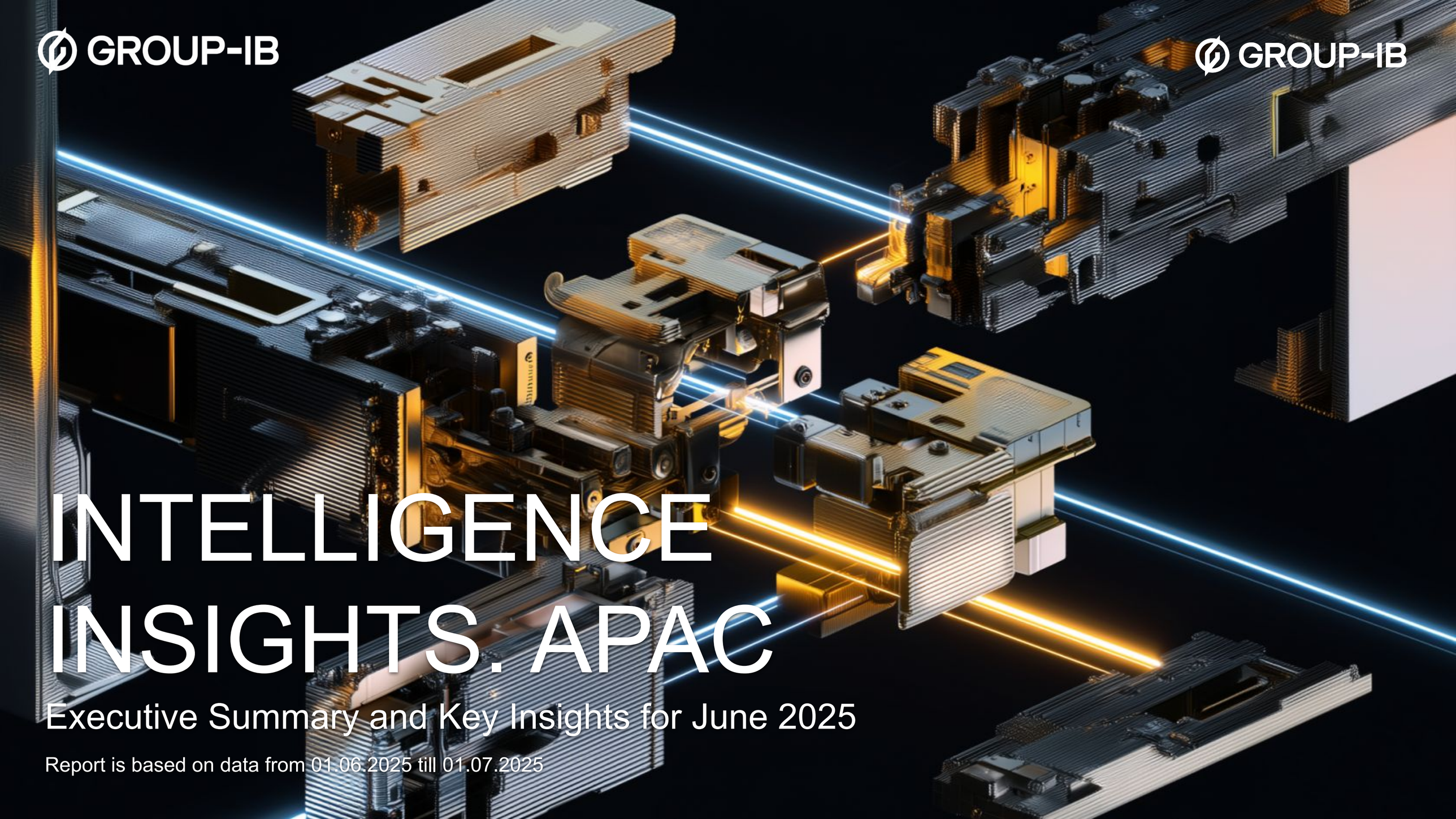


GROUP-IB

GROUP-IB

INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for June 2025

Report is based on data from 01.06.2025 till 01.07.2025

THREAT LANDSCAPE OVERVIEW

GROUP-IB

Ransomware activities

↓ 55.26%

DDoS and Hacktivism

↓ 33.77%

↑ 42.14%

Compromised Accounts

↑ 76.42%

Compromised Bank Cards

Data comparison: May 2025 - June 2025

GLOBAL INSIGHTS

Global Insights from Group-IB with a brief description:

