

February 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.

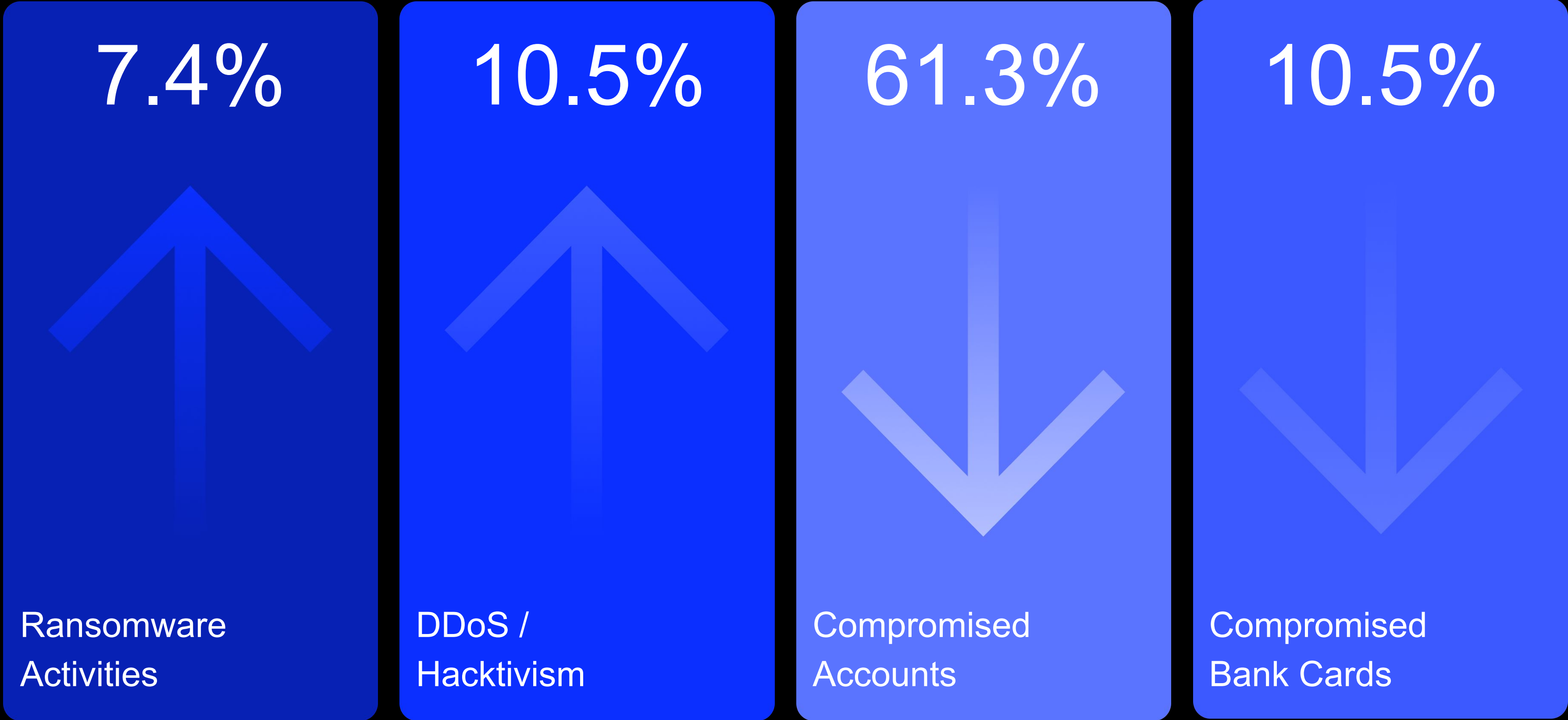
This report helps you:

- 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 January 2026 and February 2026



Key Findings & Global Cybersecurity Trends – February 2026

01. Shaping Shadows: Breaking Down New ShadowSyndicate Methods and Infrastructure

ShadowSyndicate is a prolific malicious cluster characterized by its vast server infrastructure, which researchers track through distinct SSH fingerprints and overlaps in hosting providers. Though they utilize a diverse range of toolkits like Cobalt Strike and Sliver, the group's primary role is believed to be either an IAB or a provider of bulletproof hosting for various ransomware affiliates. Recent findings by Group-IB have uncovered new SSH fingerprints and a "server rotation" technique where infrastructure is transferred between clusters to mask ownership. Despite these attempts at operational security, inaccuracies in their execution have allowed analysts to definitively link ShadowSyndicate to major ransomware operations including ClOp, ALPHV/BlackCat, and Black Basta.

