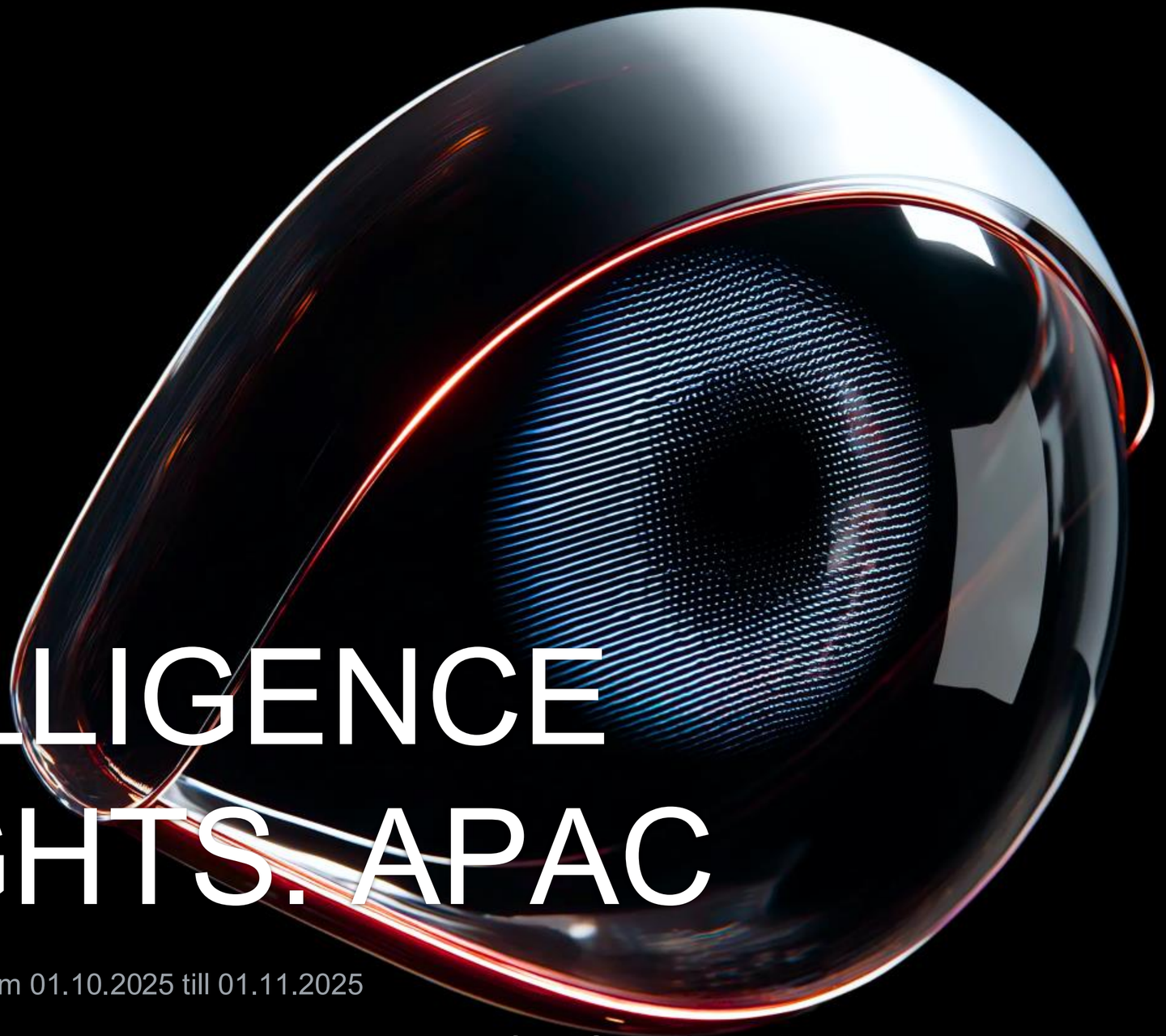
GROUP-IB



INTELLIGENCE INSIGHTS: APAC

Report is based on data from 01.10.2025 till 01.11.2025

Executive Summary and Key Insights for October 2025

THREAT LANDSCAPE OVERVIEW - APAC

GROUP-IB

Ransomware activities

↓ 2.7%

DDoS and Hacktivism

↓ 32.8%

↓ 55.5%

Compromised Accounts

↓ 56.1%

Compromised Bank Cards

Data comparison: September 2025

GLOBAL INSIGHTS

Global Insights from Group-IB with a brief description:

01

Nation State Actor UNC5221 Compromised F5's Internal Network

In August 2025, F5, a leading cybersecurity and application delivery company, detected unauthorized access to its internal systems by a highly sophisticated nation-state threat actor. The intrusion, which involved persistent access and file downloads, targeted the BIG-IP product development environment and engineering knowledge management platforms. This incident underscores ongoing challenges in securing software supply chains, with no immediate operational disruptions reported by F5. More Information.

