INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for April 2025

Report is based on data from 01.04.2025 till 01.05.2025

THREAT LANDSCAPE OVERVIEW

Ransomware activities

↓ 38.56%

DDoS and Hacktivism

↑ 42.34%

↓ 311%

Compromised Accounts

↓ 17.4%

Compromised Bank Cards

Data comparison: March 2025 - April 2025

GLOBAL INSIGHTS

Global Insights from Group-IB with a brief description:

01

Ransomware debris: an analysis of the RansomHub operation

This blog on RansomHub provides an overview into how this Ransomware-as-a-Service (RaaS) group operates, including its extortion tactics, affiliate recruitment strategies, and the features of its affiliate panel. More Information.

02

The beginning of the end: the story of Hunters International

Learn about technical details on the ransomware and Storage Software tool, how the criminals use the affiliate panel as well as information on the Hunters International ransomware group from its emergence to the end of the operation. More Information.

03

Typical Dark Web Fraud: Where Scammers Operate and What They Look Like

In the dark corners of the internet, countless individuals claim to be cybercriminals responsible for massive breaches and sensitive data leaks. These self-proclaimed threat actors often boast about hacking major corporations resulting in compromising internal resources — actions that inevitably attract the attention. In reality, many of these claims are completely false. More Information.

REGIONAL INSIGHTS

GROUP-IB

Regional Insights from Group-IB with a brief description:

01

Toll of Deception: Where Evasion Drives Phishing Forward

Group-IB researchers uncovered a highly coordinated phishing campaign in which scammers leveraged third-party JavaScript libraries such as FingerprintJS and Cleave.js to evade detection and verify input data in real time.

While techniques such as user input validation and victim selection based on IP, region, or language are commonly used by threat actors, this campaign stands out by incorporating browser fingerprinting as an additional layer of control. This approach helps restrict access to targeted victims while simultaneously complicating analysis by researchers and automated tools.

As of this writing, the phishing campaign remains active, with threat actors continuously generating and distributing new malicious links to unsuspecting victims. More Information.

02

SMS Pumping: How Criminals Turn Your Messaging Service into Their Cash Machine

SMS Pumping, also known as artificial traffic inflation, is a type of fraud where attackers exploit SMS-based services, such as one-time passwords (OTPs) or notifications, to generate excessive message traffic using fake or automated phone numbers. This causes businesses to incur inflated costs, experience false engagement, and face disruptions in their operations. Fraudsters leverage this technique for financial gain or to strain application resources.
More Information.

03

Group-IB Analysis of private Oracle database samples obtained from seller rose87168

In March 2025, a threat actor known as rose87168 offered for sale data allegedly stolen from Oracle, the American multinational computer technology corporation — specifically targeting its Oracle Cloud services. The attacker claimed the breach occurred in January 2025 and initially attempted to negotiate a private sale with Oracle, which was reportedly unsuccessful. Group-IB Threat Intelligence analysts were able to persuade the seller 'rose87168', who claimed to have Oracle Cloud databases, to share samples of the data being offered for sale. We analyzed it and presented in Threat Intelligence platform. More Information.