[Click for more information](#)

02. Operation Olalampo: Inside MuddyWater's Latest Campaign

The Iranian threat actor MuddyWater has launched a new cyber offensive titled Operation Olalampo, specifically targeting organizations and individuals across the MENA region. This campaign features four new malware variants—including the CHAR rust backdoor and GhostBackDoor—with indicators suggesting the group may be utilizing AI-assisted development. A significant technical shift involves the use of a Telegram bot for command-and-control, which has provided researchers with rare insight into the group's post-exploitation commands and data collection. Despite these new tools, the underlying infrastructure and tradecraft show clear overlaps with historical operations dating back to 2025, confirming the group's persistent regional focus.

[Click for more information](#)

03. New Phishing Infrastructure hosting Fake Okta and Microsoft 365 Login Pages (Eta Cluster)

Group-IB analysts have identified a massive phishing infrastructure, tracked as the Eta cluster, that utilizes Adversary-in-the-Middle (AiTM) kits to spoof Okta and Microsoft 365 login workflows. This sophisticated toolkit employs real-time "heartbeat" signals and backend controls to bypass Multi-Factor Authentication (MFA) and hijack active user sessions. The campaign is attributed to the SLSH group. This alliance is confirmed by the shared use of the "Oktapus" phishing kit, specific domain naming conventions, and recent 2026 intelligence claiming joint credit for these operations.

[Click for more information](#)

04. Claims to have leaked a database from youX

The youX database breach represents one of the most significant financial data compromises in Australia, involving the theft of 300GB of sensitive data from the Australian B2B FinTech company (formerly known as Drive IQ). The incident spans from February 16-28, 2026, and was perpetrated by the threat actor FulcrumSec, who initially attempted ransom negotiations before ultimately releasing sample data and threatening full disclosure.

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – February 2026

01. Beyond Tax Returns: How Shared Malware Infrastructure Scales Brand Abuse In Indonesia

The GoldFactory threat cluster has launched a sophisticated fraud campaign in Indonesia, exploiting the 2026 tax season by impersonating the official Coretax platform to target 67 million residents. The attack utilizes an industrialized chain of phishing, WhatsApp social engineering, and malicious APK sideloading to deploy malware families like Gigabud.RAT and MMRat. By abusing over 16 trusted brands across the government and financial sectors, the campaign has resulted in an estimated nationwide financial loss of up to USD 2 million. Despite this horizontal scaling, advanced predictive modeling and behavioral detection have successfully neutralized the threat for protected institutions, maintaining a fraud success rate as low as 0.027%.

[Click for more information](#)

02. GTFire Phishing Scheme: Avoiding Detection Using Google Services

The GTFire phishing campaign demonstrates a sophisticated abuse of Google's own infrastructure, specifically leveraging Google Firebase and Google Translate to host and disguise malicious login pages. By using these trusted domains as intermediary "shields," attackers successfully bypass traditional security filters and exploit the high reputation of legitimate cloud services. The operation has achieved massive global scale, impacting over 1,000 organizations across 100 countries by harvesting credentials through highly convincing brand-impersonating templates. To maintain low visibility, the scheme automatically redirects victims back to legitimate websites after their data is stolen, a tactic that significantly delays the detection of the initial security breach.

[Click for more information](#)

03. Chinese MSS Discloses Infiltration of professional online groups by foreign intelligence operatives

On February 1, 2026, China's Ministry of State Security (MSS) issued a public disclosure warning against a pervasive "virtual espionage" threat involving foreign operatives posing as industry experts or investment advisers. These actors infiltrate professional platforms like WeChat and DingTalk, utilizing social engineering tactics such as "provocative baiting" to extract sensitive technical data and internal policy details. The campaign specifically targets "New Quality Productive Forces," turning legitimate professional networks into grey markets for state secrets and high-tech industrial intelligence. This report marks a strategic shift in global intelligence, highlighting a transition from traditional human intelligence toward a hybrid model that exploits the collaborative digital economy.

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – February 2026

04. Notepad++ hijacking: Updates in Security Incident

Following a previous security incident, the Notepad++ team confirmed that while the core application remained safe, a state-sponsored threat actor compromised their former hosting provider to abuse the WinGup auto-updater. This highly selective operation targeted a limited set of high-value organizations rather than the general user base, filtering victims based on strategic importance. Because the malicious updates were hosted on external infrastructure, the vendor has limited visibility into the full attack chain or the ultimate downstream impact on those affected. To assist in remediation, Notepad++ has released a set of "as-is" Indicators of Compromise (IoCs) derived from the compromised hosting environment.

[Click for more information](#)

05. Ghost in the Battery - GhostBat cryptojacking campaign

Learn about GhostBat - a sophisticated Android malware campaign that combines banking trojan capabilities with cryptojacking functionality. The campaign primarily targets Indian users through impersonation of banking applications and government services, resulting in both financial theft and unauthorized cryptocurrency mining on victim devices. These operations use fake Indian banking and government apps to steal sensitive data, including UPI PINs and Aadhaar numbers, while covertly mining cryptocurrency. By abusing Android permissions, the malware intercepts OTPs and exfiltrates device data to attacker-controlled Telegram and Firebase servers.

