

November 2025

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.

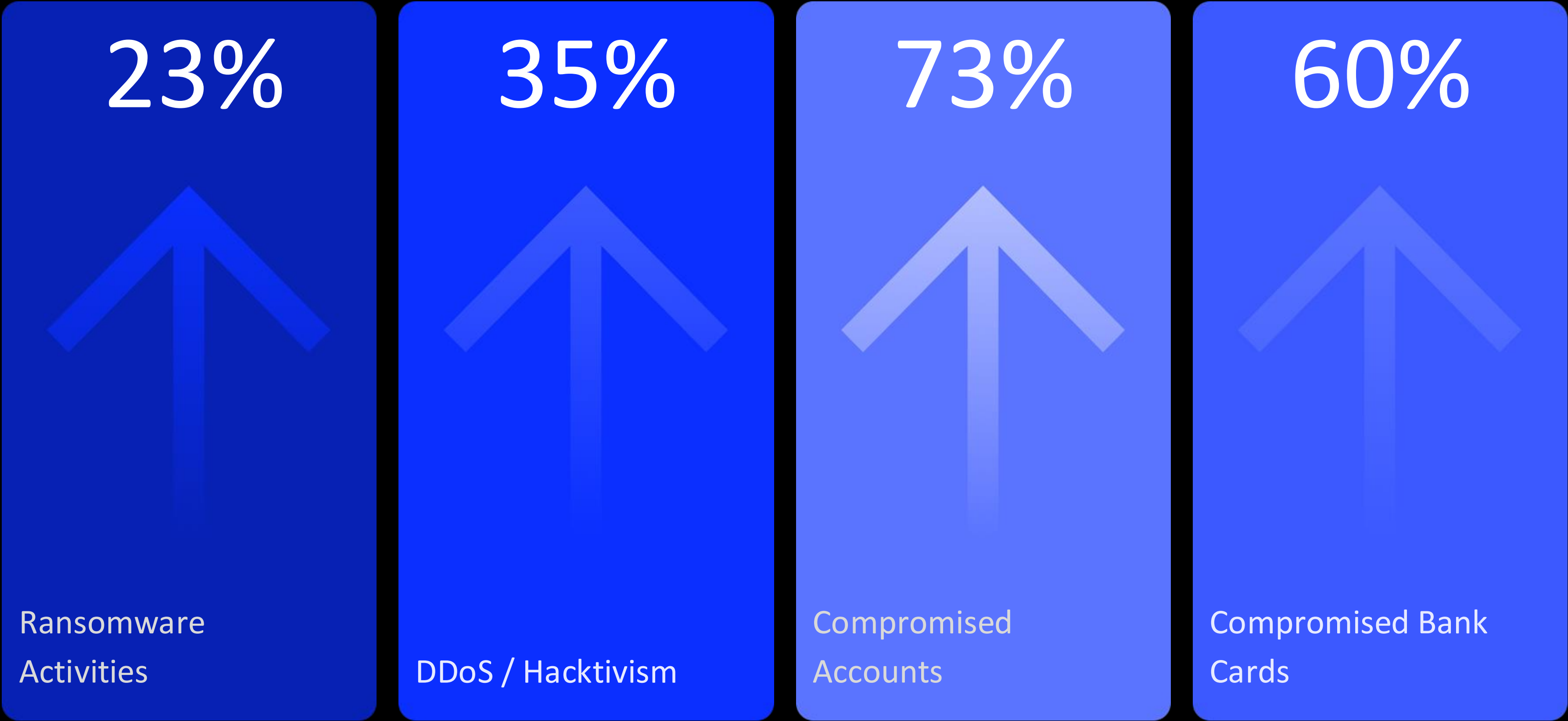
This report helps you:

- 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 October 2025 and November 2025



Key Findings & Global Cybersecurity Trends – November 2025

01. Ghosts in /proc: Manipulation and Timeline Corruption

Learn how threat actors abuse the Linux /proc filesystem to conceal malicious activity and tamper with forensic timelines. This analysis covers command-line spoofing, start-time manipulation, and the practical detection and mitigation steps defenders need to know and apply.

[Click for more information](#)

02. Uncovering a Multi-Stage Phishing Kit Targeting Italy's Infrastructure

Group-IB has identified an advanced phishing framework that closely replicates legitimate brands by using multi-layered evasion methods, CAPTCHA filtering, and Telegram channels for data exfiltration. These enabled large-scale credential theft while avoiding automated detection systems. This research highlights how phishing-as-a-service is scaling into a highly effective fraud vector by leveraging on automation.

[Click for more information](#)

03. Bloody Wolf: A Blunt Crowbar Threat to Justice

Dive into Group-IB's technical analysis which examines the techniques, tools and ongoing activity of the threat group known as Bloody Wolf. This group impersonates government agencies to gain the trust of victims before beginning phishing campaigns.

[Click for more information](#)

Key Findings & Global Cybersecurity Trends – November 2025

04. Discovery of New Rust Backdoor and Associated MuddyWater Campaigns

Group-IB identified a new campaign which can be attributed with high confidence to MuddyWater that features a previously unseen Rust-based backdoor. This marks the first known use of Rust by this threat actor. The operation closely mirrors earlier MuddyWater activity, particularly in its use of malicious documents and embedded macros. This finding highlights MuddyWater’s continued development of custom tooling while retaining familiar infection techniques.

