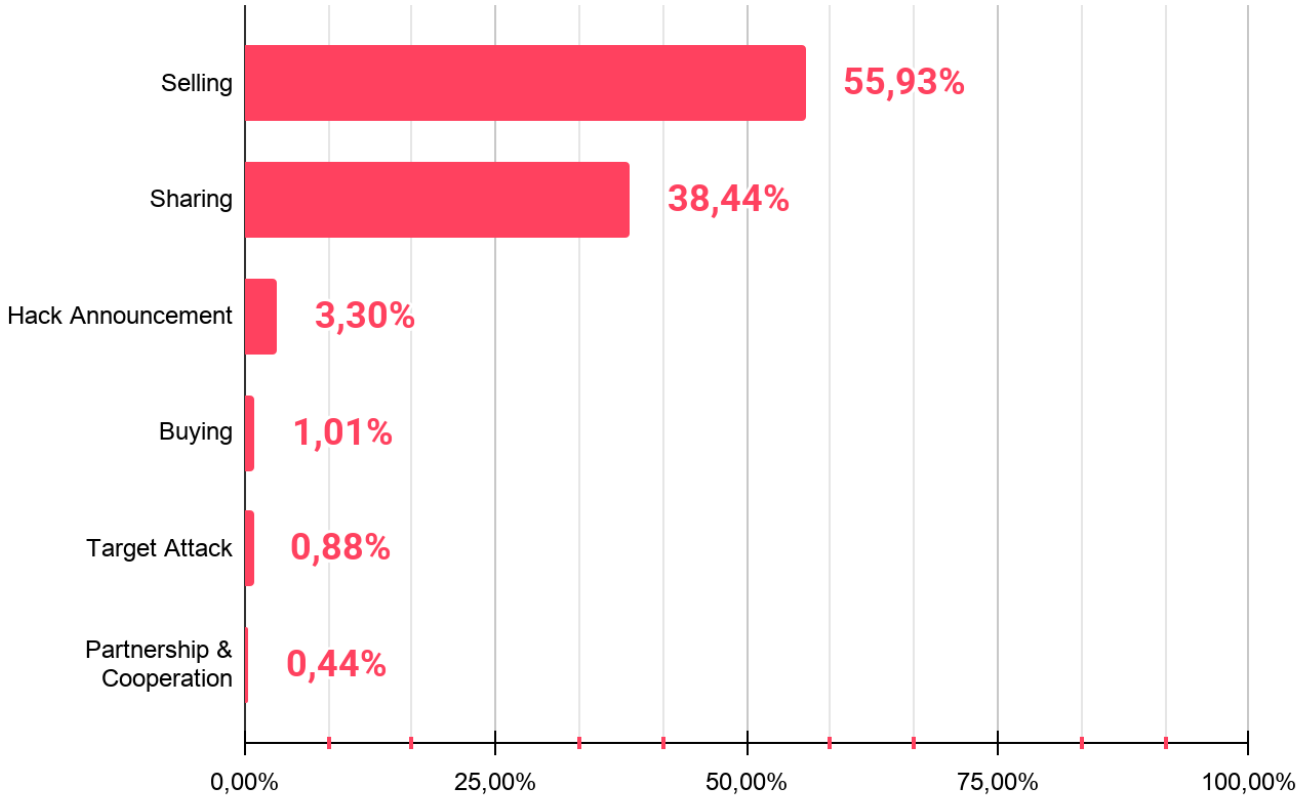
SOCRadar®
Your Eyes Beyond

APAC

Threat Landscape Report 2026

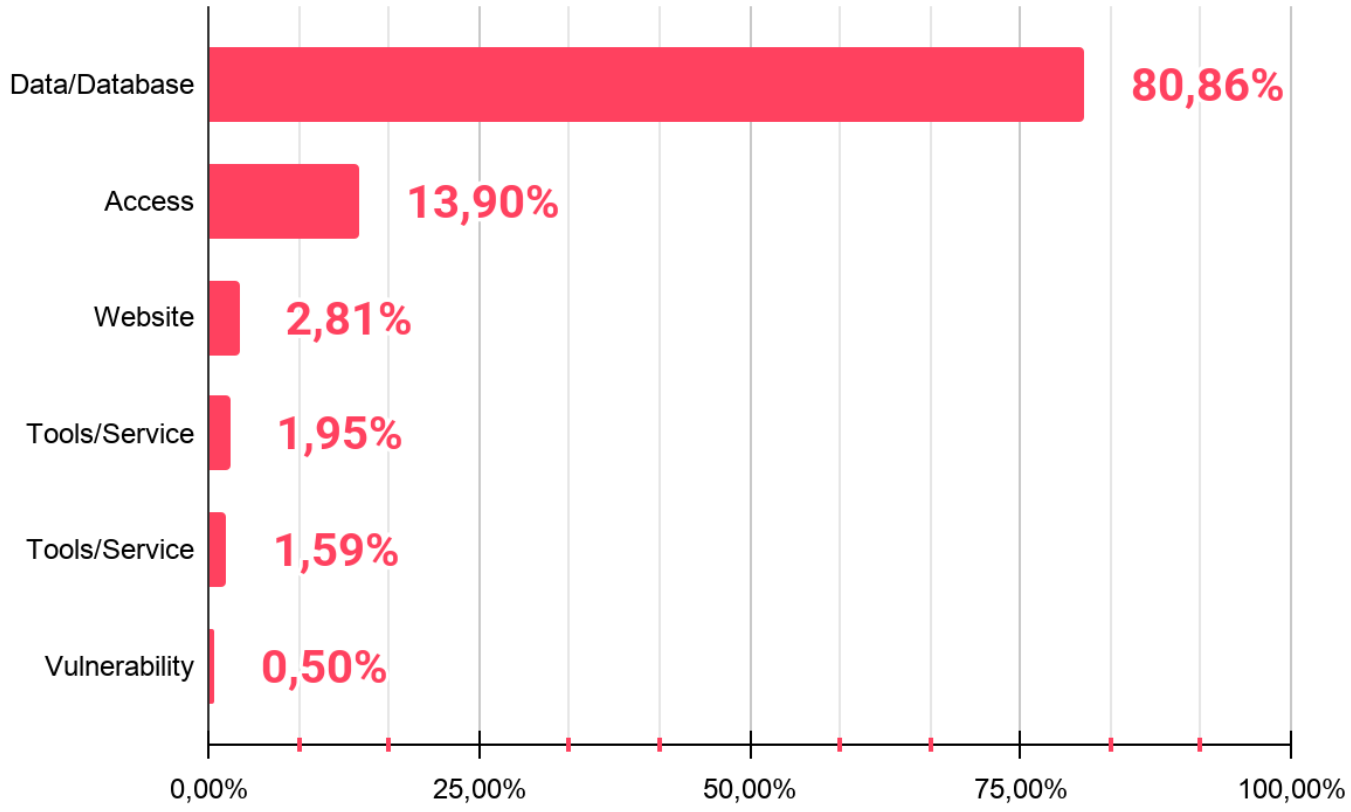
CISO Brief

Distribution of Dark Web Threats by Threat Categories



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.

