

## Rancor, Group G0075 | MITRE ATT&CK®

Archived: 2026-04-05 16:23:35 UTC

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

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

---

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