SOCRadar®

2021

Threat Landscape Report

INDONESIA

TABLE OF CONTENTS

03 | Executive Summary & Key Findings

04 | Dark Web Threats On The Rise

05 | Major Dark Web Incidents of 2021

06 | Ransomware Threats

07 | Top Ransomware Gangs Targeting Indonesia

08 | State-Sponsored APT Activities

09 | Major APT Activities Around the World

10 | Phishing Threats

11 | The Digital Industries Commonly Targeted by Phishing Attacks

12 | Critical Asset Exposures & Vulnerabilities

13 | Credentials Leaked on the Dark Web

14 | DDoS | Risk-to-Others

EXECUTIVE SUMMARY

Indonesia is a prime target for nation-state-sponsored actors as well as financially motivated ransomware gangs in 2021. This report provides organizations with an understanding of evolving cyber threats relevant to their geographical operating locations to enable security leaders to make better decisions. The intelligence provided in SOCRadar Threat Landscape Report can be used to plan organization-wide security programs, make investment decisions, and define cybersecurity requirements.

For this report, SOCRadar characterizes the threat landscape by leveraging the activity of threat actors, malware campaigns, new critical vulnerabilities and exploits, data collected from open threat sharing platforms, and SOCRadar's comprehensive data monitoring, collection, classification, and analysis capabilities. SOCRadar's unique perspective on understanding threat actors and their TTPs comes from combining information gathered from the SOCRadar CTIA Team's deep/dark web threat research, HUMINT observations, cybersecurity vendor blogs, and social media trends.

