the Windows File Signature Verification tool interface. It is titled "Signature Info" with a help icon. Below the title, there is a "Signature Verification" section showing a green checkmark icon and the text "Signed file, valid signature". The "File Version Information" section shows "Date signed" as "2021-03-17 13:36:00". There are three sections of signers: "Signers" (Microsoft Windows Hardware Compatibility Publisher, Microsoft Windows Third Party Component CA 2012, Microsoft Root Certificate Authority 2010), "Counter Signers" (Microsoft Time-Stamp Service, Microsoft Time-Stamp PCA 2010, Microsoft Root Certificate Authority 2010), and "X509 Certificates" (Microsoft Windows Hardware Compatibility Publisher, Microsoft Windows Third Party Component CA 2012, Microsoft Time-Stamp Service, Microsoft Time-Stamp PCA 2010).

### *Netfilter Signature*

In a blog post, Microsoft said it would be “refining” the signing process, partner access policies, and validation. The tech giant announced that it has already suspended the account and is now being reviewed to submit added malware signs.

“We have seen no evidence that the WHCP signing certificate was exposed. The infrastructure was not compromised, Microsoft said.

The actor’s activity is limited to the gaming sector specifically in China and does not appear to target enterprise environments. We are not attributing this to a nation-state actor at this time, the company revealed.

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, warned Microsoft.”

Nevertheless, the incident isn't entirely comforting. Many people see a signed driver as confirming that a driver or program is safe. Those users might be hesitant to install new drivers in a timely fashion if they're worried there might be malware, even if those drivers come straight from the manufacturer.

#### References:

- <https://www.gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit>
- [https://www.hackread.com/microsoft-netfilter-driver-sign-rootkit-malware/?web\\_view=true](https://www.hackread.com/microsoft-netfilter-driver-sign-rootkit-malware/?web_view=true)
- <https://newsnationusa.com/news/technology/cyber-security/hackers-trick-microsoft-into-signing-netfilter-driver-loaded-with-rootkit-malware/>