SOCRadar®
Your Eyes Beyond

INDONESIA

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

Indonesia, Southeast Asia's largest economy and a rapidly growing digital hub, has become a significant target for cyber threats in recent years. As a key player in technology, finance, and logistics in the region, Indonesia's economy is deeply integrated into the global digital landscape, making it an attractive target for cybercriminals and state-sponsored threat actors.

Recent data indicates a sharp rise in cyber-attacks targeting Indonesia's critical infrastructure and key industries. These attacks are becoming increasingly sophisticated, reflecting the evolving tactics, techniques, and procedures (TTPs) of threat actors who are increasingly focusing on more complex and targeted cyber operations.

Indonesia has faced an influx of cyber threats from various sources, including organized crime groups and nation-state actors. The country's strategic importance in international trade and its advanced technological infrastructure make it a lucrative target for cyber espionage, financial theft, and disruptive attacks.

The dark web plays a crucial role in facilitating these cyber threats, providing a platform for exchanging malicious tools, stolen data, and illicit services. The anonymity offered by the dark web presents significant challenges for Indonesian cybersecurity professionals in preempting and mitigating these threats.

This report delves into the detailed analysis of the threat landscape in Indonesia, utilizing comprehensive data from both open-source and proprietary intelligence. By monitoring cyber activity and analyzing attack patterns, our team provides an in-depth overview of the threats faced by Indonesian entities. The insights presented in this report aim to empower stakeholders across public and private sectors to bolster their cybersecurity measures, mitigate risks, and enhance the resilience of Indonesia against future cyber threats.

Top Takeaways

Dark Web Dynamics

A diverse group of 89 threat actors actively targeted Indonesian enterprises, collectively posting 234 times on the dark web, predominantly trading in database sales, which underscores the criticality of data security measures.

Eyes On Information Industry

The Information industry, making up 12.74% of dark web activities, stood out as the primary industry targeted by threat actors worldwide, highlighting its strategic importance and vulnerability to digital threats.

Ransomware Resurgence

Indonesia grappled with 130 unique ransomware incidents throughout the year, with 24 attacks pinpointing the country as the primary target, revealing a focused aggression by threat actors.

Notorious Ransomware Syndicates

Prominent ransomware groups, including LockBit 3.0, ALPHV Blackcat and Play, specifically targeted Indonesia, signifying the high stakes and sophistication of the country's cyber threat landscape.

Top Takeaways

Stealer Logs

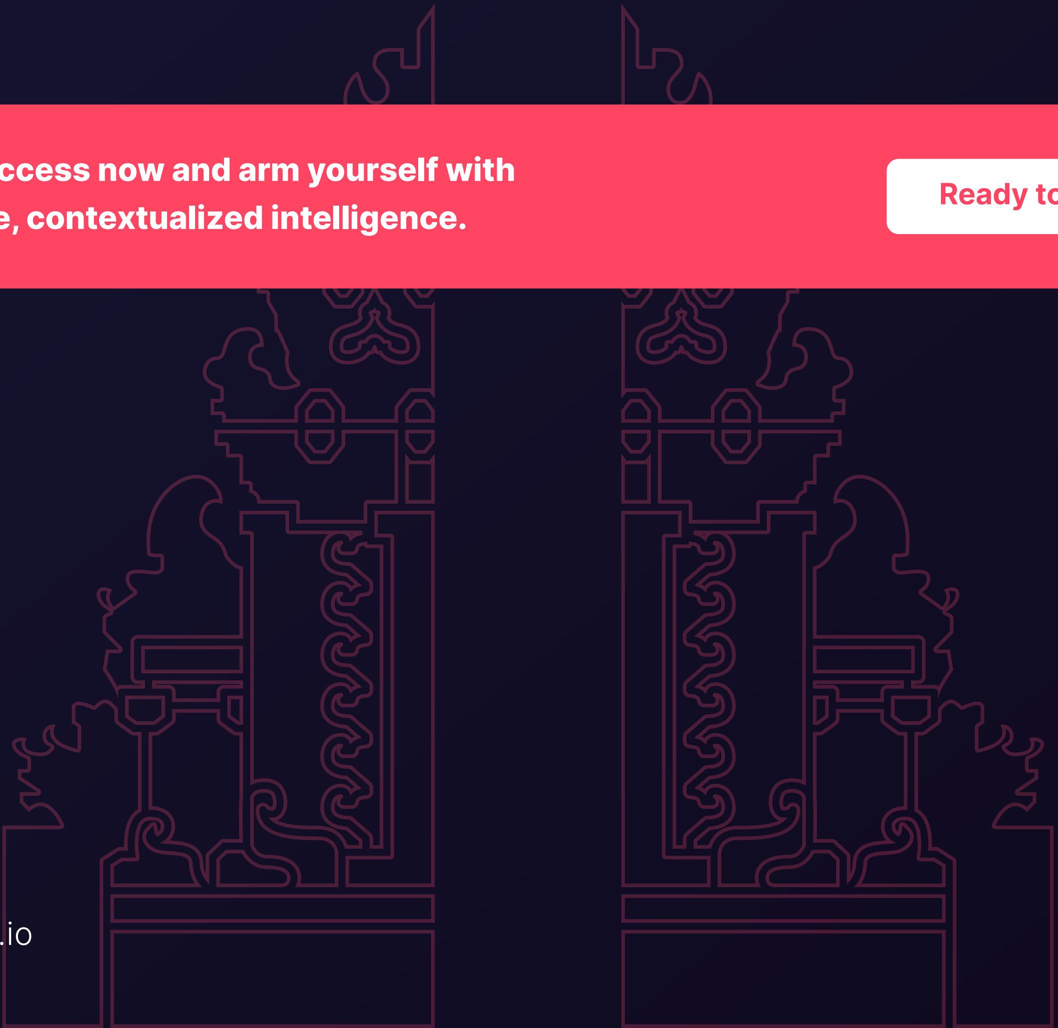
The widespread use of Stealer Logs by threat actors led to significant breaches, compromising critical data for thousands of individuals across Indonesia.

