GROUP-IB

GROUP-IB

INTELLIGENCE INSIGHTS. AUNZ

Executive Summary and Key Insights for September 2025

Report is based on data from 01.09.2025 till 01.10.2025

THREAT LANDSCAPE OVERVIEW - APAC

GROUP-IB

Ransomware activities

↑ 84.6%

DDoS and Hacktivism

↓ 55.2%

↑ 85.9%

Compromised Accounts

↓ 67.7%

Compromised Bank Cards

Data comparison: August 2025

GLOBAL INSIGHTS

Global Insights from Group-IB with a brief description:

01

Privacy-Conscious Android Users in the UAE Hit by New Spyware Campaigns

ESET researchers have uncovered two Android spyware campaigns targeting individuals interested in secure communication apps, namely Signal and ToTok. These campaigns distribute malware through deceptive websites and social engineering and appear to target residents of the United Arab Emirates (UAE). The investigation led to the discovery of two previously undocumented spyware families, Android/Spy.ProSpy, impersonating upgrades or plugins for the Signal and ToTok messaging apps; and Android/Spy.ToSpy, impersonating the ToTok app. More Information.

02

Mapping the Infrastructure and Malware Ecosystem of MuddyWater

Since early 2025, Group-IB analysts have observed that MuddyWater, known as an Iranian state-sponsored Advanced Persistent Threat (APT) group, remains active across the Middle East and Europe, with a notable surge in activity within the European region. Our latest analysis of the group's activities has revealed new intelligence regarding recent shifts in their operational characteristics and arsenal. Recent activity shows that they still rely on phishing for delivery, leveraging maldocs with malicious macros for infection. More Information.

03

From Deepfakes to Dark LLMs: 5 use-cases of how AI is Powering Cybercrime

AI in cybercrime is evolving fast, fueling AI phishing attacks, AI scam calls, AI voice cloning scams, and even AI deepfake scams. From Dark LLMs to next-gen AI phishing tactics, we break down how criminals exploit AI today and what you can do to stay protected. What we found is both reassuring and concerning. Fully autonomous AI-driven cybercrime isn't here yet. But hybrid human AI operations are already reshaping how scams are run, phishing is crafted, and malicious campaigns are managed. More Information.

04

Tortoiseshell Deploys New Malware Targeting Europe

Researchers at Check Point Research (CPR) have observed renewed activity from Nimbus Manticore (also tracked as UNC1549 or Smoke Sandstorm), a long-standing Iran-nexus APT group targeting aerospace and defense organizations in the Middle East and Europe. CPR also highlights a separate activity cluster under the Nimbus Manticore umbrella that leverages similar spear-phishing methods but focuses on different sectors and employs distinct domain naming conventions. While these operations share resources with the broader group, they exhibit unique malware traits and infrastructure. More Information.

REGIONAL INSIGHTS

GROUP-IB

Regional Insights from Group-IB with a brief description:

01

The database sale of National credit information centre of Vietnam (cic.org.vn)

On September 8, 2025, ShinyHunters on the breachsta[.]rs darkweb forum announced the sale of the entire database of the “Credit Institute of Vietnam”. Based on the context of the message and the contents of the files published as evidence, ShinyHunters most likely meant that he put up for sale the database of National credit information centre of Vietnam (cic[.]org[.]vn). More Information.

02

A new campaign using KamiKakaBot was discovered in September 2025

Group-IB Threat Intelligence Unit has identified a TAR archive containing two files: a decoy document and an XML file responsible for launching KamiKakaBot malware. The method by which these files arrived on the infected system remains unknown. However, based on the language used in the decoy document, the likely target appears to be located in Vietnam. More Information.

03

Phishing campaign targeting customers of Japanese financial institutions

During monitoring of phishing infrastructure, Group-IB discovered a prolonged and ongoing phishing campaign. The campaign, active since at least June 2024, is mainly targeting customers of Japanese financial institutions. The campaign was attributed to a Chinese-speaking threat actor that Group-IB codenamed Loloboshi. We have also found an instance where the operators created phishing pages mimicking the Japan National Police Agency. The main objective of the threat actor is to steal payment and personal details, ip addresses and other information. More Information.

04

Sale of Pakistan National Intelligence Fusion and Threat Assessment Center NIFTAC documents

Group-IB detected a new post on exploit[.]in by the threat actor xuii, who is claiming the sale of high-sensitivity documents allegedly exfiltrated from Pakistan’s National Intelligence Fusion and Threat Assessment Center (NIFTAC) and a Pakistan–Turkey Strategic Cooperation Plan. More Information

APAC and ANZ

More Information in Group-IB Threat Intelligence Portal

LOCAL INSIGHTS

GROUP-IB

Local Insights from Group-IB with a brief description:

01
HIME666 reported data leak from multiple Australian organizations
HIME666 has stated to conduct attacks against multiple Australian organizations such as the Queensland Department of Education, South Australian Government, The Good Guys Commercial, Australian Federal Police, ADF Careers, Australian Federal Police Association, Commonwealth Superannuation Corporation, and Victoria Police. The actor group claimed to have access to credentials and URLs, indicating unauthorized access to various systems. More Information.

02
Smishing Triad Phishing-as-a-Service
We have been monitoring the Smishing Triad group specializing in SMS phishing to steal and store victims' payment information, distributing their custom smishing kit named Lighthouse via a private Telegram channel. This group has been active since 2023, with over 500 templates, targeting multiple countries such as Australia, USA, UK, Canada, etc. More Information.

