Indonesia

Regional Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

Table of Contents

Executive Summary

Top Takeaways

Public Administration is the most targeted industry on the dark web, making up 34.93% of observed threats. Education follows at 12.59%, and Finance-related sectors total 9.57%.

Indonesia is the direct target in 55.7% of dark web threats, while 44.3% involve both Indonesia and other countries.

Data/Database leaks dominate dark web threat types at 88.12%, with Access sales next at 9.67%.

In threat activity categories, Sharing leads with 65%, followed by Selling at 32.3%.

For ransomware, 63.3% of attacks come from smaller or “other” groups. Babuk/Babuk2 leads named groups at 14.3%, with Fog Ransomware at 12.2% entering the top three for the first time.

28.8% of ransomware incidents target Indonesia alone, while 71.2% hit Indonesia along with other countries.

In phishing, Finance tops the sector list at 24.42%, with Telecommunications and Information Services following.

25% of phishing pages have no title, but the most common named lure is DANA e-wallet at 4.95%.

59.62% of phishing sites use HTTPS, undermining the padlock icon as a trust indicator.

Technical Details

This report based on data collected between August 2024 and August 2025

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

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.

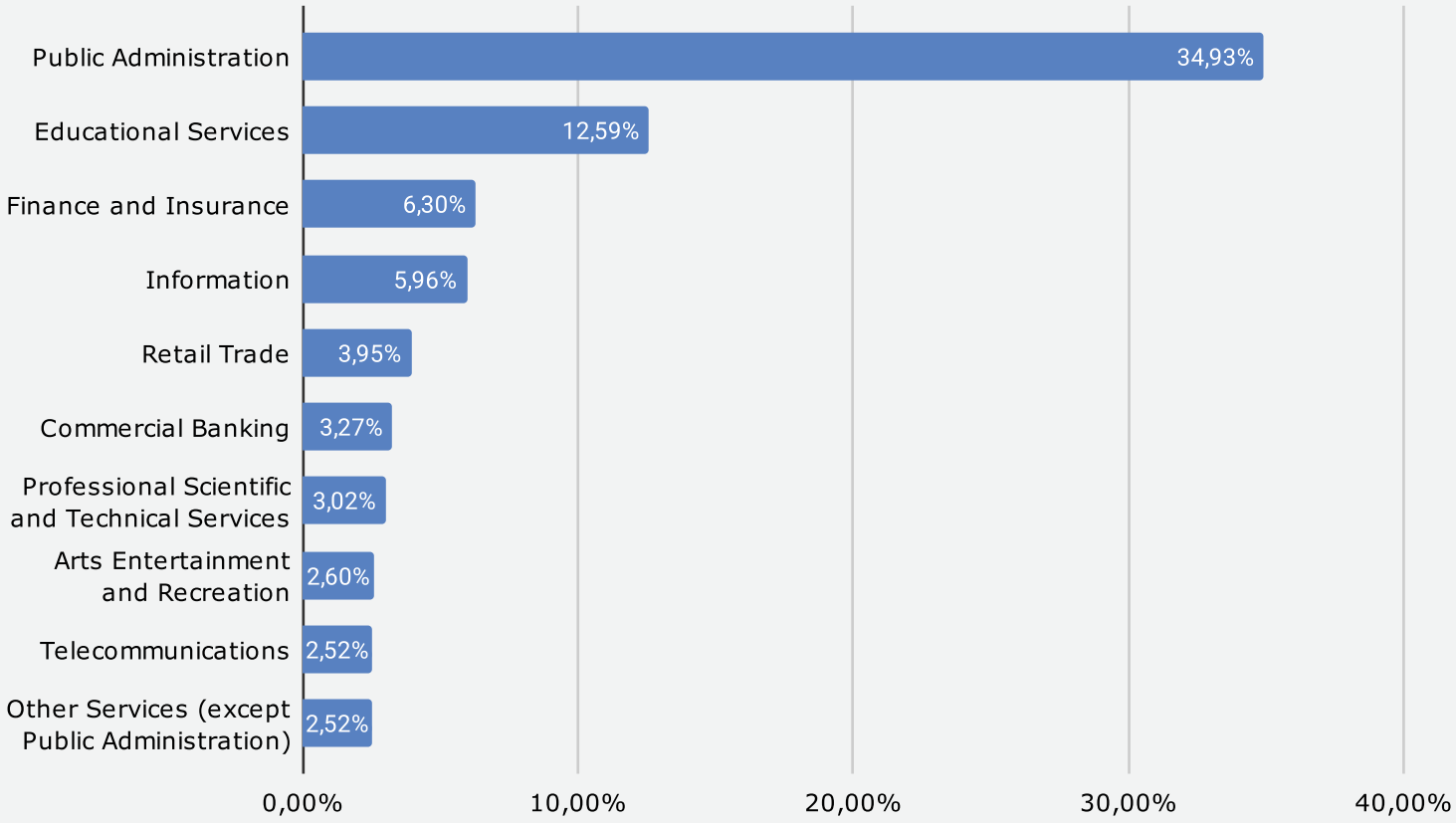
In the Ransomware Threats chapter you will find detailed information about ransomware actors targeting Indonesia, their detailed profiles and the necessary data that summarizes the ransomware activities.

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.

And lastly, the DDoS Attack Statistics shows you the latest information about the intensity of DDoS attacks and how threat actors target organizations to disrupt their operations.

