MoonWind, Software S0149 | MITRE ATT&CK®

Archived: 2026-04-05 16:13:42 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	MoonWind can execute commands via an interactive command shell.[1] MoonWind uses batch scripts for various purposes, including to restart and uninstall itself.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	MoonWind installs itself as a new service with automatic startup to establish persistence. The service checks every 60 seconds to determine if the malware is running; if not, it will spawn a new instance.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	MoonWind saves information from its keylogging routine as a .zip file in the present working directory.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	MoonWind encrypts C2 traffic using RC4 with a static key.[1]
Enterprise	T1083		File and Directory Discovery	MoonWind has a command to return a directory listing for a specified directory.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	MoonWind can delete itself or specified files.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	MoonWind has a keylogger.[1]
Enterprise	T1095		Non-Application Layer Protocol	MoonWind completes network communication via raw sockets.[1]

Domain	ID	Name	Use
Enterprise	T1571	Non-Standard Port	MoonWind communicates over ports 80, 443, 53, and 8080 via raw sockets instead of the protocols usually associated with the ports.[1]
Enterprise	T1120	Peripheral Device Discovery	MoonWind obtains the number of removable drives from the victim.[1]
Enterprise	T1057	Process Discovery	MoonWind has a command to return a list of running processes.[1]
Enterprise	T1082	System Information Discovery	MoonWind can obtain the victim hostname, Windows version, RAM amount, and screen resolution.[1]
Enterprise	T1016	System Network Configuration Discovery	MoonWind obtains the victim IP address.[1]
Enterprise	T1033	System Owner/User Discovery	MoonWind obtains the victim username.[1]
Enterprise	T1124	System Time Discovery	MoonWind obtains the victim's current time.[1]