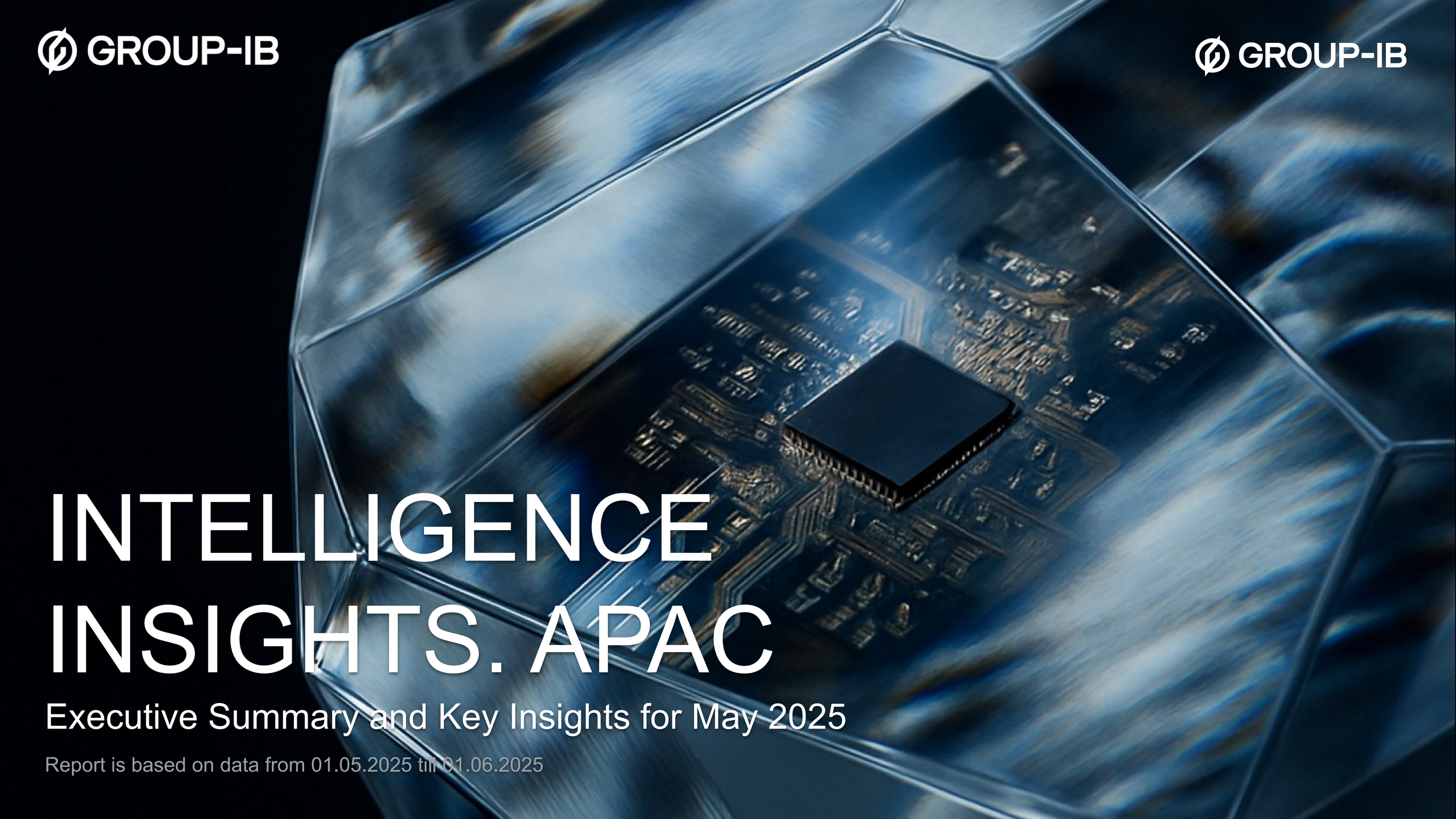
GROUP-IB

GROUP-IB



INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for May 2025

Report is based on data from 01.05.2025 till 01.06.2025

THREAT LANDSCAPE OVERVIEW

GROUP-IB

Ransomware activities

↓ 19.15%

DDoS and Hacktivism

↑ 162.29%

↑ 41.96%

Compromised Accounts

↑ 62.43%

Compromised Bank Cards

Data comparison: April 2025 - May 2025

GLOBAL INSIGHTS

GROUP-IB

Global Insights from Group-IB with a brief description:

