

## DarkHydrus, Group G0079 | MITRE ATT&CK®

Archived: 2026-04-05 16:16:57 UTC

Domain	ID	Name	Use
Enterprise	<a href="#">T1059</a> <a href="#">.001</a>	<a href="#">Command and Scripting Interpreter: PowerShell</a>	<a href="#">DarkHydrus</a> leveraged PowerShell to download and execute additional scripts for execution. <sup>[1][2]</sup>
Enterprise	<a href="#">T1187</a>	<a href="#">Forced Authentication</a>	<a href="#">DarkHydrus</a> used <a href="#">Template Injection</a> to launch an authentication window for users to enter their credentials. <sup>[3]</sup>
Enterprise	<a href="#">T1564</a> <a href="#">.003</a>	<a href="#">Hide Artifacts: Hidden Window</a>	<a href="#">DarkHydrus</a> has used <code>-WindowState Hidden</code> to conceal <a href="#">PowerShell</a> windows. <sup>[1]</sup>
Enterprise	<a href="#">T1588</a> <a href="#">.002</a>	<a href="#">Obtain Capabilities: Tool</a>	<a href="#">DarkHydrus</a> has obtained and used tools such as <a href="#">Mimikatz</a> , <a href="#">Empire</a> , and <a href="#">Cobalt Strike</a> . <sup>[1]</sup>
Enterprise	<a href="#">T1566</a> <a href="#">.001</a>	<a href="#">Phishing: Spearphishing Attachment</a>	<a href="#">DarkHydrus</a> 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. <sup>[1][3][2]</sup>
Enterprise	<a href="#">T1221</a>	<a href="#">Template Injection</a>	<a href="#">DarkHydrus</a> used an open-source tool, Phishery, to inject malicious remote template URLs into Microsoft Word documents and then sent them to victims to enable <a href="#">Forced Authentication</a> . <sup>[3]</sup>
Enterprise	<a href="#">T1204</a> <a href="#">.002</a>	<a href="#">User Execution: Malicious File</a>	<a href="#">DarkHydrus</a> 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. <a href="#">[1]</a> <a href="#">[2]</a>

---

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