SOCRadar®
Your Eyes Beyond

APAC

Threat Landscape Report 2026

Executive Summary

Top Takeaways

Public sector and financial targets dominate the threat landscape. Public Administration leads both dark web activity (18.12%) and ranks high in phishing exposure (10.26%). When combined with Banking, Finance, and Cryptocurrency targets, financially motivated and government-focused threats account for the largest share of activity across nearly every category in this report.

APAC shows two parallel threat patterns by country. Emerging digital economies like Indonesia and India lead general dark web activity, where opportunistic data theft thrives on rapid digitalization. In contrast, ransomware operators focus on wealthier markets, with Japan (28.52%) and Australia (24.33%) absorbing more than half of regional ransomware impact. Attackers clearly adjust their strategy based on victim ability to pay.

Data is the core commodity in the regional underground economy. Database leaks make up 80.86% of dark web threats, and Selling and Sharing together drive over 94% of activity. This confirms that stolen information, rather than tools or exploits, is what fuels APAC's cybercriminal markets.

The ransomware ecosystem is highly fragmented. Qilin leads at 20.9%, but the "Others" category accounts for 68.9% of attacks. Dozens of smaller groups collectively cause more damage than the top three combined, making attribution and defense increasingly difficult as the landscape shifts away from a few dominant brands.

Phishing concentrates heavily on Singapore. With 61.22% of phishing activity, Singapore's role as a financial and technology hub makes it the region's primary target for credential theft. The widespread use of HTTPS (61.5%) on phishing pages also shows that traditional trust signals like the browser padlock no longer protect users from these campaigns.

Technical Details

This report is based on data collected between April 2025 and April 2026

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around APAC.

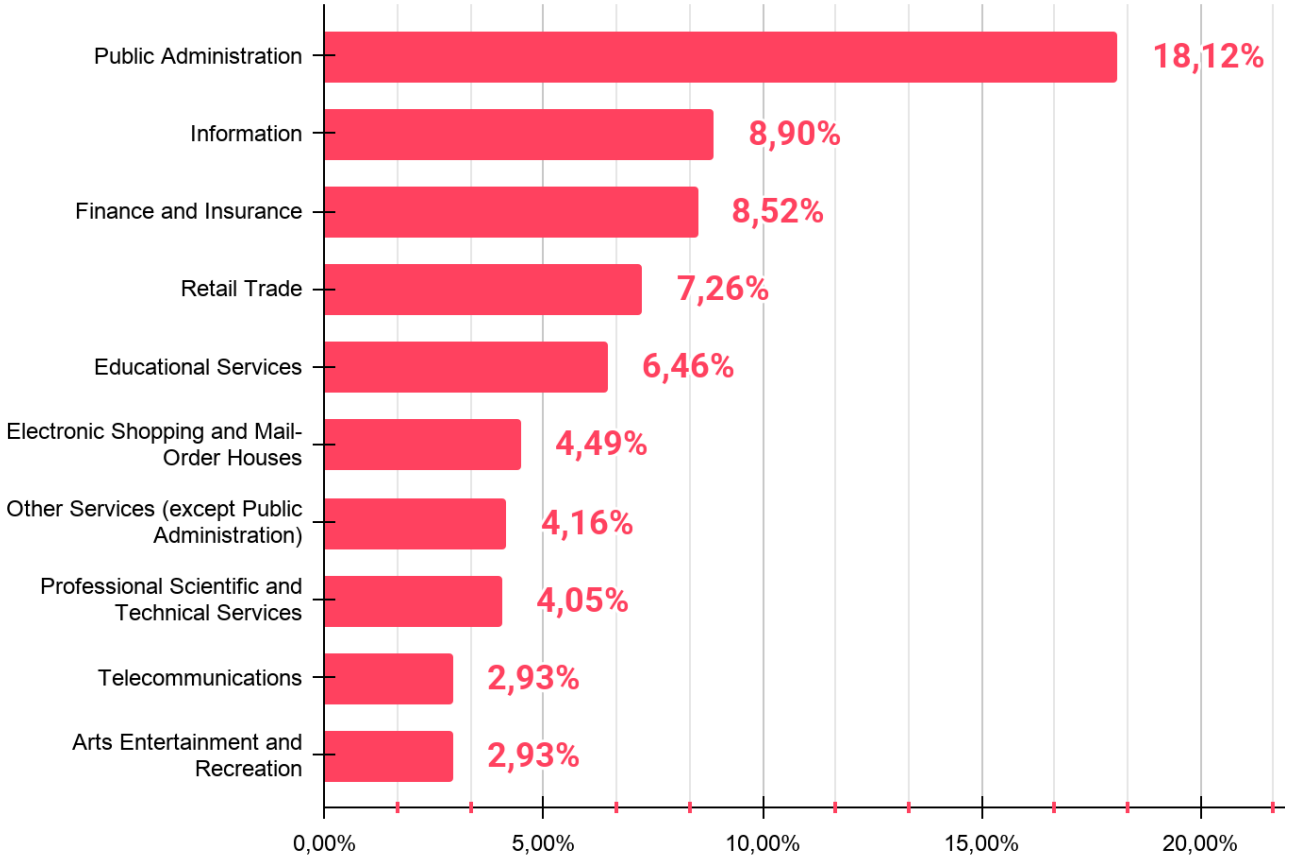
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups, and so on. These are areas where threat actors with various skill sets come together, discuss, share tools, and publish their alleged cyber attacks.

In the Ransomware Threats chapter, you will find detailed information about ransomware actors targeting APAC, their detailed profiles, and the necessary data that summarizes the ransomware activities.

The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

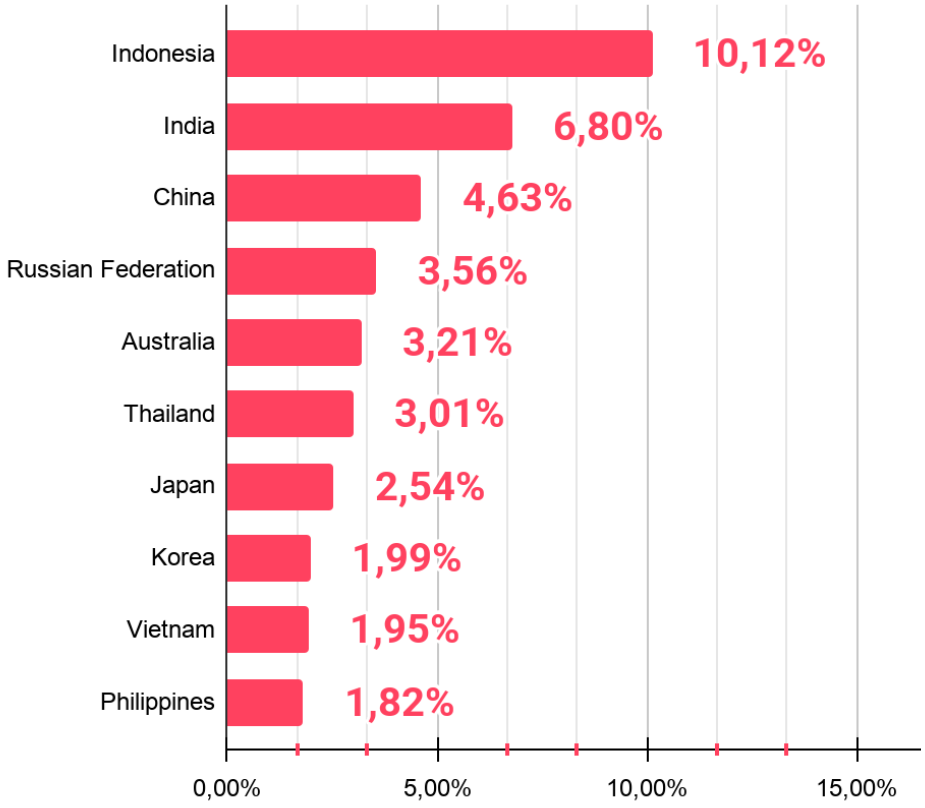
Dark Web Threats Targeting APAC

Industry Distribution of Dark Web Threats



Public Administration leads the threat landscape with 18.12%, showing that government-related systems remain the most targeted sector. This high share suggests continued interest in state data, credentials, and internal networks. Information (8.90%) and Finance and Insurance (8.52%) follow, both attractive to criminals due to the value of digital assets and personal data. Retail Trade at 7.26% and Educational Services at 6.46% show that sectors handling large user bases are also at risk. Together, these trends highlight a focus on institutions with broad data access and weaker security controls.

