[Unnamed groups: Iran] - Threat Group Cards: A Threat Actor Encyclopedia

APT group: [Unnamed groups: Iran]

Names	[Unnamed groups: Iran] *(?)*	
Country	Iran	
Sponsor	State-sponsored	
Motivation	Information theft and espionage	
First seen	2019	
Description	These are reported APT activities attributed to a country, but not to an individual threat group.	
Observed	Sectors: Aviation, Government, Industrial, IT, Telecommunications. Countries: Afghanistan, Australia, Azerbaijan, Bahrain, Colombia, Dubai, Egypt, Ethiopia, Fiji, Hong Kong, India, Indonesia, Iraq, Israel, Kenya, Kuwait, Kyrgyzstan, Lebanon, Malaysia, Mauritius, Morocco, New Zealand, Oman, Pakistan, Philippines, Qatar, South Africa, Sri Lanka, Syria, Thailand, Turkey, UAE, USA.	
Tools used		
Operations performed	2017	I Spy With My Little Eye: Uncovering an Iranian Counterintelligence Operation <https://cloud.google.com/blog/topics/threat-intelligence/uncovering-iranian-counterintelligence-operation>
	Nov 2023	Pennsylvania water authority hit with cyberattack allegedly tied to pro-Iran group <https://therecord.media/water-authority-pennsylvania-cyberattack-pro-iran-group>
	Nov 2023	North Texas water utility serving 2 million hit with cyberattack <https://therecord.media/north-texas-water-utility-cyberattack>

	Dec 2023	Florida water agency latest to confirm cyber incident as feds warn of nation-state attacks <https://therecord.media/florida-water-agency-ransomware-cisa-warning-utilities>
Counter operations	May 2019	On Friday May 5th, dozens of confidential documents labeled as “secret” were leaked on Telegram. <https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf>
	Feb 2024	Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure <https://home.treasury.gov/news/press-releases/jy2072>
	Apr 2024	Treasury Designates Iranian Cyber Actors Targeting U.S. Companies and Government Agencies <https://home.treasury.gov/news/press-releases/jy2292>
	Aug 2024	Disrupting a covert Iranian influence operation <https://openai.com/index/disrupting-a-covert-iranian-influence-operation/>
	Sep 2024	Three IRGC Cyber Actors Indicted for ‘Hack-and-Leak’ Operation Designed to Influence the 2024 U.S. Presidential Election <https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us>
	Jan 2025	Treasury Sanctions Entities in Iran and Russia That Attempted to Interfere in the U.S. 2024 Election <https://home.treasury.gov/news/press-releases/jy2766>
Information	<https://us-cert.cisa.gov/ncas/alerts/aa20-259a> <https://us-cert.cisa.gov/ncas/alerts/aa20-296a> <https://us-cert.cisa.gov/ncas/alerts/aa20-296b> <https://us-cert.cisa.gov/ncas/alerts/aa20-304a> <https://us-cert.cisa.gov/ncas/alerts/aa21-321a> <https://www.cisa.gov/ncas/alerts/aa22-264a> <https://www.cisa.gov/uscert/ncas/alerts/aa22-320a> <https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-320a> <https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf> <https://www.waterisac.org/portal/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal> <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf> <https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3981-	

	joint-odni-fbi-and-cisa-statement-on-iranian-election-influence-efforts> <https://www.cisa.gov/resources-tools/resources/how-protect-against-iranian-targeting-accounts-associated-national-political-organizations> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a> <https://www.ic3.gov/CSA/2024/241030.pdf> <https://research.checkpoint.com/2024/wezrat-malware-deep-dive/> <https://www.cisa.gov/sites/default/files/2025-06/joint-fact-sheet-Iranian-cyber-actors-may-target-vulnerable-US-networks-and-entities-of-interest-508c-1.pdf> <https://www.nozominetworks.com/blog/threat-actor-activity-related-to-the-iran-conflict>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
