RunningRAT, Software S0253 | MITRE ATT&CK®

Archived: 2026-04-05 13:20:01 UTC

Domain	ID		Name	Use
Enterprise	T1560		Archive Collected Data	RunningRAT contains code to compress files.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	RunningRAT adds itself to the Registry key `Software\Microsoft\Windows\CurrentVersion\Run` to establish persistence upon reboot.[1]
Enterprise	T1115		Clipboard Data	RunningRAT contains code to open and copy data from the clipboard.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	RunningRAT uses a batch file to kill a security program task and then attempts to remove itself.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	RunningRAT kills antimalware running process.[1]
Enterprise	T1070	.001	Indicator Removal: Clear Windows Event Logs	RunningRAT contains code to clear event logs.[1]
		.004	Indicator Removal: File Deletion	RunningRAT contains code to delete files from the victim’s machine.[1]

Domain	ID		Name	Use
Enterprise	T1056	.001	Input Capture: Keylogging	RunningRAT captures keystrokes and sends them back to the C2 server.[1]
Enterprise	T1680		Local Storage Discovery	RunningRAT gathers logical drives information and volume information.[1]
Enterprise	T1082		System Information Discovery	RunningRAT gathers the OS version and processor information.[1]

Source: https://attack.mitre.org/software/S0253/