RedCurl: The Awakening

Commercial cyber espionage remains a rare and largely unique phenomenon. We cannot rule out, however, that RedCurl's success could lead to a new trend in the cybercrime arena.

Download report

In this report:

TTPs	Discover the group's new and updated tools as well as its tactics and infrastructure characteristics mapped to the MITRE ATT&CK® matrix
Kill Chain	Gain insights into a detailed kill chain of the latest attack based on incident response activities and

	unique data from Group-IB Threat Intelligence & Attribution
IoCs and recommendations	Learn indicators of compromise and a set of mitigations to secure your organization against RedCurl attacks

About the report:

Last year, Group-IB specialists discovered a new Russian-speaking hacker group that they named RedCurl. Between 2018 and 2020, the group carried out 26 attacks for the purposes of corporate espionage and documentation theft. Group-IB identified 14 victim organizations across various industries. Seven months later, in 2021, the attacks resumed. Group-IB's most recent report details how the adversary's tactics and tools have changed and reveals the group's new victims.

About RedCurl

Goal

Corporate espionage and documentation theft

Active

Since 2018

Attack total

30, including 4 attacks since the start of 2021

Dwell time in the victim's infrastructure

2–6 months

Victims

15

Relevant reports

We see the full picture of the evolving cyber threat landscape thanks to unique tools for monitoring the infrastructure used by cybercriminals and data from battlefields:

Threat Research

Conti Armada: The ARMattack Campaign

Take a deep dive into “ARMattack”, one of the shortest yet most successful campaigns...

Learn more

Download report

Products

- Threat Intelligence
- Fraud Protection
- Managed XDR
- Attack Surface Management
- Digital Risk Protection
- Business Email Protection
- Cyber Fraud Intelligence Platform
- Unified Risk Platform
- Integrations

Resources

- Research Hub
- Success Stories
- Knowledge Hub
- Certificates
- Webinars
- Podcasts
- TOP Investigations
- Ransomware Notes

- AI Cybersecurity Hub

Partners

- Partner Program
- MSSP and MDR Partner Program
- Technology Partners
- Partner Locator

Company

- About Group-IB
- Team
- CERT-GIB
- Careers
- Internship
- Academic Aliance
- Sustainability
- Media Center
- Contact

Subscription plans

Services

Resource Center

Contact

APAC: +65 3159 3798

Subscribe to stay up to date with the latest cyber threat trends

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com