03
Malicious activities during the month
Ransomware attacks continued to happen with some Australian organizations by a few notable groups such as DragonForce, Kairos, Akira etc. Despite having a small number, DDoS and Hacktivism activities during this month saw some notable activities such as the attack against Canva, and multiple organizations claimed by DieNet and HIME666. More information can be found in Group-IB Threat Intelligence Portal.

Australia

More Information in Group-IB Threat Intelligence Portal

RANSOMWARE ACTIVITIES (APAC)

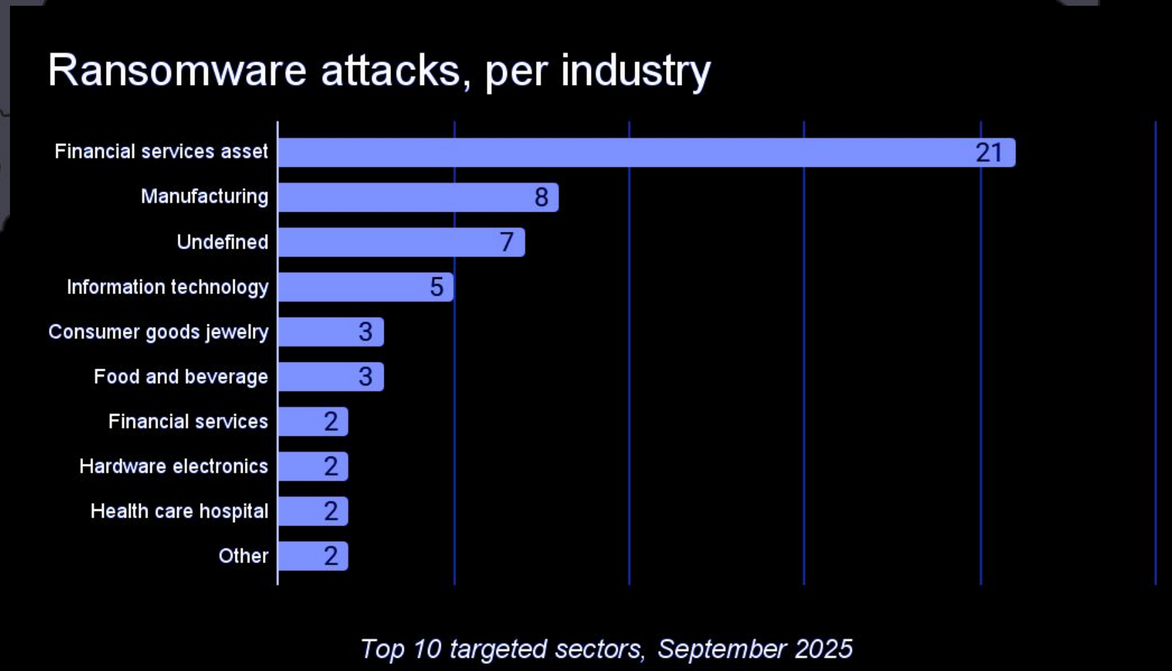
↑ 84.6%

72 ransomware incidents

GROUP-IB

Statistics regarding ransomware activities in August 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 being Financial Service & Asset Management



Top 10 targeted sectors, September 2025

Most active threat actors

Qilin
27 activities
+440%

The Gentleman
9 activities

Devman
4 activities

INC Blog
4 activities

Coinbase Cartel Ransomware
3 activities

Most targeted Countries

South Korea
28 activities
+460%

India
12 activities
+71.43%

Australia
7 activities

Thailand
6 activities
+500%

Taiwan
6 activities
+200%

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

RANSOMWARE ACTIVITIES (Australia)

↓ 27.27%

7 ransomware incidents

GROUP-IB

Statistics regarding ransomware activities in September 2025:

- **Australia** is still in the top 5 countries within the region with the highest number of ransomware attacks, claimed by a few notable groups such as DragonForce, Akira, Kairos, etc.
- The targeted sectors this month range from Healthcare, Sports, Education, to Real estate, Transportation. Although case-specific TTPs and IOCs are restricted, IoCs of this actor collected from previous incidents can be found on the Threat Intelligence Portal.

Most active threat actors (compared to the previous month)