APAC and ANZ

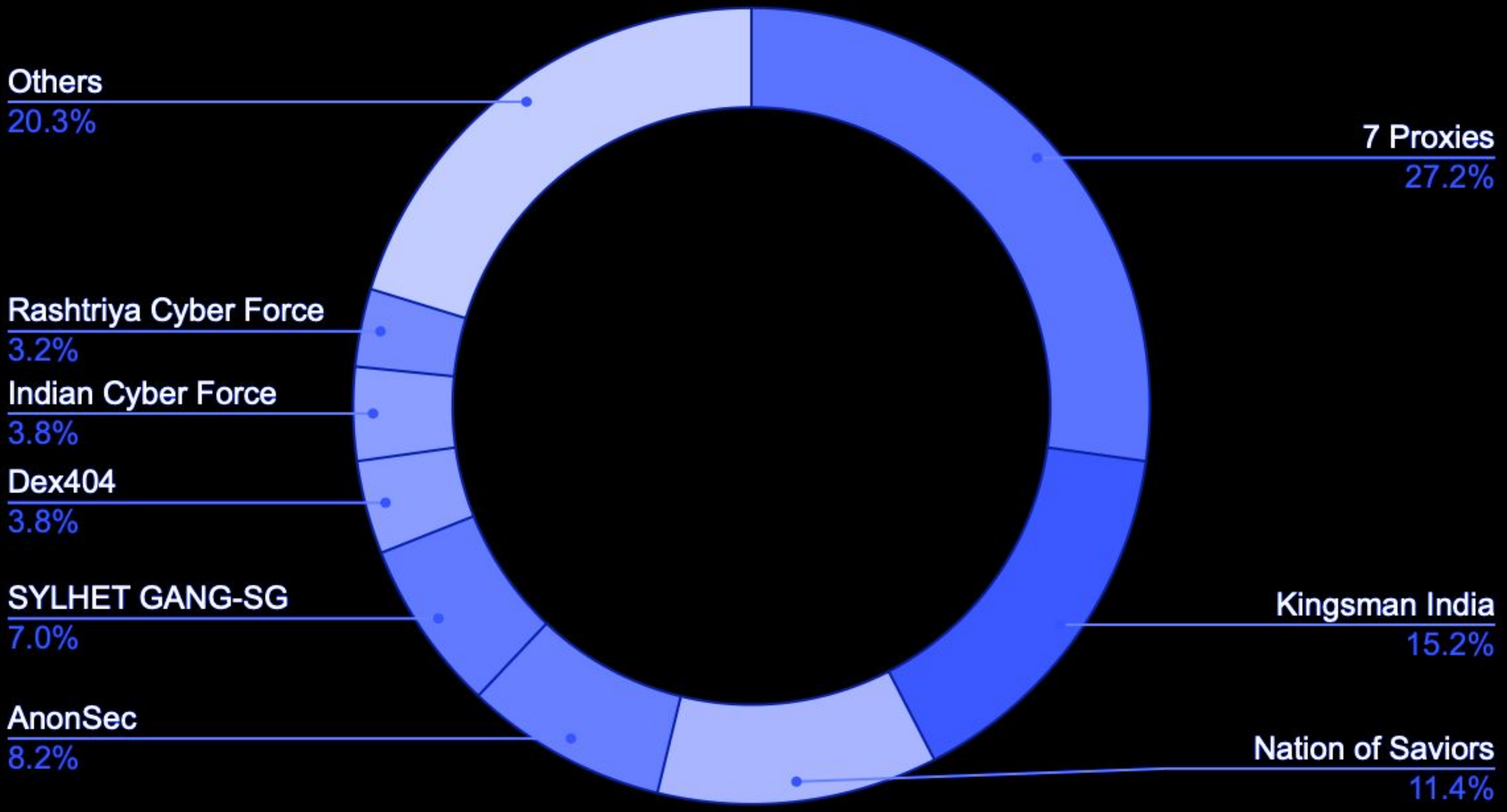
More Information in Group-IB Threat Intelligence Portal

