GROUP-IB

INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for March 2025

Report is based on data from 01.03.2025 till 01.04.2025

THREAT LANDSCAPE OVERVIEW

GROUP-IB

Ransomware activities

↑ 59.14%

DDoS and Hacktivism

↓ 44.76%

↑ 8.42%

Compromised Accounts

↑ 18.2%

Compromised Bank Cards

Data comparison: February 2025 - March 2025

GLOBAL INSIGHTS

GROUP-IB

Global Insights from Group-IB with a brief description:

01

ClickFix: The Social Engineering Technique Hackers Use to Manipulate Victims.

Discover how the ClickFix social engineering attack exploits human psychology to bypass security. Learn how hackers use this tactic and how to protect against it.

Since August 2024, the Group-IB Threat Intelligence (TI) team has researched and actively monitored the ClickFix technique in the wild. This technique has gained significant traction and widespread adoption among threat actors due to its surprising effectiveness. It is tracked by cybersecurity researchers and firms under the names ClickFix and ClearFix. More Information.

02

Unmasking the Classiscam in Central Asia

Scams like Classiscam automate fake websites to steal financial data, exploiting digitalization’s rise in developing countries, making fraud both effective and hard to detect.

Classiscam is an automated scam-as-a-service operation that uses Telegram bots to create fake websites mimicking legitimate services, deceiving victims into sharing their financial details.
In this blog, we dissect the inner working of the scam and its prevalence in Central Asia. More Information.

REGIONAL INSIGHTS

GROUP-IB

Regional Insights from Group-IB with a brief description:

01 Unknown TA targets Vietnamese entities with Sliver

Group-IB researchers have recently encountered several files that seemed to be launching a targeted attack on Vietnamese entities. We found 2 files that served as initial vectors. One file was named “list of courses” suggesting to target victims who are looking for career opportunities or courses. The other uses an acronym “VMK” - which we believe could refer to Vimarko Join Stock Company. We have also found out that the TA was likely targeting Vietnamese insurance Bảo hiểm Bảo Long.

02

The Cybercriminal with Four Faces: Revealing Group-IB's Investigation into ALTDOS, DESORDEN, GHOSTR and 0mid16B

Following the arrest of the cybercriminal behind the aliases ALTDOS, DESORDEN, GHOSTR, and 0mid16B, Group-IB provides a deep dive into his activities, uncovering striking similarities and unmasking the cybercriminal that breached more than 90 instances of data leaks worldwide over the span of four years in operation. More Information.

03

Possible Qilin Ransomware attack on Malaysia Airports Holdings Berhad

On March 23, 2025, at approximately 03:00 local time, Kuala Lumpur International Airport (KLIA1 and KLIA2) suffered a critical digital system outage that lasted more than 10 hours, disrupting:

- Flight Information Display Systems (FIDS)
- Passenger check-in processes
- Baggage handling systems
- Operational coordination

Considering the nature of the threat described and also the ransom demanded, experts associate this attack with an attack by ransomware.

04

In March 15, 2025, Satisfie from breachforums put up for sale dataset with 662 millions lines of patient health records from the Health Data Center of the Ministry of Public Health (MOPH) in Thailand.