01

Understanding Credential Harvesting via PAM: A Real-World Threat

When PAM is compromised, it can be altered to capture and store authentication credentials. These credentials can later be exfiltrated to a C2 server or manually retrieved by a threat actor. The analysis also shares how easily PAM can be compromised to harvest credentials, how to detect and respond to such attacks and the benefits of key-based SSH authentication. More Information.

02

Disguised Cyber Risks On The Colombian Shore: The Insurance Trap

Learn about the techniques cybercriminals in Colombia use to impersonate financial brands and exploit public data for vehicle insurance scams. These scams validate insurance status and show accurate car details to gain trust. Victims are lured through social media, then redirected to phishing pages or QR payment traps, and have money stolen once enter their financial info. More Information.

03

Zero-Day vulnerability for SS7 Gateway offered for sale

On May 4, 2025, a threat actor "Eternal" advertised a zero-day SQL injection vulnerability targeting an SS7 gateway on DarkForums, allowing database access and remote code execution. The same exploit was listed on BreachForums by "ViralGod," with both aliases sharing the same TOX ID, suggesting they belong to the same individual, and the exploit is being sold for $5,000. More Information.

04

Phishing campaign leveraging FakeOkta.Alpha kit - May 2025 (Alpha cluster)

Group-IB specialists discovered a new phishing campaign targeting Okta users. Based on the analysis of the phishing kit, domain registration patterns, hosting infrastructure, targeted companies, and regions, we assess with moderate confidence that this activity is associated with a sub-cluster of Scattered Spider. More Information.

05

Sale of database allegedly related to Workday

On May 9, 2025, the Telegram channel “Satanic Cloud,” run by the actor Satanic TA, claimed to have breached and obtained database allegedly from Workday, containing over 3 million user records. While the full database is restricted to paid subscribers, shared samples appear to be authentic based on overlaps with real individuals and data fields. More Information.

REGIONAL INSIGHTS

GROUP-IB

Regional Insights from Group-IB with a brief description:

01

Casino Spam Campaign Targets Over 250 Websites

Group-IB researchers uncovered over 250 WordPress legitimate looking websites compromised by a SEO spam campaign. Compromised websites have been used to inject frames promoting gambling content in a black-seo campaign active since at least 2021 until June 2025, targeting users in Spain, Poland, Australia, France, Switzerland, India, Denmark, Brazil, Netherlands, Colombia, Italy, Mexico, Vietnam, Iran, Portugal, Singapore, etc. While the technique used in this campaign is not new, the scale, and consistent use of framesets show that it remains a highly effective and actively evolving threat. More Information.

02

Exposing the AI Trading Scam: Tactics, Techniques, and Infrastructure

From our real examples and internal investigations, learn about scammers in AI trading platforms, whose schemes look so convincing that even experienced investors may not spot the deception right away. Fraudsters take advantage of people's trust in AI by creating fake AI-generated videos, fake reviews, and misleading ads to share through social media, video platforms, and low-quality blogs. Sometimes, these schemes look so convincing that even experienced investors may not spot the deception right away. More Information.

03

Recent malicious activities of BL4CK CYB3R

BL4CK CYB3R, a pro-Cambodian hacktivist group active on Telegram, claimed to engage in several DDoS attacks, Defacements, Data leaks and sales, Unauthorized access targeting government and organizations in various countries, including Vietnam, Thailand, Russia, Indonesia, India, Iraq, Pakistan, Israel, USA. Information on each attack has been updated and summarized, however, it is based on statements made by alleged threat actors and should be independently verified. More Information.

