KEYMARBLE, Software S0271 | MITRE ATT&CK®

Archived: 2026-04-05 14:12:00 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	KEYMARBLE can execute shell commands using cmd.exe.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	KEYMARBLE uses a customized XOR algorithm to encrypt C2 communications.[1]
Enterprise	T1083		File and Directory Discovery	KEYMARBLE has a command to search for files on the victim's machine.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	KEYMARBLE has the capability to delete files off the victim's machine.[1]
Enterprise	T1105		Ingress Tool Transfer	KEYMARBLE can upload files to the victim's machine and can download additional payloads.[1]
Enterprise	T1680		Local Storage Discovery	KEYMARBLE has the capability to collect information on disk devices.[1]
Enterprise	T1112		Modify Registry	KEYMARBLE has a command to create Registry entries for storing data under `HKEY_CURRENT_USER\SOFTWARE\Microsoft\WABE\DataPath`. [1]

Domain	ID	Name	Use
Enterprise	T1057	Process Discovery	KEYMARBLE can obtain a list of running processes on the system.[1]
Enterprise	T1113	Screen Capture	KEYMARBLE can capture screenshots of the victim's machine.[1]
Enterprise	T1082	System Information Discovery	KEYMARBLE has the capability to collect the computer name, language settings, the OS version, CPU information, and time elapsed since system start.[1]
Enterprise	T1016	System Network Configuration Discovery	KEYMARBLE gathers the MAC address of the victim's machine.[1]