01

Declaration trap: Crypto Drainers masquerading as European Tax Authorities

In early 2025, Group-IB started tracking a crypto drainer scam campaign in Europe that impersonates official tax authorities and tricks users into handing over access to their wallets. This threat primarily targets Dutch residents, impersonating Belastingdienst (the Dutch Tax Authority) and MijnOverheid – the official government portal that provides residents with access to personal records and emails from authorities. Recently, the scope of this cluster has expanded, targeting users beyond the Netherlands. More Information.

02

Middle East Cyber Escalation: From Hacktivism to Sophisticated Threat Operations

In light of the ongoing escalation in the Middle East, Group-IB Threat Intelligence unit has been closely monitoring cyber activity across the full spectrum of threat actors involved in the conflict—ranging from state-nexus operations to hacktivist networks. This report analyzes both the broader hacktivist ecosystem and the critical, advanced operations that pose immediate risks to regional security and civilian safety. It also provides actionable recommendations for organizations seeking to enhance their resilience against these evolving threats. More Information.

03

Phishing campaign targeting apparel, retail and luxury goods companies

The Group-IB TI team detected a new phishing campaign targeting Okta and Microsoft users, which began on June 20th 2025. 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.

04

Group-IB Analyst's Review of the Cybernews Article: “Largest Ever Data Leak Exposes Over 4 Billion User Records”

On June 6, 2025, Cybernews, in collaboration with researcher Bob Dyachenko, published an article titled:
“Largest ever data leak exposes over 4 billion user records.” Cybernews researchers reportedly discovered an unsecured database containing 637 GB of data and 4 billion records from Chinese organizations. More Information.

REGIONAL INSIGHTS

GROUP-IB

Regional Insights from Group-IB with a brief description:

01

Scattered Spider - Possible cyberattack on Qantas

On 30 June 2025, Qantas detected a cyber incident, namely an unusual activity in a third-party customer-service platform used by one of its contact centers. The airline immediately contained the system and confirmed that its core airline and safety operations were not affected. In the statement, Qantas confirmed the breach impacted approximately 6 million customer records. The data includes customer names, email addresses, phone numbers, dates of birth, and frequent-flyer numbers. The company emphasized that no credit-card details, passport data, frequent-flyer login credentials, or passwords were accessed by the attacker. More Information.

02

Admin Access for Sale – Technology Crime Suppression Division (TCSD), 5C Center

On June 17, 2025, a threat actor using the alias ITSUKI posted an offer for sale on Darkforums, advertising administrator access to the “5C Center” portal, which is reportedly linked to the Technology Crime Suppression Division (TCSD) - a specialized cybercrime and digital surveillance unit under the Royal Thai Police. More Information.

03

RAT Pantry: Stocked. Packed. Compromised.

Throughout 2025, Group-IB has been tracking a phishing campaign targeting financial institutions globally, with a significant concentration of activity observed in India. This campaign always begin with phishing emails and leveraged two primary initial attack vectors to infiltrate targeted systems: double extension attachment filenames and the use of malicious SVG files. More Information.

04

Alleged data leak containing personal information of Kazakhstan citizens

A data leak, titled "Жители Казахстана 2024" ("Residents of Kazakhstan 2024"), has been reported, allegedly containing the personal data of 16.3 million Kazakhstani citizens. An analysis of the leaked archive revealed a CSV file with the following data fields: Last Name, First Name, Patronymic, Gender, Date of Birth, Identifier, Individual Identification Number (IIN), Mobile Phone, Work Phone, Home Phone, Citizenship, Nationality, Address, Confirmed Address, and Residency Start and End Dates. More Information

