CSPY Downloader, Software S0527 | MITRE ATT&CK®

Archived: 2026-04-05 16:11:04 UTC

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	CSPY Downloader can bypass UAC using the SilentCleanup task to execute the binary with elevated privileges.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	CSPY Downloader can use GET requests to download additional payloads from C2.[1]
Enterprise	T1070		Indicator Removal	CSPY Downloader has the ability to remove values it writes to the Registry.[1]
		.004	File Deletion	CSPY Downloader has the ability to self delete.[1]
Enterprise	T1105		Ingress Tool Transfer	CSPY Downloader can download additional tools to a compromised host.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	CSPY Downloader has attempted to appear as a legitimate Windows service with a fake description claiming it is used to support packed applications.[1]
Enterprise	T1112		Modify Registry	CSPY Downloader can write to the Registry under the `%windir%` variable to execute tasks.[1]

Domain	ID		Name	Use
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	CSPY Downloader has been packed with UPX.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	CSPY Downloader can use the schtasks utility to bypass UAC.[1]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	CSPY Downloader has come signed with revoked certificates.[1]
Enterprise	T1204	.002	User Execution: Malicious File	CSPY Downloader has been delivered via malicious documents with embedded macros.[1]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	CSPY Downloader can search loaded modules, PEB structure, file paths, Registry keys, and memory to determine if it is being debugged or running in a virtual environment.[1]

Source: https://attack.mitre.org/software/S0527/