[Click for more information](#)

06. Publication of Data Related to Noel Gifts International Ltd

On February 13, 2026, a threat actor known as "Montaro" leaked sensitive data from the Singapore-based company Noel Gifts International Ltd on BreachForums. The breach, which reportedly occurred two days prior, resulted in the theft of nearly 23,000 B2B customer records and over 34,000 files from compromised AWS infrastructure. The stolen data includes names, phone numbers, and email addresses, with authenticity confirmed through overlaps with previous leaks and internal company domains. This incident highlights a significant compromise of the company's cloud storage and customer databases, specifically targeting their corporate gift and floral service operations.

[Click for more information](#)

07. Carousell Database Publication

On February 20, 2026, a threat actor known as "HighRisk" published two database archives on the Exploit forum belonging to the Singapore-based marketplace Carousell. Independent analysis of the leaked names and email addresses has confirmed the data's authenticity, showing no signs of automated generation or reliance on older public leaks. The publication includes both a full and a "cleaned" version of the data, marking the first time this specific dataset has appeared on the dark web. This suggests that the poster is likely the original attacker and the primary source of the breach involving the mobile-first C2C and B2C platform.

[Click for more information](#)

RANSOMWARE ACTIVITIES

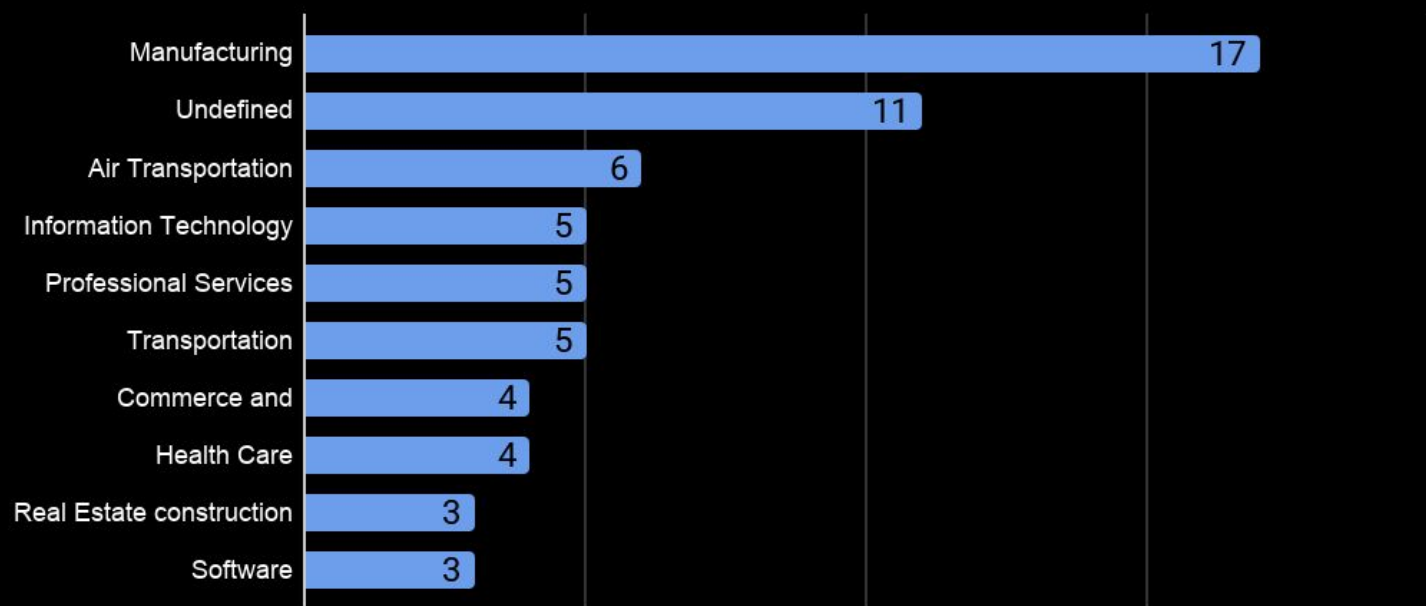
Key Events – February 2026

- Ransomware activity saw a slight increase of 7.41% compared to January. The Gentlemen turned out to be the most prolific threat actor with 29 attacks, that is about 262.5% increase in activity followed by Qilin which accounted for decrease of 37.5 percent in attacks.
- The Manufacturing sector was the primary target for the month, accounting for nearly 27% of all incidents, followed by undefined and air transportation sectors.
- In Singapore, APRO - Security & investigations, Perpetuuiti Technosoft - Enterprise Software, Obsidian Tech Labs - IT Company suffered from ransomware threats during the month.

