GRILLMARK (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:14:05 UTC

This is a proxy-aware HTTP backdoor that is implemented as a service and uses the compromised system's proxy settings to access the internet. C&C traffic is base64 encoded and the files sent to the server are compressed with aPLib.

▶ [TLP:WHITE] win_grillmark_auto (20251219 | Detects win.grillmark.)