DDOS AND HACKTIVISM

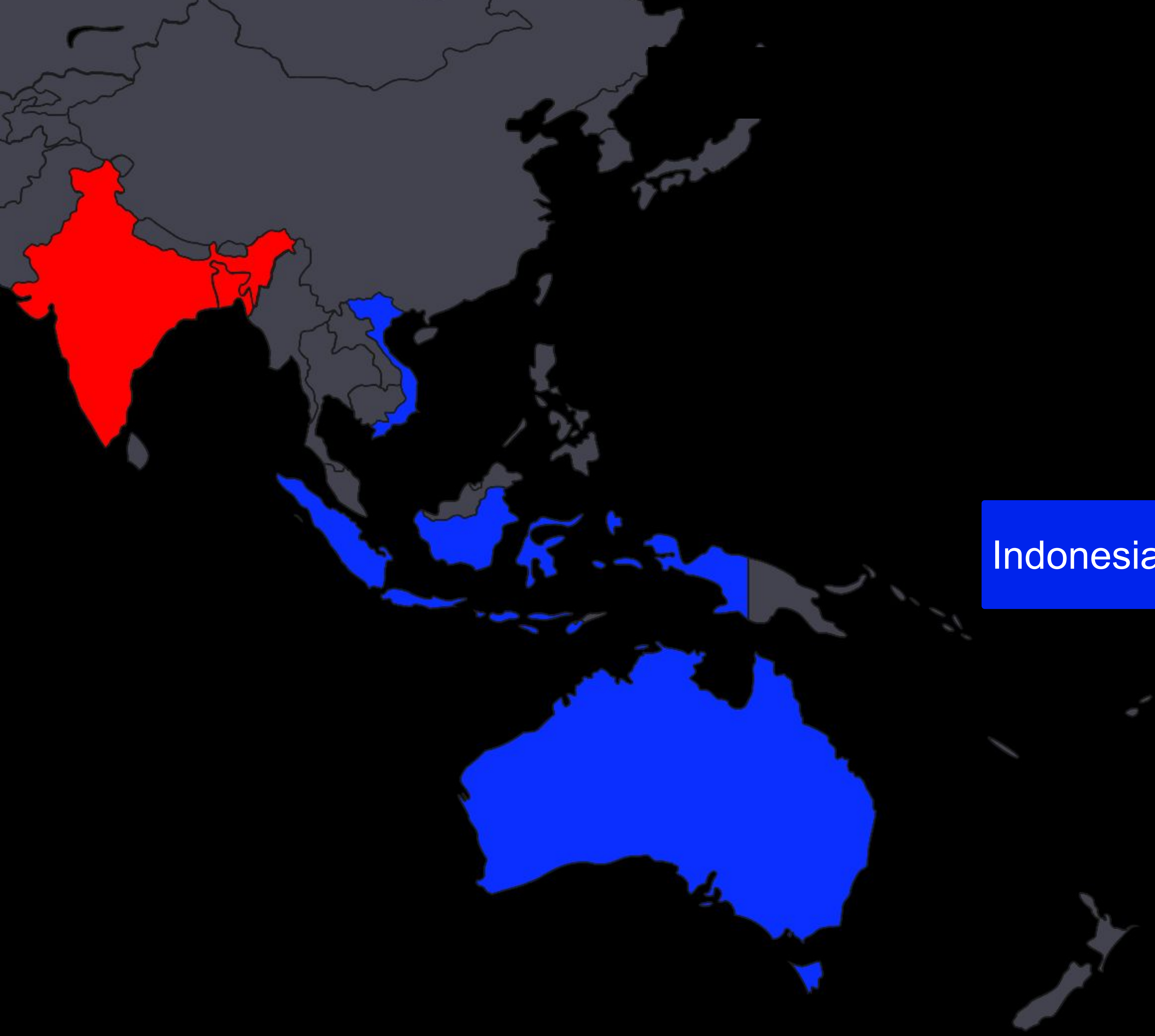
Hacktivism is the use of hacking to promote political or social agendas. Usually hacktivist groups are low-skill hackers who perform DDoS, Defacement, and Data Breaches (mostly leverages compromised accounts) attacks. Unfortunately, during the last year these groups attracted a lot of attention.

Below is a brief overview of groups that were active in the APAC region during the previous month, the threat landscape is very different from the previous month:

DDOS and Hacktivism Activities, per group



Data: number of events.



DDOS AND HACKTIVISM

Number of activities per Country, TOP 6 countries

↑ 42.34%

India, 59

Bangladesh, 23

Indonesia, 4

Vietnam, 3

Australia, 2

Data: number of events.

RANSOMWARE ACTIVITIES

↓ 38.56%

94 Ransom activities

Most active threat actors

Qilin

25 activities
+1150%

Sarcoma Ransomware

9 activities

Akira

8 activities
+14%

NightSpire

8 activities
-53%

BabukV2

7 activities
-84%

Most targeted Countries

Australia

16 activities
+14%

Singapore

14 activities
+75%

Taiwan

13 activities
-23%

India

12 activities
-54.5%

Japan

9 activities
-44%

Data: number of not unique events and activities (with updates).

