Rancor, Group G0075 | MITRE ATT&CK®

Archived: 2026-04-05 17:16:16 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Rancor has used HTTP for C2.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Rancor has used cmd.exe to execute commmands.[1]
		.005	Command and Scripting Interpreter: Visual Basic	Rancor has used VBS scripts as well as embedded macros for execution.[1]
Enterprise	T1546	.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	Rancor has complied VBScript-generated MOF files into WMI event subscriptions for persistence.[2]
Enterprise	T1105		Ingress Tool Transfer	Rancor has downloaded additional malware, including by using certutil.[1]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Rancor has attached a malicious document to an email to gain initial access.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Rancor launched a scheduled task to gain persistence using the `schtasks /create /sc` command.[1]
Enterprise	T1218	.007	System Binary Proxy Execution: Msiexec	Rancor has used `msiexec` to download and execute malicious installer files over HTTP.[1]

Domain	ID		Name	Use
Enterprise	T1204	.002	User Execution: Malicious File	Rancor attempted to get users to click on an embedded macro within a Microsoft Office Excel document to launch their malware.[1]

Source: https://attack.mitre.org/groups/G0075/