Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:53:34 UTC

Other threat group: Fxmsp

Names	Fxmsp *(self given)* ATK 134 *(Thales)* TAG-CR17 *(Recorded Future)*	
Country	Kazakhstan	
Motivation	Financial gain	
First seen	2016	
Description	(AdvIntel) Throughout 2017 and 2018, Fxmsp established a network of trusted proxy resellers to promote their breaches on the criminal underground. Some of the known Fxmsp TTPs included accessing network environments via externally available remote desktop protocol (RDP) servers and exposed active directory. Most recently, the actor claimed to have developed a credential-stealing botnet capable of infecting high-profile targets in order to exfiltrate sensitive usernames and passwords. Fxmsp has claimed that developing this botnet and improving its capabilities for stealing information from secured systems is their main goal.	
Observed	Sectors: Aviation, Education, Energy, Financial, Food and Agriculture, Government, Manufacturing, Retail, Transportation. Countries: Australia, Brazil, Canada, Chile, China, Colombia, Cyprus, Ecuador, Egypt, El Salvador, Germany, Ghana, Hong Kong, India, Indonesia, Ireland, Italy, Jamaica, Japan, Kenya, Kuwait, Malaysia, Maldives, Mexico, Netherlands, Nigeria, Oman, Pakistan, Philippines, Russia, Saudi Arabia, Singapore, South Africa, South Korea, Sri Lanka, Thailand, UAE, UK, USA, Zimbabwe.	
Tools used	RDP and exposed AD.	
Operations performed	May 2019	Breaches of Three Major Anti-Virus Companies <https://www.advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies>
Counter operations	Jul 2020	Feds indict 'fxmsp' in connection with million-dollar hacking operation

		<https://www.cyberscoop.com/fxmsp-andrey-turchin-indictment-fraud-stolen-data/>
Information	<https://www.advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies> <https://www.group-ib.com/resources/threat-research/fxmsp-report.html>	

Last change to this card: 09 December 2021

Download this actor card in PDF or JSON format