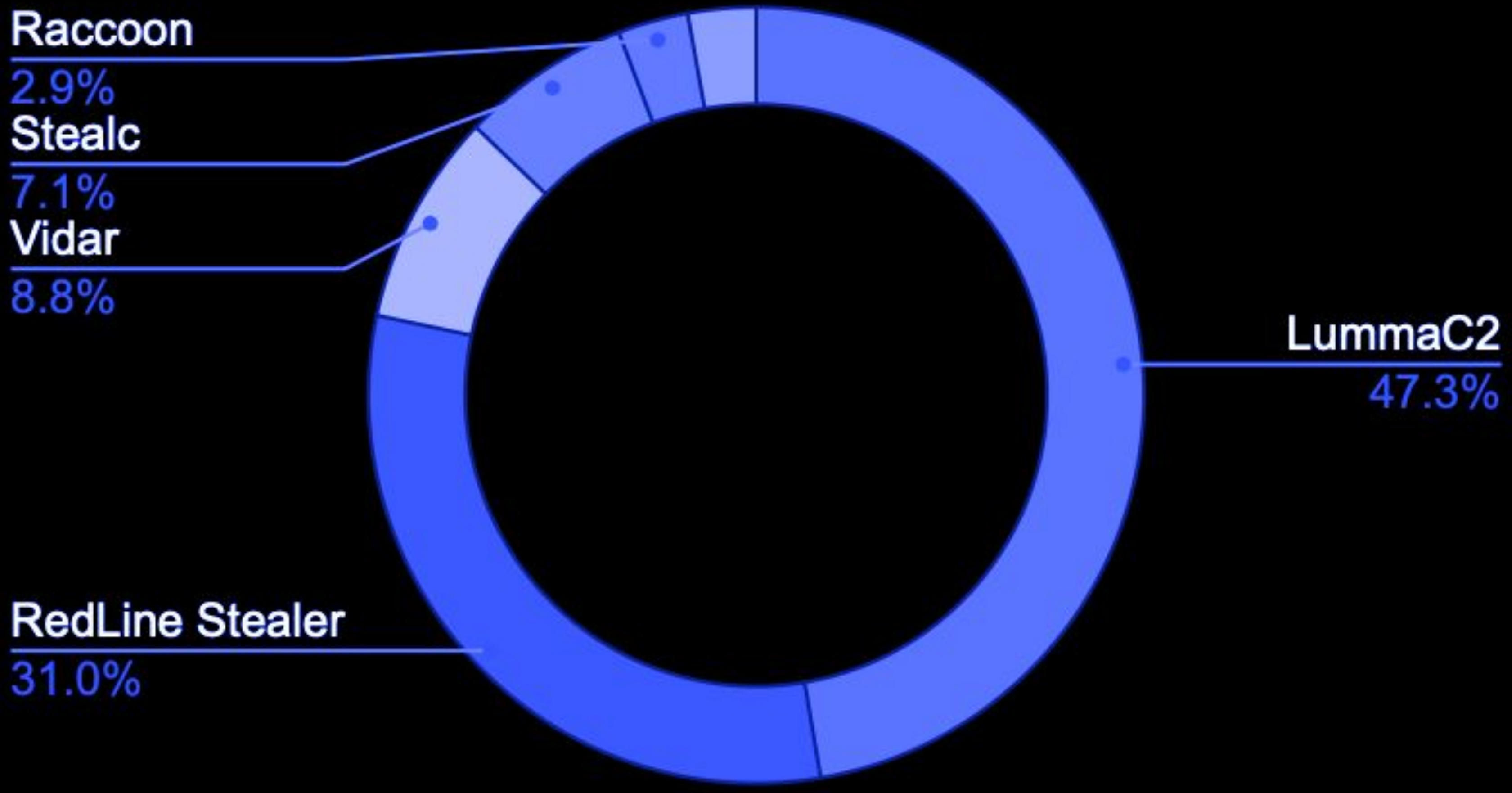
COMPROMISED DATA ↓ 311%

GROUP-IB

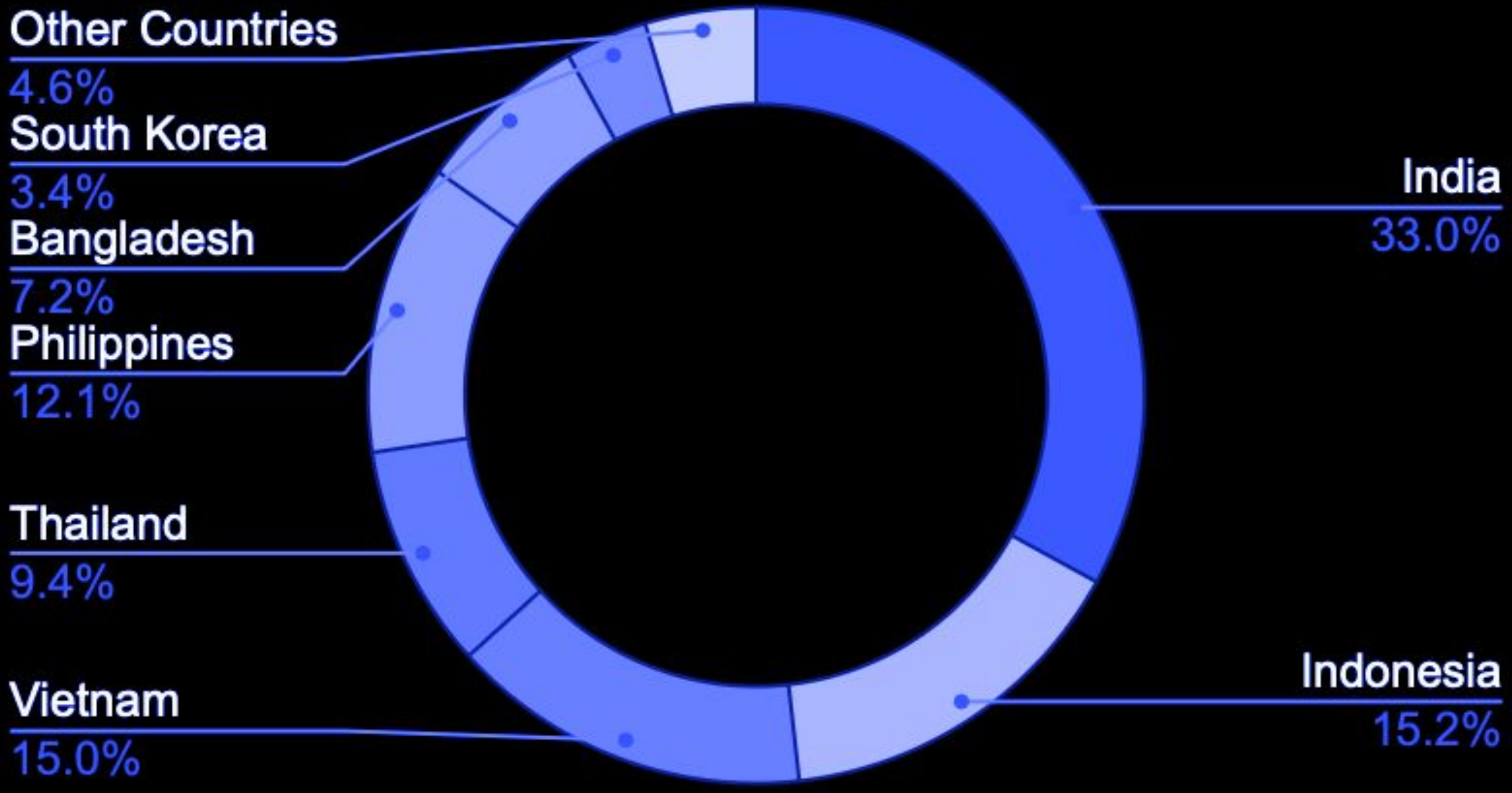
Statistics regarding compromised accounts in April 2025:

- Huge decline of the number of compromised data in APAC / ANZ compared to March 2025.
- India, Indonesia, Vietnam and Thailand - consistently high numbers of compromised data in previous months, as well as in April
- RedLine stealer, LummaC2 and Vidar - Most popular tools among others in APAC / ANZ.