[Click for more information](#)

05. Critical Unauthenticated Admin Takeover Vulnerability in FortiWeb Manager

A newly uncovered vulnerability in Fortinet’s FortiWeb Manager allows unauthenticated attackers to fully compromise its management interface and WebSocket CLI. A proof of concept observed on 6 October 2025 demonstrated how a crafted POST request could be used to create a privileged administrator account; with testing confirming that this flaw affected versions 8.0.1 and earlier. This exploit has been actively abused since early October, with no vendor advisory issued as of 13 November 2025. The vulnerability has now been assigned CVE-2025-6446.

[Click for more information](#)

06. LANDFALL Spyware: Analysis of a Zero-Click Exploit Targeting Samsung Galaxy Devices

Researchers uncovered LANDFALL, a commercial-grade Android spyware deployed through a Samsung zero-day vulnerability CVE-2025-21042 which allowed remote code execution via malicious DNG image files. Once installed, the spyware enabled extensive surveillance capabilities including audio recording, location tracking, and extraction of photos, contacts and call logs. Active from mid 2024 until Samsung patched the flaw in April 2025, the campaign aligns with broader zero-click exploitation patterns linked to private sector offensive actors operating in the Middle East.

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – November 2025

01. SideWinder Espionage Campaign Using ClickOnce Infection Chain

SideWinder, an APT group from India, is conducting a phishing campaign against government entities across South Asia. The attackers use advanced social engineering tactics, Microsoft exploitation methods, and living-off-the-land techniques to deploy malware through trusted system processes.

[Click for more information](#)

02. PDF File Share Phishing Campaign

Group-IB Threat Intelligence was alerted to a phishing campaign conducted by a threat actor known as "Xanders", who impersonated a Malaysian financial institution using fake payment notification emails. The lures directed victims to click a link labelled "Payment Advice", which redirected them to a credential-harvesting page.

[Click for more information](#)

03. Compromised Platform Abused in Thai Crypto Phishing Campaign

Since 8 November 2025, threat actors have used a compromised email automation platform Taximail to send phishing emails that impersonate major Thai companies. The messages promoted fraudulent crypto investments and appeared to pass SPF and DKIM checks. Taximail later confirmed that its platform was abused to send these spoofed emails using domains of its customers.

[Click for more information](#)

Key Findings & Regional Cybersecurity Trends – November 2025

04. Sale of South Korean Companies’ Source Codes Obtained From Shared Contractor

Between 13 to 17 November 2025, a threat actor known as “888” advertised the sale of source code from several major South Korean companies like Samsung, HD Hyundai and LG on Darkforums. While the initial access method is still unclear, analysts are moderately confident that a shared contractor may have served as an entry point for these breaches.

[Click for more information](#)

05. Fake Binary Options Investment Campaigns Through Template-Based Websites

Group-IB’s High Tech Crime Investigations Team has been tracking a binary options investment scam targeting Vietnamese users since November 2023. The campaign remains active as of November 2025, with scammers continuously creating new fraudulent pages. This report summarizes the campaign’s structure, technical set-up and social engineering methods.

[Click for more information](#)

06. Upbit Security Incident Involving Its Solana Network Assets

On 27 November 2025, South Korean crypto exchange Upbit reported that approximately KRW 54 billion (approximately USD 40 million) in Solana-ecosystem tokens were illicitly withdrawn to an unauthorized wallet. Upbit immediately suspended all deposits and withdrawals before launching an emergency security review. The exchange confirmed that only Solana-based tokens held on their platform were affected, and that losses will be fully covered by Upbit’s own assets

[Click for more information](#)