02

Red Hat breach: Crimson Collective advertises the data for sale

October 13, 2025: Despite the initial 2025-10-10 deadline of the Red Hat breach, the full data has not been publicized at the time of writing, and Crimson Collective posted a message advertising the data for sale, priced at $400,000 – $500,000. The DLS (shinyhunte[.]rs) listing of Red Hat remains marked “active”, and not “leaked”, with the same deadline and no additional samples posted. More Information.

03

Dozens of websites, banks and apps are being affected by a major Amazon Web Services outage

A major Amazon Web Services (AWS) outage on October 20, 2025, caused widespread disruption to many websites, apps, and banking services globally. The outage was triggered by a technical update to a key database service that led to Domain Name System (DNS) errors, making it impossible for many platforms to be reached. More Information.

04

Inside the Brazilian WhatsApp Trojan Surge: Self-Spreading Malware Targets Banking Users

A malware campaign was recently detected in Brazil, distributing a malicious LNK file using WhatsApp. It targets mainly Brazilians and uses Portuguese-named URLs. To evade detection, the command-and-control (C2) server verifies each download to ensure it originates from the malware itself. More Information.

REGIONAL INSIGHTS

Regional Insights from Group-IB with a brief description:

01

Database Sale. Pruksa Real Estate Public Company Limited, Thailand (Pruksa.com)

On October 30, 2025, a threat actor with the nickname AgSlowly from the Darkforums forum created a thread announcing the sale of data allegedly belonging to hxxp://pruksa[.]com (Pruksa Real Estate Public Company Limited, a real estate development company in Thailand). More Information.

02

Leaked source code from SkoolBeep

On October 30, 2025, in a continued serious of source code exfiltration, a threat actor with the nickname 888 leaked sourced code claimed to be related to SkoolBeep, an India-based school management and parent-communication platform (hxxps://www[.]skoolbeep[.]com).More Information.

03

Crypto24 Ransomware attack on Bayu Buana Travel Services

On 2025-10-27, the ransomware group Crypto24 claimed responsibility for an attack targeting Bayu Buana Travel Services. The incident was disclosed through a post on the group's leak site (DLS), where the threat actors allegedly published evidence of the breach and threatened to release sensitive data if their demands were not met. More Information.

04

Leak of SQL Database of Islamic Banking & Finance Institute Malaysia (IBFIM, ibfimonline.com)

On October 25, 2025, in the private Telegram channel "Goldpack", belonging to the well-known threat actor Chucky\Leakbase, a SQL database of the Islamic Banking & Finance Institute Malaysia (IBFIM, ibfimonline[.]com) was published. More Information

APAC and ANZ

More Information in Group-IB Threat Intelligence Portal

RANSOMWARE ACTIVITIES (APAC)

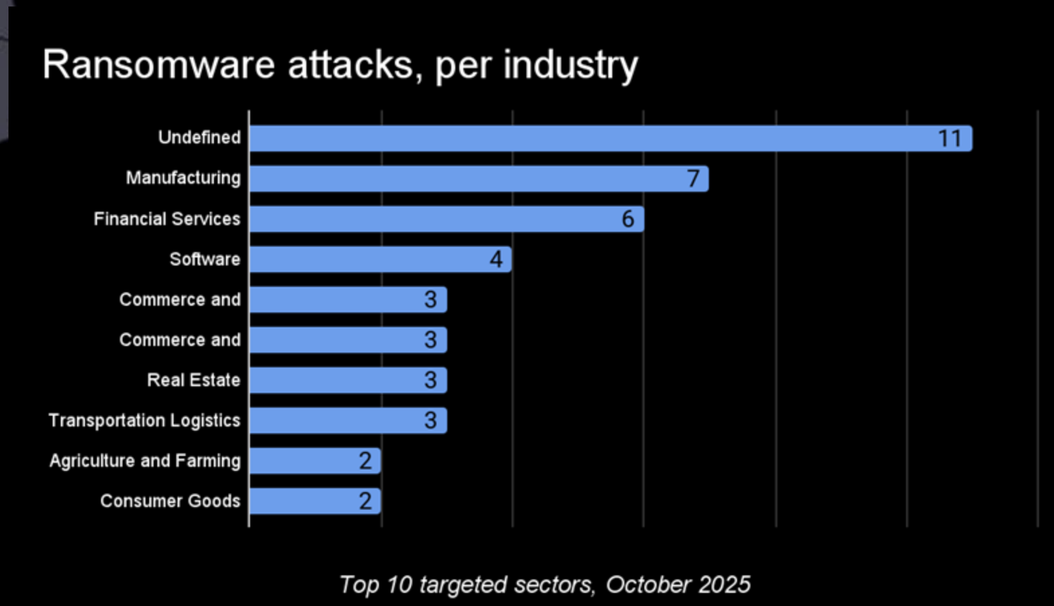
↓ 2.7%

70 ransomware incidents

GROUP-IB

Statistics regarding ransomware activities in October 2025:

- Qilin continued to be in the top most active actors in terms of ransomware activities every month, targeting different countries, especially APAC region.
- The sector landscape is very different from the previous month, with the top targeted industries Undefined, but manufacturing and financial services remain up in the list.