Kairos

2 activities

Akira

1 activity

Anubis

1 activity

DragonForce

1 activity

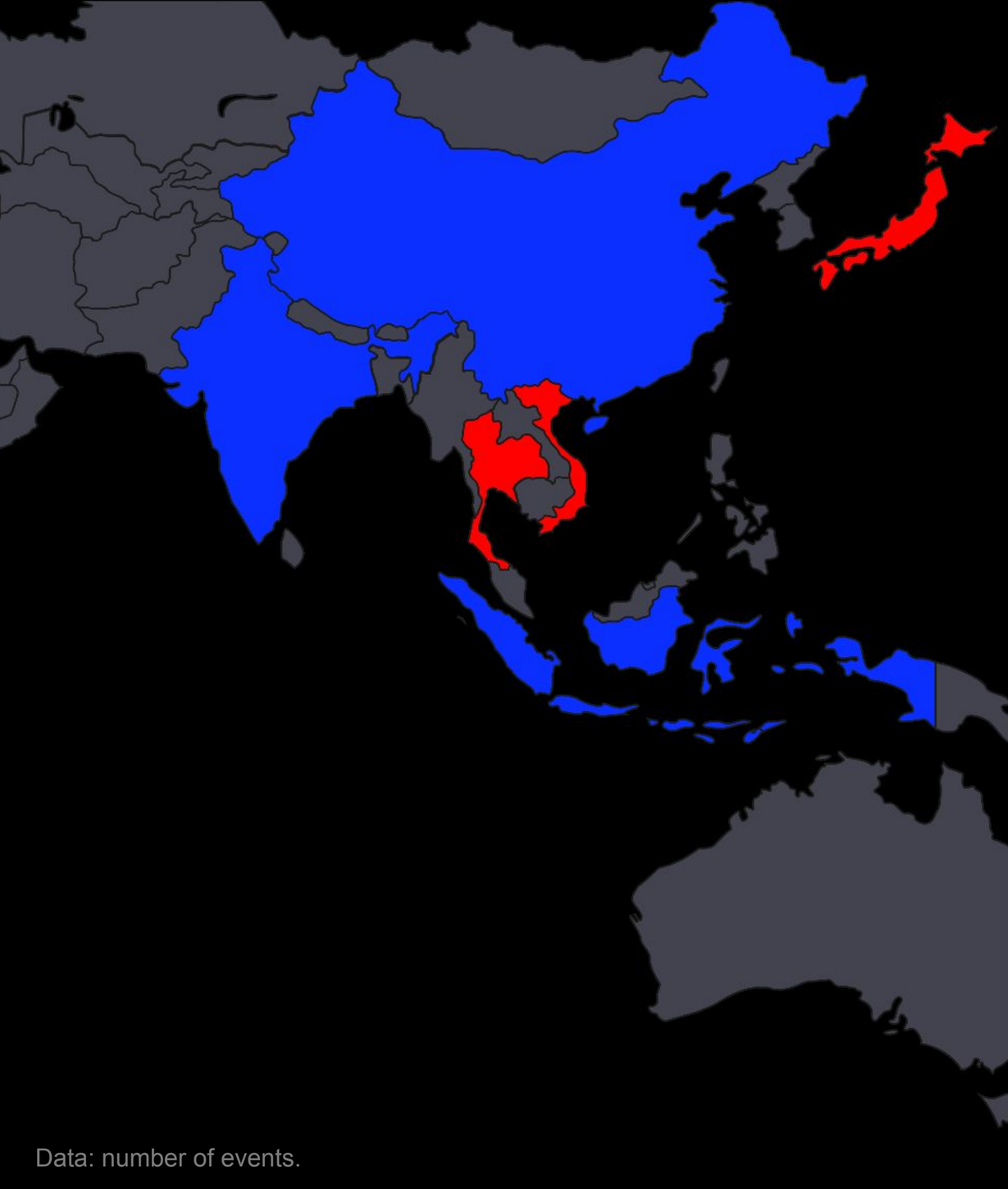
Interlock

1 activity

KillSec

1 activity

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



DDOS AND HACKTIVISM

Number of activities per Country, TOP 6 countries

137 incidents ↓55.2%

Thailand, 57	Vietnam, 19	Japan, 16
Indonesia, 12	India, 9	China, 6

Data: number of events.

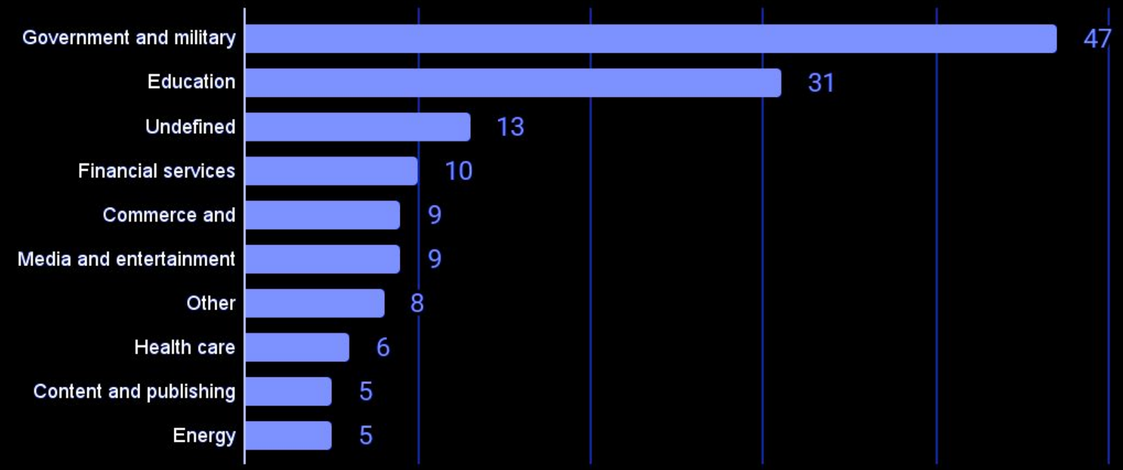
DDOS AND HACKTIVISM

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.

In **Australia,** only 2 DDoS & Hacktivism activities during the month were identified. They were claimed by 2 groups named DieNet and HIME666. DieNet's DDoS attack on Canva on September 3rd was confirmed through multiple check-host reports indicating service disruption. HIME666, a hacktivist group based in Indonesia, claimed to be behind attacks against Australian organizations, such as the Queensland Department of Education, South Australian Government, The Good Guys Commercial, Australian Federal Police, ADF Careers, Australian Federal Police Association, Commonwealth Superannuation Corporation, Victoria Police. The leak included credentials & URLs, indicating unauthorized access to various systems.