Phishing in the Digital Economy

Indonesia faced 4,046 phishing attacks, with a marked emphasis on the Information Services industry, underscoring the increasing cyber risks in this sector that is critical for data management and digital communication.

Unprecedented DDoS Attacks

Indonesia experienced a landmark DDoS attack involving 17 vectors and achieving a maximum bandwidth of 693.00 Gbps amidst a total of 43,879 DDoS incidents, illustrating the intense and escalating cyber assault landscape.



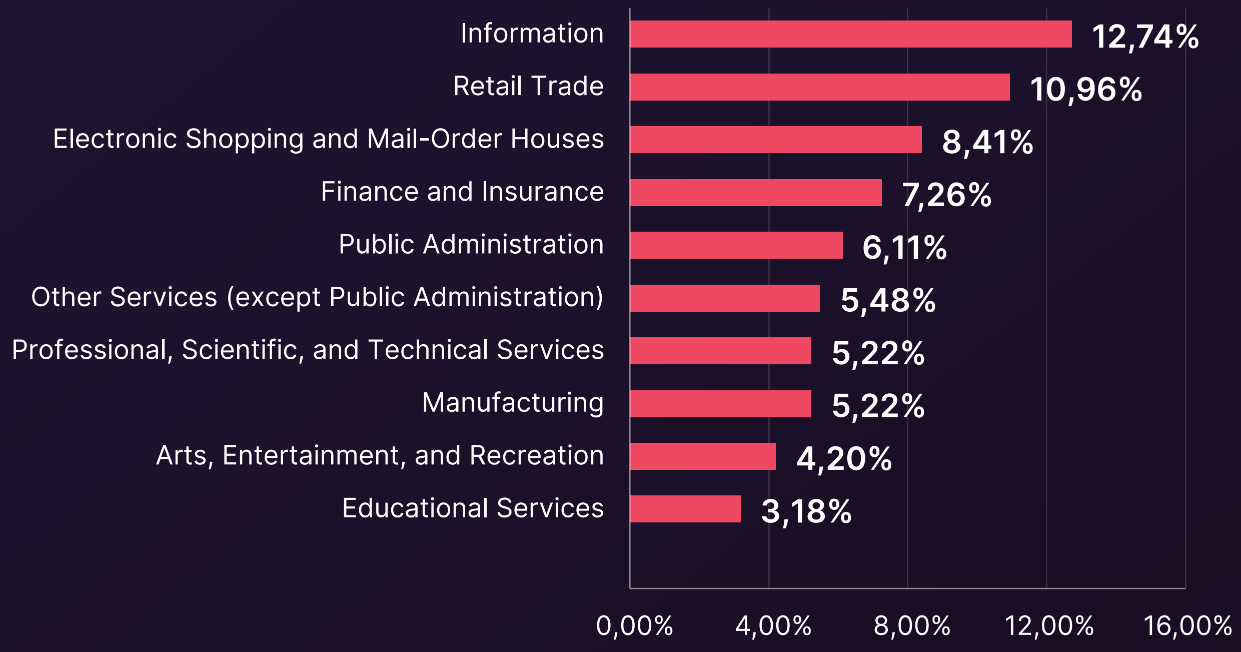
Technical Details

Dark Web Threats Targeting Indonesia

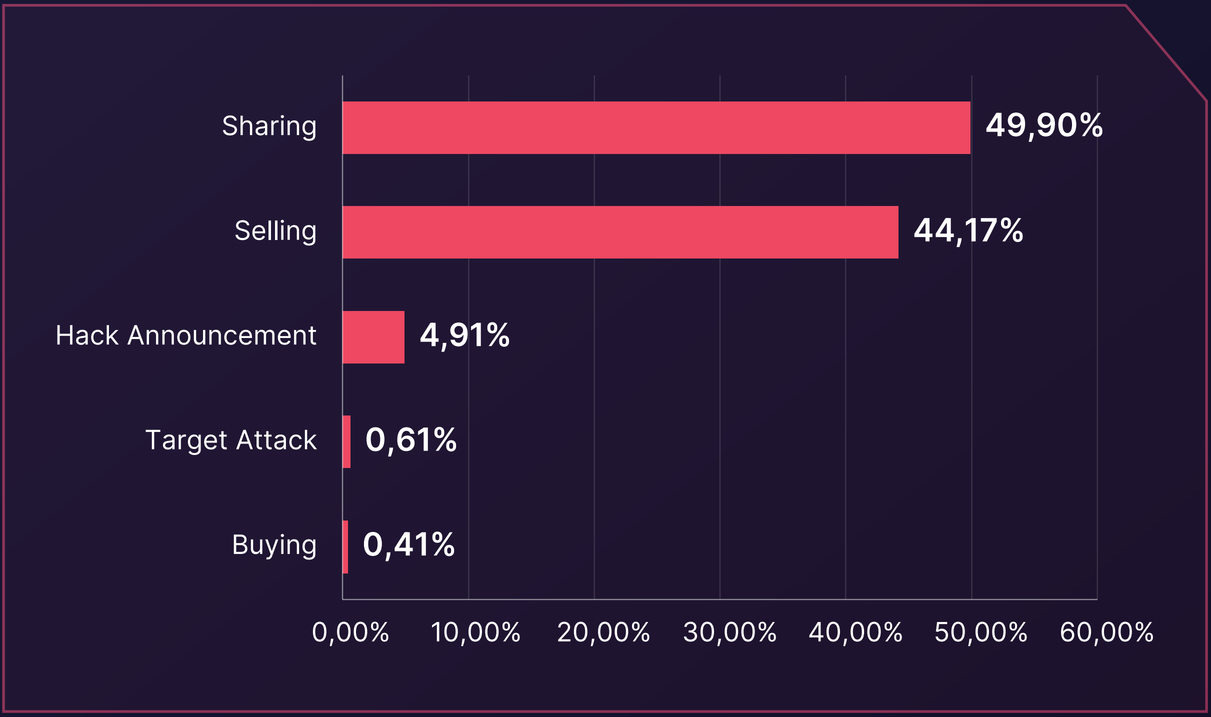
Over the preceding year, SOCRadar's Dark Web Analysts diligently monitored activities within the dark web, identifying notable trends and establishing connections between Indonesian enterprises and covert threat actors. Throughout 2023 and 2024 H1, Indonesian entities encountered a continuous barrage of cyber threats, with various actors attempting to exploit successful intrusions by trading or leveraging their gains in dark web forums.

