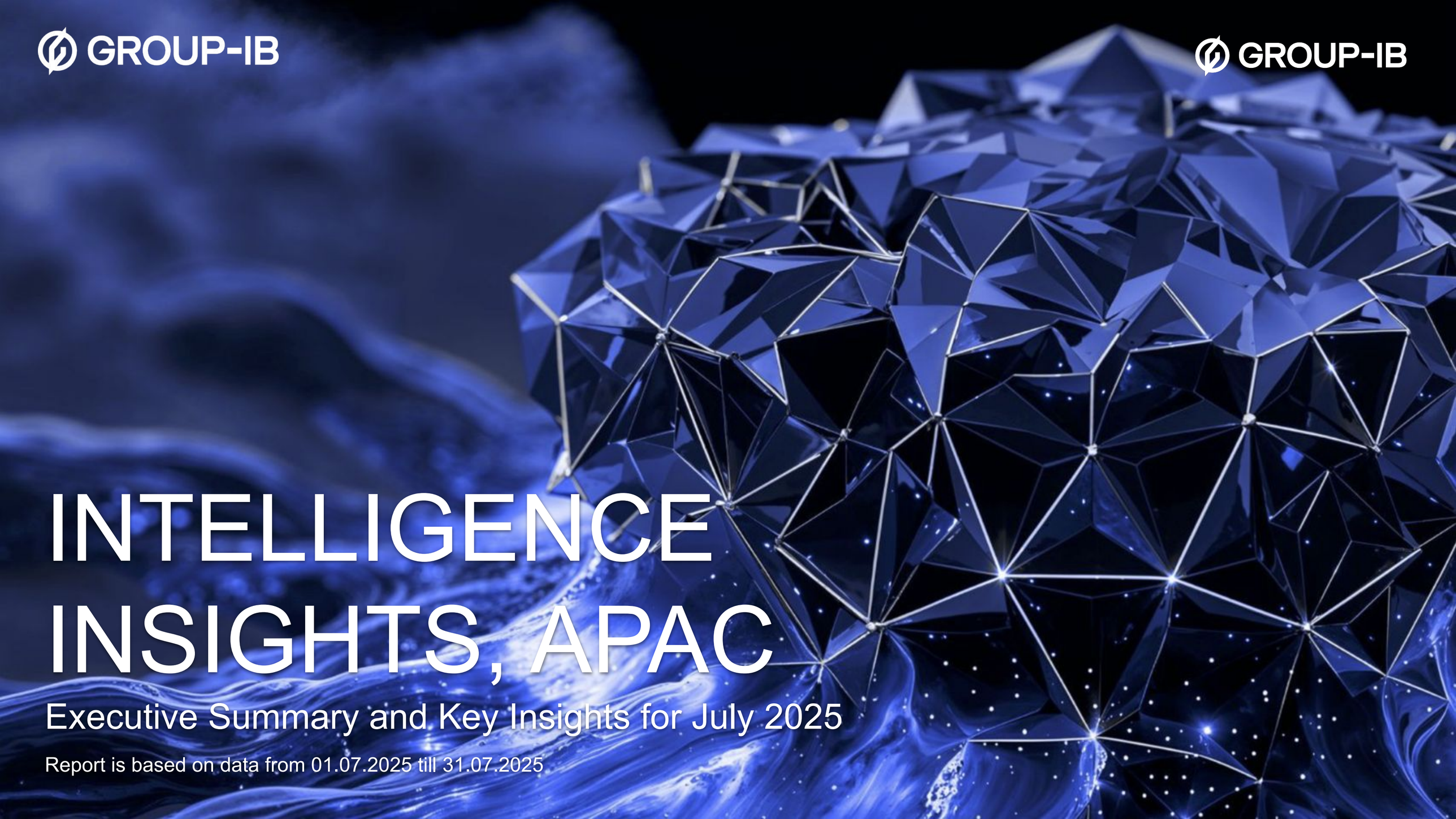


GROUP-IB

GROUP-IB

INTELLIGENCE INSIGHTS, APAC

Executive Summary and Key Insights for July 2025

Report is based on data from 01.07.2025 till 31.07.2025

THREAT LANDSCAPE OVERVIEW

GROUP-IB

Ransomware activities

↓ 29.41%

DDoS and Hacktivism

↓ 5.26%

↓ 64.17%

Compromised Accounts

↓ 61.47%

Compromised Bank Cards

Data comparison: June 2025 - July 2025

GLOBAL INSIGHTS

Global Insights from Group-IB with a brief description:

01

APT28's Authentic Antics: Exploits Authentication Pathways in New Espionage.

