Threat Bulletin: Fire in the Woods – A New Variant of FireWood

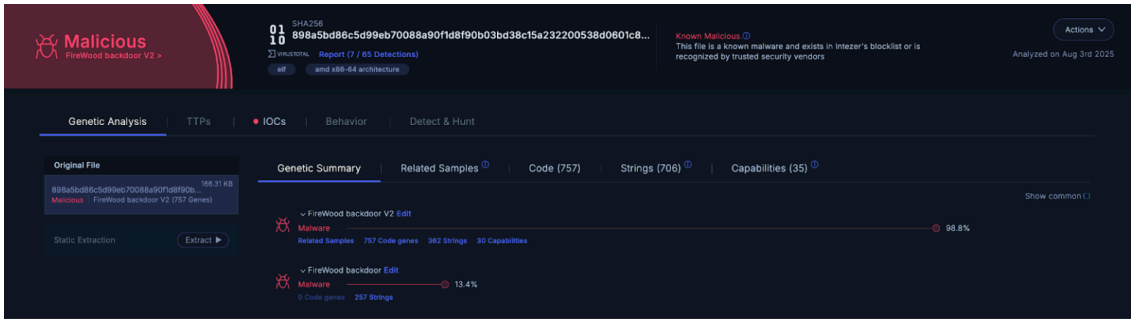
By Nicole Fishbein

Published: 2025-08-13 · Archived: 2026-04-05 22:55:16 UTC

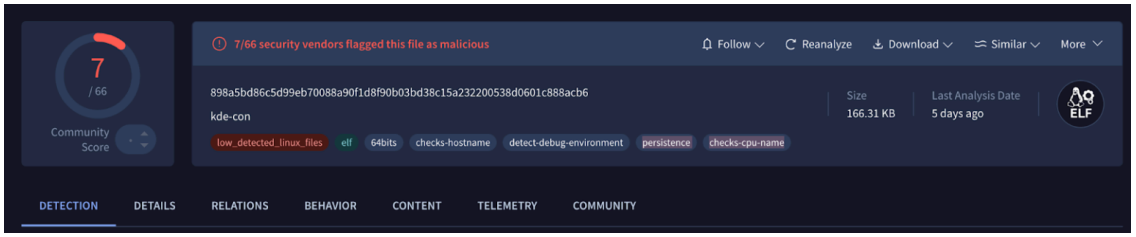
A new and low-detected variant of the FireWood backdoor was discovered by Intezer's Research Team, with some changes in the implementation and the configuration of the backdoor.

FireWood is a Linux backdoor discovered by ESET's research team. They linked it to the long-running "Project Wood" malware lineage, which dates back to at least 2005 and includes usage in the earlier Operation TooHash campaign. It functions as a remote access trojan (RAT) on Linux systems, employing kernel-level rootkit modules (e.g., usbdev.ko) and TEA-based encryption to hide its presence, maintain persistence, and communicate covertly with its command-and-control infrastructure. Once deployed, likely via web shells left on compromised Linux desktops, it enables attackers to execute commands, exfiltrate sensitive data such as system information and credentials, and operate stealthily over prolonged espionage operations. The backdoor has low confidence connections to the China-aligned Gelsemium APT group, as the overlaps may be coincidental or reflect shared tools across multiple groups.

We found a new and low-detected variant of the FireWood backdoor. The core functionality of the backdoor remains the same but we did notice some changes in the implementation and the configuration of the backdoor. It is unclear if the kernel module was also updated as we were not able to collect it.



Code analysis of the new version in Intezer.



SHA256: 898a5bd86c5d99eb70088a90f1d8f90b03bd38c15a232200538d0601c888acb6

Technical Analysis of New Firewood Variant

In the older variant, execution began with an explicit permission gate, calling `CUser::IsSuc()`, and the process would exit if this check failed. In the newer build, that early check is removed entirely. The new version defers any root-or-kernel gating until after it daemonizes and saves its PID. To achieve this, the code splits the former `SavePidAndCheckKernel()` helper into two discrete steps: an early `SavePid(pid)`, followed later by `CModuleControl::AutoLoad()` and `CheckLkmLoad()`. This separation clarifies the startup sequence and enhances the hide-via-kernel-module logic. Additionally, rather than simply sending a stripped-down identifier, the updated version builds a larger buffer containing the process name, hex-formatted port, PID, a hardcoded "kde-tra" process name, and a configurable flag (or the literal "nothing"). That extra metadata is passed through `CHideProcess::NetLinkInit()`, `CHideProcess::SendProcessName(&CHideProcess::mInstance)`, and `CHideProcess::Destroy()`.

