IPsec Helper, Software S1132 | MITRE ATT&CK®

Archived: 2026-04-02 11:17:11 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	IPsec Helper connects to command and control servers via HTTP POST requests based on parameters hard-coded into the malware.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	IPsec Helper can run arbitrary PowerShell commands passed to it.[1]
		.003	Command and Scripting Interpreter: Windows Command Shell	IPsec Helper can run arbitrary commands passed to it through `cmd.exe`.[1]
		.005	Command and Scripting Interpreter: Visual Basic	IPsec Helper can run arbitrary Visual Basic scripts and commands passed to it.[1]
Enterprise	T1005		Data from Local System	IPsec Helper can identify specific files and folders for follow-on exfiltration.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	IPsec Helper exfiltrates specific files through its command and control framework.[1]
Enterprise	T1070		Indicator Removal	IPsec Helper can delete various registry keys related to its execution and use.[1]
		.004	File Deletion	IPsec Helper can delete itself when given the appropriate command.[1]

Domain	ID		Name	Use
		.009	Clear Persistence	IPsec Helper can delete various service traces related to persistent execution when commanded.[1]
Enterprise	T1570		Lateral Tool Transfer	IPsec Helper can download additional payloads from command and control nodes and execute them.[1]
Enterprise	T1112		Modify Registry	IPsec Helper can make arbitrary changes to registry keys based on provided input.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	IPsec Helper contains an embedded XML configuration file with an encrypted list of command and control servers. These are written to an external configuration file during execution.[1]
Enterprise	T1057		Process Discovery	IPsec Helper can identify the process it is currently running under and its number, and pass this back to a command and control node.[1]
Enterprise	T1569	.002	System Services: Service Execution	IPsec Helper is run as a Windows service in victim environments.[1]
Enterprise	T1497	.003	Virtualization/Sandbox Evasion: Time Based Checks	IPsec Helper will sleep for a random number of seconds, iterating 200 times over sleeps between one to three seconds, before continuing execution flow.[1]