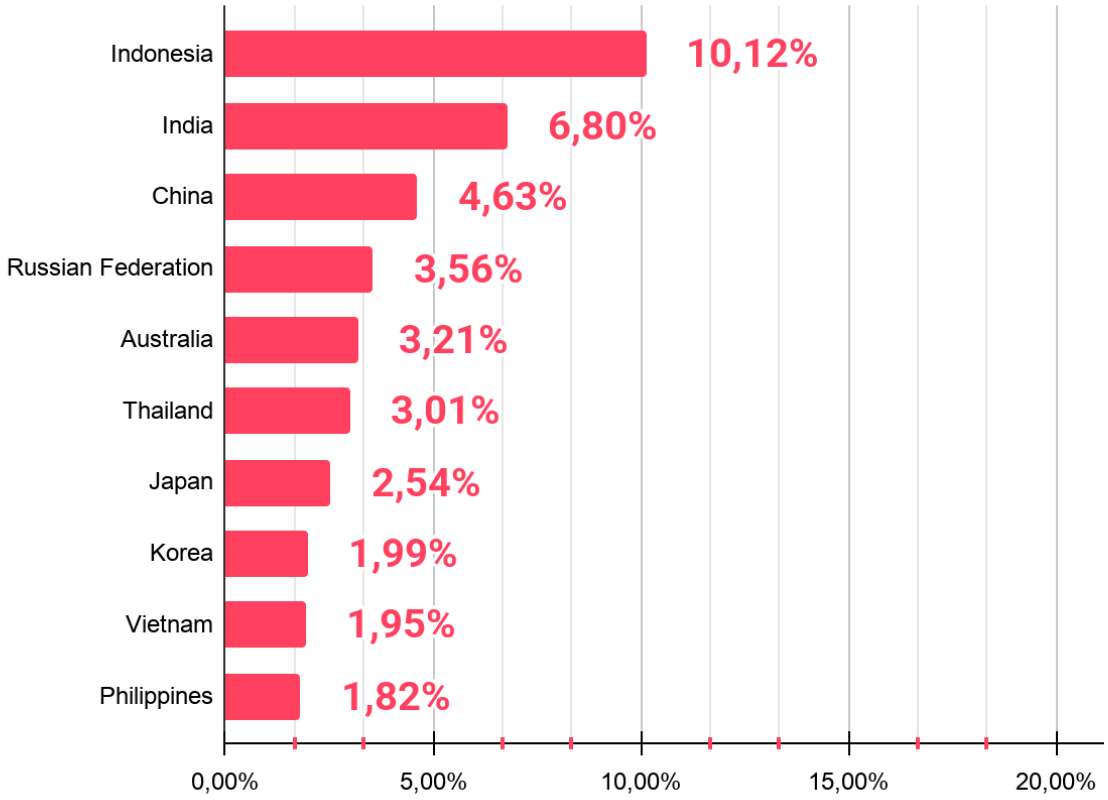
SOCRadar®
Your Eyes Beyond

APAC

Threat Landscape Report 2026

CEO Brief

Distribution of Dark Web Threats by Target Country

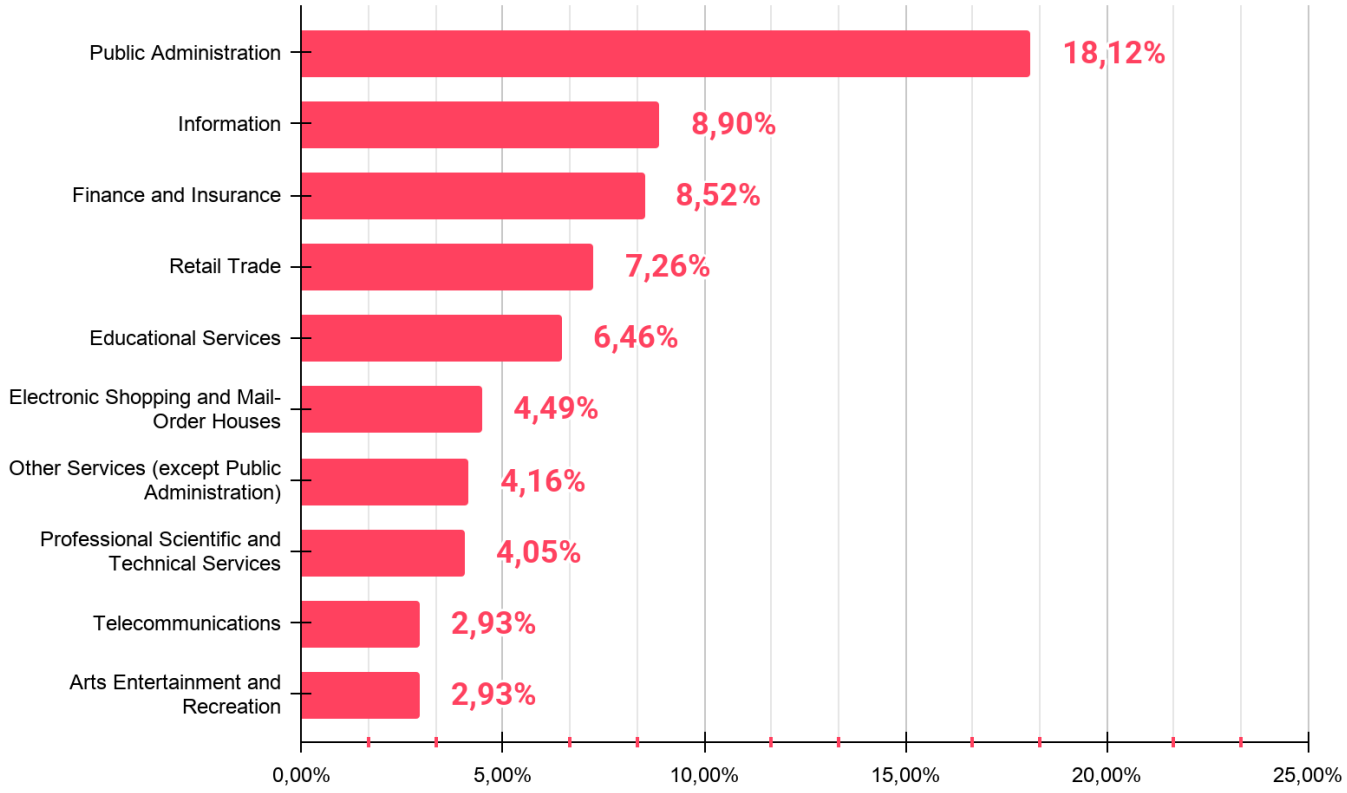


Indonesia tops dark web threat activity in APAC at 10.12%, leading the region by a wide margin. Rapid digital adoption, a large online population, and a growing e-commerce market likely contribute to this exposure. India follows at 6.80%, reflecting