APAC and ANZ

More Information in Group-IB Threat Intelligence Portal

RANSOMWARE ACTIVITIES

↓ 55.26%

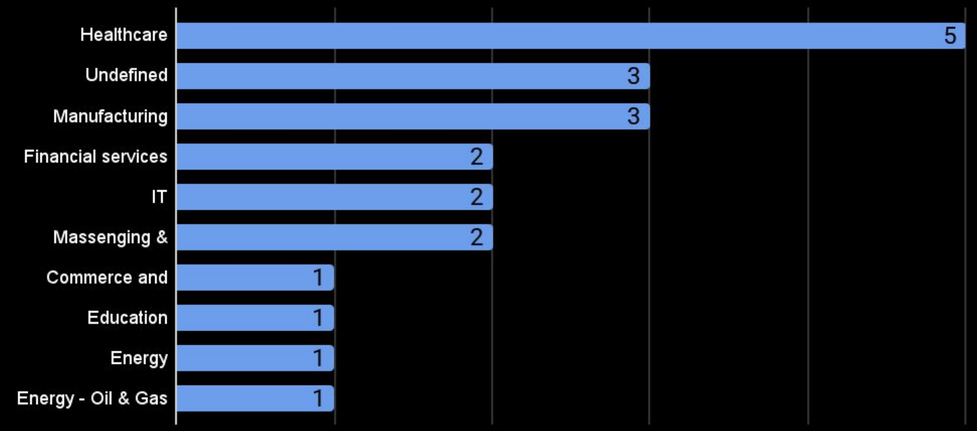
34 ransomware incidents

GROUP-IB

Statistics regarding ransomware activities in June 2025:

- **Healthcare** was the most targeted industry (5 attacks), followed by Manufacturing and Undefined sectors (3 attacks each).
- **Qilin** was the most active threat actor (5 activities), despite a 37.5% decrease in its activity.
- **Australia** experienced the highest number of country-specific attacks (11), though it also saw a 38.89% decline.

Ransomware attacks, per industry, Top 10



Top 10 targeted sectors, June 2025

Most active threat actors

Qilin
5 activities
-37.5%

Direwolf
4 activities
-33.3%

Global
4 activities

Devman
2 activities
-77.8%

Gunra
2 activities

Most targeted Countries

Australia
11 activities
-38.89%

Singapore
5 activities
-44.44%

Thailand
5 activities

India
4 activities

Japan
4 activities
-60%

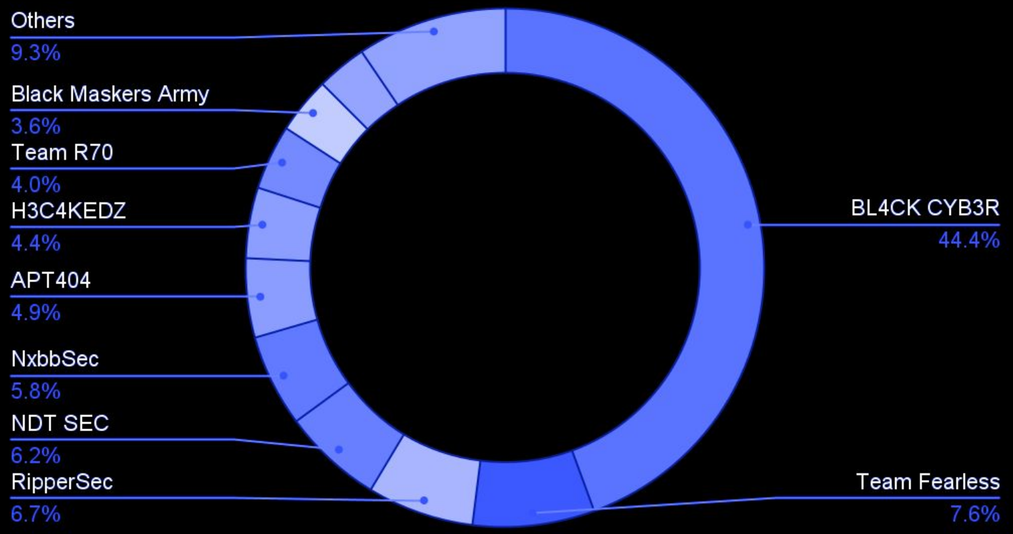
Data: number of not unique events and activities (with updates).