Distribution of Dark Web Threats by Target Country



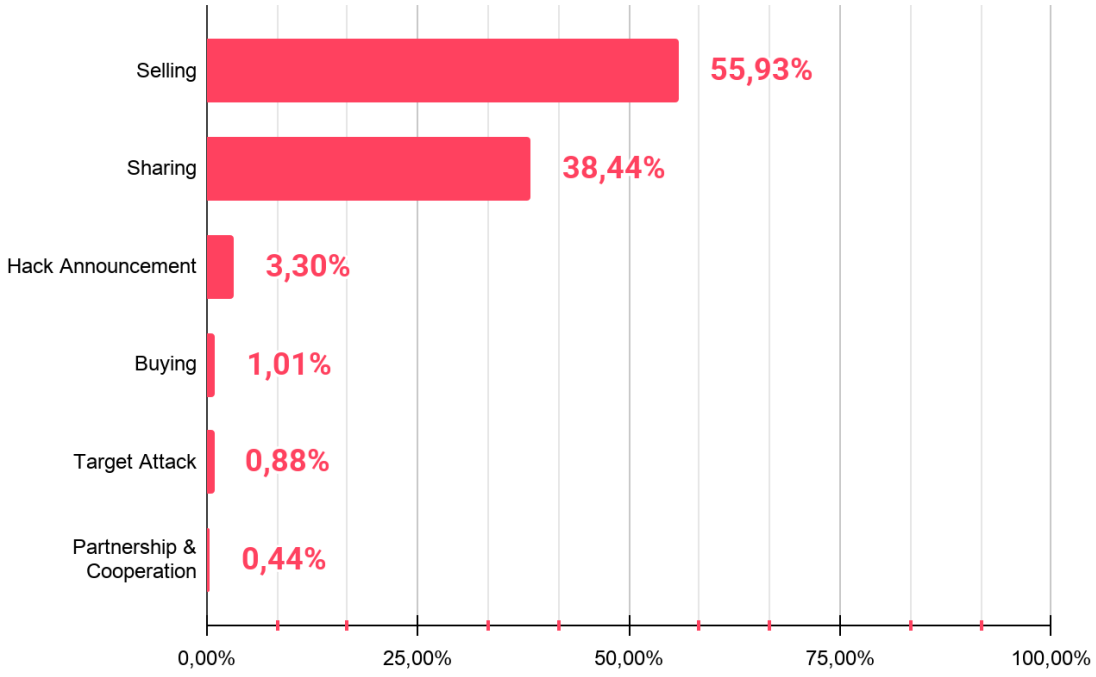
These numbers suggest that bigger economies tend to attract the threat actors

Indonesia tops dark web threat activity in APAC at 10.12%, leading the region by a wide margin. Rapid digital adoption, a large online population, and a growing e-commerce market likely contribute to this exposure. India follows at 6.80%, reflecting a similar pattern of fast digitalization paired with a vast user base that creates a broad attack surface.

China (4.63%) and the Russian Federation (3.56%) round out the top four, though activity tied to these countries often involves a mix of victim data and actor presence. Australia (3.21%) stands out as the most affected developed economy in the top five, consistent with its mature digital infrastructure and high-value targets.

Southeast Asian countries dominate the rest of the list, with Thailand, Vietnam, and the Philippines all appearing in the top ten. This concentration suggests threat actors are actively focused on the region's emerging digital economies, where security maturity often lags behind adoption rates.

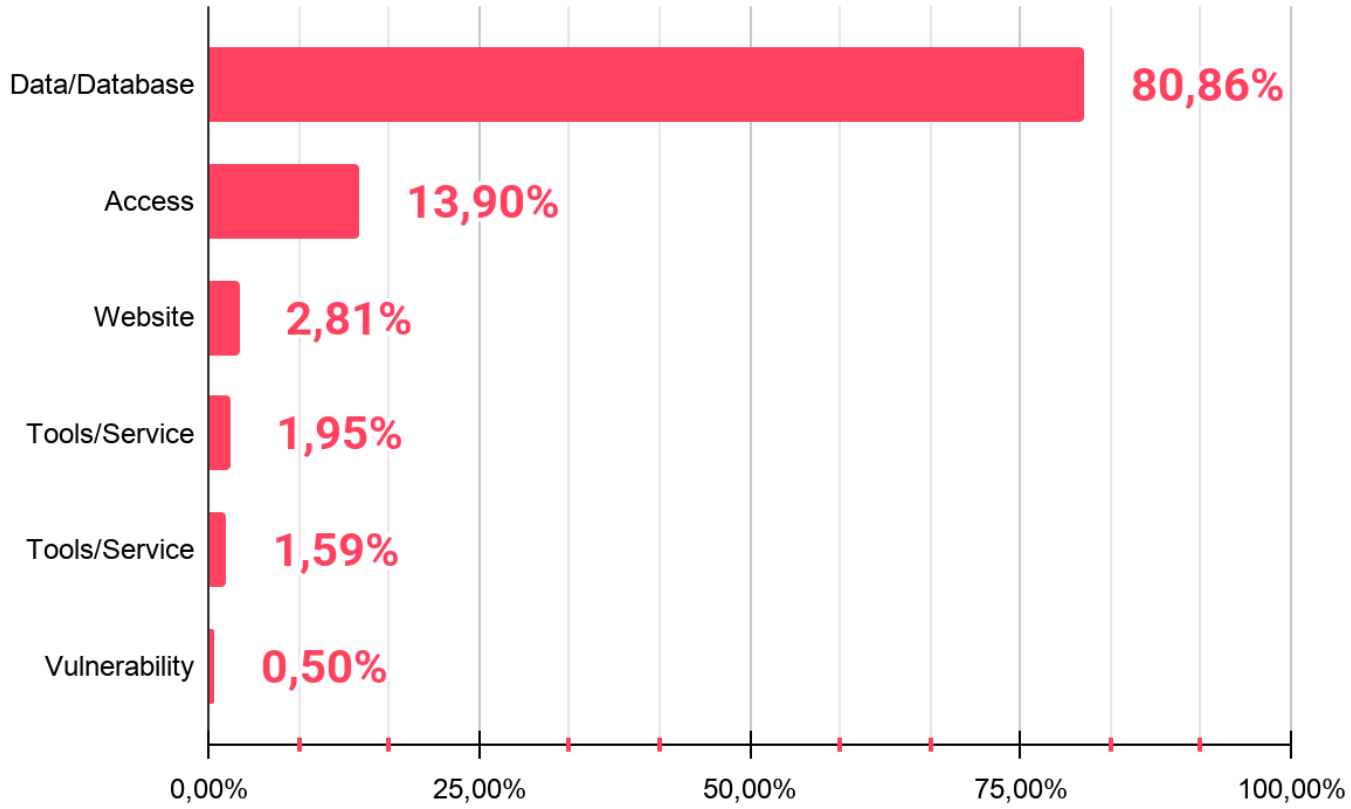
Distribution of Dark Web Threats by Threat Categories



Selling posts drives the market

Selling makes up 55.93%, showing that most activity is driven by monetization through data, access, or tools. Sharing follows with 38.44%, indicating strong community-driven exchange of compromised data or methods. Hack Announcements at 3.30% appear much less common. Buying (1.01%) and Target Attack listings (0.88%) remain low, suggesting sellers dominate the market and demand is driven more through informal negotiations than explicit requests.