Top 10 targeted sectors, October 2025

Most active threat actors

Qilin
16 activities
-40.74%

The Gentleman
10 activities
+11.11

Devman
4 activities

SafePay
4 activities

White Rabbit
4 activities

Most targeted Countries

Australia
19 activities
+171.43%

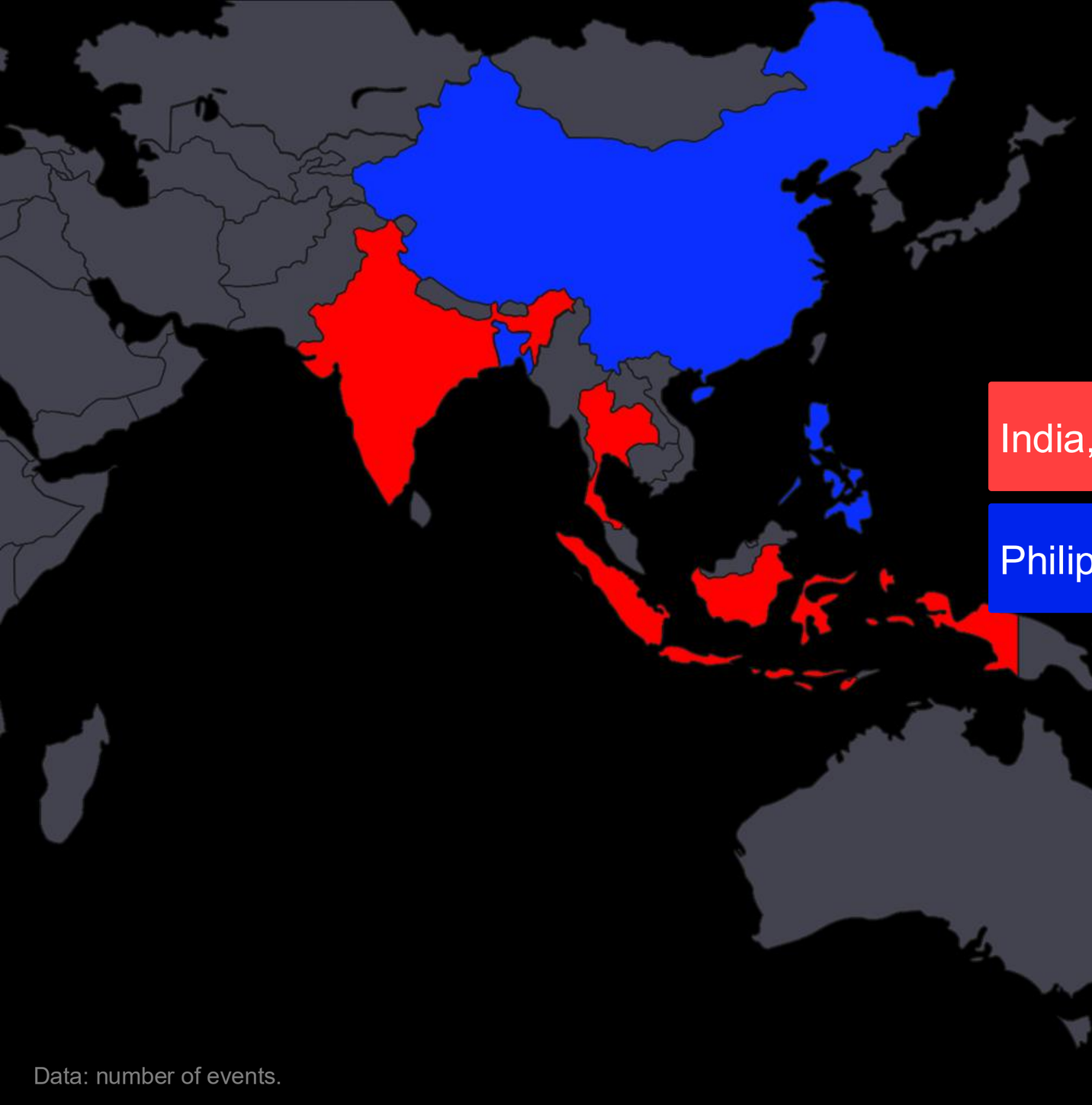
Japan
9 activities
+125.00%

India
8 activities
-33.33%

South Korea
7 activities
-75.00%

Indonesia
5 activities
+150.00%

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



DDOS AND HACKTIVISM

Number of activities per Country, TOP 6 countries

92 incidents ↓32.8%

India, 25	Thailand, 22	Indonesia, 17
Philippines, 5	Bangladesh, 4	China, 4

Data: number of events.

