GROUP-IB

GROUP-IB

INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for August 2025

Report is based on data from 01.08.2025 till 01.09.2025

THREAT LANDSCAPE OVERVIEW

GROUP-IB

Ransomware activities

↑ 62.5%

DDoS and Hacktivism

↑ 6.25%

↑ 9.0%

Compromised Accounts

↓ 44.55%

Compromised Bank Cards

Data comparison: July 2025

GLOBAL INSIGHTS

Global Insights from Group-IB with a brief description:

01

The Anatomy of a Deepfake Voice Phishing Attack

Deepfake vishing is growing due to cheap AI tools, abundant voice samples, and weak defenses like caller ID or biometrics. It uses AI-cloned voices to trick victims into sending money or disclosing sensitive data. Common targets include executives, finance staff, and the elderly, with scammers posing as banks, officials, leaders, or family to create urgency. More Information.

02

Exposing Investment Scams: AI Trading, Deepfake & Online Fraud

AI trading scams are on the rise, using deepfake videos, fake reviews, and social media campaigns to promote fraudulent platforms that promise easy profits. These schemes trick victims into depositing money and handing over sensitive personal documents. More Information.

03

Evolving Mule Tactics in the META Region Banking Sector

Mule operators in the META region have rapidly evolved from basic VPN obfuscation to advanced tactics such as SIM abuse, GPS spoofing, SIM-removal, and even physical device “muling,” where preconfigured phones are shipped across borders. These layered schemes use both willing and unwitting participants, blending digital fraud with real-world logistics to bypass traditional defenses. More Information.

04

Trust issues: How email threats hide behind your partners

Email threats has bypassed traditional defenses by hijacking trusted accounts and using AI to craft flawless messages delivering stealthy infostealers. These attacks evade reputation checks, content analysis, standard antivirus or URL scanning, making conventional tools dangerously misleading. More Information.

05

ShadowSilk: A Cross-Border Binary Union for Data Exfiltration

Group-IB uncovered an ongoing campaign by ShadowSilk, active since 2023 and targeting government organizations in Central Asia and APAC. The group overlaps with YoroTrooper in infrastructure and tools but appears to consist of Russian and Chinese speaking operators, using exploits, penetration-testing tools, dark web–sourced web panels. Despite exposure recently, ShadowSilk rebuilt infrastructure, continues leveraging Telegram bots and PowerShell, and remains highly active as of July 2025. More Information.

06

Campaign targeting Salesforce instances via Salesloft Drift application

Learn more about the update of the data exfiltration campaign targeting Salesforce instances via Drift. The threat actor breached Salesloft’s GitHub, exfiltrated repository data, and also accessed Drift’s AWS and stole OAuth tokens for customer integrations. Possibly over 700 organizations were affected. More Information.

REGIONAL INSIGHTS

GROUP-IB

Regional Insights from Group-IB with a brief description:

01

APT MuddyWater Deploys Multi-Stage Phishing to Target CFOs

A global spear-phishing campaign is targeting CFOs and finance executives, using fake Rothschild & Co recruitment lures and Firebase-hosted phishing pages to deploy remote-access tools like NetBird for persistent control. The attackers employ custom CAPTCHAs, malicious VBS scripts, and multi-stage payloads to evade detection. Infrastructure overlaps link the activity to APT MuddyWater, highlighting an evolving, highly targeted intrusion set. More Information.

02

Fortinet SSL VPN brute-forcing incidents

Learn about the brute-forcing tactics in the recent incident targeting Fortinet SSL VPNs and FortiManager. The campaign targeted many countries, including Hong Kong, Japan, etc. More Information.

03

Recent update of UNC6040 Salesforce Focused Vishing Data Theft and Exfiltration Techniques

We have continued to monitor and analyze UNC6040 which can be classified as part of ShinyHunters' activities. It targeted Salesforce environments through voice phishing and convinced victims to approve a malicious connected application in the Salesforce portal, leading to data exfiltration. More Information.

