

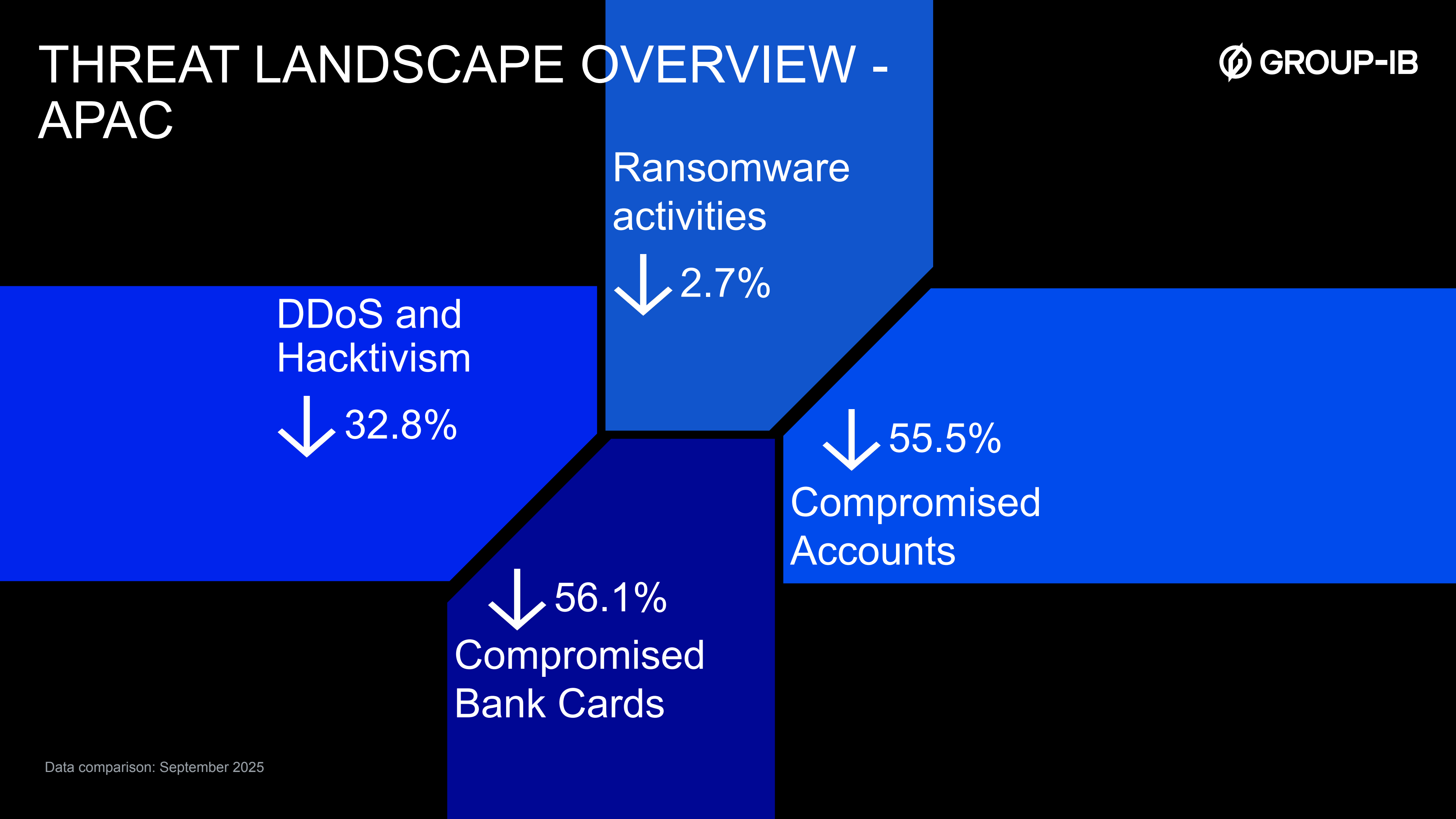


# INTELLIGENCE INSIGHTS. AUNZ

Executive Summary and Key Insights for October 2025

Report is based on data from 01.10.2025 till 01.11.2025

# THREAT LANDSCAPE OVERVIEW - APAC



# GLOBAL INSIGHTS

Global Insights from Group-IB with a brief description:

01

## **Nation State Actor UNC5221 Compromised F5's Internal Network**

In August 2025, F5, a leading cybersecurity and application delivery company, detected unauthorized access to its internal systems by a highly sophisticated nation-state threat actor. The intrusion, which involved persistent access and file downloads, targeted the BIG-IP product development environment and engineering knowledge management platforms. This incident underscores ongoing challenges in securing software supply chains, with no immediate operational disruptions reported by F5. [More Information.](#)

02

## **Red Hat breach: Crimson Collective advertises the data for sale**

October 13, 2025: Despite the initial 2025-10-10 deadline of the Red Hat breach, the full data has not been publicized at the time of writing, and Crimson Collective posted a message advertising the data for sale, priced at \$400,000 – \$500,000. The DLS (shinyhunte[.]rs) listing of Red Hat remains marked “active”, and not “leaked”, with the same deadline and no additional samples posted. [More Information.](#)

03

## **Dozens of websites, banks and apps are being affected by a major AWS outage**

A major Amazon Web Services (AWS) outage on October 20, 2025, caused widespread disruption to many websites, apps, and banking services globally. The outage was triggered by a technical update to a key database service that led to Domain Name System (DNS) errors, making it impossible for many platforms to be reached. [More Information.](#)

04

## **Inside the Brazilian WhatsApp Trojan Surge: Self-Spreading Malware Targets Banking Users**

A malware campaign was recently detected in Brazil, distributing a malicious LNK file using WhatsApp. It targets mainly Brazilians and uses Portuguese-named URLs. To evade detection, the command-and-control (C2) server verifies each download to ensure it originates from the malware itself. [More Information.](#)

05

## **Unmasking MuddyWater's New Malware Toolkit Driving International Espionage**

A recent phishing campaign, attributed with high confidence to the Iran-linked MuddyWater group, targeted over 100 government entities across the Middle East and North Africa. The attackers used a compromised mailbox accessed via NordVPN to send convincing phishing emails disguised as legitimate correspondence. These emails contained Word documents that executed malicious VBA macros to deploy the Phoenix backdoor v4. The campaign highlights how state-backed actors exploit trusted communication channels to evade detection. [More Information.](#)



# REGIONAL INSIGHTS

Regional Insights from Group-IB with a brief description:

01

## **Database Sale. Pruksa Real Estate Public Company Limited, Thailand (Pruksa.com)**

On October 30, 2025, a threat actor with the nickname AgSlowly from the Darkforums forum created a thread announcing the sale of data allegedly belonging to Pruksa Real Estate Public Company Limited, a real estate development company in Thailand. [More Information.](#)

02

## **Leaked source code from SkoolBeep**

On October 30, 2025, in a continued series of source code exfiltration, a threat actor with the nickname 888 leaked source code claimed to be related to SkoolBeep, an India-based school management and parent-communication platform. [More Information.](#)

03

## **Crypto24 Ransomware attack on Bayu Buana Travel Services**

On 2025-10-27, the ransomware group Crypto24 claimed responsibility for an attack targeting Bayu Buana Travel Services. 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. [More Information.](#)

04

## **Leak of SQL Database of Islamic Banking & Finance Institute Malaysia (IBFIM, ibfimonline.com)**

On October 25, 2025, in the private Telegram channel "Goldpack", belonging to the well-known threat actor Chucky\Leakbase, a SQL database of the Islamic Banking & Finance Institute Malaysia (IBFIM, ibfimonline[.]com) was published. [More Information](#)

