CHEESETRAY (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:16:32 UTC

CHEESETRAY is a sophisticated proxy-aware backdoor that can operate in both active and passive mode depending on the passed command-line parameters. The backdoor is capable of enumerating files and processes, enumerating drivers, enumerating remote desktop sessions, uploading and downloading files, creating and terminating processes, deleting files, creating a reverse shell, acting as a proxy server, and hijacking processes among its other functionality. The backdoor communicates with its C&C server using a custom binary protocol over TCP with port specified as a command-line parameter.

▶ [TLP:WHITE] win_cheesetray_auto (20251219 | Detects win.cheesetray.)