58 Incidents ↑ 7.41%

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

Ransomware attacks, per industry



Top 10 targeted sectors, February 2026



Most Active Threat Actor Groups

The Gentlemen 29 activities		Qilin 10 activities	
0APT 6 activities	Vect 5 activities	DragonForce 4 activities	INC Blog 4 activities

Most Targeted Countries

India 18 activities		Thailand 14 activities	
Australia 8 activities	Taiwan 8 activities	Japan 7 activities	Malaysia 7 activities

DDOS AND HACKTIVISM

Top 6 Countries – Number of Activities per Country

Thailand
267

Bangladesh
23

India
16

Cambodia
12

Myanmar
2

Australia
1

324 Incidents ↑ 161%

Data: Number of Events

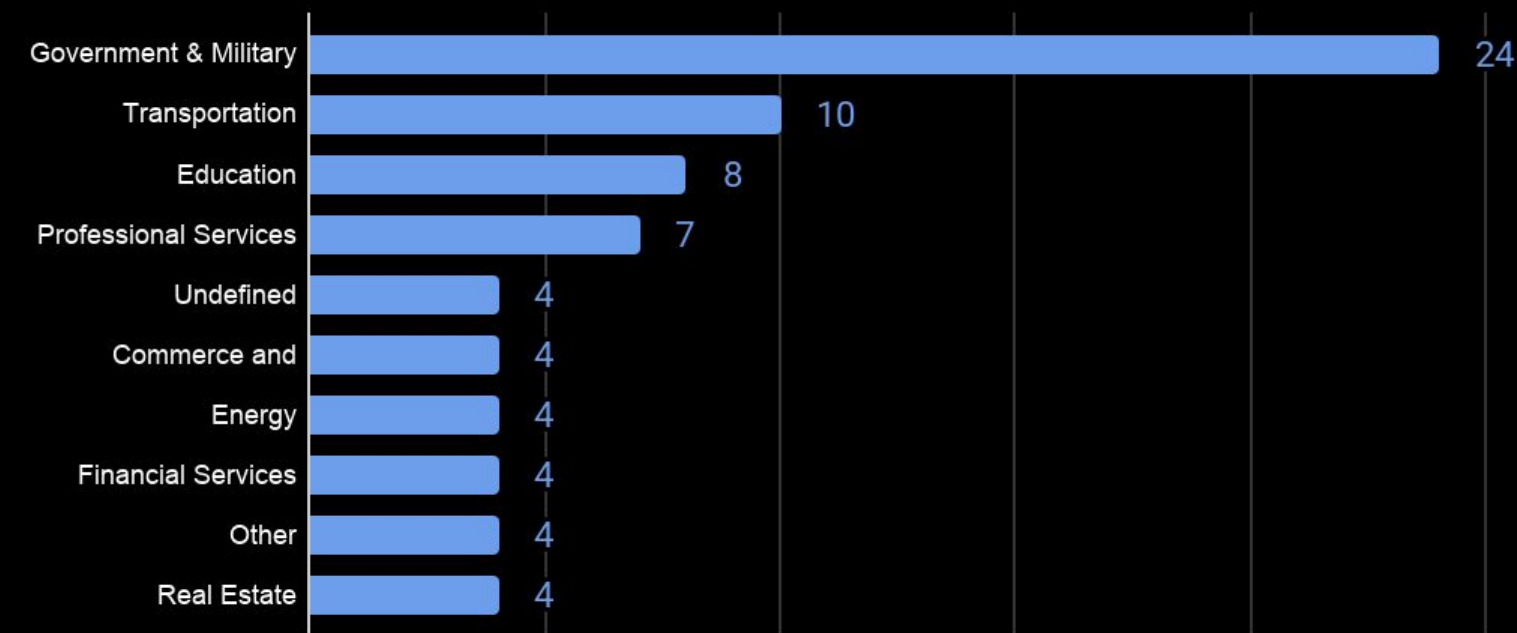
DDOS AND HACKTIVISM

In February 2026, the DDoS landscape experienced a rise with a total of 63 incidents, marking about 10.5% upward trend from the previous month. With this low increase in the volume the threat remains concentrated among a few aggressive actors, primarily led by the group RipperSec which accounted for over 39.7%, of all activity, followed closely by Noname057(16) and the Russian-linked Infrastructure Destruction Squad.

Geographically, there were more attacks on South Korea related to DDOS carried out by the TA RipperSec focused on Government and Military infrastructure which were primary targets of hacktivist and DDoS campaigns, with Transportation and Education also experiencing notable activity.