Below is a brief overview of groups that were active in the region during September, the threat landscape is very different from the previous month, along with the top 10 targeted sectors in September 2025. More information about each actor and its activity can be found on Group-IB Threat Intelligence Portal.

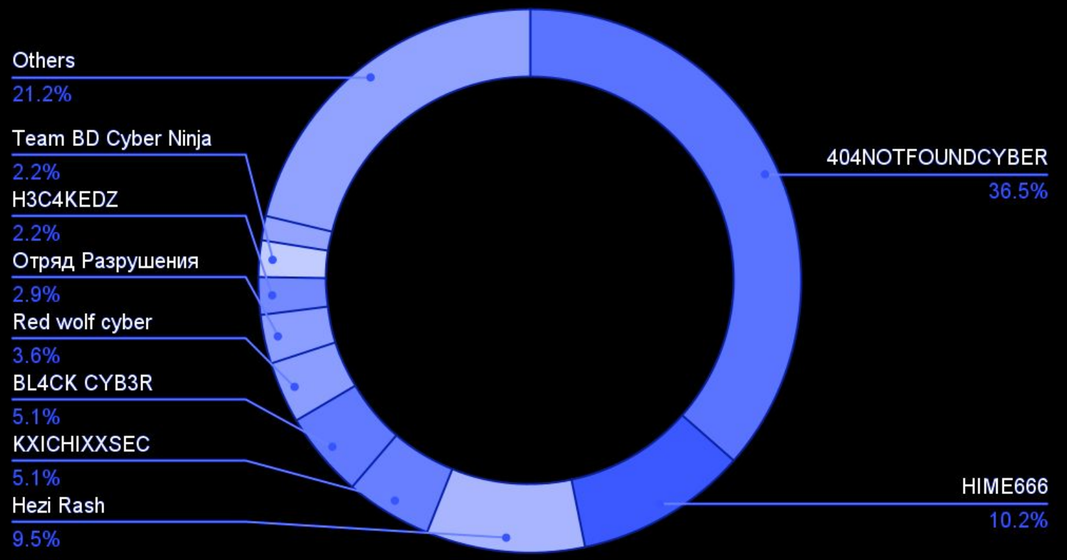
DDOS and Hacktivism Activities, per industry



Top 10 targeted sectors, September 2025

Data: number of events.

