ROADSWEEP, Software S1150 | MITRE ATT&CK®

Archived: 2026-04-05 16:52:10 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	ROADSWEEP has been placed in the start up folder to trigger execution upon user login.[2]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	ROADSWEEP can open cmd.exe to enable command execution.[1][2]
Enterprise	T1486		Data Encrypted for Impact	ROADSWEEP can RC4 encrypt content in blocks on targeted systems.[1][3][2]
Enterprise	T1491	.001	Defacement: Internal Defacement	ROADSWEEP has dropped ransom notes in targeted folders prior to encrypting the files.[2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	ROADSWEEP can decrypt embedded scripts prior to execution.[1][3]
Enterprise	T1480		Execution Guardrails	ROADSWEEP requires four command line arguments to execute correctly, otherwise it will produce a message box and halt execution.[1][3][2]
Enterprise	T1083		File and Directory Discovery	ROADSWEEP can enumerate files on infected devices and avoid encrypting files with .exe, .dll, .sys, .lnk, or . lck extensions. [1][3][2]

Domain	ID		Name	Use
Enterprise	T1070	.004	Indicator Removal: File Deletion	ROADSWEEP can use embedded scripts to remove itself from the infected host.[1][2]
Enterprise	T1490		Inhibit System Recovery	ROADSWEEP has the ability to disable `SystemRestore` and Volume Shadow Copies.[1][3]
Enterprise	T1559		Inter-Process Communication	ROADSWEEP can pipe command output to a targeted process.[1]
Enterprise	T1680		Local Storage Discovery	ROADSWEEP can enumerate logical drives on targeted devices.[1][2]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	The ROADSWEEP binary contains RC4 encrypted embedded scripts.[1][3][2]
Enterprise	T1120		Peripheral Device Discovery	ROADSWEEP can identify removable drives attached to the victim's machine.[1]
Enterprise	T1489		Service Stop	ROADSWEEP can disable critical services and processes.[1]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	ROADSWEEP has been digitally signed with a certificate issued to the Kuwait Telecommunications Company KSC.[3]

Source: https://attack.mitre.org/software/S1150