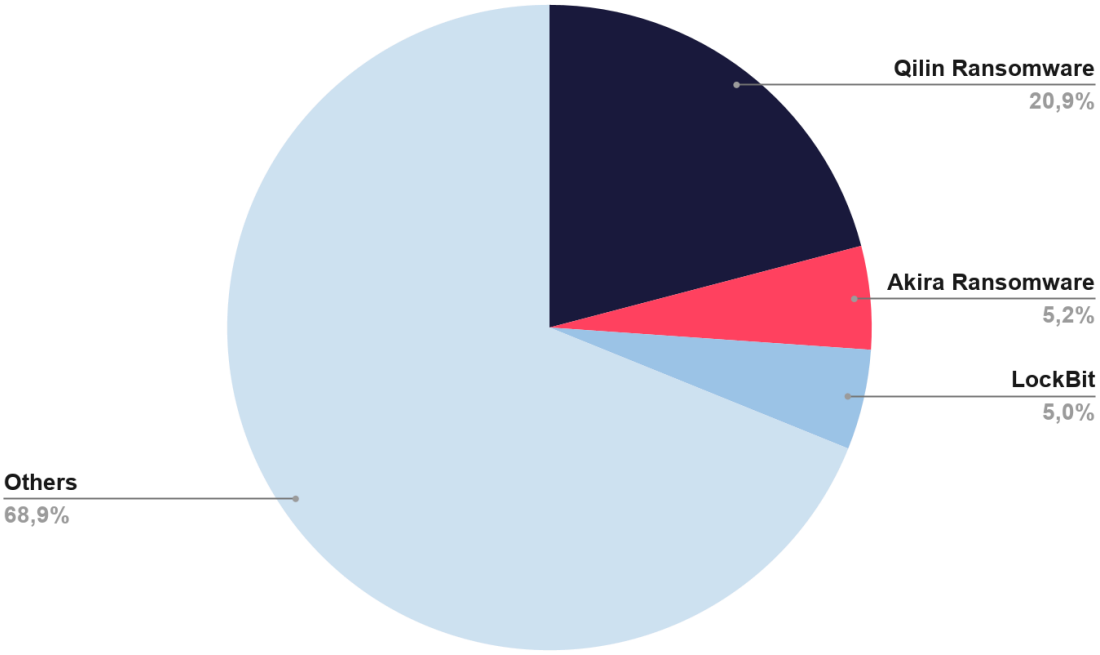
Distribution of Dark Web Threats by Threat Type



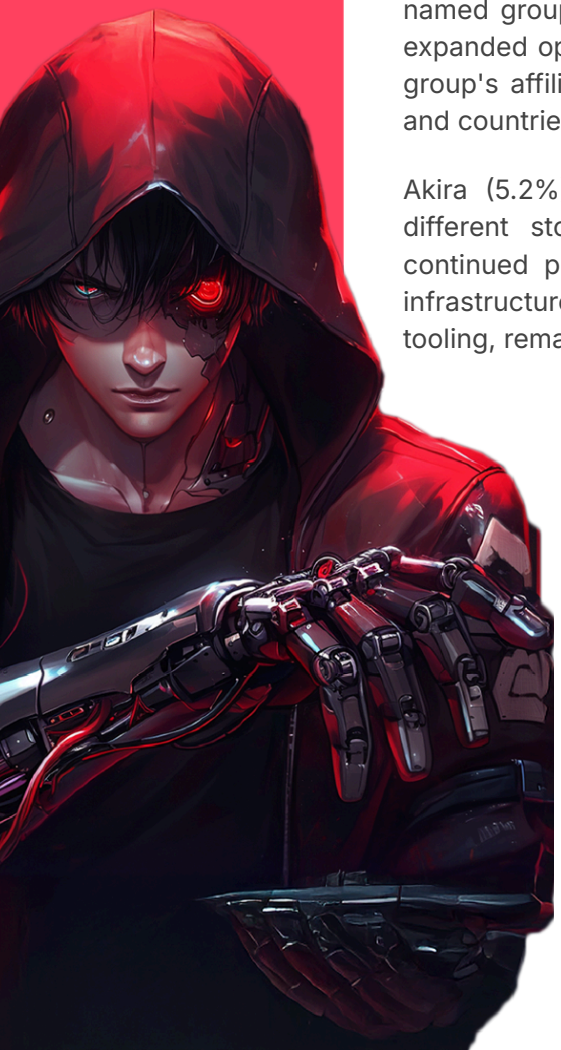
Data and database leaks dominate APAC dark web threats at 80.86%, confirming that stolen information is the core commodity in the regional underground economy. This aligns with the earlier finding that Selling and Sharing together drive over 94% of activity, since databases are the most common asset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