05

## **Exposing the Immediate Era Fraud in Singapore**

Group-IB recently uncovered a scam operation targeting Singapore, which uses the images and likeness of local officials to lure victims into a fake investment platform. The campaign leverages paid Google Ads and layered redirect sites leading to a Mauritius-registered forex platform, fronted by a licensed legal entity to appear legitimate. By combining verified ads, fake media outlets, and deepfake technology, scammers created a sophisticated cross-border fraud scheme that mimics real financial services and exploits public trust. [More Information](#)

06

## **The Illusion of Wealth: Inside the Engineered Reality of Investment Scam Platforms**

Learn about investment scam campaigns where people are lured into fraudulent forex/crypto trading platforms. The report explains step-by-step how the scammers utilize social engineering tactics, manipulate the victims to deposit and withdraw money. We also describes the fraud actor structures behind these schemes, and highlights key infrastructure artifacts identified. [More Information](#)



# LOCAL INSIGHTS

Local Insights from Group-IB with a brief description:

01

## Qantas Airways Limited data published on “Scattered LAPSUS\$ Hunters” DLS

On October 10, 2025, the threat group “Scattered Spider/ShinyHunters/Lapsus” (now abbreviated as SLSH) published data from several victims on its data leak site, including Qantas Airways, Australia’s flag carrier. The Qantas breach, first disclosed on June 30, 2025, affected the airline’s contact center in Manila, Philippines. Attackers reportedly gained access to Qantas’s Salesforce customer service platform during a call with a support agent. The leaked data includes names, phone numbers, frequent flyer details, birthdates, gender, location data, and session information. [More Information.](#)

02

## Ransomware activities during the month

In addition to SLSH's activities, other actor groups continue to be active in attacks against Australia. Notable names such as Qilin, Anubis, CI0p, etc. announced multiple ransomware attacks to organizations of various industries, including OzSoft Solutions, Aip Asset Management, Cavalry Consulting, Kevmor, etc. [More Information on Group-IB Threat Intelligence Portal.](#)

03

## DDoS and Hacktivism activities during the month

Although there was only one hacktivism incident recorded in October 2025, Australia continued to observe DDoS and Hacktivism due to the political tension, especially the Palestine-Israel conflict. Seacret, an Israeli-American cosmetics company, were targeted by CyberToufan actor group who claimed to have information from this company's e-commerce website, including sensitive information such as emails, passwords, phone numbers, and home addresses of customers. [More information on Group-IB Threat Intelligence Portal.](#)



# RANSOMWARE ACTIVITIES (APAC)

↓ 2.7%

70 ransomware incidents

Statistics regarding ransomware activities in October 2025:

- Qilin continued to be in the top most active actors in terms of ransomware activities every month, targeting different countries, especially APAC region.
- The sector landscape is very different from the previous month, with the top targeted industries Undefined, but manufacturing and financial services remain up in the list.

