

December 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.

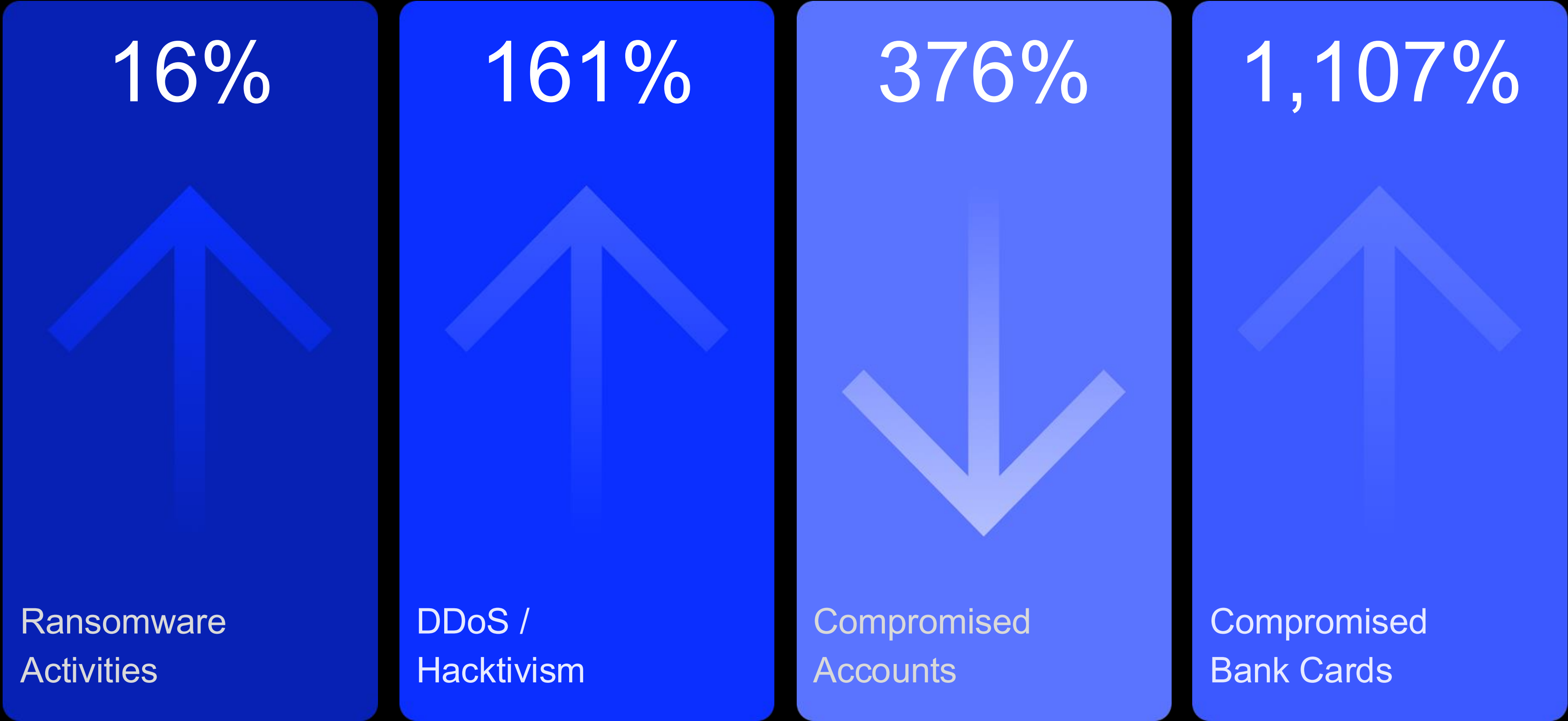
This report helps you:

- 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 November 2025 and December 2025



Key Findings & Global Cybersecurity Trends – December 2025

01. Stranger Threats Are Coming: Group-IB Cyber Predictions for 2026 and Beyond

Explore our strategic forecasts of the cyber threat landscape in 2026, with a focus on how autonomous attacks, AI-powered malware, agentic extortion, adversary-in-the-middle (AITM) threats, and AI-driven exploitation of crypto and stablecoin vulnerabilities will impact organizations globally and across the Asia-Pacific region. Our insights are powered by annual proprietary research, advanced data analytics, leading cybersecurity events, and collaboration with industry veterans.

[Click for more information](#)

02. Fighting Credit Fraud in Uzbekistan: An Uphill Battle Against Social Engineering

Online lending in Uzbekistan is growing rapidly, and so is credit fraud. Fraudsters commonly impersonate bank or government officials and use social engineering tactics such as fake calls or malware. This report examines the key drivers behind the surge in fraudulent loans and highlights practical security measures financial institutions can adopt. It also outlines recent government initiatives, including self-blocking of loan applications and legal exemptions that protect victims from repaying fraudulent debts.

[Click for more information](#)

03. Choose Your Fighter: A New Stage in the Evolution of Android SMS Stealers in Uzbekistan

Learn about the evolution of Android malware in Uzbekistan, with a new wave of attacks detected in October 2025 that leverage advanced droppers, encrypted payloads, and anti-analysis techniques. Attackers have shifted from distributing obvious trojan APKs to stealthy droppers disguised as legitimate apps, capable of silently deploying malware even without internet access. Group-IB analysts also profile a tracked threat actor group and introduces Wonderland, a previously unknown Android SMS stealer with bidirectional C2 capabilities that enables real-time commands, USSD requests, and SMS abuse.