04

Sale of Personal Documents of Australian Citizens

On May 19, 2025, an actor using the alias bulkpalace advertised personal documents of Australian citizens on the XSS forum, later claiming to offer 39 full ID packages and an additional 21,000 records in a follow-up post. While no samples were publicly shared, the data sources were partially revealed in private conversations and further analyzed by Group-IB. More Information

APAC and ANZ

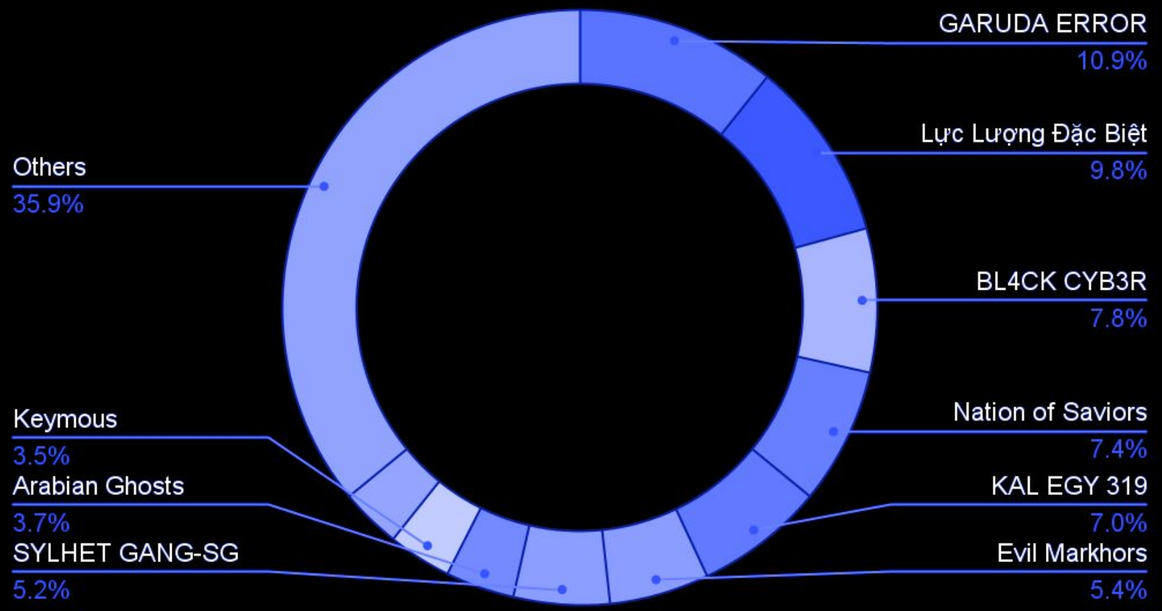
More Information in Group-IB Threat Intelligence Portal

DDOS AND HACKTIVISM

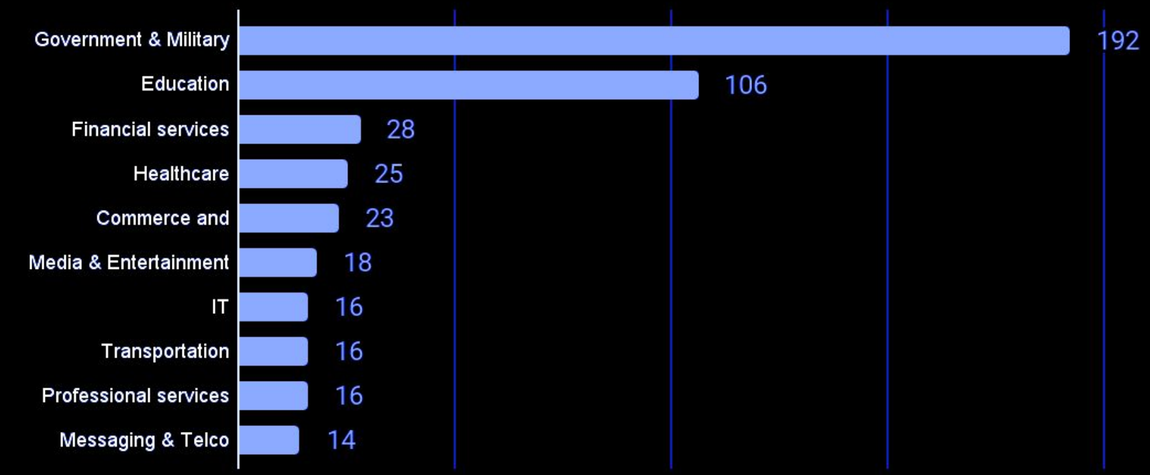
GROUP-IB

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 and ANZ regions during the previous month, the threat landscape is very different from the previous month, along with the top 10 targeted sectors in May 2025:

