MoustachedBouncer, Group G1019 | MITRE ATT&CK®

Archived: 2026-04-05 16:02:06 UTC

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	MoustachedBouncer has used plugins to execute PowerShell scripts.[1]
		.007	Command and Scripting Interpreter: JavaScript	MoustachedBouncer has used JavaScript to deliver malware hosted on HTML pages.[1]
Enterprise	T1659		Content Injection	MoustachedBouncer has injected content into DNS, HTTP, and SMB replies to redirect specifically-targeted victims to a fake Windows Update page to download malware.[1]
Enterprise	T1074	.002	Data Staged: Remote Data Staging	MoustachedBouncer has used plugins to save captured screenshots to `.\AActdata\` on an SMB share.[1]
Enterprise	T1068		Exploitation for Privilege Escalation	MoustachedBouncer has exploited CVE-2021-1732 to execute malware components with elevated rights.[1]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	MoustachedBouncer has used malware plugins packed with Themida.[1]
Enterprise	T1090		Proxy	MoustachedBouncer has used a reverse proxy tool similar to the GitHub repository revsocks.[1]
Enterprise	T1113		Screen Capture	MoustachedBouncer has used plugins to take screenshots on targeted systems.[1]

Domain	ID		Name	Use
Mobile	T1655	.001	Masquerading: Match Legitimate Name or Location	MoustachedBouncer has used legitimate looking filenames for malicious executables including MicrosoftUpdate845255.exe.[1]

Source: https://attack.mitre.org/groups/G1019