[Click for more information](#)

Key Findings & Global Cybersecurity Trends – December 2025

04. Empty Promises in MENA: How Online Quick Cash Schemes Exploit the Gig Economy

Fake online job ads are widely circulating on social media in Arab countries, exploiting the post-COVID rise in remote work to lure victims with promises of easy income. These scams impersonate trusted companies or authorities and use localized language, currencies, and dialects to appear legitimate across MENA markets. Once users engage with ads on platforms like Facebook, Instagram, or TikTok, scammers move conversations to private messaging apps to steal personal and financial data. This blog explains how these organized schemes operate, who they target, and practical steps to avoid becoming a victim.

[Click for more information](#)

05. Emerging Spyware Campaign Leveraging Fake Updates to Compromise Messaging Apps

A spyware campaign targeting popular messaging apps was revealed following a CISA alert in late November 2025. Using commercial spyware delivered via phishing, malicious QR codes, impersonation, and zero-click exploits, attackers gain access to accounts and sensitive communications. The campaign remains active across the US, Middle East, and Europe, primarily targeting high-value individuals such as government, military, and civil society figures, with multiple threat actors suspected.

[Click for more information](#)

06. Overview of Intellexa Predator Attack Architecture: From Exploits To Covert Espionage

Learn about a prolonged and technically sophisticated surveillance campaign leveraging Intellexa's Predator spyware against iOS and Android devices. The operation uses advanced zero-day exploit chains and multiple delivery vectors, including malicious links, ISP-level traffic injection, and abuse of online advertising infrastructure, to achieve stealthy, high-privilege access. Based on the research findings, the report also provides key insights and defensive recommendations.

[Click for more information](#)

Key Findings & Global Cybersecurity Trends – December 2025

07. World-Class Exploitation of React2Shell (CVE-2025-55182) Vulnerability

Group-IB analysts have prepared a detailed analysis of the critical vulnerability known as React2Shell (CVE-2025-55182), synthesizing information regarding its technical mechanics, observed exploitation by various threat actors, and recommended defense and detection strategies.

[Click for more information](#)

08. Cyber Attack on Venezuelan Oil & Gas Industry

In December 2025, PDVSA confirmed a major cyberattack that deployed destructive wiper malware, affecting its administrative and logistical systems and effectively halting crude export operations. While operational technology systems remained intact, the attack disrupted cargo scheduling, certification, and clearance, forcing terminal shutdowns and tanker diversions. This report describes the incident using OSINT, shipping data, and malware analysis, framing it as a potential case of hybrid warfare following closely after geopolitical tensions involving Venezuelan oil assets. The incident highlights an escalating cyber risk for state-owned oil and gas enterprises worldwide.

[Click for more information](#)

09. ZeroDay GitHub Exposure: Analysis Of Public Phishing Kits

Group-IB analysts have discovered ZeroDay GitHub by analysing scans of phishing URLs on URLscan. These scans displayed custom CAPTCHA/Cloudflare-like verification pages and were communicating with a GitHub-hosted text file that was used to retrieve a randomly selected redirect URL.

[Click for more information](#)

Key Findings & Global Cybersecurity Trends – December 2025

10. APT42 AI-Enhanced Operations using Gemini LLM

Group-IB analysts have monitored and analyzed the activity of APT42 on using AI to automate the processing of sensitive intelligence data, from building a custom utility to operationalize stolen data, conducting spear-phishing, to utilizing Gemini to increase the credibility and speed of their lure creation.

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – December 2025

01. Hook For Gold: Inside GoldFactory's Campaign That Turns Apps Into Goldmines

Group-IB analysts have continuously monitored GoldFactory, the actor group that has been operating mobile trojans targeting both iOS and Android users. We have identified more than 300 unique samples of modified banking applications and over 11,000 infections, demonstrating the growing scale and sophistication of these campaigns. The threat actor impersonated government services to gain trust and used publicly available frameworks to intercept and alter app behavior. The group also deployed loaders including Gigabud, Remo, MMRat, and a new test variant, Gigaflower, with experimental OCR and QR scanning features.

[Click for more information](#)

02. 80GB Of Data For Sale: Cal-Comp Electronics

On 1 December 2025, a threat actor with the nickname el_farado posted 80GB of data of the Thai electronic computer manufacturing company Cal-Comp Electronics for sale. The actor also published documents containing sensitive data such as technical documentation, internal messages, and a map of the security infrastructure (cameras, guard posts, schedules, access procedures, etc.), with timestamps until November 2025, which may indirectly indicate the date of the data breach and the validity of the stolen data.

[Click for more information](#)

03. SQL Database Publication For Internal Domain Of Department Of Agriculture Of Thailand

On 14 December 2025, a threat actor named Chucky\Leakbase published the SQL database of the Department of Agriculture of Thailand. The published SQL database included personal information (names, ID numbers, phone numbers, addresses, emails) of 11,874 Thai farmers and their families.

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – December 2025

04. The Rise of Fake Shipment Tracking

Learn about Dracula, a Ph-a-a-S (Phishing as a Service) Chinese-language platform which has been used in phishing attacks against organizations (government, airlines) and services (postal, financial) in over 100 countries. Dracula offers to cybercriminals more than 20,000 counterfeit domains (to spoof brands) and over 200 templates.