04

HomeLandJustice campaign targeting global governments

Iranian-aligned Homeland Justice operators used a compromised Oman MFA mailbox to launch spear-phishing attacks impersonating diplomatic emails. Malicious attachments deployed smalware for persistence and DNS manipulation. The campaign, tied to geopolitical tensions, leveraged 100+ compromised accounts and VPN-masked infrastructure to target global government entities, including Japan, Korea, Thailand, Bangladesh, etc. More Information

05

Hacktivists at War: The Cambodia–Thailand Cyber Escalation

Due to the political tension between Cambodia and Thailand, series of cyberattacks have emerged from a large number of hacktivist groups. Learn more about the overview of hacktivism activities during the past month, their attack techniques and especially Group-IB's recommendations against the threats caused from this conflict. More Information

APAC and ANZ

More Information in Group-IB Threat Intelligence Portal

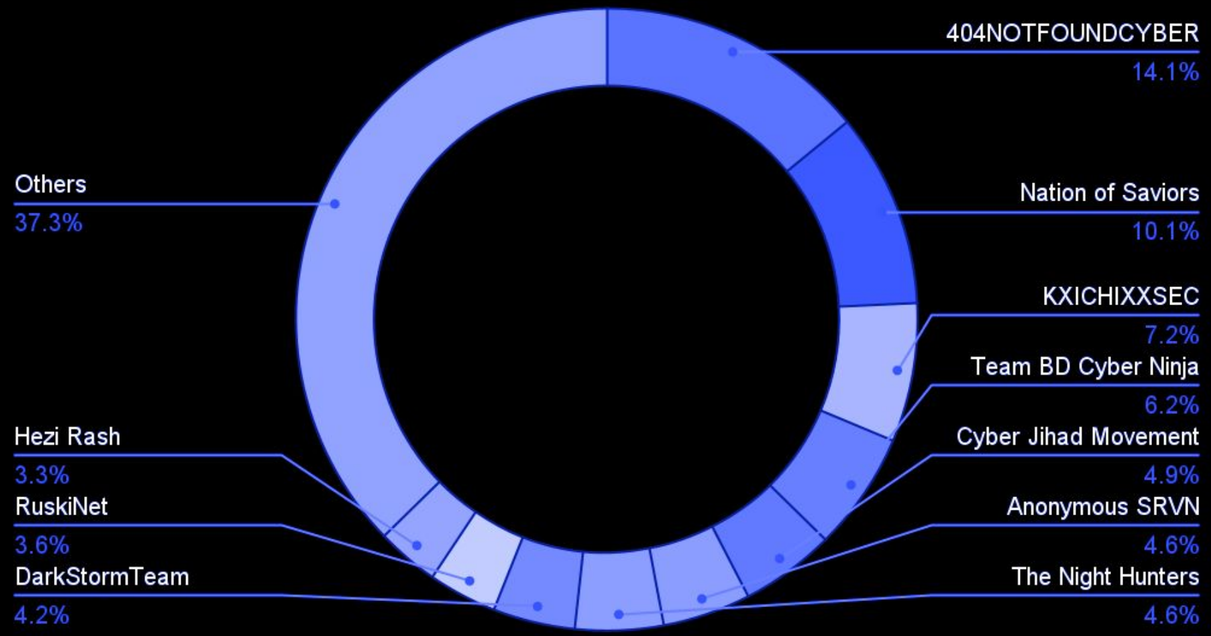
DDOS AND HACKTIVISM

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 during the previous month, the threat landscape is very different from the previous month, along with the top 10 targeted sectors in August 2025.

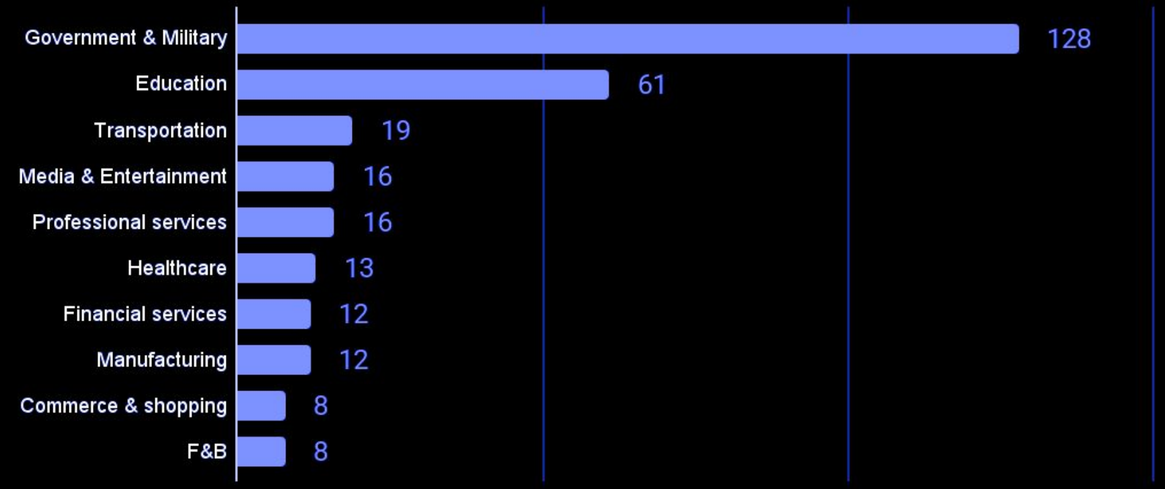
Due to the tension between some countries in the region, the top active actors continue to be mostly the ones motivated by the conflict and target the Government & Military sector. More information about each actor and its activity can be found on Group-IB Threat Intelligence Portal.