Most active threat actors

**Qilin**

16 activities  
-40.74%

**The Gentleman**

10 activities  
+11.11

**Devman**

4 activities

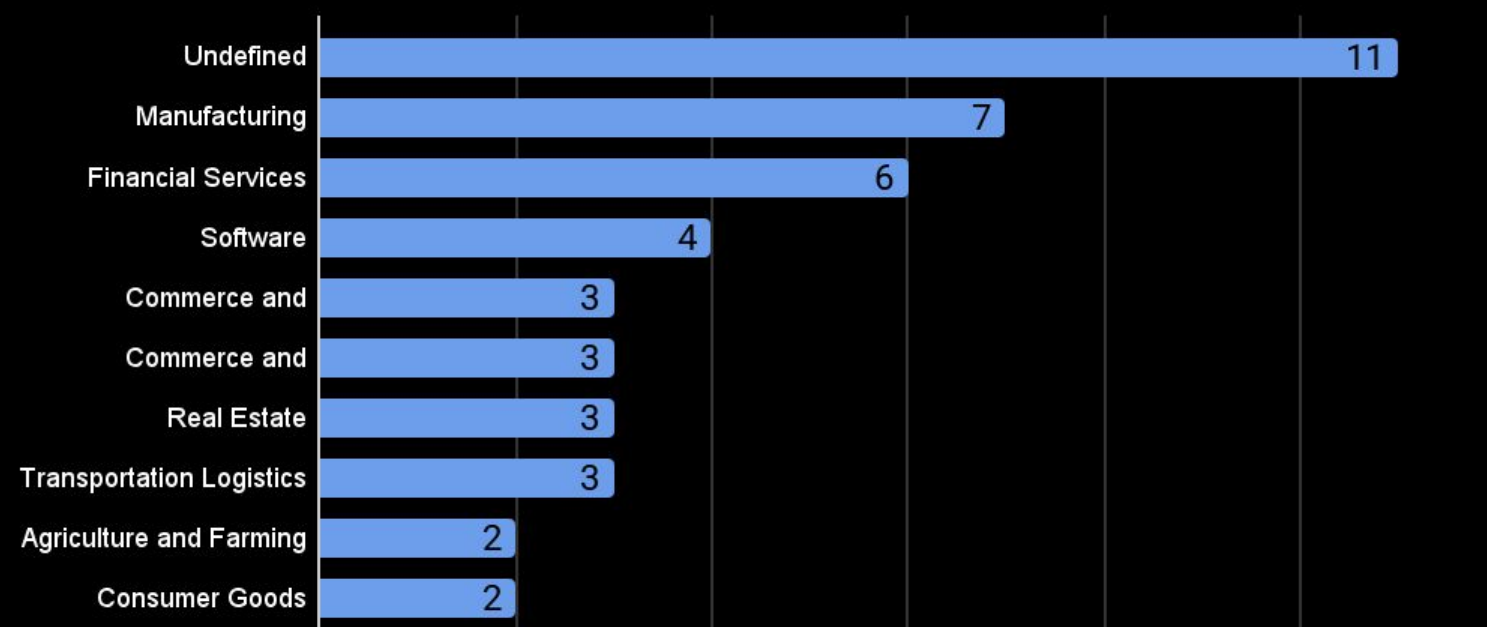
**SafePay**

4 activities

**White Rabbit**

4 activities

## Ransomware attacks, per industry



Top 10 targeted sectors, October 2025

Most targeted Countries

**Australia**

19 activities  
+171.43%

**Japan**

9 activities  
+125.00%

**India**

8 activities  
-33.33%

**South Korea**

7 activities  
-75.00%

**Indonesia**

5 activities  
+150.00%

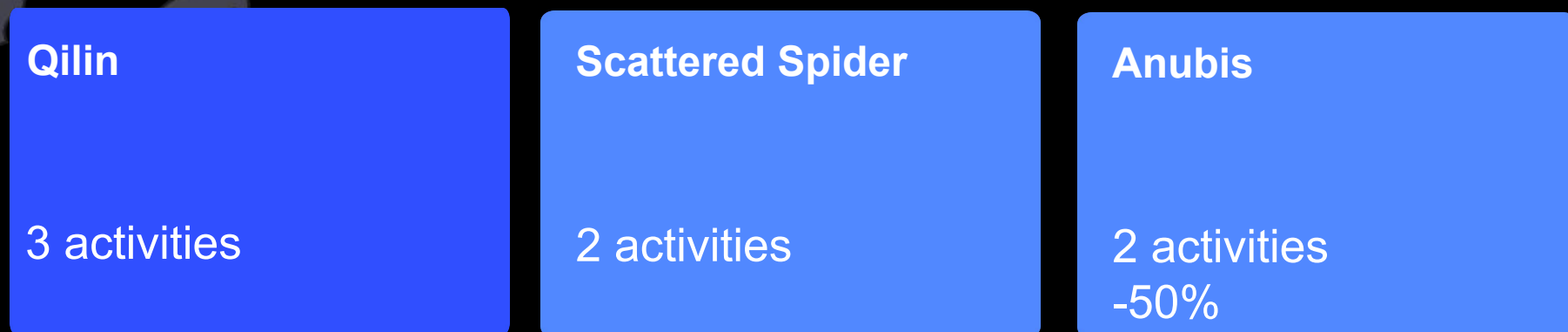
# RANSOMWARE ACTIVITIES

## (Australia) 19 ransomware incidents

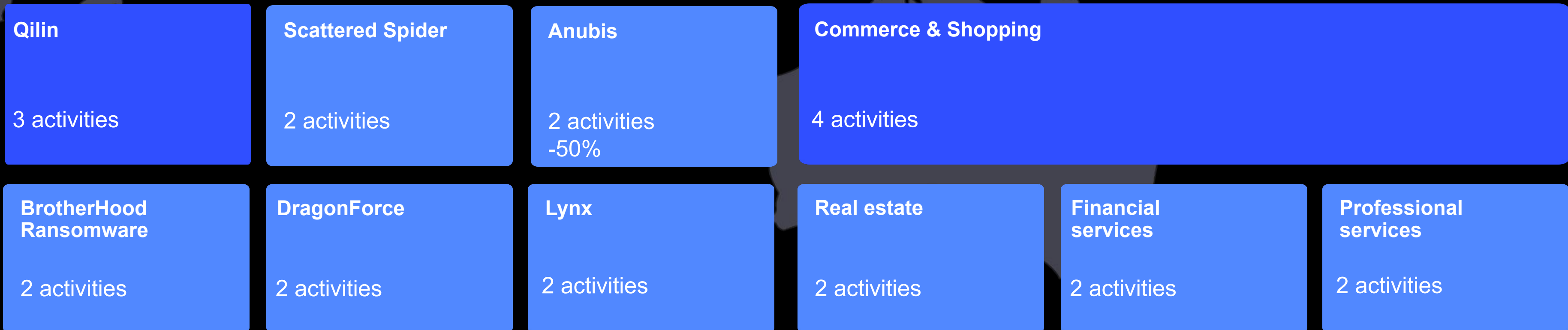
Statistics regarding ransomware activities in October 2025:

- **Australia** is still in the top 5 countries in the region with the highest number of ransomware attacks, claimed by a few actor groups such as DragonForce, Qilin, Scattered Spider, etc.
- The most notable incident was **Scattered Spider's** data publication of several companies, including **Qantas Airways**. The incident was first reported in June 2025, it is believed that the threat actor gained access to a customer service platform. Leaked data includes names, phone numbers, frequent flyer details, birthdates, gender, location data, and session information. The timestamps seen in the present lines are consistent with the threat actor's claims about the compromise date of June 2025.
- Although case-specific TTPs and IOCs are restricted, IoCs of these actors collected from previous incidents can be found on the Threat Intelligence Portal.

Most active threat actors (compared to the previous month)



Most targeted industries



# DDOS AND HACKTIVISM

Number of activities per Country, TOP 6 countries

92 incidents ↓ 32.8%

India, 25	Thailand, 22	Indonesia, 17
Philippines, 5	Bangladesh, 4	China, 4

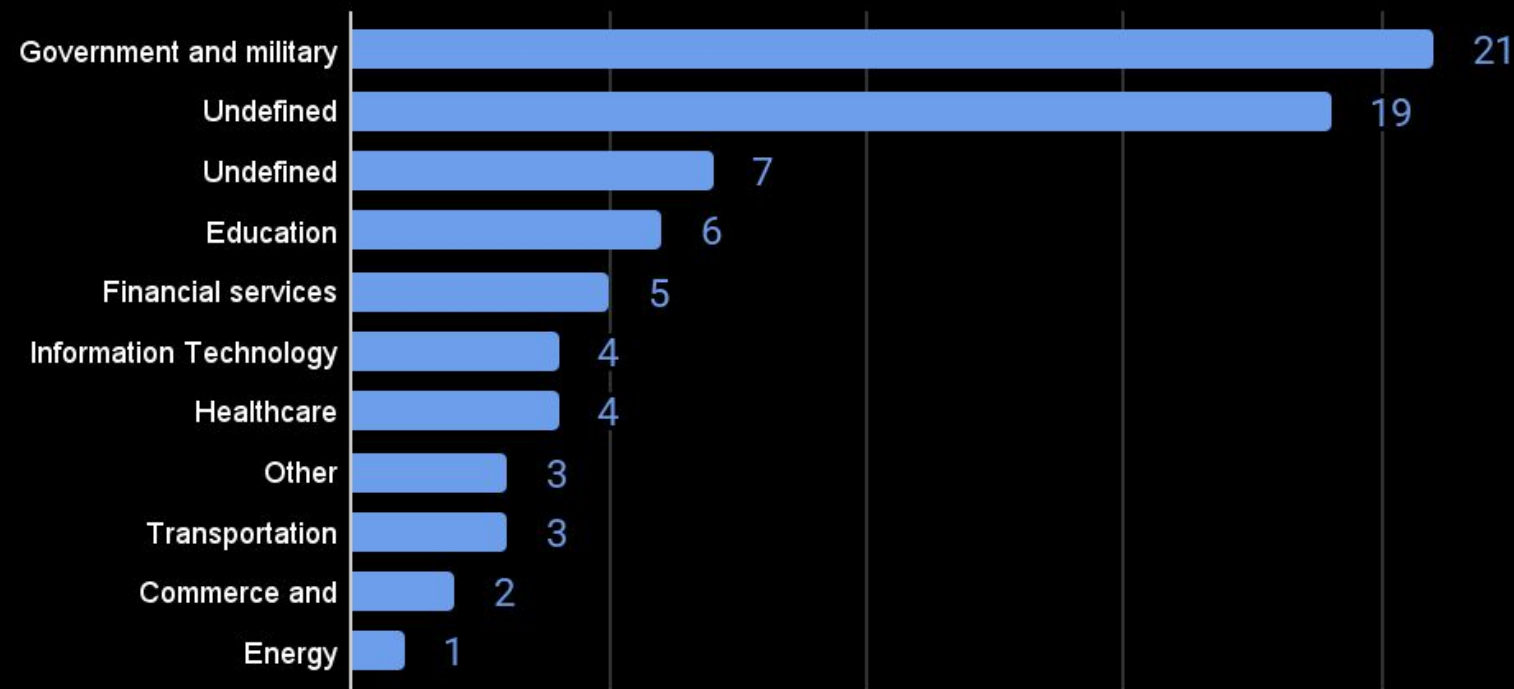
# DDOS AND HACKTIVISM

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.

In **Australia**, only 1 Hacktivism incident was recorded in October 2025. CyberToufan, a Pro-Palestine hacktivists group, claimed to possess data of the Israeli-American cosmetics company Seacret. According to the threat actor, leaked data includes sensitive information such as emails, passwords, phone numbers, and home addresses of customers. More information on Group-IB Threat Intelligence Portal.