During this period, SOCRadar observed 234 dark web forum posts linked to 89 distinct threat actors. Information emerged as the most prominently affected industry among the targeted industries, representing 12.74% of the identified cyber threats during this period. Following closely behind, the Retail Trade and Electronic Shopping industries accounted for 10.96% and 8.41%, respectively.

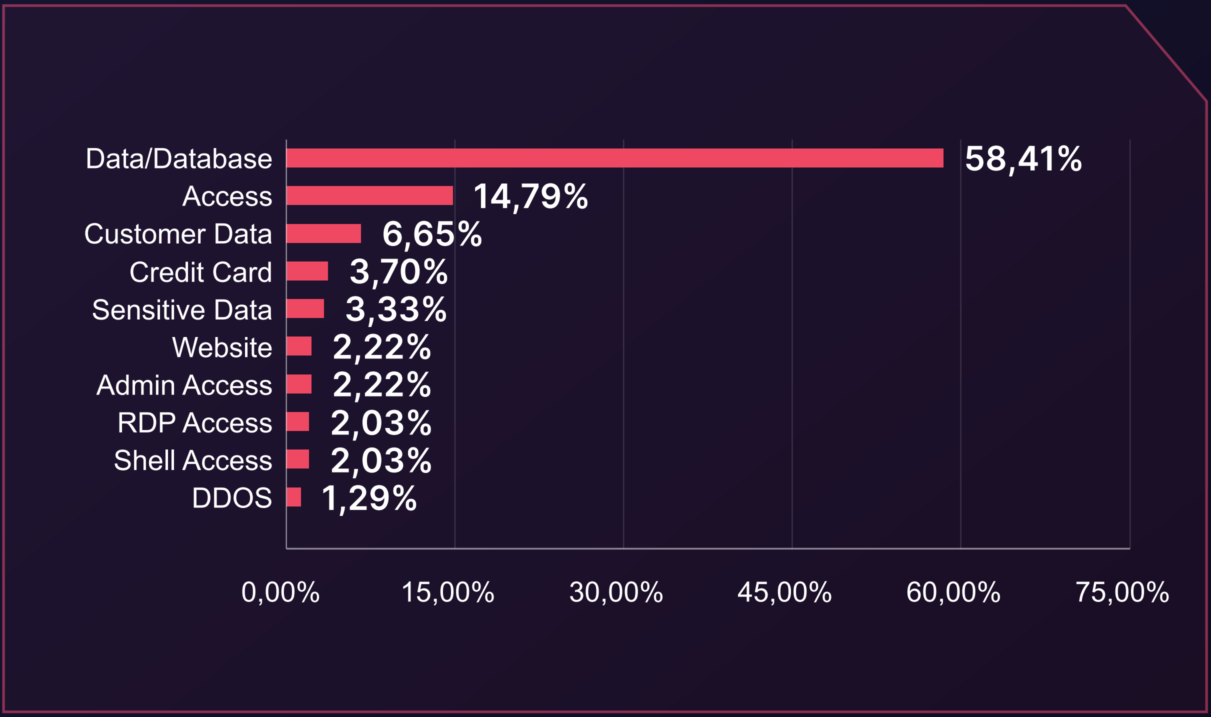
Industry Distribution of Dark Web Threats