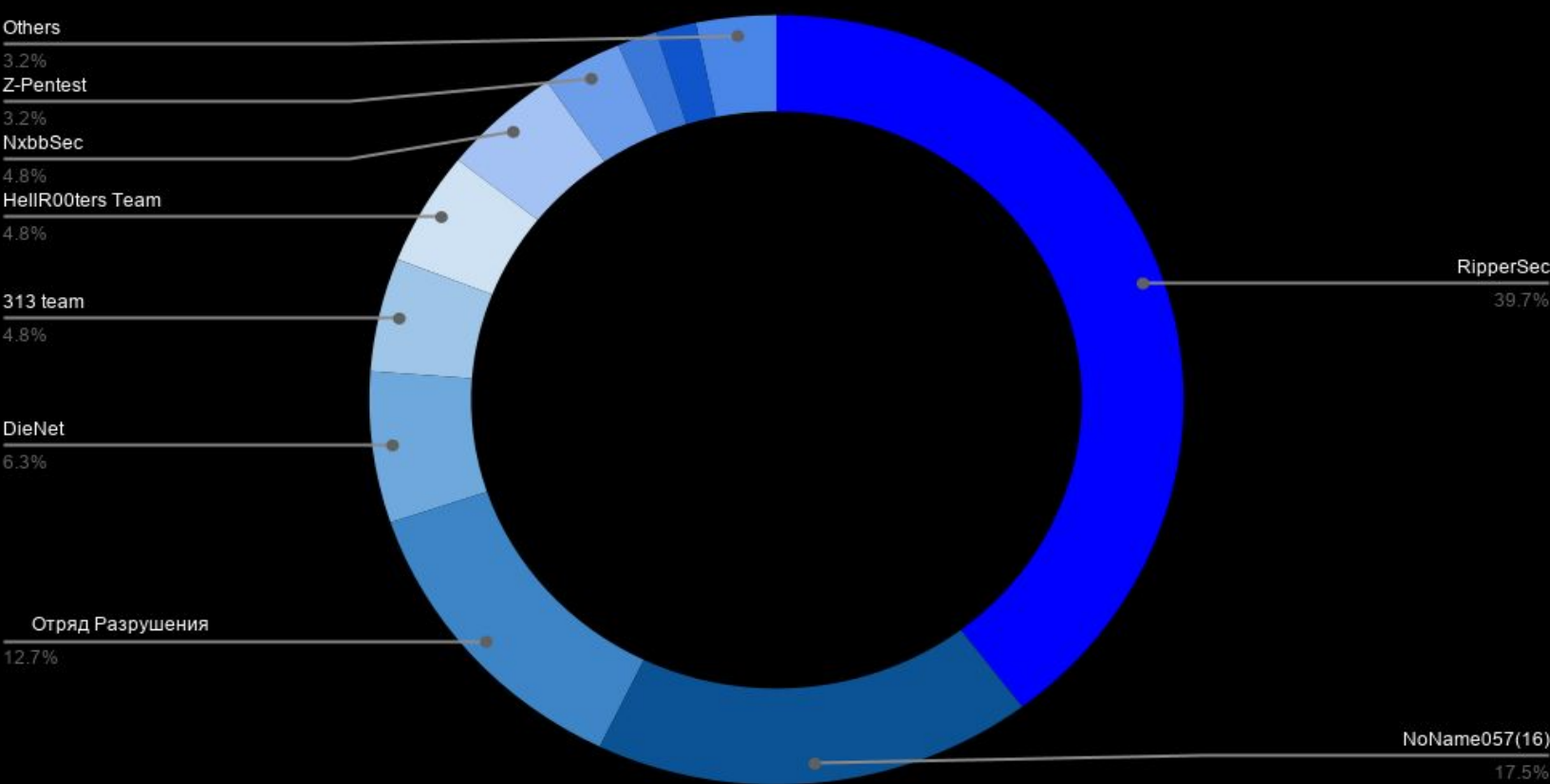
Data: Number of Events

DDOS and Hacktivism Activities, per industry



Top 10 targeted sectors, February 2026

DDOS and Hacktivism Activities, per group



COMPROMISED ACCOUNTS

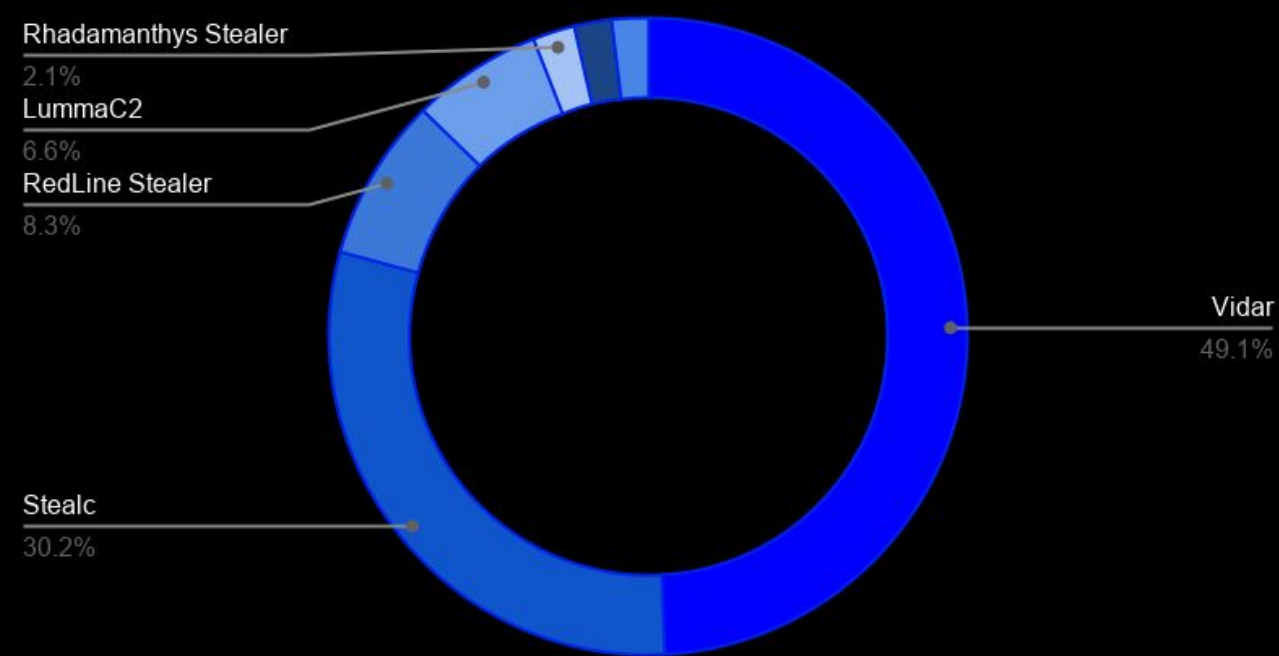
Key Events – February 2026

- The number of compromised accounts reached 2,337,460, representing an dip of -61.37% compared to January. The reason for this is that in January we onboarded a new source of compromised accounts. A large volume of data was ingested from this source, which caused a temporary spike in the statistics. The chart should now normalize and reflect the usual trend going forward.
- Vidar remained the dominant malware threat, responsible for nearly half of all compromises with 1,147,896 accounts, followed by Stealc (705,425) and RedLine Stealer (193,721).
- Geographically, India was the most impacted nation with 696,697 compromised accounts, accounting for 34.7% of the total. Other significant hotspots included Indonesia (327,249 accounts), Bangladesh (197,432 accounts), and Vietnam (189,046 accounts).