RANSOMWARE ACTIVITIES

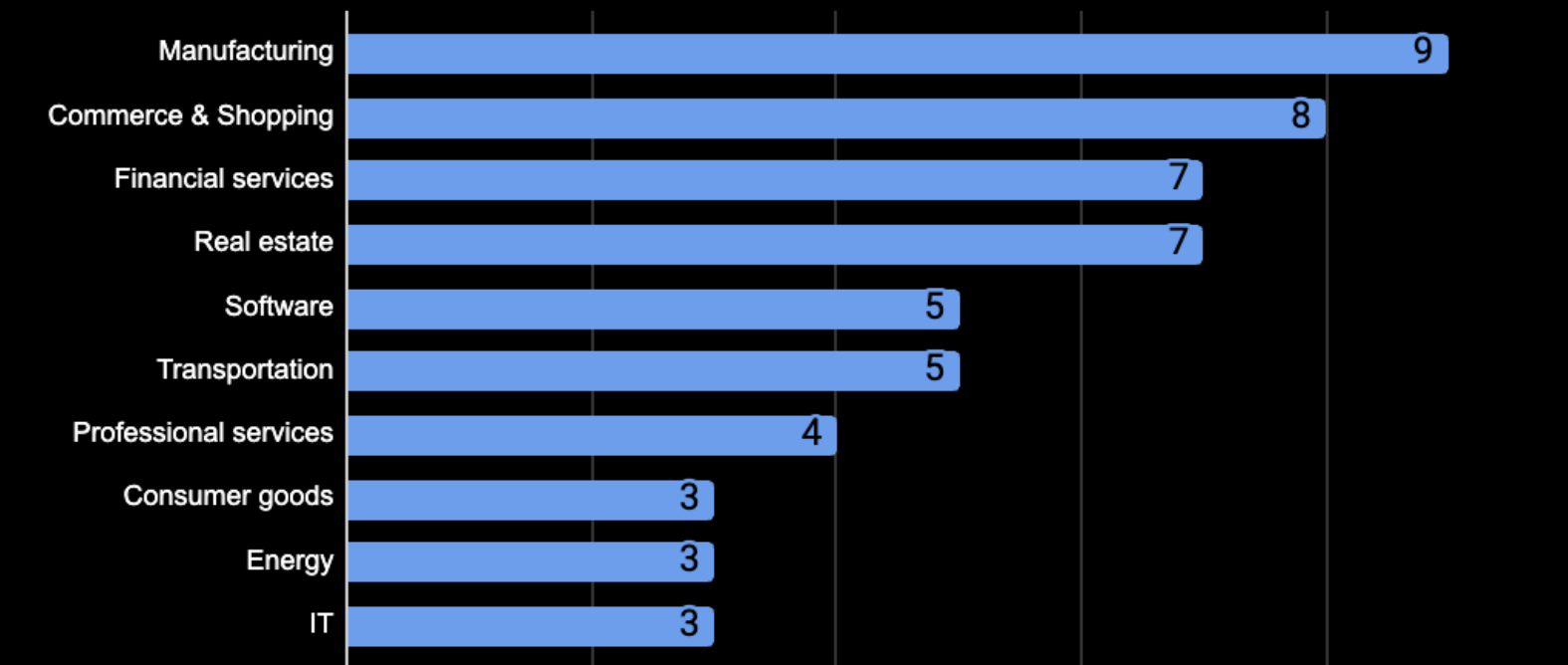
Key Events – November 2025

- The main threat actor groups continue to be the same ones from previous month (click [here](#) for October 2025 edition), namely **The Gentlemen** and **Qilin**.
- A majority of the attacks occur in the **Manufacturing, Commerce & Shopping, and Financial Services** sectors.

86 Incidents ↑ 23%

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

Ransomware Attacks by Industry



Most Active Threat Actor Groups

The Gentlemen		Dire Wolf	
11 activities		11 activities	
↑ 10%			
NightSpire	Qilin	Cl0p	DragonForce
7 activities	7 activities	6 activities	5 activities
	↓ 56%		

Most Targeted Countries

Australia		India	
15 activities		14 activities	
↓ 21%			
Thailand	Japan	Vietnam	China
10 activities	9 activities	8 activities	6 activities

DDOS AND HACKTIVISM

Top 6 Countries – Number of Activities per Country

Thailand
30

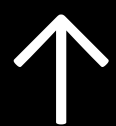
Bangladesh
17

India
16

Philippines
14

Cambodia
12

Indonesia
11

124 Incidents  35%

Data: Number of Events

DDOS AND HACKTIVISM

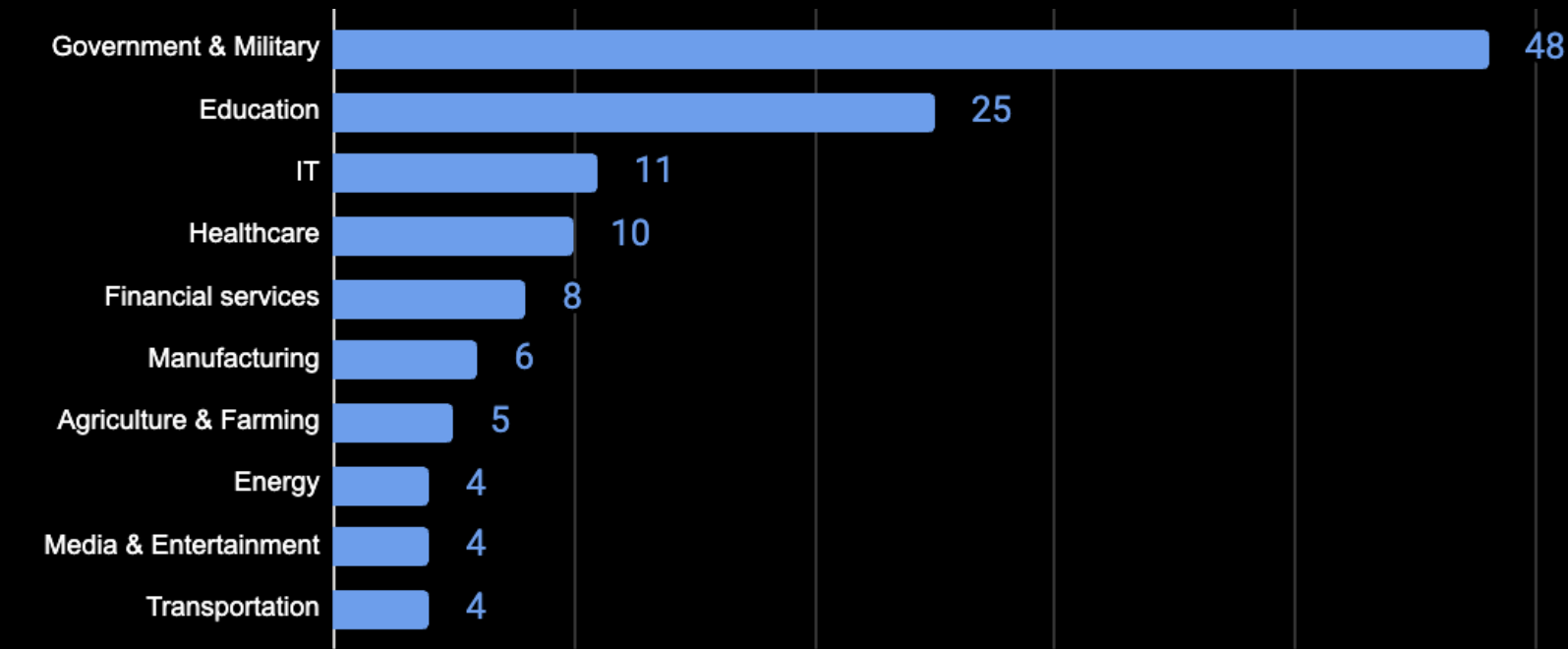
Hacktivism refers to the use of hacking activities to advance political or social agendas. Hacktivist groups are typically low-skilled actors who carry out attacks such as DDoS, Defacement, and Data Breaches (by mostly leveraging on compromised accounts).

