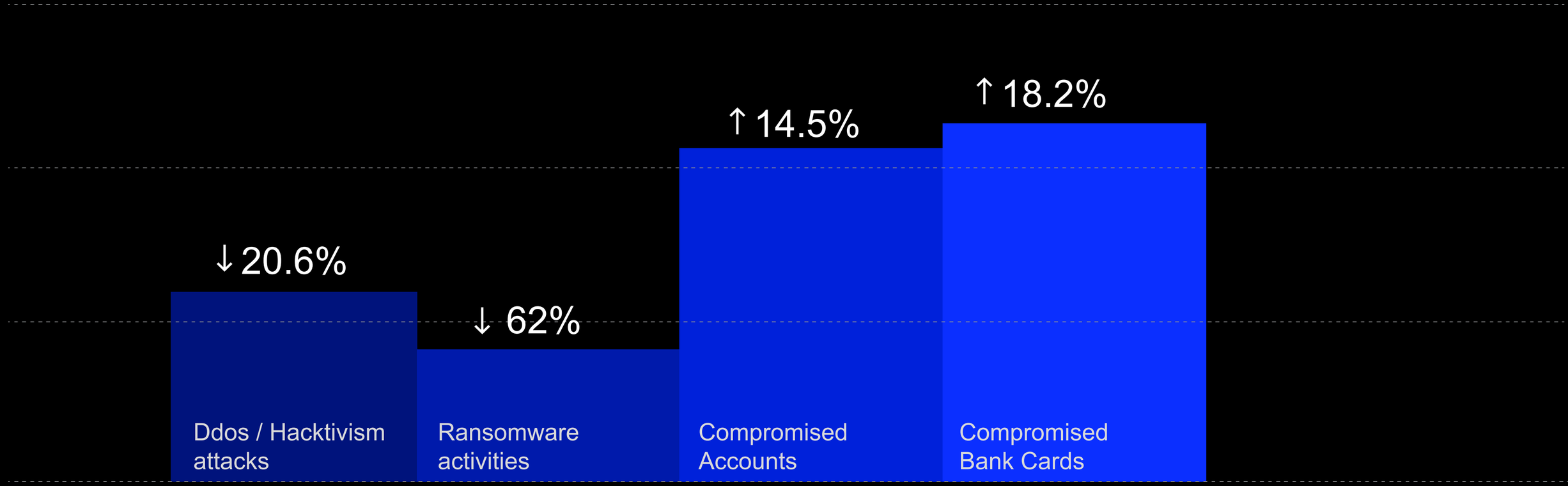
INTELLIGENCE INSIGHTS. APAC

Executive Summary and Key Insights for February 2025

Report is based on data from 01.02.2025 till 01.03.2025

THREAT LANDSCAPE OVERVIEW



Data comparison: January 2025 - February 2025

GLOBAL TRENDS

GROUP-IB

Global Trends from Group-IB with a brief description:

01

Group-IB’s High-Tech Crime Trends Report 2025 exposes how global events fuel regional and local threats.

We’ve launched our highly anticipated High-Tech Crime Trends Report 2025, offering a comprehensive analysis of the evolving cyber threat landscape. The report highlights how state-sponsored espionage, ransomware, underground marketplaces, and AI-driven cybercrime are feeding into one another, creating a self-sustaining cycle of digital threats.
More Information.

02

The Dark Side of Automation and Rise of AI Agents: Emerging Risks of Card Testing Attacks.

Card testing attacks exploit stolen credit card details through small, unnoticed purchases to verify active cards for larger fraud. Cybercriminals use bots, proxies, and automation to evade detection, making real-time fraud prevention challenging. Learn how these attacks work and how to protect against them.
More Information.

REGIONAL TRENDS

GROUP-IB

Regional Trends from Group-IB with a brief description:

01
Group-IB contributes to joint operation of **Royal Thai Police and Singapore Police Force leading to arrest of cybercriminal behind more than 90 data leaks worldwide**. More Information.

02
RansomHub Never Sleeps Episode 1: The evolution of modern ransomware
Modern groups exploit unpatched vulnerabilities, use advanced reconnaissance techniques, and leverage automation to scale their operations. In this first part of a trilogy of Group-IB blogs on ransomware, we'll deep-dive into RansomHub, which emerged in early 2024, and how it exemplifies this evolution. Through innovation and rapid adaptation, this RaaS group has solidified its position as a significant threat in today's cybersecurity landscape. More Information.