Distribution of Dark Web Threats by Threat Type

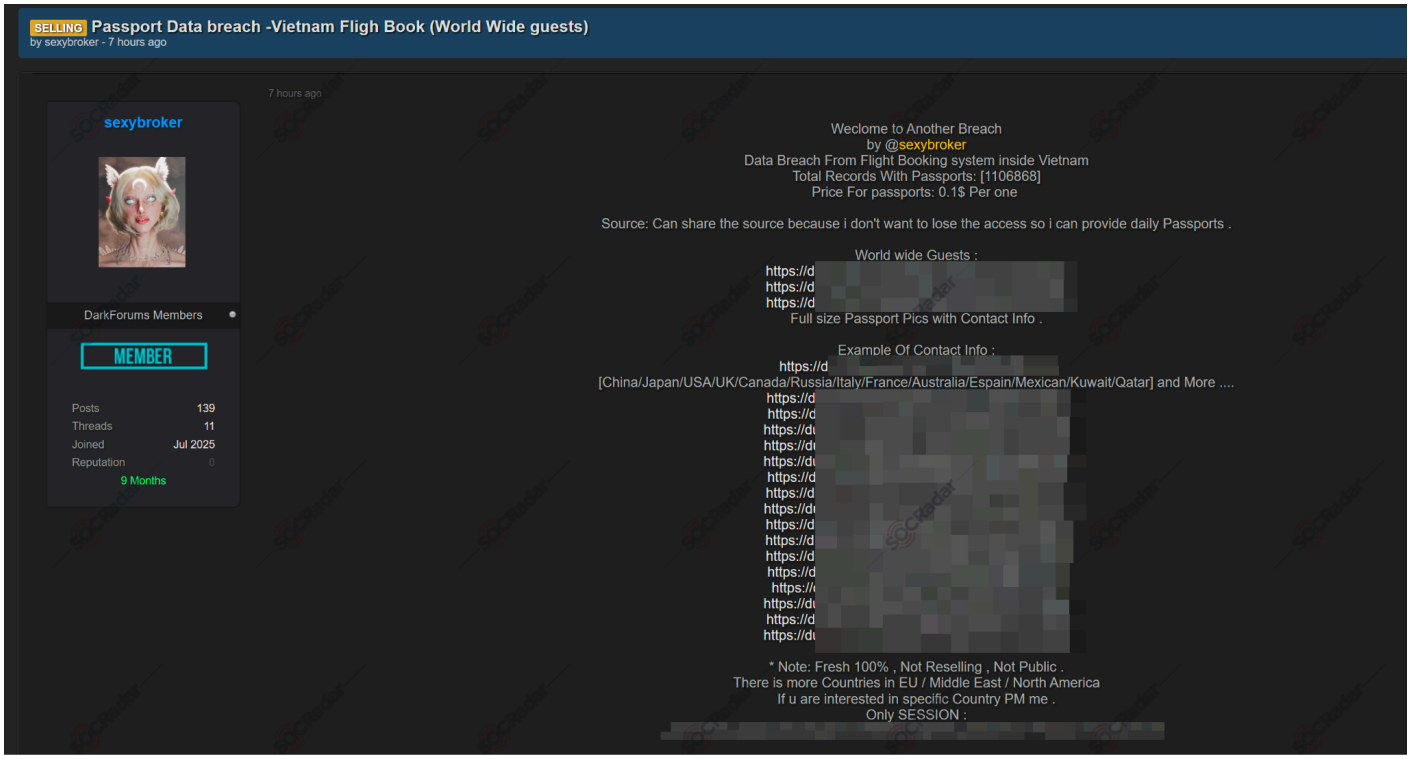


Data and database leaks dominate APAC dark web threats at 80.86%, confirming that stolen information is the core commodity in the regional underground economy. This aligns with the earlier finding that Selling and Sharing together drive over 94% of activity, since databases are the most common asset moved through both channels.

Access-related listings follow at 13.90%, covering items like compromised credentials, VPN access, and RDP entries. While much smaller in volume, access sales are often the starting point for ransomware and targeted intrusions, making this category more impactful than its share suggests.

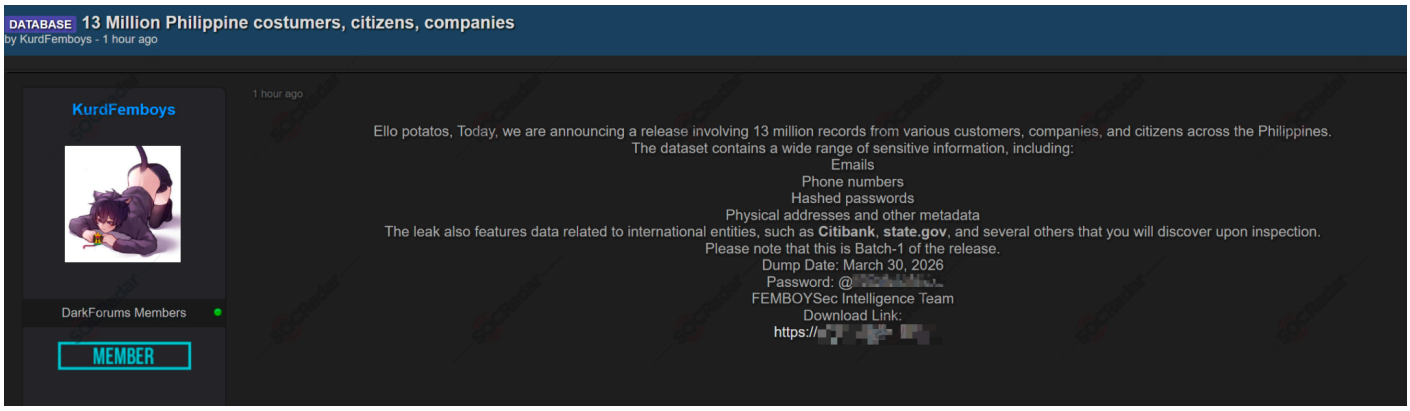
Recent Dark Web Activities Targeting Entities in APAC

The Alleged Passport Data of a Vietnamese Flight Booking System are on Sale



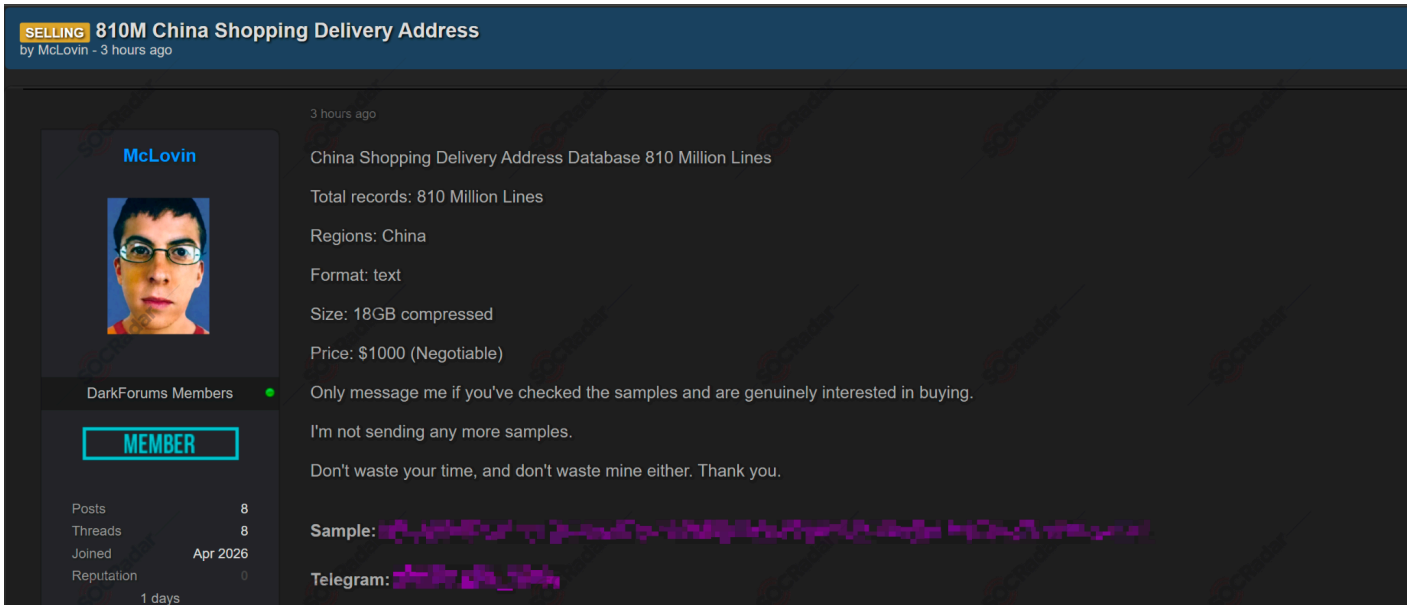
SOCRadar has detected a new alleged passport data sale on a Dark Web forum. The post claims the data originates from a flight booking system in Vietnam and includes 1,106,868 passport records. The seller is offering each passport at $0.10 and states the listing contains full-size passport images along with contact information covering guests from multiple countries across Europe, the Middle East, and North America.

Alleged Sensitive Data Leak Targets Philippines Citizens



SOCRadar has detected a new alleged sensitive data leak on a Dark Web forum. The post claims the dataset contains 13 million records belonging to customers, companies, and citizens across the Philippines. The exposed information reportedly includes emails, phone numbers, hashed passwords, physical addresses, and other metadata.

