Moriya (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:21:50 UTC

This tool is a passive backdoor which allows attackers to inspect all incoming traffic to the infected machine, filter out packets that are marked as designated for the malware and respond to them. This forms a covert channel over which attackers are able to issue shell commands and receive back their outputs.

▶ [TLP:WHITE] win_moriya_auto (20251219 | Detects win.moriya.)
