Nebulae, Software S0630 | MITRE ATT&CK®

Archived: 2026-04-05 15:38:59 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Nebulae can achieve persistence through a Registry Run key.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Nebulae can use CMD to execute a process.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Nebulae can create a service to establish persistence.[1]
Enterprise	T1005		Data from Local System	Nebulae has the capability to upload collected files to C2.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Nebulae can use RC4 and XOR to encrypt C2 communications.[1]
Enterprise	T1083		File and Directory Discovery	Nebulae can list files and directories on a compromised host.[1]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	Nebulae can use DLL side-loading to gain execution.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Nebulae has the ability to delete files and directories.[1]

Domain	ID		Name	Use
Enterprise	T1105		Ingress Tool Transfer	Nebulae can download files from C2.[1]
Enterprise	T1680		Local Storage Discovery	Nebulae can discover logical drive information including the drive type, free space, and volume information.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	Nebulae has created a service named "Windows Update Agent1" to appear legitimate.[1]
		.005	Masquerading: Match Legitimate Resource Name or Location	Nebulae uses functions named `StartUserModeBrowserInjection` and `StopUserModeBrowserInjection` indicating that it's trying to imitate chrome_frame_helper.dll.[1]
Enterprise	T1106		Native API	Nebulae has the ability to use `CreateProcess` to execute a process.[1]
Enterprise	T1095		Non-Application Layer Protocol	Nebulae can use TCP in C2 communications.[1]
Enterprise	T1057		Process Discovery	Nebulae can enumerate processes on a target system.[1]