Top Ransomware Groups Targeting APAC



Few big names, many small crews

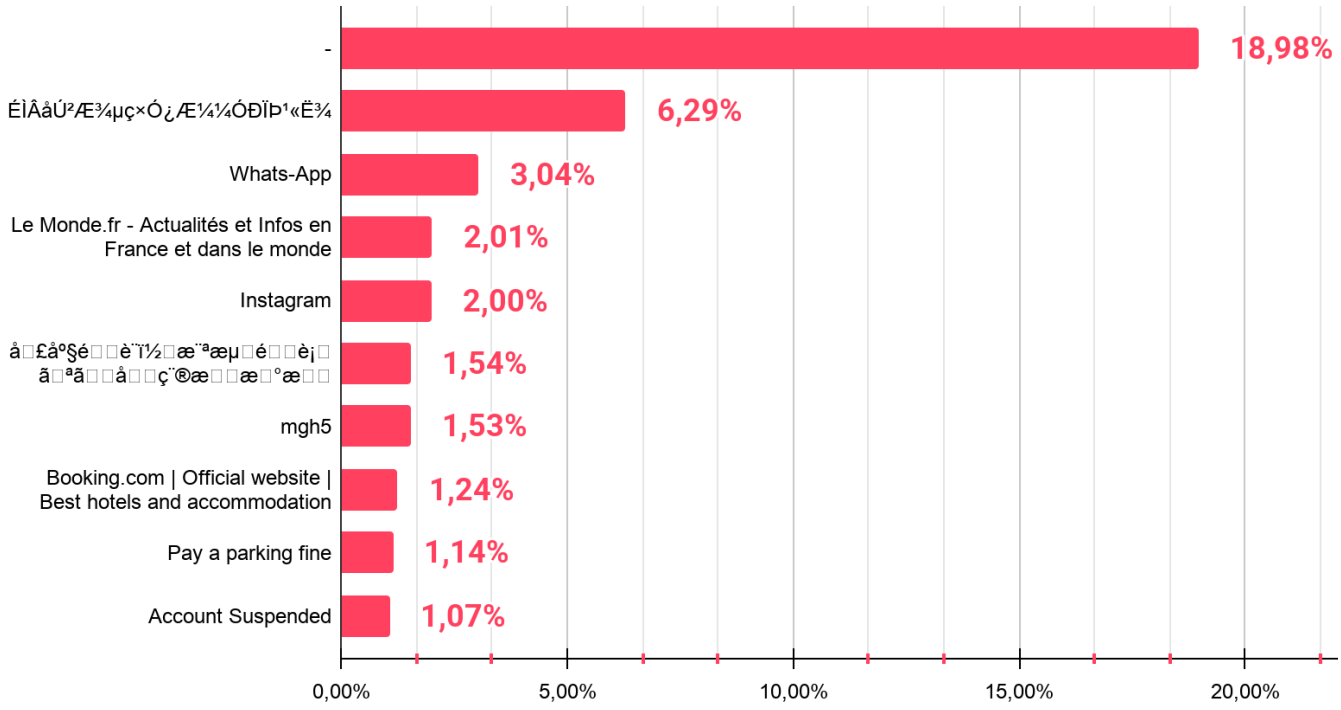


Qilin leads ransomware activity against APAC at 20.9%, standing well ahead of other named groups. Its dominance reflects a broader trend seen through 2025, where Qilin expanded operations after several rival groups were disrupted by law enforcement. The group's affiliate-driven model allows it to scale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