DDOS and Hacktivism Activities, per group

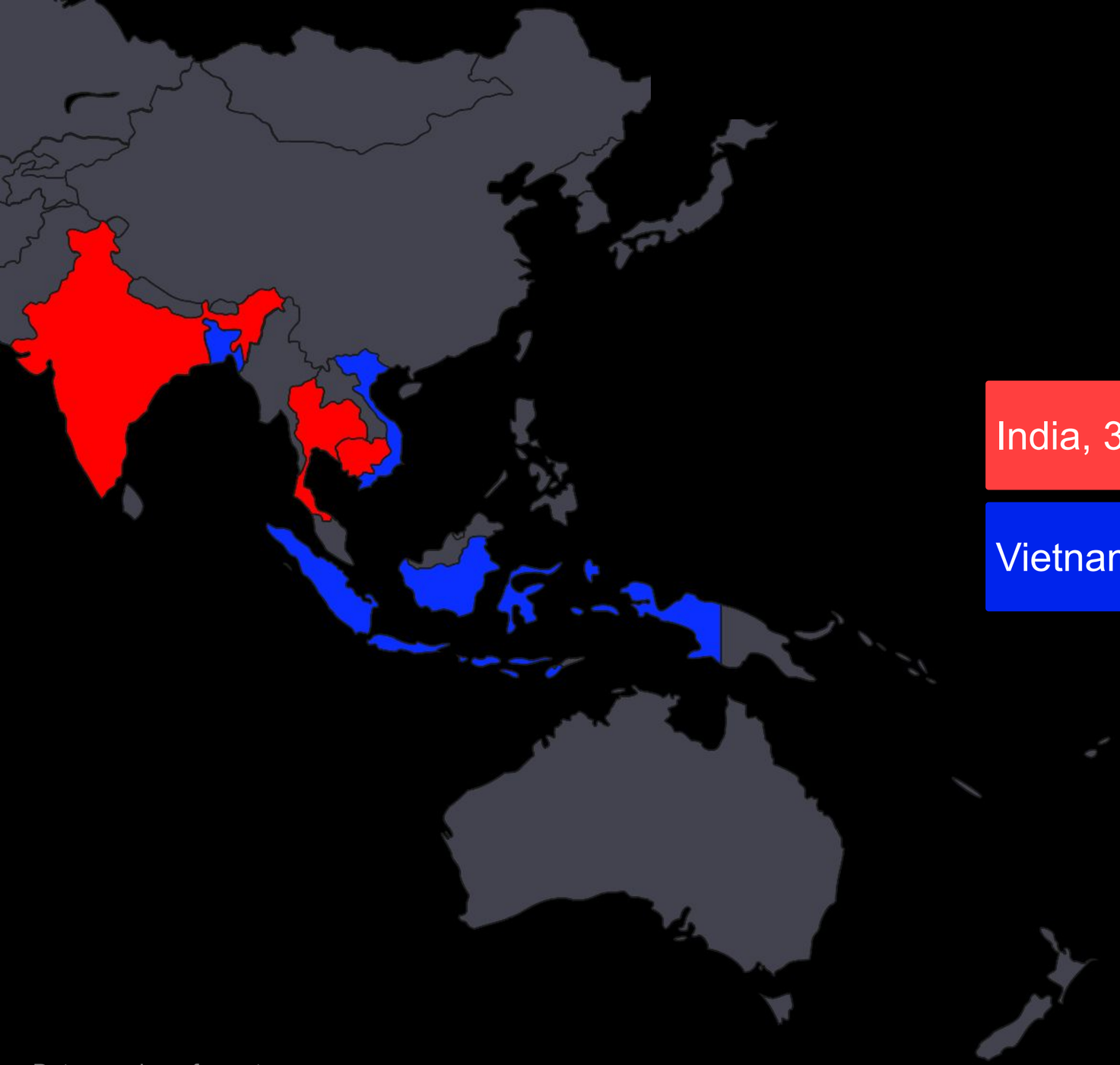


DDOS and Hacktivism Activities, per industry



Top 10 targeted sectors, May 2025

Data: number of events.



