Fast Insights for a Microsoft-Signed Netfilter Rootkit

By Giancarlo Lezama

Published: 2021-08-10 · Archived: 2026-04-05 21:20:14 UTC

Automate malware analysis of Netfilter rootkit and other advanced threats. Obtain deep insights without long, manual effort.

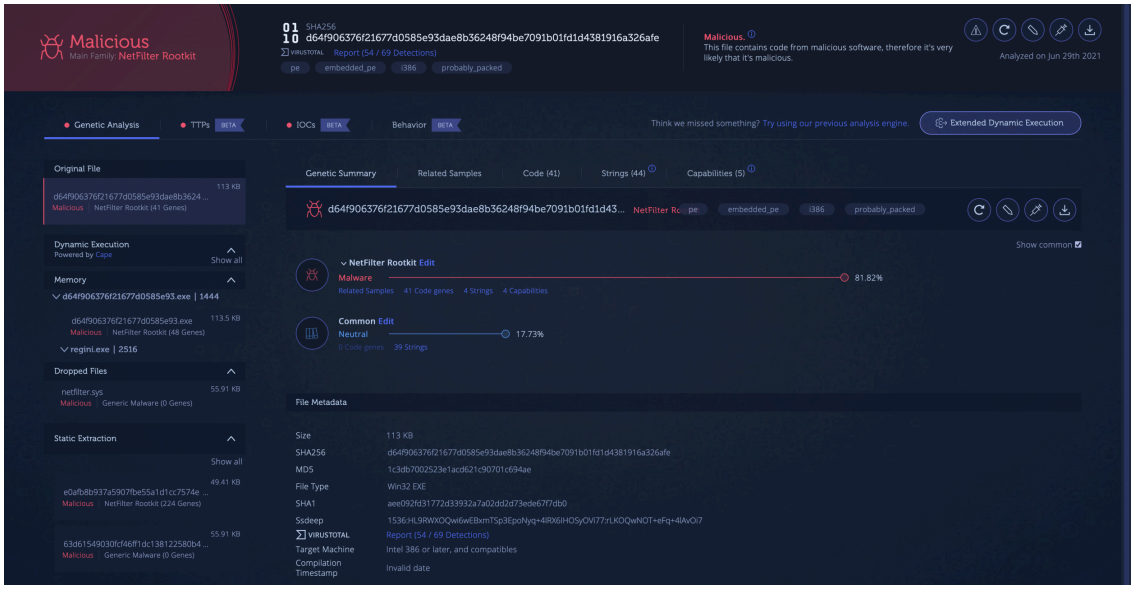
News broke in June about a malicious Netfilter rootkit signed by Microsoft. This was significant in that Windows machines only run drivers with valid signatures. Since drivers can obtain the maximum level of permissions on a machine, they are gold for any threat actor who can obtain such access.

Thanks to malware analysts like Karsten Hahn, additional samples of this malware dating back to March were uncovered, along with details on how they operate. Let's look at the genetic analysis of these samples to see how you can quickly identify them as Netfilter rootkit, as well as understand their capabilities and obtain similar artifacts despite the valid signature.

The Netfilter rootkit was found in a driver signed by Microsoft. This rare technique bypasses defenses, such as Antivirus tools, by making the file appear legitimate, despite the fact that it is tampered with malicious code. Obfuscated strings were also found in this file, which is very uncommon for a legitimate file. When the file is executed, other URLs can be identified, each with a specific purpose, including redirecting infected endpoints to other IP addresses; for self-updating the malware and receiving the valid root certificate.

Detection of malware with valid signatures is challenging. Since these samples are signed legitimately by Microsoft, even Antivirus software can be fooled into trusting them. An analyst could try investigating the abnormal network connections made to the URLs during execution. The URLs might be useful for this variant but there is no way of telling what changes could be made to URLs in future malware variants, or whether the external server the rootkit connects to is hidden from network detection tools through methods such as DynDNS or proxies. Not to mention, how do you know the full extent of the capabilities in the driver? Once a rootkit is executed, it will totally own a machine with maximum permissions, hiding its activities from even endpoint detection solutions.

