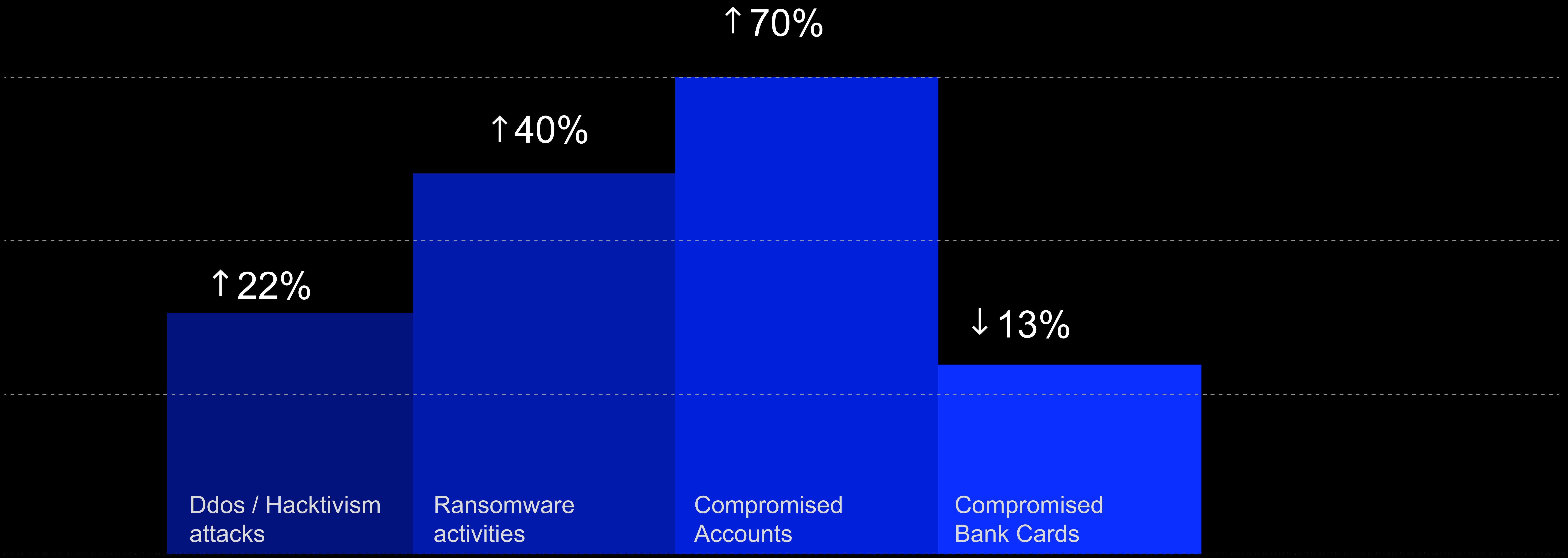
GROUP-IB

INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for January 2025

Report is based on data from 01.01.2025 till 01.02.2025

THREAT LANDSCAPE OVERVIEW



Data comparison: December 2024 - January 2025

GLOBAL TRENDS

Global Trends from Group-IB with a brief description:

01
Discover how the **Lynx** Ransomware-as-a-Service (RaaS) group operates, detailing the workflow of their affiliates within the panel, their cross-platform ransomware arsenal, customizable encryption modes, and advanced technical capabilities.

Ransomware remains one of the most profitable cyberthreats, with new variants and business models evolving faster than many organizations can respond. These attacks have become both more pervasive and more sophisticated.

The Lynx RaaS group stands out for its highly organized platform, structured affiliate program, and robust encryption methods. In this blog, we provide an exclusive look at Lynx's affiliate panel, internal communications, and technical arsenal, revealing how this criminal ecosystem orchestrates ransomware attacks and manages victims.

More information in our blog.

02
Group-IB cyber fraud analysts have uncovered an ongoing real-estate scam targeting expatriates working in, or relocating to the Middle East.

The scheme involves scammers using fake ads based on real property listings on popular real estate platforms, and then shifting the negotiations to instant messaging services, such as Telegram or WhatsApp. As soon as their victims transfer the payment for the property, the money is then funnelled via mule accounts and the listing is deleted, leaving the victims with no recourse.