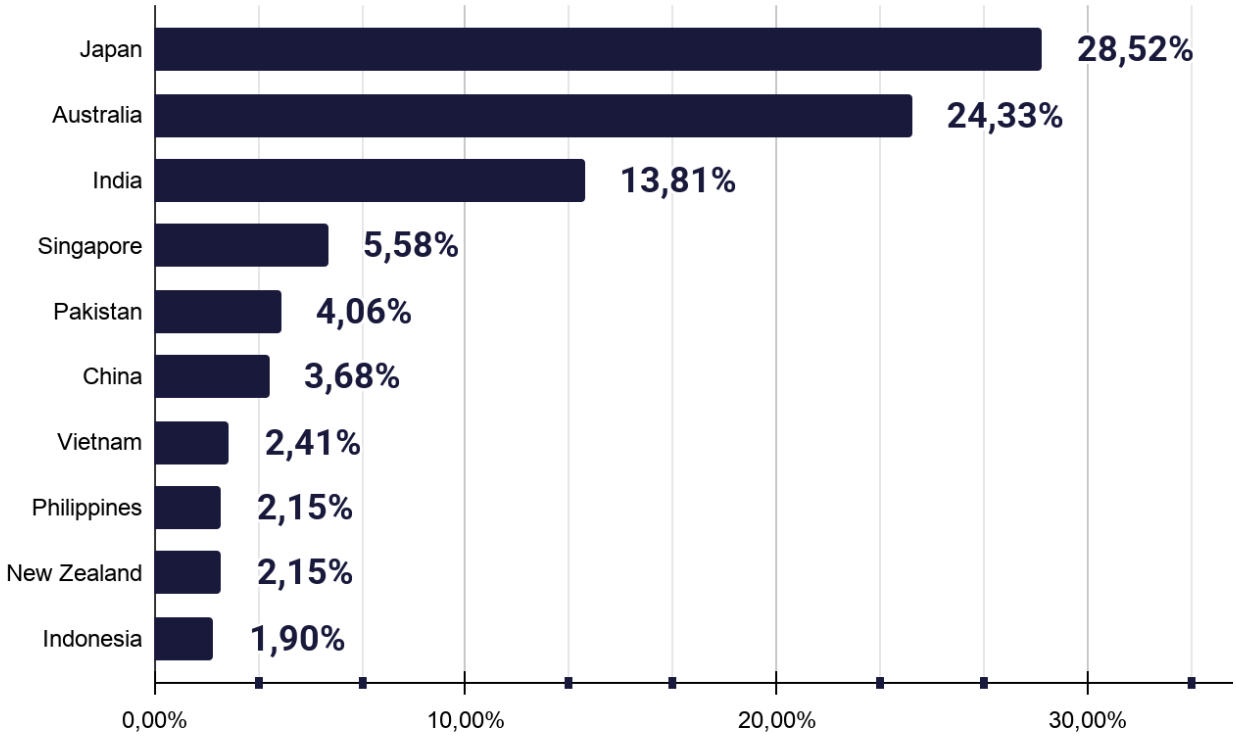
Alleged Address Data Sale Targets Chinese Citizens



SOCRadar has detected a new alleged address data sale on a Dark Web forum. The post claims the database contains 810 million shopping delivery address records belonging to citizens in China. The dataset is offered in text format with a compressed size of 18GB. The threat actor is selling the data for $1,000 and states the price is negotiable.

Ransomware Threats Targeting APAC

Distribution of Ransomware Attacks by Primary Target Country

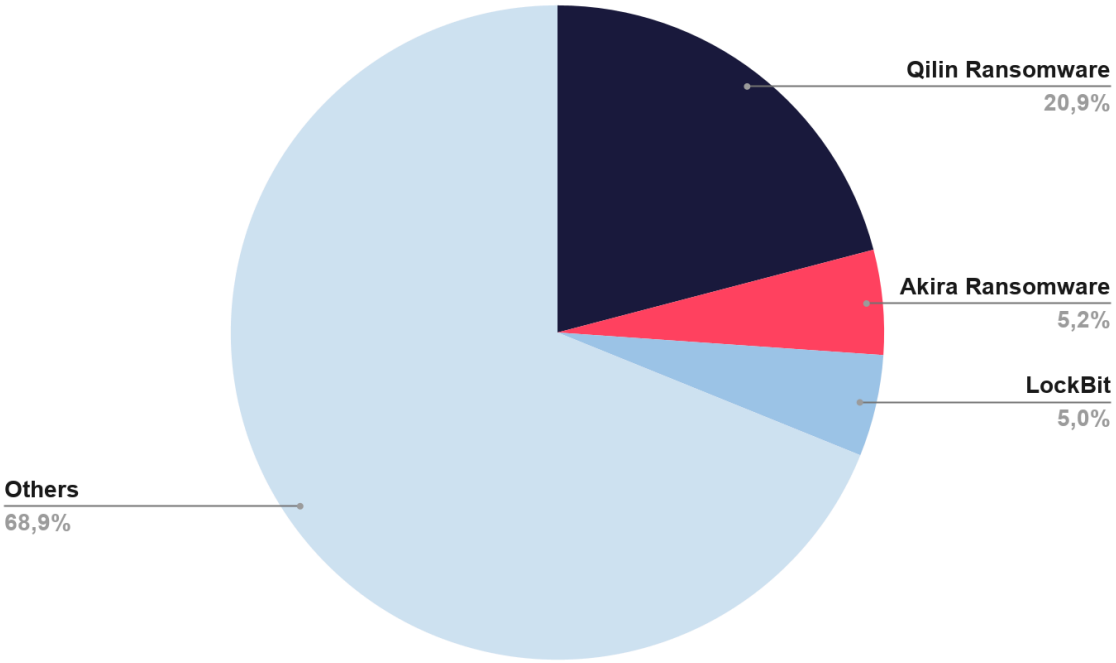


Japan leads ransomware impact in APAC at 28.52%, followed closely by Australia at 24.33%. Together these two developed economies absorb more than half of all regional ransomware activity. Their large industrial bases, high reliance on digital operations, and the strong financial returns attackers can extract make them priority targets for groups like Qilin and Akira.

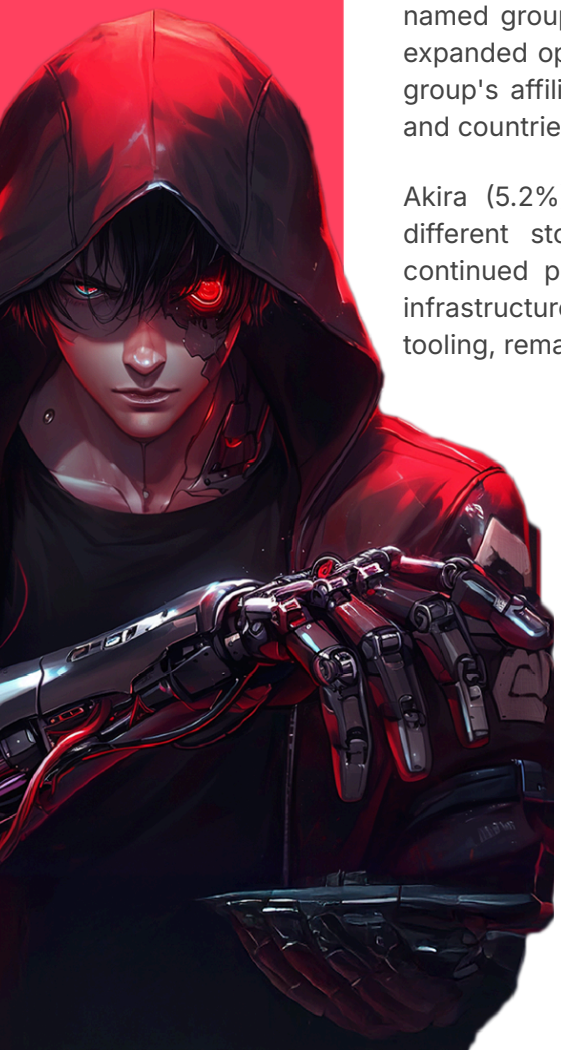
India ranks third at 13.81%, reflecting both the size of its economy and the rapid expansion of its digital infrastructure. Singapore (5.58%) follows as another mature market drawing attacker attention, particularly given its role as a regional financial and technology hub.

The contrast with the dark web data is notable. Indonesia and India led general dark web activity, but ransomware operators clearly favor wealthier economies where ransom payments are more likely. This split suggests two parallel threat patterns in APAC: opportunistic data theft targeting emerging digital markets, and focused ransomware campaigns aimed at countries with higher ability to pay.