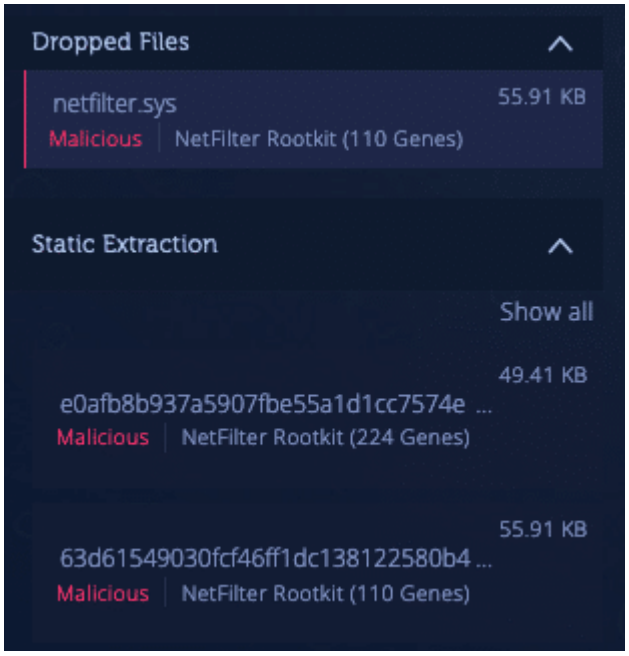
Let's take a look at the analysis of the Netfilter Dropper sample referenced in the aforementioned article.

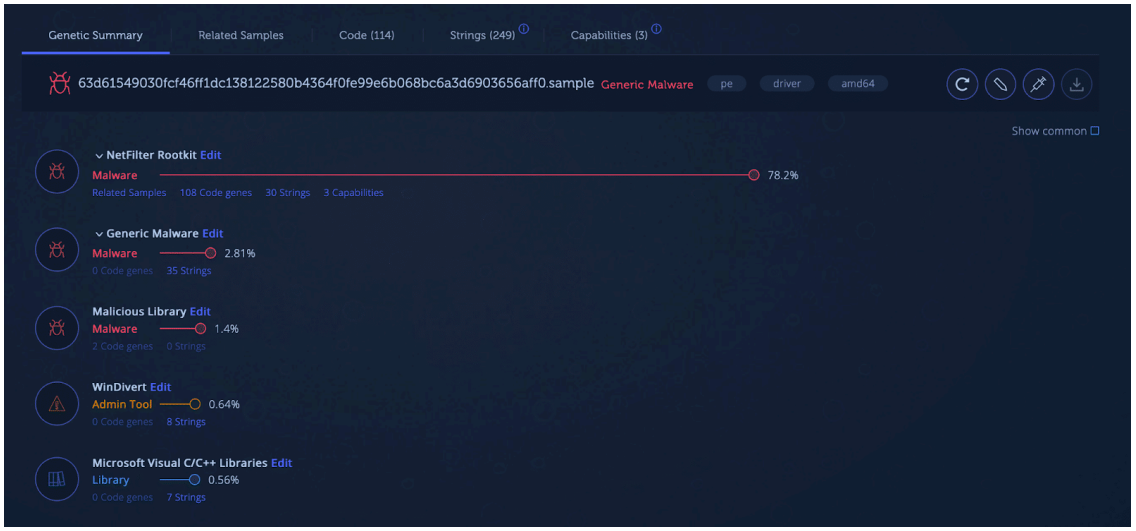


With Intezer Analyze you can analyze malware threats in seconds, with every tool you need to do so in one place: *genetic code analysis*, *sandboxing*, *memory analysis* and *static analysis*.

The original file is classified as Netfilter rootkit, where an analysis of the code finds that the file shares 41 code genes, or about 81% of its code (click Show common code), with previously identified Netfilter rootkit samples. It is clear that although the uploaded dropper has a valid signature, the code itself is identified as malicious and belongs to the Netfilter rootkit.