03
Recent malicious campaigns with KamiKakaBot targeted financial organizations in Vietnam
Group-IB specialists during the investigation discovered several malicious archives with previously known malicious tool belonging to APT Dark Pink. The archive contains 3 files. Instead of traditionally using a legal executable with a malicious DLL that launches using DLL sideloading technique, cybercriminals use a malicious LNK file that infects target machines when victims double-click it. As a result, KamiKakaBot was launched.
More information in Group-IB Threat Intelligence.

04
HIZBULLAH CYB3R team, RipperSec threat actors attacking and continuously reporting data leaks targeting government institutions and companies in Malaysia.
KillSec ransomware threat actor continue ransomware attacks targeting companies in India.
More information in Group-IB Threat Intelligence.

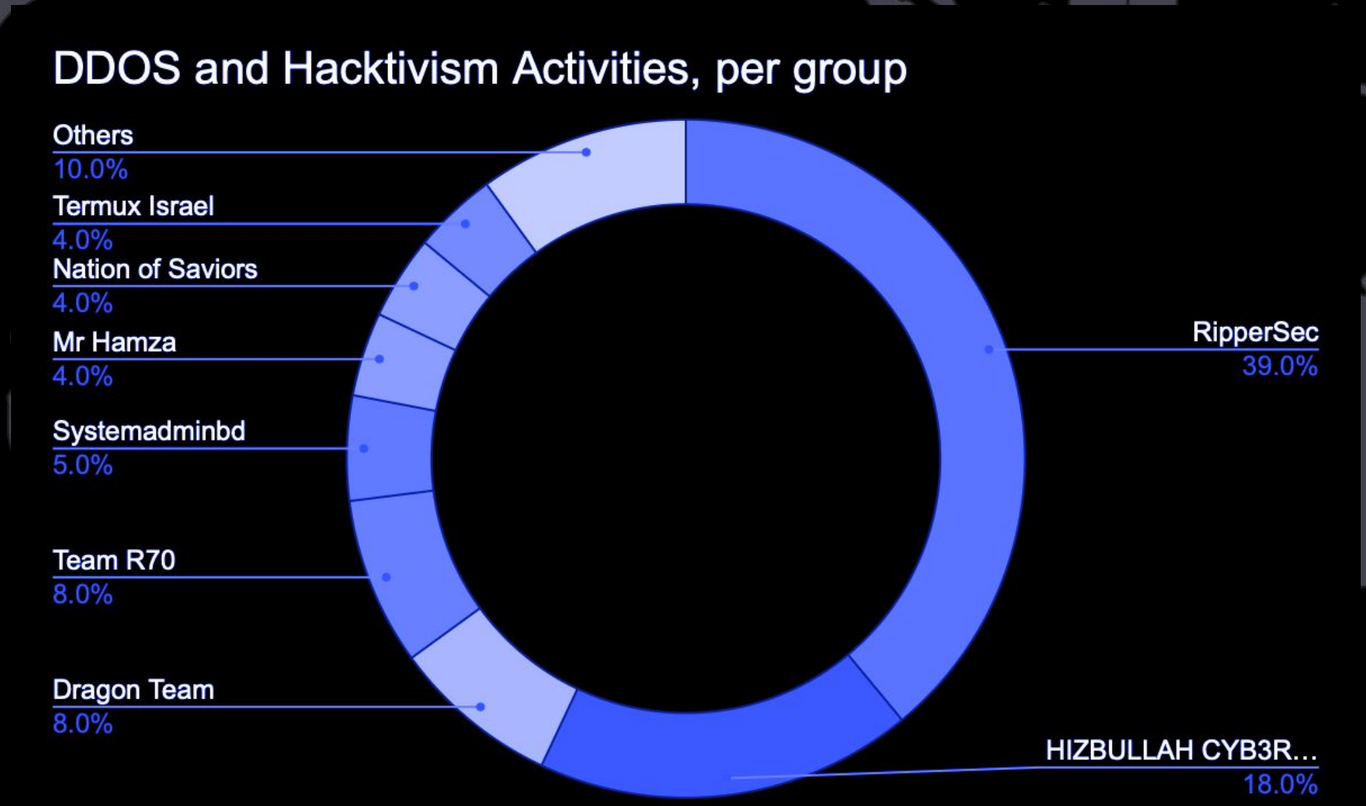
APAC and ANZ

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 region during the previous month:

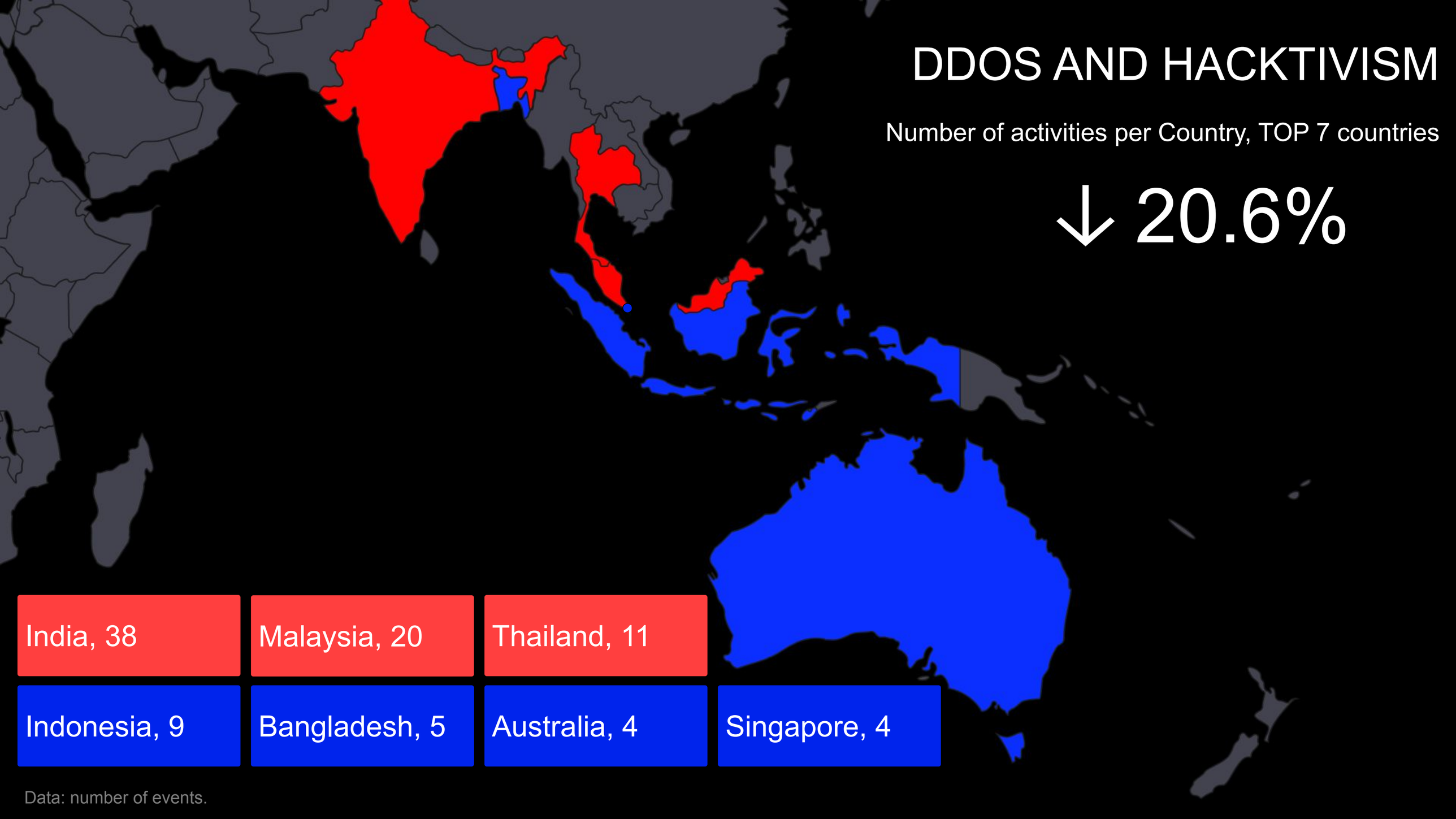


Data: number of events.

DDOS AND HACKTIVISM

Number of activities per Country, TOP 7 countries

↓ 20.6%



Data: number of events.