Top Ransomware Groups Targeting APAC



Few big names, many small crews



Qilin leads ransomware activity against APAC at 20.9%, standing well ahead of other named groups. Its dominance reflects a broader trend seen through 2025, where Qilin expanded operations after several rival groups were disrupted by law enforcement. The group's affiliate-driven model allows it to scale attacks quickly across multiple sectors and countries.

Akira (5.2%) and LockBit (5%) follow at a similar level, though their positions tell different stories. Akira has steadily grown since its emergence, while LockBit's continued presence is notable given the law enforcement actions that targeted its infrastructure. Its share suggests remnants of the operation, or affiliates using its tooling, remain active in the region.

The "Others" category at 68.9% is the most telling figure. It points to a highly fragmented ransomware ecosystem in APAC, where dozens of smaller groups and emerging brands collectively cause more damage than the top three combined. This fragmentation makes defense and attribution increasingly difficult.

A Closer Look into The Top 3 Ransomware Groups

Qilin Ransomware

Qilin, also known as Agenda Ransomware, represents a formidable threat in cybercrime. This ransomware, one of the known Ransomware-as-a-Service (RaaS) groups, is designed with adaptability in mind, allowing it to customize attacks based on its victims' specific environments. Originating from a sophisticated background, Qilin leverages advanced tactics to extort organizations.

The primary objective of Qilin ransomware is financial gain through extortion. It targets organizations across various sectors, with a particular focus on healthcare and education. These sectors are often chosen due to their reliance on critical data and the generally lower levels of cybersecurity compared to more financially-focused industries. By encrypting essential files and demanding a ransom for their decryption, Qilin aims to create significant operational disruptions, compelling victims to pay the demanded ransom to restore their systems.

You can visit our **blog post** to read the rest of the threat actor profile.

Akira Ransomware

Since its discovery in early 2023, Akira Ransomware has evolved from a seemingly ordinary addition to the ransomware landscape to a significant threat affecting many businesses and critical infrastructure entities.

The ransom group employs a double extortion strategy, first exfiltrating data and then encrypting devices within the targeted network. Payment is then demanded not only for decrypting files but also for preventing the exposure of leaked data.

The Akira ransomware group frequently demands hefty ransoms, primarily targeting large enterprises across North America, Europe, and Australia. The malware typically spreads through targeted threat campaigns using phishing emails or exploiting software vulnerabilities, focusing on industries such as education, finance, manufacturing, and healthcare.

You can visit our ***blog post*** to read the rest of the threat actor profile.

LockBit

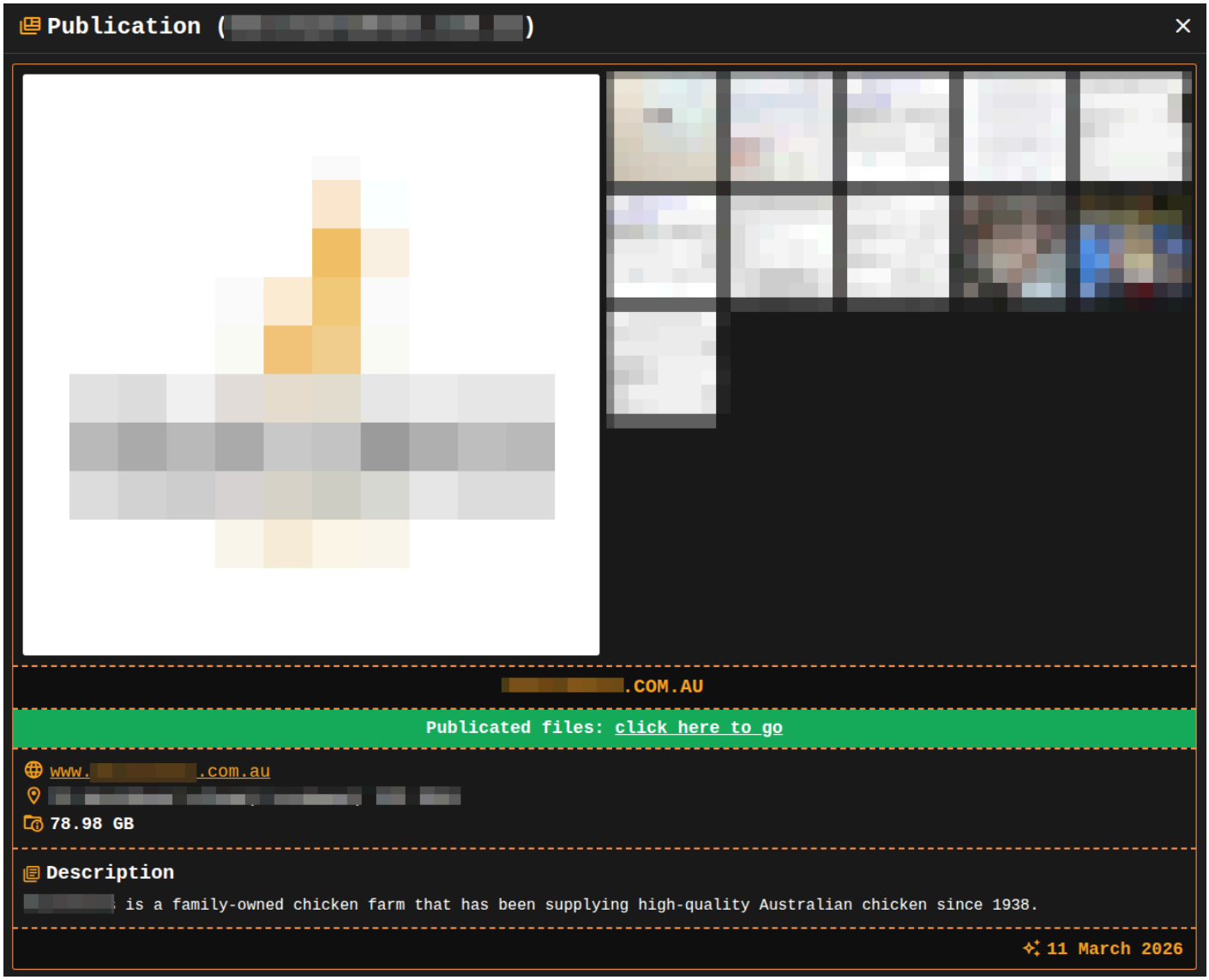
LockBit is a Ransomware-as-a-Service (RaaS) Gang first observed in 2019, now operating through successive variants (LockBit 2.0, 3.0, 4.0, and 5.0). It provides malware to affiliates worldwide, enabling coordinated attacks on businesses, healthcare, government, and critical infrastructure. LockBit is known for double extortion and employs professional tactics like hiring initial-access brokers, recruiting insider agents, and even sponsoring hacker contests and bug bounty programs to improve its code. The group has extorted hundreds of millions of dollars from thousands of victims, making it one of the most prolific ransomware operations.

By 2024, LockBit was widely recognized as a leading ransomware threat. More than 2,000 organizations (in healthcare, finance, retail, government, and other sectors) have been targeted by LockBit affiliates. Even as its leaders face charges and some operations are disrupted, LockBit's ongoing development shows that this RaaS operation remains a major cybercrime menace.

You can visit our **blog post** to read the rest of the threat actor profile.