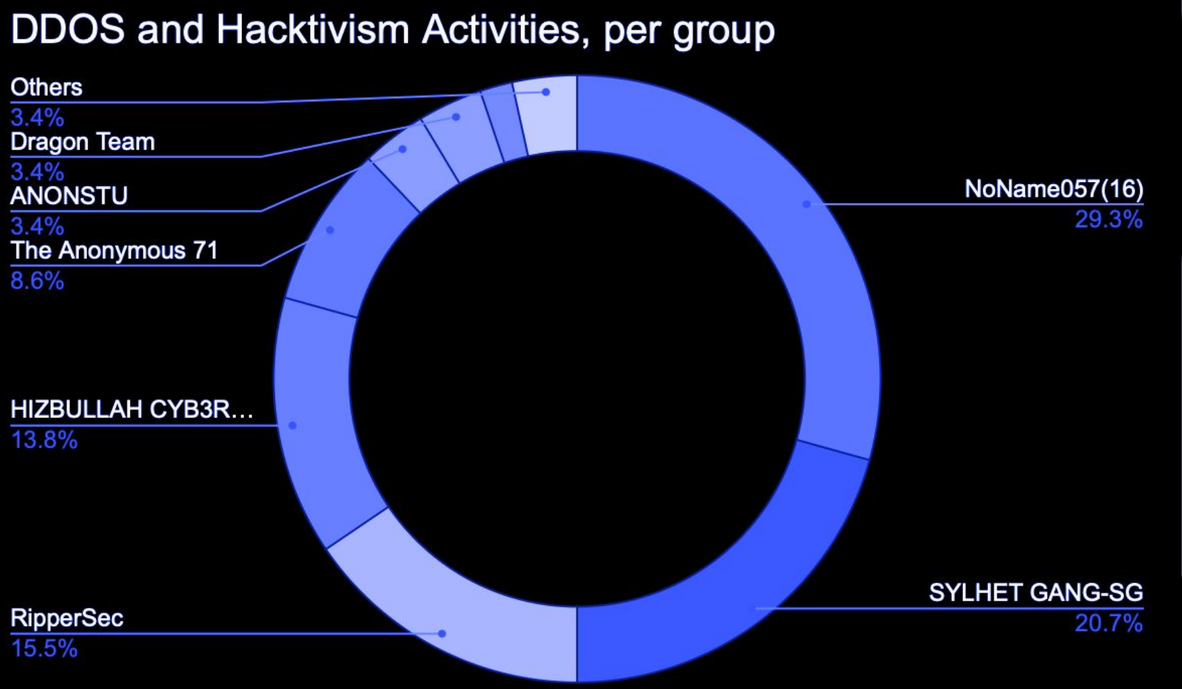
APAC and ANZ

More Information in Group-IB Threat Intelligence Portal

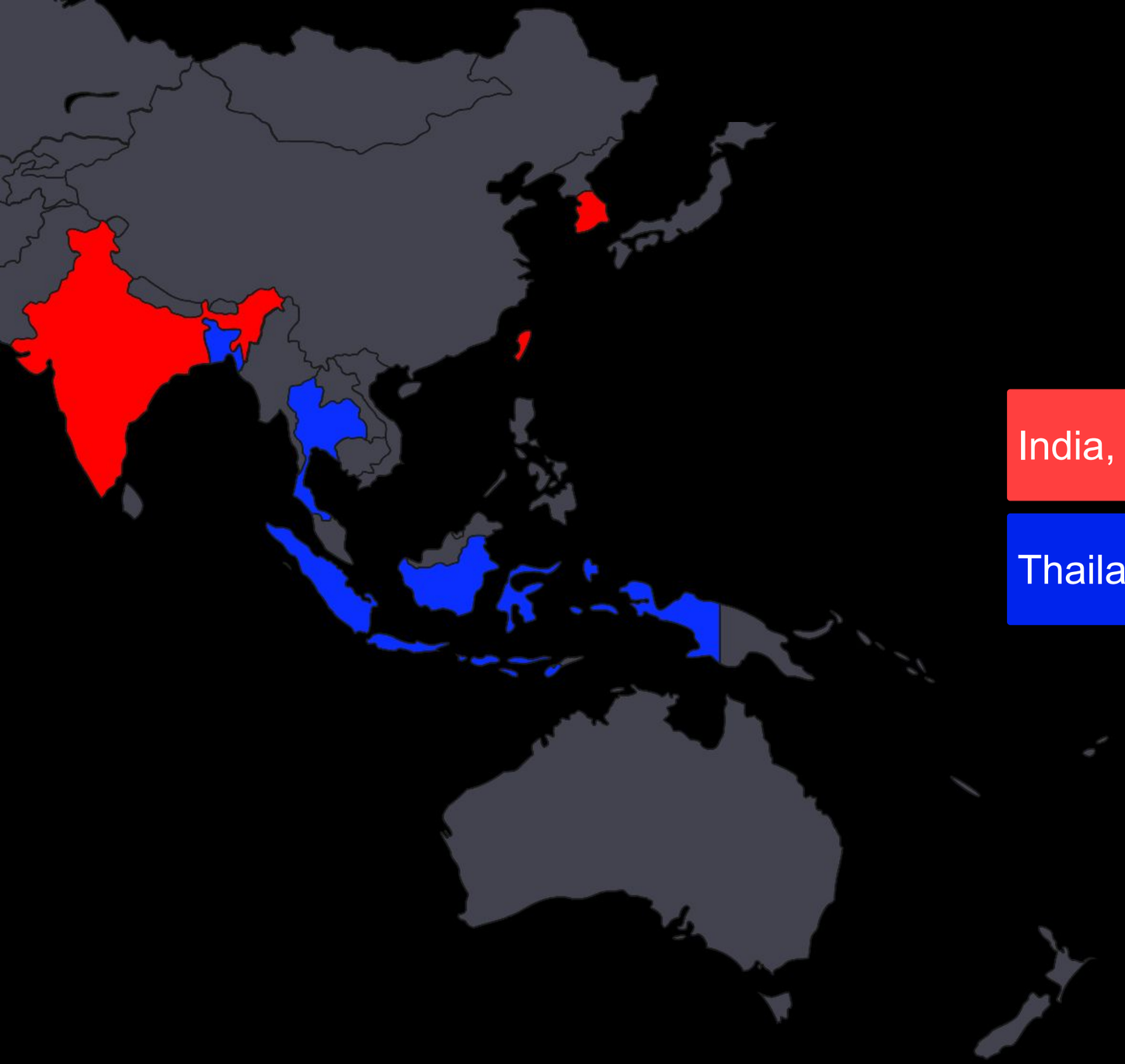
DDOS AND HACKTIVISM

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:



Data: number of events.



DDOS AND HACKTIVISM

Number of activities per Country, TOP 6 countries

↓ 44.76%

India, 27	Taiwan, 17	South Korea, 5
Thailand, 4	Indonesia, 3	Bangladesh, 2

Data: number of events.