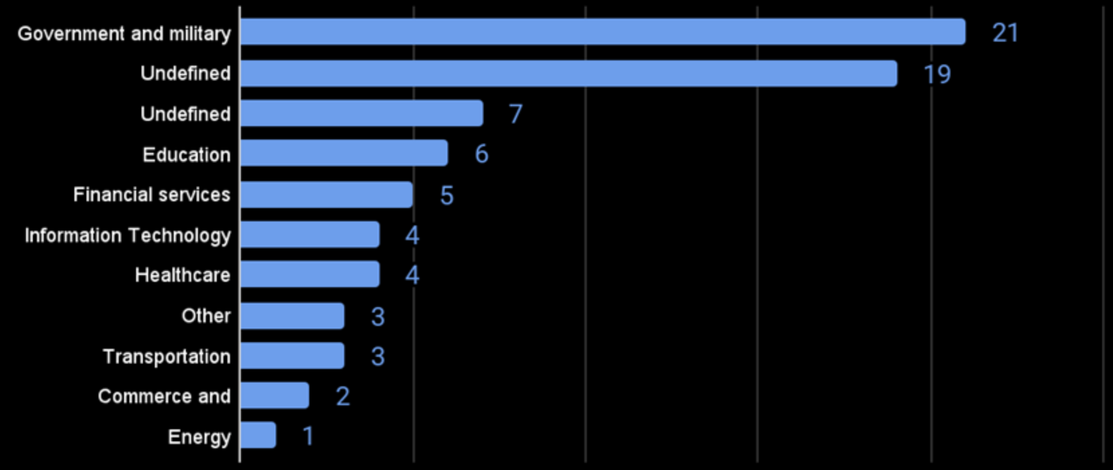
DDOS AND HACKTIVISM (APAC)

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 October 2025.

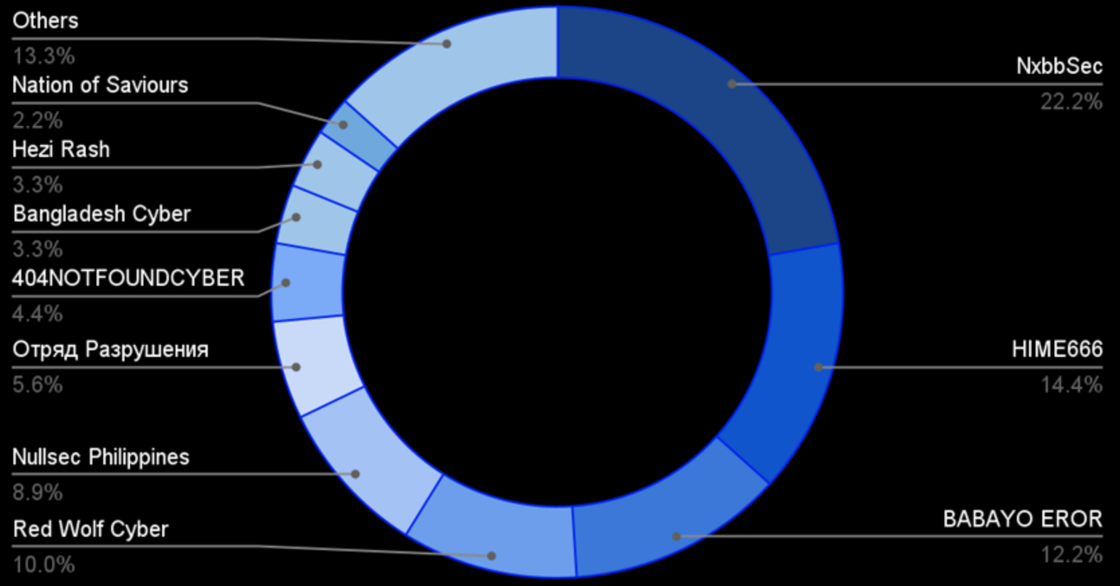
More information about each actor and its activity can be found on Group-IB Threat Intelligence Portal.

DDOS and Hacktivism Activities, per industry



Top 10 targeted sectors, October 2025

DDOS and Hacktivism Activities, per group



Data: number of events.