Distribution of Dark Web Threats by Post Type



Distribution of Dark Web Threats by Threat Type



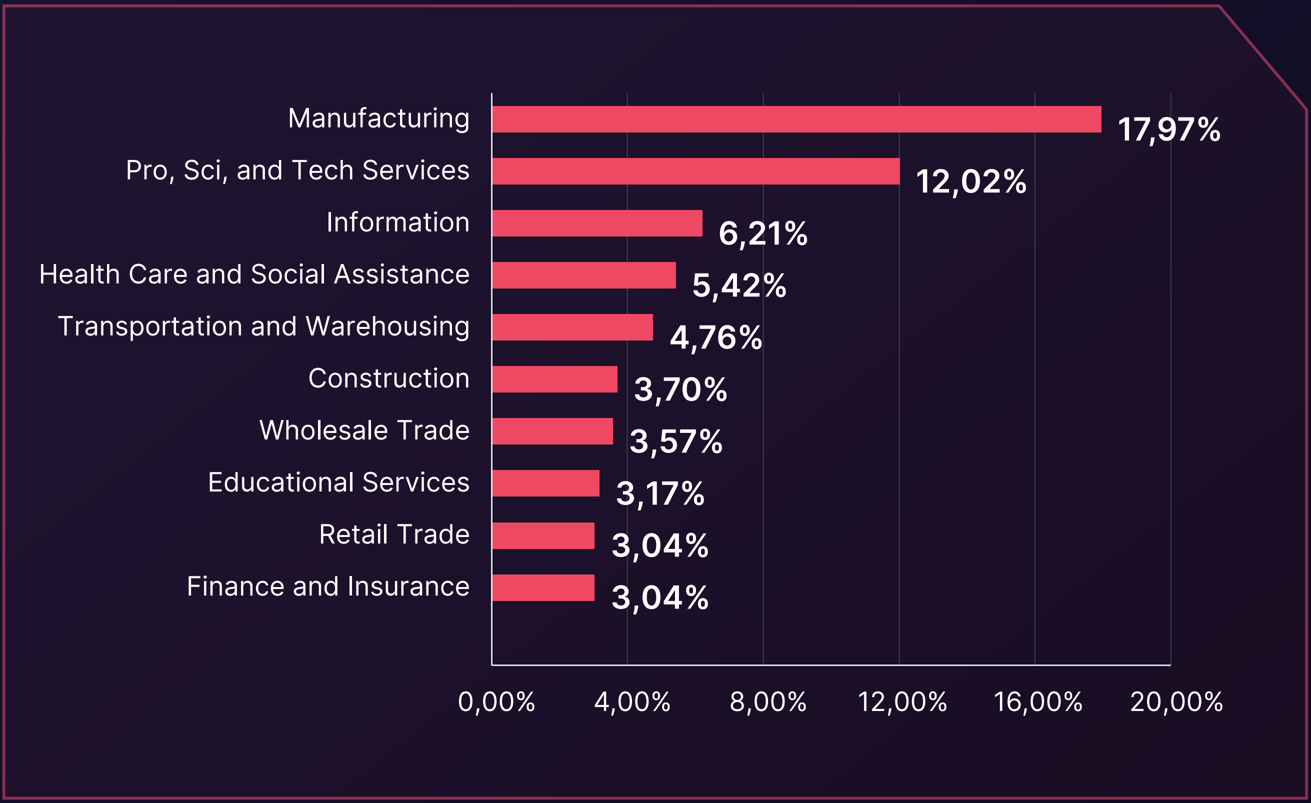
Ransomware Attacks Targeting Indonesia

Ransomware attacks represent significant threats to organizations, often resulting in dire consequences such as extensive data loss and the exposure of sensitive information. SOCRadar's surveillance has identified 130 instances of ransomware victim notifications attributable to various ransomware threat actors and/or groups.

Of the 130 ransomware attacks referenced, Indonesia emerges as the primary target in 24 cases, with the nation also featuring among the most affected countries in the remaining 106 global incidents.

Manufacturing emerges as the most prominently affected sector among the targeted industries, representing 17.97% of the identified ransomware attacks during this period. Following this, the Professional, Scientific, and Technical Services industry accounted for 12.02% of the attacks, while the Information industry experienced 6.21% of the ransomware incidents.

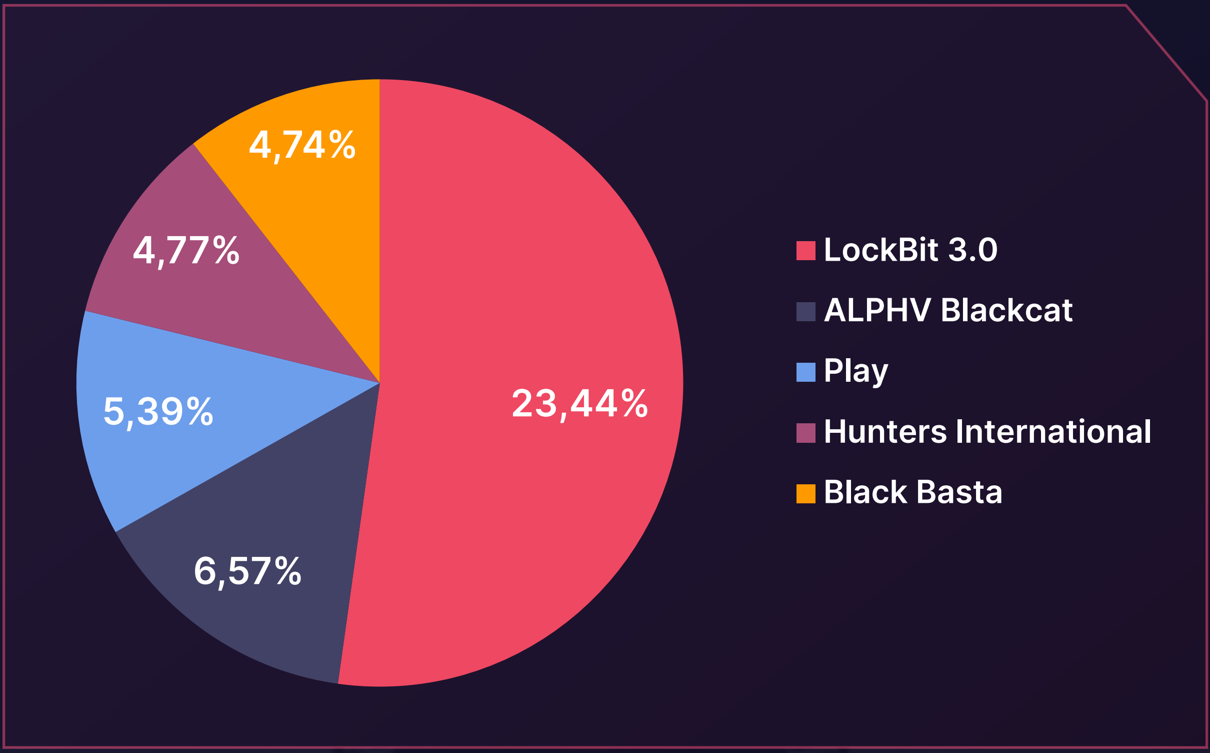
Distribution of Ransomware Attacks by Industry



Top Ransomware Groups Targeting Indonesia

When examining the top ransomware groups targeting Indonesia, **LockBit 3.0** emerges as the most prolific threat, accounting for 23.44% of the attacks. Following closely, **ALPHV Blackcat** represents 6.57% of the ransomware incidents, while **Play** and **Hunters International** account for 5.39% and 4.77%, respectively. Following closely behind, **Black Basta** accounted for 4.74% of the ransomware attacks. The remaining 55.18% is attributed to various other ransomware groups.

