StrifeWater, Software S1034 | MITRE ATT&CK®

Archived: 2026-04-05 16:07:17 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	StrifeWater can execute shell commands using `cmd.exe` .[1]
Enterprise	T1005		Data from Local System	StrifeWater can collect data from a compromised host.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	StrifeWater can encrypt C2 traffic using XOR with a hard coded key.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	StrifeWater can send data and files from a compromised host to its C2 server.[1]
Enterprise	T1083		File and Directory Discovery	StrifeWater can enumerate files on a compromised host.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	StrifeWater can self delete to cover its tracks.[1]
Enterprise	T1105		Ingress Tool Transfer	StrifeWater can download updates and auxiliary modules.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	StrifeWater has been named `calc.exe` to appear as a legitimate calculator program. [1]

Domain	ID		Name	Use
Enterprise	T1106		Native API	StrifeWater can use a variety of APIs for execution.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	StrifeWater has create a scheduled task named `Mozilla\Firefox Default Browser Agent 409046Z0FF4A39CB` for persistence.[1]
Enterprise	T1113		Screen Capture	StrifeWater has the ability to take screen captures.[1]
Enterprise	T1082		System Information Discovery	StrifeWater can collect the OS version, architecture, and machine name to create a unique token for the infected host.[1]
Enterprise	T1033		System Owner/User Discovery	StrifeWater can collect the user name from the victim's machine.[1]
Enterprise	T1124		System Time Discovery	StrifeWater can collect the time zone from the victim's machine.[1]
Enterprise	T1497	.003	Virtualization/Sandbox Evasion: Time Based Checks	StrifeWater can modify its sleep time responses from the default of 20-22 seconds.[1]