[Click for more information](#)

05. APT SideWinder Activity Targeting Border Guard Bangladesh (BGB) and Bangladesh Computer Council (BCC)

Group-IB analysts identified a SideWinder campaign targeting Bangladeshi government institutions, including the Border Guard Bangladesh (BGB) and the Bangladesh Computer Council (BCC). The attackers used phishing emails with malicious lures that directed victims to fake login pages. To access decoy documents, targets were tricked into entering their email credentials, enabling credential theft.

[Click for more information](#)

06. Tracking DPRK IT Workers Activity Through Technical and Behavioral Indicators

Learn about the recent discovery regarding highly dangerous IT Workers scheme, including the relationships between these accounts, highlight selected resumes, and describe the tools used by the threat actors to seek employment in legitimate companies.

[Click for more information](#)

REGIONAL INSIGHTS



Key Findings & Regional Cybersecurity Trends – December 2025

07. Error524: Analysis Of A Multi-Brand Smishing And Phishing Campaign

Learn about a large-scale smishing and phishing campaign active since the second half of 2025, targeting users across industries such as loyalty programs, logistics, financial services, telecommunications, and energy. The operation focuses mostly on LATAM but extending to countries in APAC region such as China, Vietnam, Thailand, using localized SMS messages and shortened links to steal personal and credit card data. The infrastructure is highly optimized, relying on Cloudflare-proxied phishing sites, real-time monitoring, and phishing-as-a-service toolkits.

[Click for more information](#)

RANSOMWARE ACTIVITIES

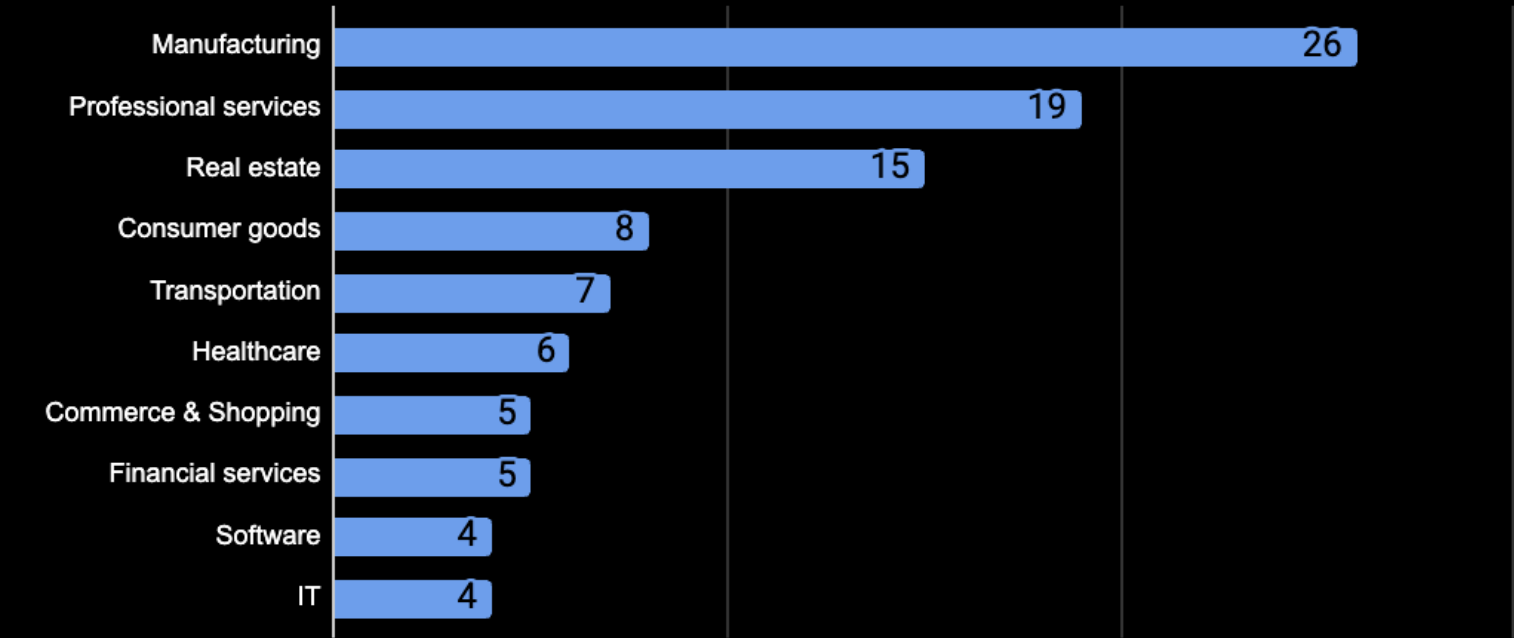
Key Events – December 2025

- The main threat actor groups for the past few months continue to be **The Gentlemen**, **Qilin** and **Dire Wolf** (click [here](#) for November 2025 edition).
- **Manufacturing** continues to be the most targeted sector, followed by **Professional Services** and **Real Estate**.
- **LockBit** returns with some ransomware attacks against cooperations in India, Thailand and Malaysia

106 Incidents ↑ 16%

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

Ransomware Attacks by Industry – Top 10 Targeted Sectors



Most Active Threat Actor Groups

Qilin		Lockbit	
17 activities		15 activities	
↑ 142%			
Dire Wolf	SafePay	The Gentlemen	RaLord
11 activities	10 activities	6 activities	5 activities
↑ 10%		↓ 45%	