Below is an overview of the active threat actor groups and the top 10 industries targeted across APAC in October 2025. More information on each actor and their activity can be found on Group-IB Threat Intelligence Portal.

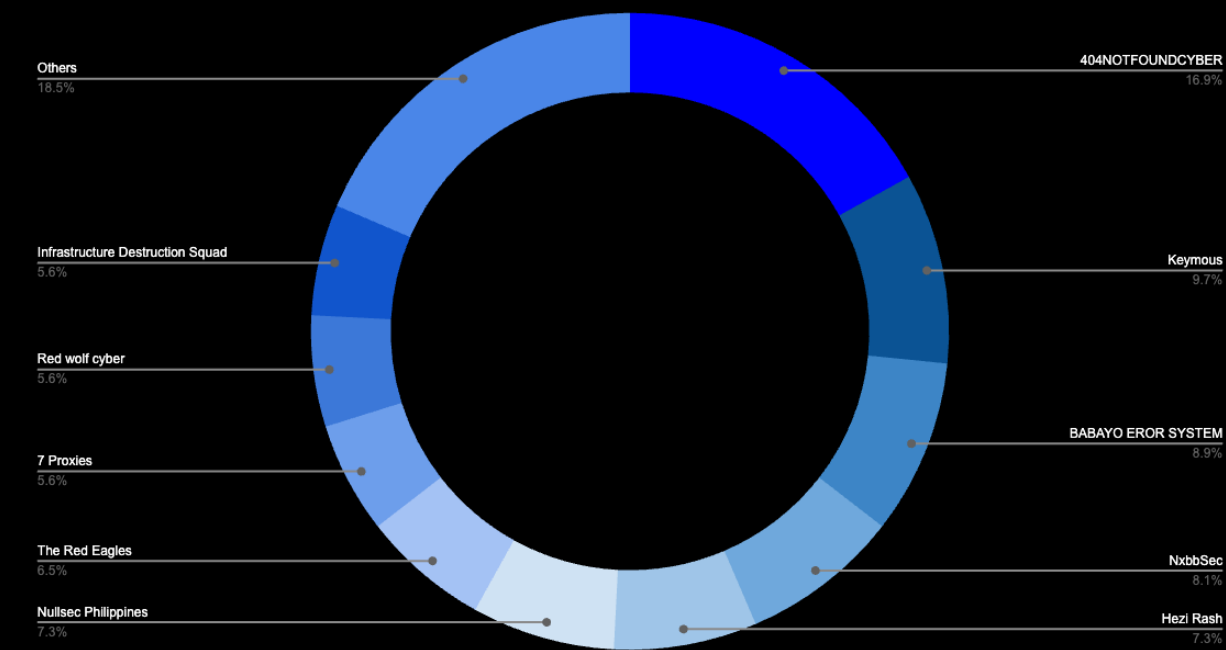
Due to ongoing tensions between some countries, the most active actors continue to be the ones motivated by their conflicts and target the Government & Military sector.

