Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:06:28 UTC

APT group: APT 42

Names	APT 42 *(Mandiant)* GreenBravo *(Recorded Future)*
Country	Iran
Sponsor	State-sponsored, Islamic Revolutionary Guard Corps (IRGC)’s Intelligence Organization (IRGC-IO)
Motivation	Information theft and espionage
First seen	2015
Description	(Mandiant) Mandiant assesses with high confidence that APT42 is an Iranian state-sponsored cyber espionage group tasked with conducting information collection and surveillance operations against individuals and organizations of strategic interest to the Iranian government. We further estimate with moderate confidence that APT42 operates on behalf of the Islamic Revolutionary Guard Corps (IRGC) Intelligence Organization (IRGC-IO) based on targeting patterns that align with the organization's operational mandates and priorities. Active since at least 2015, APT42 is characterized by highly targeted spear phishing and surveillance operations against individuals and organizations of strategic interest to Iran. The group’s operations, which are designed to build trust and rapport with their victims, have included accessing the personal and corporate email accounts of government officials, former Iranian policymakers or political figures, members of the Iranian diaspora and opposition groups, journalists, and academics who are involved in research on Iran. After gaining access, the group has deployed mobile malware capable of tracking victim locations, recording phone conversations, accessing videos and images, and extracting entire SMS inboxes.

	APT42 has a demonstrated ability to alter its operational focus as Iran's priorities evolve over time. We anticipate APT42 will continue to conduct cyber espionage operations in support of Iran's strategic priorities in the long term based on their extensive operational history and imperviousness to public reporting and infrastructure takedowns. The full published report covers APT42's recent and historical activity dating back to at least 2015, the group's tactics, techniques, and procedures, targeting patterns, and elucidates historical connections to Magic Hound, APT 35, Cobalt Illusion, Charming Kitten. APT42 partially coincides with public reporting on ITG18.	
Observed	Sectors: Education, Government, Healthcare, Manufacturing, Media, Non-profit organizations, Pharmaceutical and Legal and professional services. Countries: Australia, Bulgaria, Iran, Italy, Malaysia, Norway, UAE, UK, Ukraine, USA.	
Tools used	BROKEYOLK, CHAIRSMACK, DOSTEALER, Ghambar, GORBLE, MAGICDROP, PINEFLOWER, POWERPOST, SILENTUPLOADER, TABBYCAT, TAMECAT, VBREVSHELL, VINETHORN.	
Operations performed	Sep 2022	Iran: State-Backed Hacking of Activists, Journalists, Politicians <https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians>
	Feb 2024	Iranian backed group steps up phishing campaigns against Israel, U.S. <https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/>
Information	<https://www.mandiant.com/media/17826> <https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations>	

Last change to this card: 23 October 2024

Download this actor card in PDF or JSON format