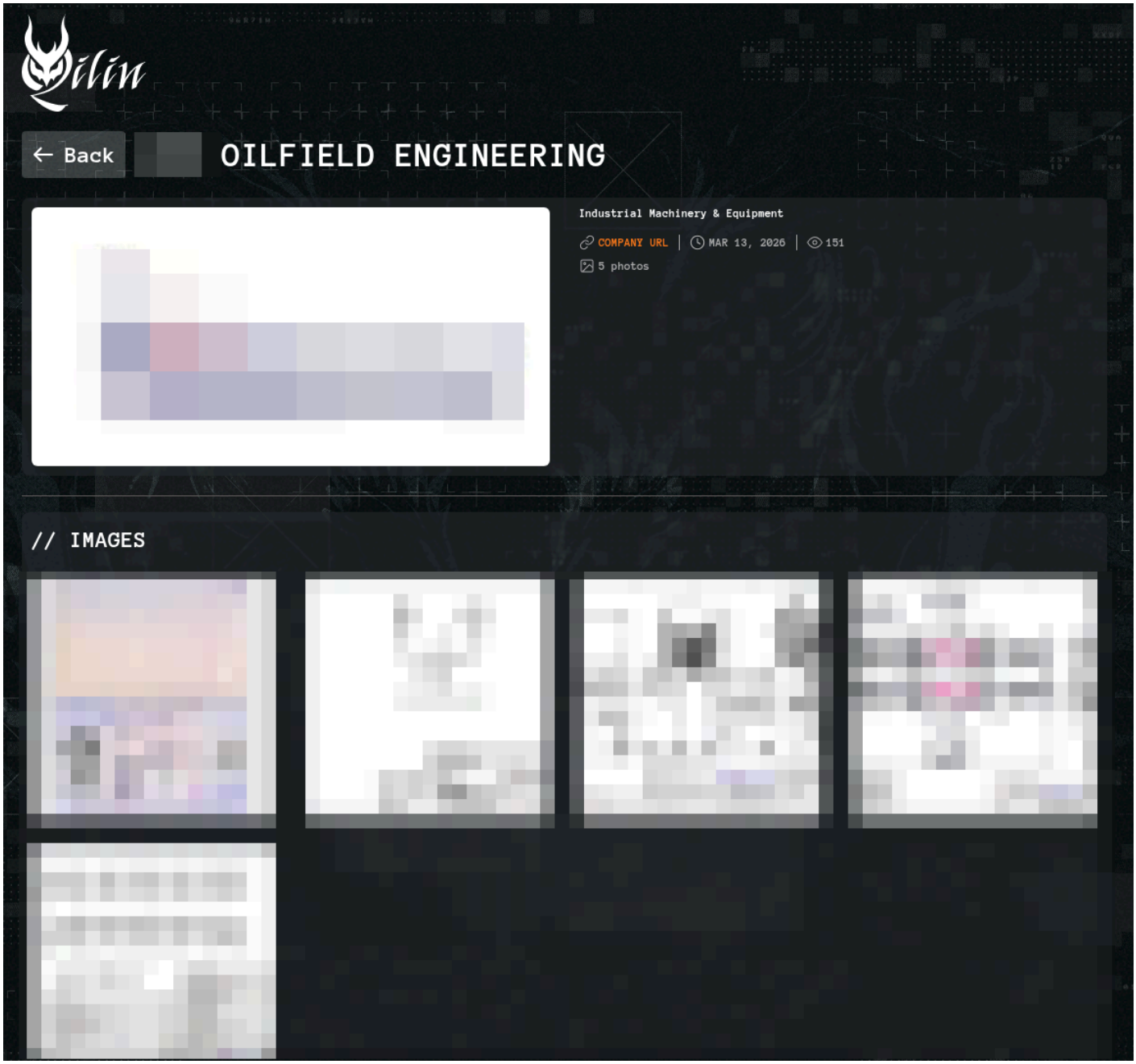
Recent Ransomware Attacks Targeting Entities in APAC

DragonForce Ransomware Group Allegedly Targets Australian Poultry Supplier



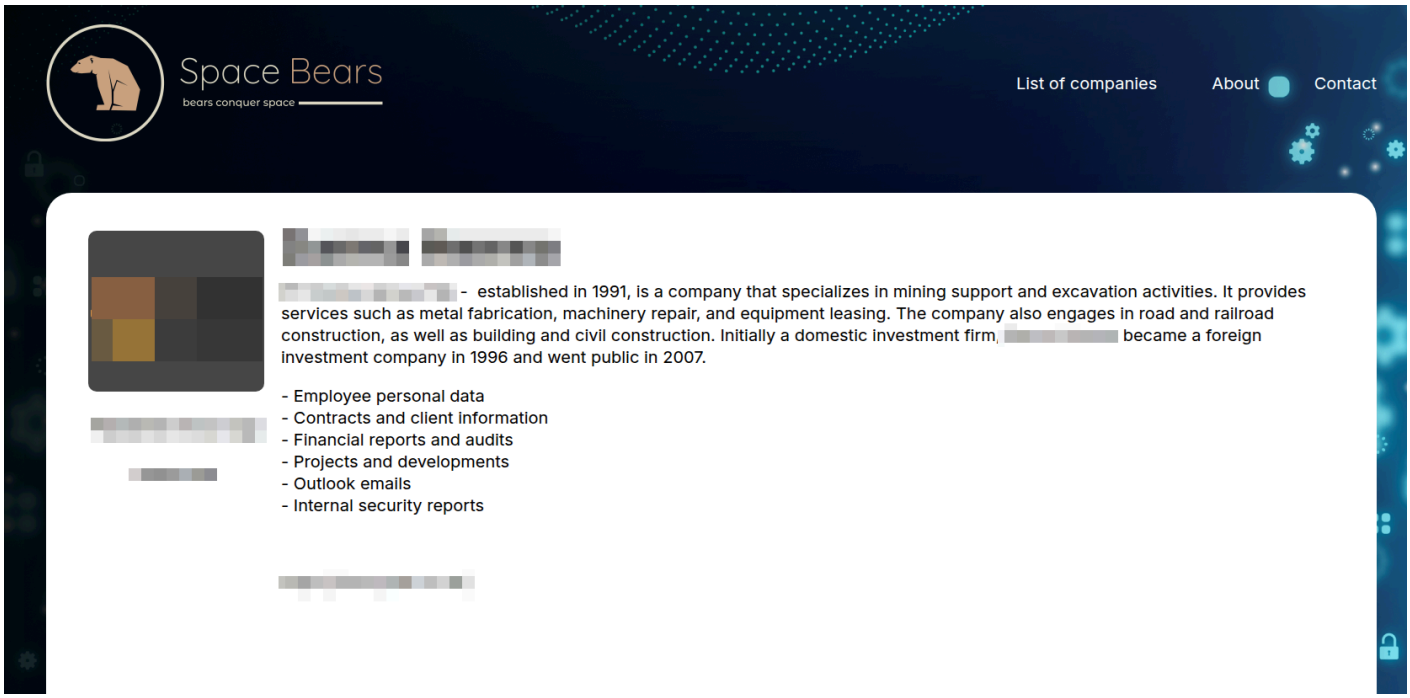
SOCRadar has detected a new alleged ransomware victim on the DragonForce leak site. The victim is reported to be a family-owned poultry supplier based in Australia that has been providing chicken products since 1938. Further details regarding the scope of the incident or the data involved have not been disclosed on the post.

Qilin Ransomware Group Allegedly Targets Singaporean Oilfield Equipment Manufacturer

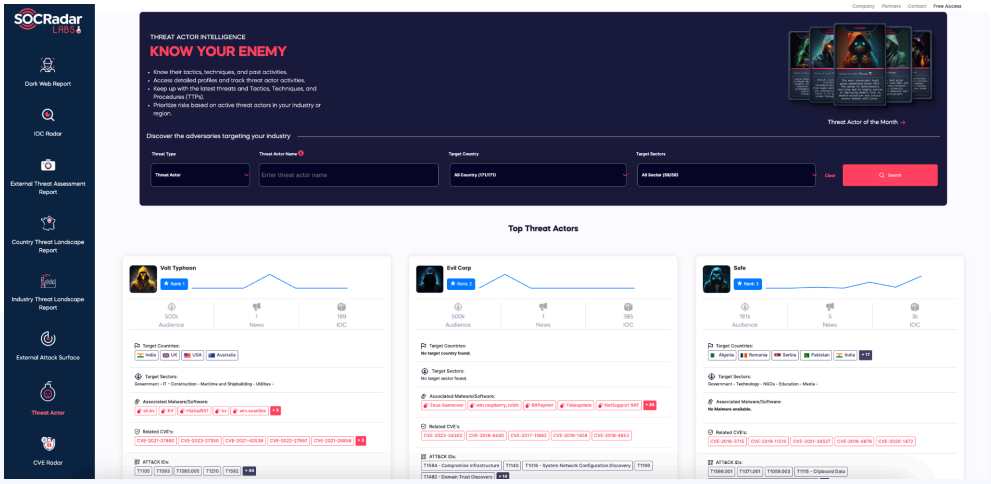


SOCRadar has detected a new alleged ransomware victim on the Qilin leak site. The victim is reported to be a Singapore-based company operating in the oilfield equipment sector, specializing in the design and manufacturing of wellhead pressure control, flow control equipment, wireline tools, coiled tubing tools, and subsea products. The company also provides recertification and rental services.