RANSOMWARE ACTIVITIES

↓ 62.5%

54 Ransom activities

GROUP-IB

Most active threat actors

KillSec

16 activities
-11.1%

APT73

6 activities
- 33.3%

RansomHub

5 activities
-28.6%

Space Bears

5 activities
-66%

Lynx

4 activities

Most targeted Countries

India

15 activities
-65.91%

Japan

8 activities
-20%

Australia

7 activities
-68.18%

Singapore

5 activities
-68.75

Malaysia

4 activities
-20%

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

COMPROMISED DATA ↑ 14.5%

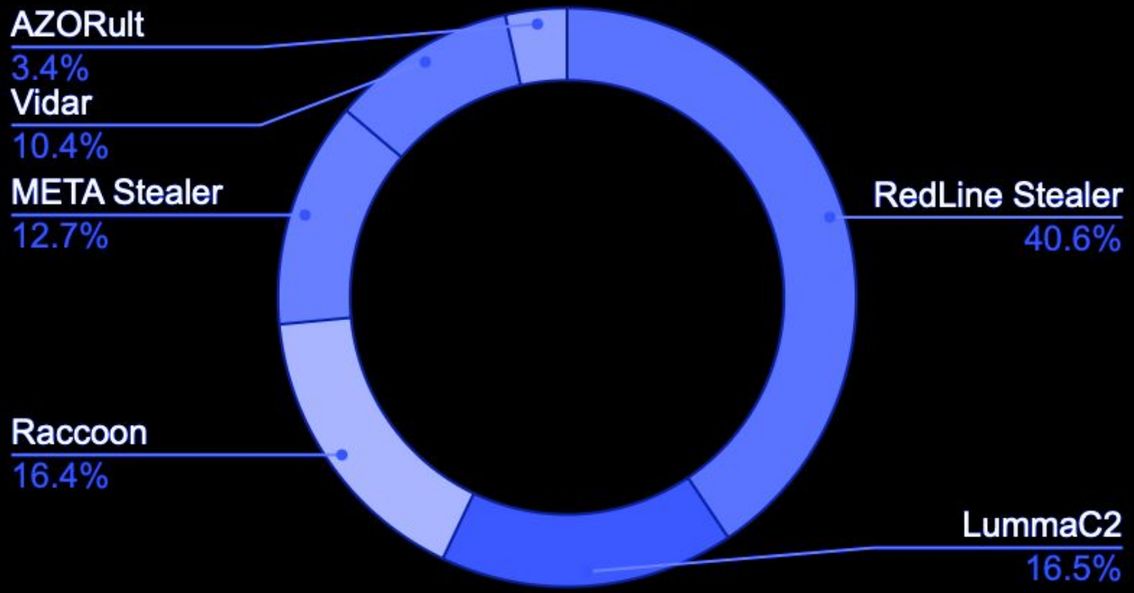
GROUP-IB

Statistics regarding compromised accounts.

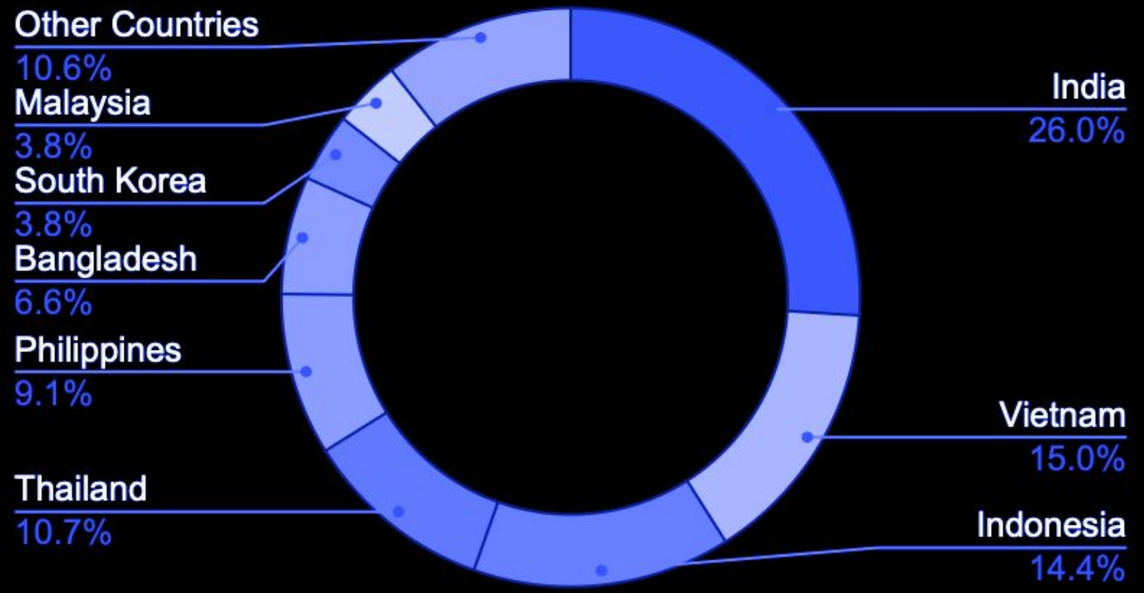
Key Trends in February 2025:

- Further increase of the number of compromised data in APAC compared to January 2025.
- India, Vietnam and Thailand - consistently high numbers of compromised data in previous months, as well as in February
- RedLine stealer, LummaC2 and Raccoon - Most popular tools among others.