Most Targeted Countries

India		Malaysia	
13 activities		13 activities	
↓ 7%			
Australia	Japan	Singapore	Thailand
12 activities	12 activities	11 activities	10 activities
↓ 20%	↑ 33%		

DDOS AND HACKTIVISM

Top 6 Countries – Number of Activities per Country

Thailand
267*

Bangladesh
23

India
16

Cambodia
12

Myanmar
2

Australia
1

* This number is nearly 9
times than November 2025

324 Incidents ↑ 161%

Data: Number of Events

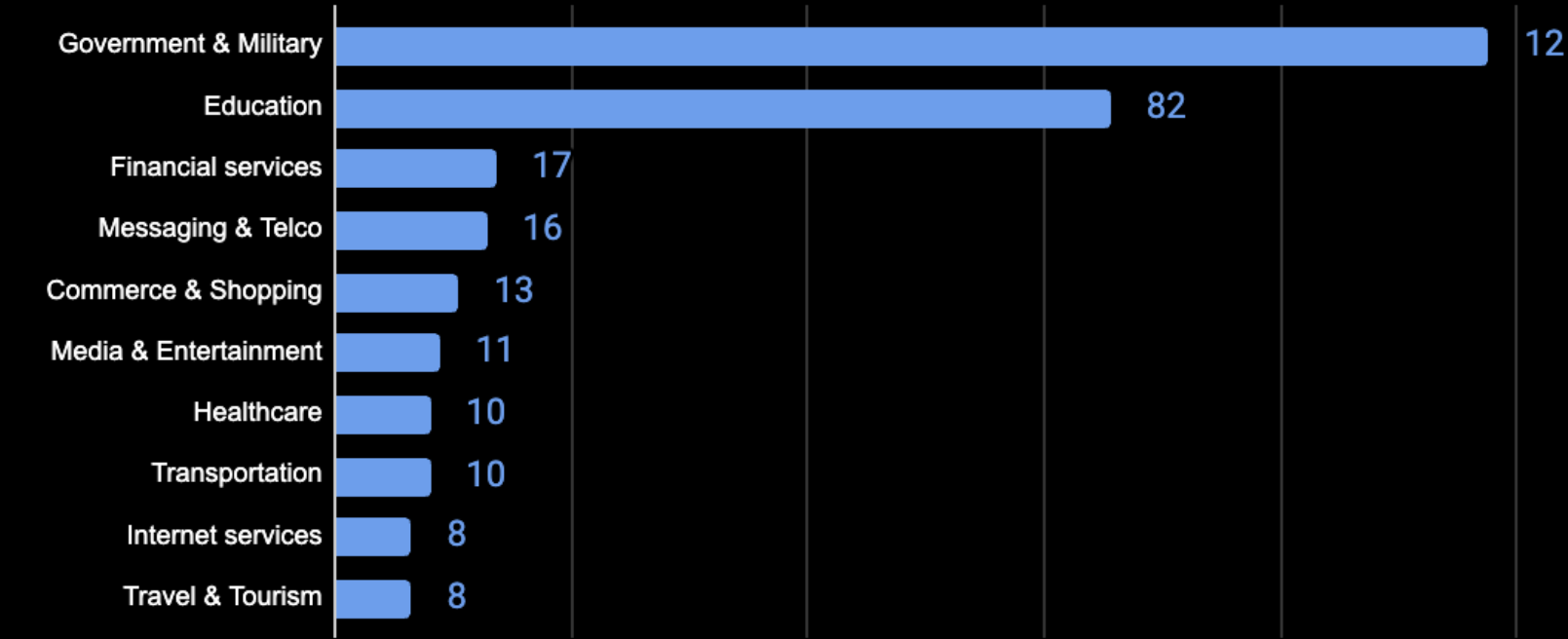
DDOS AND HACKTIVISM

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).