Phishing Attacks - Distribution by Phishing Page Title



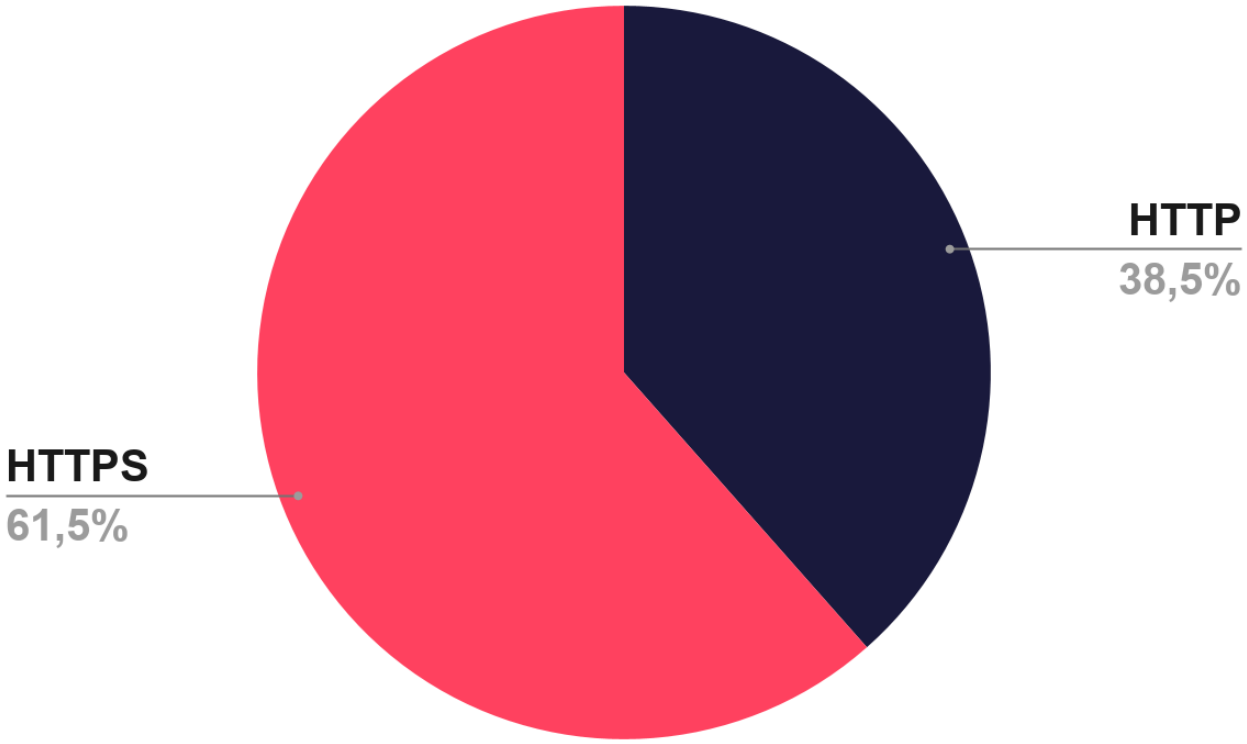
Phishing page titles in APAC show a clear mix of brand impersonation and generic lures. Nearly 19% of pages have no title at all, which is a common technique to avoid detection by automated scanners that rely on metadata for classification.

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 from providers like Let's Encrypt 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.

Recommendations for CISOs:

- **Implement Advanced Dark Web Monitoring:**
  Deploy specialized tools to track and analyze Dark Web activity, focusing on data breaches and illicit marketplaces. Regularly share intelligence with peer organizations to pre-empt emerging threats.

- **Strengthen Ransomware Resilience:**
  Develop comprehensive incident response plans, conduct frequent penetration testing, and maintain robust, secure backups. Prioritize protection for high-value sectors such as finance and information services.

- **Enhance Phishing Detection and User Awareness:**
  Integrate sophisticated anti-phishing solutions that detect HTTPS anomalies and deceptive page titles. Roll out targeted training programs to improve employee vigilance against social engineering.

- **Prioritize Data Protection & Access Controls:**
  Enforce strict multi-factor authentication, ensure encryption of sensitive data, and regularly audit access privileges to minimize the risk of credential compromise and data theft.

- **Focus on Critical Infrastructure Security:**
  Invest in specialized defenses for sectors like transportation, utilities, and public administration. Emphasize resilience planning and regular simulations to ensure rapid recovery from attacks.

- **Collaborate and Share Intelligence:**
  Engage with industry peers and national cybersecurity frameworks to exchange threat intelligence. Collaboration can provide early warnings and collective response strategies against diverse cyber threats.

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.