MCMD, Software S0500 | MITRE ATT&CK®

Archived: 2026-04-05 14:18:37 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	MCMD can use HTTPS in communication with C2 web servers.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	MCMD can use Registry Run Keys for persistence.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	MCMD can launch a console process (cmd.exe) with redirected standard input and output.[1]
Enterprise	T1005		Data from Local System	MCMD has the ability to upload files from an infected device.[1]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	MCMD can modify processes to prevent them from being visible on the desktop.[1]
Enterprise	T1070	.009	Indicator Removal: Clear Persistence	MCMD has the ability to remove set Registry Keys, including those used for persistence.[1]
Enterprise	T1105		Ingress Tool Transfer	MCMD can upload additional files to a compromised host.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	MCMD has been named Readme.txt to appear legitimate.[1]

Domain	ID		Name	Use
Enterprise	T1027		Obfuscated Files or Information	MCMD can Base64 encode output strings prior to sending to C2.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	MCMD can use scheduled tasks for persistence.[1]

Source: https://attack.mitre.org/software/S0500