Subgroup: [Unnamed group USA] - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:41:23 UTC

APT group: Subgroup: [Unnamed group USA]

Names	[Unnamed group USA] *(?)*
Country	USA
Sponsor	State-sponsored, CIA
Motivation	Information theft and espionage
First seen	2019
Description	A subgroup of the CIA. (ClearSky) Over the last few weeks, several significant leaks regarding a number of Iranian APTs took place. After analyzing and investigating the documents we conclude that they are authentic. Consequently, this causes considerable harm to the groups and their operation. The identity of the actor behind the leak is currently unknown, however based on the scope and the quality of the exposed documents and information, it appears that they are professional and highly capable. This leak will likely hamstring the groups' operation in the near future. Accordingly, in our assessment this will minimize the risk of potential attacks in the next few months and possibly even year. Note –most of the leaks are posted on Telegram channels that were created specifically for this purpose. Below are the three main Telegram groups on which the leaks were posted: • Lab Dookhtegam pseudonym ("The people whose lips are stitched and sealed" –translation from Persian) –In this channel attack tools attributed to the group 'OilRig, APT 34, Helix Kitten, Chrysene' were leaked; including a webshell that was inserted into the Technion, various tools that were used for DNS attacks, and more. • Green Leakers–In this channel attack tools attributed to the group 'MuddyWater, Seedworm, TEMP.Zagros, Static Kitten' were leaked. The group's name and its symbol are identified with the "green movement", which led the protests in Iran after the Presidential elections in 2009. These protests were heavily repressed by the revolutionary guards (IRGC) • Black Box–Unlike the previous two channels this has been around for a long time.

	On Friday May 5th, dozens of confidential documents labeled as “secret” (a high confidentiality level in Iran, one before the highest –top secret) were posted on this channel. The documents were related to Iranian attack groups’ activity. See [Unnamed groups: Iran].	
Observed	Countries: China, Iran, North Korea, Russia.	
Tools used		
Operations performed	Jul 2019	Hackers breach FSB contractor, expose Tor deanonymization project and more <https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tor-deanonymization-project/>
	Mar 2020	Hackers breach FSB contractor and leak details about IoT hacking project <https://www.zdnet.com/article/hackers-breach-fsb-contractor-and-leak-details-about-iot-hacking-project/>
Information	<https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf> <https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html> <https://www.zdnet.com/article/report-cia-most-likely-behind-apt34-and-fsb-hacks-and-data-dumps/>	

Last change to this card: 11 March 2024

Download this actor card in PDF or JSON format