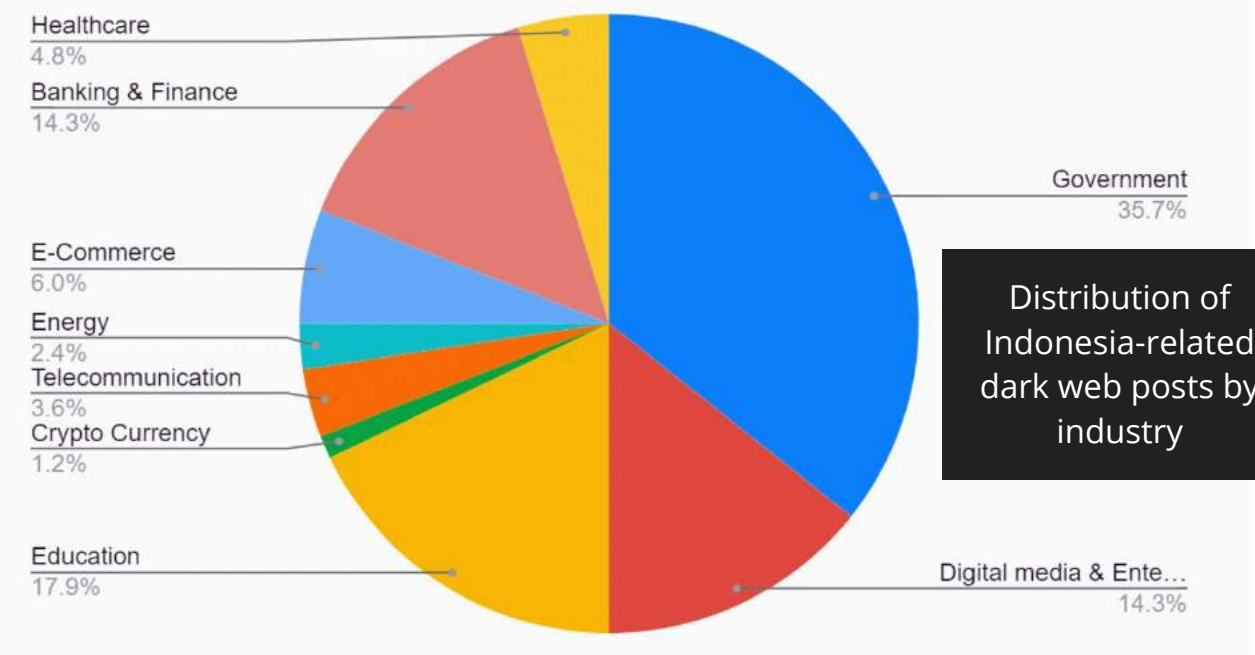
KEY FINDINDS

- **Of the more than 60 posts seen regarding Indonesian assets in the last three months, 10% were ransomware threats, 15% were unauthorized network access sales, and more than 50% were database sharing.**
- **24 APT groups have targeted leading organizations in the energy, telecommunications, high-tech, and finance industries.**
- **Indonesian companies and public institutions are observed to attract the attention of ransomware groups such as REvil, Conti, Avaddon, and LockBit.**
- **Nearly 20,000 phishing attacks targeting Indonesia have been detected since the start of 2021, a 38% increase from last year.**
- **More than 1 billion exposed credentials were identified by SOCRadar, most of which depend on plaintext passwords in Indonesia.**

Dark Web Threats On The Rise

For threat actors, the dark web underground ecosystem has become a #1 communication channel and a global marketplace with various hacking tools available for purchase.

Dark web vendors have allegedly orchestrated mass data breaches. Over the last three months, the SOCRadar CTIA Team detected more than 60 posts related to Indonesian entities.



Distribution of Indonesia-related dark web posts by industry

10% of these posts were ransomware threats, 15% were unauthorized network access sales, and more than 50% were database sharing. These campaigns have exposed an extensive dataset belonging to different companies from various sectors, including local government, education, law enforcement, agriculture.