DDOS AND HACKTIVISM

Number of activities per Country, TOP 6 countries

↑ 162.29%

India, 314	Cambodia, 41	Thailand, 34
Vietnam, 29	Indonesia, 20	Bangladesh, 19

Data: number of events.

RANSOMWARE ACTIVITIES ↓ 19.15%

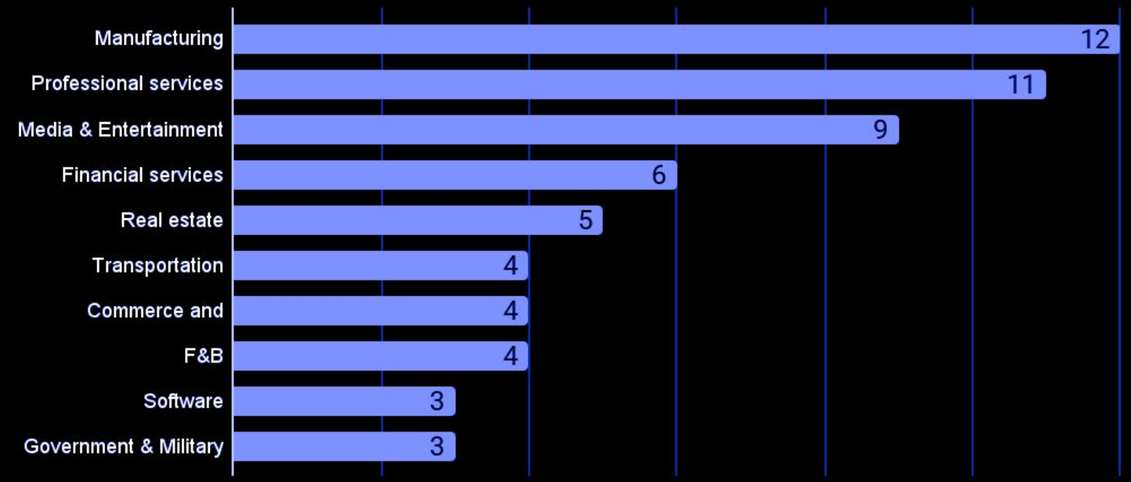
GROUP-IB

76 ransomware incidents

Statistics regarding ransomware activities in May 2025:

- Devman and Qilin still had various attacks targeting different countries, especially APAC region.
- Activities associated with the new group, J group, continued to rise throughout the past 2 months.
- Activities associated with Rhysia and Direwolf were detected again during May 2025.