Compromised Accounts by Malware



Compromised Accounts by Country



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

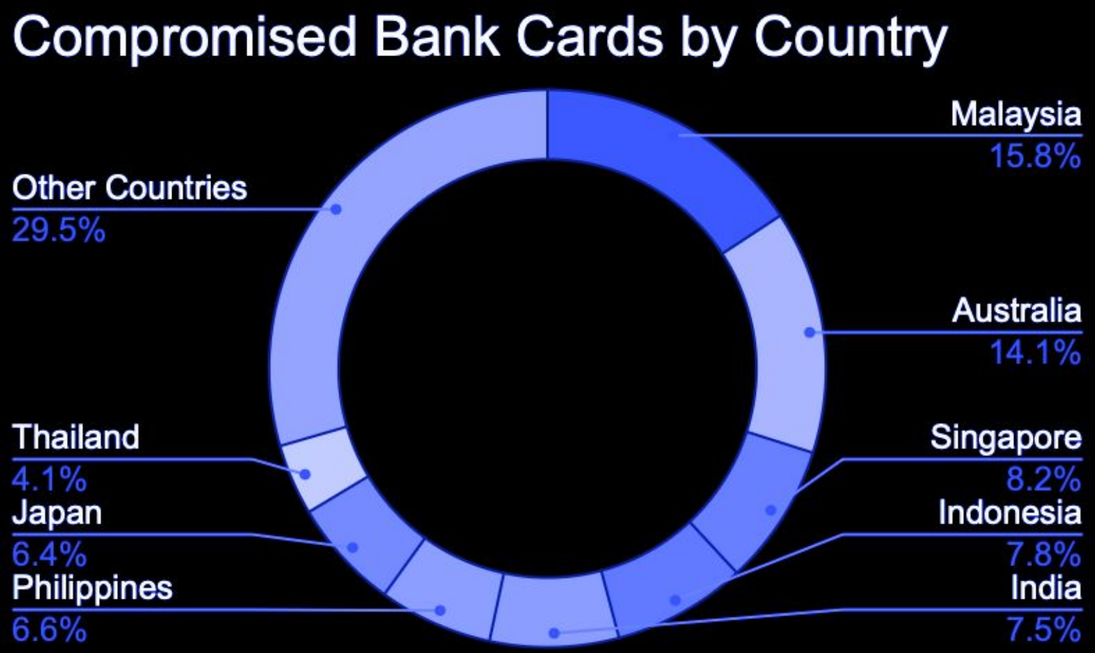
COMPROMISED BANK CARDS ↑ 18.2%

GROUP-IB

Statistics regarding compromised accounts.

Key Trends in February 2025:

- A little increase in the number of compromised bank cards in APAC and ANZ.
- The Number of compromised accounts in Australia, Malaysia and Singapore is consistently high.
- Main sources of information - data leaks 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.

HIGH TECH CRIME TRENDS REPORT

Download To Read Now

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

Save The Date - APAC Webinar

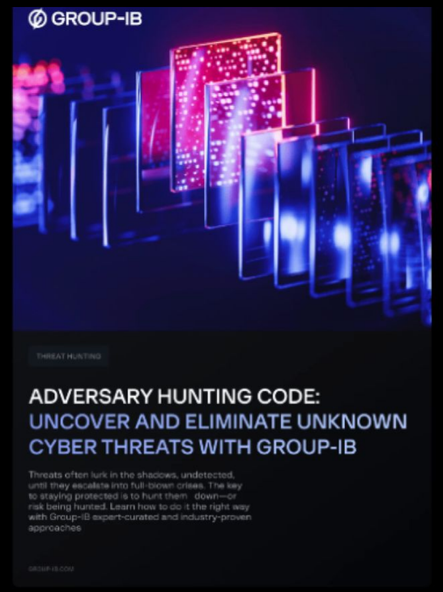
- Tuesday 18 April 2025, 11 AM GMT+8
- Look out for the Registration Link on our LinkedIn.