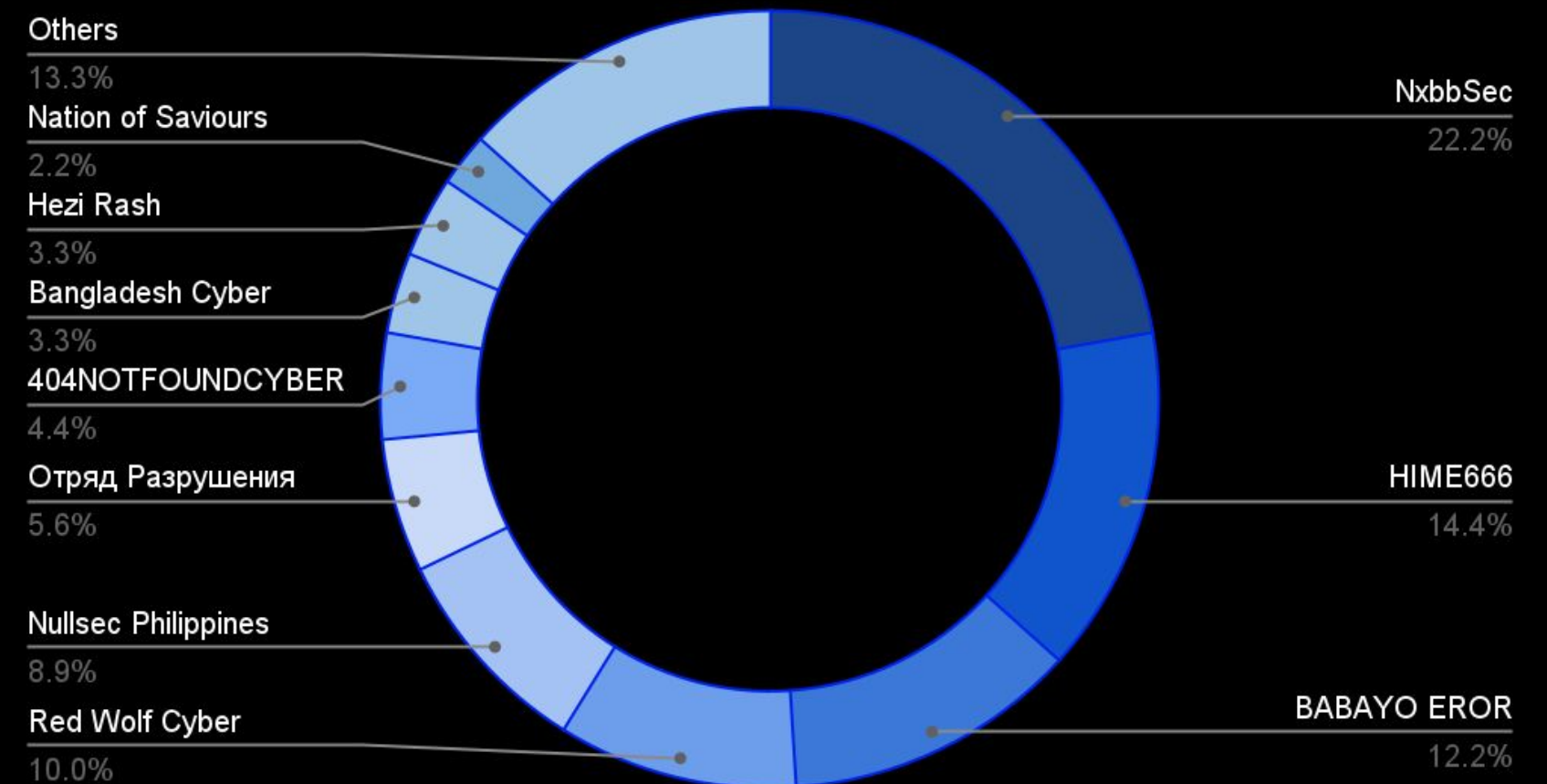
Below is a brief overview of groups that were active in the region during the previous month, the threat landscape is very different from the previous month, along with the top 10 targeted sectors in October 2025.