RANSOMWARE ACTIVITIES

↑ 59.14%

148 Ransom activities

Most active threat actors

BabukV2

42 activities

RansomHub

21 activities
+200%

NightSpire

17 activities

Hunters International

11 activities
+266%

Akira and KillSec

7 activities each

Most targeted Countries

India

25 activities
+4.17%

Taiwan

17 activities
+88%

China

15 activities
+400%

Australia

14 activities
–12.5%

Japan

14 activities
+40%

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

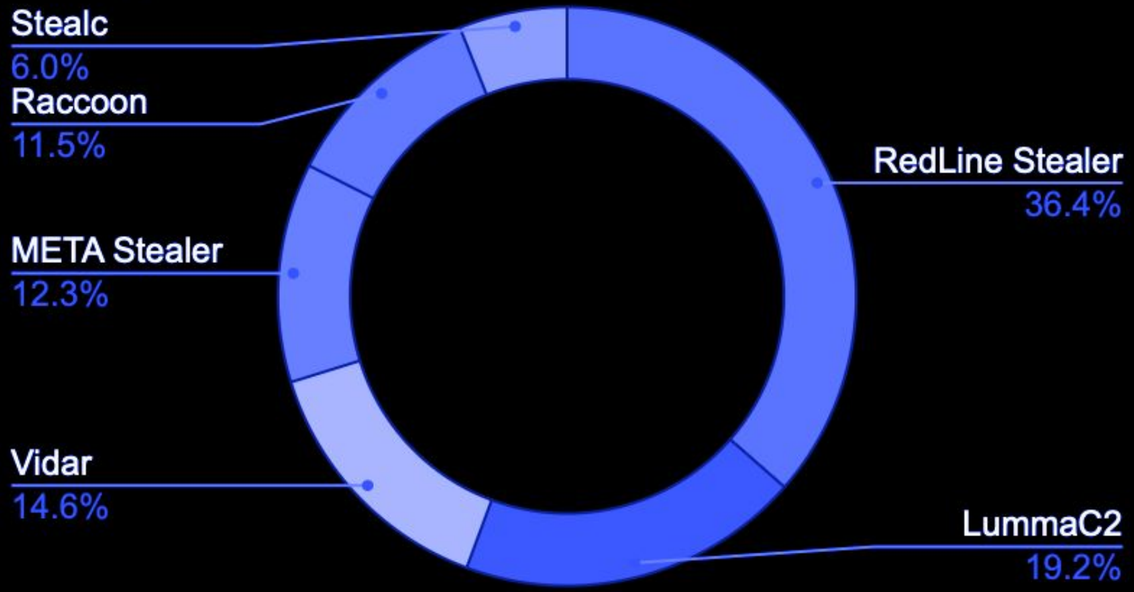
COMPROMISED DATA ↑ 8.42%

GROUP-IB

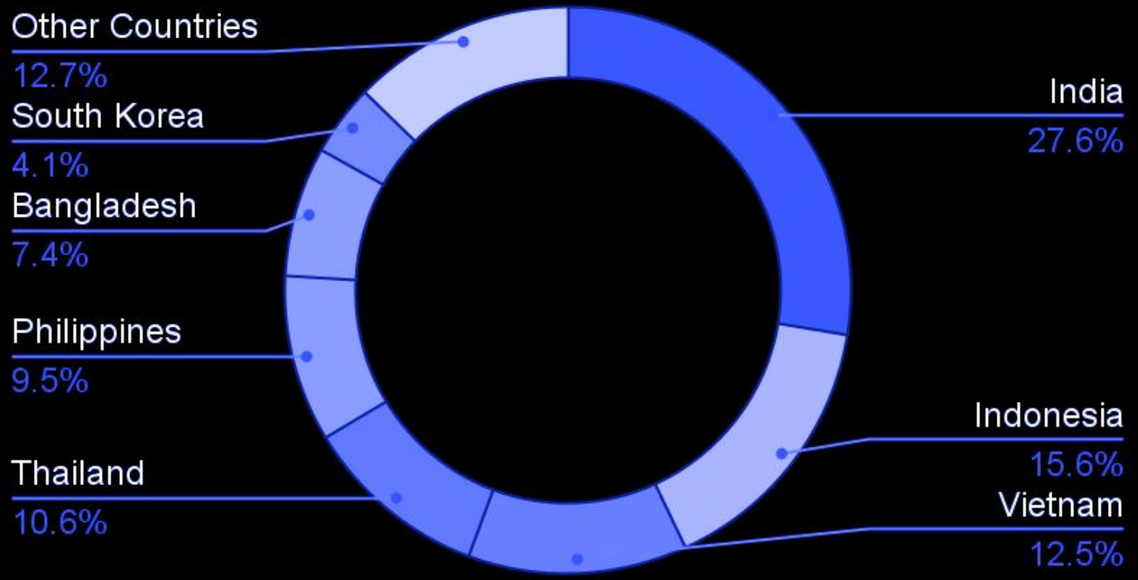
Statistics regarding compromised accounts in March 2025:

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

Compromised Accounts by Malware



Compromised Accounts by Country



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

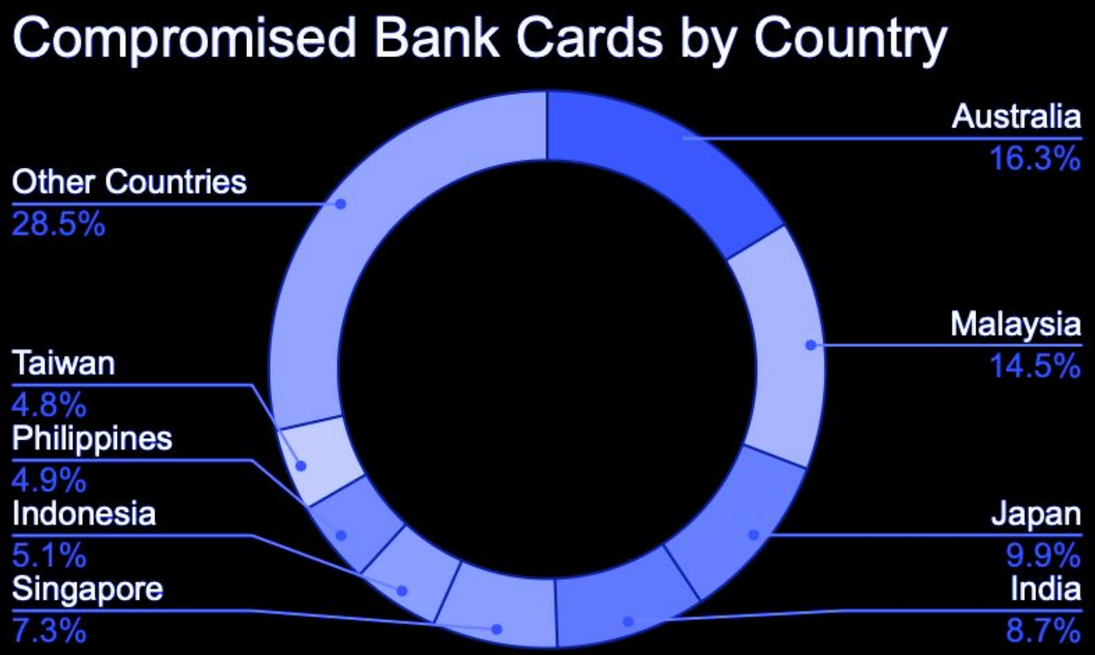
COMPROMISED BANK CARDS ↑ 18.2%

GROUP-IB

Statistics regarding compromised accounts.