DDOS AND HACKTIVISM

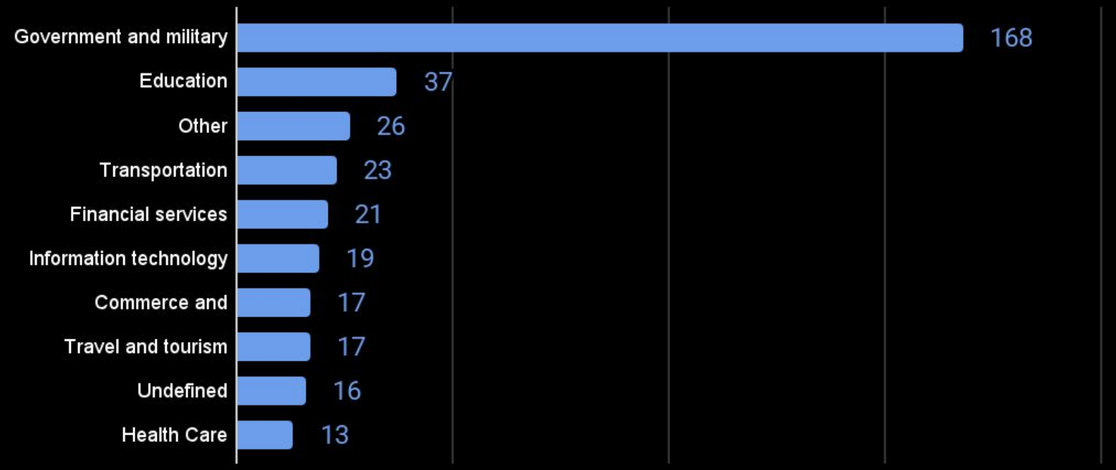
GROUP-IB

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 June 2025:

By Actor



By Industry



Top 10 targeted sectors

Data: number of events.

DDOS AND HACKTIVISM

Number of activities per Country, TOP 6 countries

↓33.77%

Thailand, 144 +323.53%	India, 69 -78.03%	Vietnam, 17 -41.38%
Indonesia, 16 -20.00%	South Korea, 13	Japan, 11

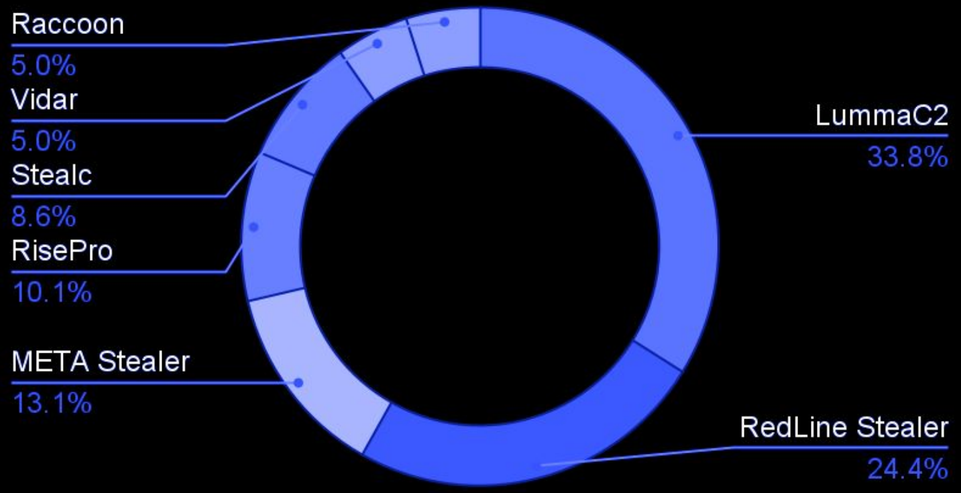
Data: number of events.