Ransomware attacks, per industry



Top 10 targeted sectors, May 2025

Most active threat actors

Devman
9 activities
+200%

Qilin
8 activities
-68%

Direwolf
6 activities

Rhysida
6 activities

J group
5 activities
+150%

Most targeted Countries

Australia
18 activities
+12.50%

Japan
10 activities
+11.11%

Singapore
9 activities
–35.71%

Malaysia
7 activities
-22.22%

Taiwan
6 activities
–53.85%

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

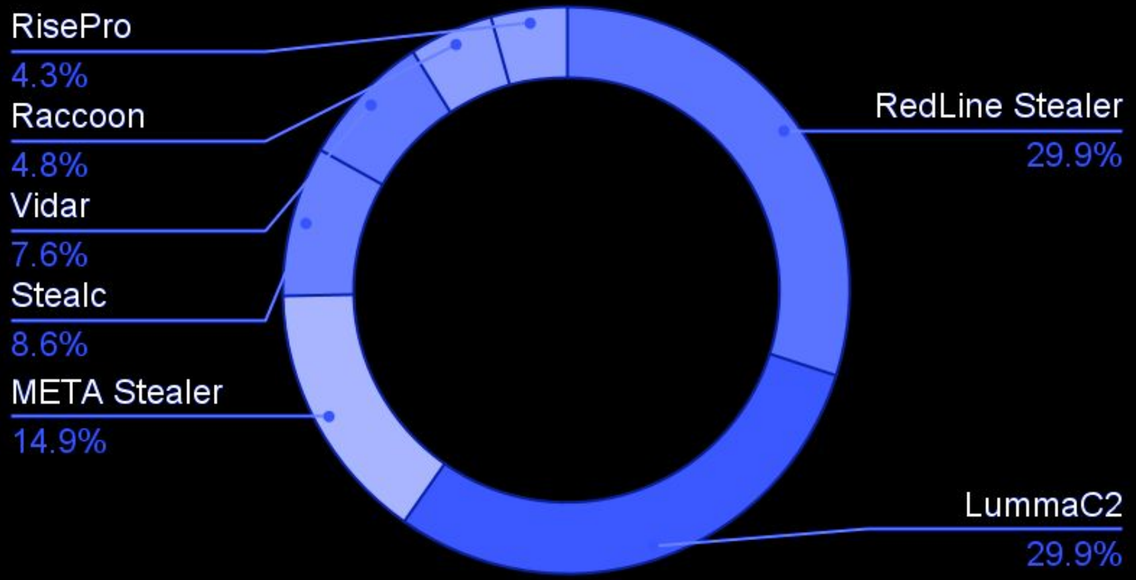
COMPROMISED DATA ↑ 41.96%

GROUP-IB

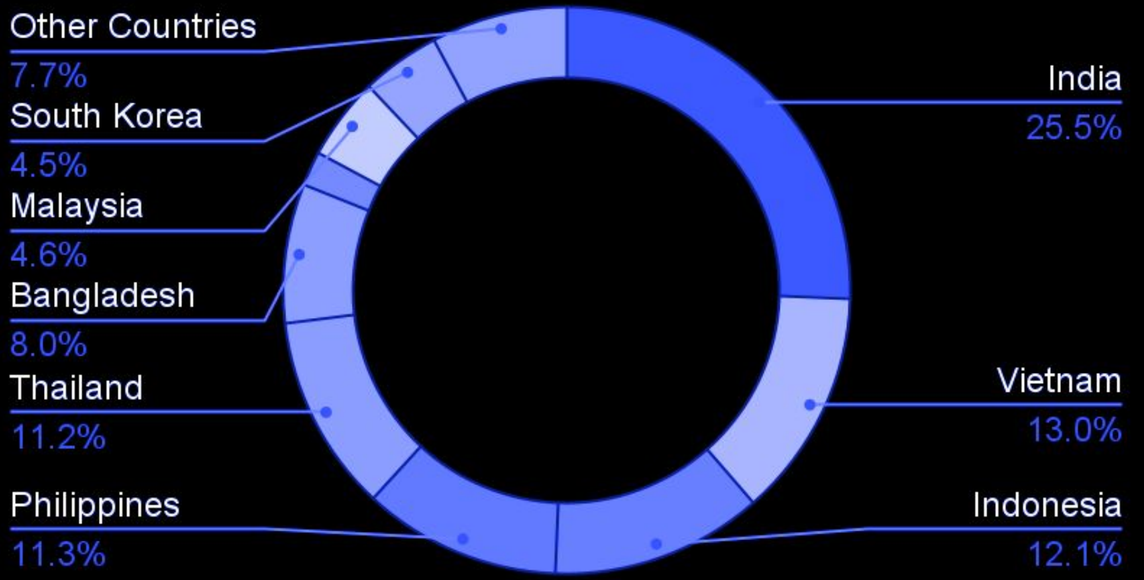
Statistics regarding compromised accounts in May 2025:

- Despite having a significant plunge between March and April, the compromised data in May started to see a notable increase, implying that technical controls and security hygiene should be strengthened, along with enhancing monitoring by subscribing to threat intel feeds.
- India, Indonesia, Vietnam and Thailand continue to have the highest numbers of compromised data since the beginning of 2025.
- RedLine stealer, LummaC2 are still the most popular tools among others in APAC / ANZ. META Stealer also has a surge in usage this month by increasing at 92.41% compared to April 2025.