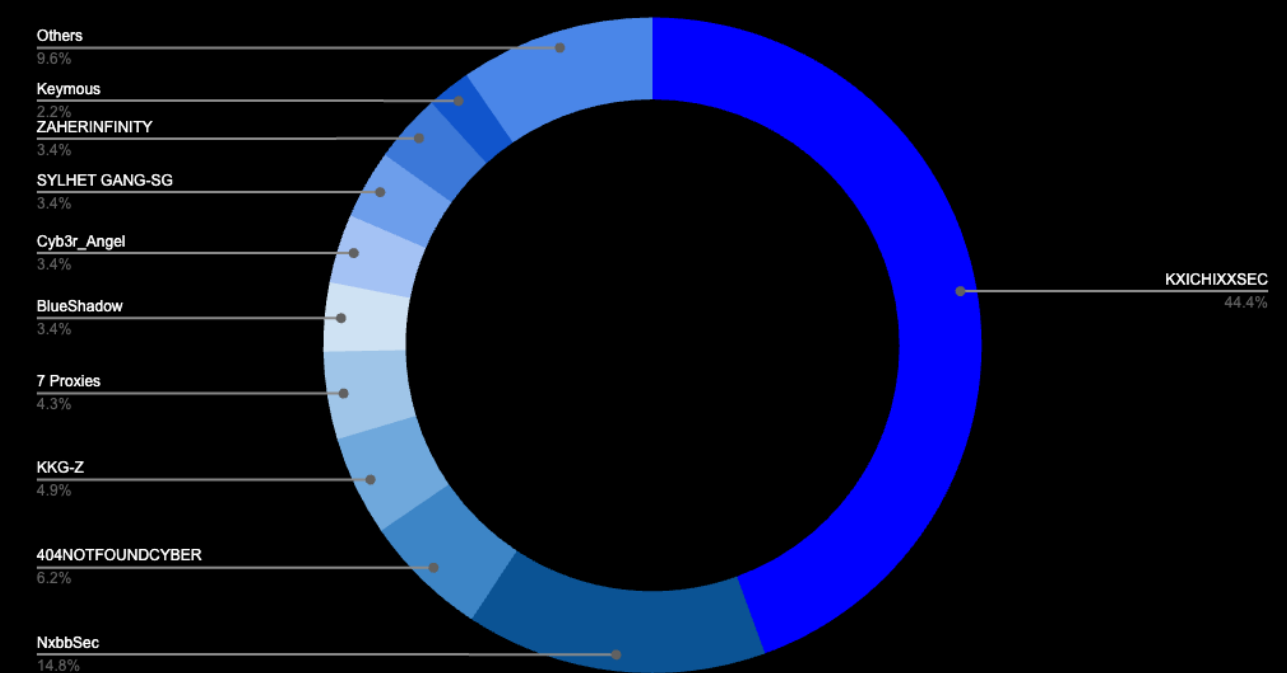
Many DDoS and Hacktivism incidents during December 2025 were due to recent political tensions, with Thailand experiencing 9 times more incidents compared to November 2025. Most of the activities were from KXICHIXXSEC, a Cambodian hacktivist threat actor which appeared during the conflict between Cambodia and Thailand, and is known for conducting attacks on Thailand government body websites. Other main actors continue to be NXBBSEC and 404NOTFOUNDCYBER. A new notable hacktivist group motivated by the political tension is KKG-Z (first seen in December 2025), 7 Proxies (first seen in April 2025) and BlueShadow (first seen in December 2025)..

Data: Number of Events

DDoS and Hacktivism Activities by Industry



DDoS and Hacktivism Activities by Threat Actor Group



COMPROMISED ACCOUNTS

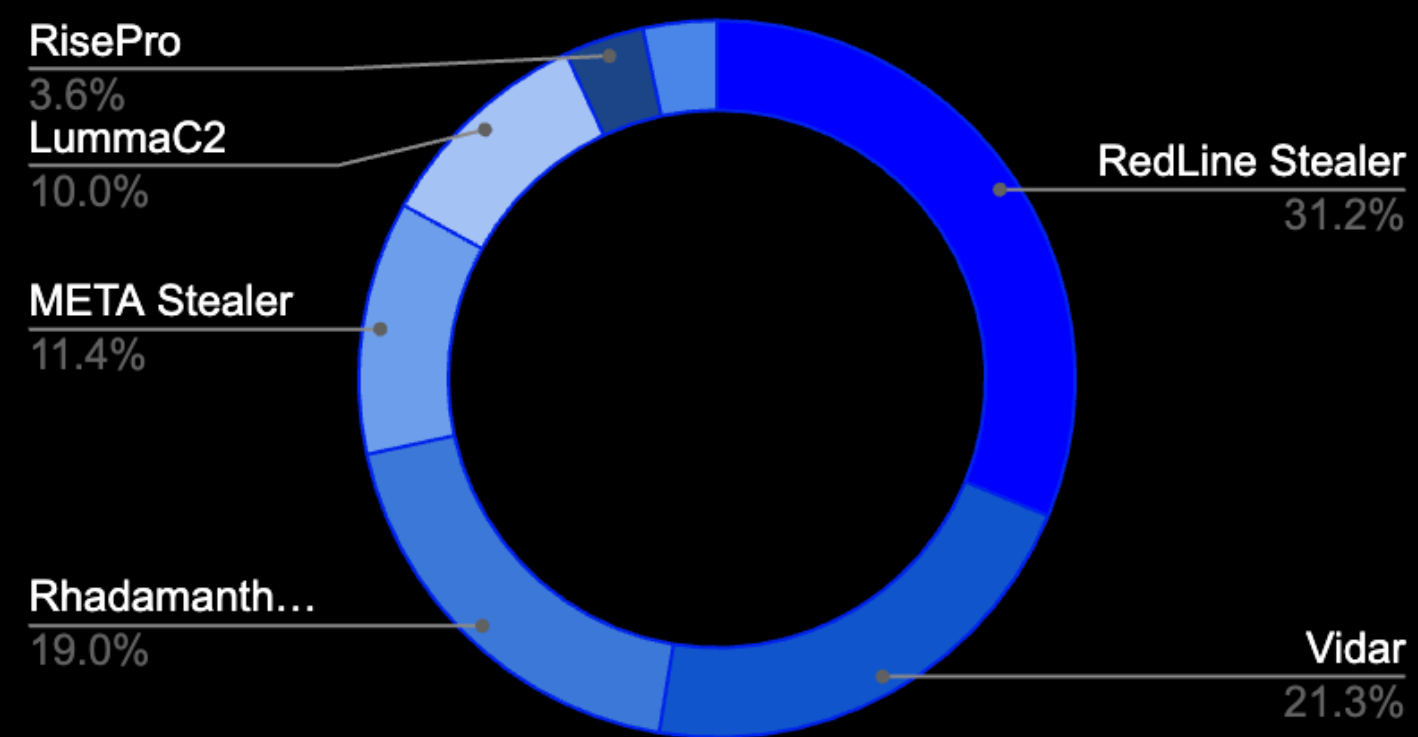
Key Events – December 2025

- 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 more than 31% of compromises; followed by LummaC2, Stealc, and RisePro.
- Rhadamanthys Stealer, which targets different browsers such as Brave, Edge, Chrome, Firefox and Opera Software, emerges among the top 3 malware this month.