Key highlights of this blog:

- The median financial loss per case of this fraud scheme type in the Middle East is $3,064 USD, with estimated annual losses by victims in the millions of dollars.
- Scammers utilise real property listings to create fake property ads on legitimate real-estate platforms in order to lure their victims.
- Based on geohash data uncovered by our analysts, the scammers seem to originate from Syria, sometimes using VPNs or GPS spoofing programs to mask their location.

More information here.

REGIONAL TRENDS

Regional Trends from Group-IB with a brief description:

01
We see an increase in phishing attacks targeting Indonesia Bank Sector. The number of targeted phishing attacks increased, targeting the biggest banks in Indonesia.

02
Recent malicious campaigns with KamiKakaBot targeted financial organizations in Vietnam.

Group-IB specialists during the investigation discovered several malicious archives with previously known malicious tool belonging to APT Dark Pink. The archive contains 3 files. Instead of traditionally using a legal executable with a malicious DLL that launches using DLL sideloading technique, cybercriminals use a malicious LNK file that infects target machines when victims double-click it. As a result, KamiKakaBot was launched.
More information.

03
Group-ib published a blog about the Social Engineering in Action: How Fraudsters Exploit Trust with Fake Refund Schemes in the Middle East. The same schemes are widely used in APAC and ANZ regions. More information here.

Fraudsters have devised a sophisticated social engineering scheme that has proven its effectiveness in deceiving customers in the Middle East into disclosing their credit card credentials. This scheme involves impersonating government officials to gain the trust of its victims and utilizing Remote Access Software to steal user’s sensitive data. The scam specifically targets individuals who have previously submitted commercial complaints to the government services portal, either through its website or mobile app, regarding products or services purchased from online merchants.

04
Group-IB researchers discovered a series of attacks on government organizations in the CIS and APAC countries by ShadowSilk threat actor group, During the analysis, it was established that the attacks were carried out starting in 2023. The attackers were able to gain access to quite a number of organisations. More information here.

APAC and ANZ

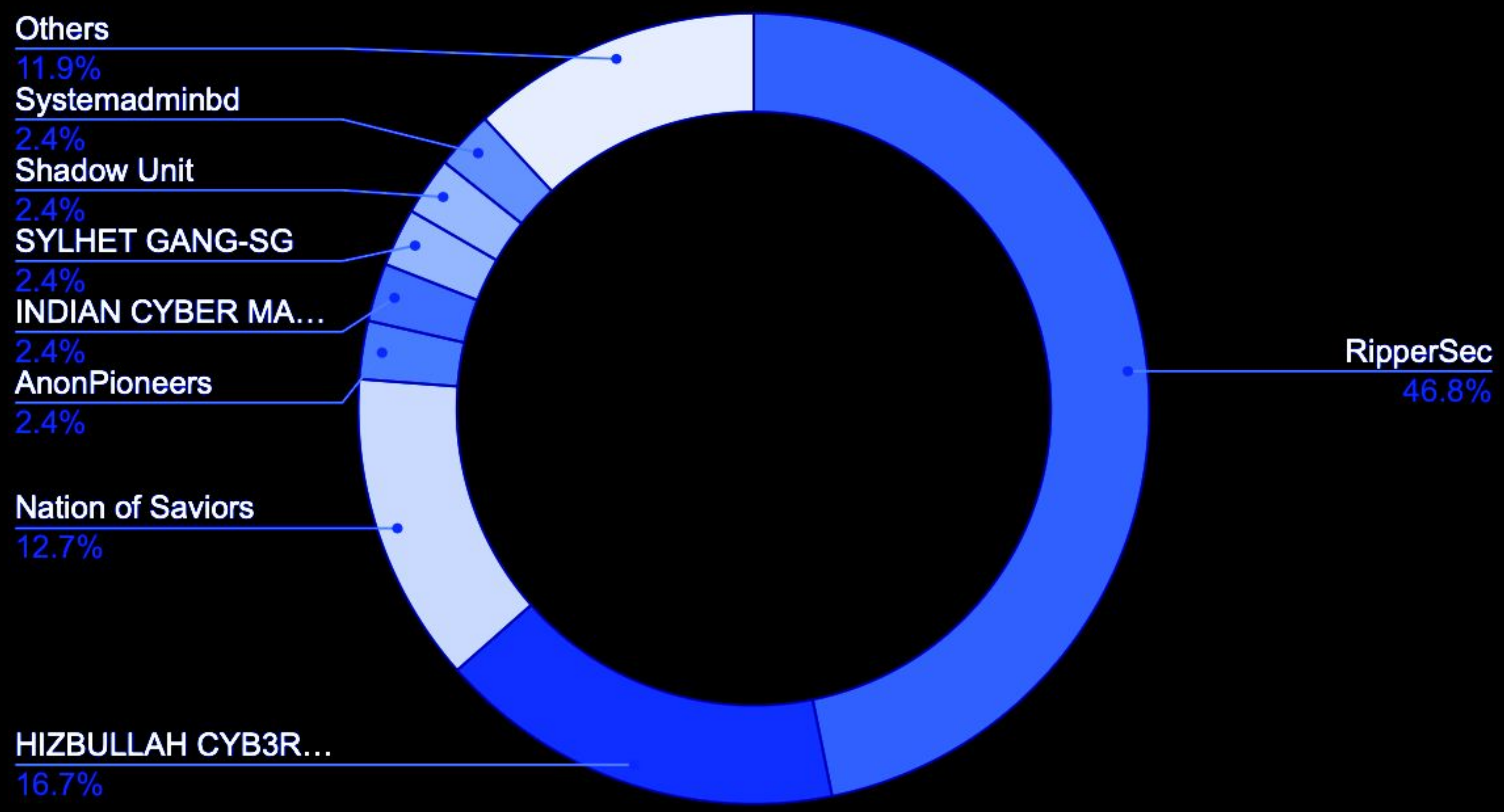
More Information in Group-IB Threat Intelligence Portal