Note the typo in the method name "Destroy", this error also appears in the older Firewood variant. Another typo persists in both versions in the following error message: "Get Memory Faile".

New evasion implementation and comparison of main functions

On the networking side, the older version read configuration settings that defined both the number of days between beaconing and a `delayTime` specifying the interval between packets. It also used a randomized time-window algorithm to stagger connections. The new build collapses all of this into a straightforward `while (true)` loop. After waiting for the configured startup delay, it continuously calls `ConnectToSvr()`, sleeping briefly on failure, until success or until the overall timer expires, then cleans up and exits. By removing the multi-stage scheduling and random timing logic, the connection routine becomes more predictable and maintainable, trading temporal obfuscation for reliable C2 reachability.

Overall, the communication protocol and C2 setup remain the same; the only significant change is that the new version no longer relies on timeouts from the configuration.

Both Firewood versions collect information about the user and the infected machine. The new variant adds a fallback for OS detection: whereas the older version reads distribution data from `/etc/issue`, the new version falls back to `/etc/issue.net` if `/etc/issue` is unavailable, parsing the data in the same way.

The backdoor defines file paths used by both itself and its kernel module. The new variant sets paths for root users as:

```
 /usr/lib/.kde-root/

/usr/lib/.kde-root/lib/

/usr/lib/.kde-root/data/

/usr/lib/.kde-root/kdeinit

/usr/lib/.kde-root/pid

/etc/init.d/rc.local
```

For non-root users, it uses:

```
 $HOME/.kde-root/

$HOME/.kde-root/lib/

$HOME/.kde-root/data/

$HOME/.kde-root/kdeinit

$HOME/.kde-root/pid

$HOME/.bashrc
```

By contrast, the older variant for root users used:

```
 /etc/init.d/rc.local

/etc/rc.d/rc.local

/etc/init.d/boot.local
```

And for non-root users:

```
 $HOME/.bashrc
```

The FireWood backdoor supports a number of commands documented by ESET. The new variant removes some commands and adds others. It drops commands for changing beacon intervals and delay times (command IDs 0x111, 0x113, 0x114), as these settings are no longer used. It also removes the file-read command (ID 0x201). The process-hiding command has moved to ID 0x202 (from 0x112), and the `HideModule` function was removed. A new command (`SetAutoKillEl` , ID 0x160) toggles or sets an “auto-kill” feature in the agent.

Besides these commands, there are also three commands that appear in both versions and were not previously documented:

- Command id 0x109: A command that indicates a change in the connection configuration.
- Command id 0x192: Gets a file from the C2 and execute it using the system function. Unlike the previously documented command id 0x185, this command calls first ‘CFileControl::FileUp’ to receive the file from the C2.
- Command id 0x195: Exfiltration of files with the following extensions: v2, .k2, .W2, and drive.C2.

We also located an older sample submitted to VirusTotal from Iran on February 5, 2025:

```
4c293309a7541edb89e3ec99c4074584328a21309e75a46d0ddb4373652ee0d6
```

Additionally, we found a sample from the Philippines submitted on May 7, 2022; its code is identical to the one we analyzed:

```
d7be3494b3e1722eb28f317f3b85ee68bf7ea5508aa2d5782392619e078b78af
```

IOCs

New Firewood Version

```
898a5bd86c5d99eb70088a90f1d8f90b03bd38c15a232200538d0601c888acb6

d7be3494b3e1722eb28f317f3b85ee68bf7ea5508aa2d5782392619e078b78af
```

Old Firewood Version

```
cff20753e36a4c942dc4dab5a91fd621a42330e17a89185a5b7262280bcd9263

4c293309a7541edb89e3ec99c4074584328a21309e75a46d0ddb4373652ee0d6
```

Source: https://intezer.com/blog/threat-bulletin-firewood/