SharpStage, Software S0546 | MITRE ATT&CK®

Archived: 2026-04-05 14:17:39 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	SharpStage has the ability to create persistence for the malware using the Registry autorun key and startup folder.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	SharpStage can execute arbitrary commands with PowerShell.[1][2]
		.003	Command and Scripting Interpreter: Windows Command Shell	SharpStage can execute arbitrary commands with the command line.[1][2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	SharpStage has decompressed data received from the C2 server.[2]
Enterprise	T1105		Ingress Tool Transfer	SharpStage has the ability to download and execute additional payloads via a DropBox API.[1][2]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	SharpStage has a persistence component to write a scheduled task for the payload.[1]
Enterprise	T1113		Screen Capture	SharpStage has the ability to capture the victim's screen.[1][2]
Enterprise	T1082		System Information Discovery	SharpStage has checked the system settings to see if Arabic is the configured language.[2]

Domain	ID		Name	Use
Enterprise	T1614	.001	System Location Discovery: System Language Discovery	SharpStage has been used to target Arabic-speaking users and used code that checks if the compromised machine has the Arabic language installed.[2]
Enterprise	T1102		Web Service	SharpStage has used a legitimate web service for evading detection.[1]
Enterprise	T1047		Windows Management Instrumentation	SharpStage can use WMI for execution.[1] [2]

Source: https://attack.mitre.org/software/S0546