Compromised Accounts by Malware



Compromised Accounts by Country



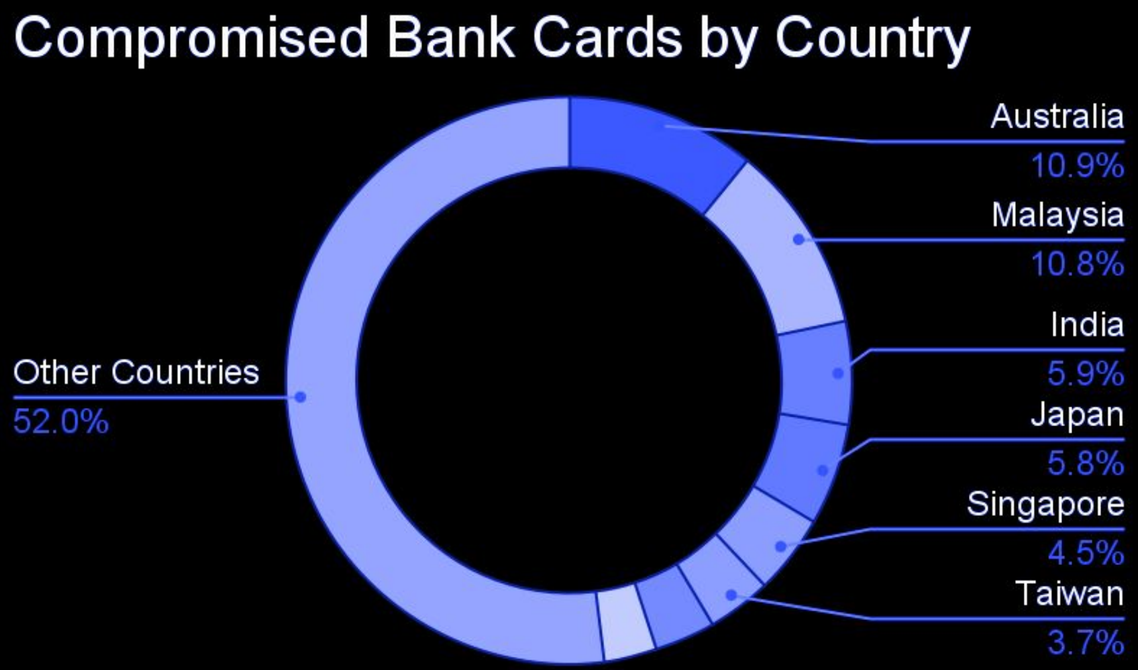
Data: number of events. Each malware can be part of the same event.

COMPROMISED BANK CARDS ↑ 62.43%

GROUP-IB

Statistics regarding compromised accounts in May 2025:

- The number of compromised bank cards in APAC and ANZ continued to increase significantly since March 2025, with statistics in Australia and Malaysia are 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.

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

Devman

Targeted industries:

Manufacturing
Construction
Healthcare
Information technology
Human resources services
E-commerce
Financial services
Consumer goods
Government and Military
Telecommunications
Hospital
Pharmaceutical
Media and entertainment
Environmental consulting
Transportation

Period of Activity:	April 2025 - Present
Targeted countries:	Worldwide (APAC & ANZ: Singapore, Thailand, China, Japan, Philippines, Taiwan, Vietnam, etc.)
Attribution:	N/A
Intent:	Financially motivated

Attack Summary

Devman is a ransomware operator discovered in April 2025. Devman has been identified as an affiliate of the Qilin ransomware group. However, recent activity indicates that this threat actor is pursuing independent operations. Devman has launched his own Data Leak Site (DLS), where he publishes details about his victims and provides commentary on the methods used during the intrusions.

Key Observations

- The threat actor exploits the EternalBlue vulnerability using Metasploit's msfconsole to gain access to the victim’s environment.
- The threat actor used PowerShell commands and custom scripts to collect files, and leveraging valid credentials and Mimikatz for credential dumping.

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

BL4CK CYB3R

Targeted industries:

- Government and military
- Financial services
- Transportation
- Information technology
- Education

Period of Activity:	March 2025 - Present
Targeted countries:	Worldwide (APAC & ANZ: Vietnam, Indonesia, Russia, Thailand, India, Pakistan, etc.)
Attribution:	Cambodia
Intent:	N/A

Attack Summary

BL4CK CYB3R is a pro-Cambodian hacktivist group active on the Telegram channel since March 2025. Since then, this hacktivist group claims to engage in several attacks targeting various countries.

