NanoCore, Software S0336 | MITRE ATT&CK®

Archived: 2026-04-05 13:13:32 UTC

Domain	ID		Name	Use
Enterprise	T1123		Audio Capture	NanoCore can capture audio feeds from the system.[1][3]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	NanoCore creates a RunOnce key in the Registry to execute its VBS scripts each time the user logs on to the machine.[2]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	NanoCore can open a remote command-line interface and execute commands.[3] NanoCore uses JavaScript files.[2]
		.005	Command and Scripting Interpreter: Visual Basic	NanoCore uses VBS files.[2]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	NanoCore uses DES to encrypt the C2 traffic.[3]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	NanoCore can modify the victim's anti-virus.[1][3]
		.004	Impair Defenses: Disable or Modify System Firewall	NanoCore can modify the victim's firewall.[1][3]
Enterprise	T1105		Ingress Tool Transfer	NanoCore has the capability to download and activate additional modules for execution.[1][3]

Domain	ID		Name	Use
Enterprise	T1056	.001	Input Capture: Keylogging	NanoCore can perform keylogging on the victim's machine.[3]
Enterprise	T1112		Modify Registry	NanoCore has the capability to edit the Registry.[1][3]
Enterprise	T1027		Obfuscated Files or Information	NanoCore's plugins were obfuscated with Eazfuscater.NET 3.3.[3]
Enterprise	T1016		System Network Configuration Discovery	NanoCore gathers the IP address from the victim's machine.[1]
Enterprise	T1125		Video Capture	NanoCore can access the victim's webcam and capture data.[1][3]