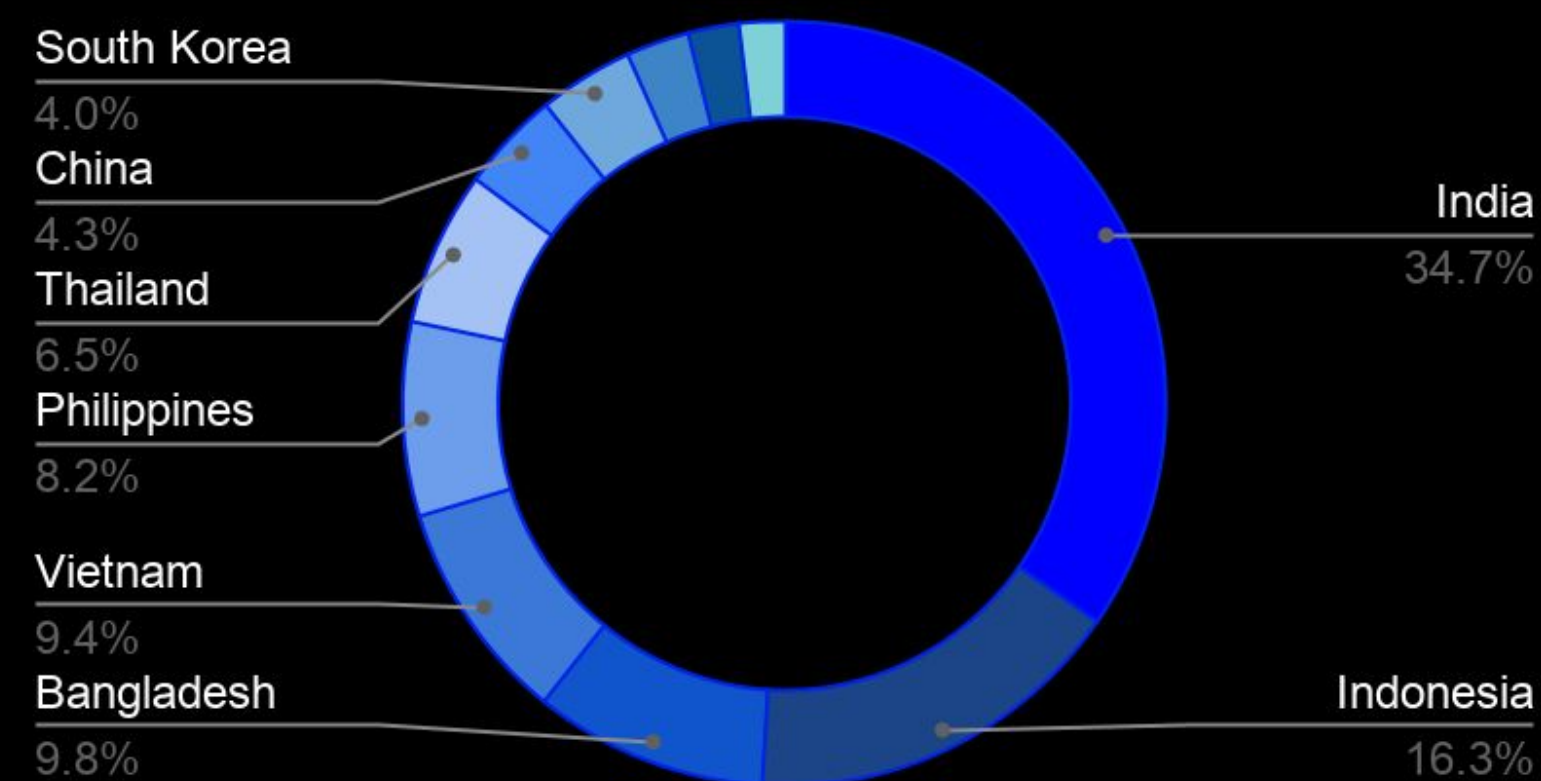
2,337,460 data leaks ↓ 61.37%

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

Compromised Accounts by Malware



Compromised Accounts by Country



COMPROMISED BANK CARDS



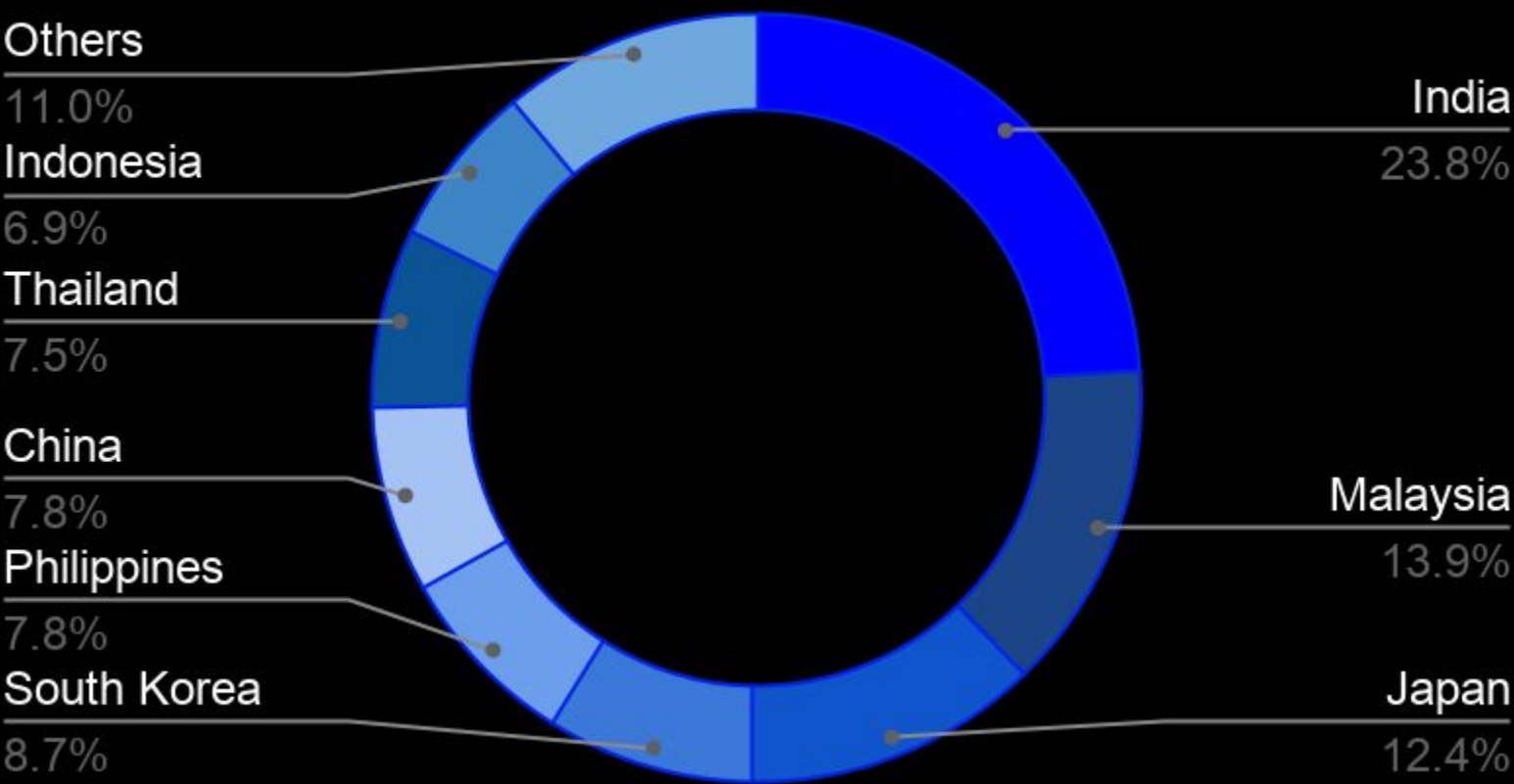
Key Events – February 2026

- In February 2026, the volume of compromised bank cards saw a further 10% decline, dropping to a total of 42,249 incidents. This activity was heavily