Compromised Accounts by Malware



Compromised Accounts by Country



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

COMPROMISED BANK CARDS ↓ 17.4%

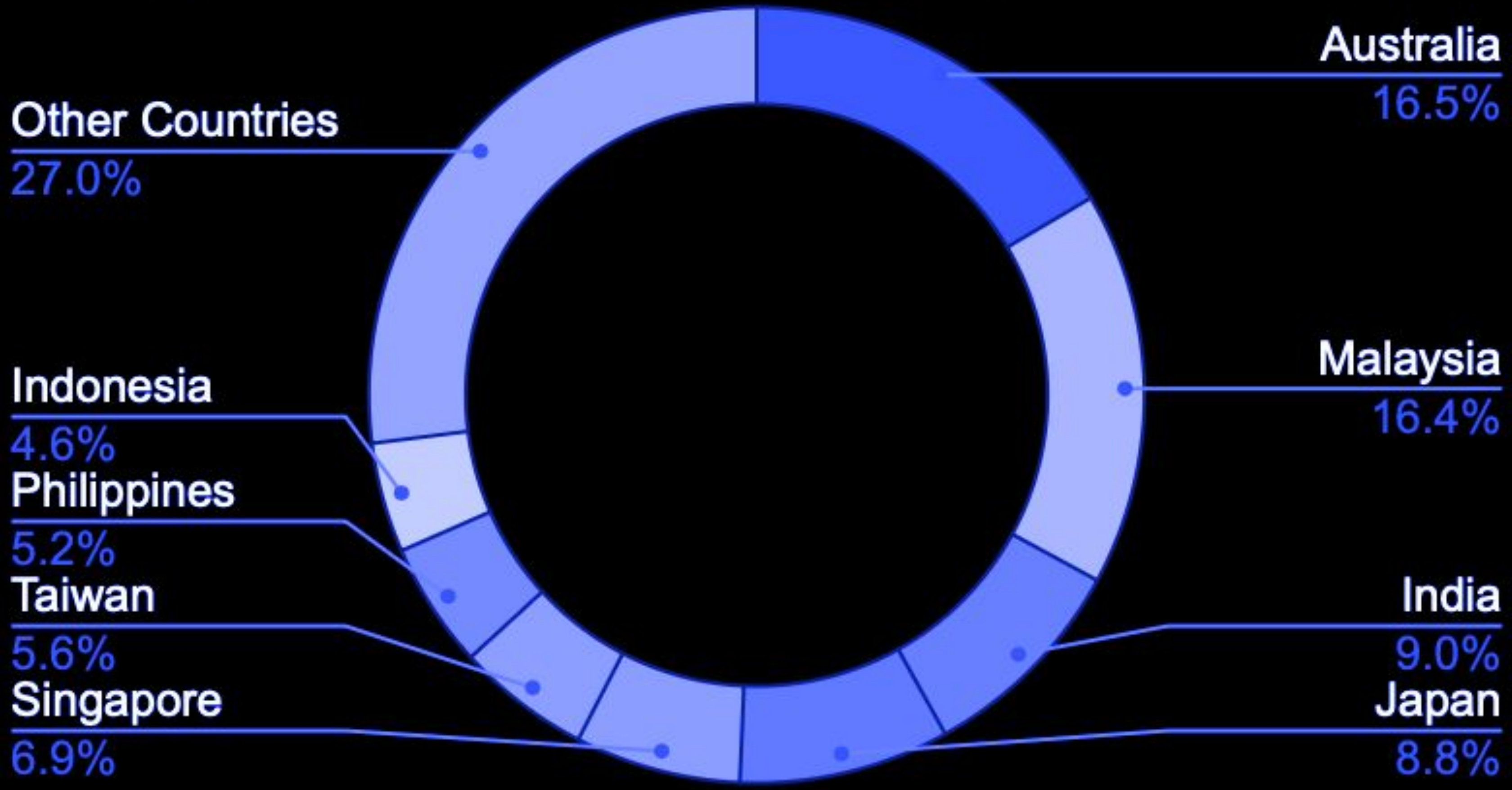
GROUP-IB

Statistics regarding compromised accounts.

Key Trends in April 2025:

- Further increase in the number of compromised bank cards in APAC and ANZ compared to February.
- 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.