Key Observations

The group does not limit itself to specific industries but appears to prioritize in government websites/agencies and financial institutions.

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

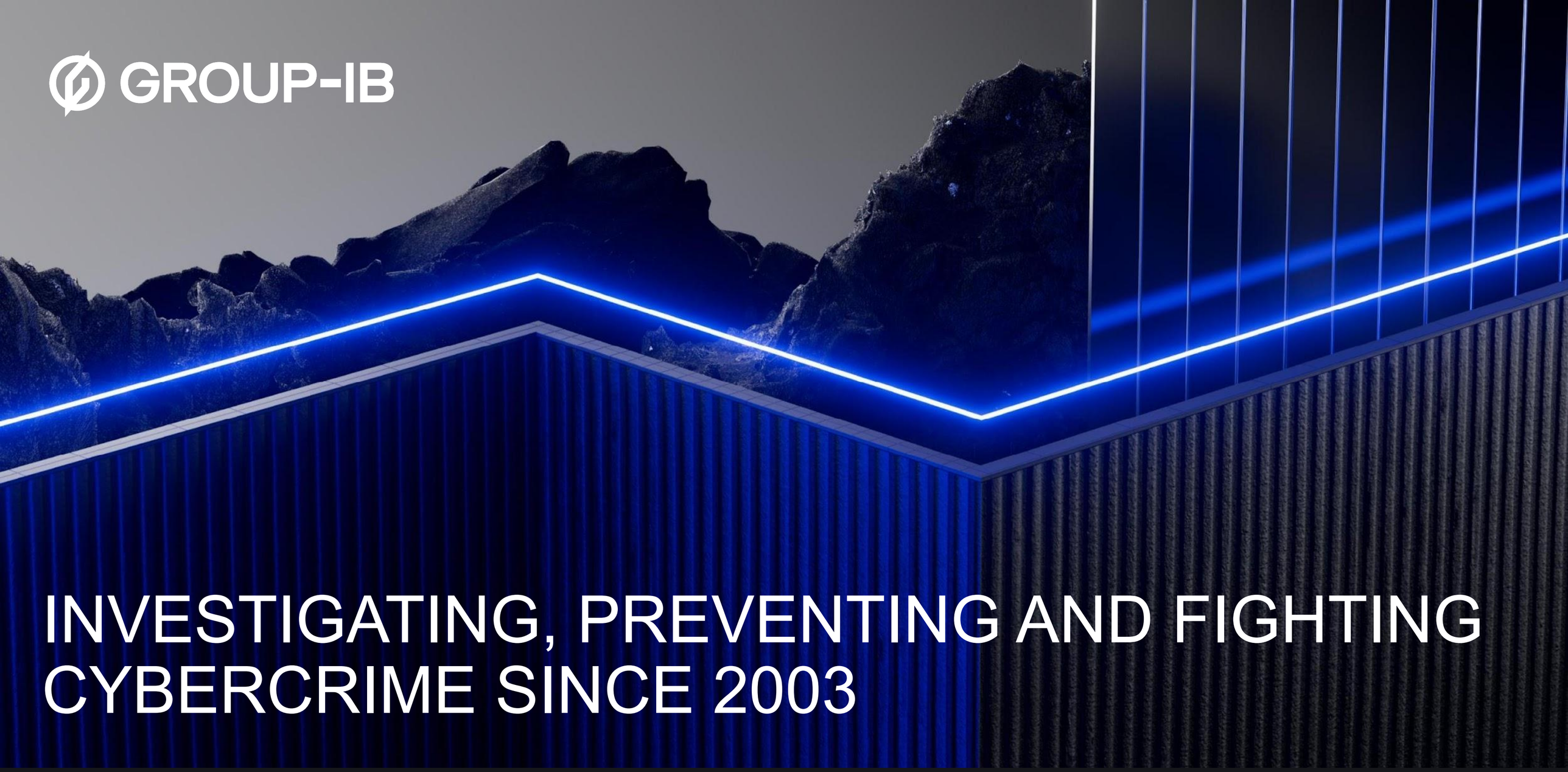
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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