concentrated in the Asia-Pacific region, with Malaysia, India, and Japan emerging as the primary targets. The distribution of this stolen data is increasingly centralized on Telegram, which serves as the leading source for nearly 68.5% of all compromises, followed by TG bot and leaks.

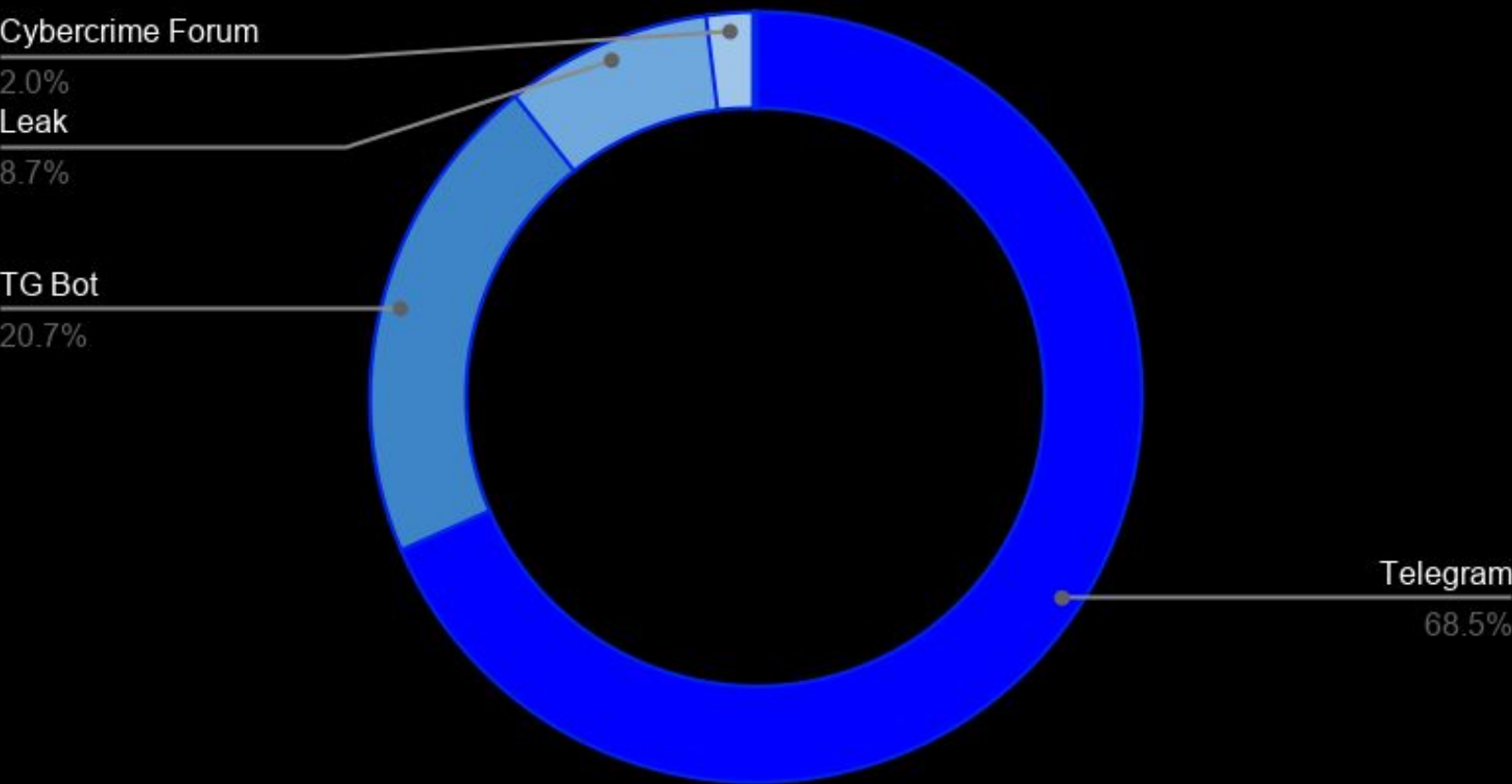
42,249 bank cards leaked ↓10.5%

Data: Percentage of Events

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