DDOS and Hacktivism Activities, per group

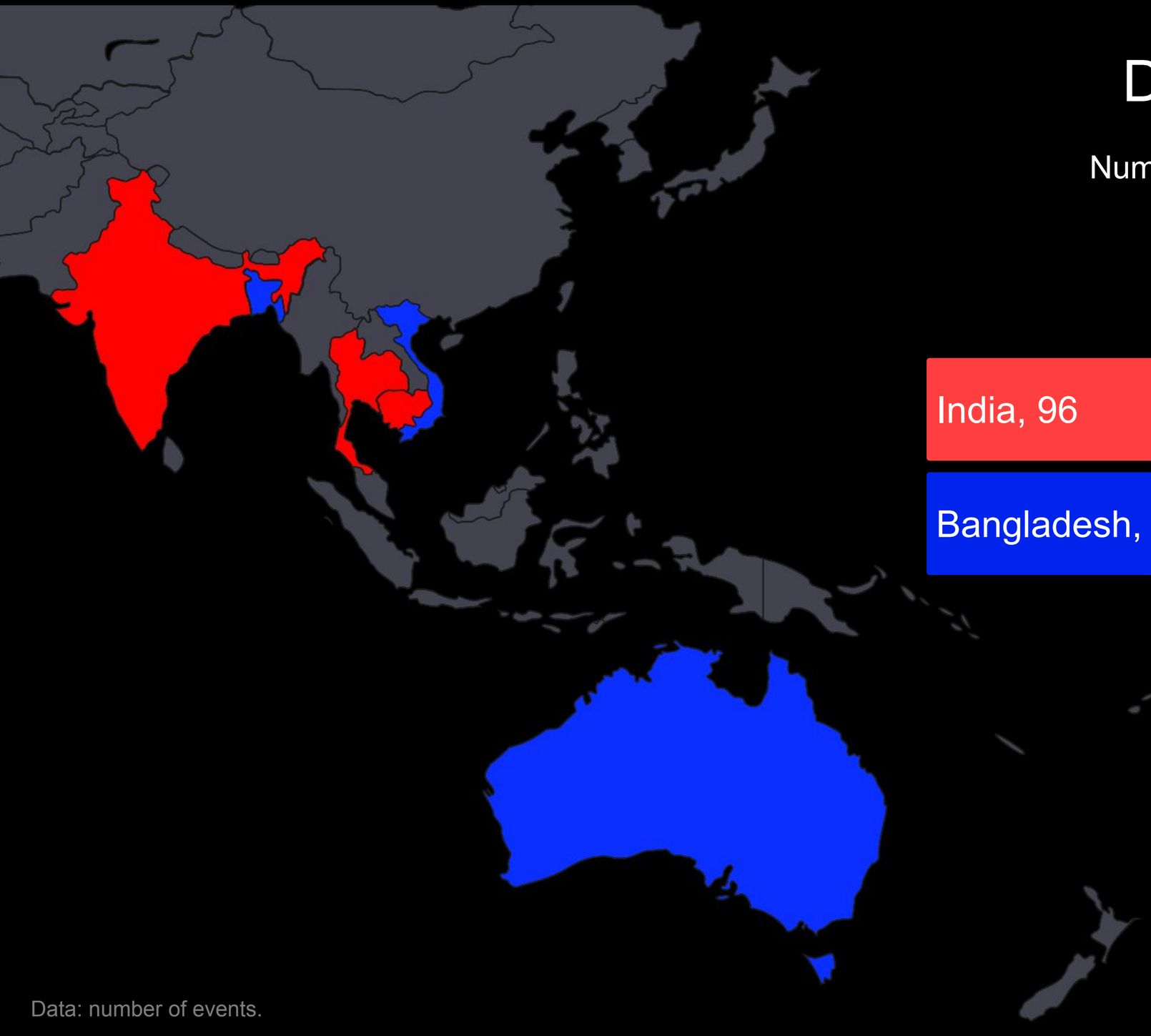


Data: number of events.

