ELMER (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:10:03 UTC

ELMER is a non-persistent proxy-aware HTTP backdoor written in Delphi, and is capable of performing file uploads and downloads, file execution, and process and directory listings. To retrieve commands, ELMER sends HTTP GET requests to a hard-coded CnC server, and parses the HTTP response packets received from the CnC server for an integer string corresponding to the command that needs to be executed.

▶ [TLP:WHITE] win_elmer_auto (20201014 | autogenerated rule brought to you by yara-signator)