DDOS AND HACKTIVISM

Hacktivism is the use of hacking to promote political or social agendas. Usually hacktivist groups are low-skill hackers who perform DDoS, Defacement, and Data Breaches (mostly leverages compromised accounts) attacks. Unfortunately, during the last year these groups attracted a lot of attention.

Below is a brief overview of groups that were active in the APAC region during the previous month:

DDOS and Hacktivism Activities, per group

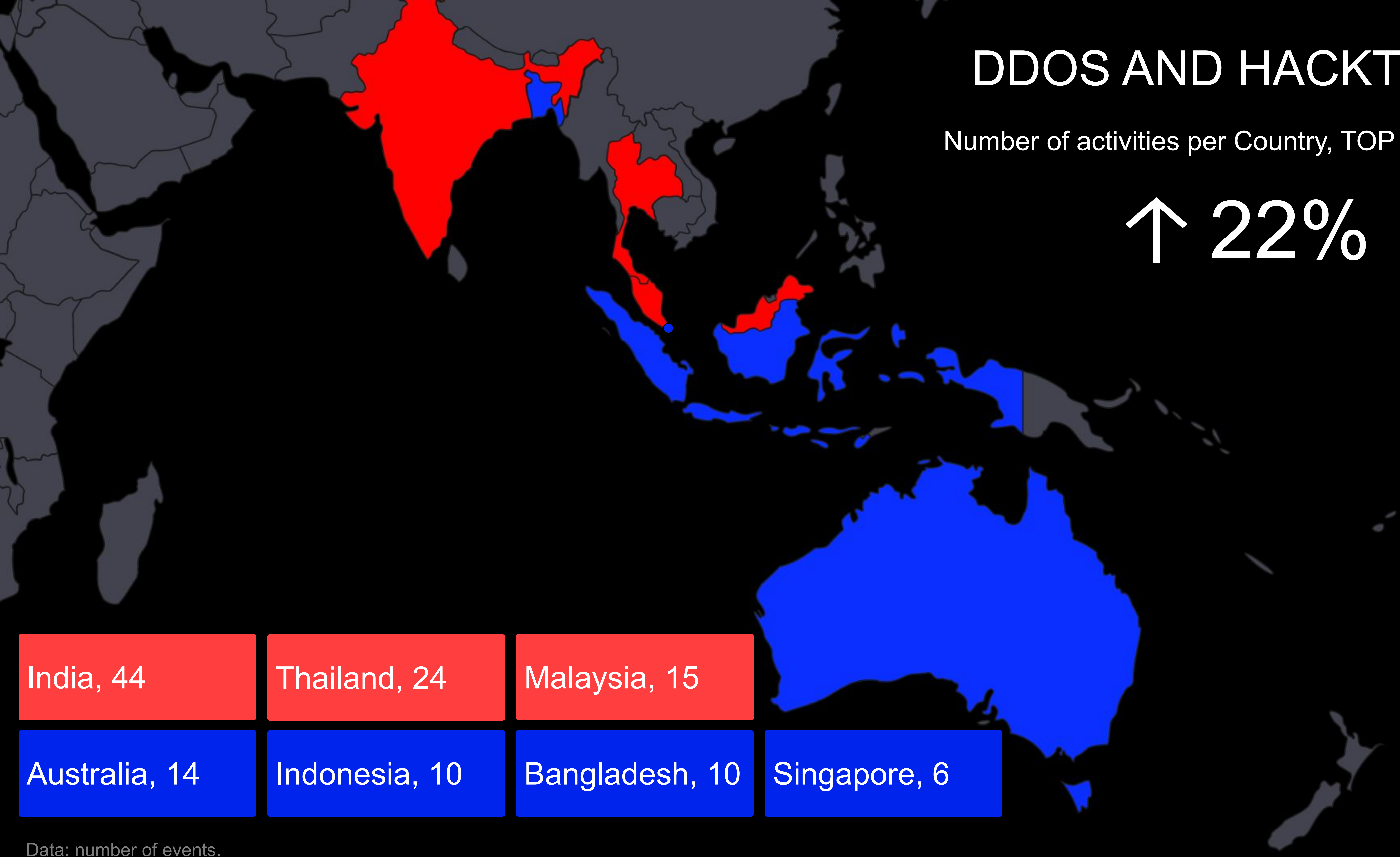


Data: number of events.

DDOS AND HACKTIVISM

Number of activities per Country, TOP 7 countries

↑ 22%



India, 44

Thailand, 24

Malaysia, 15

Australia, 14

Indonesia, 10

Bangladesh, 10

Singapore, 6

Data: number of events.