## DDOS and Hacktivism Activities, per industry



Top 10 targeted sectors, October 2025

## DDOS and Hacktivism Activities, per group



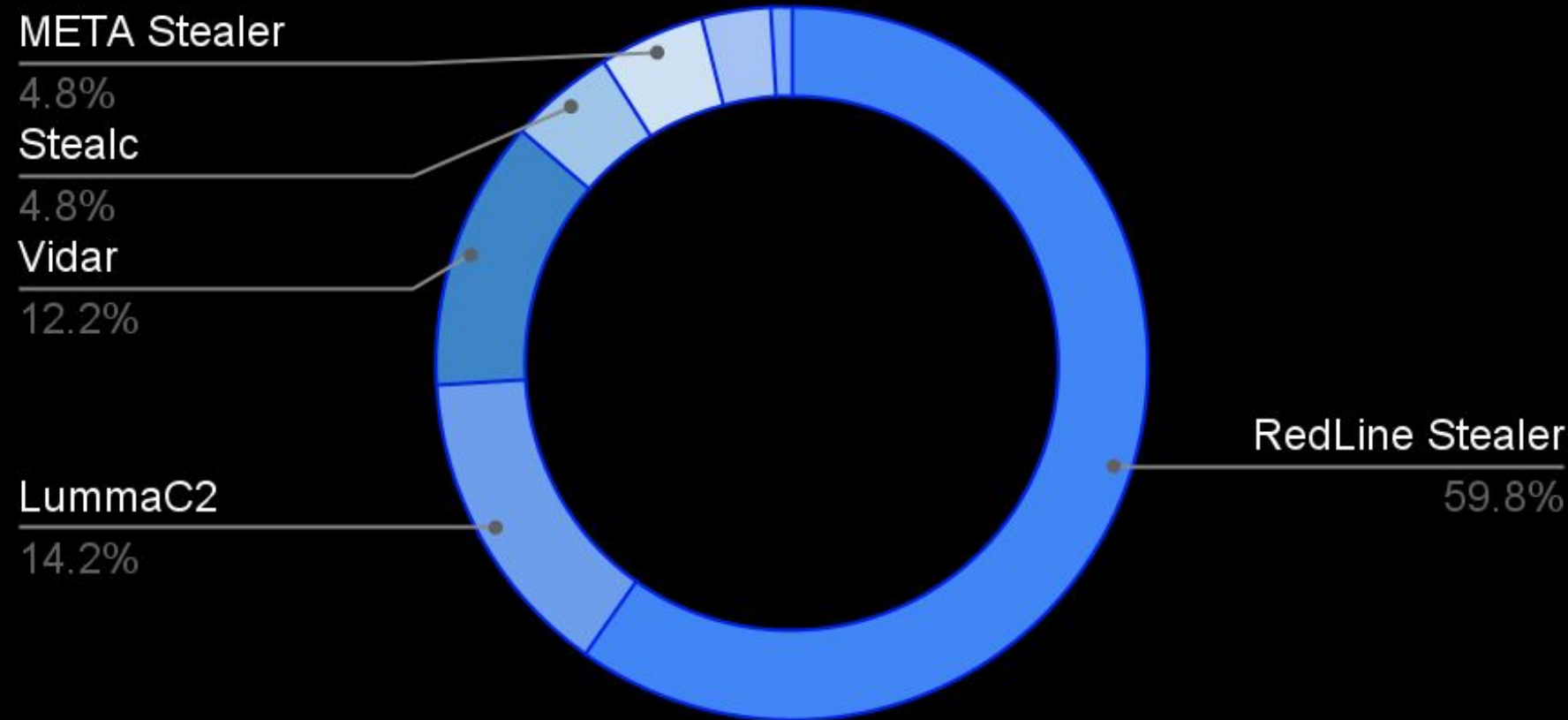
# COMPROMISED DATA (APAC) ↓ 55.5%

7,106,357 data leaked

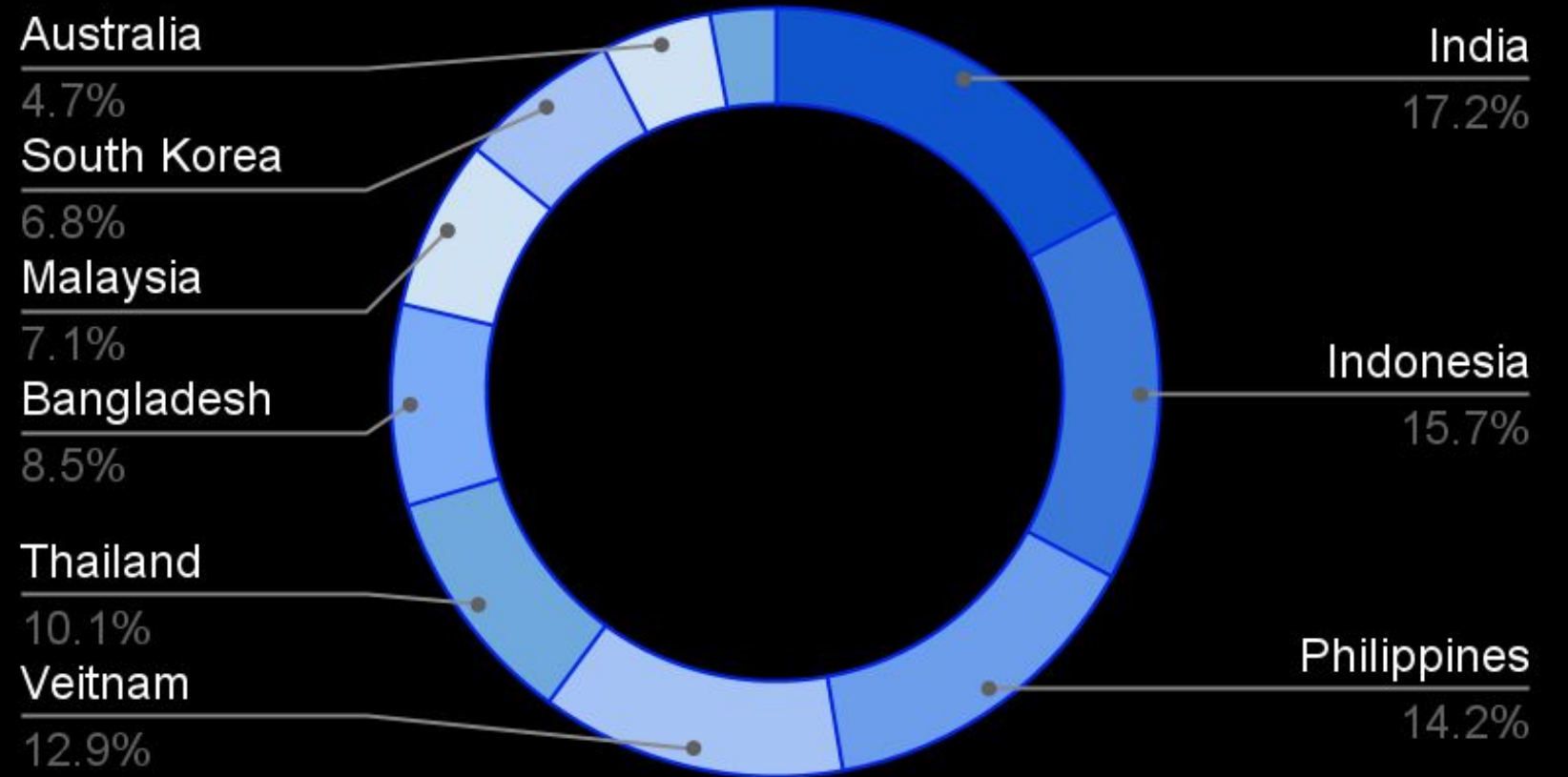
Statistics regarding compromised accounts in October 2025:

- In October 2025, RedLine Stealer was the most dominant malware in APAC, accounting for over half (59.8%) of all compromised accounts, followed by LummaC2 (14.2%) and Vidar (12.2%).
- India (17.2%), Indonesia (15.7%), and Philippines (14.2%) were the most impacted countries, representing the top three in the region.
- The data highlights a continued dominance of RedLine Stealer campaigns across APAC, with significant infection clusters in Southeast and South Asia.

