

# Microsoft signed a malicious Netfilter rootkit

By Karsten Hahn

Published: 2021-06-26 · Archived: 2026-04-05 17:52:44 UTC

06/25/2021



Reading time: 3 min (805 words)

What started as a false positive alert for a Microsoft signed file turns out to be a WFP application layer enforcement callout driver that redirects traffic to a Chinese IP. How did this happen?

Last week our alert system notified us of a possible false positive because we detected a driver<sup>[1]</sup> named "Netfilter" that was signed by Microsoft. Since Windows Vista, any code that runs in kernel mode is required to be tested and signed before public release to ensure stability for the operating system. Drivers without a Microsoft certificate cannot be installed by default.

In this case the detection was a true positive, so we forwarded our findings to Microsoft who promptly added malware signatures to Windows Defender and are now conducting an internal investigation. At the time of writing it is still unknown how the driver could pass the signing process.

---

## Signature Info ⓘ

---

### Signature Verification

✔ Signed file, valid signature

### File Version Information

Date signed 2021-03-17 13:36:00

### 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

### X509 Certificates

- + Microsoft Windows Hardware Compatibility Publisher
- + Microsoft Windows Third Party Component CA 2012
- + Microsoft Time-Stamp Service
- + Microsoft Time-Stamp PCA 2010

## String decoding

The first thing I noted after opening the strings view are some strings that looked encoded or encrypted. While this is not necessarily a sign of a malicious file, it is odd that a driver obfuscates a part of their strings.

I decoded the strings using the following Python snippet.

## Similar samples

Searching for this URL as well as the PDB path and the similar samples feature on Virustotal we found older samples as well as the dropper<sup>[2]</sup> of the netfilter driver. The oldest sample<sup>[3]</sup> signatures date back to March 2021. Virustotal queries to find similar samples via URL and PDB path are listed below.



The URL **hxxp://110.42.4.180:2081/u** in the decoded string listing is the server of the rootkit. The Netfilter driver<sup>[1]</sup> connects to it for fetching configuration information.

After connecting to the hardcoded URL **hxxp://110.42.4.180:2081/u** the server replies with the following string.

```
http://110.42.4.180:2081/p|http://110.42.4.180:2081/s|http://110.42.4.180:2081/h?|http://110.42.4.180:2081/c|http://110.42.4.180:2081/v?
```

Each URL has a specific purpose.

URL	Purpose
hxxp://110.42.4.180:2081/p	Proxy settings
hxxp://110.42.4.180:2081/s	Redirection IPs
hxxp://110.42.4.180:2081/h?	Ping with CPU-ID
hxxp://110.42.4.180:2081/c	Root certificate
hxxp://110.42.4.180:2081/v?	Self update

## IP redirection

The core functionality of the malware is its IP redirection. A list of targeted IP addresses are redirected to **45(.)248.10.244:3000**. These IP addresses as well as the redirection target are fetched from **hxxp://110.42.4.180:2081/s**.

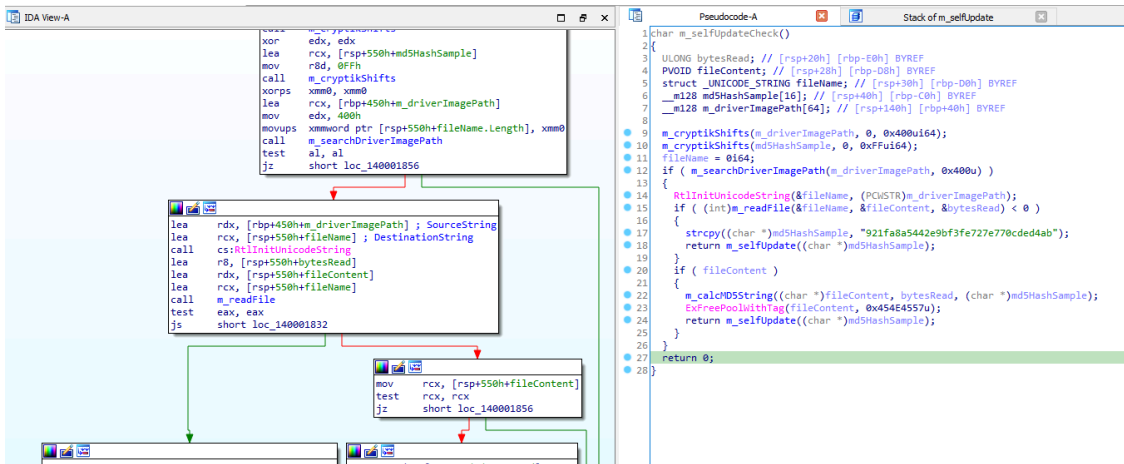
Researcher [@jaydinbas](#) reversed the redirection configuration in [this tweet](#) and provided the latest decoded configuration in a [pastebin](#). The general format as observed by [@cci\\_forensics](#) and [@jaydinbas](#) is **[<redirection\_target>-<port\_number>]{<ip\_to\_redirect1>|<ip\_to\_redirect2>|...}**

```
[4094359597-3000]{1464145256|69263383|497747674|2982364076|2551807136|3772516455|764096103|86040599|44762842|1363722247|102817815|52486167|4270973207|1382844424|3424802919|2669828199|3796332335|799737562|1443357739|4198110568|3707017152|1495160748|1525830477|2283279464|1015774818|1832714087|191815703|423092247|867314886|1973505994|3349269402|3443154063|3115381295|649849191|172557221|924686107|227626803|244402991|1826395243|1605686178|3542016279|3270455440|3111378691|644940709|247776410|3337446336|1622463394|382429463|2002031814|2632891358|3502796604|1454523308|2802502972|1877660058|656086938|4243976092|2792397948|740892773|2635273576|2102695110|9935182|3729368389|2325472555|1834992941|3102683280|804335770|4074970231|3481813932|2107196332|3452652335|2651645799|871190682|2382952747|3352445868|1028593000|90176418|4232242219|2596488108|395723692|3391624552|217355367|3020952936|4056641837|3576298029|3379469394|459882668|771699303|3573841963|2134185320|4087497644|3322760039|62210988|2088846252|93209516|2903577960|246089434|3426424168|3970977639|4001613379|2316109722|55386213|1513125052|830136167|2336269637|2487264581|254988698|174242411|3675854184|1000227756|106953634|3910271563|1668696774|2981011560|924325224|4196577161|2652837224|3883815115|2672563560|667441882|472061288|3423999336|635061164|2816801579|706804503|2135954792|3063497644|3803951786|3214492588|1102959010|183420570|4258087852|2597650093|1856430721|1681462632|289976
```

