Fire Chili (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:24:51 UTC

The purpose of this rootkit/driver is hiding and protecting malicious artifacts from user-mode components(e.g. files, processes, registry keys and network connections).
According to Fortguard Labs, this malware uses Direct Kernel Object Modification (DKOM), which involves undocumented kernel structures and objects, for its operations, why this malware has to rely on specific OS builds.

▶ [TLP:WHITE] win_firechili_auto (20251219 | Detects win.firechili.)
