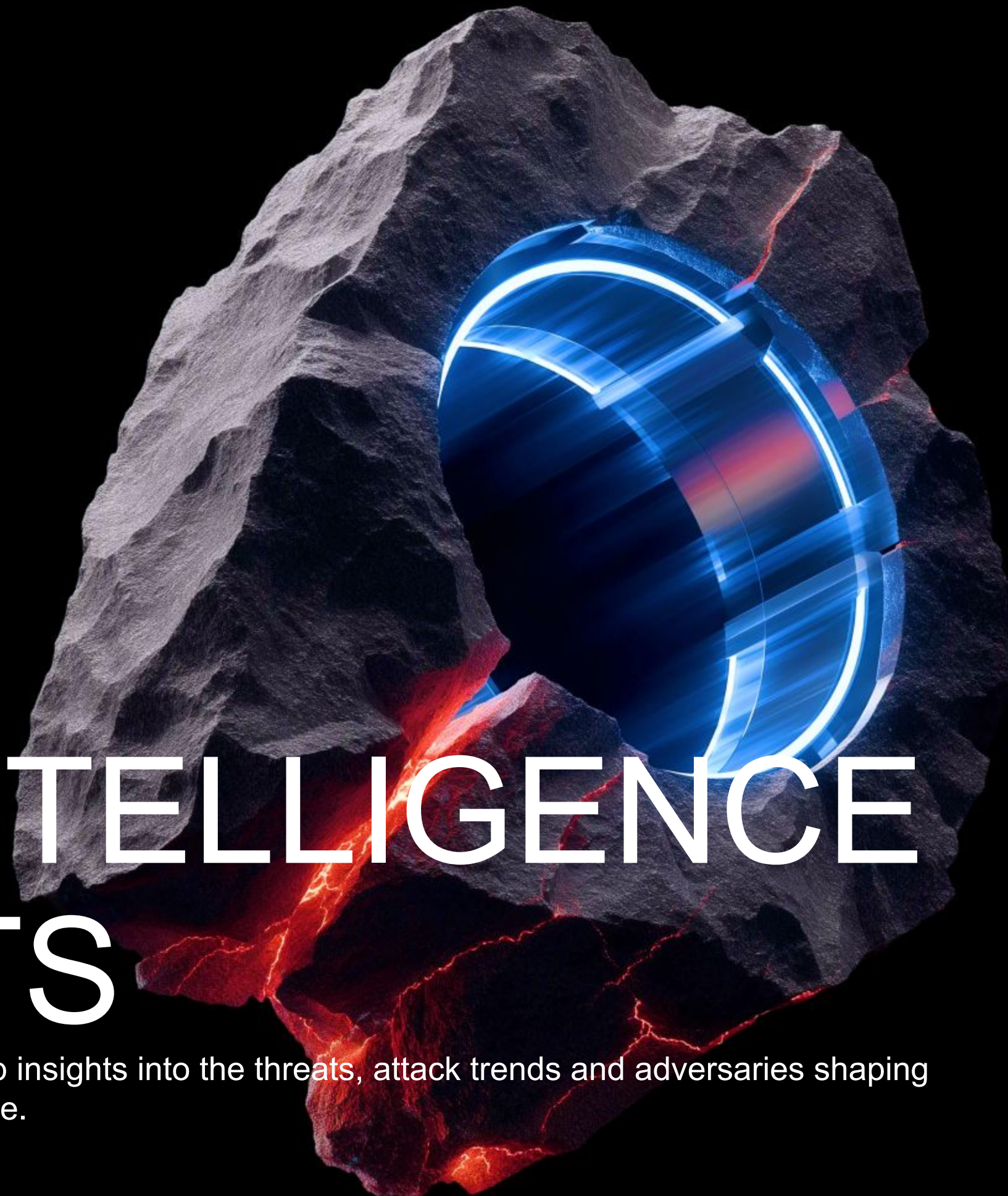


March 2026

APAC INTELLIGENCE INSIGHTS

Actionable threat intelligence and sharp insights into the threats, attack trends and adversaries shaping the Asia-Pacific cybersecurity landscape.



WHY THIS REPORT MATTERS



The Asia-Pacific (APAC) region continues to experience **rapid digital growth**, making it a prime target for cybercriminals, organised threat groups and nation-state-aligned actors.

This report helps you:

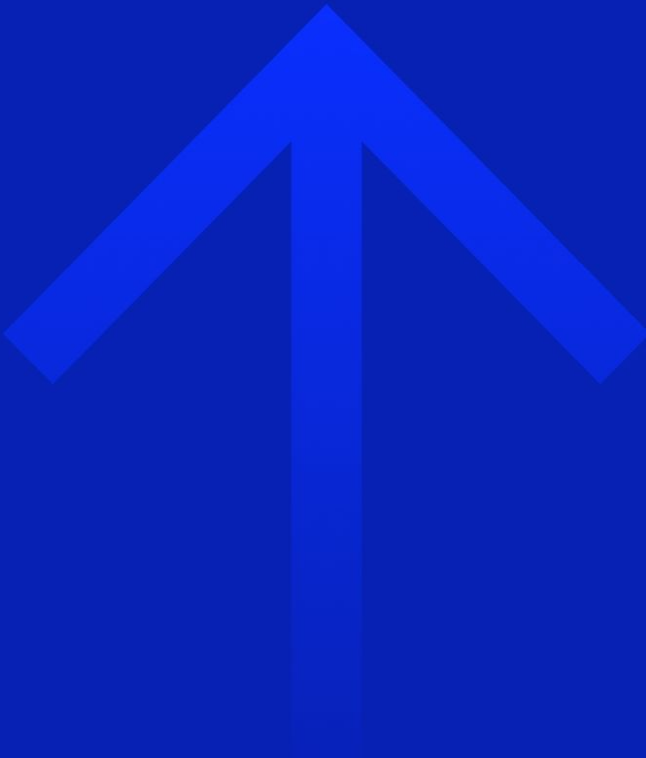
- Understand **how cyber threats are evolving across APAC**
- Identify **which industries and geographies are most targeted**
- Anticipate **new attack techniques and criminal business models**
- Translate intelligence into **practical defensive actions**
- Whether you are responsible for **security strategy, risk management, fraud prevention, or regulatory compliance**, this report provides clarity in a fast-changing threat landscape.



