Contopee (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:55:43 UTC

FireEye described this malware as a proxy-aware backdoor that communicates using a custom-encrypted binary protocol. It may use the registry to store optional configuration data. The backdoor has been observed to support 26 commands that include directory traversal, file system manipulation, data archival and transmission, and command execution.

▶ [TLP:WHITE] win_contopee_auto (20251219 | Detects win.contopee.)
