# Sagerunex (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:54:58 UTC

According to Symantec, Sagerunex is a backdoor that is fairly resilient and implements multiple forms of communication with its command-and-control (C&C) server. Its logs are encrypted and the encryption algorithm used is AES256-CBC with 8192 rounds of SHA256 for key derivation based on a hardcoded key. It supports multiple modes methods for communicating via HTTP (proxy-aware).

▶ [TLP:WHITE] win_sagerunex_auto (20251219 | Detects win.sagerunex.)

---