## Compromised Accounts by Malware Top 7



## Compromised Accounts by Country

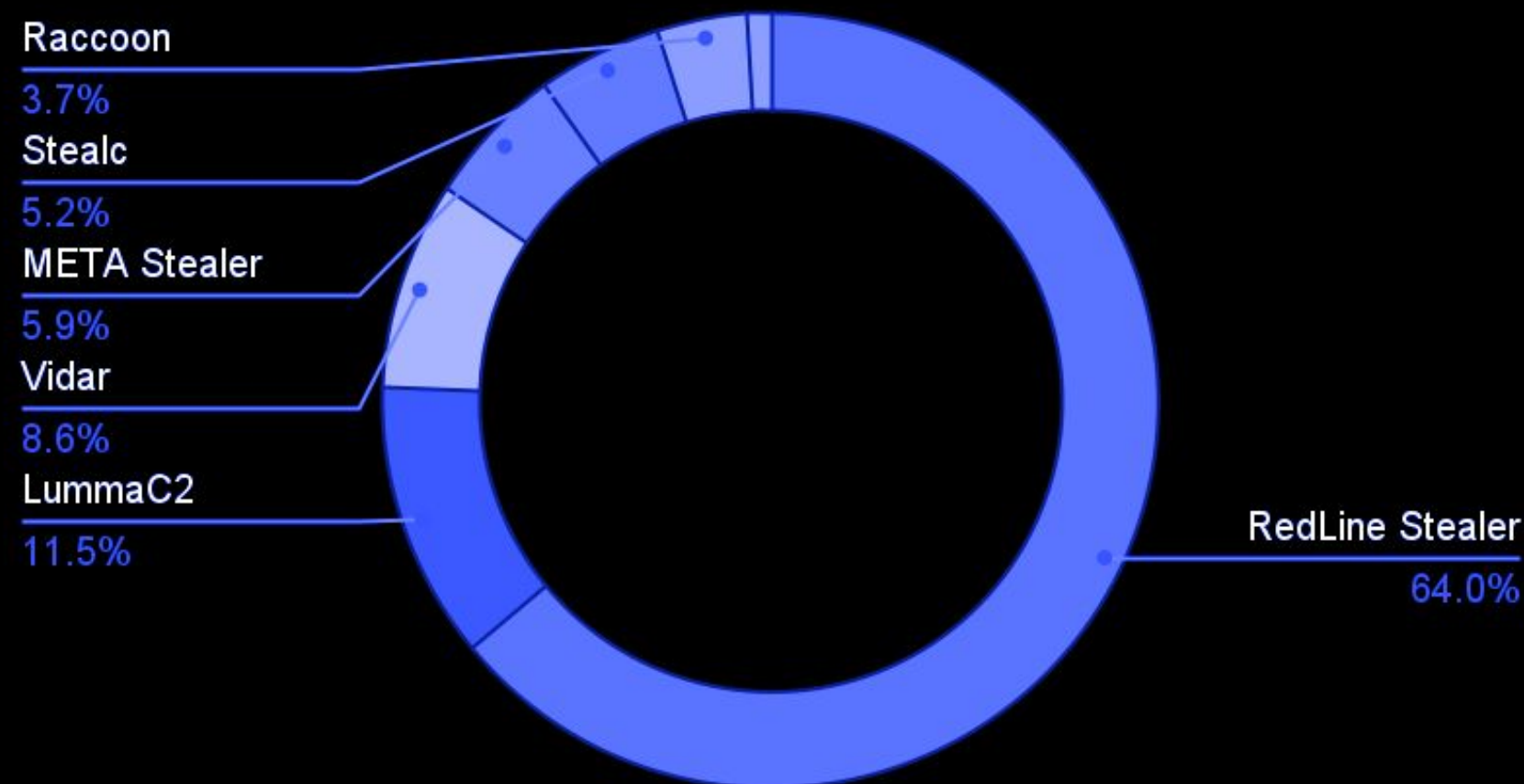


# COMPROMISED DATA ↓ 85.80% (Australia)

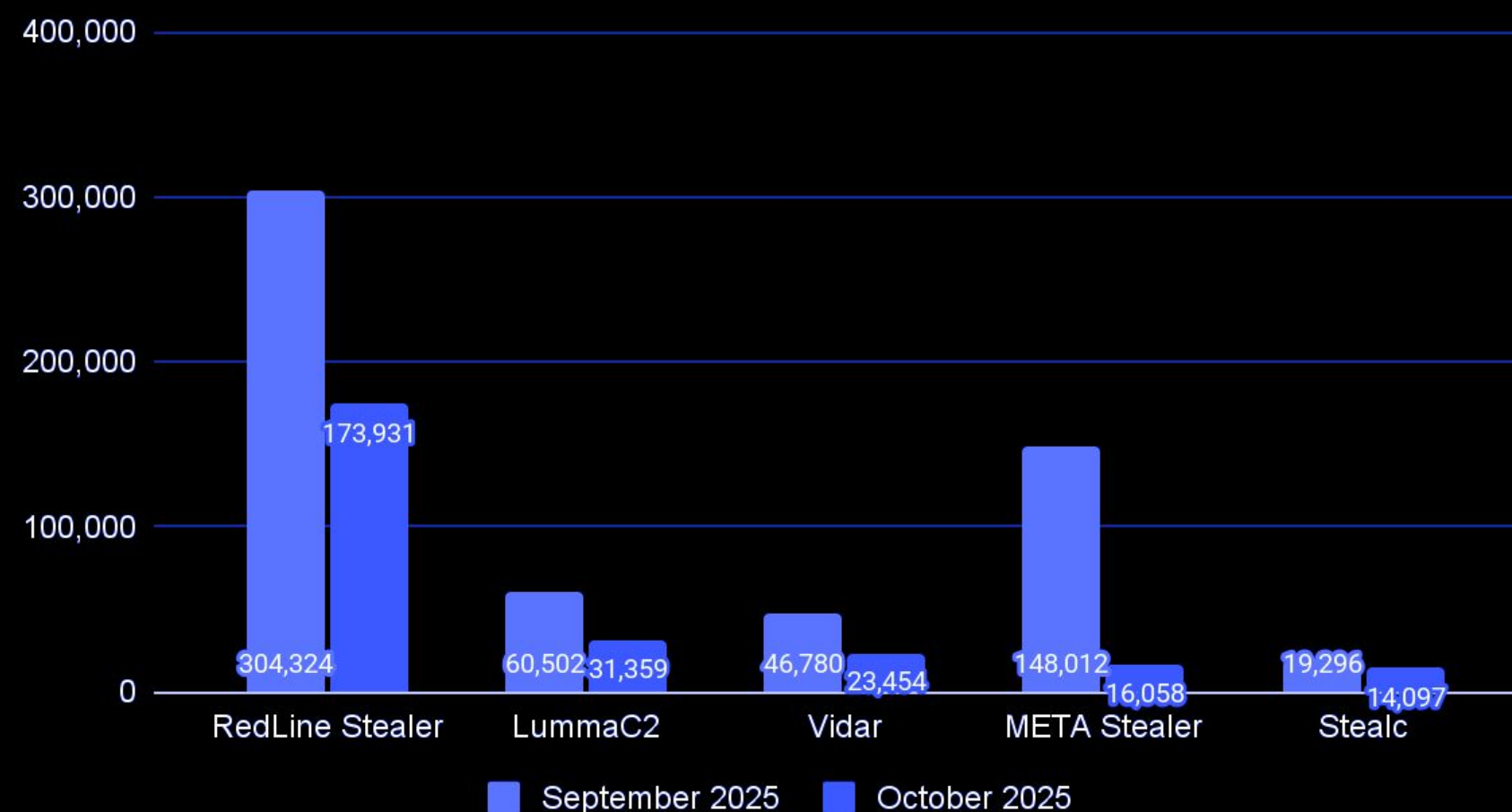
Statistics regarding compromised accounts in October 2025:

- RedLine Stealer, LummaC2 and META Stealer are still the top malware families responsible for nearly 80% of the compromised accounts in Australia during the month.
- The majority of leaked data is from stealer logs cloud, which are primarily distributed through Telegram channels. Most affected accounts this month are associated with domains belonging to Google, Discord, and Roblox. It is recommended that organizations continue to strengthen technical controls and security hygiene, while enhancing monitoring capabilities through the integration of reputable threat intelligence feeds.