COMPROMISED DATA (APAC) ↓ 55.5%

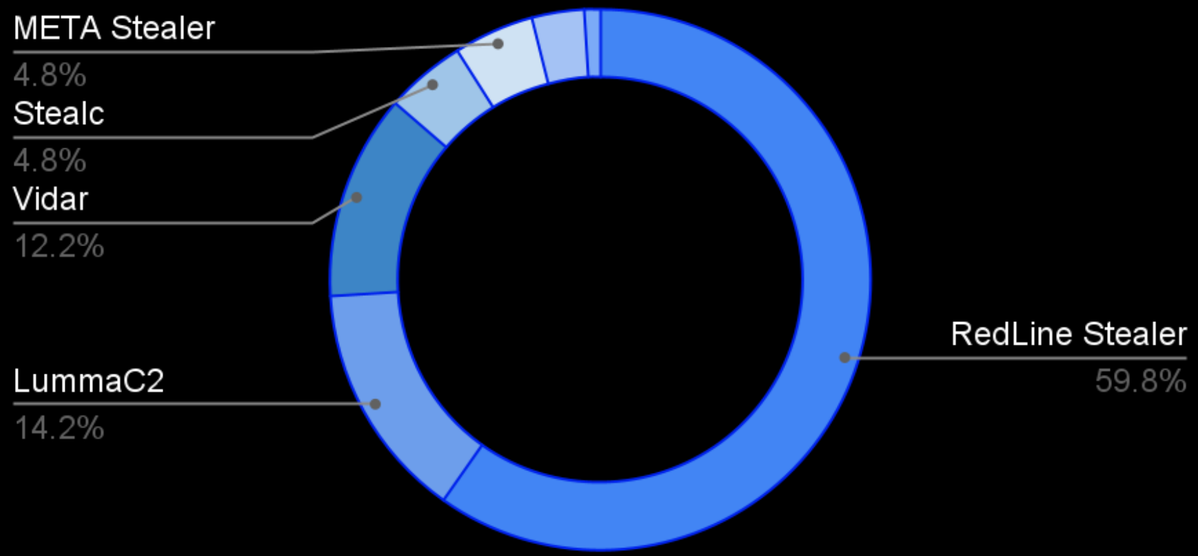
7,106,357 data leaked

GROUP-IB

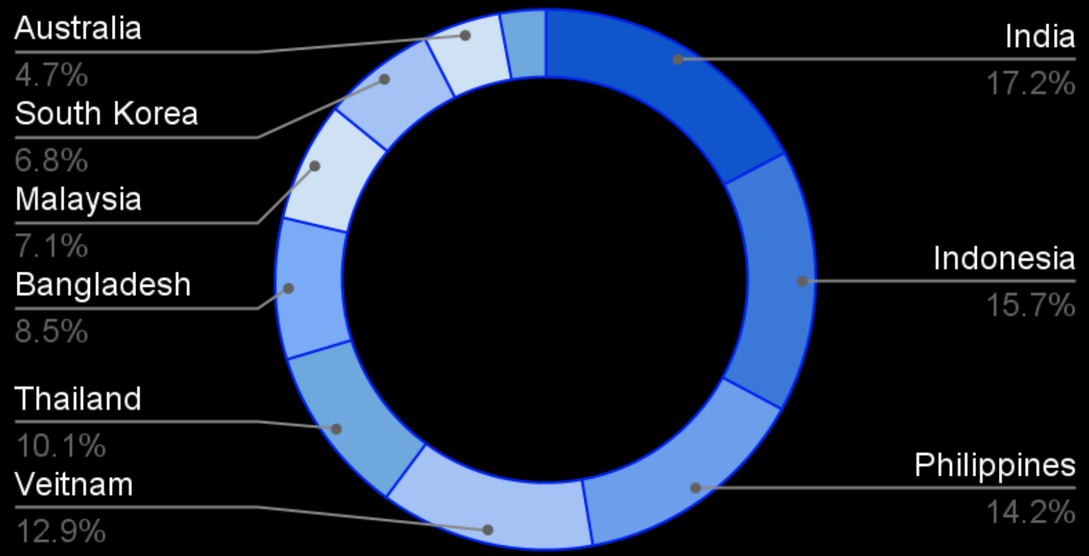
Statistics regarding compromised accounts in October 2025:

- In October 2025, RedLine Stealer was the most dominant malware in APAC, accounting for over half (59.8%) of all compromised accounts, followed by LummaC2 (14.2%) and Vidar (12.2%).
- India (17.2%), Indonesia (15.7%), and Philippines (14.2%) were the most impacted countries, representing the top three in the region.
- The data highlights a continued dominance of RedLine Stealer campaigns across APAC, with significant infection clusters in Southeast and South Asia.

Compromised Accounts by Malware Top 7



Compromised Accounts by Country



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

COMPROMISED BANK CARDS (APAC)