RANSOMWARE ACTIVITIES

GROUP-IB

↑ 40%

94 Ransom activities

Most active threat actors

SafePay

18 activities
+ 125%

FunkSec

10 activities
- 55%

KillSec

10 activities

Space Bears

10 activities
+11%

Cl0p

9 activities

Most targeted Countries

India

29 activities
+ 20,83%

Singapore

14 activities
+ 180%

Australia

13 activities
+ 0%

New Zealand

7 activities
+40%

Vietnam

5 activities
+0%

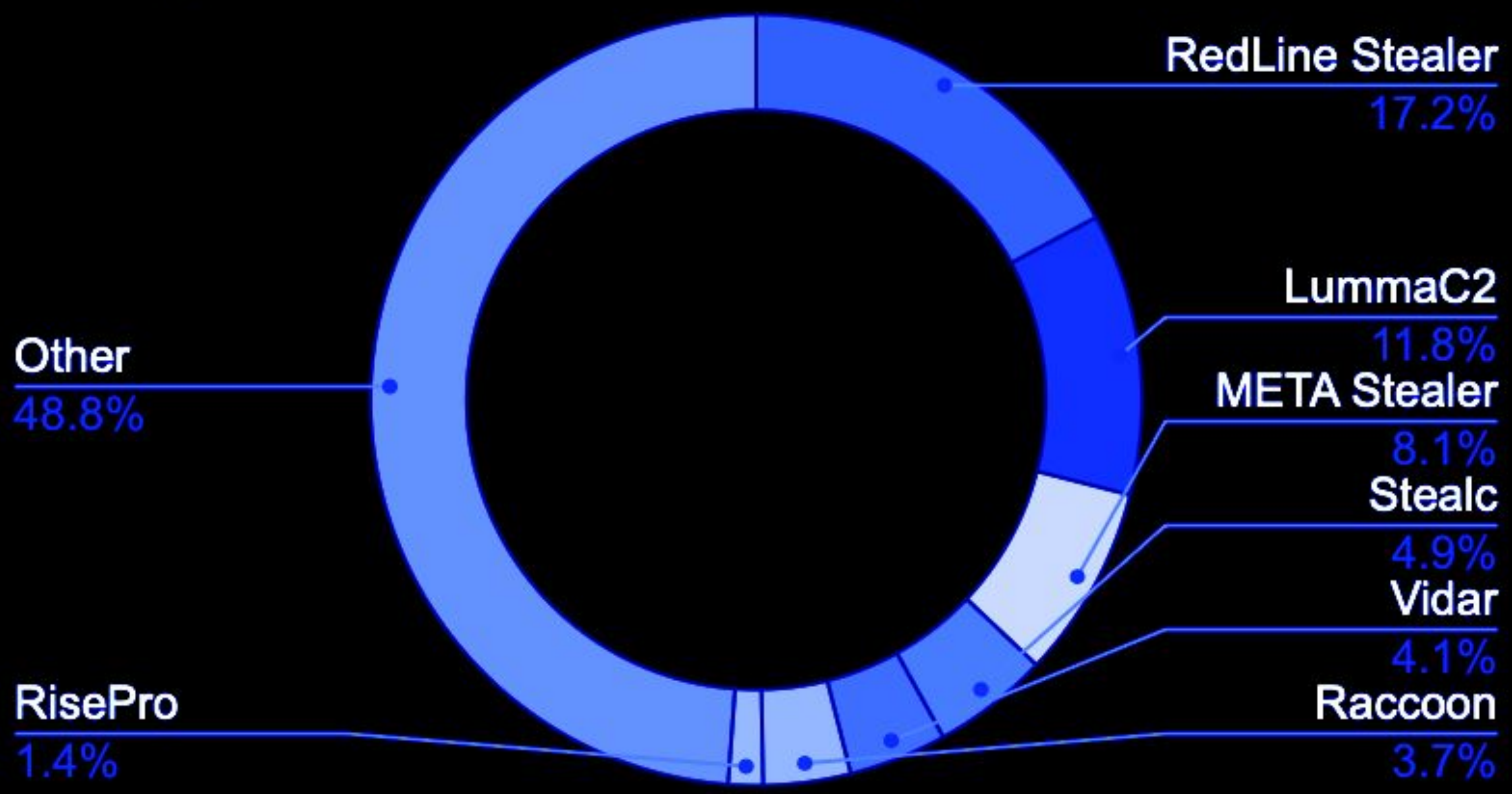
COMPROMISED DATA ↑ 70%

Statistics regarding compromised accounts.

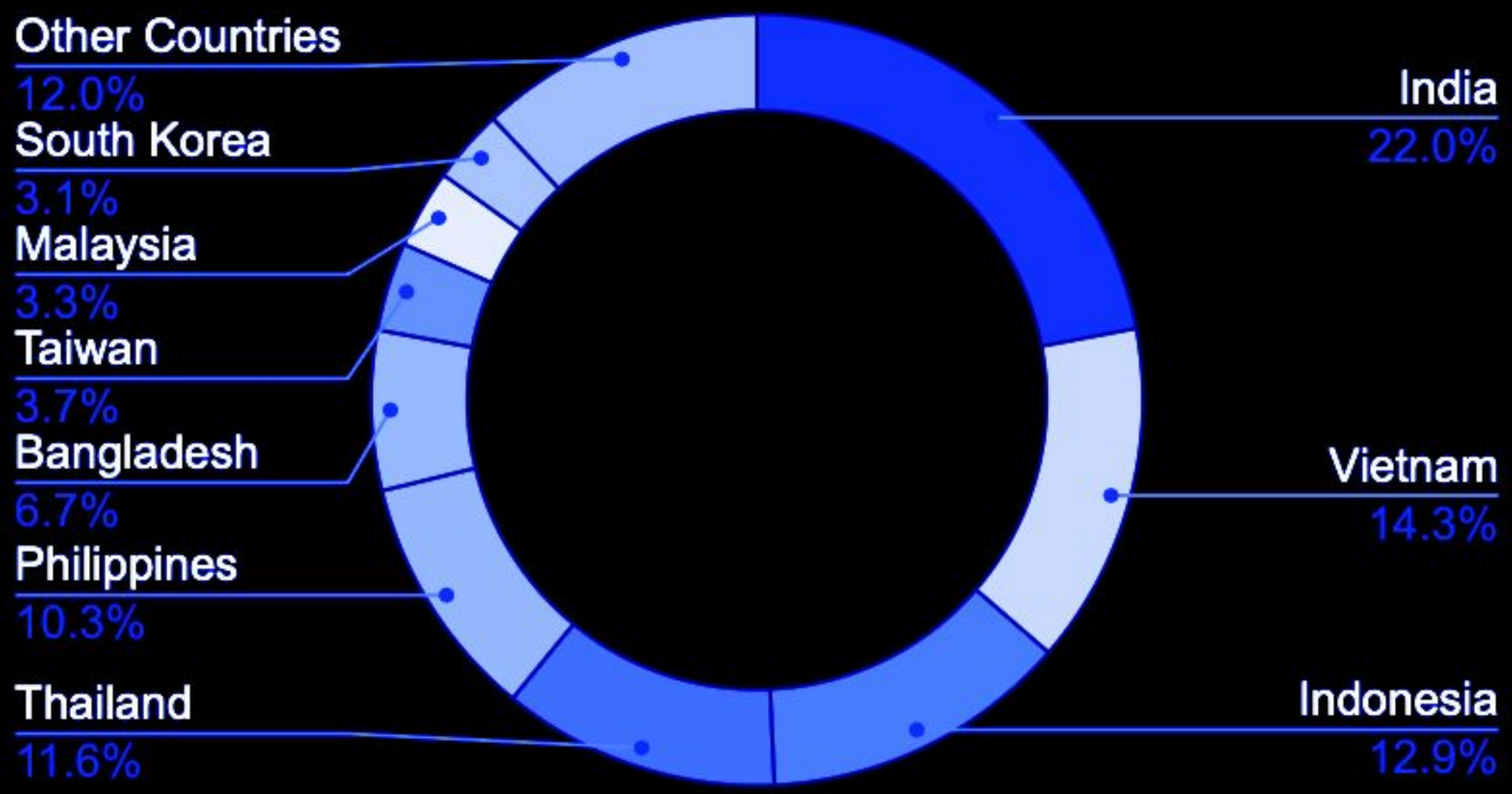
Key Trends in January 2025:

- Significant increase in the number of compromised accounts in APAC and ANZ, especially in Vietnam
- The Number of compromised accounts in India, Indonesia and Vietnam is consistently high, again.
- RedLine stealer, LummaC2 and META - unchangeable leaders among other tools.

Compromised Accounts by Malware



Compromised Accounts by Country



Data: number of events. Each malware can be part of the same event.

COMPROMISED BANK CARDS

↓ 13%

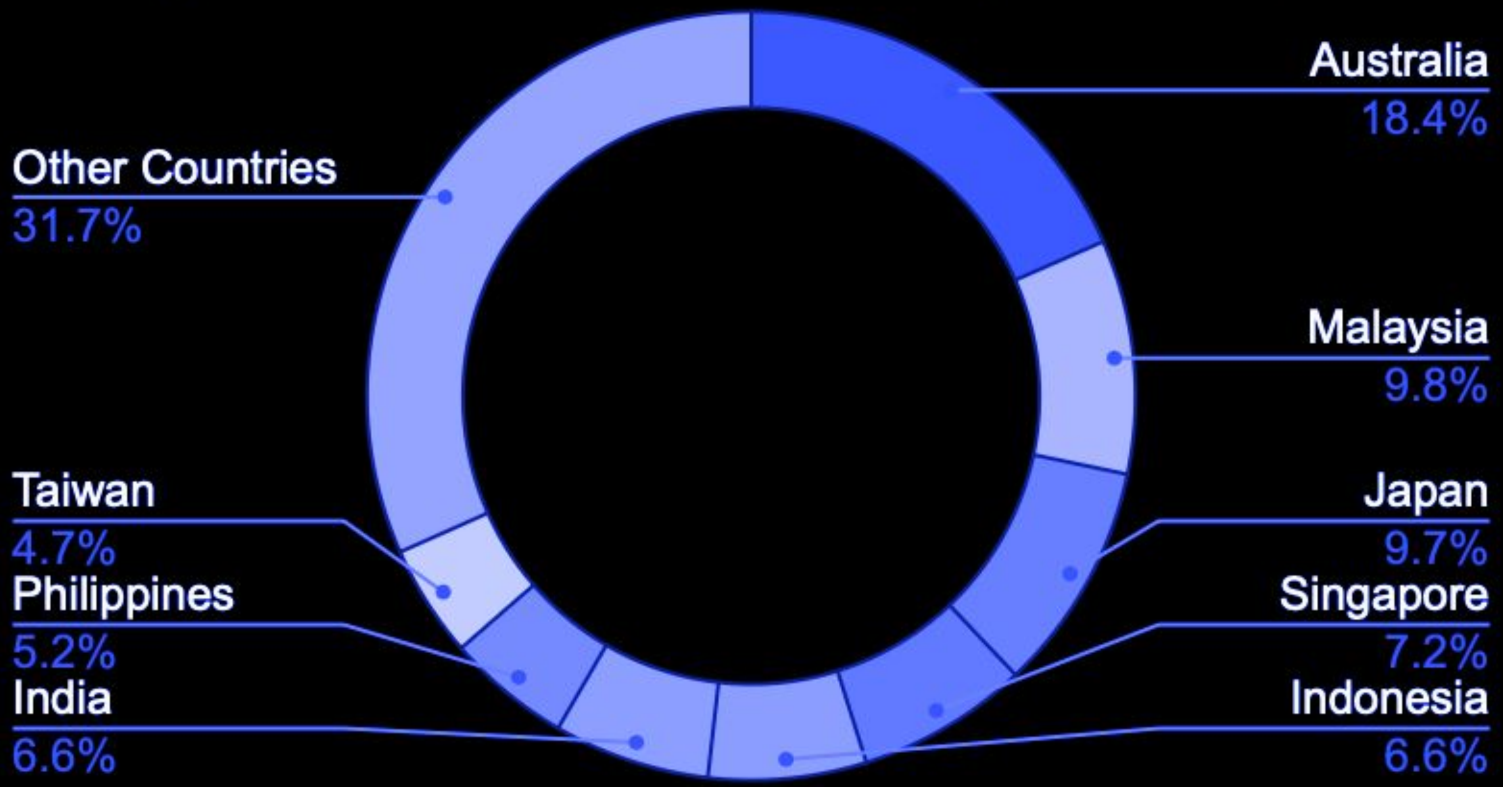
GROUP-IB

Statistics regarding compromised accounts.

Key Trends in January 2025:

- A little decrease in the number of compromised bank cards in APAC and ANZ.
- The Number of compromised accounts in Australia, Malaysia and Singapore is consistently high.
- Main sources of information - data leaks and phishing attacks. Phishing was and is a constant threat to any company in any industry.

Compromised Bank Cards by Country



Data: number of events. Each malware can be part of the same event

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

Clop

Targeted industries:

- Manufacturing
- Information technology
- Financial services
- Software
- Education
- Healthcare
- Transportation
- Retail

Period of Activity:	2019 - Present
Targeted countries:	Worldwide
Attribution:	Unknown
Intent:	Financially-motivated

Attack Summary

In December 2024, the Clop ransomware group leveraged critical vulnerabilities – CVE-2024-50623 and CVE-2024-55956 in Cleo's file transfer software to gain unauthorized access and steal data from multiple organizations.

Key Observations

- Clop deployed Malichus backdoors for prolonged network infiltration.
- The group indicated selective deletion of sensitive government, medical, and research data to avoid escalation.