IUK calls out Russian military intelligence (GRU) for use of an espionage tool called AUTHENTIC ANTICS, which is a malware targeting the Windows Operating System. The malware runs within the Outlook process and produces periodic login prompts to intercept and exfiltrate Microsoft Office account credentials and tokens.More Info

02

Fake summon malspam campaign targeting Brazilian companies.

On July 28, 2025, Group-IB's threat intelligence detected a multi-stage malspam campaign targeting Brazilian companies aiming to install a malicious Chrome-based extension, in order to steal credentials and cookies. According to the infection chain, this campaign targets only Windows users.More Info

03

Mr Hamza announced DDoS attack on Israeli site

The Group-IB Threat Intelligence team identified a claim by the threat actor Mr Hamza, who announced a DDoS attack on a website in Tel Aviv, Israel. The attackers claimed to have encrypted the site's contents, causing a significant disruption.More Info

04

NoName057(16) announced DDoS attacks on German government websites

The Group-IB Threat Intelligence team identified a series of DDoS attacks claimed by the threat actor NoName057(16) targeting various German government websites. The attackers provided check-host reports as evidence of the disruptions.More Info

REGIONAL INSIGHTS

GROUP-IB

Regional Insights from Group-IB with a brief description:

01

Clashes on the border between Thailand and Cambodia

A long-standing territorial dispute flared again on 28 May 2025, resulting in a Cambodian soldier's death. Hostilities spiked on 24 July with artillery and air strikes. Thai officials reported over 10 fatalities, and evacuations on the Thai side topped 40,000. In parallel, pro-Cambodian hacktivists (AnonsecKh/Bl4ckCyb3r) conducted DDoS and defacement attacks on Thai entities.More Info

02

New Android banking trojan targeting Vietnamese users

Group-IB analysts discovered the distribution of TTDK.apk through phishing websites with different schemes, such as eKYC bank websites impersonating the local Vietnamese bank. A TTDK, or trung tâm đăng kiểm, is an authorized Vehicle Registration and Inspection Center in Vietnam.More Info

03

UNC3886 Campaign Dynamics and Operational Insights

UNC3886, also called Fire Ant, is a China nexus cyber-espionage group first reported publicly in 2022, though telemetry places its activity as early as late 2021. It pursues strategic access to government, telecommunications, technology, defense, energy, and other critical-infrastructure environments across the United States, Europe, and Asia, with Singapore highlighted as a current focal point.More Info

04

RootSec reported data leak

The Group-IB Threat Intelligence team has identified a claim by the threat actor RootSec regarding a data leak. The message includes sensitive information such as an email address and password, indicating unauthorized access to personal data.More Info