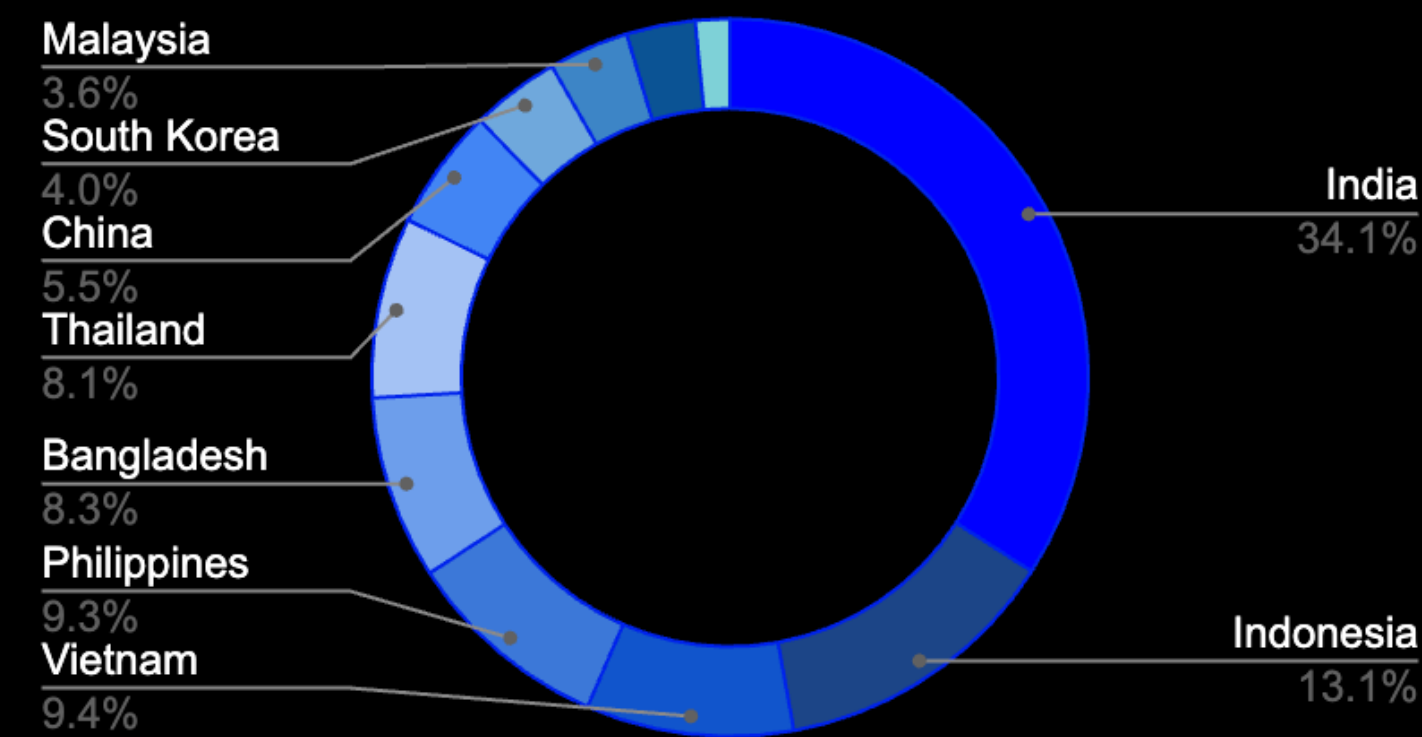
5,553,033 data leaks ↓ 376%

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

Compromised Accounts by Malware



Compromised Accounts by Country



COMPROMISED BANK CARDS

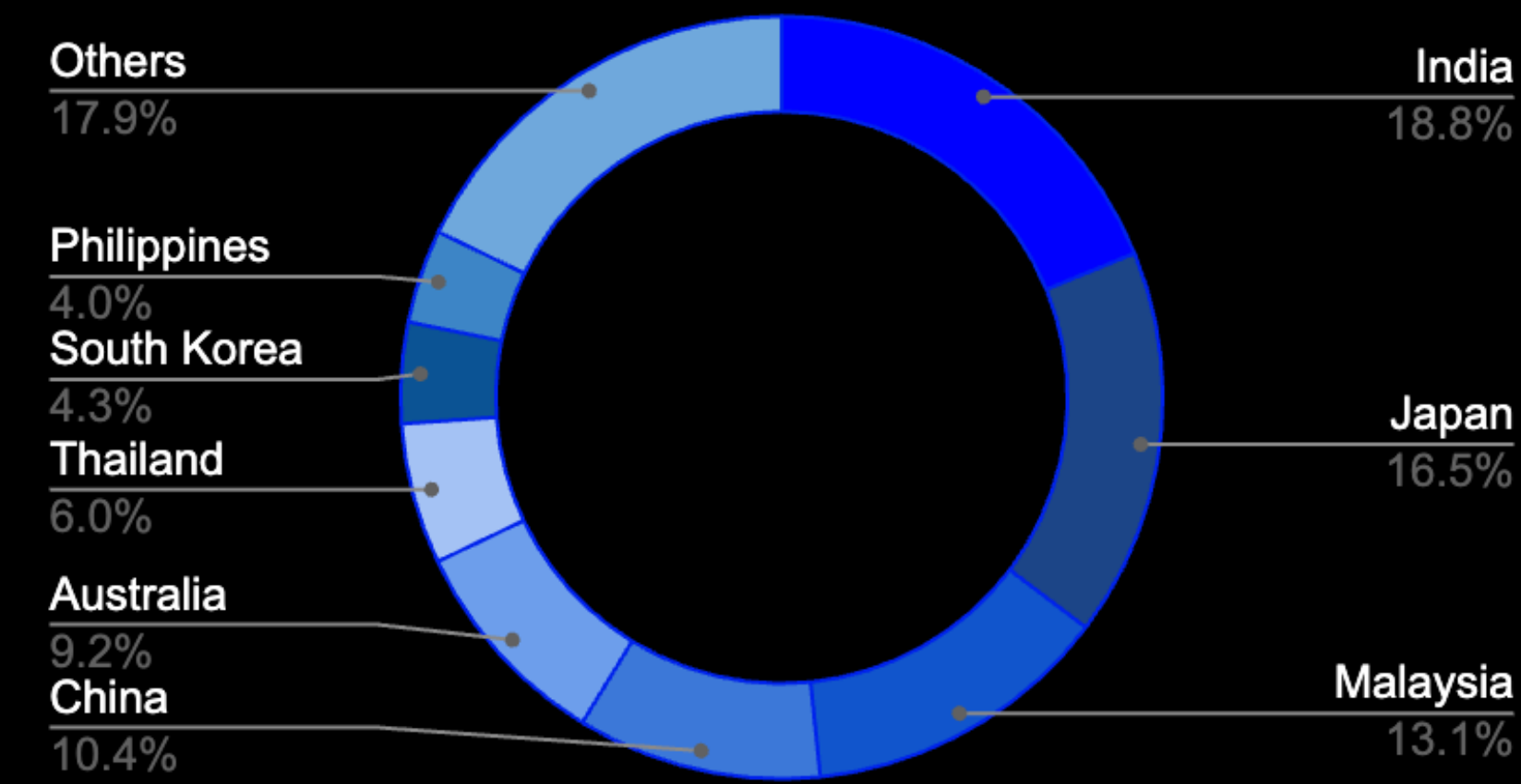
Key Events – December 2025

- 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.
- Significant increase in number of compromised bank cards recorded due to Group-IB’s constant efforts in finding and adding new sources in order to provide more comprehensive information.