DDOS and Hacktivism Activities, per group



COMPROMISED DATA (APAC) ↑ 85.9%

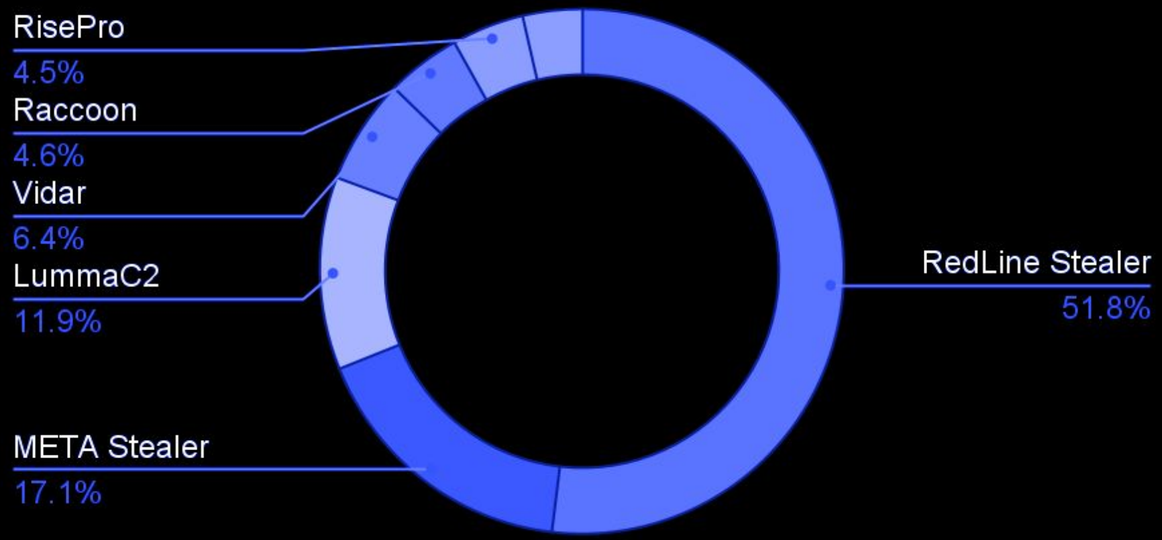
15,941,958 data leaked

GROUP-IB

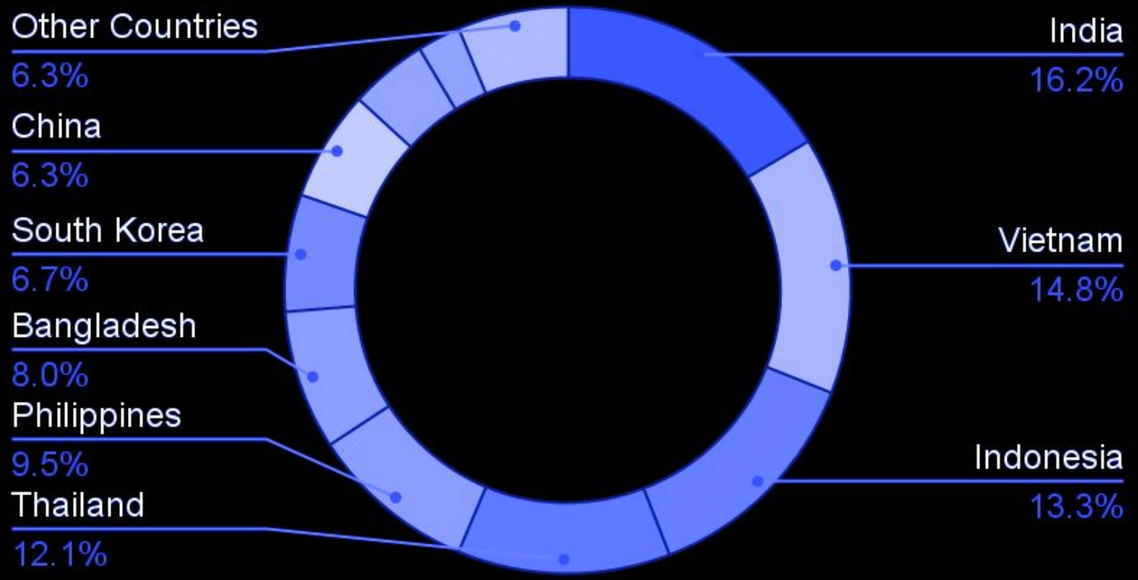
Statistics regarding compromised accounts in September 2025:

- In September 2025, RedLine Stealer was the most dominant malware in APAC, accounting for over half (51.8%) of all compromised accounts, followed by META Stealer (17.1%) and LummaC2 (11.9%).
- India (16.2%), Vietnam (14.8%), and Indonesia (13.3%) 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



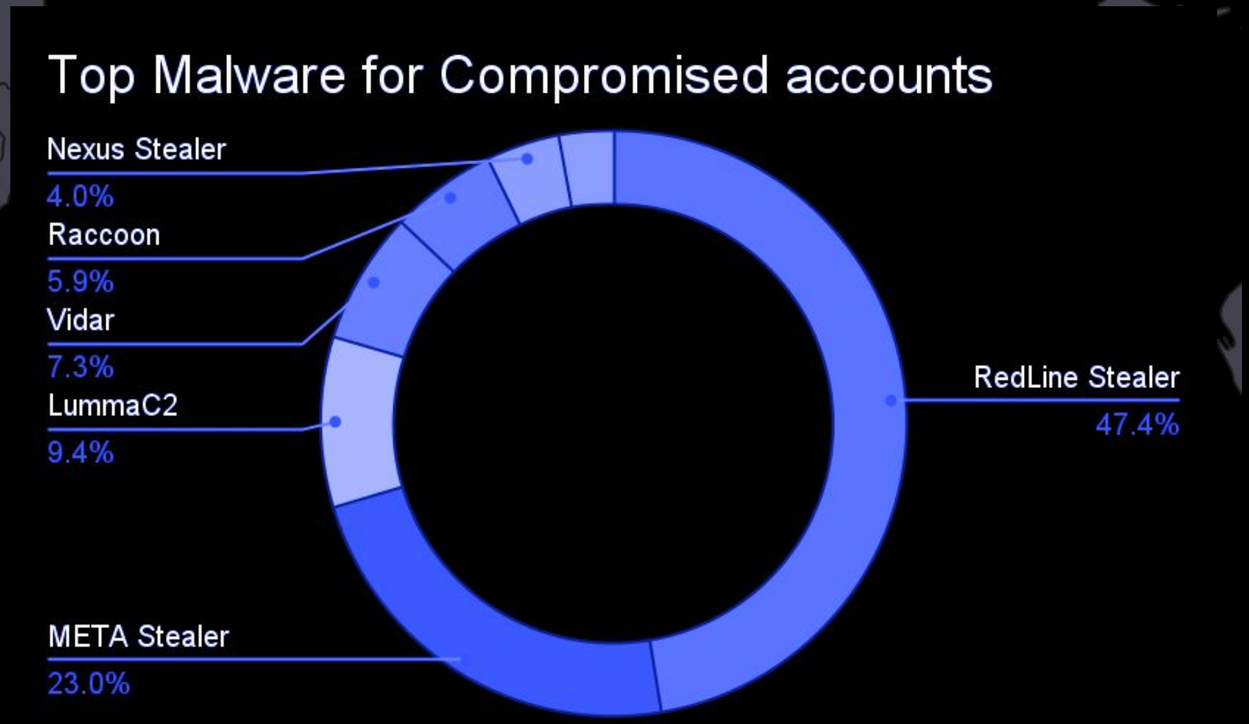
Data: number of events. Each malware can be part of the same event.