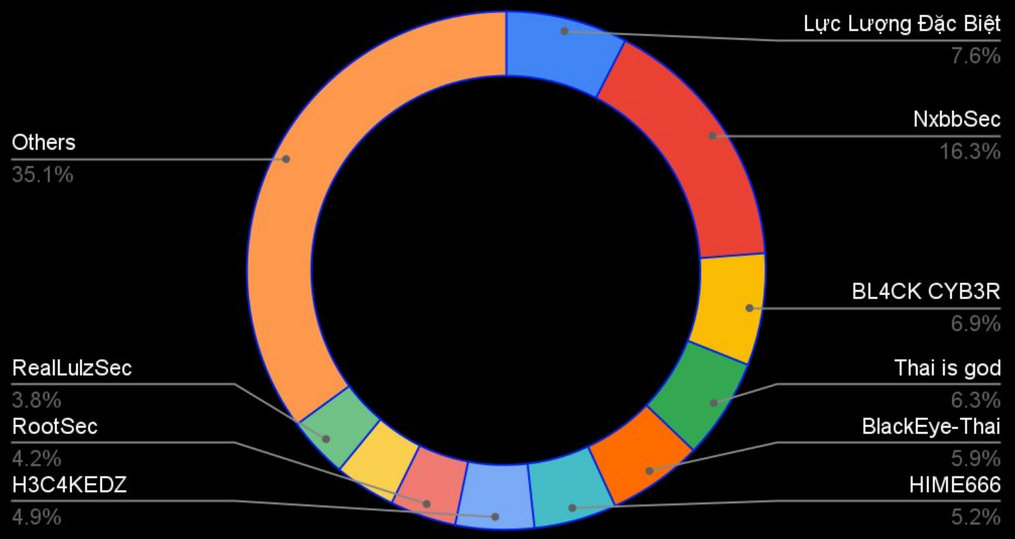
APAC and ANZ

More Information in Group-IB Threat Intelligence Portal

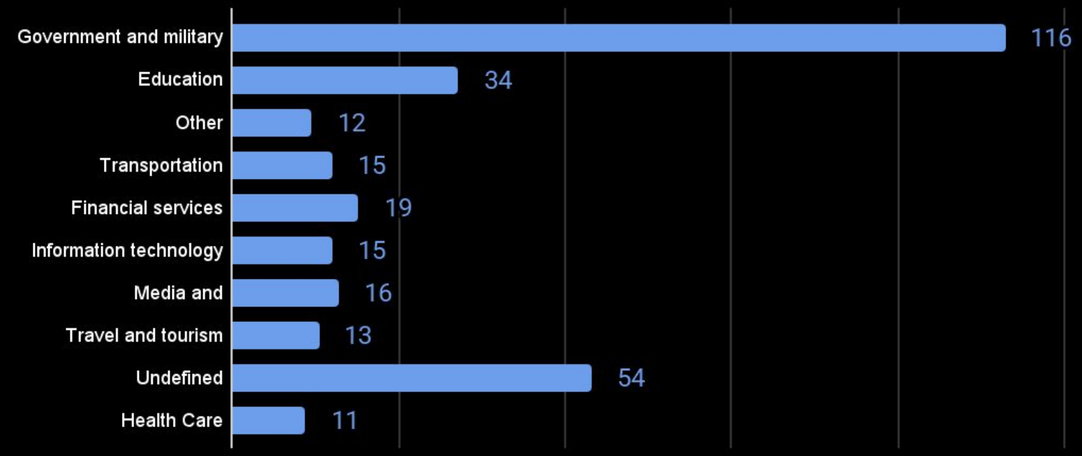
DDOS AND HACKTIVISM

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

By Actor



By Industry



Top 10 targeted sectors

Data: number of events.

RANSOMWARE ACTIVITIES

↓ 29.41%

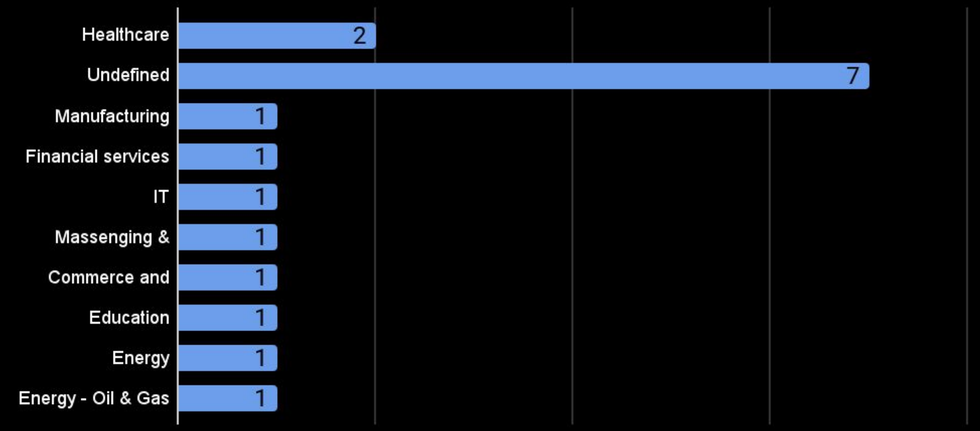
24 ransomware incidents

GROUP-IB

Statistics regarding ransomware activities in July 2025:

- **Healthcare** suffered about two attacks, most attacks happened in Undefined sectors (7 attacks).
- **Qilin and Eldorado** were the most active threat actor (8 activities total), despite a 20% decrease in qilin activity.
- **Australia** experienced the highest number of country-specific attacks (7), though it also saw a 36.36% decline. Taiwan reported 3 attacks whereas last month it was zero.