Top Ransomware Groups Targeting Targeting Indonesia



Top Threat Actors Targeting Indonesian Organizations

Lockbit 3.0 Ransomware Group

LockBit

Country of Origin: Russia

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Europe, Thailand, Taiwan
Target Sectors:	Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services
Attack Type:	Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Remote Desktop Protocol:	T1021.001
Data Encrypted for Impact:	T1486

LockBit 3.0, a successor to LockBit and LockBit 2.0, operates as a Ransomware-as-a-Service (RaaS) group. Since January 2020, LockBit has shifted to an affiliate-based model, employing various tactics to target businesses and critical infrastructure organizations. They are known for employing strategies like double extortion and initial access broker affiliates, as well as recruiting insiders and hosting hacker recruitment contests. With over 1,500 victim announcements on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's shutdown. As of the first quarter of 2023, they remain the most prolific group, boasting over 300 announced victims.

For more detailed information about the Lockbit 3.0 Ransomware Group, you can visit our blog post.

ALPHV Blackcat Ransomware Group

BlackCat Ransomware

Country of Origin: Russia

BlackCat, or ALPHV, is a ransomware group known for being the pioneer to use Rust and the group first announced its RaaS affiliate program in a dark web forum in December 2021.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Germany, Australia, France, Italy, Spain
Target Sectors:	Professional Services, Manufacturing, Healthcare, Finance, Information Technology
Attack Type:	Spearphishing, Stolen Credentials, RaaS, Ransomware, Triple-Extortion

-TTPs-

User Execution: Malicious File:	T1204.002
Defacement:	T1491
Data Encrypted for Impact:	T1486

BlackCat, or ALPHV, is a ransomware group known for being the first to use Rust -a cross-platform language programming language that allows for easy malware customization for different operating systems, such as Windows and Linux- successfully. The group has been able to evade detection and successfully encrypt their victims' files by using Rust, which allows them to target multiple operating systems and bypass security controls that are not designed to analyze malware written in Rust.

For more detailed information about the ALPHV BlackCat Ransomware Group, you can visit our blog post.

Play Ransomware Group

Play Ransomware

Country of Origin: Unknown

Play Ransomware (PlayCrypt) is a ransomware group first observed in June 2022. The group commonly targets organizations based in Latin America but mainly focuses on Brazil.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	Latin America, India, Hungary, Spain, Netherlands, United States
Target Sectors:	Manufacturing, Education, Real Estate, Technology, Transportation, Healthcare
Attack Type:	Compromised Valid Accounts, LOLBins, Ransomware, Data Exfiltration

-TTPs-

Process Injection:	T1055
Input Capture:	T1068
Proxy:	T1090

Play Ransomware is a ransomware group notorious for their advanced tactics and the use of intermittent encryption, a method that allows them to partially encrypt files and evade detection. Initially observed in 2022, they target exposed RDP servers and exploit vulnerabilities in FortiOS to gain network access. Their operations include double extortion, where they threaten to leak stolen data if ransoms are not paid. The group has targeted various sectors, including IT companies, banks, and governmental organizations.

For more detailed information about the Play Ransomware Group, you can visit our blog post.

Are you curious about which threat actors are targeting your industry?

Try SOCRadar's Operational Intelligence

Stealer Log Statistics
Top Domains in Indonesia

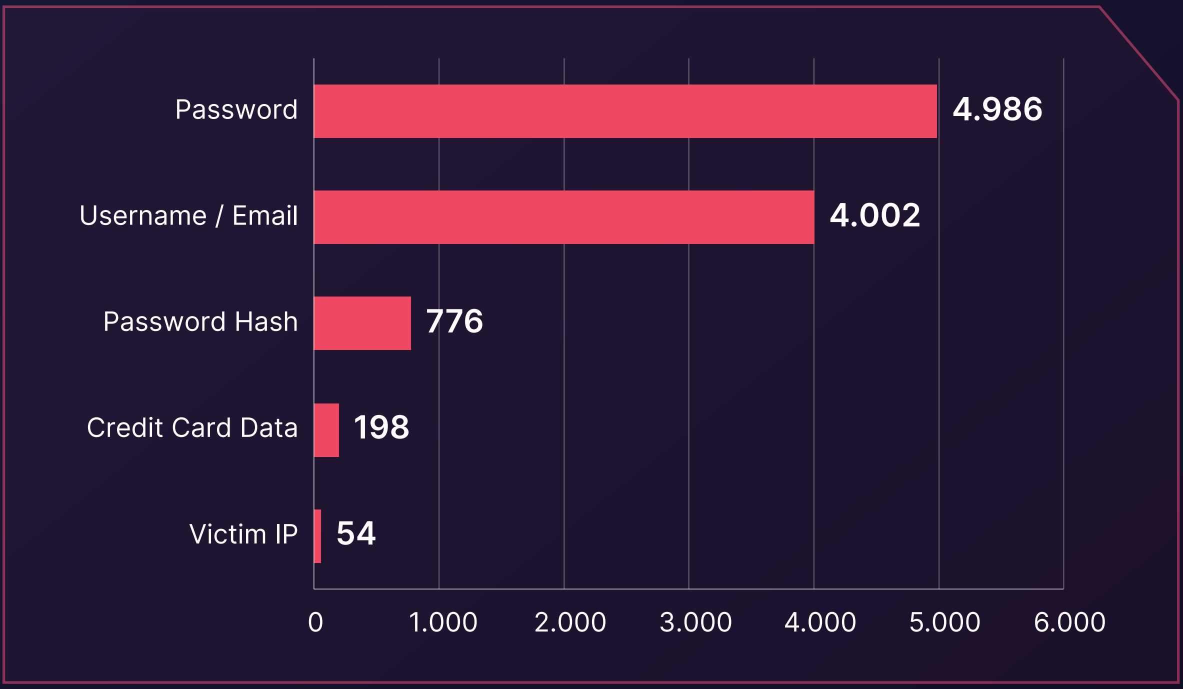
Throughout 2023 and 2024 H1, thousands of users' user IDs/email addresses, passwords, credit card data, password hashes, and victim IP address information were compromised via Stealer Logs from the computers of users who have accounts or access to some of the highest traffic domains in the Indonesia.