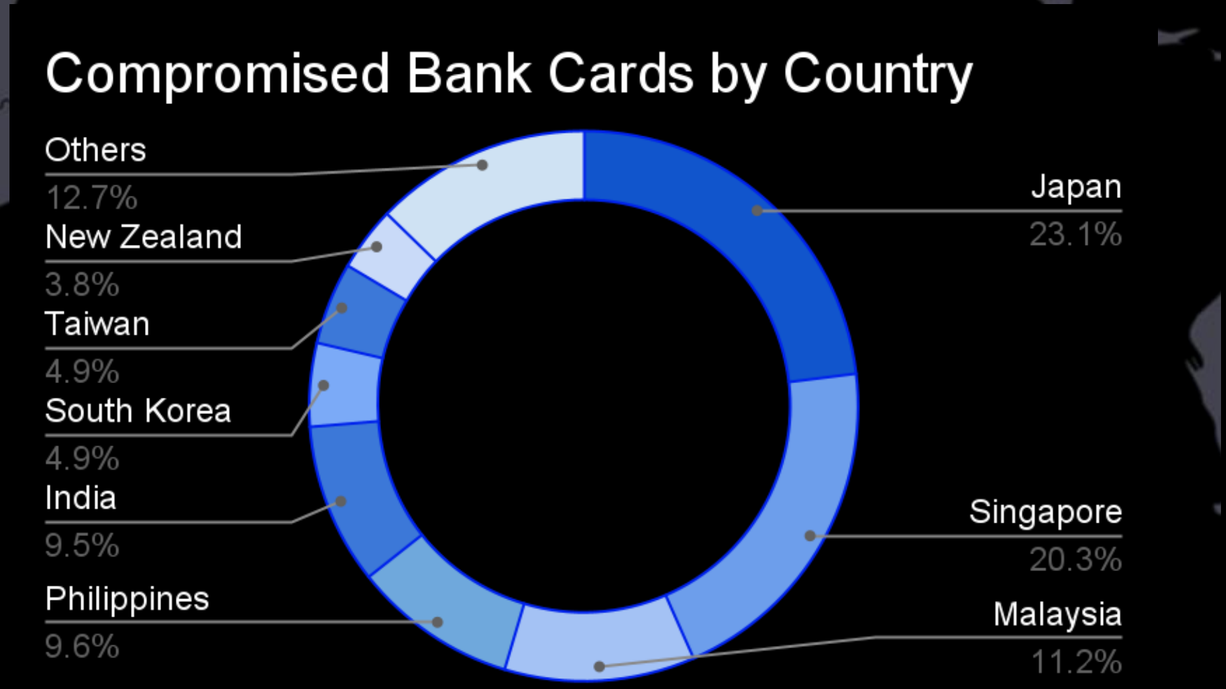
3185 bank cards leaked

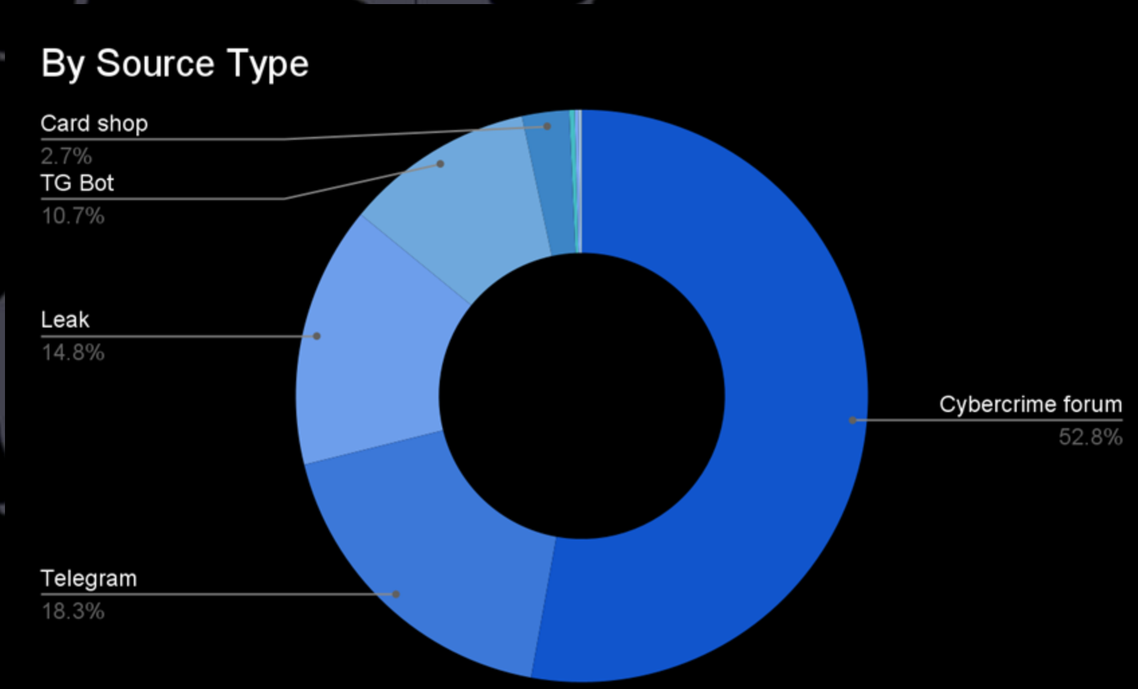
↓ 56.1%

GROUP-IB

Statistics regarding compromised accounts in October 2025:

- Japan (23.1%), Singapore (20.3%) and Malaysia (11.2%) recorded the highest number of compromised bank cards in APAC for October 2025, together accounting for over half of all cases.
- The majority of compromised card data originated from Cybercrime forum, and Telegram source type.