APAC THREAT LANDSCAPE

Month-on-Month Comparison between February 2026 and March 2026

106.9%



Ransomware
Activities

85.8%



DDoS /
Hacktivism

15.56%



Compromised
Accounts

102.2%



Compromised
Bank Cards

Key Findings & Global Cybersecurity Trends – March 2026

01. Cybersecurity Strategy Planning: The Essential Reset for Security Teams and Leaders in 2026

Cybersecurity is widely discussed at the boardroom table, but integrating it into the broader business context is where the gap lies: it shows up in uninformed security investments and decisions, misaligned business expectations, increased threat exposure without threat prioritization, and a lack of shared understanding of the current vs. desired security posture.

[Click for more information](#)

02. The Rise of Fake Shipment Tracking Scams in MEA

According to the 2024 Universal Postal Union's State of the Postal Sector report , postal services now serve a population of 7.3 billion people, and without them, a country's GDP could drop by a median of 7%.

And according to Statista, about 161 billion parcels were shipped worldwide in 2022 alone. Some of the top countries driving this volume include:

- China, which handled roughly 110 billion parcels in 2022, by far the largest share of global parcel traffic.
- United States, which shipped about 21 billion parcels in the same year.
- Japan, with around 9 billion parcels in 2022.

[Click for more information](#)

03. Six Supply Chain Attack Groups to Watch Out for in 2026

SaaS platforms, open-source ecosystems, MSPs, and cloud integrations now act as force multipliers, where a single compromise can create a ripple effect and affect hundreds of downstream organizations.

The methods used by the six threat actors described below show how supply chain abuse ties together phishing, data breaches, ransomware, and espionage into one interconnected attack ecosystem.

[Click for more information](#)

04. Conflict Watch Update: Week 5 — State-Linked Malware Campaigns, Infrastructure Targeting, and Escalating Hybrid Pressure

During Week 5, the threat landscape demonstrates a further escalation into coordinated hybrid operations, combining state-linked cyber campaigns, opportunistic destructive activity, infrastructure targeting narratives, and large-scale fraud exploitation.

This report continues Group-IB monitoring of the cyber dimension of the ongoing Iran–Israel–U.S. escalation and related regional developments.

Previous updates covering earlier phases of the conflict are available here: [Conflict Watch Reporting](#)

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – March 2026

01. Hasta la vista, Hastalamuerte: An Overview of The Gentlemen's TTPs

The report provides an overview on tactics, techniques, and procedures (TTPs) of The Gentlemen observed by Group-IB in intrusions conducted by its affiliates, as well as relevant information about the group's capabilities collected from underground private sources.

[Click for more information](#)

02. DieNet claimed DDoS attack on Kuwait Finance House

The Group-IB Threat Intelligence team identified a DDoS attack claimed by the threat actor DieNet targeting the website of Kuwait Finance House. The message indicates multiple connection attempts with varying response times, suggesting a disruption in service.

[Click for more information](#)

03. HIME666 claimed data leak from multiple countries

The Group-IB Threat Intelligence team identified a message from the threat actor HIME666, who claimed to possess a 30TB+ database collection containing over 100,000 private databases. The databases reportedly include information from various countries such as the Netherlands, France, Belgium, Italy, Germany, Switzerland, Poland, Vietnam, Iran, Sweden, the USA, Spain, Greece, Colombia, Ukraine, India, and others. The databases are said to contain sensitive information like phone numbers, emails, citizen data, passports, and more.

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – March 2026

04. Evil Markhors claimed defacement of multiple websites

The Group-IB Threat Intelligence team identified a defacement attack by Evil Markhors targeting multiple websites, including those in Israel, Belgium, and China. The attack involved altering web pages to display unauthorized content.

[Click for more information](#)

05. Hider_Nex claimed DDoS attacks on South Korean government websites

The Group-IB Threat Intelligence team identified a series of DDoS attacks claimed by the threat actor Hider_Nex targeting various South Korean government websites. The attacks were confirmed through check-host reports.

[Click for more information](#)

06. Everest Ransomware attack on Hyundai Elevator

On 2026-03-06, the ransomware group Everest claimed responsibility for an attack targeting Hyundai Elevator. The incident was disclosed through a post on the group's leak site (DLS), where the threat actors allegedly published evidence of the breach and threatened to release sensitive data if their demands were not met.