Ransomware attacks, per industry, Top 10



Top 10 targeted sectors, July 2025

Most active threat actors

Qilin
4 activities
-20%

ElDorado
4 activities

INC Blog
3 activities

Devman
3 activities
50%

Gunra
2 activities

Most targeted Countries

Australia
7 activities
-36.36%

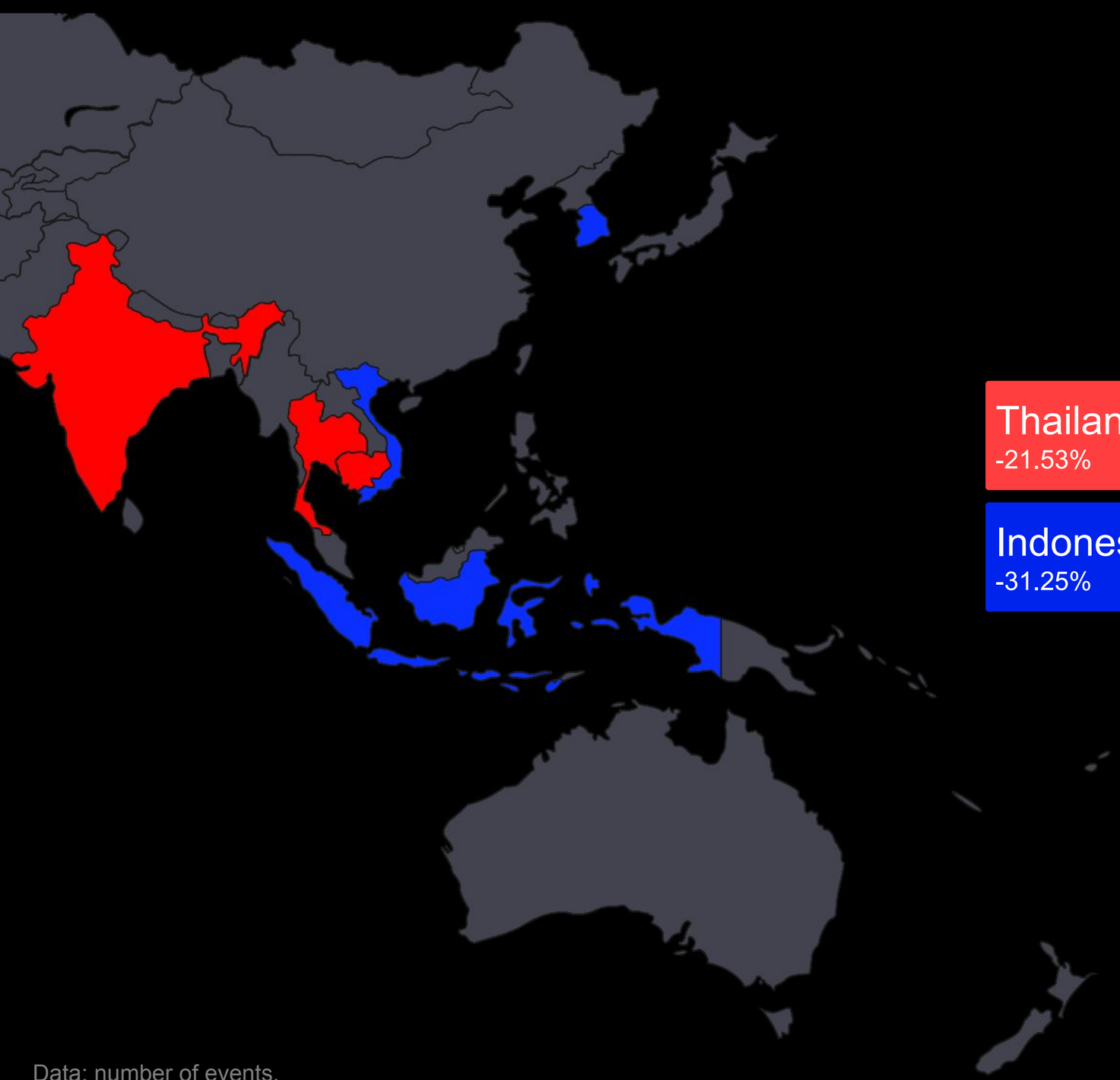
Thailand
3 activities
-40%

Japan
3 activities
-25%

Taiwan
3 activities

India
2 activities
-50%

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



DDOS AND HACKTIVISM

Number of activities per Country, TOP 6 countries

↑2.59%

Thailand, 113 -21.53%	Cambodia, 72	India, 47 -31.88%