Data: percentage of events

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

NxbbSec

Targeted industries:

- Government and Military
- Education
- Health Care
- Professional Services
- Media and Entertainment
- Commerce and Shopping
- Content and Publishing
- Internet Services
- Community and Lifestyle
- Financial Services
- Information Technology
- Real Estate
- Sales and Marketing
- Consumer Goods
- Energy
- Messaging and Telecommunications
- Transportation
- Travel and Tourism
- Advertising
- Clothing and Apparel
- Food and Beverage
- Music and Audio
- Other

Period of Activity:	May 2025 - Present
Targeted countries:	Worldwide (APAC & ANZ: Thailand, Vietnam, Myanmar, Vietnam, Cambodia, Philippines, Hong Kong, India)
Attribution:	Cambodia
Intent:	Hacktivism

Attack Summary

NXBBSEC is a hacktivist team based in Cambodia that has been involved in various cyber activities. They have claimed responsibility for hacking various Thailand websites with messages that included political and derogatory remarks directed at Thailand and Cambodia's territorial disputes under the campaign

Key Observations

NxbbSec targets Thai websites and promotes narratives from other Cambodian hacktivist groups such as BL4CK CYB3R and Kxichixxsec. The actor primarily performs DDoS and website defacement attacks.

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

Qilin

Targeted industries:

- Government and Military
- Financial Services
- Other
- Education
- Health Care
- Real Estate
- Software
- Transportation
- Agriculture and Farming
- Information Technology
- Internet Services
- Messaging and Telecommunications
- Travel and Tourism
- Consumer Electronics
- Design
- Gaming
- Manufacturing
- Privacy and Security
- Sales and Marketing
- Sports
- Commerce and Shopping

Period of Activity:	2022 - Present
Targeted countries:	Worldwide (APAC & ANZ: Indonesia, India, Pakistan, China, Vietnam. Australia, Hong Kong, Japan, Malaysia, Philippines, Singapore, Thailand)
Attribution:	Russian
Intent:	Ransom and data extortion

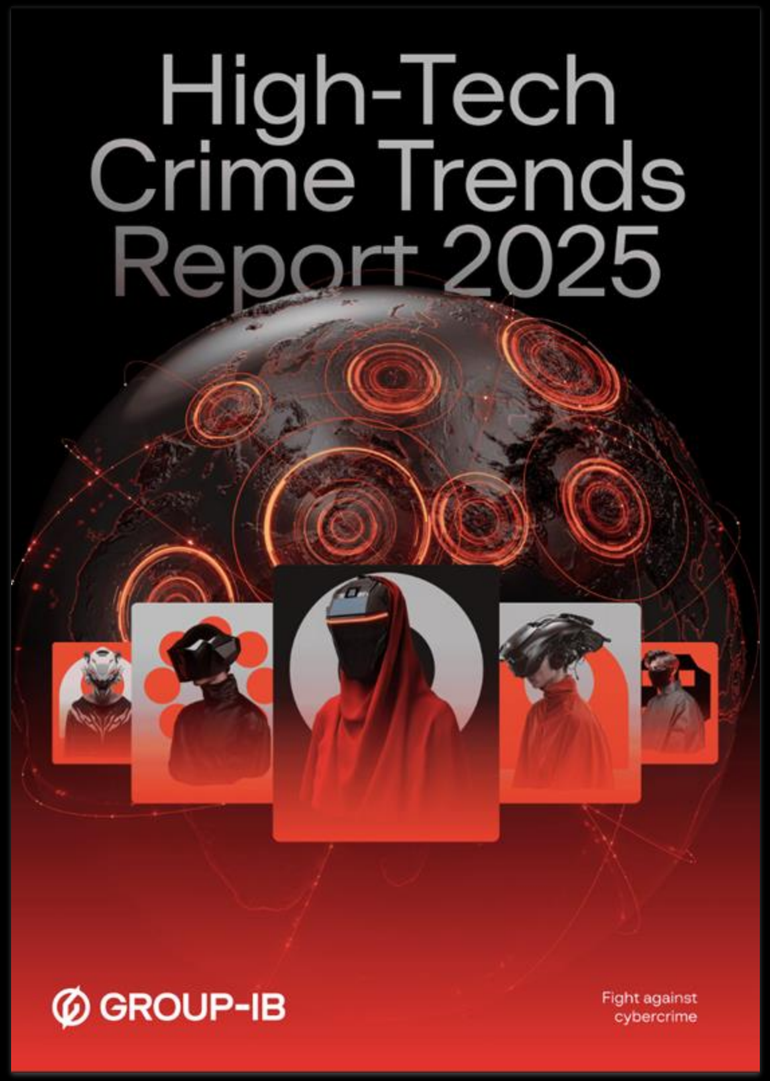
Attack Summary

Qilin (RaaS, aka Agenda) gains initial access typically via compromised credentials, phishing, or exposed remote services moved laterally, exfiltrated sensitive data, then deployed ransomware across Windows and/or Linux/ESXi environments. Victims faced encryption, operational outages, and public data leaks (double extortion).

