EVILNUM, Software S0568 | MITRE ATT&CK®

Archived: 2026-04-05 15:07:57 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	EVILNUM can achieve persistence through the Registry Run key.[1][2]
Enterprise	T1041		Exfiltration Over C2 Channel	EVILNUM can upload files over the C2 channel from the infected host.[2]
Enterprise	T1070		Indicator Removal	EVILNUM has a function called "DeleteLeftovers" to remove certain artifacts of the attack.[2]
		.006	Timestomp	EVILNUM has changed the creation date of files.[2]
Enterprise	T1105		Ingress Tool Transfer	EVILNUM can download and upload files to the victim's computer.[1][2]
Enterprise	T1112		Modify Registry	EVILNUM can make modifications to the Regsitry for persistence.[2]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	EVILNUM can search for anti-virus products on the system.[2]
Enterprise	T1539		Steal Web Session Cookie	EVILNUM can harvest cookies and upload them to the C2 server.[2]
Enterprise	T1218	.010	System Binary Proxy Execution: Regsvr32	EVILNUM can run a remote scriptlet that drops a file and executes it via

Domain	ID		Name	Use
				regsvr32.exe.[1]
		.011	System Binary Proxy Execution: Rundll32	EVILNUM can execute commands and scripts through rundll32.[2]
Enterprise	T1082		System Information Discovery	EVILNUM can obtain the computer name from the victim's system.[2]
Enterprise	T1033		System Owner/User Discovery	EVILNUM can obtain the username from the victim's machine.[2]
Enterprise	T1102	.003	Web Service: One-Way Communication	EVILNUM has used a one-way communication method via GitLab and Digital Point to perform C2.[2]
Enterprise	T1047		Windows Management Instrumentation	EVILNUM has used the Windows Management Instrumentation (WMI) tool to enumerate infected machines.[2]