Indonesia, 21 -31.25%	Vietnam, 12 -29.41 %	S. Korea, 12 -7.69%

Data: number of events.

COMPROMISED DATA (APAC)

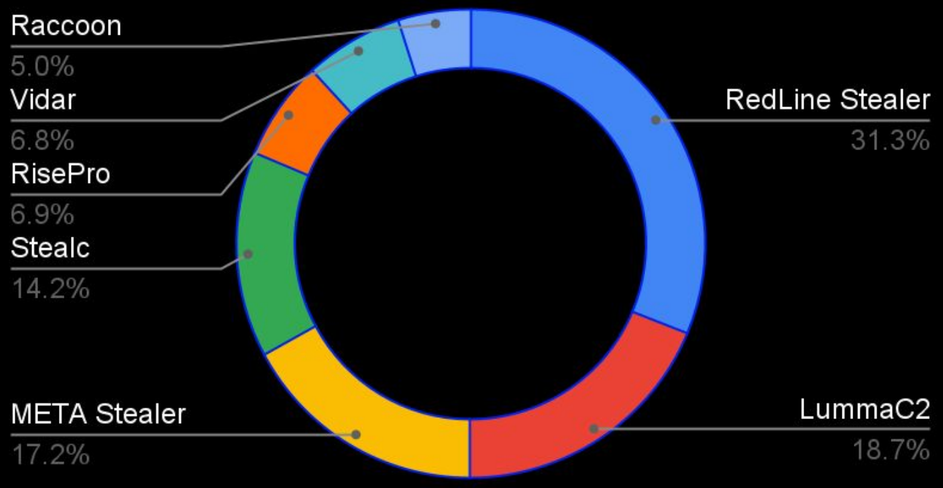
↓ 64.17%

GROUP-IB

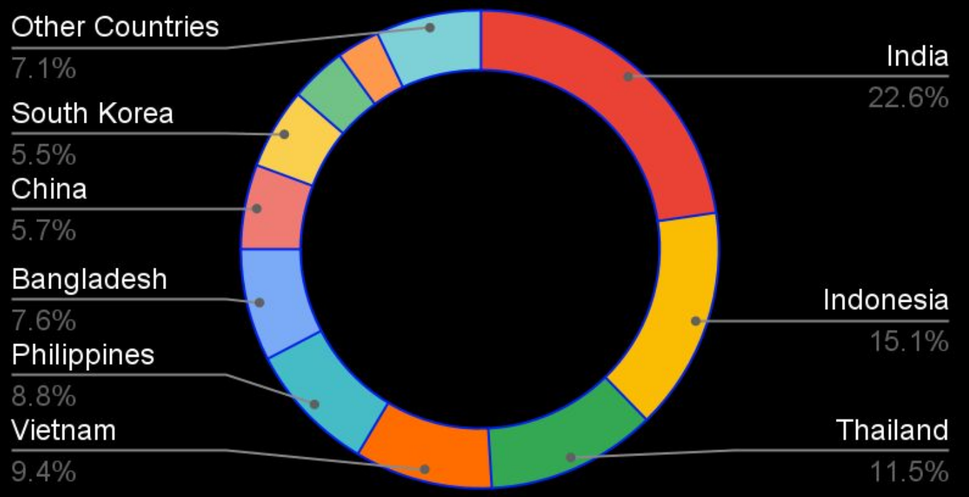
Statistics regarding compromised accounts in July 2025 for APAC:

- In July 2025, **RedLine Stealer** (31.3%) and **LummaC2** (18.7%) were the most prevalent malware types responsible for compromised accounts.
- **India** accounted for the largest share of compromised accounts at 22.6%, followed by **Indonesia** (15.1%) and **Thailand** (11.5%).
- **LummaC2** and **RedLine Stealer** represent half (50%) of all compromised accounts by malware in July.