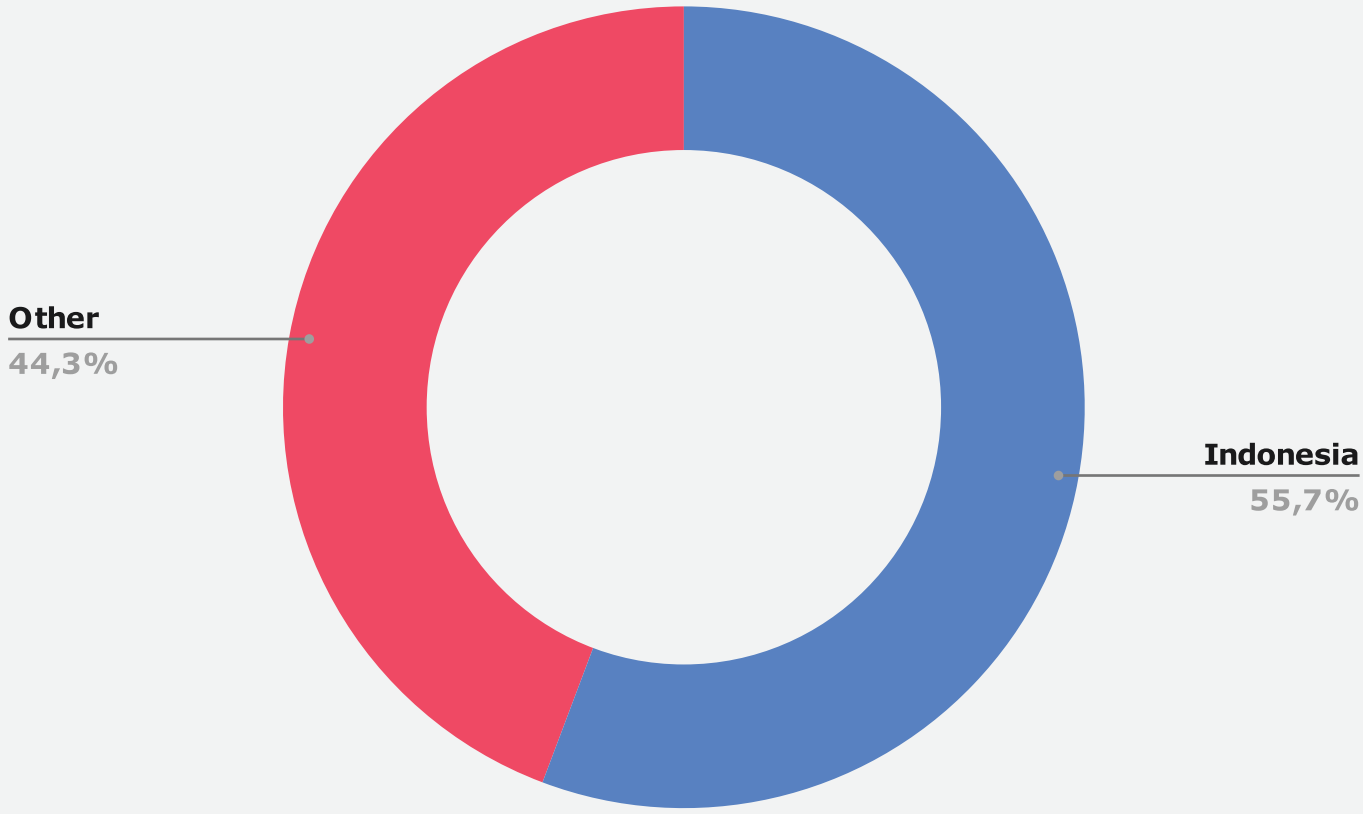
Dark Web Threats Targeting Indonesia

Industry Distribution of Dark Web Threats



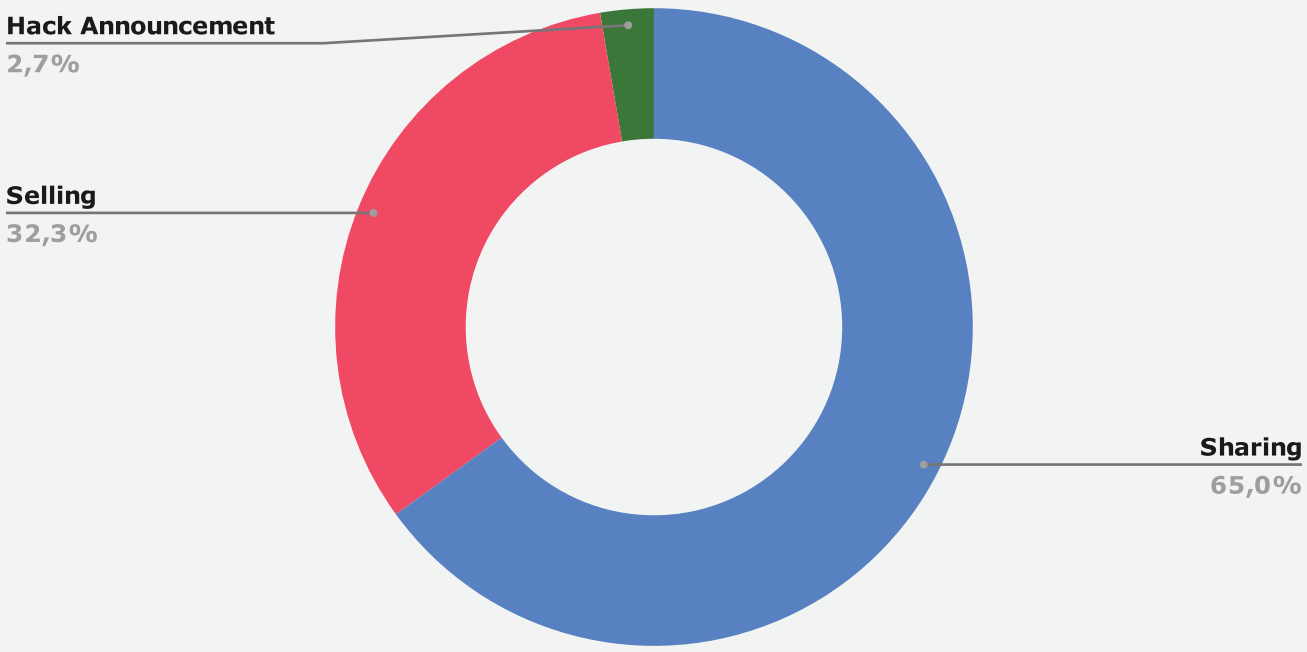
Public Administration dominates dark web exposure at 34.93%, which signals sustained interest in government data and credentials. Education ranks second with 12.59%, likely due to open networks and large stores of student and staff PII. Finance and Insurance at 6.30%, plus Commercial Banking at 3.27%, bring financial targets to 9.57% in total.

Distribution of Dark Web Threats by Primary Target Country



More than half of the recorded dark web threats targeting Indonesia, 55.7%, targeted the country alone. This shows a strong focus by threat actors on Indonesian systems, data, and users. The remaining 44.3% targeted Indonesia and other countries. They involve Indonesian-linked entities through global supply chains or shared platforms.

