DarkHydrus, Group G0079 | MITRE ATT&CK®

Archived: 2026-04-05 12:47:54 UTC

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	DarkHydrus leveraged PowerShell to download and execute additional scripts for execution.[1][2]
Enterprise	T1187		Forced Authentication	DarkHydrus used Template Injection to launch an authentication window for users to enter their credentials.[3]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	DarkHydrus has used `-WindowStyle Hidden` to conceal PowerShell windows. [1]
Enterprise	T1588	.002	Obtain Capabilities: Tool	DarkHydrus has obtained and used tools such as Mimikatz, Empire, and Cobalt Strike.[1]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	DarkHydrus has sent spearphishing emails with password-protected RAR archives containing malicious Excel Web Query files (.iqy). The group has also sent spearphishing emails that contained malicious Microsoft Office documents that use the "attachedTemplate" technique to load a template from a remote server.[1][3][2]
Enterprise	T1221		Template Injection	DarkHydrus used an open-source tool, Phishery, to inject malicious remote template URLs into Microsoft Word documents and then sent them to victims to enable Forced Authentication.[3]
Enterprise	T1204	.002	User Execution: Malicious File	DarkHydrus has sent malware that required users to hit the enable button in Microsoft Excel to allow an .iqy

Domain	ID		Name	Use
				file to be downloaded.[1][2]

Source: https://attack.mitre.org/groups/G0079/