By Malware, Top 7



By Country



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

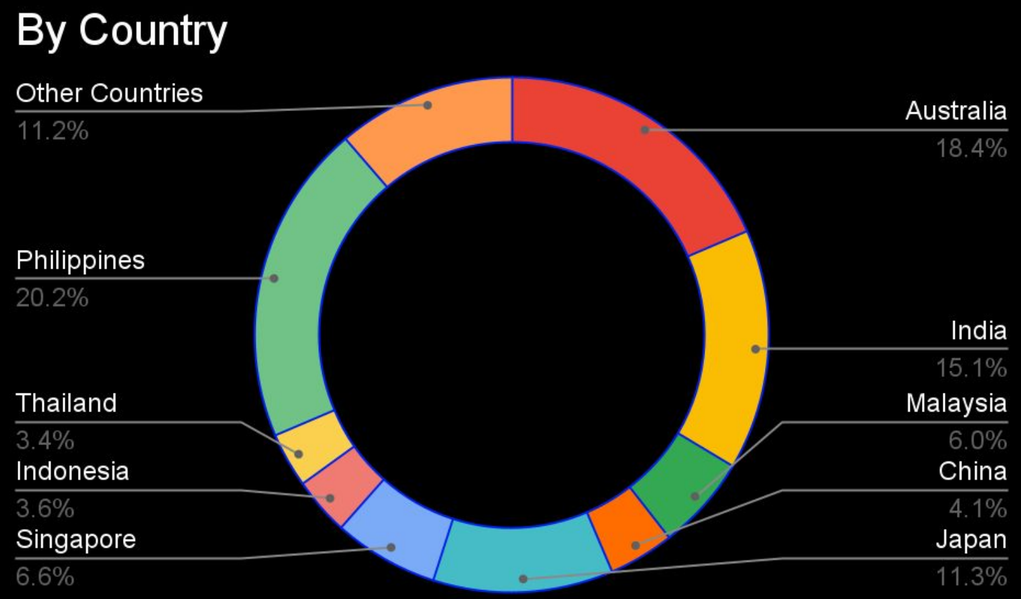
COMPROMISED BANK CARDS (APAC)