- Data exfiltrated in the Cleo breaches is reportedly deleted from their servers as part of internal policy shifts.

STAY SMART. STAY CONNECTED. STAY SECURED

GROUP-IB

GROUP-IB

Threat intelligence

Threat evolution in Q4 2024

GROUP-IB.COM

APAC
+65 3159 3798

EU & NA
+31 20 226 90 90

MEA
+971 4 568 1785

Read now in Group-IB TI platform

GROUP-IB

CYBERSECURITY ULTIMATE ASSESSMENT GUIDE

PART 1. ASSESSMENT COMPASS

GROUP-IB.COM

E-GUIDE

Read now

GROUP-IB

THREAT HUNTING

ADVERSARY HUNTING CODE: UNCOVER AND ELIMINATE UNKNOWN CYBER THREATS WITH GROUP-IB

Threats often lurk in the shadows, undetected, until they escalate into full-blown crises. The key to staying protected is to hunt them down—or risk being hunted. Learn how to do it the right way with Group-IB expert-curated and industry-proven approaches

GROUP-IB.COM

Read now

CONCLUSIONS AND RECOMMENDATIONS

GROUP-IB

The evolving threat landscape poses significant risks to organizations across various sectors. The incidents discussed in this report underscore the need for robust security measures and proactive threat management. To safeguard your organization, consider implementing the following recommendations:

ENHANCE SECURITY AWARENESS TRAINING

Regularly educate employees on recognizing phishing attempts, social engineering tactics, and safe online practices.

STRENGTHEN IT INFRASTRUCTURE

Ensure all systems are updated with the latest security patches and employ multi-factor authentication (MFA) to enhance access controls.

CONDUCT REGULAR SECURITY AUDITS

Perform periodic assessments of your IT environment to identify and mitigate potential vulnerabilities.