DDOS and Hacktivism Activities, per industry



Top 10 targeted sectors, August 2025



DDOS AND HACKTIVISM

Number of activities per Country, TOP 6 countries

↑ 6.25%

India, 96	Thailand, 91	Cambodia, 31
Bangladesh, 29	Australia, 18	Vietnam, 14

Data: number of events.

RANSOMWARE ACTIVITIES ↑ 62.5%

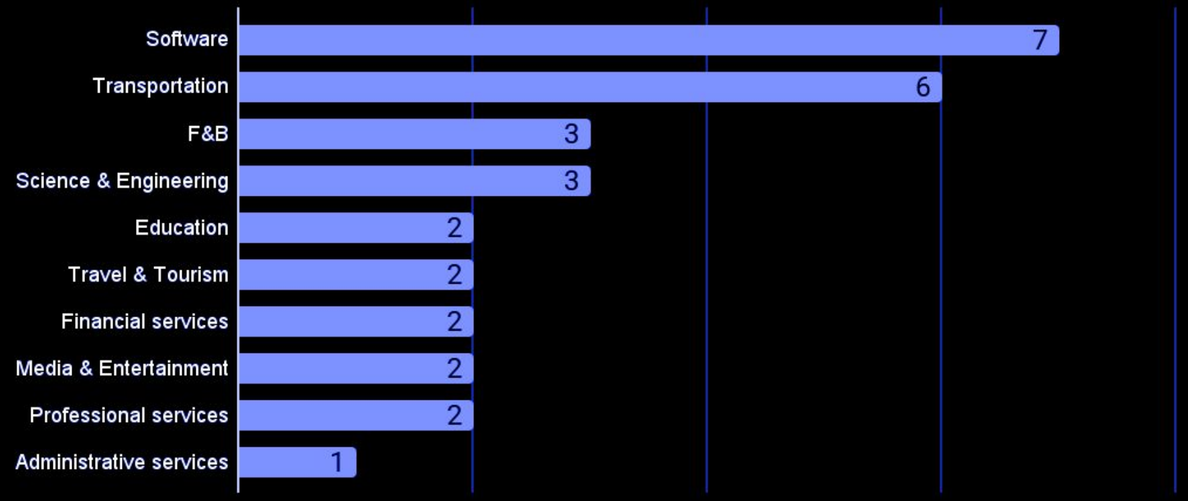
GROUP-IB

39 ransomware incidents

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 Software, Transportation, F&B.

