Cutting Kitten, TG-2889 - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Cutting Kitten, TG-2889

Names	Cutting Kitten *(CrowdStrike)* TG-2889 *(SecureWorks)* G0003 *(MITRE)*	
Country	Iran	
Sponsor	State-sponsored, security company ITSecTeam	
Motivation	Information theft and espionage	
First seen	2012	
Description	Cleaver is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver. Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). This group evolved into Magic Hound, APT 35, Cobalt Illusion, Charming Kitten.	
Observed	Sectors: Aerospace, Aviation, Chemical, Defense, Education, Energy, Financial, Government, Healthcare, Oil and gas, Technology, Telecommunications, Transportation, Utilities and (banks: Bank of America, US Bancorp, Fifth Third Bank, Citigroup, PNC, BB&T, Wells Fargo, Capital One and HSBC). Countries: Canada, China, France, Germany, India, Israel, Kuwait, Mexico, Netherlands, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, UAE, UK, USA.	
Tools used	CsExt, DistTrack, Jasus, KAgent, Leash, Logger Module, MPKBot, Net Crawler, PupyRAT, PVZ-In, PVZ-Out, SynFlooder, SysKit, TinyZBot, WndTest, zhCat, zhMimikatz.	
Operations performed	2012	Operation “Cleaver” Operation Cleaver has, over the past several years, conducted a significant global surveillance and infiltration campaign. To date it has successfully evaded detection by existing security technologies. The group is believed to work from Tehran, Iran, although auxiliary team

		members were identified in other locations including the Netherlands, Canada, and the UK. The group successfully leveraged both publicly available, and customized tools to attack and compromise targets around the globe. The targets include military, oil and gas, energy and utilities, transportation, airlines, airports, hospitals, telecommunications, technology, education, aerospace, Defense Industrial Base (DIB), chemical companies, and governments. <https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf>
	2013	Attack on the Bowman Avenue Dam Iranian hackers infiltrated the control system of a small dam less than 20 miles from New York City two years ago, sparking concerns that reached to the White House, according to former and current U.S. officials and experts familiar with the previously undisclosed incident. <https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559>
	2015	Network of Fake LinkedIn Profiles While tracking a suspected Iran-based threat group known as Threat Group-2889 (TG-2889), Dell SecureWorks Counter Threat Unit (CTU) researchers uncovered a network of fake LinkedIn profiles. These convincing profiles form a self-referenced network of seemingly established LinkedIn users. CTU researchers assess with high confidence the purpose of this network is to target potential victims through social engineering. <https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles>
Counter operations	Mar 2016	U.S. indicts Iranians for hacking dozens of banks, New York dam <https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0003/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
