Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:25:09 UTC

APT group: Hexane

Names	Hexane *(Dragos)* Lyceum *(SecureWorks)* Cobalt Lyceum *(SecureWorks)* Siamesekitten *(ClearSky)* ATK 120 *(Thales)* Yellow Dev 9 *(PWC)* G1001 *(MITRE)*	
Country	Iran	
Motivation	Information theft and espionage	
First seen	2017	
Description	(Dragos) Dragos identified a new activity group targeting industrial control systems (ICS) related entities: Hexane. Dragos observed this group targeting oil and gas companies in the Middle East, including Kuwait as a primary operating region. Additionally, and unlike other activity groups Dragos tracks, Hexane also targeted telecommunication providers in the greater Middle East, Central Asia, and Africa, potentially as a stepping stone to network-focused man-in-the-middle and related attacks. The threat actor shows similarities with other groups such as APT 33, Elfin, Magnallium and OilRig, APT 34, Helix Kitten, Chrysene, both active since at least 2017 and involved in attacks on oil and gas companies. Anyway, experts pointed out that the Hexane group has differed TTPs and has its own arsenal.	
Observed	Sectors: Energy, Oil and gas, Telecommunications. Countries: Israel, Kuwait, Morocco, Saudi Arabia, Tunisia, UAE and Middle East, Central Asia and Africa.	
Tools used	DanBot, DanDrop, Decrypt-RDCMan.ps1, Get-LAPSP.ps1, Marlin, Milan, kl.ps1, Shark.	
Operations performed	May 2021	New Iranian Espionage Campaign By “Siamesekitten” – Lyceum <https://www.clearskysec.com/siamesekitten/>

	2021	In 2021, we have been able to identify a new cluster of the group's activity, focused on two entities in Tunisia <https://securelist.com/lyceum-group-reborn/104586/>
	Jul 2021	Who are latest targets of cyber group Lyceum? <https://www.accenture.com/us-en/blogs/cyber-defense/iran-based-lyceum-campaigns>
	Sep 2021	Operation "Out to Sea" OilRig was particularly active in September – December 2021, iterating on a campaign we are calling Out to Sea. OilRig operators have been developing and deploying iterative improvements to the DanBot backdoor, with Shark, Milan, and Marlin, an ESET exclusive. <https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf>
	Mar 2022	Mid March, an Israeli energy company received an email with the subject "Russian war crimes in Ukraine". <https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/>
	Jun 2022	Lyceum .NET DNS Backdoor <https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor>
	Jun 2022	ClearSky discovered a new malware associated with the Iranian SiameseKitten (Lyceum) group with medium-high confidence. <https://www.clearskysec.com/wp-content/uploads/2022/06/Lyceum-suicide-drone-23.6.pdf>
Information	<https://dragos.com/resource/hexane/> <https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G1001/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