[Click for more information](#)

07. Qilin Ransomware attack on Omesti Berhad

On 2026-03-03, the ransomware group Qilin claimed responsibility for an attack targeting Omesti Berhad (omesti[.]com). The incident was disclosed through a post on the group's leak site (DLS), where the threat actors allegedly published evidence of the breach and threatened to release sensitive data if their demands were not met.

[Click for more information](#)

RANSOMWARE ACTIVITIES

120 Incidents

↑ 106.9%

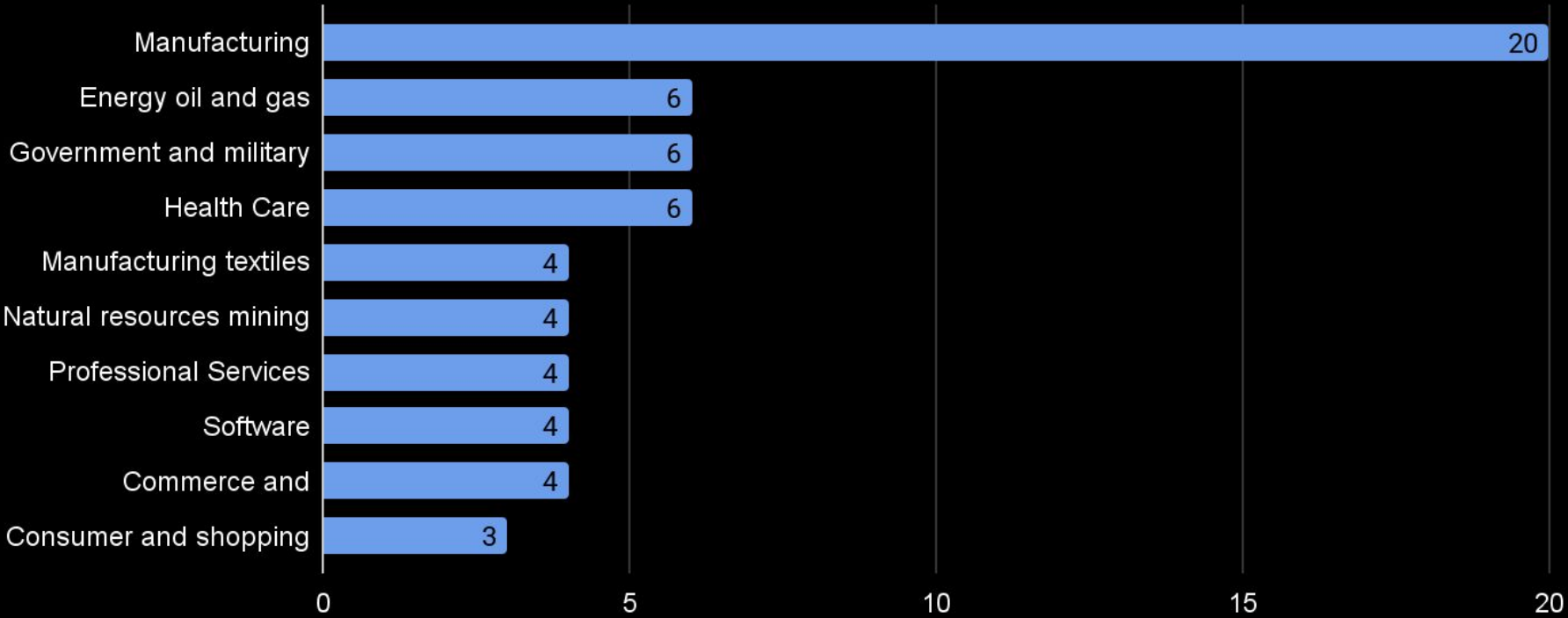
 GROUP-IB

Data: Number of Non-Unique Events and Activities (with Updates)

Key Events – March 2026

- Threat activity has more than doubled MoM (+107%), indicating rapid escalation
- Activity is heavily concentrated under a single dominant threat actor, The Gentlemen
- Targeting is focused on APAC, particularly Australia, Thailand, and India
- Manufacturing is the most impacted sector, suggesting supply chain targeting
- Secondary focus on critical infrastructure (energy, government, healthcare) increases potential impact severity

Ransomware attacks, per industry



Top 10 targeted sectors, March 2026

Most Active Threat Actor Groups

The Gentlemen 36 activities		Qilin 12 activities	
Gunra 8 activities	Payload Ransom 8 activities	Lockbit 6 activities	Dire Wolf 5 activities

Most Targeted Countries

Australia 18 activities		Thailand 18 activities	
India 16 activities	Malaysia 11 activities	Taiwan 11 activities	Japan 10 activities