DEPLOY ADVANCED THREAT DETECTION TOOLS

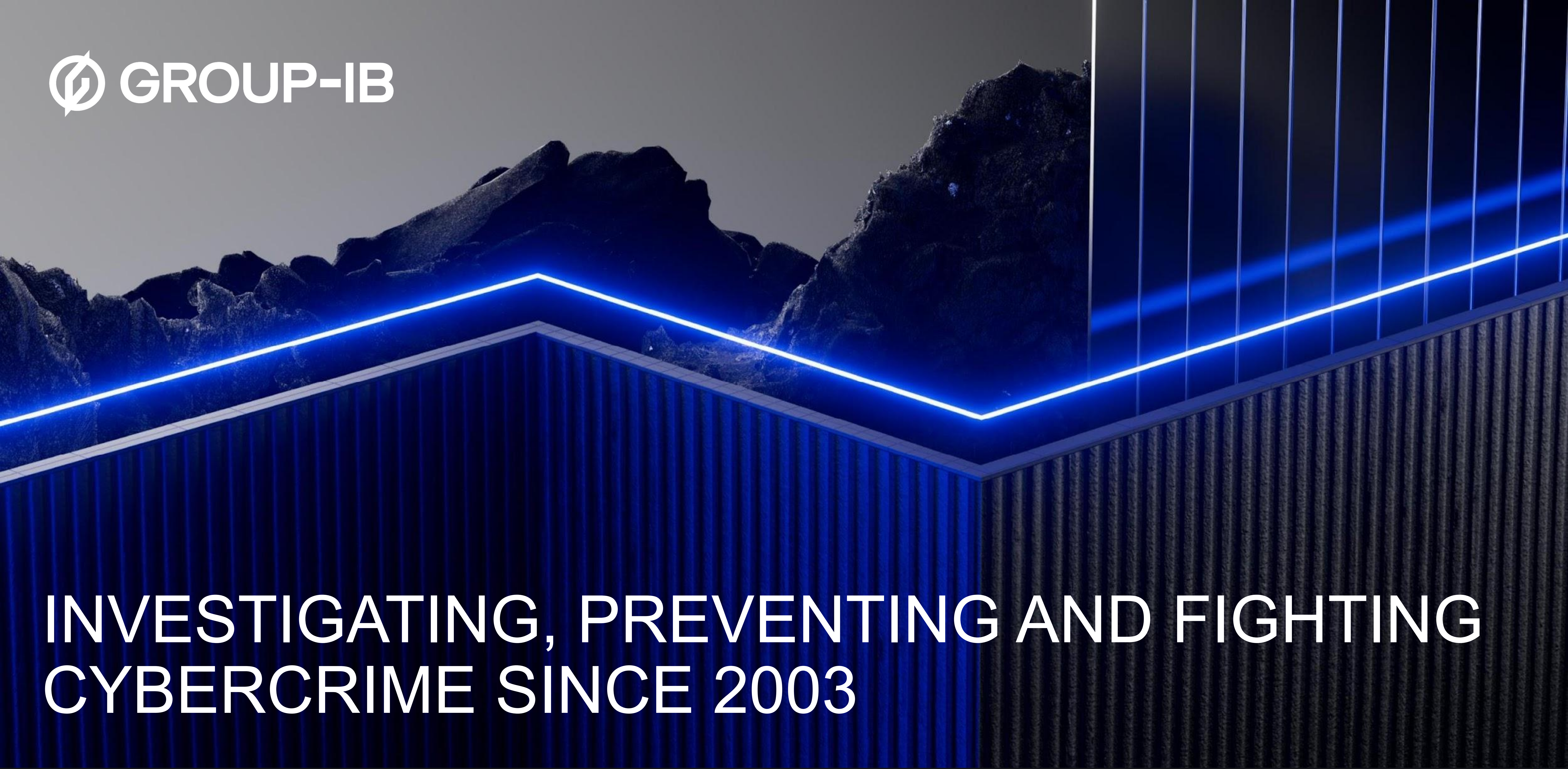
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

ESTABLISH INCIDENT RESPONSE PROTOCOLS

Develop and regularly update an incident response plan to quickly address and mitigate the impact of security breaches.

COLLABORATE WITH THREAT INTELLIGENCE SERVICES

Leverage threat intelligence services to stay informed about emerging threats and adjust your security strategies accordingly.



GROUP-IB

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM

GROUP-IB.COM/BLOG
+971 45681785

LINKEDIN FACEBOOK TWITTER INSTAGRAM