a similar pattern of fast digitalization paired with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

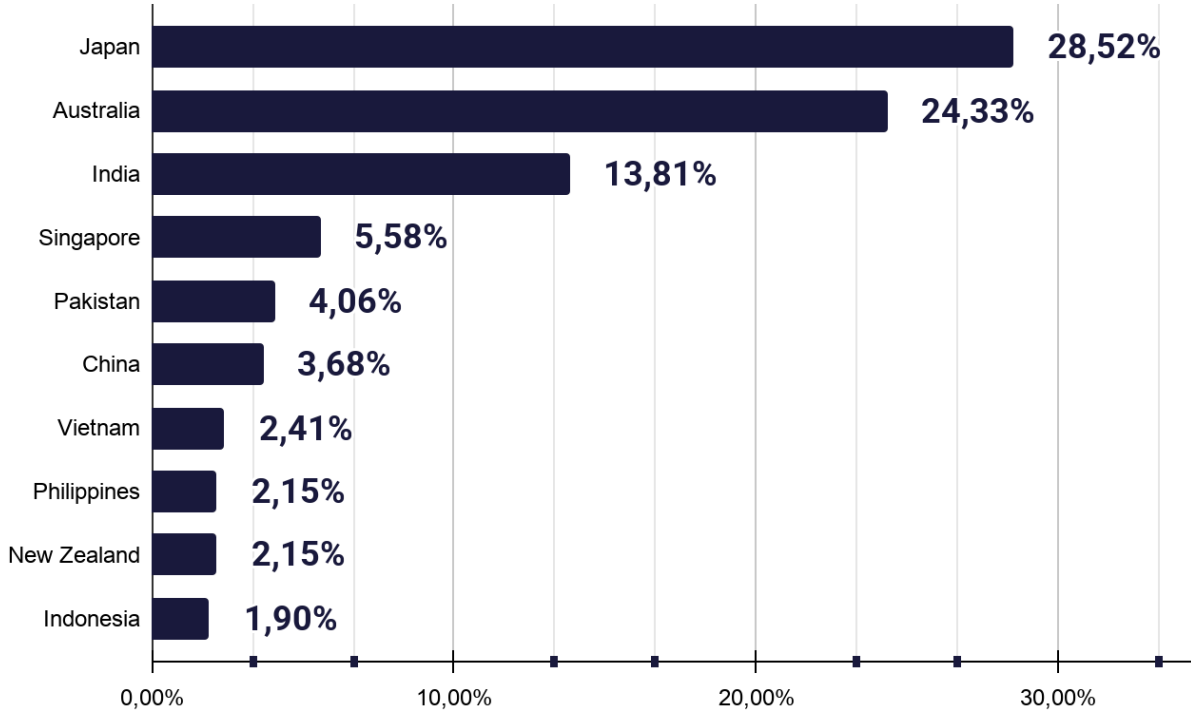
Southeast Asian countries dominate the rest of the list, with Thailand, Vietnam, and the Philippines all appearing in the top ten. This concentration suggests threat actors are actively focused on the region's emerging digital economies, where security maturity often lags behind adoption rates.