Ransomware attacks, per industry



Top 10 targeted sectors, August 2025

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

Most active threat actors

Qilin
8 activities
+100%

J group
5 activities

Cl0p
3 activities

Dire Wolf
3 activities

DragonForce
3 activities

Most targeted Countries

Australia
7 activities
+0%

India
7 activities
+200%

Japan
5 activities
+66.7%

South Korea
5 activities

Malaysia
4 activities
+100%

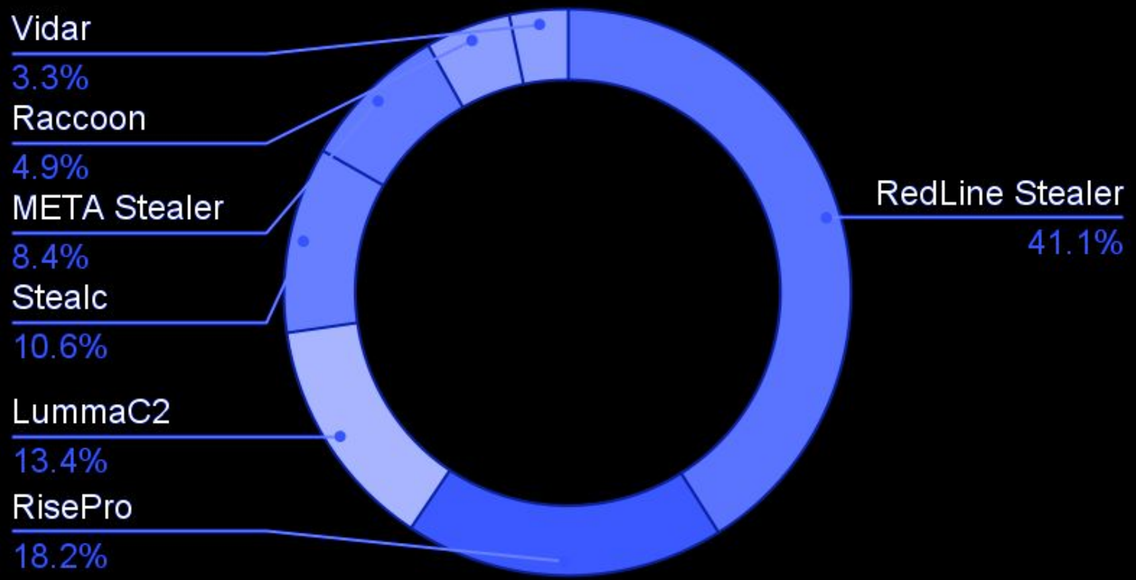
COMPROMISED DATA ↑ 9.0%

GROUP-IB

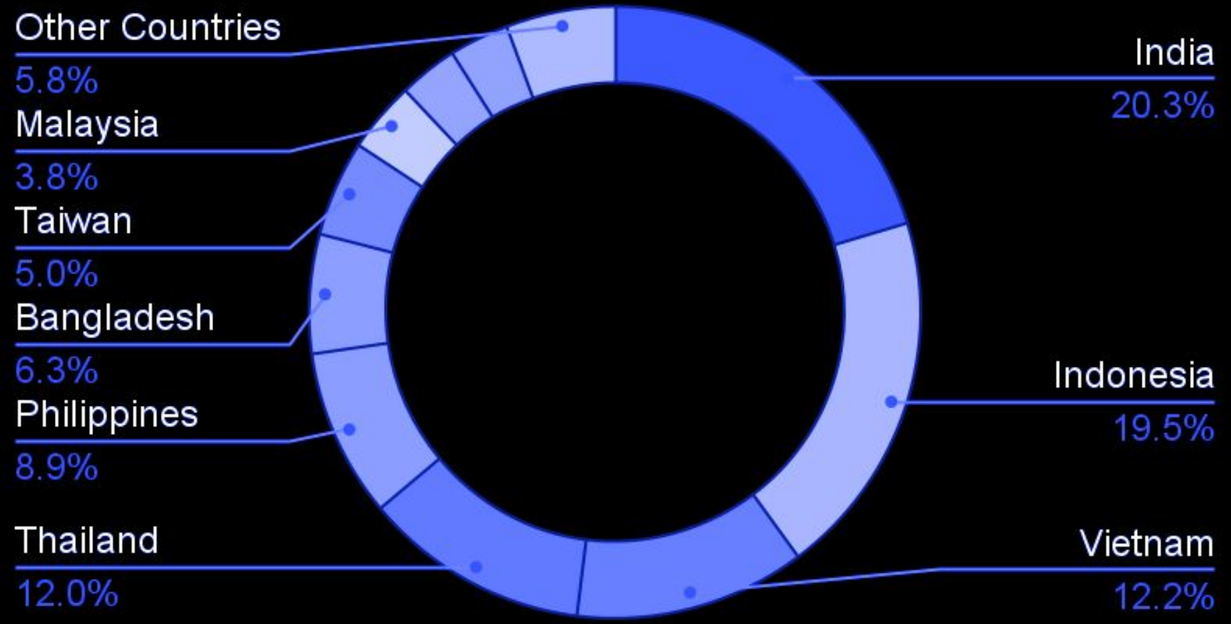
Statistics regarding compromised accounts in August 2025:

- The compromised data in August saw a slight increase compared to last month. Technical controls and security hygiene should still 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.
- Almost all of the data come from Stealer logs cloud, which are distributed mostly via Telegram. Most of the victim's domain are from Google accounts, Facebook and Roblox.

