Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:22:01 UTC

APT group: DarkHydrus, LazyMeerkat

Names	DarkHydrus *(Palo Alto)* LazyMeerkat *(Kaspersky)* ATK 77 *(Thales)* Obscure Serpens *(Palo Alto)* G0079 *(MITRE)*	
Country	Iran	
Sponsor	State-sponsored	
Motivation	Information theft and espionage	
First seen	2016	
Description	DarkHydrus is a threat group that has targeted government agencies and educational institutions in the Middle East since at least 2016. The group heavily leverages open-source tools and custom payloads for carrying out attacks. Some analysts track Dark Hydrus, APT 19, Deep Panda, C0d0so0 and Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens as the same group, but it is unclear from open source information if the groups are the same.	
Observed	Sectors: Education, Government. Countries: Iran and Middle East.	
Tools used	Cobalt Strike, Mimikatz, Phishery, RogueRobin.	
Operations performed	Jun 2018	On June 24, 2018, Unit 42 observed DarkHydrus carrying out a credential harvesting attack on an educational institution in the Middle East. The attack involved a spear-phishing email with a subject of “Project Offer” and a malicious Word document as an attachment. <https://unit42.paloaltonetworks.com/unit42-darkhydrus-uses-phishery-harvest-credentials-middle-east/>
	Jul 2018	Attack on Middle East Government This attack diverged from previous attacks we observed from this group

		as it involved spear-phishing emails sent to targeted organizations with password protected RAR archive attachments that contained malicious Excel Web Query files (.iqy). <https://unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/>
	Jan 2019	New Attacks in the Middle East 360 Threat Intelligence Center captured several lure Excel documents written in Arabic in January 9, 2019. A backdoor dropped by macro in the lure documents can communicate with C2 server through DNS tunnel, as well as Google Drive API. <https://ti.360.net/blog/articles/latest-target-attack-of-darkhydruns-group-against-middle-east-en/> <https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/>
Information	<https://unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0079/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=obscureserpens>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