## Top Malware for Compromised accounts



## Malware Activity Comparison, September-October 2025



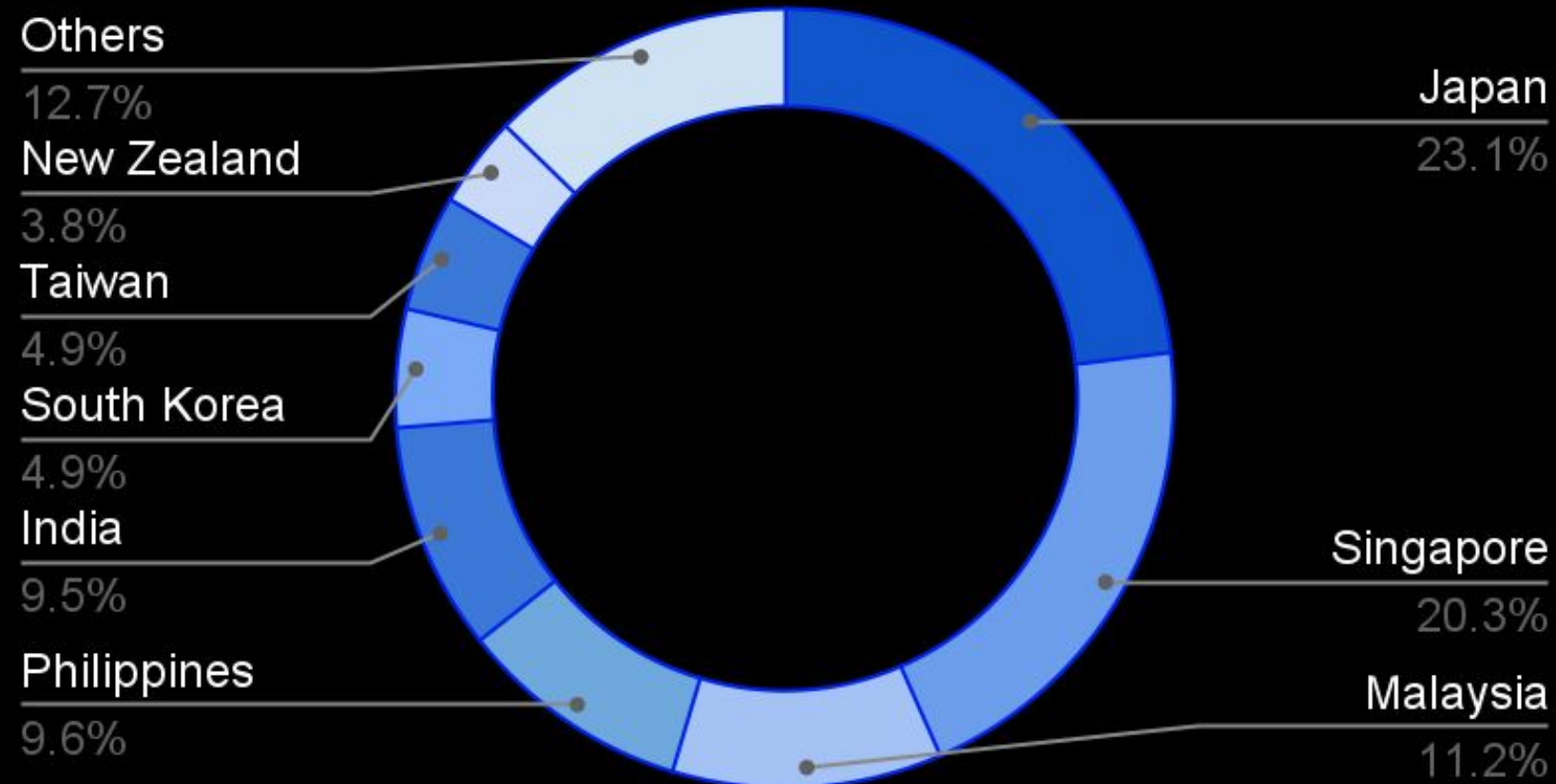
# COMPROMISED BANK CARDS (APAC) 3185 bank cards leaked

# ↓ 56.1%

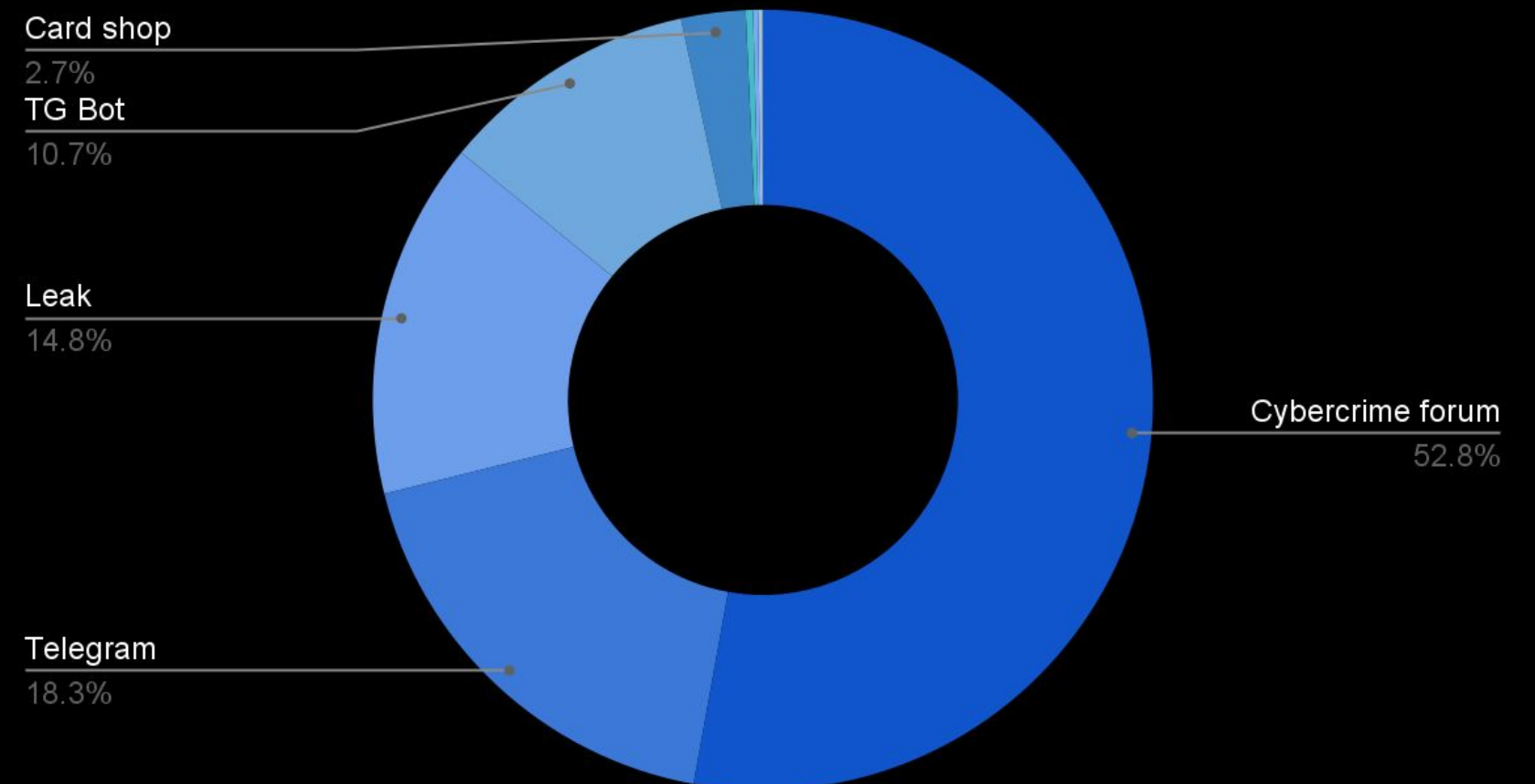
Statistics regarding compromised accounts in October 2025:

- Japan (23.1%), Singapore (20.3%) and Malaysia (11.2%) recorded the highest number of compromised bank cards in APAC for October 2025, together accounting for over half of all cases.
- The majority of compromised card data originated from Cybercrime forum, and Telegram source type.