The table below lists the domains associated with Indonesia having the highest traffic.

kompas.com
detik.com
bolasport.com
tokopedia.com
liputan6.com
otakudesu.cloud
kemdikbud.go.id
lazada.co.id
samehadaku.email
shopee.co.id

The graph below showcases the distribution of the compromised user data obtained through Stealer Logs across the highest-traffic domains associated with Indonesia.

Stealer Logs - Compromised Data



The data reveals significant dissemination of compromised information, including **4,986** passwords, **4,002** usernames/emails, **776** password hashes, **198** credit card data entries, and **54** compromised victim IPs, each representing significant instances of compromise.

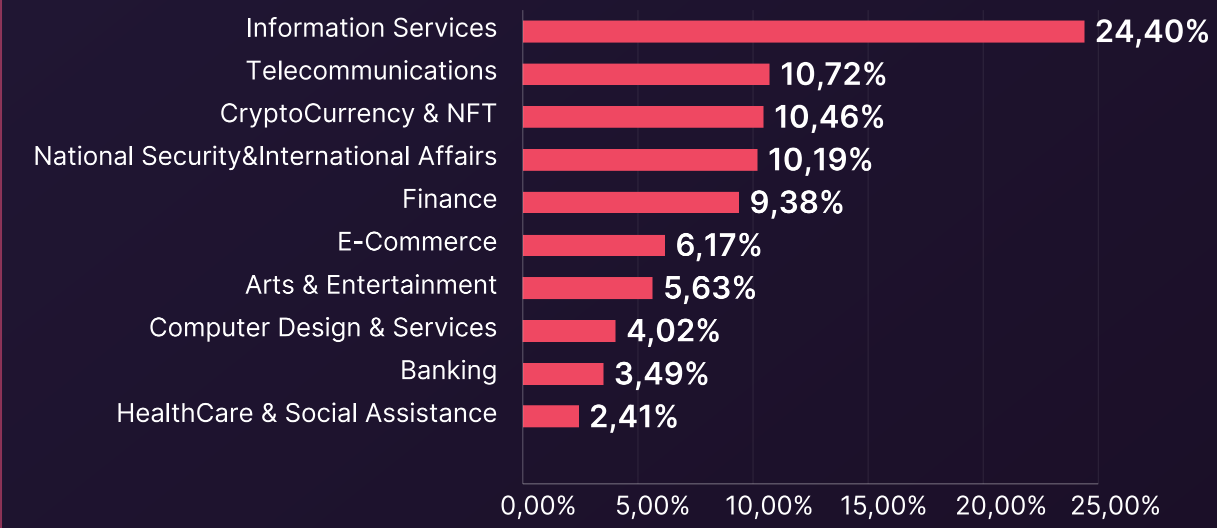
These discoveries emphasize the gravity of data compromise occurrences impacting users in the digital sphere of Indonesia emphasizing the urgent necessity for robust cybersecurity protocols to efficiently alleviate such risks.

Phishing Threats Targeting Indonesia

Phishing is an effective method to initially breach an organization's infrastructure by deceiving individuals into divulging sensitive credentials on fraudulent websites.

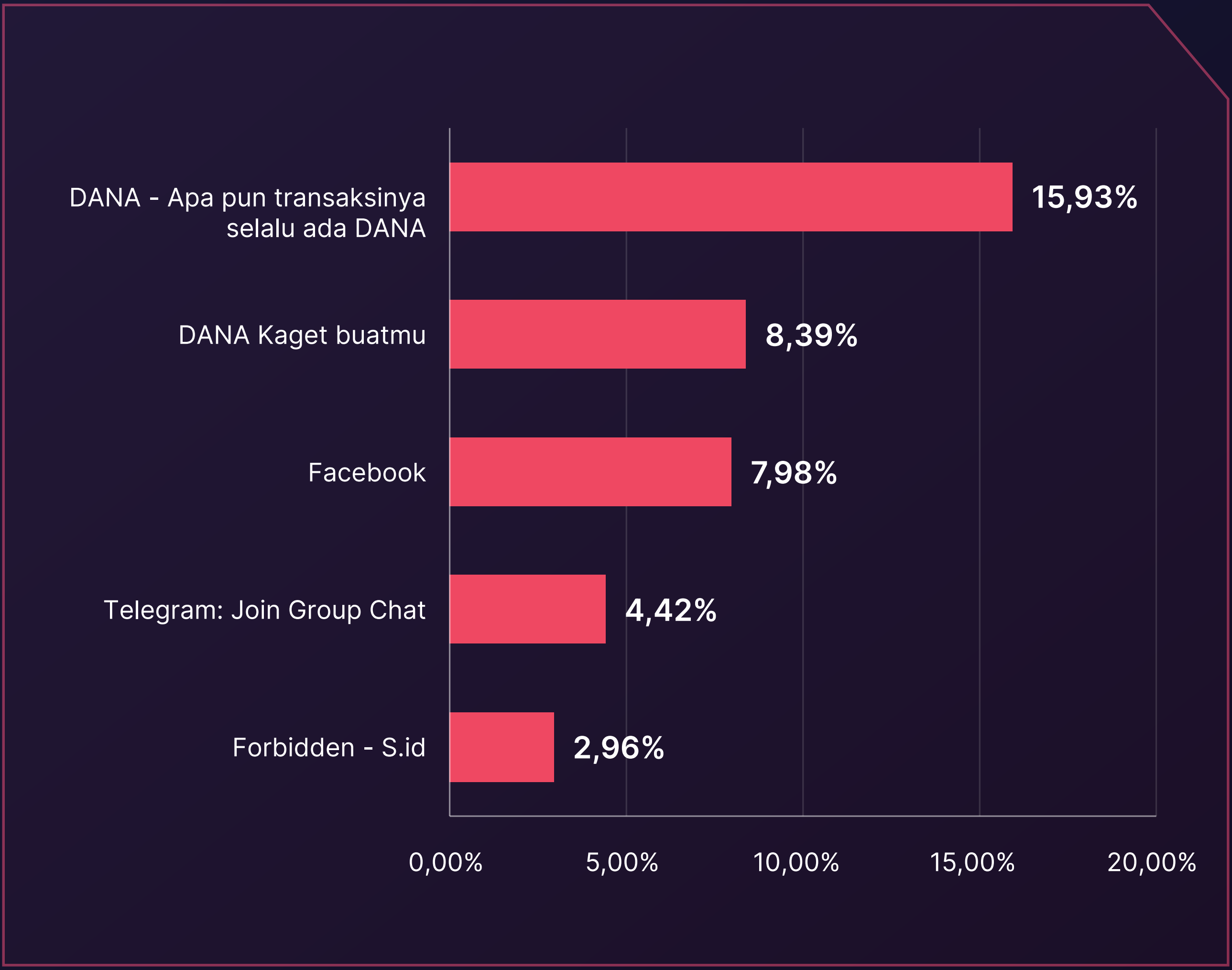
Typically, phishing attacks are coupled with social engineering tactics to acquire such credentials. Over the past year, Indonesian enterprises have encountered **4,046 distinct instances of phishing attacks**, primarily targeting the **Information Services** industry.