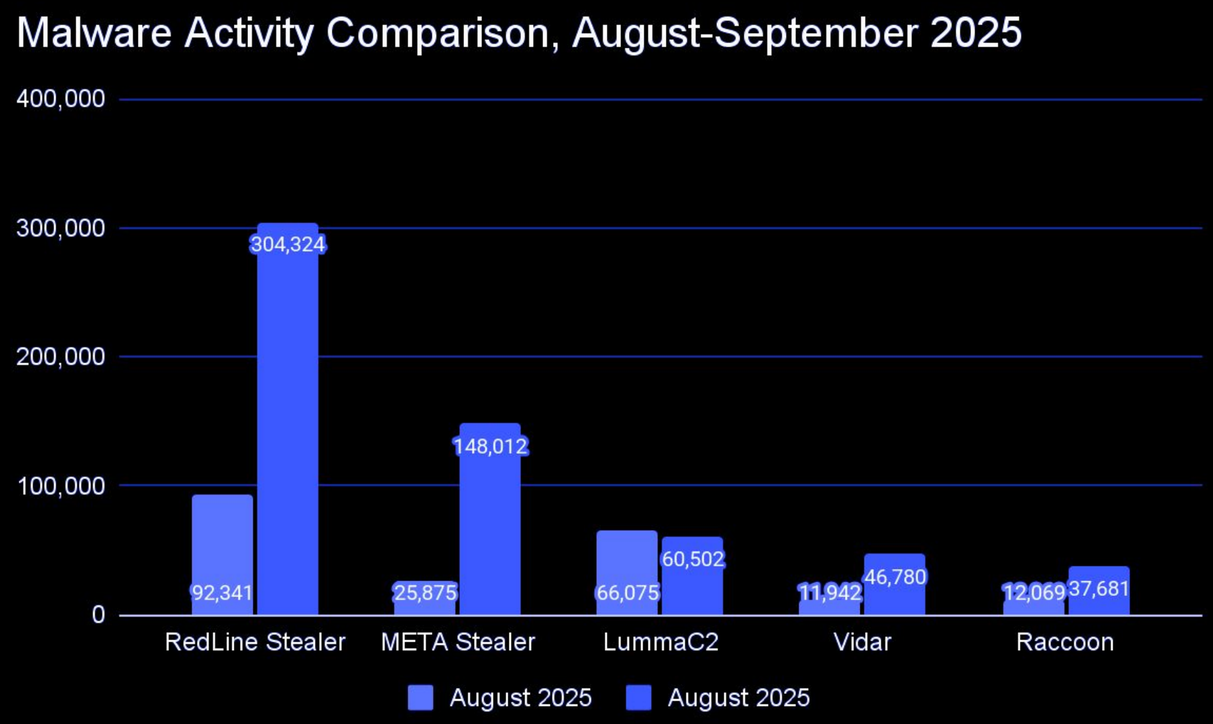
COMPROMISED DATA (Australia) ↑ 60.15%

GROUP-IB

Statistics regarding compromised accounts in September 2025:

- RedLine Stealer, LummaC2 and META Stealer are still the top malware families responsible for nearly 80% of the compromised accounts in Australia during the month.
- Almost all of the data come from Stealer logs cloud, which are distributed mostly via Telegram. Most of the victim's domain are from Roblox, Facebook, Google and Microsoft accounts, following by other services such as Discord, Netflix, Twitch, etc.





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

COMPROMISED BANK CARDS (APAC)