DDOS AND HACKTIVISM

Top 6 Countries – Number of Activities per Country

India

16

South Korea

15

Thailand

5

Australia

3

Malaysia

3

Viet Nam

3

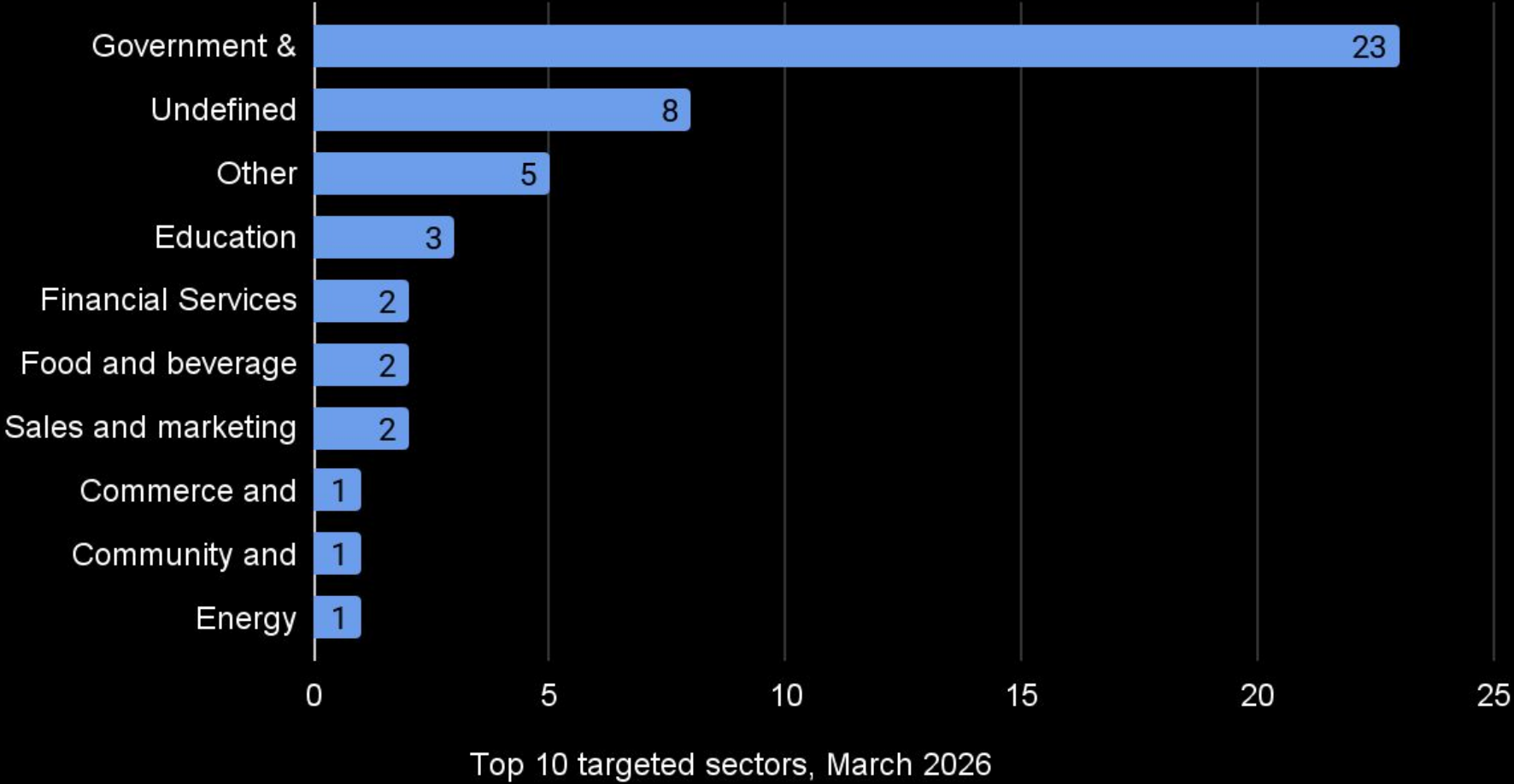
46 Incidents ↓85.8%

Data: Number of Events

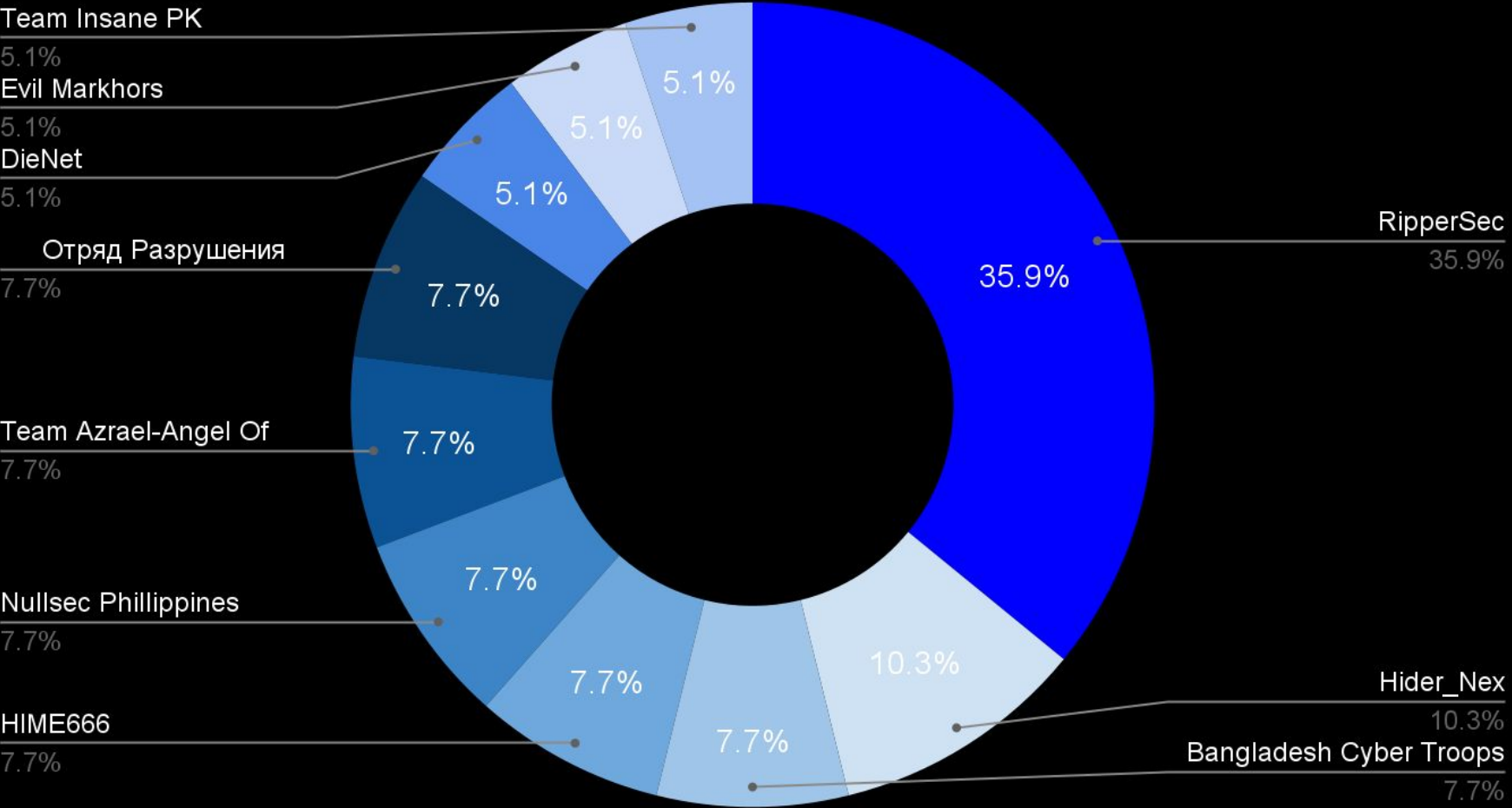
DDOS AND HACKTIVISM

- Top APAC countries: India (16) and South Korea (15) account for ~80% of DDOS activity; Thailand, Australia, Malaysia, and Vietnam have smaller incidents.
- Trend: Activity dropped sharply by 85.8% compared to last month.
- Threat groups: RipperSec is the most active (36.8% of incidents), with other groups showing fragmented activity.
- Targeted industries: Government & Military are primary targets (50%), followed by undefined and other sectors; finance and education see minor attacks.

