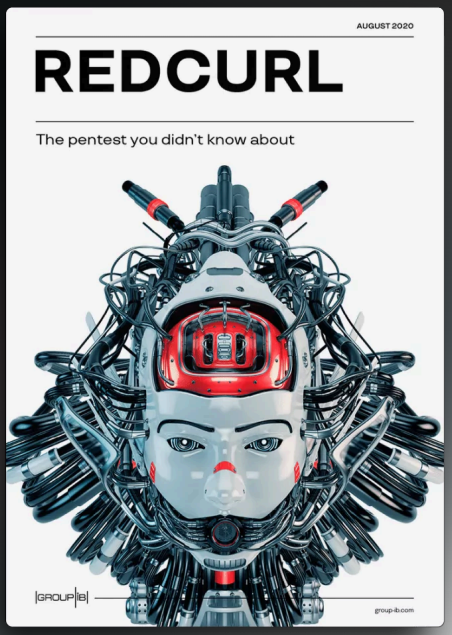
GROUP-IB



RedCurl: The Pentest You Didn't Know About

The APT group continues to successfully attack enterprise companies in North America, Europe, and CIS countries after remaining undetected for years. Their goal is carefully planned, targeted cyber espionage.

View report

In this report:

TTPs	First description of TTPs and infrastructure of the new threat actor

Kill Chain	Detailed kill chain based on unique incident response data
Attribution	Possible connections with Red October and Cloud Atlas campaigns

For RedCurl it makes no difference whether to attack a consulting company in Canada or a Russian bank. Because the contents of the victim's documents and records can be much more valuable than the contents of their own wallets: the consequences of espionage can amount to tens of millions of dollars, despite the lack of direct financial losses.

RedCurl implements various techniques to stay undetected for months. The lack of indicators and technical data about the group makes it easier for the threat actor to remain active. We continue to track new attacks worldwide and therefore included IoCs in the report, which organizations can use to check their networks for signs of RedCurl infections.

Rustam Mirkasymov
Head of Cyber Threat Research

Advanced protection against cyber threats

Group-IB's security ecosystem provides comprehensive protection for your IT infrastructure based on our unique cyber intelligence and deep analysis of attacks and incident response.

- Threat Intelligence
- Fraud Protection
- Managed XDR
- Digital Risk Protection

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

Ransomware Uncovered 2021/2022

The well-known complete guide to the latest tactics, techniques, and procedures of ransomware operators...

Learn more

Download report

GROUP-IB

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