Data: Number of Events

DDoS and Hacktivism Activities by Industry



DDoS and Hacktivism Activities by Threat Actor Group



COMPROMISED ACCOUNTS

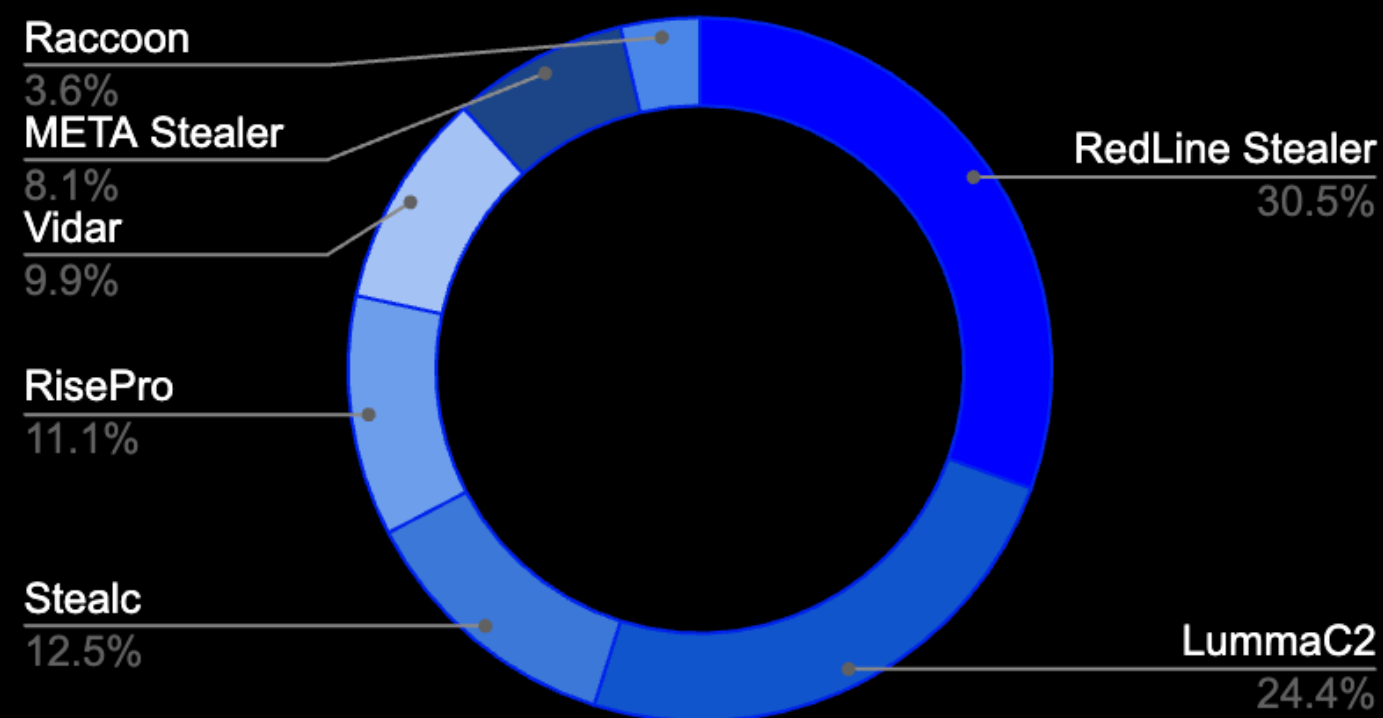
Key Events – November 2025

- India, Indonesia, the Philippines and Thailand continue to have the highest numbers of compromised data since the beginning of 2025.
- Almost all data came from Stealer log clouds, which are mostly distributed via Telegram. Most victim domains comprise of Google, Facebook and Roblox accounts.
- RedLine Stealer remains the main malware responsible for 30% of compromises; followed by LummaC2, Stealc, and RisePro.