60
Threat posts over the last 3 months

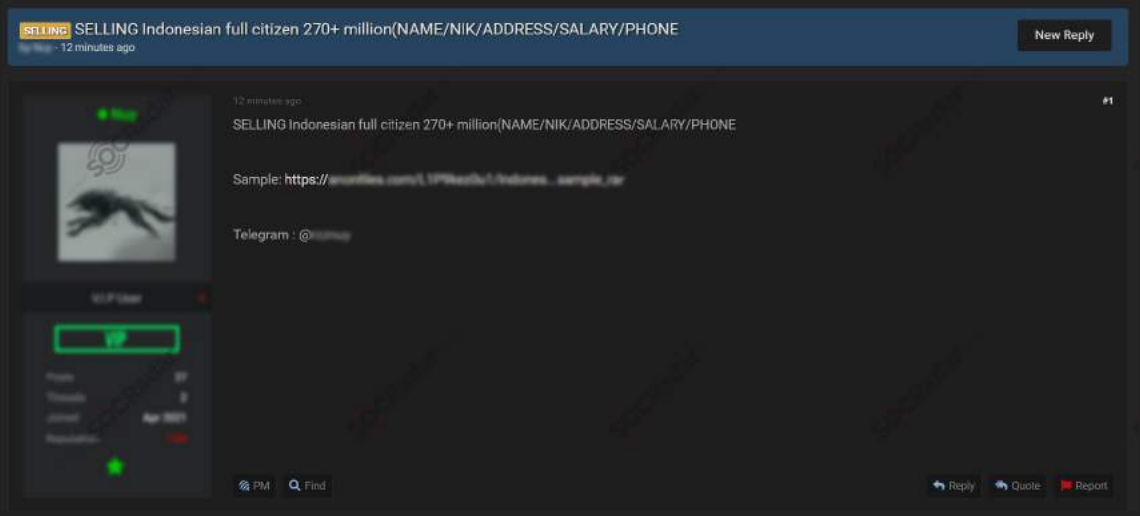
25+
Dark web threat actors / aliases

Government
The most targeted sector

Leaked database
The most common threat category

Major Dark Web Incidents of 2021

PII of Over 270 Million Indonesian Citizens Leaked

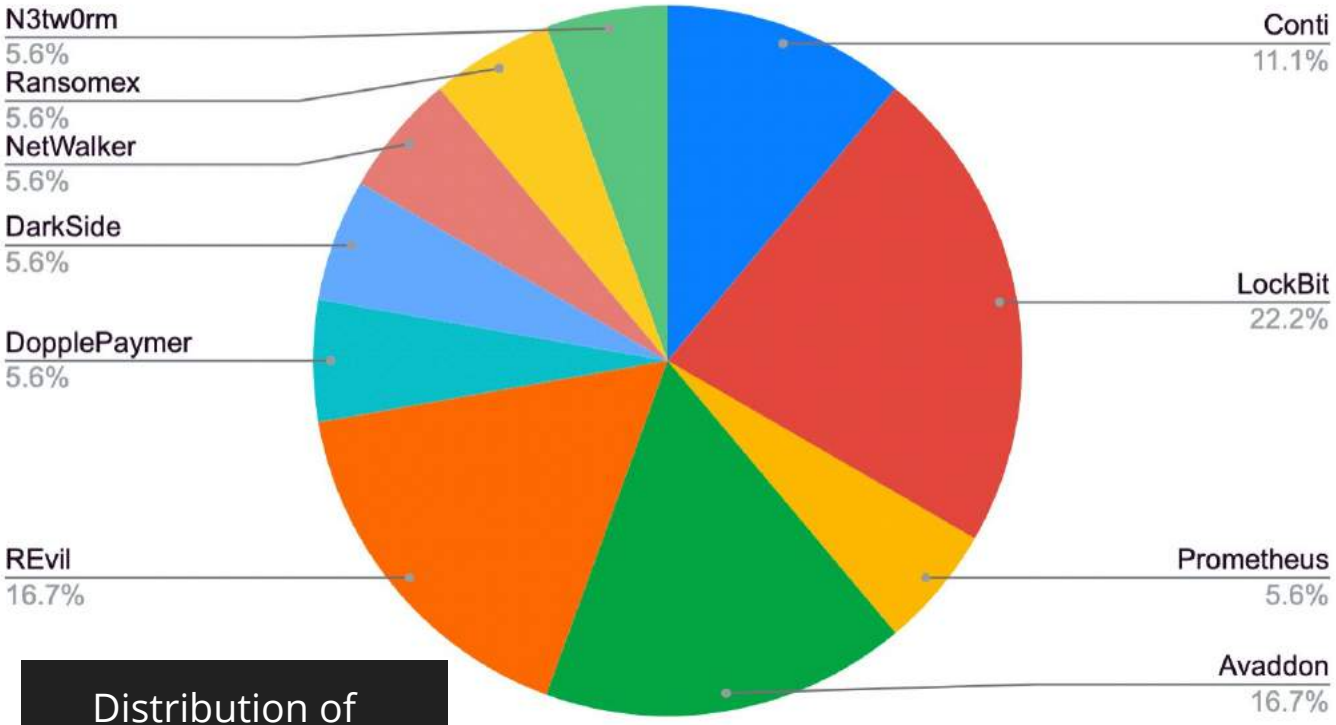


On July 1, 2021, on a dark web forum monitored by SOCRadar, a vendor attempted to sell databases allegedly including Indonesian citizens. It is not clear how the vendor obtained the databases, but the source might be from government surveys. According to the dark web post, leaked information comprises First Name, Last Name, Date of Birth, Mobile Phone Number, National Identity Numbers, and salaries for some individuals.

On July 28, 2021, a dark web vendor offered to sell a database assertedly belonging to an Insurance company Indonesia on a dark web forum tracked by SOCRadar. The Jakarta-based victim firm has a revenue of $335 billion with more than 900 employees. A vendor who claimed to sell a collection of 460,000 documents for seven thousand dollars implements that the database was gathered from the customer information belonging to over two million clients.

Ransomware Threats

Ransomware attacks today go beyond data hijacking. Ransomware gangs now leak victim organizations' confidential data, which calls a Double Extortion Tactic. These cybercriminals threaten to release the victims' data by using pressure tactics, further increasing victims' need to protect their precious reputations.