Compromised Accounts by Malware



Compromised Accounts by Country



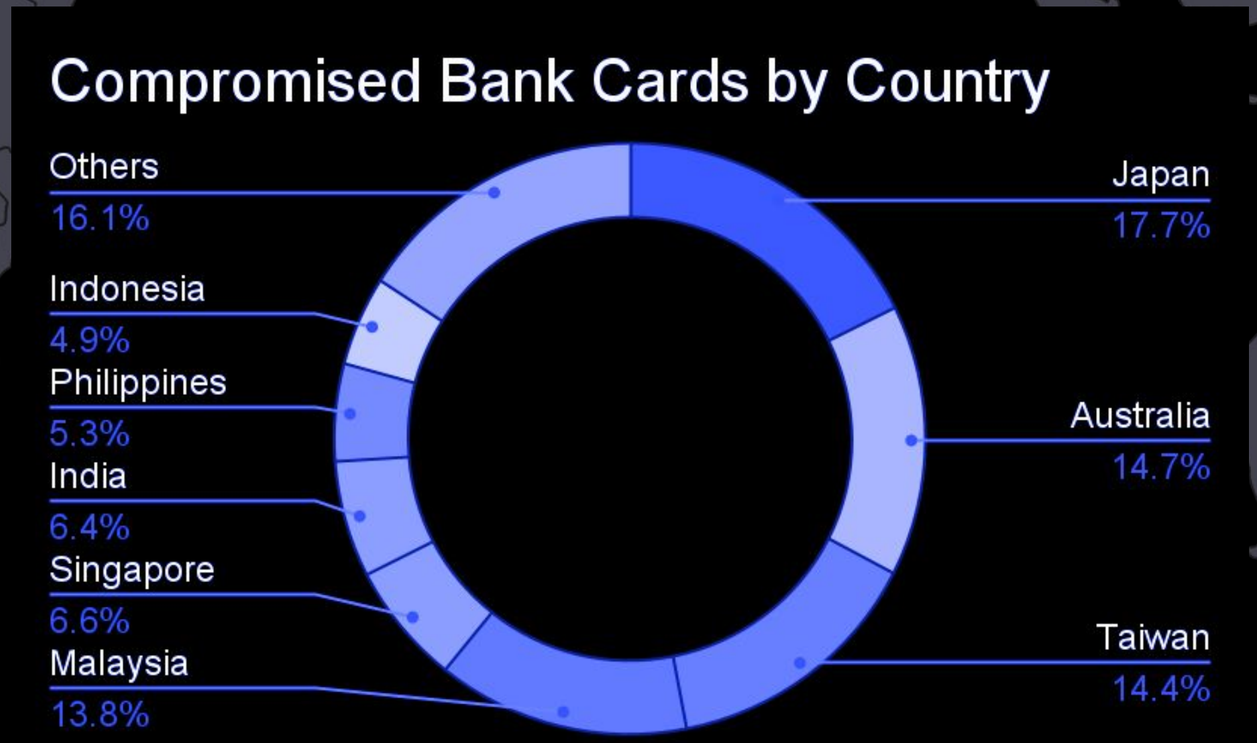
Data: number of events. Each malware can be part of the same event.

COMPROMISED BANK CARDS ↓ 44.55%

GROUP-IB

Statistics regarding compromised accounts in August 2025:

- The decrease in compromised bank cards from the region during the month also came with a slight change in top affected countries, with Japan having the highest number of incidents, followed by Australia, Taiwan and Malaysia.
- Main sources of information - data leaks from Telegram, mostly due to info-stealer/scraper, botnet/loader, credential/Credit stealer malwares, 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

MuddyWater

Targeted industries:

Hardware
Telecommunications
Government & Military
Education
Transportation
Energy
IT
Financial services
Manufacturing
Travel & Tourism
Financial services
Healthcare
Real estate
Professional services
Travel & Tourism

Period of Activity:	February 2017 - Present
Targeted countries:	Worldwide (APAC & ANZ: Australia, Indonesia, Cambodia, Singapore, Thailand, Vietnam, Laos)
Attribution:	Iran
Intent:	Financially motivated

Attack Summary

MuddyWater, or TA450 and Seedworm, is a sophisticated threat actor group believed to be state-sponsored by the Iranian Ministry of Intelligence and Security (MOIS).

Key Observations

This actor group are observed to be long-term persistence and frequently refreshes their tools. They primarily use spear phishing, exploits, malware distribution via phishing emails.