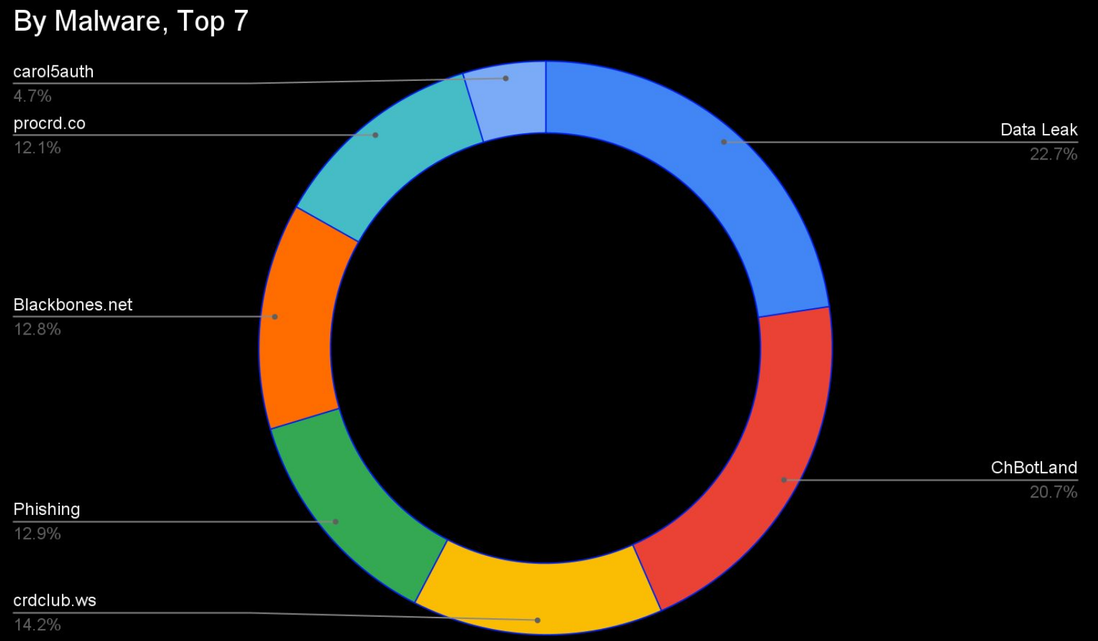
↓ 61.47%

GROUP-IB

Statistics regarding compromised accounts in July 2025:

- **Philippines** accounts for the largest share of compromised bank cards, representing 20.2% of the total, followed by Australia at 18.4% and India at 15.1%.
- Both **Data leak** and **ChkBotLand** are responsible for the highest percentage of compromised bank cards by malware, each contributing 22.7% and 20.7%.
- While a few malware types dominate, a wide range of malware families, including **crdclub.ws** (14.2%) and **blackbones.net**(12.8%), contribute to the compromised bank cards, indicating a varied threat landscape.





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

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

UNC3886

Targeted industries:

- Utilities
- Messaging and telecommunications
- Energy
- Commerce and shopping
- Internet services
- Clothing and apparel
- Professional services
- Consumer electronics
- Consumer goods
- Artificial intelligence
- Community and lifestyle
- Data and analytics
- Lending and investments
- Design
- Food and beverage
- Gaming
- Health care
- Information technology
- Media and entertainment
- Other
- Payments
- Transportation
- Privacy and security
- Sales and marketing
- Travel and tourism

Period of Activity:	Dec 2021 - Present
Targeted countries:	Worldwide (APAC & ANZ: Singapore)
Attribution:	China
Intent:	cyber espionage

Attack Summary

UNC3886, also known as Fire Ant, is a China based cyber espionage group that has been active since late 2021 and targets critical government telecommunications technology defense and energy infrastructure across the United States, Europe, and Asia. The group exploits zero day vulnerabilities in specific devices to achieve initial access. To sustain their presence they deploy publicly available rootkits, steal credentials, and leverage trusted services to establish control channels for long term intelligence gathering.

Key Observations

UNC3886 is a highly sophisticated China-nexus threat actor primarily engaged in cyber espionage. The group is known for exploiting zero-day vulnerabilities in network appliances such as VMware ESXi, Fortinet FortiOS, and Juniper firewalls to gain persistent and covert access to high-value targets. By operating within appliance-level and virtualized environments, UNC3886 effectively evades traditional endpoint detection tools. It deploys custom malware families like STARBABY and SIMPLESEA to maintain access, execute commands, and exfiltrate sensitive data. The group's focus is on long-term intelligence gathering rather than immediate disruption, aligning with strategic Chinese cyber objectives.

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

SideWinder

Targeted industries:

Government and military
Education
Financial services
Information technology
Media and entertainment
Transportation
Commerce and shopping
Science and engineering
Real estate
Administrative services
Content and publishing
Internet services
Agriculture and farming
Consumer goods
Manufacturing
Professional services
Software
Travel and tourism
Advertising
Community and lifestyle
Data and analytics
Energy
Messaging and telecommunications
Design
Gaming
Hardware
Lending and investments
Privacy and security

Period of Activity:	July 2016 - Present
Targeted countries:	Worldwide (APAC & ANZ: China, Pakistan, Sri lanka, Philippines)
Attribution:	India
Intent:	state-aligned cyber espionage

Attack Summary

The SIDEWINDER group (also known as Rattlesnake, Hardcore Nationalist (HN2), T-APT-04) has been in operation since at least 2012. The group is engaged in cyber espionage on members of South Asian state institutions (governments, military institutions). The attacks target both Windows and Android users.To gain initial access, emails with malicious attachments are mainly used. Territorial conflicts between China, India, Nepal, and Pakistan are used as bait topics.