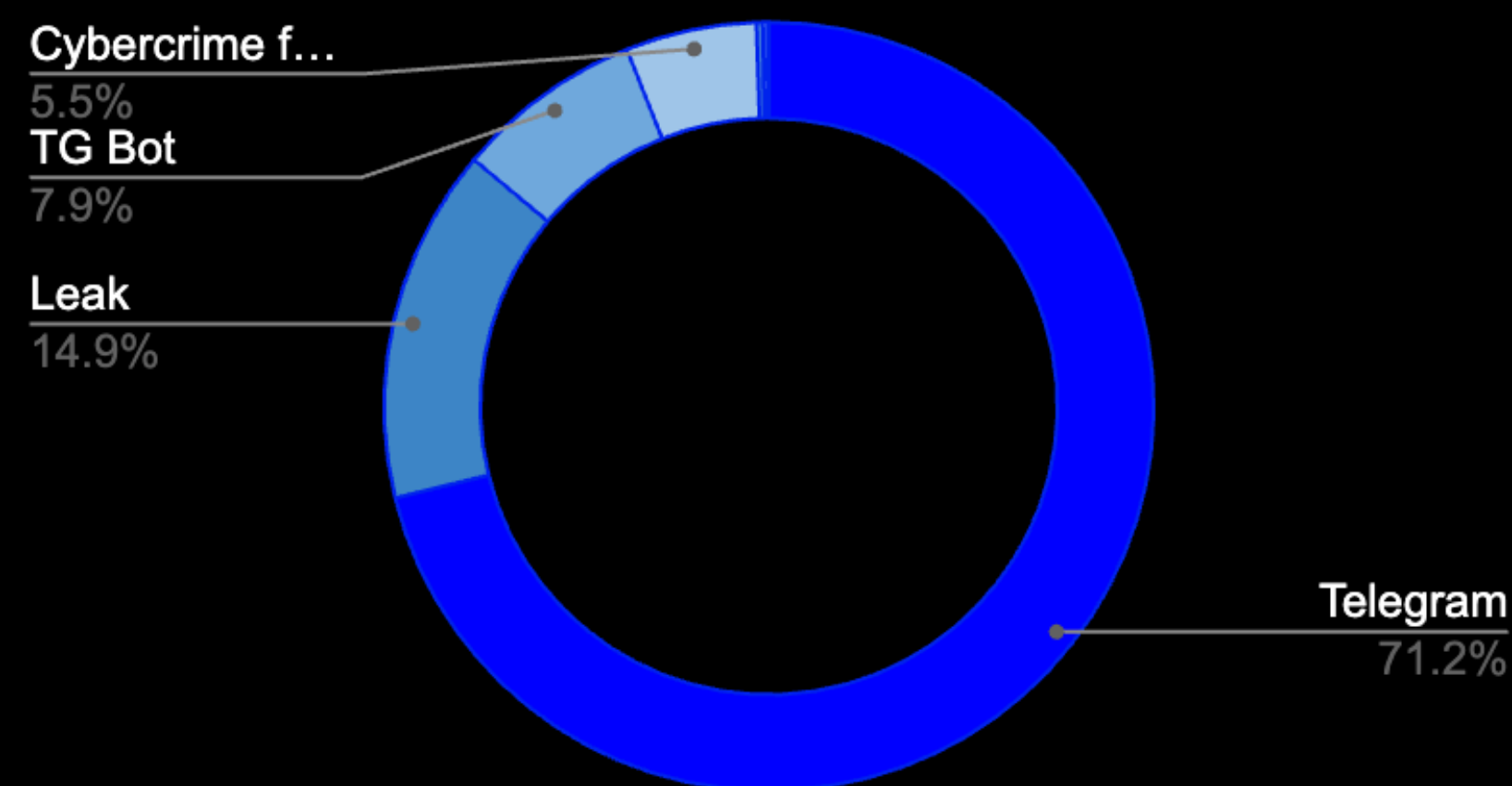
56,8965 bank cards leaked ↑ 1017%

Data: Percentage of Events

Compromised Bank Cards by Country



Compromised Bank Cards by Source Type



ADVERSARY OF THE MONTH



Threat actor group

KXICHIXXSEC

Targeted industries:

Education, Government & Military, Health Care, Commerce & Shopping, Food & Beverage, Financial Services, Real Estate, Consumer Electronics, Data & Analytics, Hardware, Information Technology, Internet Services, Messaging & Telco, Content & Publishing, Media & Entertainment, Manufacturing, Transportation, Professional Services, Travel & Tourism.

Period of Activity:

July 2025 – Present

Targeted countries:

Thailand, Vietnam, Sweden

Attribution:

Cambodia

Intent:

APAC-tension

Attack Summary