ADVERSARY OF THE MONTH

GROUP-IB

Threat actor group

BIGBROTHER

Targeted industries:

Government and Military

Period of Activity:	July 2025 - Present
Targeted countries:	Worldwide (APAC & ANZ: India, Malaysia, Indonesia, Philippines, Thailand)
Attribution:	N/A
Intent:	Financially motivated

Attack Summary

This threat actor was first seen at the end of July 2025 on Darkforums.

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

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

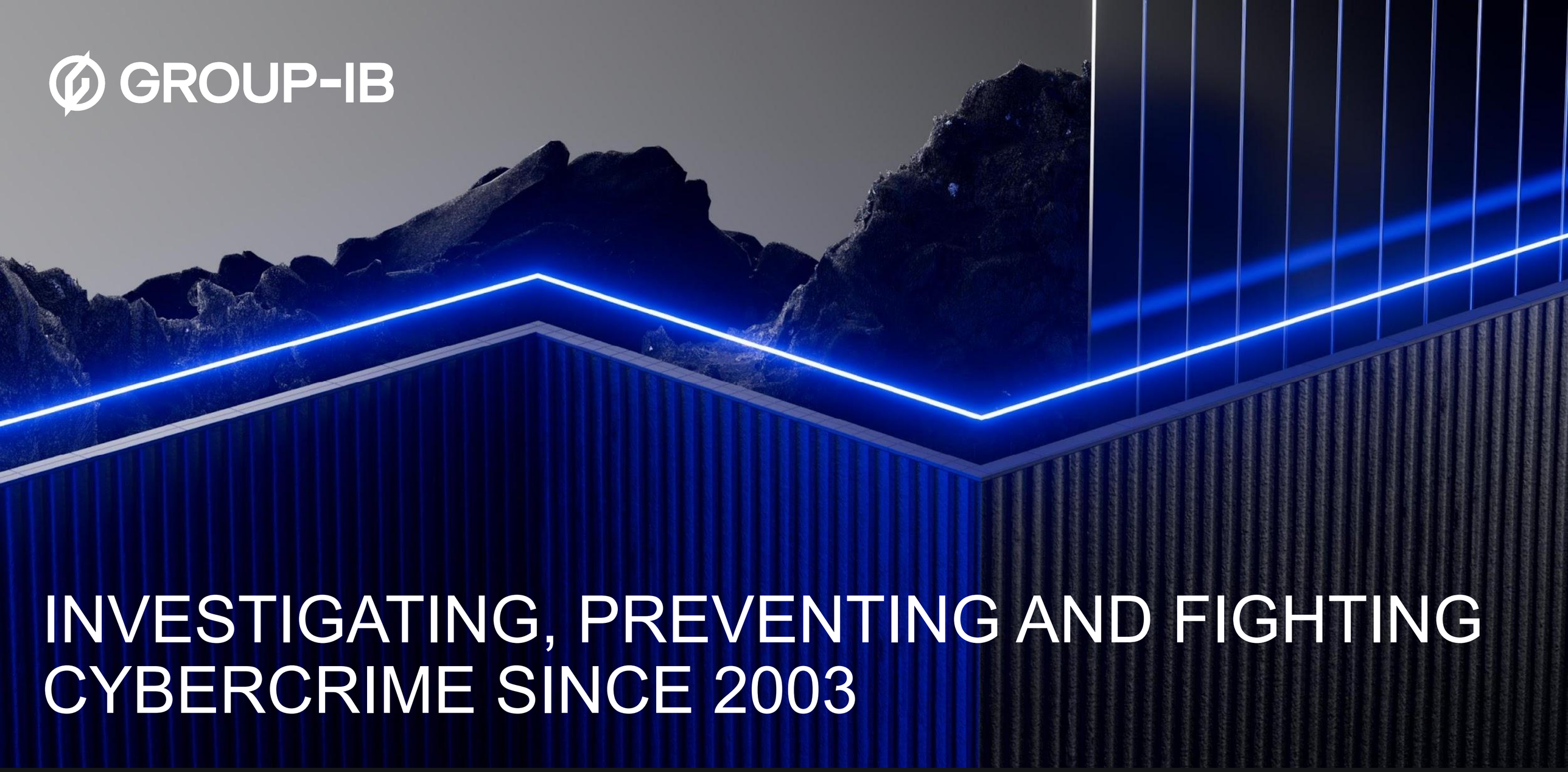
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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