Distribution of Dark Web Threats by Threat Categories

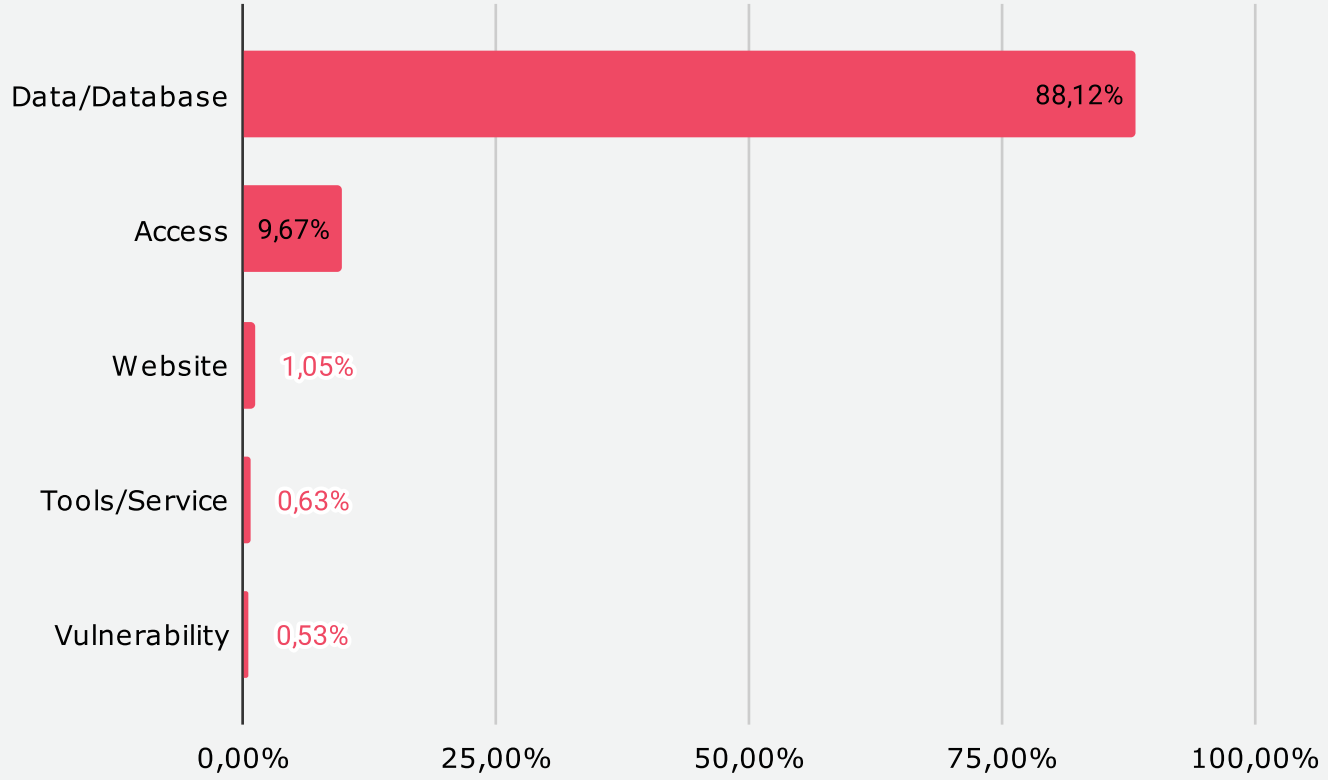


Sharing makes up the largest share of dark web threats at 65%, showing that most activity involves distributing stolen data, credentials, or tools without direct sale. This often serves as a way to build reputation, attract partners, or prepare for later monetization.

Selling accounts for 32.3%, which still represents a significant market for direct profit, with offers ranging from personal data to access to compromised systems.

Hack Announcements are rare at 2.7%, but they can signal upcoming large-scale leaks or campaigns, giving early warning for targeted sectors.

Distribution of Dark Web Threats by Threat Type



Data and database-related threats dominate the dark web landscape at 64.78%, indicating a strong focus on exfiltrating and distributing sensitive information. Access threats follow at 27.88%, suggesting significant demand for unauthorized entry points into systems or networks. Website compromises (3.31%), malicious tools/services (2.88%), and vulnerabilities (1.14%) are far less frequent, highlighting that attackers prioritize tangible assets like data and credentials over exploits or technical resources. The trend points to data as the primary commodity driving underground activity.

Recent Dark Web Activities Targeting Entities in Indonesia

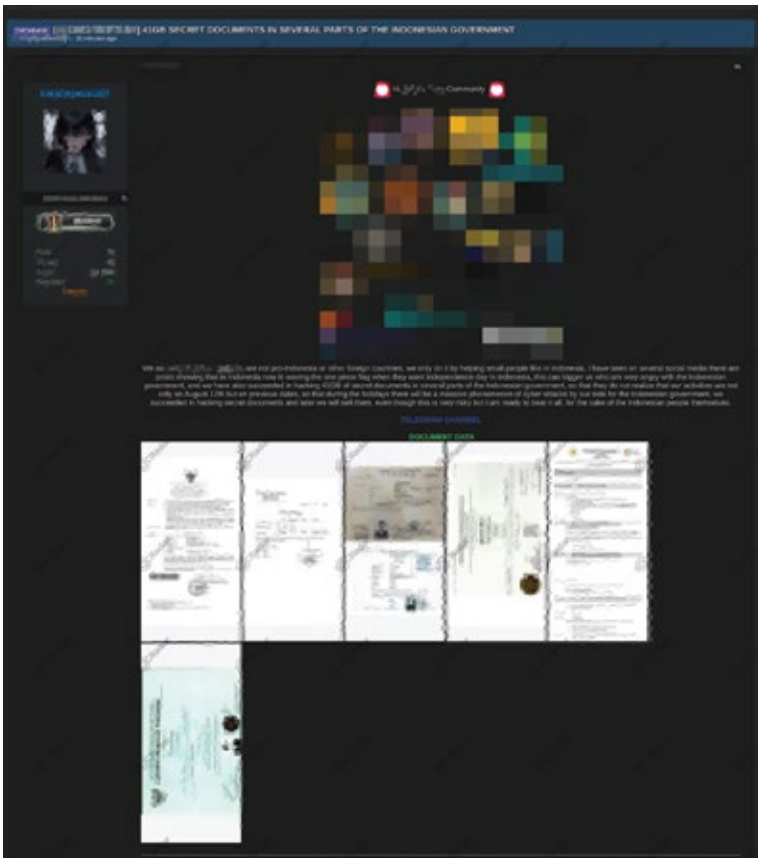
The Alleged Data of Indonesian Citizens are on Sale

SOCRadar has detected a new post on a dark web hacking forum advertising what the seller claims is personal data belonging to Indonesian citizens. The listing, labeled “DATA KAB LAHAT”, reportedly includes:

National Identification Numbers (NIK), addresses, and additional personal details.

The dataset is being offered for $100, with contact information provided via a Telegram handle.