Phishing Attacks - Distribution by Industry



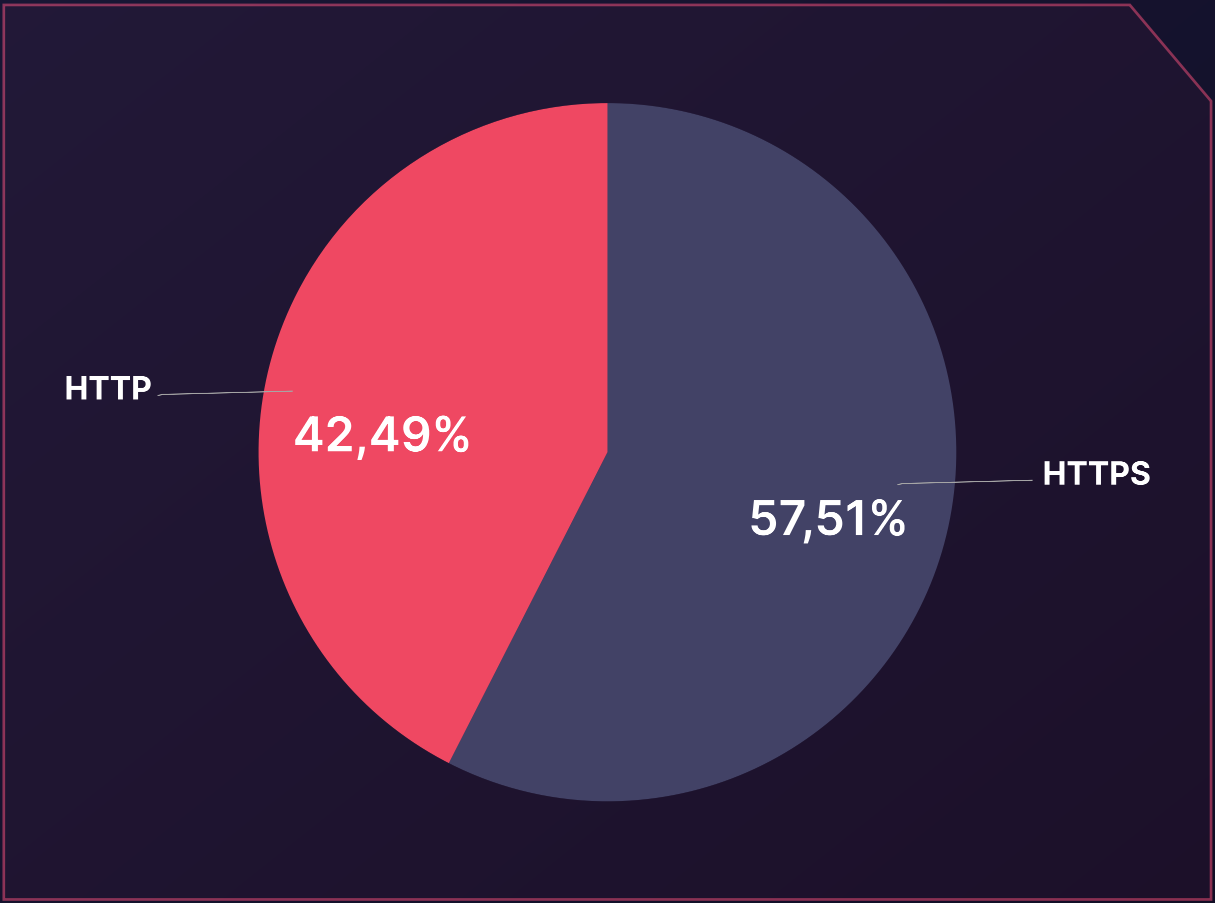
The graph below illustrates the distribution of Page Titles used by threat actors for phishing attacks. Notably, the data reveals a predominant usage of the **DANA - Apa pun transaksinya selalu ada DANA** (DANA - Whatever the transaction, DANA is always there.) page title.