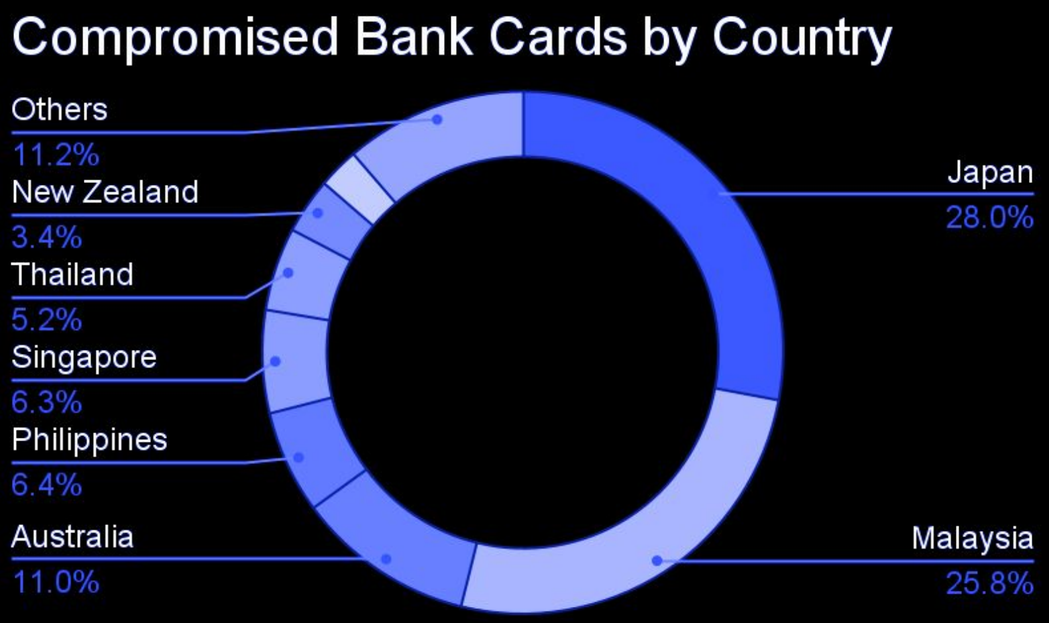
11,305 bank cards leaked

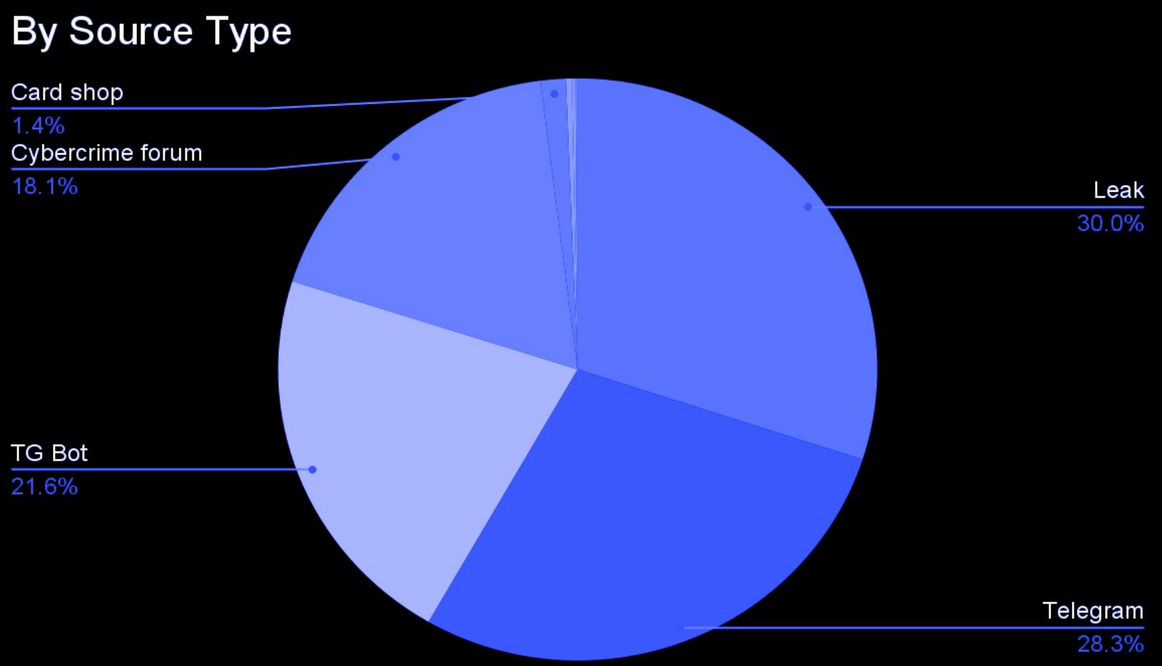
↓ 67.7%

GROUP-IB

Statistics regarding compromised accounts in September 2025:

- Japan (28%) and Malaysia (25.8%) recorded the highest number of compromised bank cards in APAC for September 2025, together accounting for over half of all cases.
- The majority of compromised card data originated from leak sources, Telegram channels, and TG bots, indicating strong activity in illicit data-sharing platforms.





Data: percentage of events

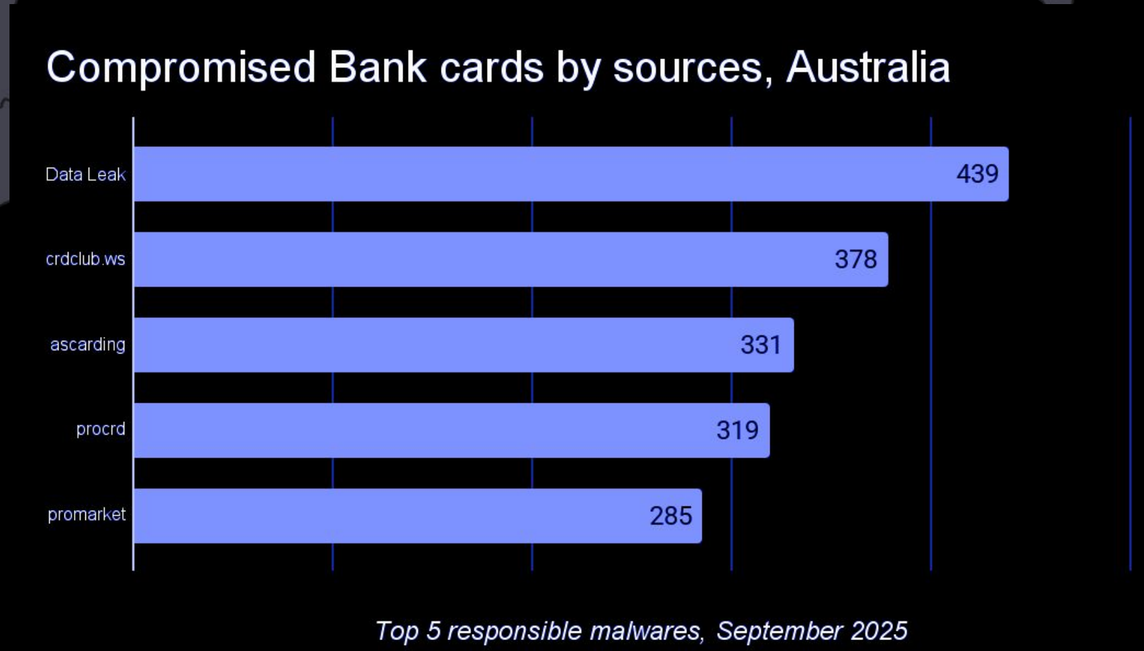
COMPROMISED BANK CARDS (Australia)

↓ 75.34%

GROUP-IB

Statistics regarding compromised accounts in September 2025:

- Despite seeing a decrease compared to last month, **Australia** is still the top 3 country in the region with the highest number of compromised cards during the month.
- Most of the leaks come from info-stealer/scraper, botnet/loader, credential/Credit stealer malwares.
- Over 57% of the compromised card comes from MASTERCARD, followed by VISA (39.98%), with a small amount from American Express, Maestro and JCB.