The Alleged Data of Many Indonesian Governments are on Sale

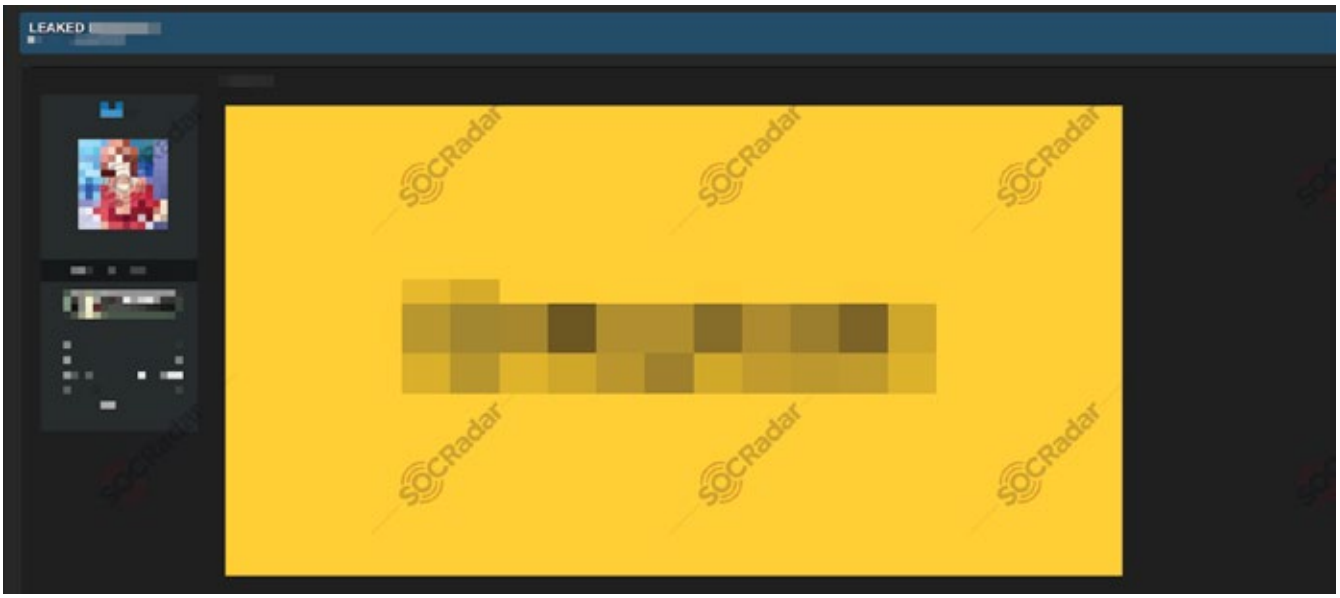


SOCRadar has identified a dark web forum post claiming the sale of 41GB of sensitive documents allegedly stolen from multiple Indonesian government entities. The actor behind the post describes the attack as politically motivated, citing anger toward the government over certain social media activity.

In the message, the threat actor states they will launch a wave of cyberattacks against government systems during the Indonesian Independence Day holidays on August 17. They further claim the breach has already occurred in previous weeks and that the stolen data will be sold despite the risks involved.

According to the post, the compromised data consists of “secret documents” from several government departments. The actor also references a Telegram channel as a point of contact and potential outlet for further leaks.

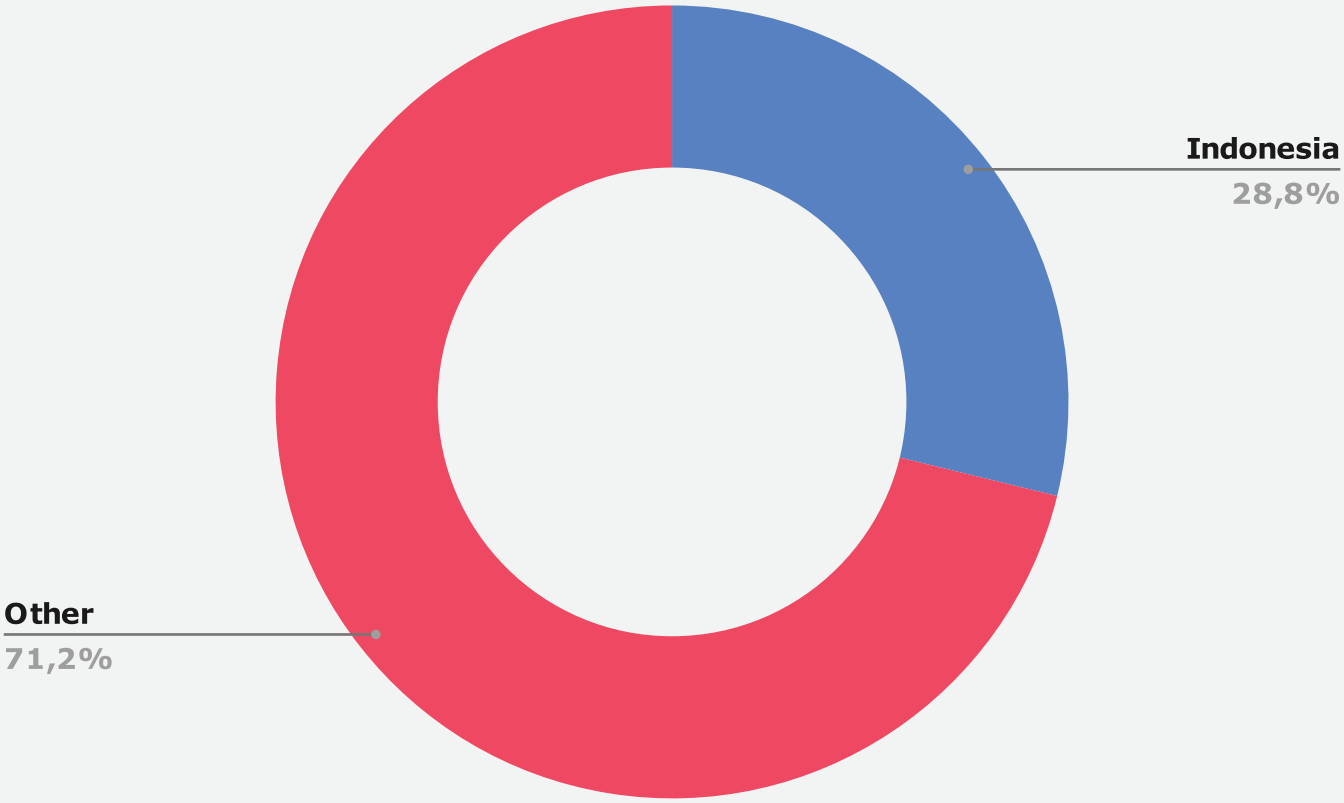
Alleged Banking Sector Database Leak Detected on Dark Web



SOCRadar has observed a new post on a dark web forum advertising what the seller claims is a leaked database from a financial institution operating in the banking sector.