Key Observations

SideWinder is a highly active and persistent threat actor believed to be aligned with Indian state interests.The group is known for using spear-phishing emails with weaponized documents, exploiting old vulnerabilities, and deploying custom malware like RCShell and DelphiSpy. SideWinder frequently updates its tools and infrastructure to avoid detection, and its campaigns consistently reflect strong geopolitical motivations rather than financial intent.

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

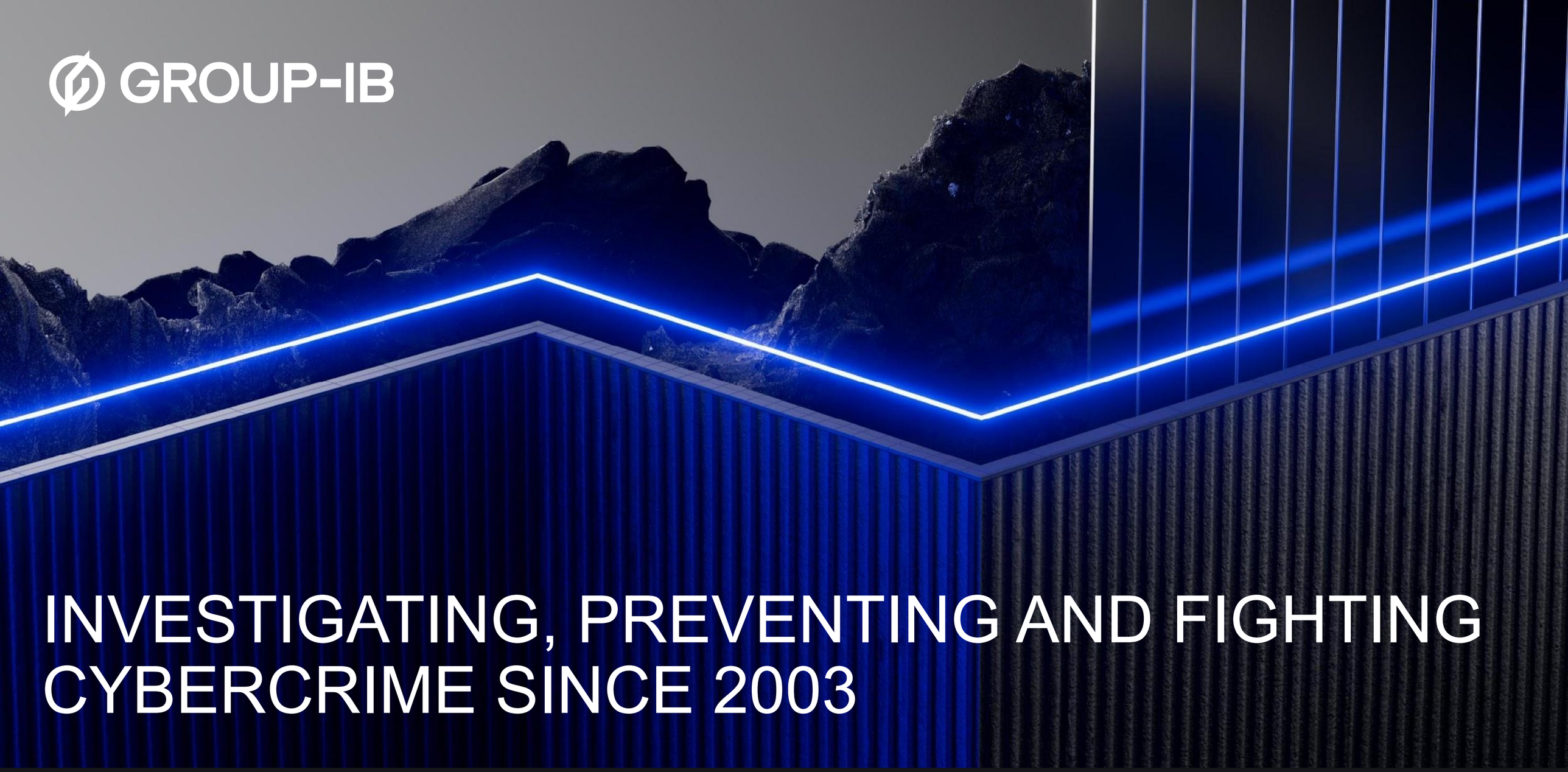
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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