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 Ransomware Attacks by Primary Target Country

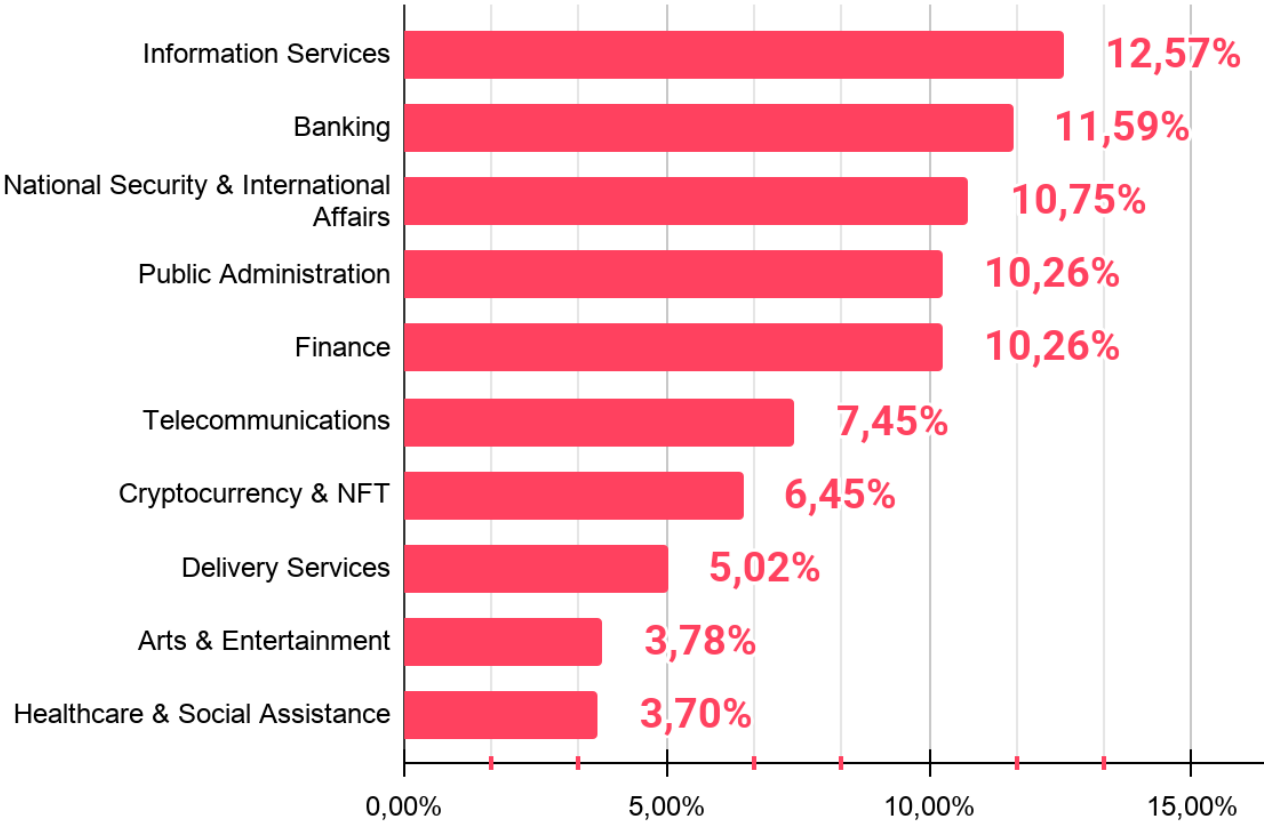


Japan leads ransomware impact in APAC at 28.52%, followed closely by Australia at 24.33%. Together these two developed economies absorb more than half of all regional ransomware activity. Their large industrial bases, high reliance on digital operations, and the strong financial returns attackers can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