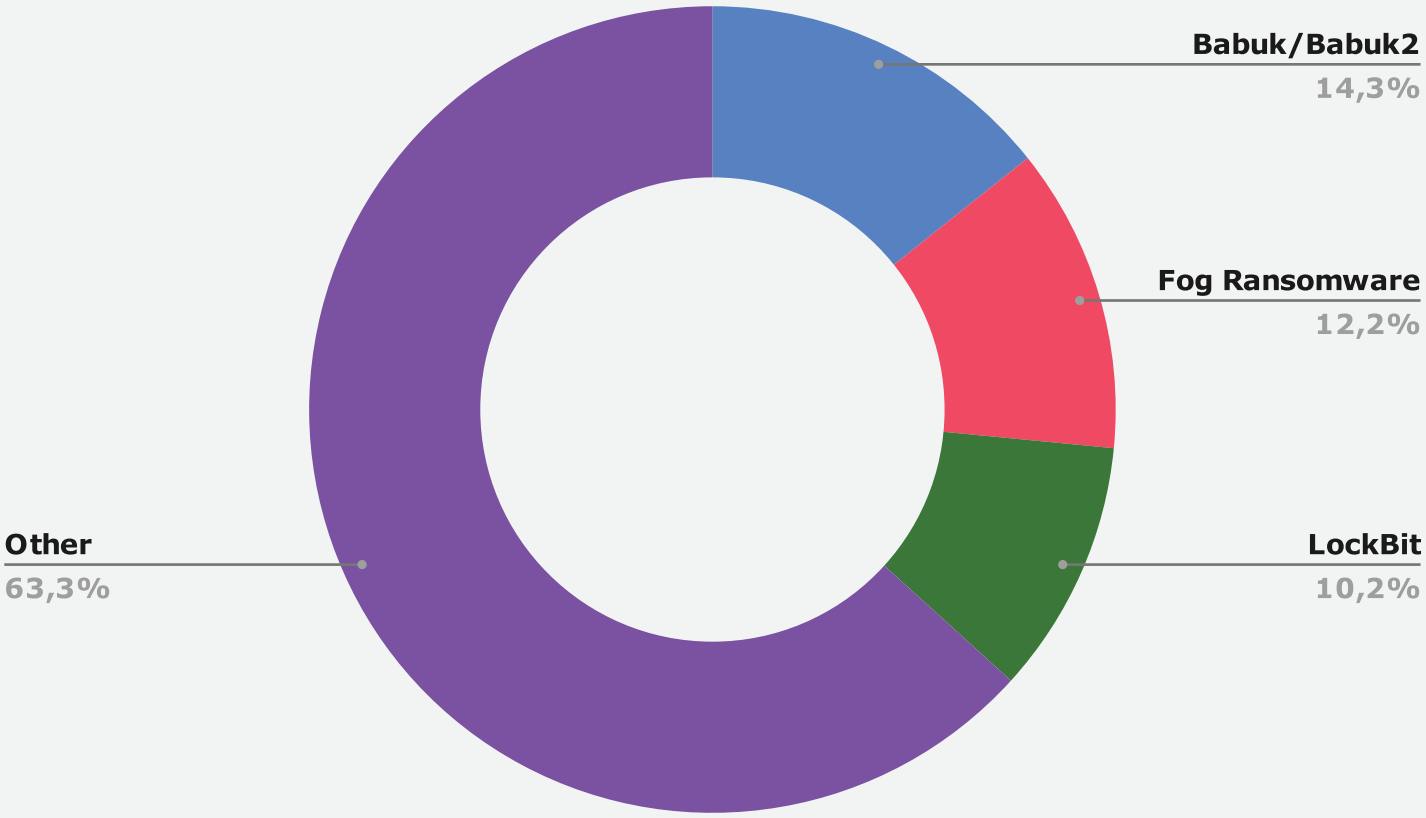
Ransomware Threats Targeting Indonesia

Distribution of Ransomware Attacks by Country



Indonesia-only targets make up 28.8% of ransomware attacks in the dataset. The remaining 71.2% involved Indonesia alongside other countries, showing that most incidents here are part of wider campaigns. This pattern shows that many ransomware groups operate globally and hit multiple regions at once, by targeting shared supply chains.

Top Ransomware Groups Targeting Indonesia



Other ransomware groups still dominate with 63.3%, highlighting the wide range of smaller actors targeting Indonesia.

Babuk/Babuk2 leads the named groups at 14.3%, continuing its pattern of both encrypting and stealing data.

Fog Ransomware comes next at 12.2%. While its activity is not entirely new, this is the first time it has climbed into the top three, showing a rise in prominence and possibly expanding targeting in the region.

A Closer Look into The Top 3 Ransomware Groups

Babuk/Babuk2 Ransomware

Babuk, originally emerging in 2020, became infamous for its ransomware attacks on large organizations and government agencies. After internal conflicts led to the leak of its source code, the group disbanded, giving rise to Babuk V2, which shifted to data theft and extortion.

In 2025, a new iteration, Babuk2, resurfaced under the alias Bjorka, a notorious hacker known for targeting the Indonesian government. While claiming massive data breaches and extortion, Babuk2's true capabilities are unclear, with many of its leaks seeming to be recycled from previous incidents. Despite doubts, Babuk2 continues to capitalize on fear and reputation, pushing its ransomware operation for profit.

You can visit our *blog post* for more detailed information about RansomHub.

Fog Ransomware

Fog Ransomware emerged in April 2024, was first detected in the wild in early May, primarily targeting US based educational institutions targeting both Windows and Linux endpoints. It operates as a multi-pronged extortion campaign, utilizing a TOR-based data leak site (DLS) to list victims and host stolen data for those who refuse to comply with ransom demands.

Researchers classify Fog as a ransomware variant rather than a ransomware group, distinguishing between the entities responsible for developing the encryptor software and those carrying out hands-on-keyboard attacks. This distinction is crucial, as ransomware groups often present themselves as unified entities when, in reality, they operate through independent affiliate groups.

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

LockBit Ransomware

LockBit 3.0, succeeding LockBit and LockBit 2.0, functions as a Ransomware-as-a-Service (RaaS) entity.

Since January 2020, LockBit has transitioned to an affiliate-based model, employing diverse methodologies to target businesses and critical infrastructure entities.

Noteworthy tactics include double extortion and the utilization of initial access broker affiliates, alongside recruitment efforts involving insiders and hacker recruitment competitions.