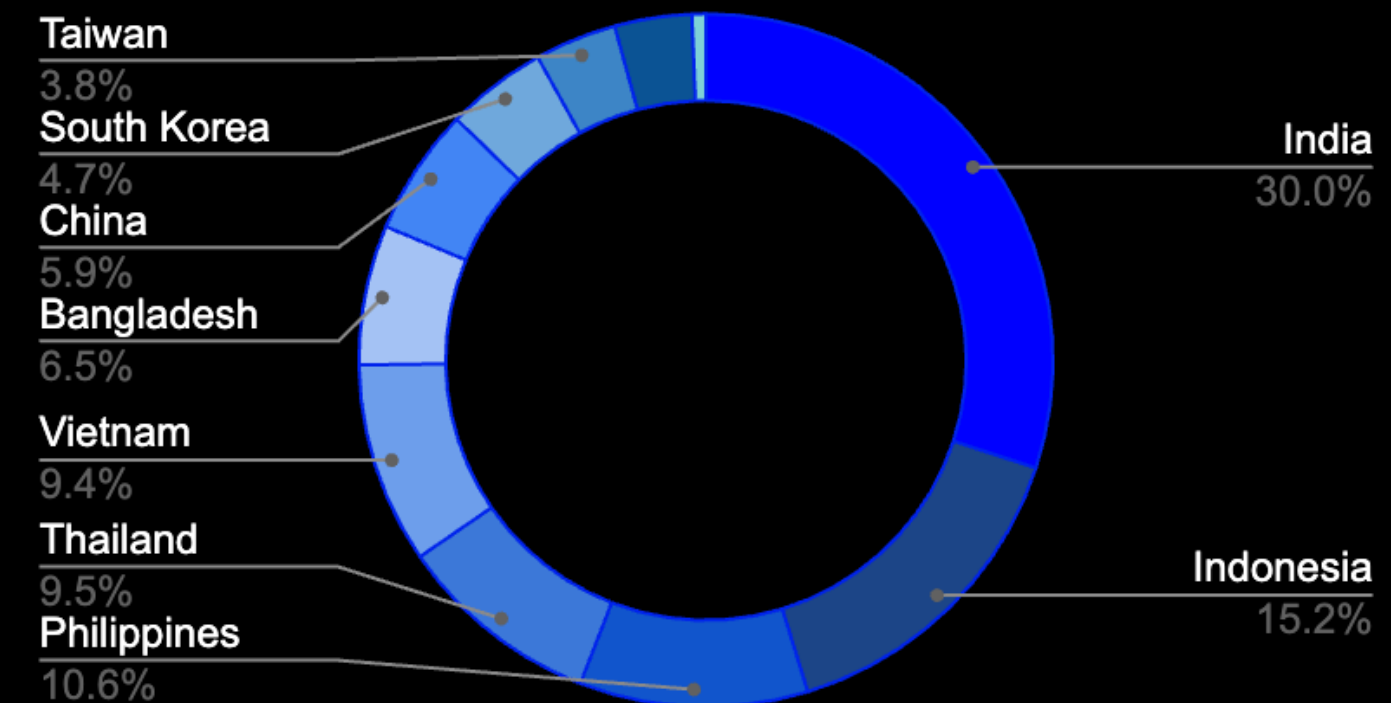
26,444,002 data leaks **↑ 73%**

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

Top 7 Malwares



Compromised Accounts by Country



COMPROMISED BANK CARDS

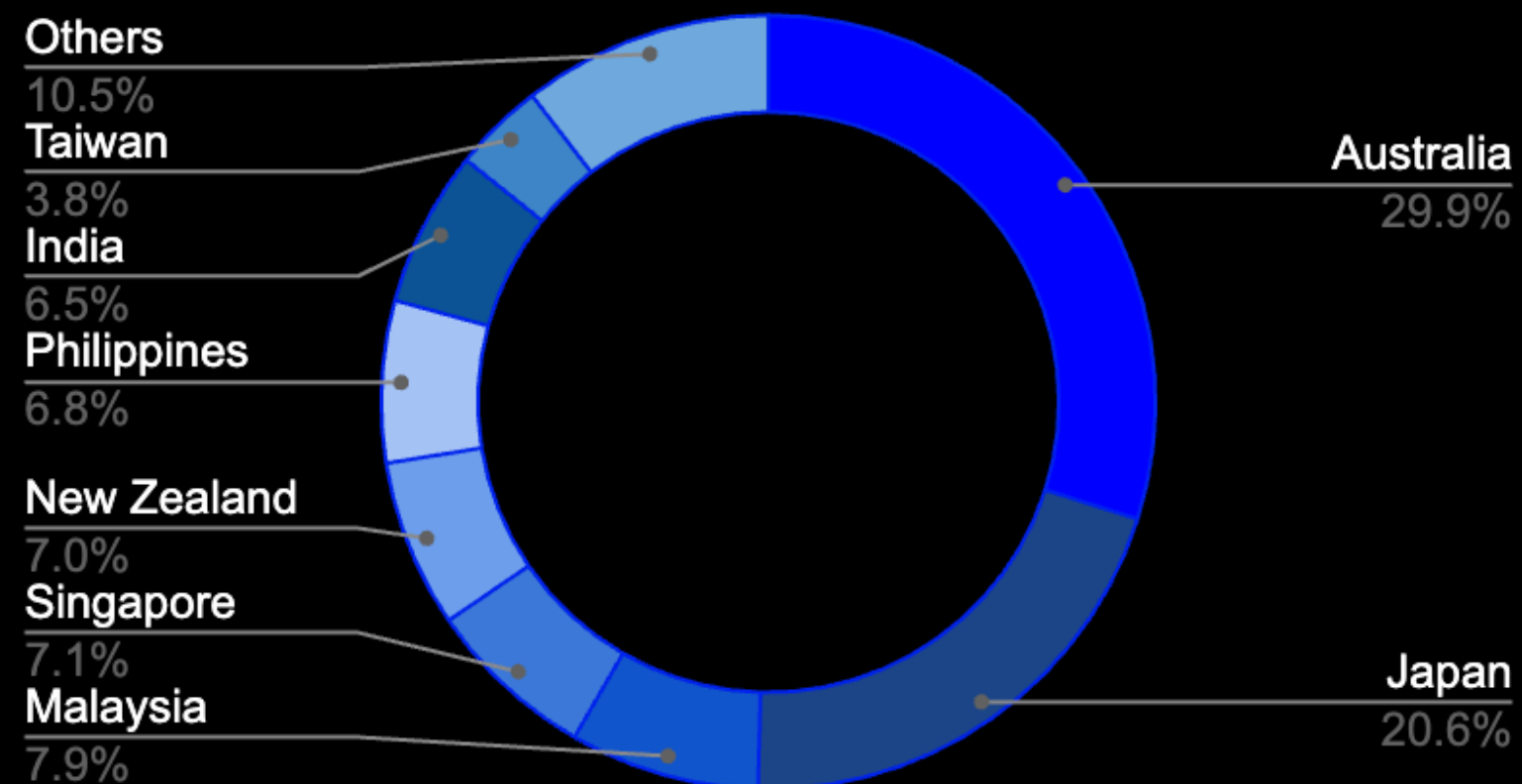
Key Events – November 2025

- The top countries affected remain Japan, Malaysia, Singapore and Australia. This trend has persisted for the past few months.
- The main source of information is data leaks from Telegram, mostly due to info-stealer/scrapper, botnet/loader, credential/credit stealer malwares, and phishing attacks. Phishing remains a constant threat across all countries.

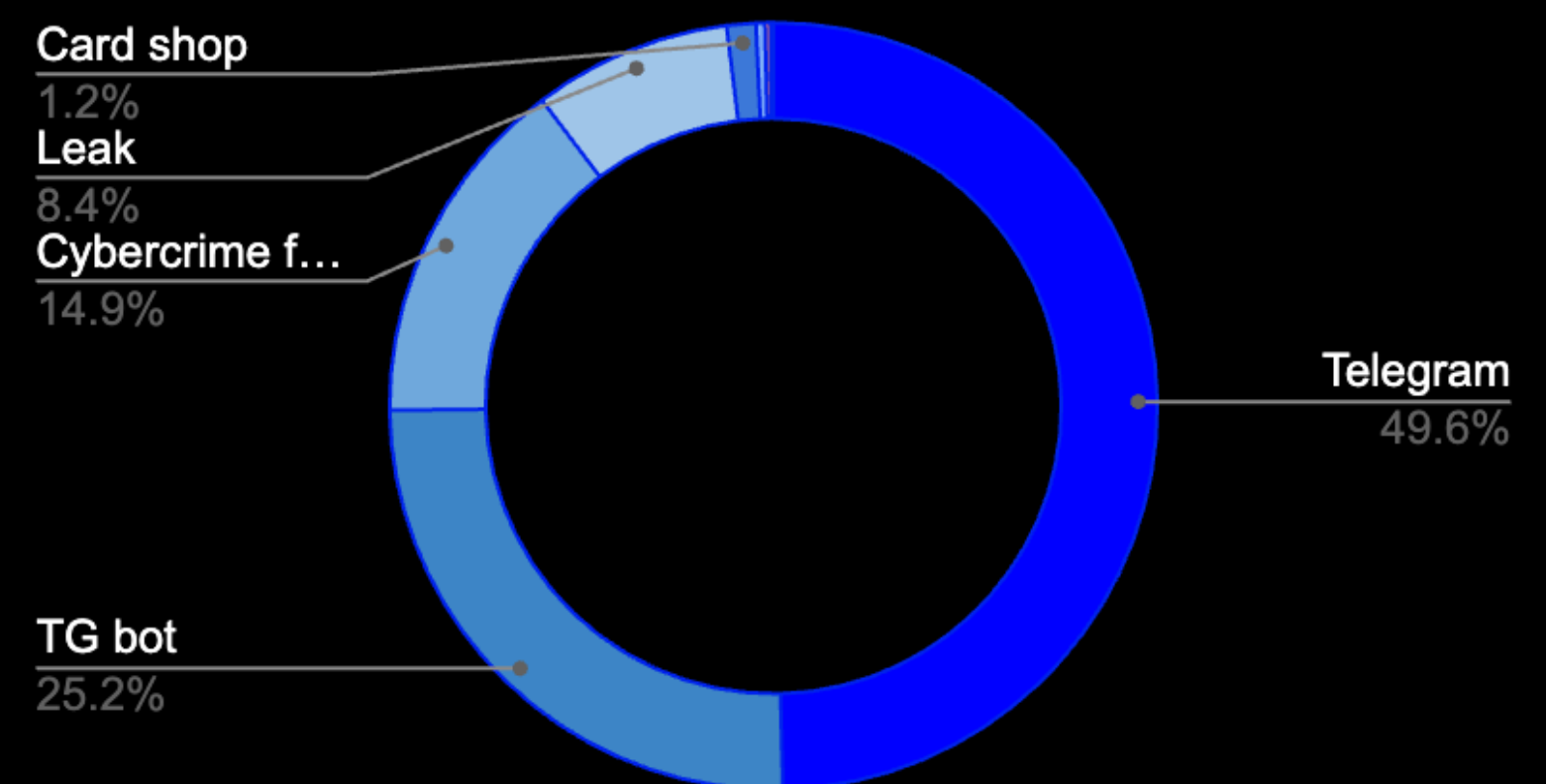
5,090 bank cards leaked **↑ 60%**

Data: Percentage of Events

Compromised Bank Cards by Country



Compromised Bank Cards by Source Type



ADVERSARY OF THE MONTH



Threat actor group

SideWinder

Targeted industries:

Government and military, Hardware, Commerce and shopping, Education, Energy, Financial services, Health care, Internet services, Media and entertainment, Messaging and telecommunications, Science and engineering, Software, Transportation

Period of Activity: July 2026 – Present

Targeted countries: China, Bangladesh, Philippines, India, Indonesia, Cambodia, Singapore, Vietnam

Attribution: India

Intent: Financially motivated

Attack Summary

- The SideWinder group (also known as Rattlesnake, Hardcore Nationalist (HN2), T-APT-04) is engaged in cyber espionage on members of South Asian state institutions like governments and military. Their attacks target both Windows and Android users.