DDOS and Hacktivism Activities, per industry



DDOS and Hacktivism Activities, per group



COMPROMISED ACCOUNTS

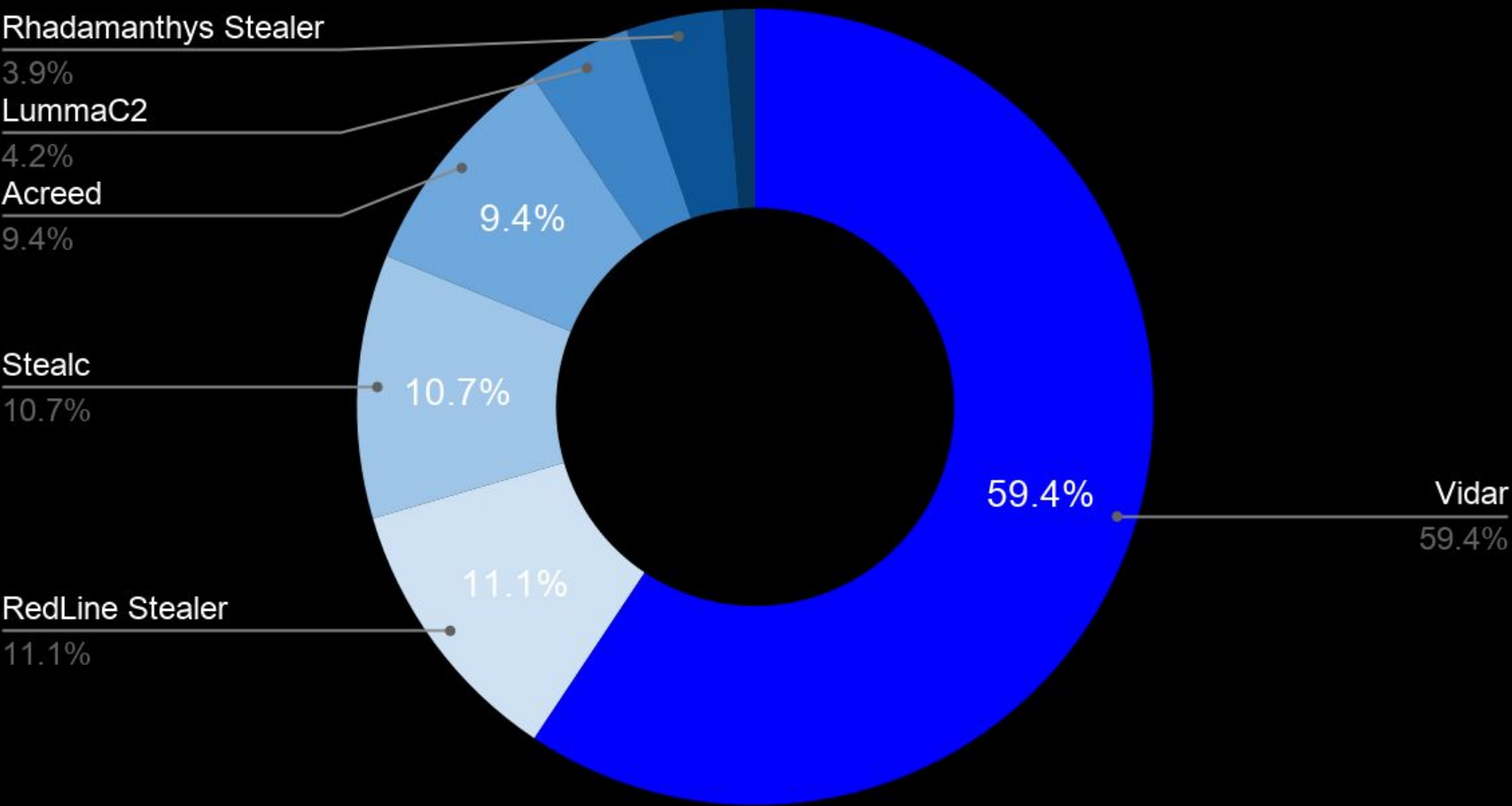
1,973,828 data leaks ↓ 15.56%

Data: Number of Events. Each malware can be part of the same event.

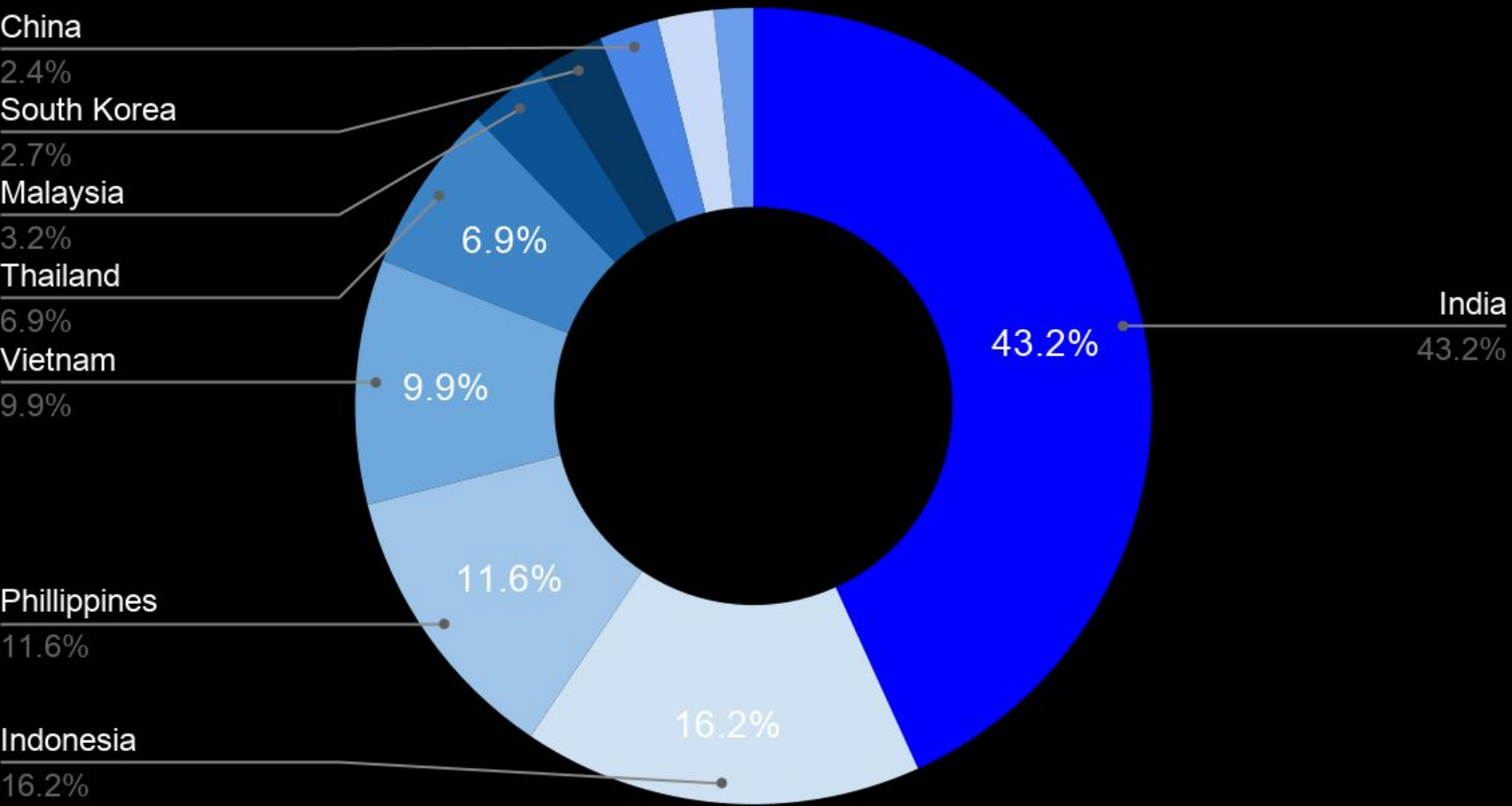
Key Events – March 2026

- Malware: Vidar is the main threat, causing ~70% of compromised accounts; RedLine Stealer, Stealc, and Acreed are secondary threats.
- Geography: India is the hardest hit (42%), followed by Indonesia (16%) and the Philippines (11%); Southeast Asia accounts for ~70% of incidents.
- Trend: Total compromised accounts dropped 15.6% month-over-month, but numbers remain high.

