Koadic (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:24:30 UTC

Koadic is an open-source post-exploitation framework for Windows, created by zerosum0x0 and available on GitHub. The framework is written in Python and can generate JScript and VBScript payloads which can be written to disk or mapped directly into memory. Its capabilities include remote desktop access, command execution, lateral movement via SMB, file transfer, credential theft using Mimikatz, port scanning, and system information collection. It can also collect specific system information and targeted files based on their name or extension.

▶ [TLP:WHITE] win_koadic_auto (20251219 | Detects win.koadic.)