- KXICHIXXSEC, or NUNZTAMZY, is a Cambodian hacktivist threat actor active since July 26, 2025. The group appeared during the conflict between Cambodia and Thailand, and primarily attacks Thai websites with DDoS attacks and amplifies messages from other Cambodian hacktivists like NXBBSEC, BL4CK CYB3R and others.

Key Observations

- In December 2025, the hacktivist group is observed to have 144 attacks, most of which were defacement activities on multiple organizations including Thailand Department of Employment, Ministry of Labour, Royal Society of Thailand, and Office of the Private Education Commission.
- The group's main target is Thailand government and education websites, while also conducting some attacks towards some organizations in Vietnam.

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

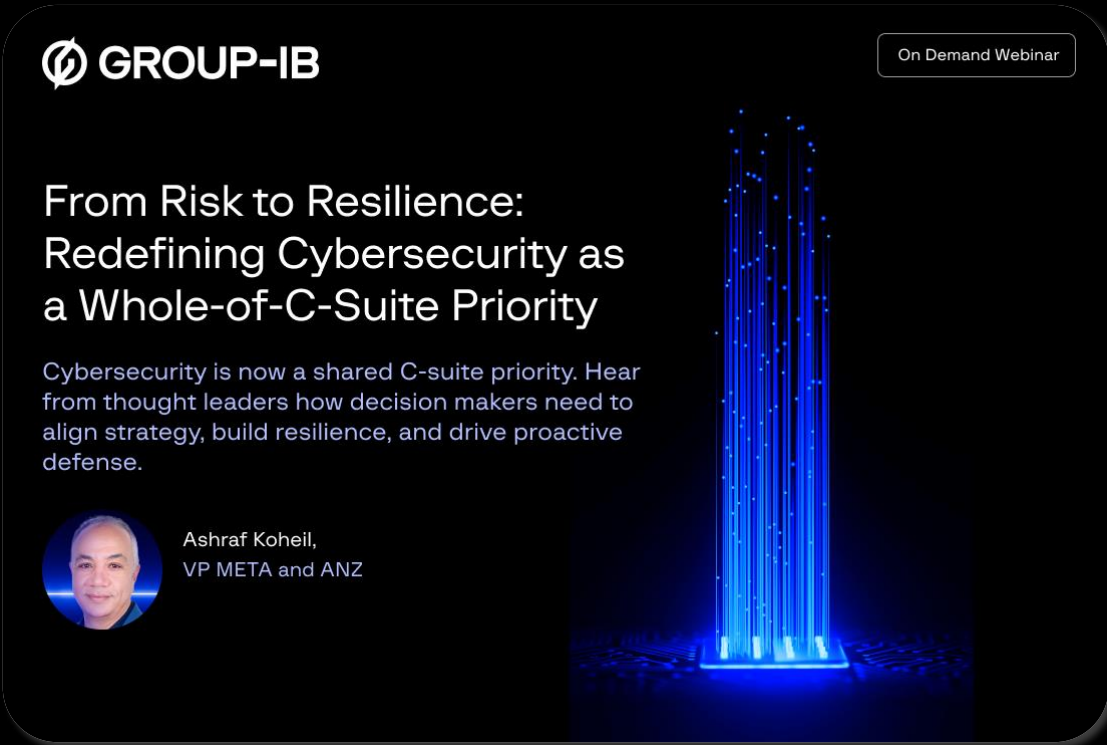
RECENT RESOURCES



Read now



Discover more



Watch now

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003