homefry (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:35:05 UTC

a 64-bit Windows password dumper/cracker that has previously been used in conjunction with AIRBREAK and BADFLICK backdoors. Some strings are obfuscated with XOR x56. The malware accepts up to two arguments at the command line: one to display cleartext credentials for each login session, and a second to display cleartext credentials, NTLM hashes, and malware version for each login session.

▶ [TLP:WHITE] win_homefry_auto (20251219 | Detects win.homefry.)