Phishing Attacks - Distribution by Industry

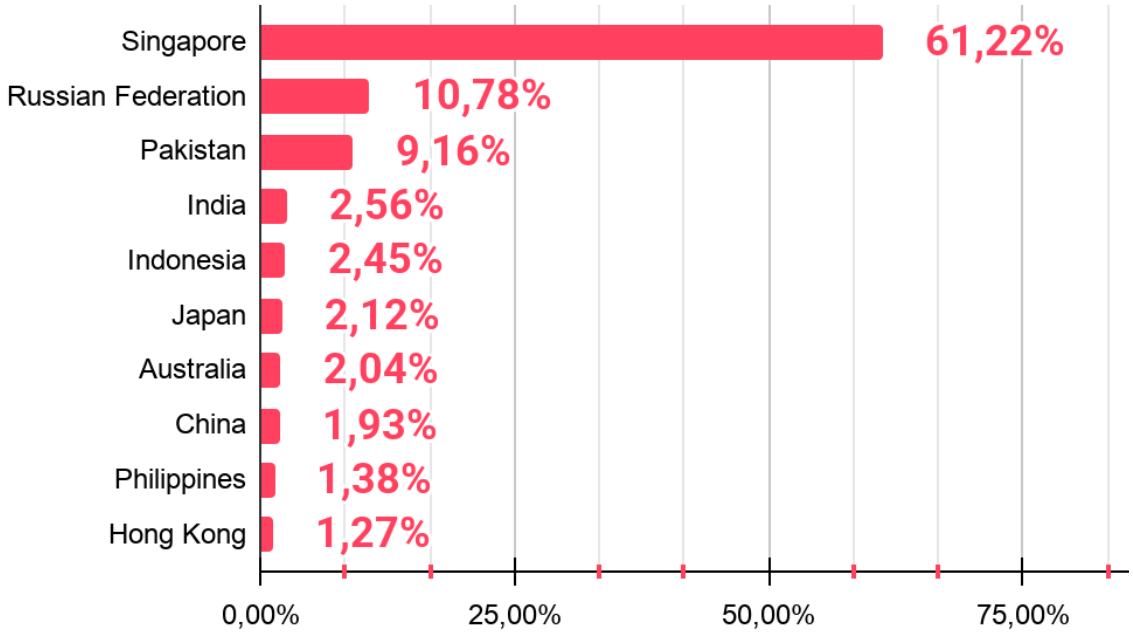


Phishing in APAC spreads more evenly across industries than other threat types, with the top five sectors each holding around 10–12% of activity. Information Services leads at 12.57%, followed by Banking (11.59%) and National Security & International Affairs (10.75%). The strong presence of government-linked 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



Singapore stands out sharply in phishing activity at 61.22%, far ahead of any other country in the region. This concentration likely 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 portals for every language

Recommendations for CEOs:

- **Invest in Cybersecurity as a Strategic Priority:**
  Allocate sufficient budget and resources to bolster cybersecurity measures, recognizing that robust digital defenses are critical to protecting the company's reputation and financial assets.

- **Foster a Culture of Security:**
  Champion cybersecurity at the executive level to ensure it is integrated into business strategy. Encourage cross-departmental collaboration and continuous employee training to minimize risks stemming from phishing and insider threats.

- **Enhance Risk Management and Business Continuity:**
  Develop and regularly update comprehensive risk management and incident response plans. Prioritize investments in cybersecurity insurance and business continuity planning to mitigate potential financial impacts from cyber incidents.

- **Leverage Data-Driven Cyber Intelligence:**
  Utilize insights from threat intelligence reports to inform decision-making. Understanding evolving risks—such as ransomware and Dark Web threats—can guide strategic investments and partnerships for improved defense.

- **Strengthen Regulatory and Compliance Posture:**
  Stay ahead of evolving regulatory requirements and industry standards. Proactive compliance can reduce legal risks and build trust with customers, investors, and partners.

- **Collaborate with Industry Peers and Stakeholders:**
  Engage with cybersecurity forums, industry groups, and government initiatives to share best practices and intelligence. Such collaboration enhances overall resilience and can lead to collective responses to emerging 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.