Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:33:47 UTC

APT group: RedCurl

Names	RedCurl *(Group-IB)* Red Wolf *(BI.ZONE)* Earth Kapre *(Trend Micro)*	
Country	[Unknown]	
Motivation	Information theft and espionage	
First seen	2018	
Description	(ZDNet) Security researchers have uncovered a new Russian-speaking hacking group that they claim has been focusing on the past three years on corporate espionage, targeting companies across the world to steal documents that contain commercial secrets and employee personal data. Named RedCurl, the activities of this new group have been detailed in a 57-page report released today by cyber-security firm Group-IB. The company has been tracking the group since the summer of 2019 when it was first called to investigate a security breach at a company hacked by the group. Since then, Group-IB said it identified 26 other RedCurl attacks, carried out against 14 organizations, going as far back as 2018.	
Observed	Sectors: Construction, Financial, Retail and travel agencies and law and consulting firms. Countries: Australia, Canada, Germany, Mexico, Norway, Russia, Spain, UK, Ukraine, USA.	
Tools used	Impacket, LaZagne.	
Operations performed	2021	RedCurl: The awakening <https://www.group-ib.com/resources/threat-research/red-curl-2.html>
	Nov 2022	RedCurl hackers return to spy on 'major Russian bank,' Australian company <https://therecord.media/redcurl-hackers-russian-bank-australian-company>

	2023	Hunting the hunter: BI.ZONE traces the footsteps of Red Wolf <https://bi-zone.medium.com/hunting-the-hunter-bi-zone-traces-the-footsteps-of-red-wolf-3677783e164d>
	2023	Unveiling Earth Kapre aka RedCurl’s Cyberespionage Tactics With Trend Micro MDR, Threat Intelligence <https://www.trendmicro.com/en_us/research/24/c/unveiling-earth-kapre-aka-redcurls-cyberespionage-tactics-with-t.html>
	Mar 2025	RedCurl's Ransomware Debut: A Technical Deep Dive <https://www.bitdefender.com/en-us/blog/businessinsights/redcurl-qwcrypt-ransomware-technical-deep-dive>
Information	<https://www.zdnet.com/article/redcurl-cybercrime-group-has-hacked-companies-for-three-years/> <https://www.group-ib.com/resources/threat-research/red-curl.html> <https://www.esentire.com/blog/unraveling-the-many-stages-and-techniques-used-by-redcurl-earthkapre-apt>	

Last change to this card: 21 April 2025

Download this actor card in PDF or JSON format