With over 1,500 victim disclosures on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's cessation. As of the first quarter of 2023, they retain their position as the most prolific group, with over 300 disclosed victims.

You can visit our *blog post* for more detailed Lockbit 3.0 Ransomware Group information.

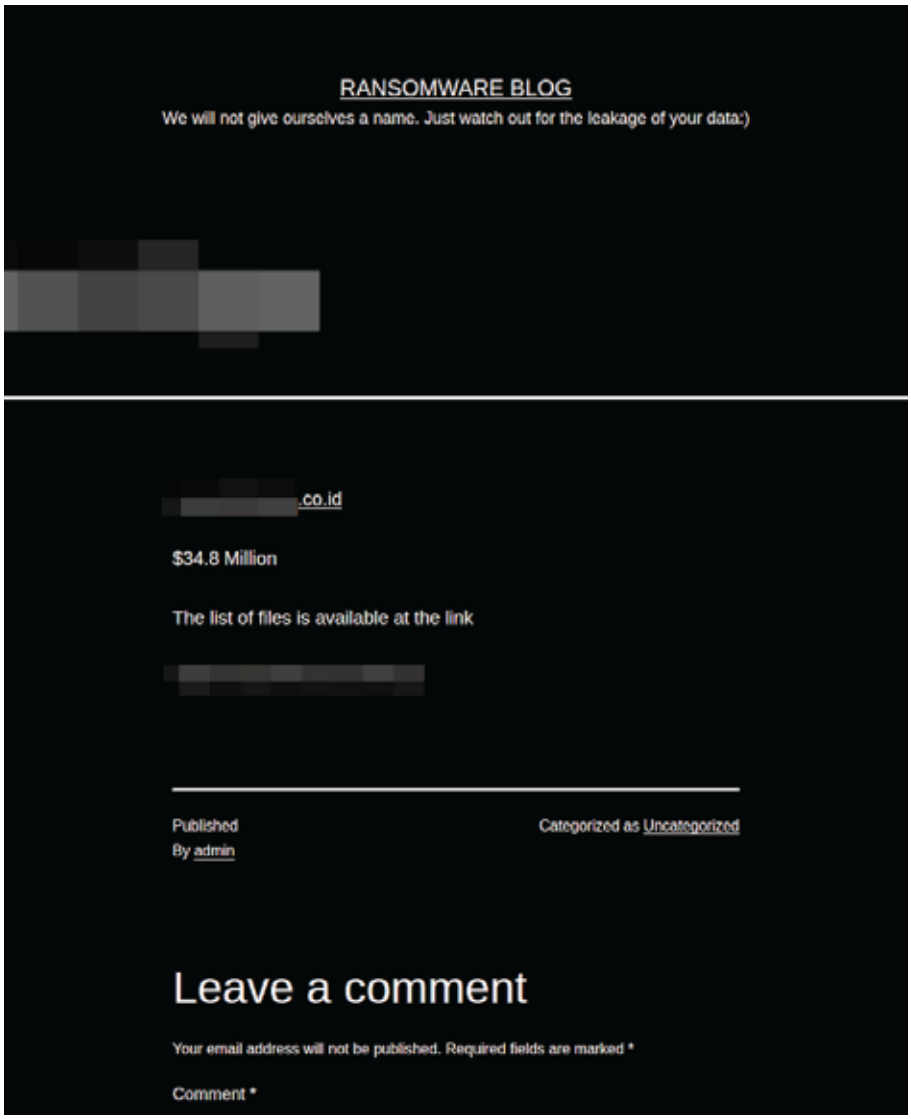
Recent Ransomware Attacks Targeting Entities in Indonesia

Funksec Ransomware Group Claims Local Government Sector Target in Indonesia

SOCRadar has identified a new entry on the Funksec ransomware group's leak site, allegedly involving a local government website in Indonesia.

The targeted site is described as providing information and public services for a village community, including local governance updates, community resources, and visitor information.

MedusaLocker Ransomware Group Claims Attack on Indonesian Wholesale & Distribution Sector



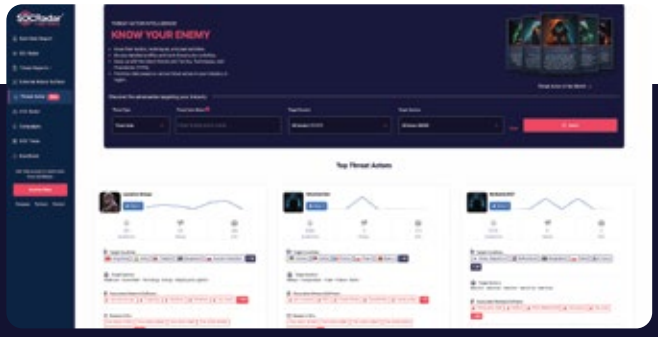
SOCRadar has observed a new post on the MedusaLocker ransomware group's leak site, allegedly targeting a company in Indonesia's wholesale and distribution sector.

According to the listing, the victim organization generates approximately $34.8 million in revenue. The ransomware group claims to possess a list of stolen files, which they have made available via an external link.

Fog Ransomware Group Claims Attack on Indonesian IT Services Sector

SOCRadar has detected a new listing on the Fog ransomware group's leak site, allegedly involving a major IT solutions and software development company in Indonesia.

