NavRAT, Software S0247 | MITRE ATT&CK®

Archived: 2026-04-05 13:10:10 UTC

Domain	ID		Name	Use
Enterprise	T1071	.003	Application Layer Protocol: Mail Protocols	NavRAT uses the email platform, Naver, for C2 communications, leveraging SMTP.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	NavRAT creates a Registry key to ensure a file gets executed upon reboot in order to establish persistence.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	NavRAT leverages cmd.exe to perform discovery techniques.[1] NavRAT loads malicious shellcode and executes it in memory.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	NavRAT writes multiple outputs to a TMP file using the >> method.[1]
Enterprise	T1105		Ingress Tool Transfer	NavRAT can download files remotely.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	NavRAT logs the keystrokes on the targeted system.[1]
Enterprise	T1057		Process Discovery	NavRAT uses `tasklist /v` to check running processes.[1]
Enterprise	T1055		Process Injection	NavRAT copies itself into a running Internet Explorer process to evade detection.[1]

Domain	ID	Name	Use
Enterprise	T1082	System Information Discovery	NavRAT uses `systeminfo` on a victim's machine.[1]

Source: https://attack.mitre.org/software/S0247/