Kapeka, Software S1190 | MITRE ATT&CK®

Archived: 2026-04-05 18:21:15 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Kapeka utilizes HTTP for command and control.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Kapeka allows for arbitrary Windows command execution.[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	Kapeka utilizes JSON objects to send and receive information from command and control nodes.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Kapeka utilizes obfuscated JSON structures for various data storage and configuration management items.[1]
Enterprise	T1070	.009	Indicator Removal: Clear Persistence	Kapeka will clear registry values used for persistent configuration storage when uninstalled.[1]
Enterprise	T1036	.008	Masquerading: Masquerade File Type	Kapeka masquerades as a Microsoft Word Add-In file, with the extension `.wll`, but is a malicious DLL file.[2][1]
Enterprise	T1112		Modify Registry	Kapeka writes persistent configuration information to the victim host registry.[1]
Enterprise	T1106		Native API	Kapeka utilizes WinAPI calls to gather victim system information.[1]

Domain	ID		Name	Use
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	Kapeka utilizes AES-256 (CBC mode), XOR, and RSA-2048 encryption schemas for various configuration and other objects.[1]
Enterprise	T1090		Proxy	Kapeka can identify system proxy settings via `WinHttpGetIEProxyConfigForCurrentUser()` during initialization and utilize these settings for subsequent command and control operations.[1]
Enterprise	T1012		Query Registry	Kapeka queries registry values for stored configuration information.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Kapeka persists via scheduled tasks.[2][1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	Kapeka is a Windows DLL file executed via ordinal by `rundll32.exe`.[2][1]
Enterprise	T1082		System Information Discovery	Kapeka utilizes WinAPI calls and registry queries to gather system information.[1]