COMPROMISED DATA (APAC) ↑ 42.14%

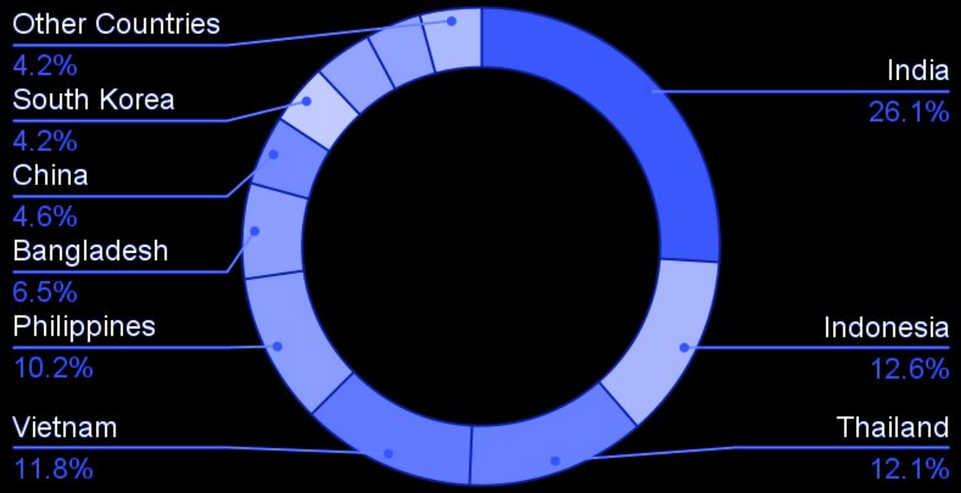
Statistics regarding compromised accounts in June 2025 for APAC:

- In June 2025, **LummaC2** (33.8%) and **RedLine Stealer** (24.4%) were the most prevalent malware types responsible for compromised accounts.
- **India** accounted for the largest share of compromised accounts at 26.1%, followed by **Indonesia** (12.6%) and **Thailand** (12.1%).
- **LummaC2** and **RedLine Stealer** represent over half (58.2%) of all compromised accounts by malware in June.

By Malware, Top 7



By Country



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

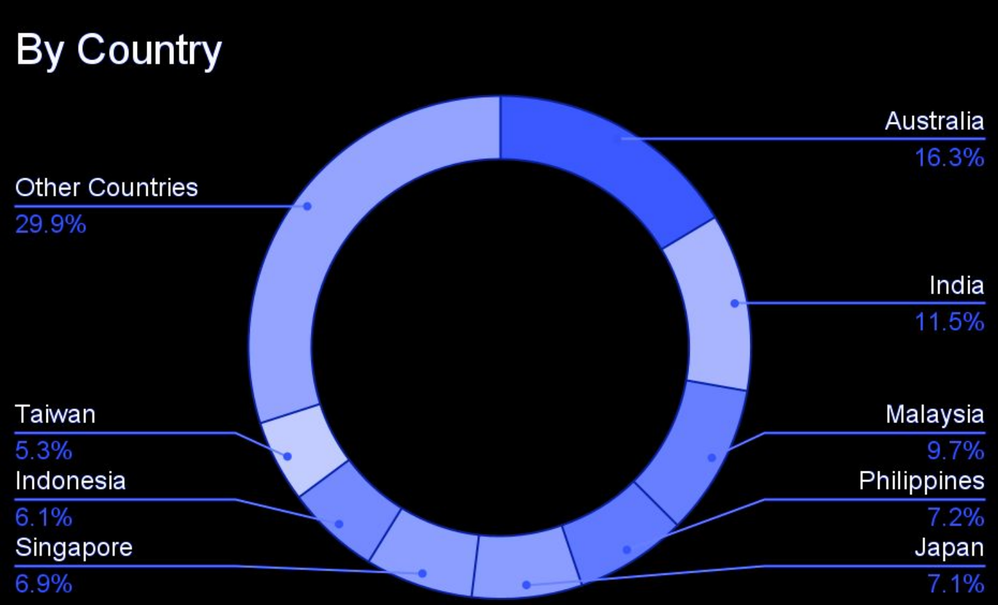
COMPROMISED BANK CARDS (APAC)

