Remcos, Software S0332 | MITRE ATT&CK®

Archived: 2026-04-05 15:37:51 UTC

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Remcos has a command for UAC bypassing.[3]
Enterprise	T1123		Audio Capture	Remcos can capture data from the system's microphone.[3]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Remcos can add itself to the Registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` for persistence.[3]
Enterprise	T1115		Clipboard Data	Remcos steals and modifies data from the clipboard.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Remcos can launch a remote command line to execute commands on the victim's machine.[3]
		.006	Command and Scripting Interpreter: Python	Remcos uses Python scripts.[1]
Enterprise	T1083		File and Directory Discovery	Remcos can search for files on the infected machine.[1]
Enterprise	T1105		Ingress Tool Transfer	Remcos can upload and download files to and from the victim's machine.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	Remcos has a command for keylogging.[3][2]

Domain	ID		Name	Use
Enterprise	T1112		Modify Registry	Remcos has full control of the Registry, including the ability to modify it.[1]
Enterprise	T1027		Obfuscated Files or Information	Remcos uses RC4 and base64 to obfuscate data, including Registry entries and file paths.[2]
Enterprise	T1055		Process Injection	Remcos has a command to hide itself through injecting into another process.[3]
Enterprise	T1090		Proxy	Remcos uses the infected hosts as SOCKS5 proxies to allow for tunneling and proxying.[1]
Enterprise	T1113		Screen Capture	Remcos takes automated screenshots of the infected machine.[1]
Enterprise	T1125		Video Capture	Remcos can access a system's webcam and take pictures.[3]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	Remcos searches for Sandboxie and VMware on the system.[2]

Source: https://attack.mitre.org/software/S0332/