Tropical Scorpius, RomCom - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:16:53 UTC

APT group: Tropical Scorpius, RomCom

Names	Tropical Scorpius *(Palo Alto)* RomCom *(Palo Alto)* Void Rabisu *(Trend Micro)* DEV-0978 *(Microsoft)* Storm-0671 *(Microsoft)* Storm-0978 *(Microsoft)* UNC2596 *(Mandiant)* CIGAR *(Mandiant)* UAC-0180 *(CERT-UA)* TA829 *(Proofpoint)*	
Country	Russia	
Motivation	Information theft and espionage, Financial gain	
First seen	2019	
Description	(Palo Alto) The most recent Unit 42 Ransomware Threat Report includes observations of Cuba Ransomware impacting 33 organizations. As of July 2022, Tropical Scorpius has used Cuba Ransomware to impact 27 additional organizations across multiple vectors, such as Professional and Legal Services, State and Local Government, Manufacturing, Transportation and Logistics, Wholesale and Retail, Real Estate, Financial Services, Health Care, High Technology, Utilities and Energy, Construction, and Education. A total of 60 organizations were exposed by this ransomware gang on its leak site since the group first surfaced in 2019.	
Observed	Sectors: Construction, Education, Energy, Financial, Government, Healthcare, High-Tech, Manufacturing, Shipping and Logistics, Transportation.	
Tools used	Cuba, Industrial Spy, ROMCOM RAT, Underground.	
Operations performed	Jul 2022	Unattributed RomCom Threat Actor Spoofing Popular Apps Now Hits Ukrainian Militaries

		<https://blogs.blackberry.com/en/2022/10/unattributed-romcom-threat-actor-spoofing-popular-apps-now-hits-ukrainian-militaries>
	Nov 2022	RomCom Threat Actor Abuses KeePass and SolarWinds to Target Ukraine and Potentially the United Kingdom <https://blogs.blackberry.com/en/2022/11/romcom-spoofing-solarwinds-keepass>
	Feb 2023	Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals <https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html>
	Jun 2023	Storm-0978 attacks reveal financial and espionage motives <https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/>
	Jun 2023	Void Rabisu Targets Female Political Leaders with New Slimmed-Down ROMCOM Variant <https://www.trendmicro.com/en_us/research/23/j/void-rabisu-targets-female-leaders-with-new-romcom-variant.html>
	Jul 2023	RomCom Threat Actor Suspected of Targeting Ukraine's NATO Membership Talks at the NATO Summit <https://blogs.blackberry.com/en/2023/07/romcom-targets-ukraine-nato-membership-talks-at-nato-summit>
	Oct 2024	RomCom exploits Firefox and Windows zero days in the wild <https://www.welivesecurity.com/en/eset-research/romcom-exploits-firefox-and-windows-zero-days-in-the-wild/>
Information	<https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/> <https://thehackernews.com/2025/04/nebulous-mantis-targets-nato-linked.html> <https://www.proofpoint.com/us/blog/threat-insight/10-things-i-hate-about-attribution-romcom-vs-transferloader>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