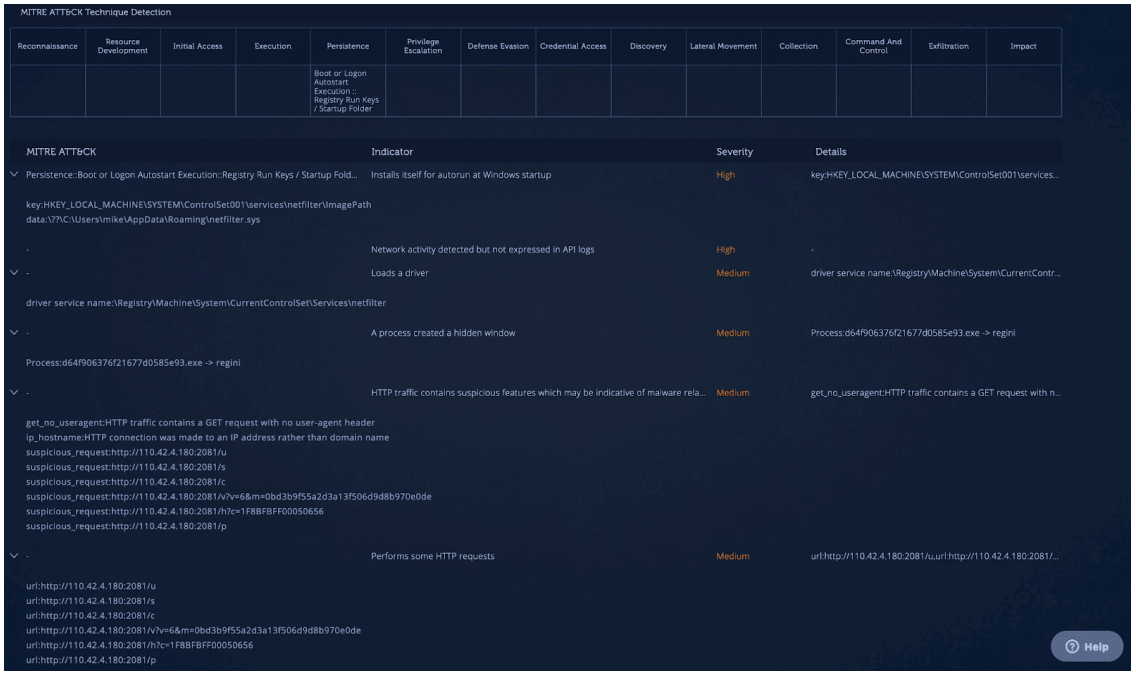
Sometimes, an analysis isn't always this easy. Files can be obfuscated by being packed, encoded, or delivered in the form of installers. For this reason, Intezer also has the ability to statically extract relevant files packed in the original file, as well as dynamically execute the original file in order to see how it executes. In this particular analysis, the driver is embedded in the dropper, which gets dropped onto the disk during execution in the sandbox.



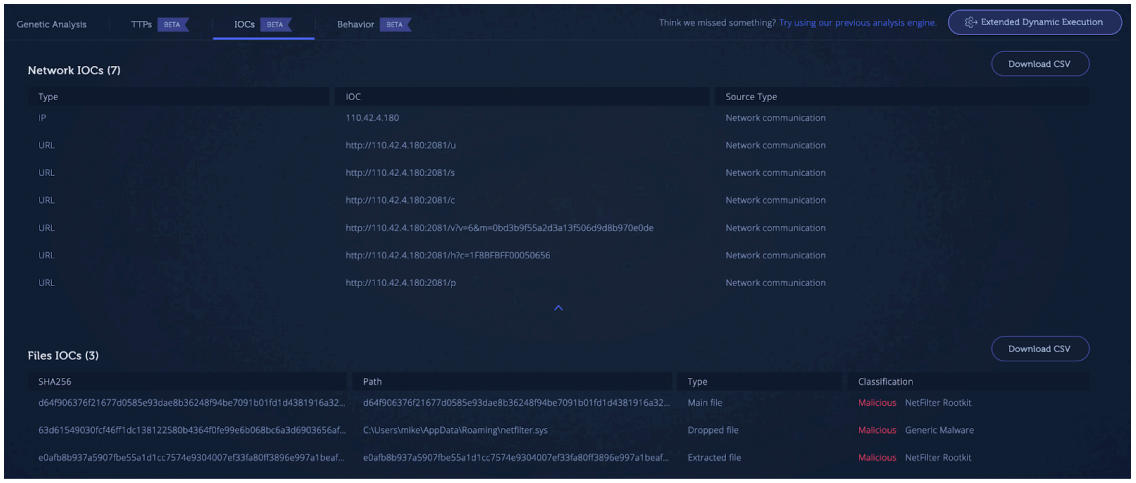


With Intezer Analyze you don't get a blackbox. Instead, you can see exactly in which malware samples the malicious Netfilter rootkit code of the dropper (as well as the dropped files) have been seen before.

Intezer's sandboxing capabilities capture what the file did during execution within the context of the MITRE ATT&CK® framework. This provides an immediate sense of what suspicious or malicious activity the file is capable of in order to help you assess the risk. The highest risk behavior found in this file is the ability to persist on an endpoint by making adjustments to the Windows Registry.



Another interesting behavior is the resulting network activity from the file's execution, providing us with network IoCs for this file. These network IoCs, along with the file's IoCs uncovered when the file was executed or via static extraction, make up the full list of IoCs shown in a separate tab for ease of access.



The network IoCs are identical to the ones provided in the GData article, each with a distinct purpose as mentioned.

To summarize, there is a lot of information related to the investigation of this malware that can be easily extracted through genetic code analysis and other fundamental techniques with Intezer 's malware analysis tool.

Consider that most malware must evolve into new variants in order to evade detection but their code mostly remains the same. Behavioral analysis and signatures can be evaded by advanced malware like this Netfilter rootkit, but the code doesn't lie.

Intezer Analyze covers every malware-related incident. Scan files, live machines, memory dumps and URLs (coming soon) to get fast verdicts, TTPs, IoCs and more. Sign up for free and start with 50 file uploads per month.
