Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:07:50 UTC

APT group: ITG18

Names	ITG18 *(IBM)*	
Country	Iran	
Motivation	Information theft and espionage	
First seen	2013	
Description	(IBM) IBM X-Force Incident Response Intelligence Services (IRIS) has uncovered rare details on the operations of the suspected Iranian threat group ITG18, which overlaps with Magic Hound, APT 35, Cobalt Illusion, Charming Kitten, Rocket Kitten, Newscaster, NewsBeef and APT 42. In the past few weeks, ITG18 has been associated with targeting of pharmaceutical companies and the U.S. presidential campaigns. Now, due to operational errors—a basic misconfiguration—by suspected ITG18 associates, a server with more than 40 gigabytes of data on their operations has been analyzed by X-Force IRIS analysts. Rarely are there opportunities to understand how the operator behaves behind the keyboard, and even rarer still are there recordings the operator self-produced showing their operations. But that is exactly what X-Force IRIS uncovered on an ITG18 operator whose OPSEC failures provide a unique behind-the-scenes look into their methods, and potentially, their legwork for a broader operation that is likely underway.	
Observed	Sectors: Defense, Government, Pharmaceutical. Countries: USA.	
Tools used		
Operations performed	May 2020	During a three-day period in May 2020, IBM X-Force IRIS discovered the 40 GBs of video and data files being uploaded to a server that hosted numerous ITG18 domains used in earlier 2020 activity. Some of the videos showed the operator managing adversary-created accounts while others showed the operator testing access and exfiltrating data from previously compromised accounts. <https://securityintelligence.com/posts/new-research-exposes-iranian-threat-group-operations/>

Information	<https://securityintelligence.com/posts/new-research-exposes-iranian-threat-group-operations/> <https://securityintelligence.com/posts/itg18-operational-security-errors-plague-iranian-threat-group/>

Last change to this card: 13 September 2022

Download this actor card in PDF or JSON format
