NESTEGG (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:38:55 UTC

NESTEGG is a memory-only backdoor that can proxy commands to other infected systems using a custom routing scheme. It accepts commands to upload and download files, list and delete files, list and terminate processes, and start processes. NESTEGG also creates Windows Firewall rules that allows the backdoor to bind to a specified port number to allow for inbound traffic.

▶ [TLP:WHITE] win_nestegg_auto (20251219 | Detects win.nestegg.)
