Spica, Software S1140 | MITRE ATT&CK®

Archived: 2026-04-05 14:50:13 UTC

Domain	ID		Name	Use
Enterprise	T1560		Archive Collected Data	Spica can archive collected documents for exfiltration.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Spica can use an obfuscated PowerShell command to create a scheduled task for persistence.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Upon execution Spica can decode an embedded .pdf and write it to the desktop as a decoy document.[1]
Enterprise	T1083		File and Directory Discovery	Spica can list filesystem contents on targeted systems.[1]
Enterprise	T1105		Ingress Tool Transfer	Spica can upload and download files to and from compromised hosts.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	Spica has created a scheduled task named `CalendarChecker` for persistence on compromised hosts.[1]
Enterprise	T1095		Non-Application Layer Protocol	Spica can use JSON over WebSockets for C2 communications.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Spica has created a scheduled task named `CalendarChecker` to establish persistence.[1]

Domain	ID	Name	Use
Enterprise	T1539	Steal Web Session Cookie	Spica has the ability to steal cookies from Chrome, Firefox, Opera, and Edge browsers. [1]

Source: https://attack.mitre.org/software/S1140