Key Observations

So far the actor operates as a RaaS affiliate model, relying on affiliates to find and exploit victims. Targets are high-value organisations healthcare, manufacturing, critical infrastructure, and large enterprises. Impact profile: large ransom demands, operational outages, and reputational/regulatory fallout for victims.

HIGH TECH CRIME TRENDS REPORT



Download To Read Now

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

Watch: High-Tech Crime Trends 2025 Deep Dive in APAC Webinar

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

Watch: APAC Intelligence Insights H1-2025 Review & H2 Forecasts

- https://www.group-ib.com/resources/webinars/apac-intelligence-insights-h1-2025/

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

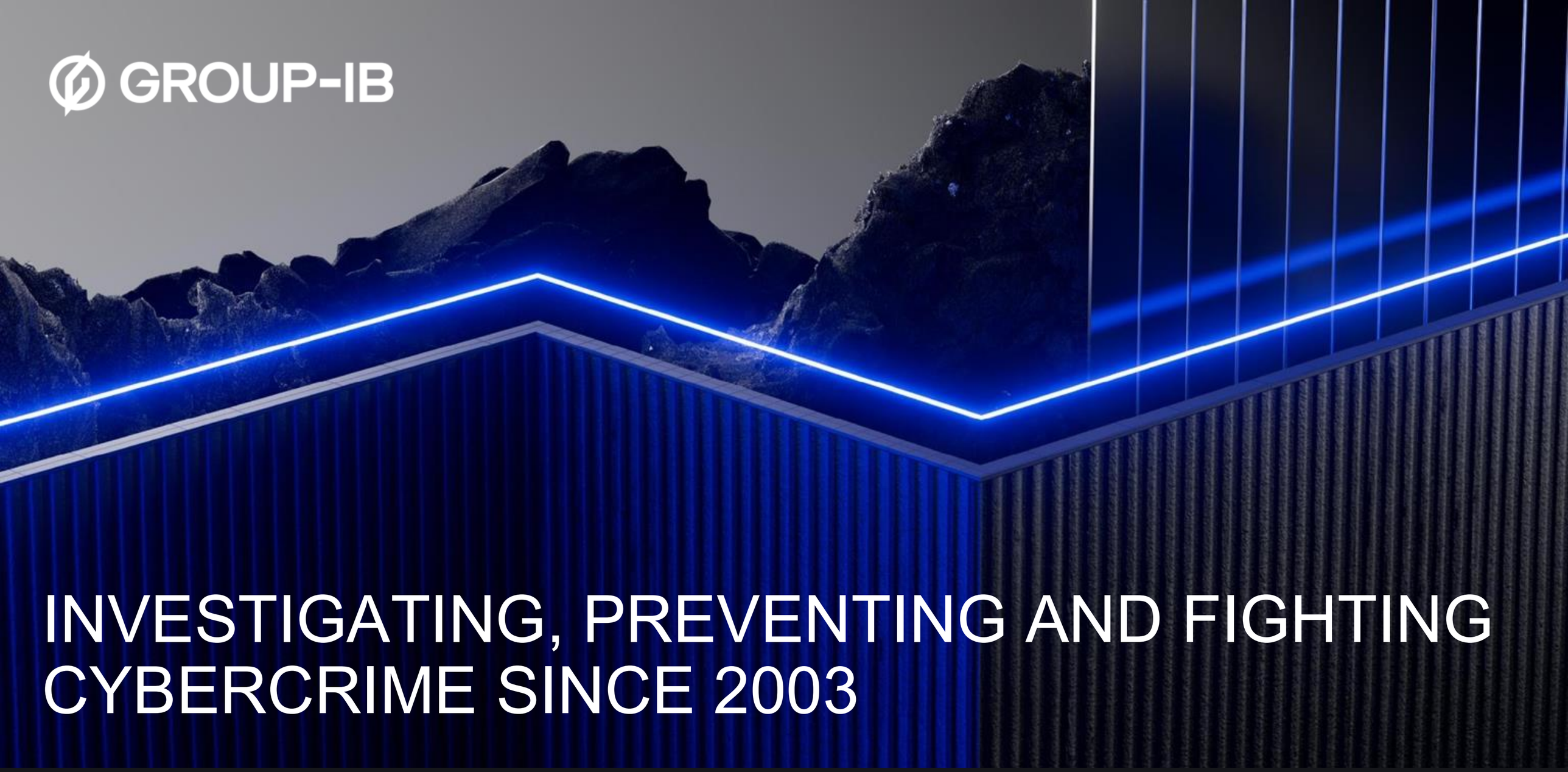
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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.



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