Compromised Accounts by Malware



Compromised Accounts by Country



COMPROMISED BANK CARDS

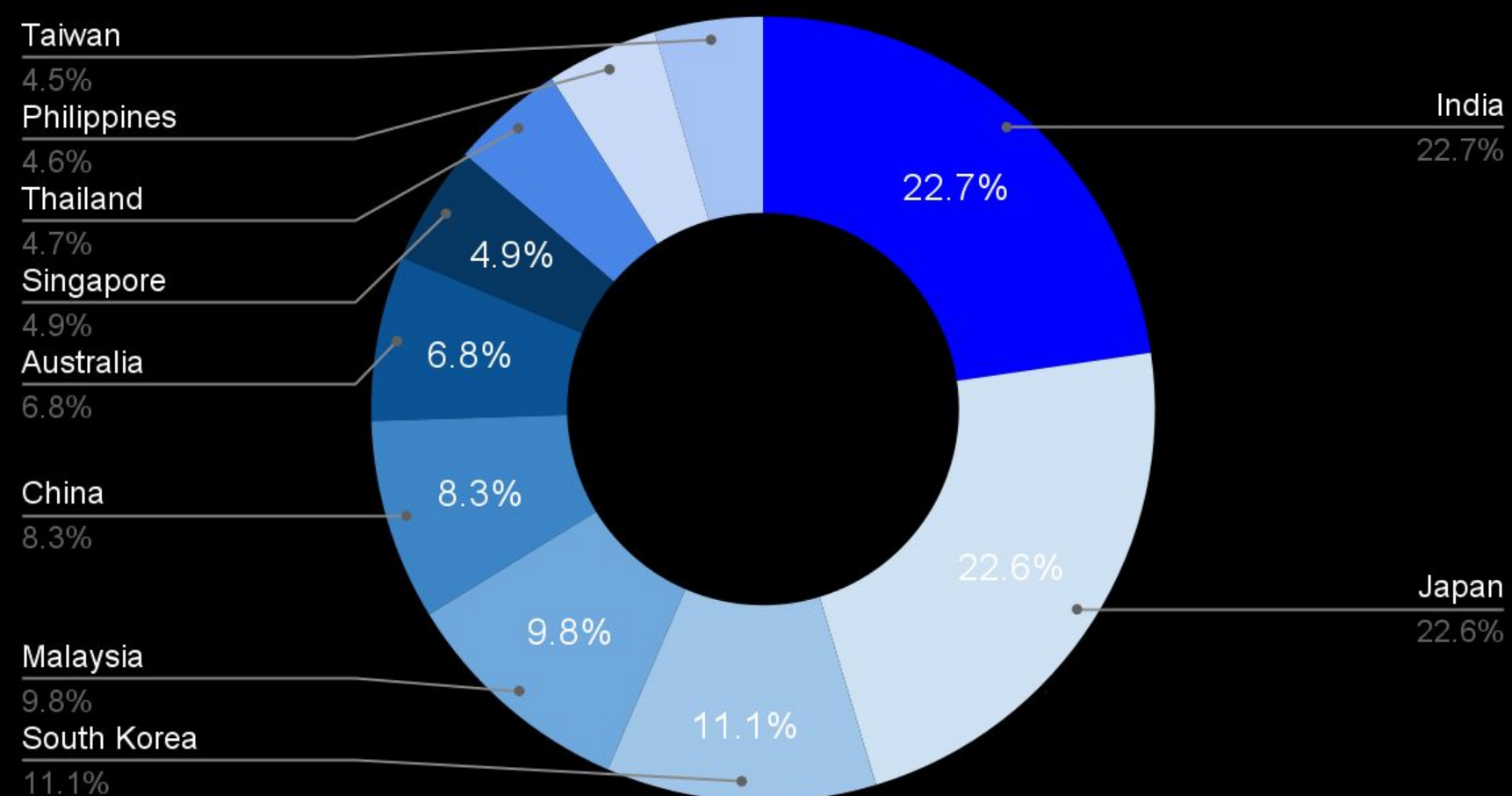
Key Events – March 2026

85,421 bank cards leaked ↑ 102.2%

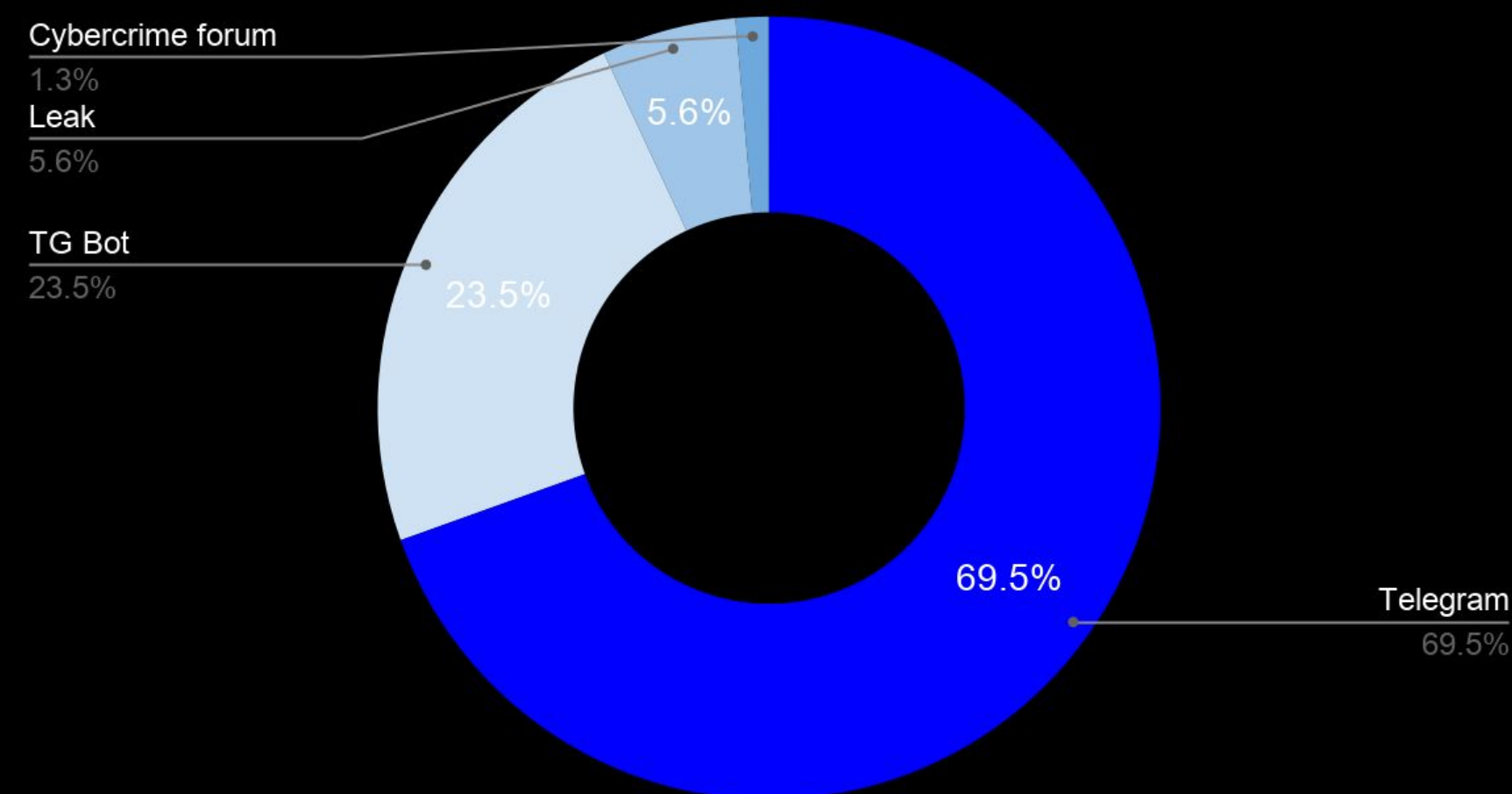
Data: Percentage of Events

- Compromised bank cards increased 102.2% MoM, indicating a sharp surge in threat activity
- Telegram and TG bots are the primary distribution channels, dominating the ecosystem
- India and Japan are the most impacted, contributing ~42% of total cases
- Threat exposure is widely distributed across APAC, not limited to a single market

Compromised Bank Cards by Country



Compromised Bank Cards by Source type



ADVERSARY OF THE MONTH



Threat actor group

The Gentlemen

Targeted industries:

"Government & military, Education, Financial services, Messaging & Telco, Software, Internet services, Lending & investments, Travel & tourism, Commerce & shopping, Agriculture, F&B, Gaming, Health care, Manufacturing, Media & entertainment, Professional services, Real estate, Sports

Period of Activity: May 2025 – Present

Targeted countries: Worldwide (APAC: Japan, Vietnam, Indonesia, India, China, Thailand, South Korea, Taiwan, Malaysia)

Attribution: N/A

Intent: Ransomware

Attack Summary

- The Gentlemen is a financially motivated ransomware group believed to consist of approximately 15 members, including a former affiliate of the Qilin ransomware group operating under the alias “hastalamuerte” (also known as Arm Corp) on the RAMP forum. The group was first observed by analysts in May 2025, although a Windows ransomware sample linked to the operation was uploaded to VirusTotal from Sweden on July 17, 2025. The operation focuses on data exfiltration and ransomware-based extortion, operating a Tor-based data leak site (DLS) to pressure victims. Unlike traditional Ransomware-as-a-Service models, the group reportedly does not maintain an affiliate panel and instead distributes ransomware builders and decryptors directly through Tox messenger, with negotiations with victims also conducted through the same channel.

Key Observations

- Available information suggests with moderate confidence that “hastalamuerte” is the administrator of The Gentlemen operation. The actor has previously demonstrated credibility in underground communities as a Qilin affiliate and currently possesses leaked ransomware builders from families such as LockBit ransomware, Conti ransomware, HelloKitty ransomware, and VanHelsing ransomware, which may be reused or modified to develop new variants, including potential Linux and ESXi versions reportedly being developed with assistance from ChatGPT. The group is expected to primarily target technology companies, insurance firms, financial services, and banking organizations, as these sectors are considered more likely to pay ransom demands, and the operation may expand as additional threat actors join the group.

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003