Spacebears Ransomware Group Allegedly Targets Indonesian Mining Services Provider



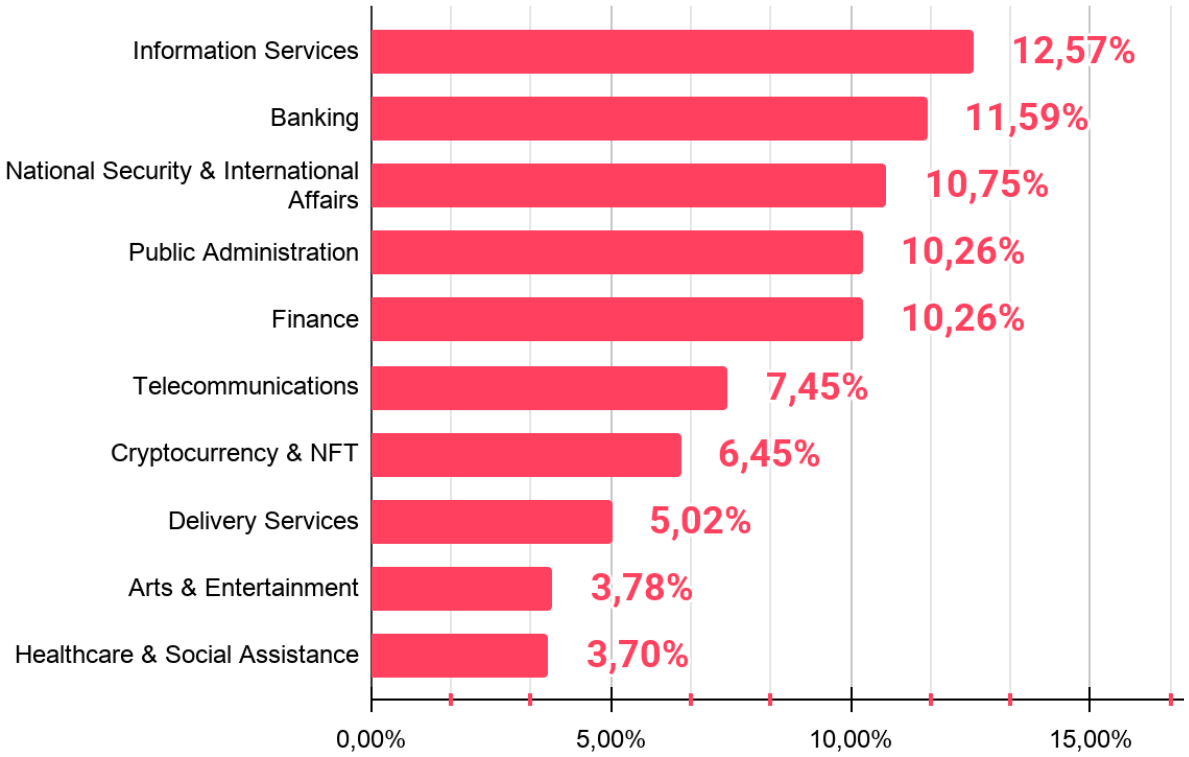
SOCRadar has detected a new alleged ransomware victim on the Spacebears leak site. The victim is reported to be an Indonesian company operating in the mining support and excavation sector, offering services such as metal fabrication, machinery repair, equipment leasing, and construction. The threat actor claims to have exfiltrated employee personal data, contracts, client information, financial reports, project details, Outlook emails, and internal security reports.



*SOCRadar enhances cybersecurity measures with its **Threat Actor Intelligence Module**, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.*

Phishing Threats Targeting APAC

Phishing Attacks - Distribution by Industry

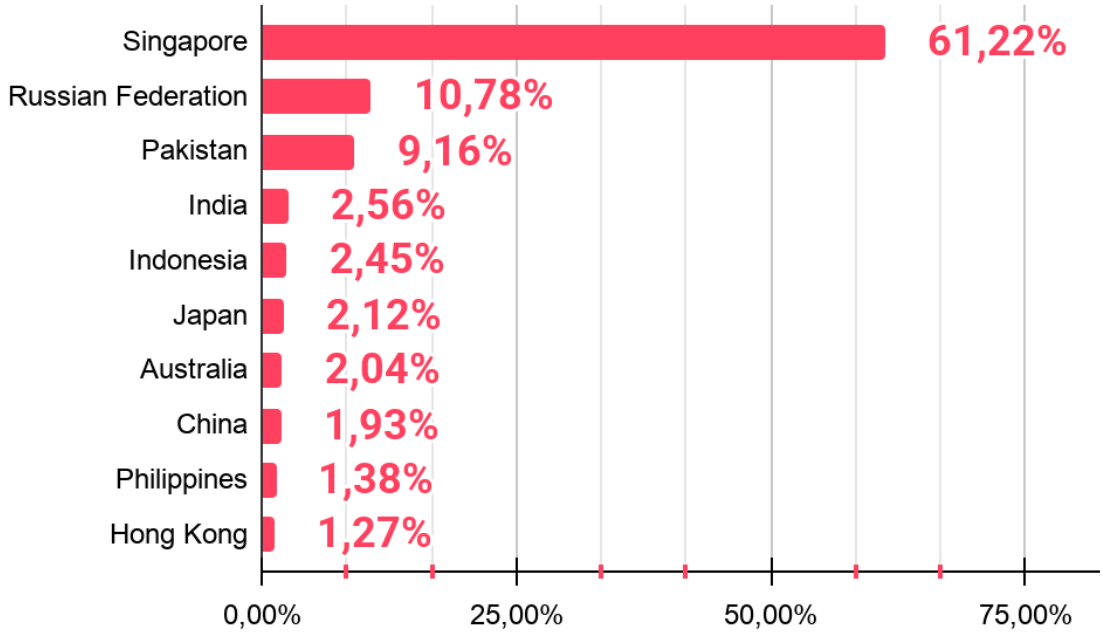


Phishing in APAC spreads more evenly across industries than other threat types, with the top five sectors each holding around 10–12% of activity. Information Services leads at 12.57%, followed by Banking (11.59%) and National Security & International Affairs (10.75%). The strong presence of government-linked targets aligns with the earlier finding that Public Administration (10.26%) is also the most exposed sector on the dark web.

Financial targets are especially prominent when Banking, Finance (10.26%), and Cryptocurrency & NFT (6.45%) are combined. Together they account for over 28% of phishing activity, confirming that credential theft tied to financial gain remains the main motivation behind phishing campaigns in the region.

Telecommunications (7.45%) and Delivery Services (5.02%) round out the consumer-facing targets, both commonly abused in SMS and parcel delivery scams. The wide spread across sectors shows that phishing actors in APAC cast a broad net, adapting lures to match whichever brands offer the highest click-through potential.

