Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:15:59 UTC

APT group: Iridium

Names	Iridium *(Resecurity)*	
Country	Iran	
Motivation	Information theft and espionage	
First seen	2018	
Description	(Kaspersky) Iridium is an APT that uses proprietary techniques to bypass two-factor authentication for critical applications, according to security firm Resecurity. A researcher has attributed a recently publicized attack on Citrix' internal network to the Iranian-linked group known as Iridium – and said that the data heist involved 6 terabytes of sensitive data. The culprit is an APT that uses proprietary techniques to bypass two-factor authentication for critical applications and services for further unauthorized access to virtual private networks and single sign-on systems, according to Resecurity. "[Iridium] has hit more than 200 government agencies, oil and gas companies and technology companies, including Citrix Systems Inc.," they said. Threatpost has reached out for further details as to how the firm is linking the APT to the attack and will update this post accordingly.	
Observed	Sectors: Government, Oil and gas, Technology.	
Tools used	China Chopper, LazyCat, Powerkatz, Recon, reGeorg and Ckife Webshells.	
Operations performed	Dec 2018	Attacks on Australian government <https://www.scmagazine.com/home/security-news/apts-cyberespionage/iridium-cyberespionage-gang-behind-aussie-parliament-attacks/> <https://blog.yoroi.company/research/the-arsenal-behind-the-australian-parliament-hack/>
	Dec 2018	Breach of Citrix <https://threatpost.com/ranian-apt-6tb-data-citrix/142688/>

Information	<https://hub.packtpub.com/resecurity-reports-iriduim-behind-citrix-data-breach-200-government-agencies-oil-and-gas-companies-and-technology-companies-also-targeted/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