HIGH TECH CRIME TRENDS REPORT

Download To Read Now

- https://www.group-ib.com/landing/high-tech-crime-trends-2025/

Get The Webinar High-Tech Crime Trends 2025 Deep Dive in APAC

- https://www.group-ib.com/resources/webinars/apac-high-crime-trends-report-2025-deep-dive/

CONCLUSIONS AND RECOMMENDATIONS

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

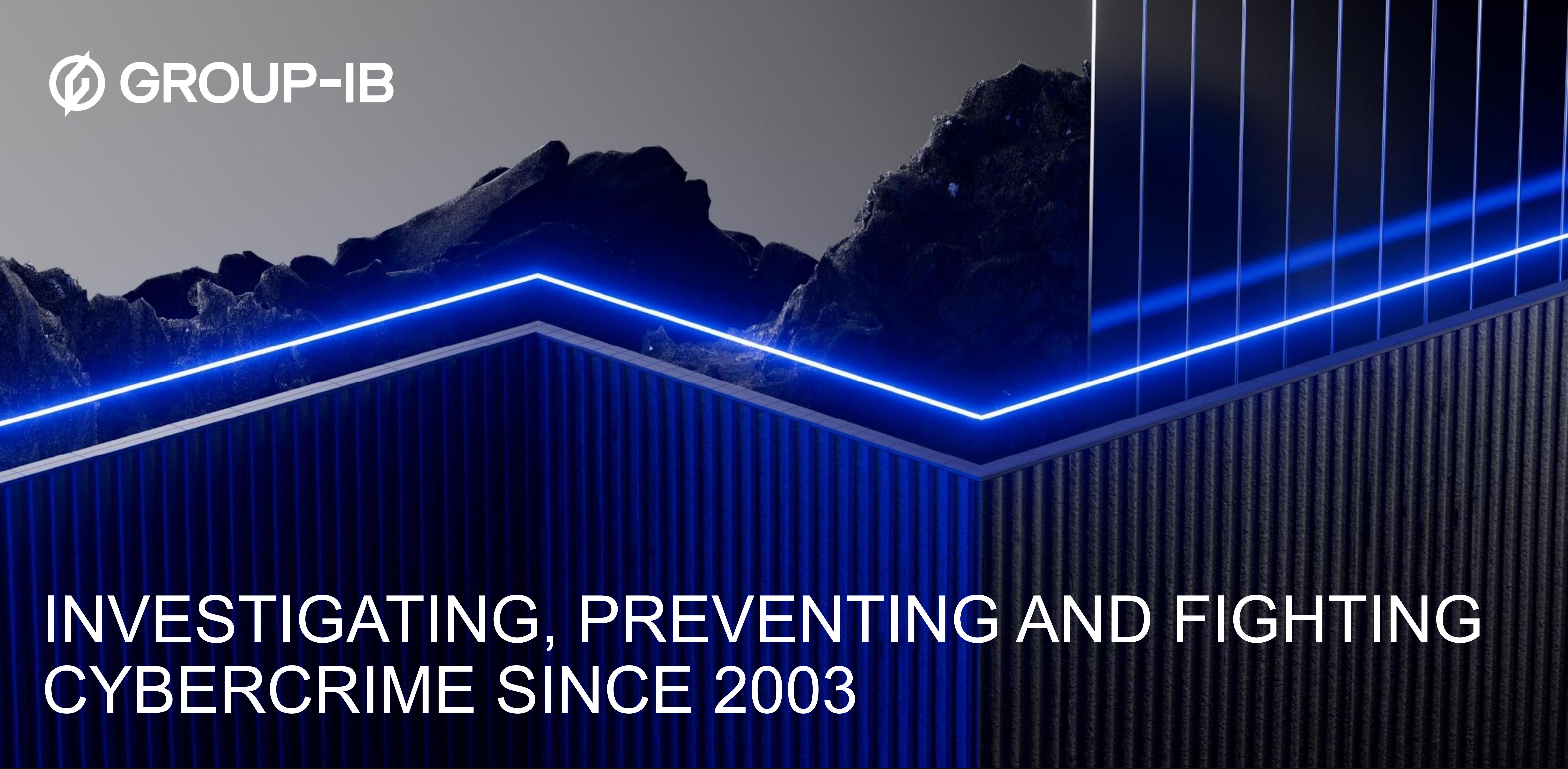
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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
+65 3159 3798

LINKEDIN FACEBOOK TWITTER INSTAGRAM