Key Observations

- Attackers primarily target Windows users through phishing emails containing malicious attachments, often themed around territorial tensions between China, India, Nepal, and Pakistan. These campaigns commonly deploy JavaScript loaders that deliver the DUser.dll payload, use domains impersonating victim organizations for C2 communication, and rely on DLL side-loading to execute final modules.
- On Android, the group uses credential-phishing techniques and distributes malicious apps through various marketplaces to conduct espionage.
- Recently a coordinated phishing campaign attributed to Sidewinder has targeted government and military institutions across Nepal, Bangladesh, Sri Lanka, Pakistan, and Turkey. The group created highly convincing fake login and document-upload pages and hosted them on services to steal credentials. Infrastructure mapping shows that the operation followed a repeatable pattern across multiple countries, focusing on high-value institutions and replicating interfaces familiar to government and defense personnel, making the fraudulent portals appear legitimate.

CONCLUSIONS AND RECOMMENDATIONS

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.

STAY SMART. STAY CONNECTED. STAY SECURED



Subscribe to our mailing list

RECENT RESOURCES



GROUP-IB

ATM

RECEIPT

Threat ResearchTrend ReportAnalytical ReportsWhite Papers

UNC2891:
ATM Threats
Never Die

GROUP-IB.COM

Read now



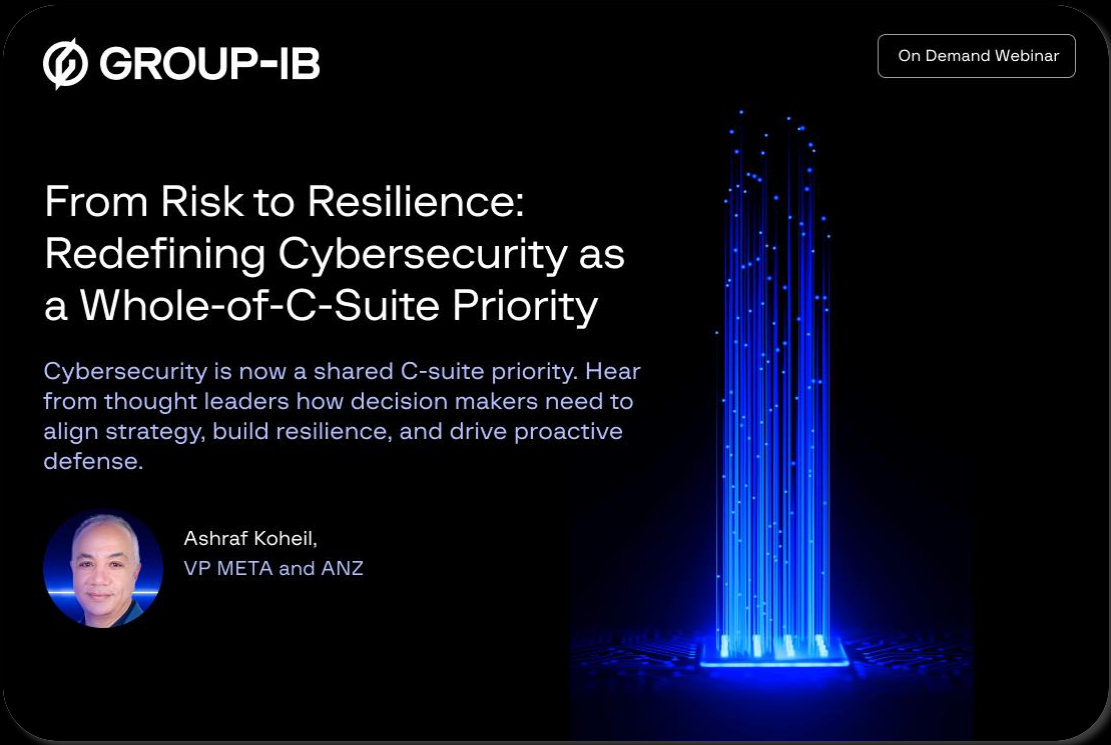
GROUP-IB

AI innovationAI toolsExpert talksAI eventsAI Red TeamingAI Readiness AssessmentTailored features

Group-IB AI
Cybersecurity Hub

Learn. Test. Evolve Your Defenses

Discover more



GROUP-IB

On Demand Webinar

From Risk to Resilience:
Redefining Cybersecurity as
a Whole-of-C-Suite Priority

Cybersecurity is now a shared C-suite priority. Hear from thought leaders how decision makers need to align strategy, build resilience, and drive proactive defense.



Ashraf Koheil,
VP META and ANZ

Watch now

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003