Sakula, Software S0074 | MITRE ATT&CK®

Archived: 2026-04-05 18:30:52 UTC

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Sakula contains UAC bypass code for both 32- and 64-bit systems.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Sakula uses HTTP for C2.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Most Sakula samples maintain persistence by setting the Registry Run key `SOFTWARE\Microsoft\Windows\CurrentVersion\Run\` in the HKLM or HKCU hive, with the Registry value and file name varying by sample.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Sakula calls cmd.exe to run various DLL files via rundll32 and also to perform file cleanup. Sakula also has the capability to invoke a reverse shell.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Some Sakula samples install themselves as services for persistence by calling WinExec with the `net start` argument.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Sakula encodes C2 traffic with single-byte XOR keys.[1]

Domain	ID		Name	Use
Enterprise	T1574	.001	Hijack Execution Flow: DLL	Sakula uses DLL side-loading, typically using a digitally signed sample of Kaspersky Anti-Virus (AV) 6.0 for Windows Workstations or McAfee's Outlook Scan About Box to load malicious DLL files.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Some Sakula samples use cmd.exe to delete temporary files.[1]
Enterprise	T1105		Ingress Tool Transfer	Sakula has the capability to download files.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	Sakula uses single-byte XOR obfuscation to obfuscate many of its files.[1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	Sakula calls cmd.exe to run various DLL files via rundll32.[1]

Source: https://attack.mitre.org/software/S0074/