Phishing Attacks - Distribution by Target Country



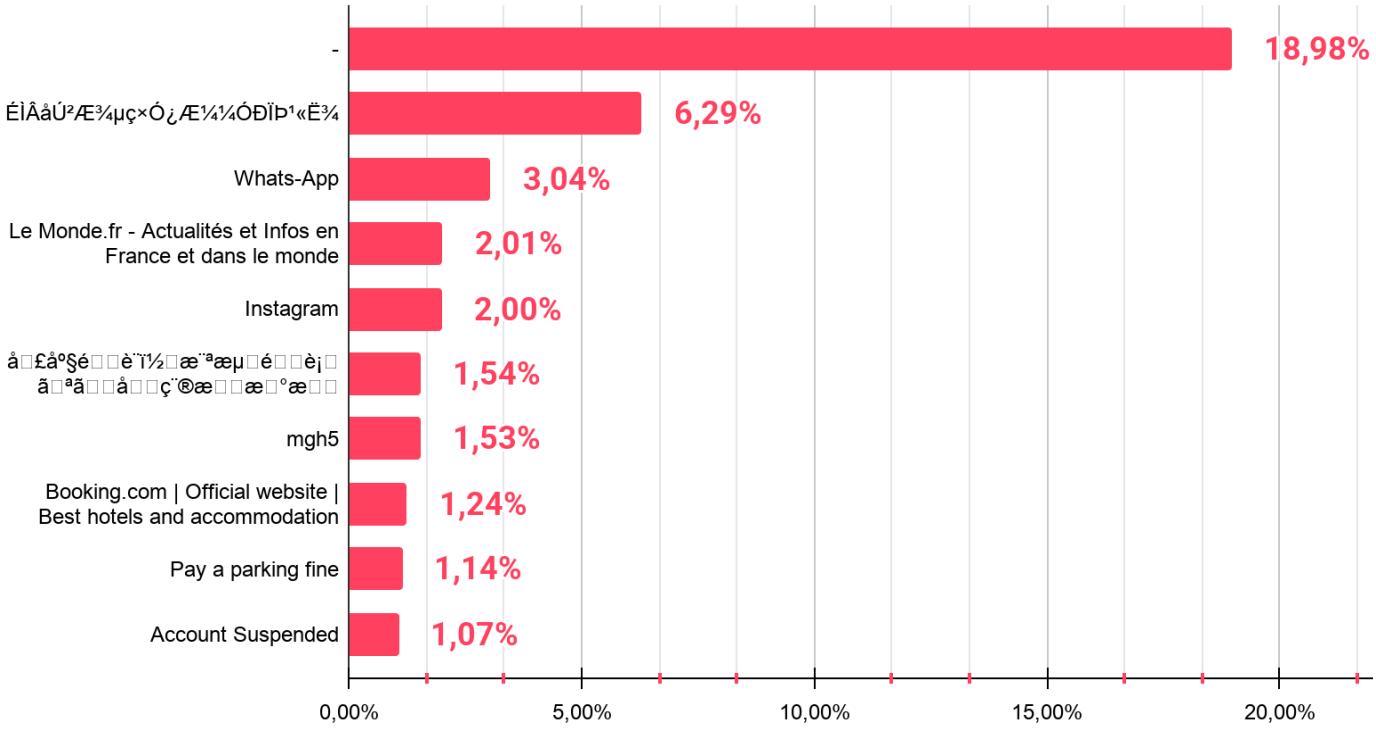
Phishing portals for every language

Singapore stands out sharply in phishing activity at 61.22%, far ahead of any other country in the region. This concentration reflects its role as a major financial and technology hub, where a high density of banks, fintech firms, and global company headquarters creates a target-rich environment. Brand impersonation of Singapore-based financial services is a common pattern in regional phishing campaigns.

The Russian Federation (10.78%) and Pakistan (9.16%) follow at much lower levels. Their presence in this list may reflect both victim exposure and infrastructure used to host phishing pages targeting APAC users.

The contrast with ransomware and dark web data is striking. Countries like Japan, Australia, India, and Indonesia, which dominate other threat categories, each account for only around 2% of phishing activity here. This suggests phishing operators in APAC are heavily focused on Singapore's financial ecosystem, while broader data theft and ransomware campaigns spread across a wider set of countries with different victim profiles.

Phishing Attacks - Distribution by Phishing Page Title



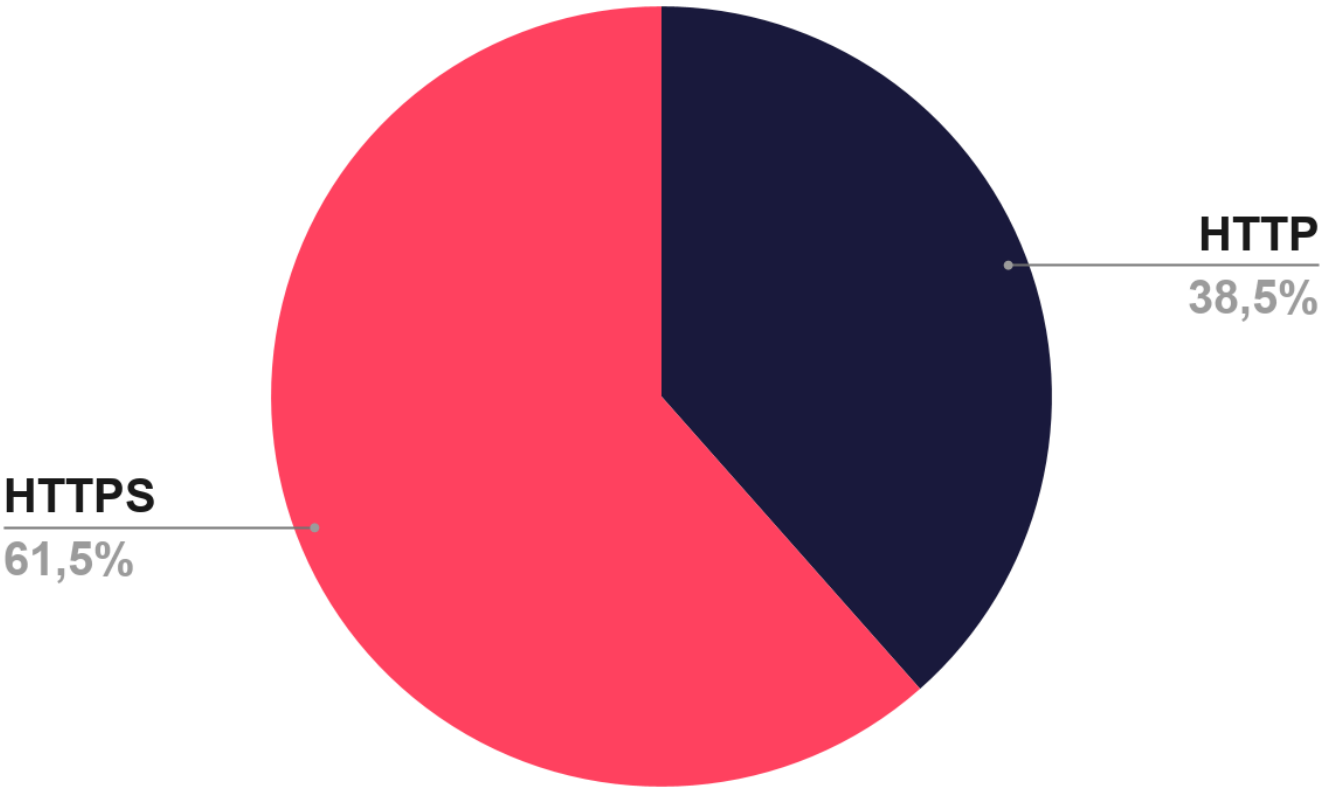
Phishing page titles in APAC show a clear mix of brand impersonation and generic lures. Nearly 19% of pages have no title at all, which is a common technique to avoid detection by automated scanners that rely on metadata for classification.

Among identifiable titles, WhatsApp (3.04%) and Instagram (2.00%) stand out as social media impersonation targets, often used to steal credentials or hijack accounts for further scams. Booking.com (1.24%) reflects ongoing abuse of the travel sector, where fake reservation pages trick users into entering payment details.

Several titles point to financial and banking lures, including Japanese-language pages impersonating account setup flows at Yokohama Bank. This connects directly to the earlier finding that Banking and Finance together drive a large share of phishing activity in the region.

Generic lures like "Pay a parking fine" and "Account Suspended" round out the list. These low-effort templates rely on urgency rather than brand trust, showing that both targeted and mass-market phishing tactics remain active across APAC.

Phishing Attacks - Distribution by SSL/TLS Protocol



HTTPS accounts for 61.5% of phishing pages targeting APAC, while plain HTTP makes up the remaining 38.5%. The majority use of HTTPS confirms a long-running shift in phishing tactics, where attackers rely on free SSL certificates to make their pages appear legitimate.

The padlock icon in browsers, once treated as a sign of safety, no longer offers meaningful protection against phishing. Users who were trained to "look for the lock" are now more likely to trust malicious pages that carry valid certificates. This makes visual trust signals unreliable as a defense layer.

That said, the 38.5% share of HTTP pages is still notable. It shows that a large portion of phishing operations in APAC remain low-effort, relying on quick setup and short-lived domains rather than added legitimacy. This split points to two parallel approaches in the region: polished campaigns built for credibility, and high-volume disposable pages built for speed.

Strategic Recommendations

- **Enhance Endpoint Security:** Implement advanced anti-malware, regular device audits, and employee training on safe browsing practices.
- **Strengthen Phishing Defense:** Invest in phishing detection systems, web filtering tools, and employee training on recognizing phishing attempts.
- **Enforce Multi-Factor Authentication (MFA):** Apply MFA across critical systems to protect against stolen credentials.
- **Fortify Ransomware Defenses:** Regularly back up data, segment networks, and develop incident response plans for ransomware attacks.
- **Monitor Dark Web Activity:** Use Dark Web monitoring to detect exposed company data early and respond quickly to breaches.
- **Collaborate on Cyber Threat Intelligence:** Share insights with industry peers and stay informed about emerging threats and new attack vectors.
- **Secure Communications and Data:** Ensure encryption for sensitive communications and transactions, and train employees on secure data handling.
- **Proactive Vulnerability Management:** Regularly apply patches and conduct penetration testing to address potential system vulnerabilities.
- **Build a Cybersecurity Culture:** Foster ongoing employee training, phishing simulations, and establish clear security policies to ensure a security-first mindset across the organization.

Who is SOCRadar?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.