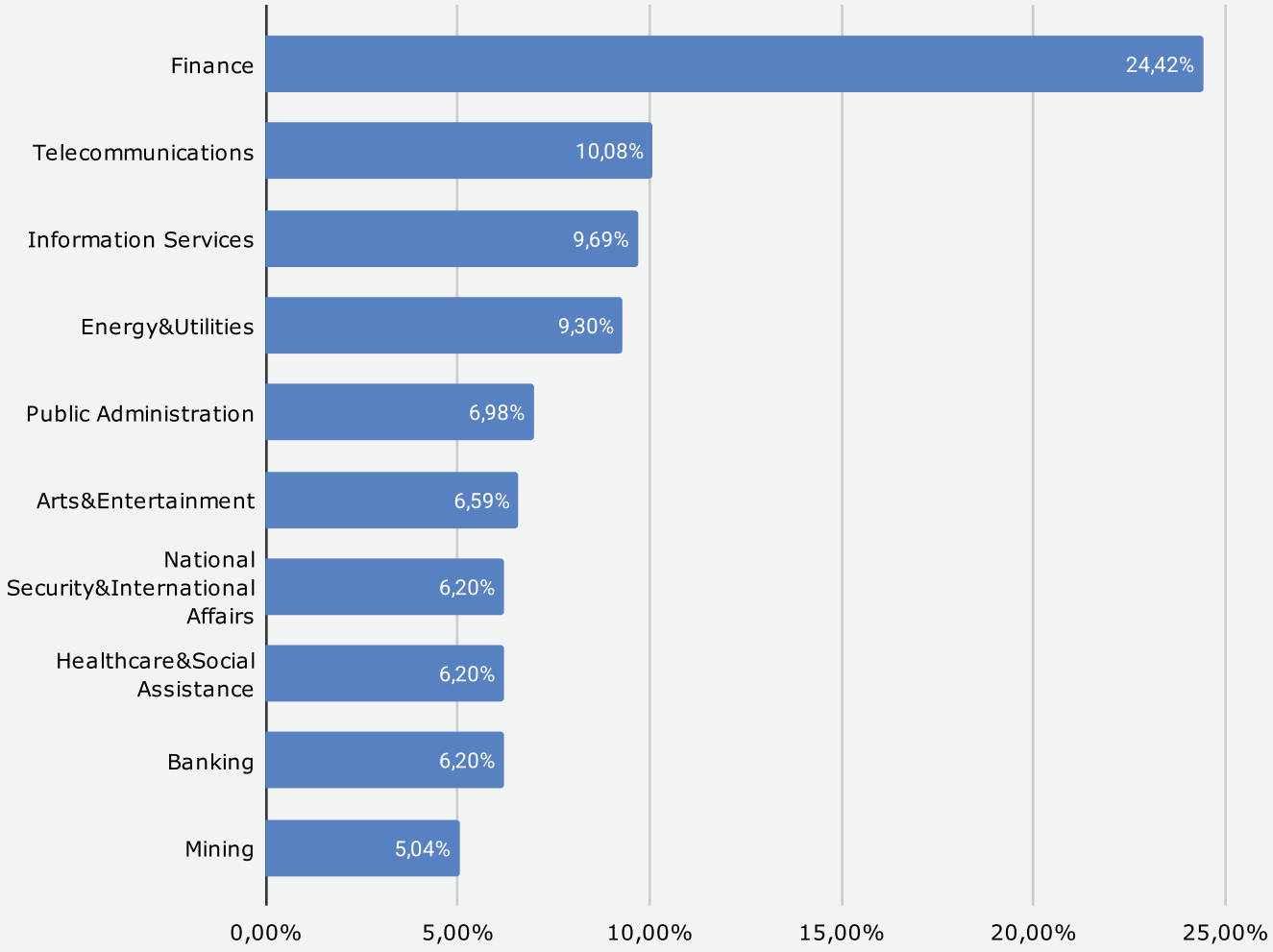
The targeted organization is described as one of the largest in its field, providing technology solutions and development services to numerous clients across various industries.



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 Indonesia

Phishing Attacks - Distribution by Industry



Finance leads phishing targets with 24.42%, reflecting the high value of credentials and financial data for fraud and account takeover.

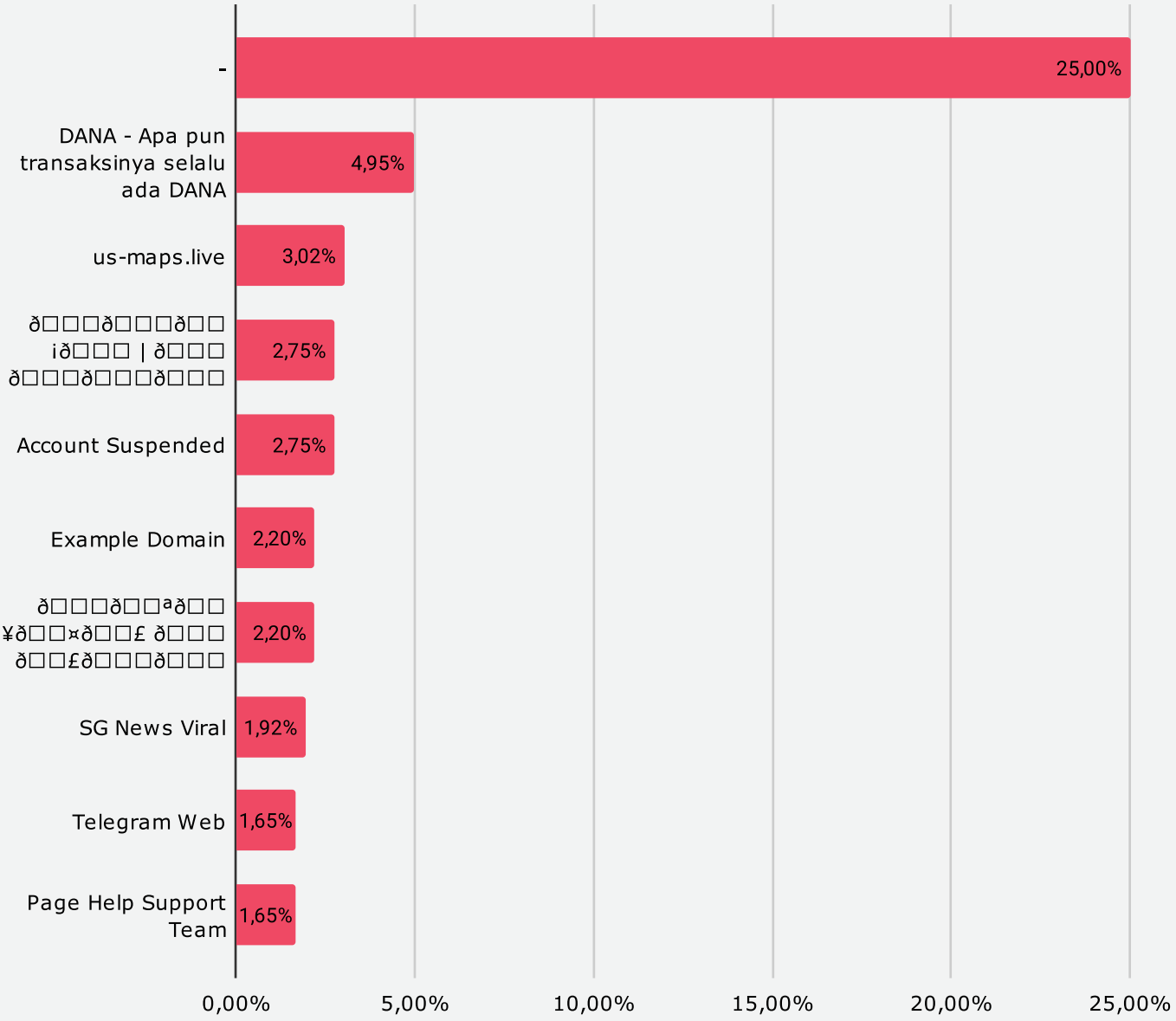
Telecommunications (10.08%) and Information Services (9.69%) follow, both attractive for access to customer accounts and infrastructure that can be leveraged in further attacks.