## Compromised Bank Cards by Country



## By Source Type



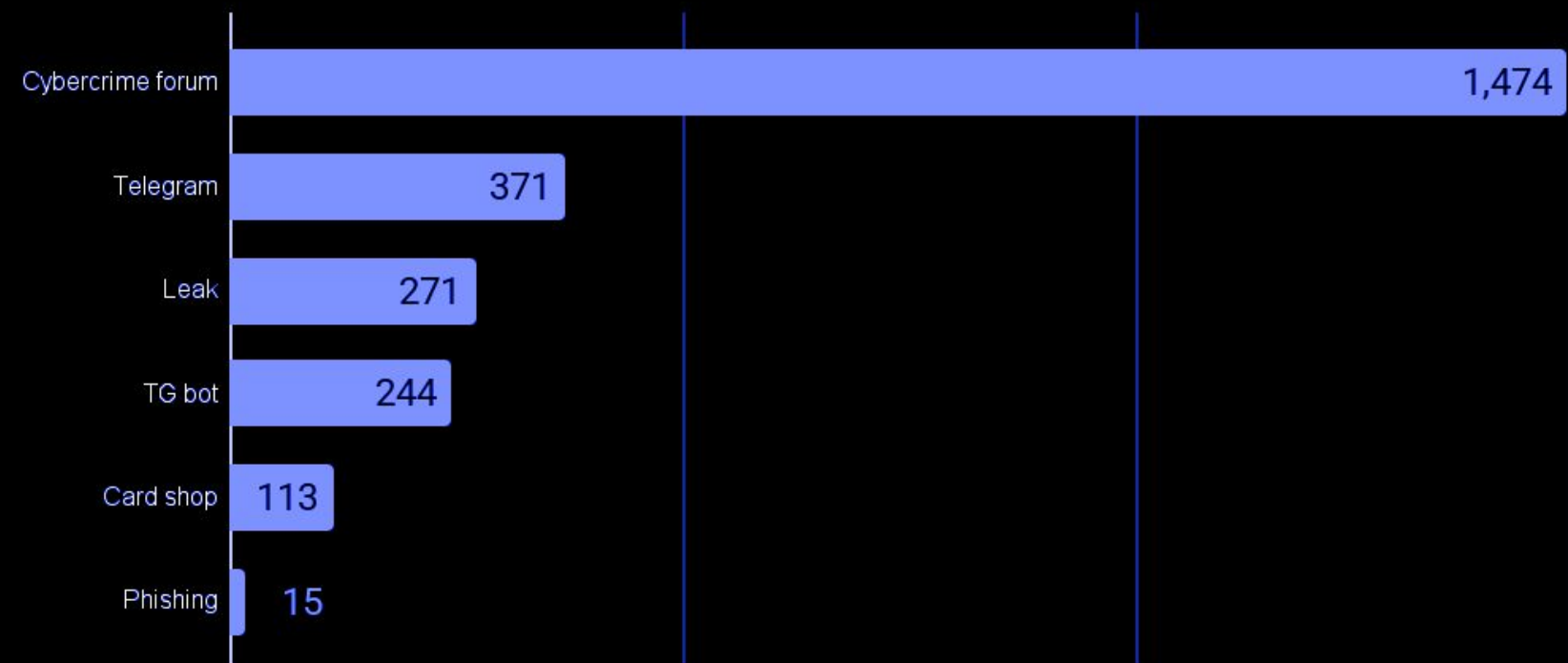
# COMPROMISED BANK CARDS (Australia)

↑ 35.51%

Statistics regarding compromised accounts in October 2025:

- Despite seeing a decrease compared to last month, **Australia** is still the top 3 country in the region with the highest number of compromised cards during the month.
- The majority of leaked card data comes from info-stealer or scraper tools, botnet and loader activities, as well as credential and credit-stealer malware.
- Over 50% of the compromised card comes from MASTERCARD, followed by VISA (44.39%), with a small amount from American Express.

## Compromised Bank cards by sources, Australia



Top 6 source types, October 2025



Threat actor group

## Scattered Spider

Targeted industries:

Messaging & Telco  
Financial services  
Commerce & Shopping  
Software  
Transportation  
Clothing & Apparel  
F&B  
Professional services

Media & Entertainment  
Sales & Marketing  
IT  
Lending & Investment  
Transportation  
Travel & Tourism  
Healthcare

Period of Activity:

May 2022 - Present

Targeted countries:

Worldwide (APAC & ANZ: Australia, Vietnam, India, Singapore, Japan, South Korea, Thailand, Taiwan, etc.)

Attribution:

United Kingdom

Intent:

Financially motivated

## Attack Summary

Scattered Spider (UNC3944/Storm-0875) was discovered in 2022. Recently they joined ShinyHunters and Lapsus to claim breaches of several major companies. While some claims referenced old Breachforums leaks, other data was confirmed genuine and recent. Evidence, including shared domains and PGP signatures, suggests SLSH's links to former Breachforums owners, possibly through access gained via forum moderation or multiple aliases.

## Key Observations

One of their tactics often include SIM swapping attacks followed by the establishment of persistence using compromised accounts. They also use social engineering to gain initial access via SMS and Telegram in some cases, or leaked credentials, as well as a vulnerability that allows to perform remote code execution. The actor group is also observed to perform phishing cluster abusing Salesforce and crypto-wallet brands between late July and early August 2025.



Threat actor group

## NxbbSec

Targeted industries:

Government and Military	Consumer Goods
Education	Energy
Health Care	Messaging and Telecommunications
Professional Services	Transportation
Media and Entertainment	Travel and Tourism
Commerce and Shopping	Advertising
Content and Publishing	Clothing and Apparel
Internet Services	Food and Beverage
Community and Lifestyle	Music and Audio
Financial Services	Other
Information Technology	
Real Estate	
Sales and Marketing	

Period of Activity:

May 2025 - Present

Targeted countries:

Worldwide (APAC & ANZ: Thailand, Vietnam, Myanmar, Vietnam, Cambodia, Philippines, Hong Kong, India)

Attribution:

Cambodia

Intent:

Hactivism

## Attack Summary

NXBBSEC is a hacktivist team based in Cambodia that has been involved in various cyber activities. They have claimed responsibility for hacking various Thailand websites with messages that included political and derogatory remarks directed at Thailand and Cambodia's territorial disputes under the campaign

## Key Observations

NxbbSec targets Thai websites and promotes narratives from other Cambodian hacktivist groups such as BL4CK CYB3R and Kxichixxsec. The actor primarily performs DDoS and website defacement attacks.



Threat actor group

## Qilin

Targeted industries:

Government and Military

Financial Services

Other

Education

Health Care

Real Estate

Software

Transportation

Agriculture and Farming

Information Technology

Internet Services

Messaging and

Telecommunications

Travel and Tourism

Consumer Electronics

Design

Gaming

Manufacturing

Privacy and Security

Sales and Marketing

Sports

Commerce and Shopping

Period of Activity:

2022 - Present

Targeted countries:

Worldwide (APAC & ANZ: Indonesia, India, Pakistan, China, Vietnam. Australia, Hong Kong, Japan, Malaysia, Philippines, Singapore, Thailand)

Attribution:

Russian

Intent:

Ransom and data extortion

## Attack Summary

Qilin (RaaS, aka Agenda) gains initial access typically via compromised credentials, phishing, or exposed remote services moved laterally, exfiltrated sensitive data, then deployed ransomware across Windows and/or Linux/ESXi environments. Victims faced encryption, operational outages, and public data leaks (double extortion).

## Key Observations

So far the actor operates as a RaaS affiliate model, relying on affiliates to find and exploit victims. Targets are high-value organisations healthcare, manufacturing, critical infrastructure, and large enterprises. Impact profile: large ransom demands, operational outages, and reputational/regulatory fallout for victims.

## High-Tech Crime Trends Report 2025

### Download To Read Now

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

### Watch The Webinar: High-Tech Crime Trends 2025 Deep Dive in APAC

- <https://www.group-ib.com/resources/webinars/apac-high-crime-trends-report-2025-deep-dive/>

### Watch The Webinar: APAC Intelligence Insights H1-2025 Review & H2 Forecasts

- <https://www.group-ib.com/resources/webinars/apac-intelligence-insights-h1-2025/>

# 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.

# INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003