Top 5 responsible malwares, September 2025

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

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

404NOTFOUNDCYBER

Targeted industries:

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

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

Attack Summary

Cambodian hacktivist threat actor was first seen in July 2025. Became active during the escalation between Thailand and Cambodia

Key Observations

The actor conducts DDoS and defacement attacks on Thai websites and amplifies messages from other Cambodian groups like BL4CK CYB3R, Kxichixxsec.

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

HIME666

Targeted industries:

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

Period of Activity:	April 2025 - Present
Targeted countries:	Worldwide (APAC & ANZ: Indonesia, India, China, Vietnam. Australia, Hong Kong, Japan, Malaysia, Philippines, Singapore, Thailand)
Attribution:	Indonesia
Intent:	Hacktivism

Attack Summary

HIME666 is a hacktivist group based in Indonesia, primarily active on the Telegram channel hxxps://t[.]me/Himenisme666 since April 2025.

Key Observations

So far the actor group targets the Government & Military sector, aiming at elling compromised data, web access of governmental bodies of several countries.

HIGH TECH CRIME TRENDS REPORT

GROUP-IB

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/

APAC Intelligence Insights H1-2025 Review & H2 Forecasts

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

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

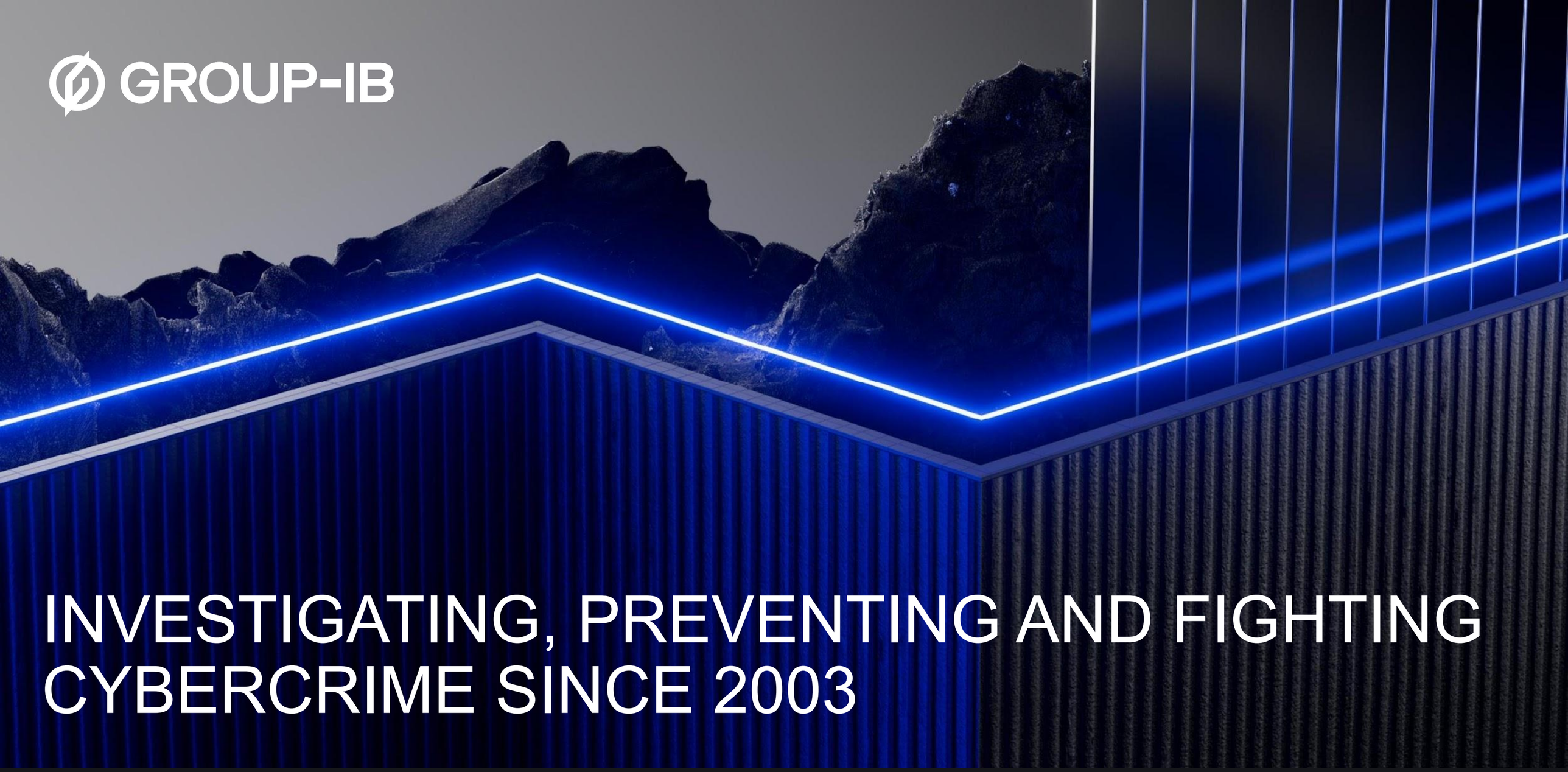
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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