Energy & Utilities at 9.30% shows that critical infrastructure is also in scope, where disruption can have wide operational impact.

The spread across sectors shows phishing is not limited to finance or IT-heavy industries.

Attackers appear to focus on either direct monetary gain or gaining a foothold in networks that link to more valuable targets.

Phishing Attacks - Distribution by Phishing Page Title

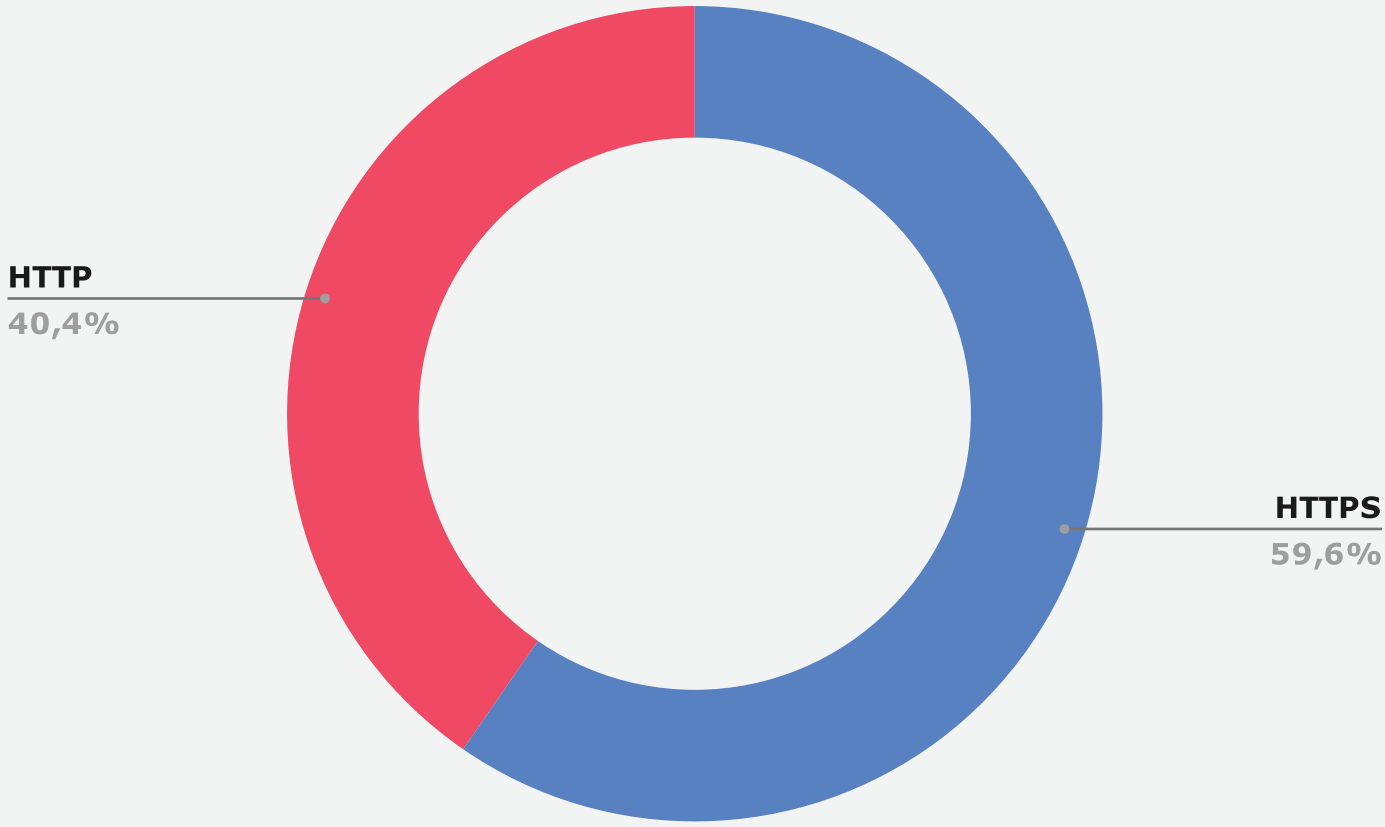


A quarter of phishing pages (25.00%) have no clear title, which is common when attackers either fail to configure metadata or use blank titles to avoid detection by automated systems. The most common named lure is “DANA - Apa pun transaksinya selalu ada DANA” at 4.95%, directly imitating a popular Indonesian e-wallet service to harvest credentials or payment details. Other entries like “us-maps.live” (3.02%) and “SG News Viral” (1.92%) suggest the use of topical or curiosity-driven themes to draw clicks.

Some pages mimic service or account issues, such as “Account Suspended” (2.75%) and “Page Help Support Team” (1.65%), which play on urgency and fear to push victims into quick action. Titles like “Telegram Web” (1.65%) show attempts to compromise messaging accounts for further phishing or fraud.

The mix of financial impersonation, urgent security notices, and topical bait reflects a broad approach, aiming to hook different victim profiles with both local and global themes.

Phishing Attacks - Distribution by SSL/TLS Protocol



Most phishing pages (59.62%) use HTTPS, showing that attackers actively obtain valid SSL/TLS certificates to make their sites look legitimate. This trend reduces the value of the “padlock” icon as a trust signal for users, since it now appears on a majority of malicious pages. HTTP is still used in 40.38% of cases, often for quick, disposable campaigns or when targeting less security-aware victims.

The high adoption of HTTPS in phishing suggests that attackers understand how to exploit user trust in secure-looking websites. It also means that relying on protocol type alone is ineffective for detection.

DDoS Attack Statistics

The threat landscape was pretty active for Indonesia.

- The **peak bandwidth** witnessed during a DDoS attack reached 172.01 Gbps, highlighting a significant capacity from the cyber threats.
- The **highest recorded throughput** during these incidents was 46.25 Mpps.
- Most DDoS attacks lasted **169.75** Minutes on average.
- **45,101 DDoS Attacks** were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for Indonesian targets.

The numbers above show that Indonesia faces a serious DDoS risk. The attacks don't take too long, but the amount of attacks and their size are considerable threats to organizations.

Top DDoS Attack Vectors

Attack Vector	Number of Attacks
DNS Amplification	12,349
TCP RST	12,191
TCP ACK	10,934
TCP SYN	9,468
STUN Amplification	5,421

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®?

Your Eyes Beyond

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.