STAY SMART. STAY CONNECTED. STAY SECURED

GROUP-IB

Read now in Group-IB TI platform

Read now



Read now

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

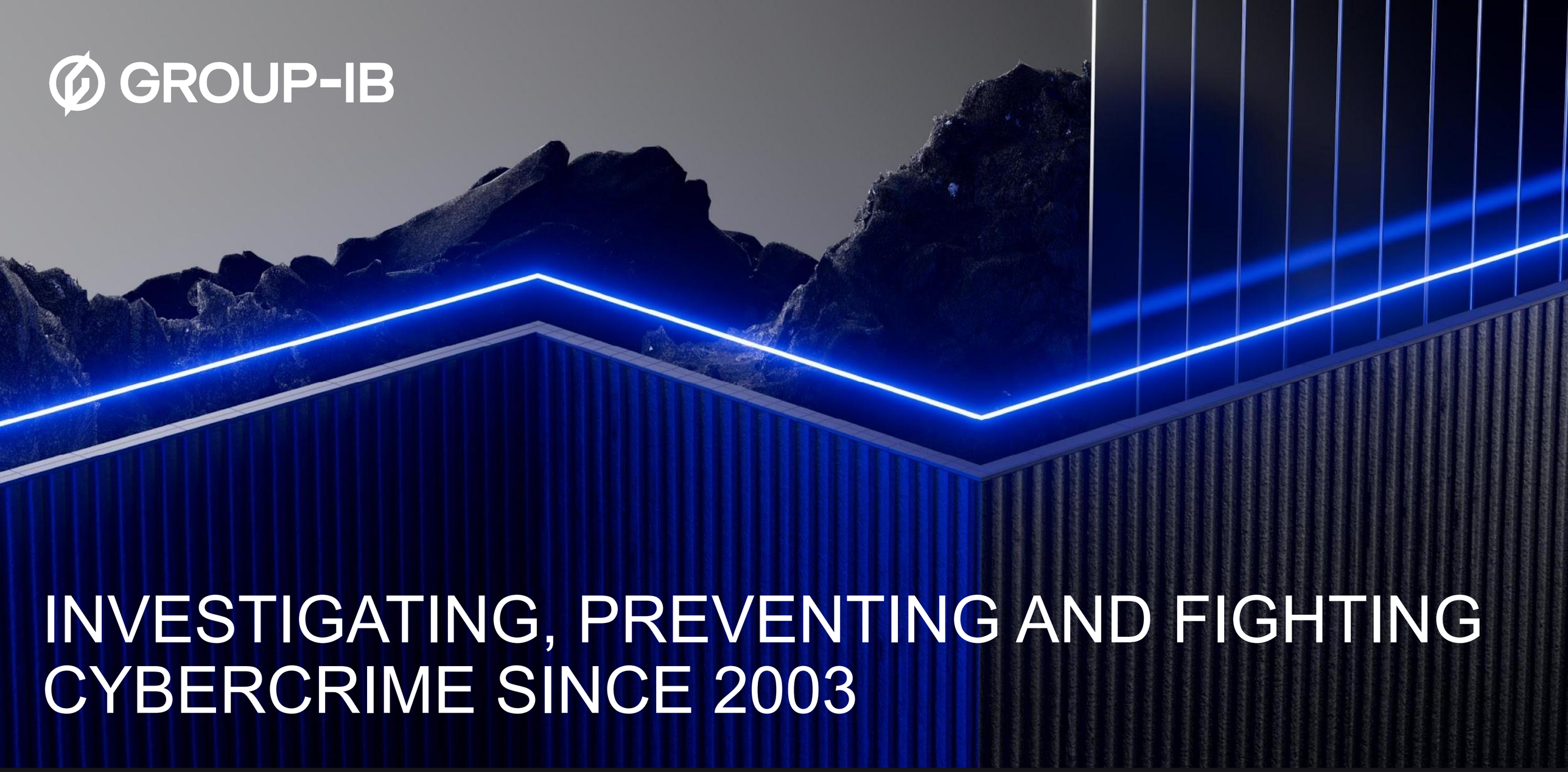
Utilize state-of-the-art security solutions, such as intrusion detection systems (IDS) and endpoint detection and response (EDR), to detect and respond to threats in real-time.

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