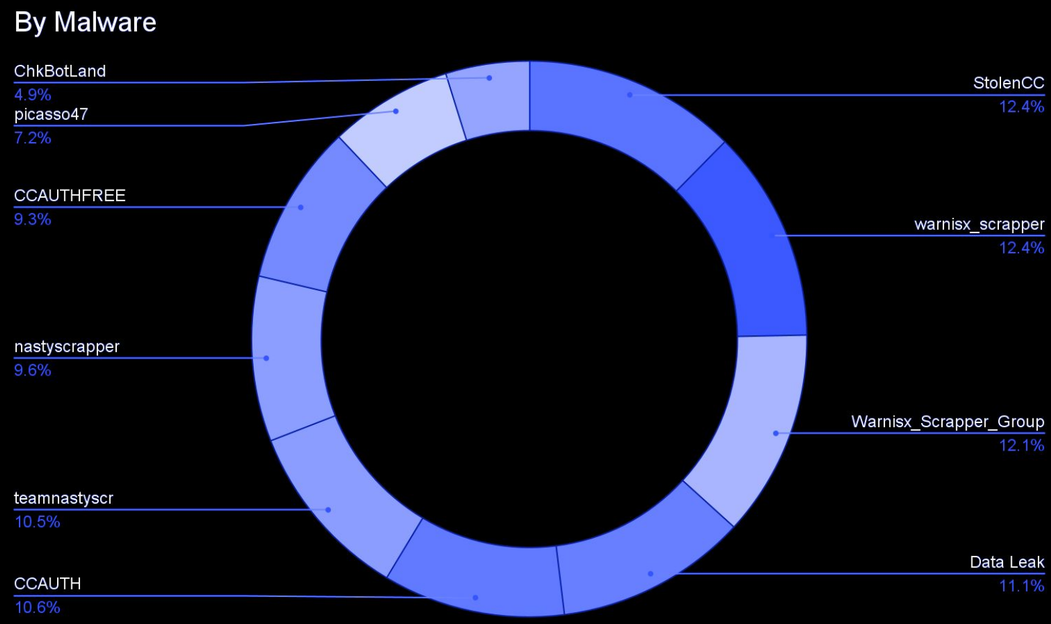
↑ 76.42%

GROUP-IB

Statistics regarding compromised accounts in June 2025:

- **Australia** accounts for the largest share of compromised accounts, representing 16.3% of the total, followed by India at 11.5% and Malaysia at 9.7%.
- Both **StolenCC** and **warnisx_scrapper** are responsible for the highest percentage of compromised bank cards by malware, each contributing 12.4%.
- While a few malware types dominate, a wide range of malware families, including **Warnisx_Scrapper_Group** (12.1%) and **Data Leak**"(11.1%), 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

Scattered Spider

Targeted industries:

- Financial services
- Messaging and telecommunications
- Software
- 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:	May 2025 - Present
Targeted countries:	Worldwide (APAC & ANZ: Australia, India, Singapore, South Korea, Thailand)
Attribution:	United Kingdom
Intent:	N/A

Attack Summary

Scattered Spider is a group originally discovered by CrowdStrike analysts in June 2022. Utilizing phishing and SIM swapping attacks to hijack Microsoft Azure admin accounts and gain access to virtual machines.

The actor abuse the Azure Serial Console to install remote management software for persistence and abuse Azure Extensions for stealthy surveillance. Serial Console in the Azure portal provides access to a text-based console for virtual machines (VMs) and virtual machine scale set instances running either Linux or Windows.
During the attacks they perform Living off the Land attacks (LoTL) tactics.

Key Observations

Their tactics often include SIM swapping attacks followed by the establishment of persistence using compromised accounts. SIM swapping is a type of account takeover fraud that generally targets a weakness in two-factor authentication and two-step verification in which the second factor or step is a text message (SMS) or call placed to a mobile telephone.

Recent public reporting has suggested that threat actors used tactics consistent with Scattered Spider to target retail organization and deploy DragonForce ransomware. Previously they additionally used ALPHV (BlackCat).

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

Team Fearless

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:	June 2025 - Present
Targeted countries:	Worldwide (APAC & ANZ: Vietnam, South Korea, Indonesia, India, Cambodia)
Attribution:	N/A
Intent:	Hacktivism

Attack Summary

Hacktivist group which was first seen on 2 June 2025 on Telegram. Team Fearless was observed to engage in DDoS attacks targeting Israel, Ukraine, Vietnam and other countries.

At the time of writing Team Fearless appears to be more focused on resharing attacks from allegedly affiliated hacktivist groups with similar motivations.

