Molerats, Operation Molerats, Gaza Cybergang, Group G0021

Archived: 2026-04-02 11:30:32 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Molerats saved malicious files within the AppData and Startup folders to maintain persistence.[3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Molerats used PowerShell implants on target machines.[3]
		.005	Command and Scripting Interpreter: Visual Basic	Molerats used various implants, including those built with VBScript, on target machines. [3][6]
		.007	Command and Scripting Interpreter: JavaScript	Molerats used various implants, including those built with JS, on target machines.[3]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	Molerats used the public tool BrowserPasswordDump10 to dump passwords saved in browsers on victims.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Molerats decompresses ZIP files once on the victim machine.[3]
Enterprise	T1105		Ingress Tool Transfer	Molerats used executables to download malicious files from different sources.[3][6]
Enterprise	T1027	.015	Obfuscated Files or Information: Compression	Molerats has delivered compressed executables within ZIP files to victims.[3]

Domain	ID		Name	Use
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Molerats has sent phishing emails with malicious Microsoft Word and PDF attachments.[3][6][4]
		.002	Phishing: Spearphishing Link	Molerats has sent phishing emails with malicious links included.[3]
Enterprise	T1057		Process Discovery	Molerats actors obtained a list of active processes on the victim and sent them to C2 servers.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Molerats has created scheduled tasks to persistently run VBScripts.[6]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	Molerats has used forged Microsoft code-signing certificates on malware.[5]
Enterprise	T1218	.007	System Binary Proxy Execution: Msiexec	Molerats has used msiexec.exe to execute an MSI payload.[6]
Enterprise	T1204	.001	User Execution: Malicious Link	Molerats has sent malicious links via email trick users into opening a RAR archive and running an executable.[3][6]
		.002	User Execution: Malicious File	Molerats has sent malicious files via email that tricked users into clicking Enable Content to run an embedded macro and to download malicious archives.[3][6][4]