Encoded redirection configuration

## Update mechanism

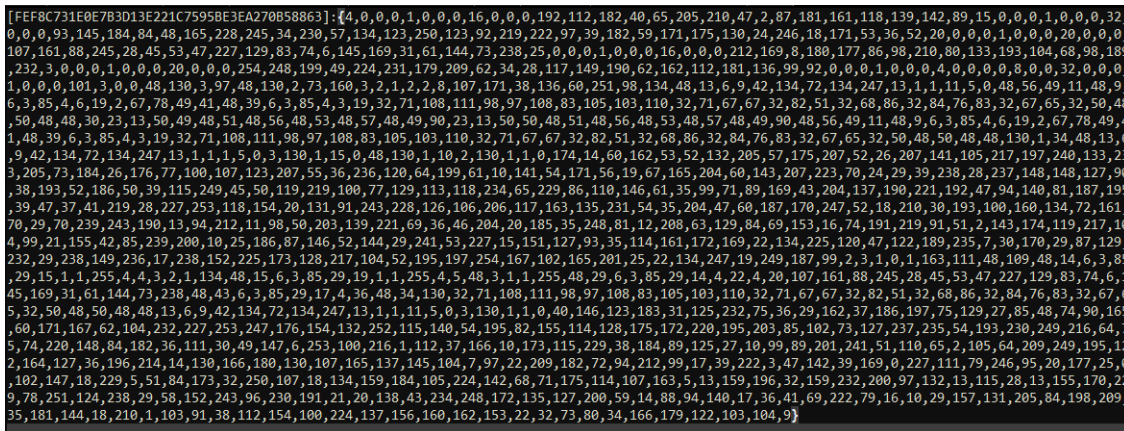
The sample has a self-update routine that sends its own MD5 hash to the server via **hxxp://110.42.4.180:2081/v?v=6&m=<md5>**. A request might look like this: **hxxp://110.42.4.180:2081/v?v=6&m=921fa8a5442e9bf3fe727e770cded4ab**. The server then responds with the URL for the latest sample, e.g., **hxxp://110.42.4.180:2081/d6** or with OK if the sample is up-to-date. The malware replaces its own file accordingly.



Code that checks if the driver is up-to-date and replaces it with a newest version.

## Root certificate

The rootkit receives a root certificate via `hxxp://110.42.4.180:2081/c` and writes it to `\Registry\Machine\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\`. The data that is returned from the server has the format [`<certificate name>`]:{`<certificate data blob>`}



Root certificate data as it is sent by the server

## Proxy

At `hxxp://110.42.4.180:2081/p` the malware requests the proxy which it sets as **AutoConfigURL** in the registry key `\Software\Microsoft\Windows\CurrentVersion\Internet Settings`. The returned value at the time of writing is `hxxp://ptaohuawu.bagua.com.hgdjkggh.com:2508/baidu.txt`

## Sample hashes

Description	SHA256
[1] Netfilter driver	63d61549030fcf46ff1dc138122580b4364f0fe99e6b068bc6a3d6903656aff0
[2] Netfilter dropper	d64f906376f21677d0585e93dae8b36248f94be7091b01fd1d4381916a326afe

Description	SHA256
[3] Netfilter driver, older version signed in March	115034373fc0ec8f75fb075b7a7011b603259ecc0aca271445e559b5404a1406

More hashes related to the Netfilter rootkit are in [this spreadsheet](#) created by [Florian Roth](#).

---

---

#### Share Article

---

#### Content

- [String decoding](#)
  - [Similar samples](#)
  - [Dropper and installation](#)
  - [Command and control server](#)
  - [IP redirection](#)
  - [Update mechanism](#)
  - [Root certificate](#)
  - [Proxy](#)
  - [Sample hashes](#)
  - [Contributions](#)
- 
- 

Source: <https://www.gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit>