FireWood Malware Targets Linux Systems for Command Execution and Da

Data: 2025-08-15 08:51:58

Autor: Inteligência Against Invaders

Intezer's Research Team has uncovered a new, low-detection variant of the FireWood backdoor, a

sophisticated Linux-based remote access trojan (RAT) initially discovered by ESET researchers.

Linked to the “Project Wood” malware lineage dating back to 2005, FireWood is associated with espionage campaigns like Operation TooHash and shows low-confidence ties to the China-aligned Gelsemium APT group, though these overlaps could stem from shared tooling among multiple threat actors.

Discovery of New Variant

The malware deploys kernel-level rootkit modules, such as usbdev.ko, and uses TEA-based encryption for stealthy communication with command-and-control (C2) servers.

Typically introduced via web shells on compromised Linux desktops, it enables attackers to execute arbitrary commands, exfiltrate sensitive data including system details and credentials, and maintain long-term persistence for covert operations.

The new variant retains core functionalities but introduces refinements in implementation and configuration, enhancing its evasion and operational efficiency without altering the fundamental protocol.

In the updated FireWood variant, significant changes streamline the startup sequence and evasion tactics.

Unlike the older version, which enforced an explicit permission check via CUser::IsSuc() at execution onset, the new build eliminates this gate, deferring root-or-kernel validations until after daemonization and PID saving.

This is achieved by splitting the former SavePidAndCheckKernel() into discrete steps: an initial SavePid(pid) call, followed by CModuleControl::AutoLoad() and CheckLkmLoad().

Technical Enhancements

Such separation clarifies the initialization process and bolsters kernel-module-based hiding.

Networking behaviors have also been simplified; the previous multi-stage beaconing with randomized delays and configurable intervals (e.g., days between beacons and delayTime) is replaced by a straightforward while (true) loop.

After a configured startup delay, it repeatedly invokes ConnectToSvr(), with brief sleeps on failures, until success or timeout, prioritizing reliable C2 connectivity over temporal obfuscation.

System information gathering sees a minor upgrade, adding a fallback to /etc/issue.net if /etc/issue is unavailable for OS detection, while parsing remains consistent.

File path configurations for persistence differ notably: root users now use /etc/udev/rules.d/90-persistent-net.rules and /etc/modprobe.d/usbdev.conf, with non-root paths set to $HOME/.kde4/share/config/kdeglobals and $HOME/.kde4/share/config/kde.conf.

This contrasts with the older variant’s /etc/udev/rules.d/70-persistent-net.rules and /etc/modprobe.d/usb-storage.conf for root, and $HOME/.bashrc for non-root.

Command handling has evolved, with the new variant dropping obsolete IDs like 0x111, 0x113, 0x114 (beacon interval adjustments) and 0x201 (file-read), reflecting the simplified networking.

According to the report, Process-hiding shifts to ID 0x202 from 0x112, and HideModule is removed, while a novel SetAutoKillEl (ID 0x160) introduces togglable auto-kill functionality.

Undocumented commands persist, including 0x109 for connection config changes, 0x192 for C2-fetched file execution via CFileControl::FileUp and system calls (differing from 0x185), and 0x195 for exfiltrating files with extensions .v2, .k2, .W2, and drive.C2.

Persistent typos, such as “Destroy” in method names and “Get Memory Faile” in errors, carry over from prior builds.

While the kernel module’s status remains unconfirmed due to collection challenges, these modifications suggest an emphasis on maintainability and adaptability in espionage scenarios.

Indicators of Compromise

Variant	SHA256 Hash	Submission Details
New FireWood Version	898a5bd86c5d99eb70088a90f1d8f90b03bd38c15a232200538d0601c888acb6	Analyzed by Intezer
Older Sample (Iran)	4c293309a7541edb89e3ec99c4074584328a21309e75a46d0ddb4373652ee0d6	Submitted February 5, 2025
Sample (Philippines)	d7be3494b3e1722eb85ee68bf7ea5508aa2d5782392619e078b78af	Submitted May 7, 2022; identical to new variant