Key Observations

- The group appears to operate motivated by the Israel-Palestine conflict.
- They heavily put a strong focus on disrupting network availability and operations.
- For the data theft, the group frequently leverages web-based channels to extract compromised information.

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

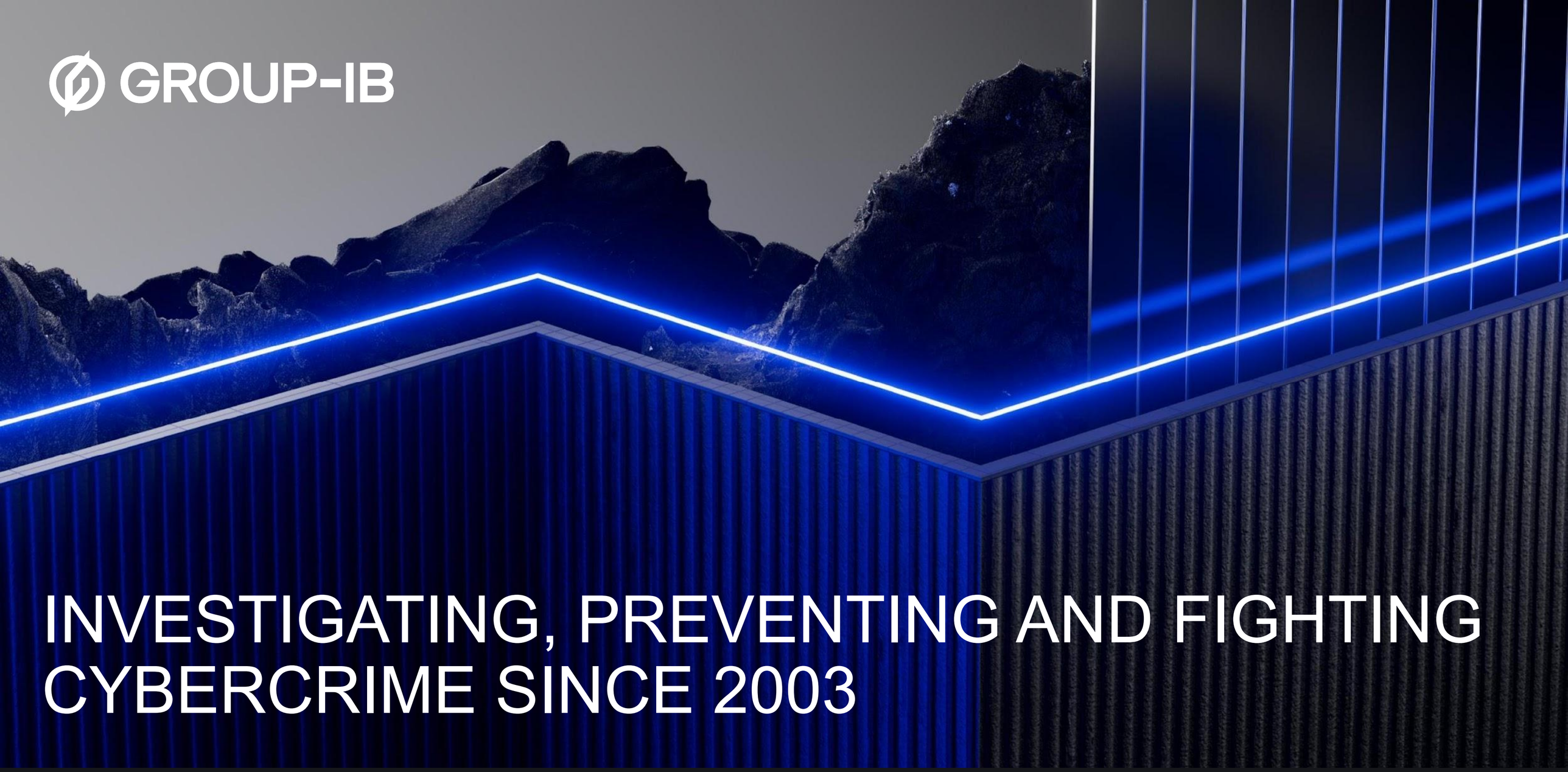
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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