Phishing Attacks - Distribution by Phishing Page Title



When closely examining the SSL/TLS protocols of domains prepared for phishing attacks by threat actors, we observe an increasing trend in the usage of HTTPS compared to the past.

Phishing Attacks- Distribution by SSL/TLS Protocol



DDoS Attack Statistics

Indonesia experienced a dynamic DDoS threat landscape marked by considerable cyber activity in 2023.

- The most extensive multivector DDoS attack recorded encompassed **17 vectors**, featuring prevalent techniques such as **DNS Amplification** and **ICMP** attacks.
- The maximum bandwidth observed during a DDoS attack reached **693.00 Gbps** (peak aggregate bandwidth in one minute), indicating the severe capacity of these cyber threats.
- The highest recorded throughput during these incidents was **79.00 Mpps** (peak aggregate throughput in one minute), underscoring the intense rate at which data packets were sent.
- On average, each DDoS attack lasted for **54 minutes**, indicating a strategy focused on short but effective service disruptions.
- A total of **43,879** DDoS attacks were recorded throughout the year, illustrating a high frequency of cyber-attacks aimed at targets in Indonesia.

Attack Vector	Number of Attacks in 2023
TCP RST	10,083
TCP ACK	9,625
TCP SYN	7,906
ICMP	7,732
DNS Amp	7,288

The ongoing evolution of DDoS tactics underscores the importance of implementing stringent monitoring and resilient defense mechanisms to safeguard essential infrastructures and ensure uninterrupted service delivery. Enhance your DDoS defense with SOCRadar's DoS Resilience module, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks.

Lessons Learned: Key Insights and Strategic Recommendations

Several critical lessons and recommendations have emerged after examining the cybersecurity threats facing Indonesian organizations. These insights, enhanced by SOCRadar's capabilities, provide a strategic roadmap to bolster cyber resilience and safeguard operational integrity. Here are the key takeaways from our analysis:

Vigilance in an Evolving Cyber Threat Landscape

The dynamic nature of the cyber threat landscape, marked by an increase in dark web activities and ransomware incidents related to Indonesia, demands constant vigilance. Organizations must keep pace with these changes by adapting their security strategies. By adopting a proactive approach like SOCRadar’s Extended Threat Intelligence solution, organizations can gain real-time insights into emerging threats, positioning them to counteract cyber adversaries proactively.

Implementation of Multi-layered Security Measures

Given the broad spectrum of industries targeted by cyber threats, it is essential to implement multi-layered security defenses. SOCRadar supports these efforts with its proactive Threat Intelligence and monitoring services, ensuring comprehensive protection.

Consistent Guard Against Ransomware

The persistent threat posed by ransomware underscores the need for strong defensive and responsive strategies. SOCRadar’s Attack Surface Management capabilities are crucial for businesses to identify potential ransomware threats and to formulate effective countermeasures.

Continuous Employee Education and Training

The ongoing risk of phishing attacks makes continuous education and training for employees imperative. Enhancing their ability to recognize phishing tactics and detection methods is vital. SOCRadar's Digital Risk Protection suite provides comprehensive VIP Protection and Brand Protection services, effectively addressing the challenges posed by identity-based attacks.

Robust Defenses Against Stealer Malware

With France frequently targeted by Stealer malware, strengthening defenses against this malicious software is crucial. SOCRadar’s Identity & Access Intelligence module is vital in detecting and mitigating data breach threats, enhancing an organization’s security framework.

Strategies Against DDoS Attacks

As DDoS attacks become more complex and voluminous, organizations must prioritize the implementation of robust DDoS mitigation strategies. This involves deploying advanced DDoS protection technologies that can absorb high-volume traffic and mitigate multi-vector attack strategies effectively.

Enhance your DDoS defense with SOCRadar's DoS Resilience module, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks. Leveraging state-of-the-art AI and cloud technologies, this module provides a crucial layer of protection for global organizations.

Conclusion

Adopting a proactive and comprehensive approach to cybersecurity is crucial for Indonesian organizations. By partnering with advanced solutions like SOCRadar, they can enhance their defenses and effectively navigate the evolving cyber threat landscape.

Building a culture of risk awareness and implementing proactive mitigation strategies fortifies defenses against dynamic threats. Utilizing Cyber Threat Intelligence empowers teams to respond to immediate threats and confidently prepare for future challenges.

Collaboration among cybersecurity professionals, supported by robust CTI frameworks, is essential for safeguarding digital assets and maintaining organizational resilience against cyber threats.

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.

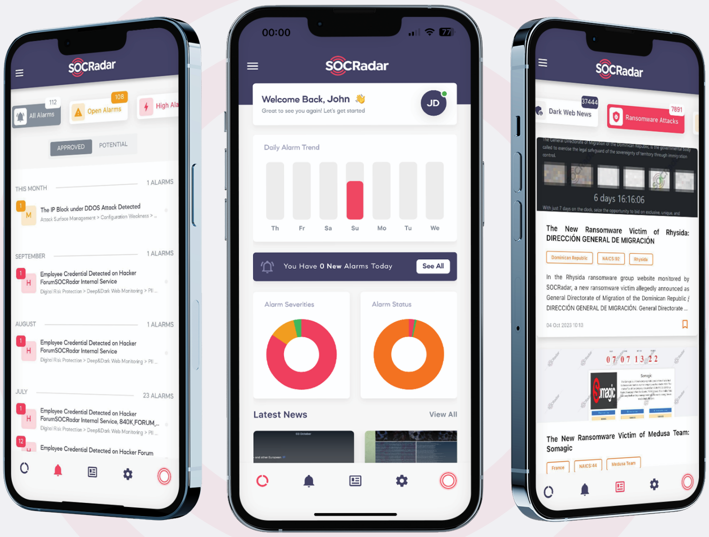
360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store



GET IT ON Google Play

Gartner Peer Insights™ 4.9/5 ★★★★★