Key Trends in March 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.



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

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

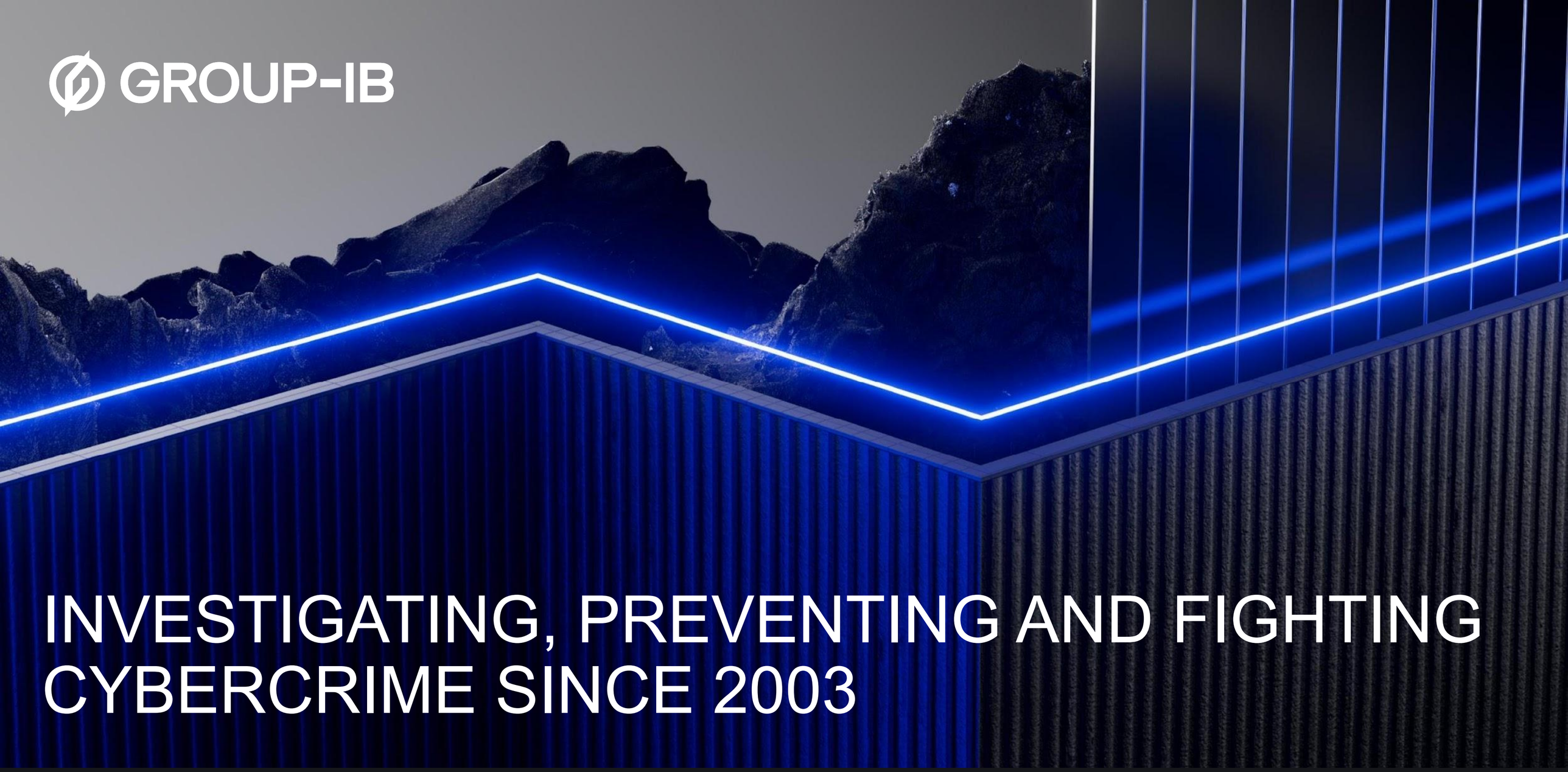
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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.



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