Distribution of ransomware gang activities.
Source: SOCRadar **DarkMirror**

Looking at the information provided by SOCRadar DarkMirror, Indonesian companies and public agencies are observed to attract the attention of ransomware groups such as REvil, Conti, Avaddon, and LockBit.

Top Ransomware Gangs Targeting Indonesia

LockBit

- Ransomware-as-a-service (RaaS) operator.
- It's one of the best designed lockers in terms of encryption speed and overall functionality.
- The long list of victims has lately included the consultancy firm - Accenture.

REvil

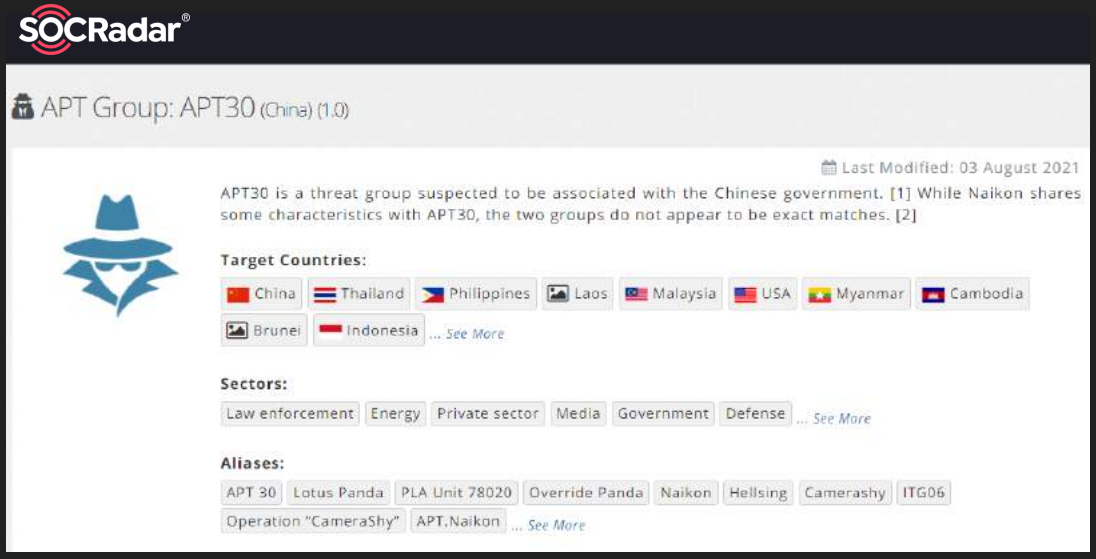
- Ransomware-as-a-service (RaaS) operator, also called Sodinokibi.
- The group has pulled off several high-profile attacks on enterprises like the Apple supplier Quanta Computer Inc., meat supplier JBS, tech giant Acer and Kaseya.
- The data leak site of REvil is called Happy Blog.

Avaddon

- First observed in February 2020.
- Recent victims include the American company American Bank Systems (ABS), and more recently the insurer Group AXA.
- Avaddon is usually distributed via phishing campaigns through e-mails containing obfuscated JPEG or ZIP attachments.

State-Sponsored APT Activities

Advanced persistent threat (APT) actors are historically one of the biggest challenges for the region. Specific APT groups have targeted leading organizations in the energy, telecommunications, high-tech, and finance industries. To get one step ahead during the long-running territorial disputes, such as the one about the South China Sea, is believed to be the primary motivation of the state-sponsored actors.



Over the last few months, the SOCRadar CTIA team has observed multiple activities reflecting these motivations by continuously collecting data from surface, deep and dark web sources while tracking 28 APT groups that have targeted Indonesia's government, military, and private sectors.

Significant APT Groups

APT41

Last activity:
September 23, 2021

APT17

Last activity:
July 8, 2021

APT30

Last activity:
August 3, 2021

APT32

Last activity:
September 9, 2021

Major APT Activities

4 Hackers Tied to China Charged by the US

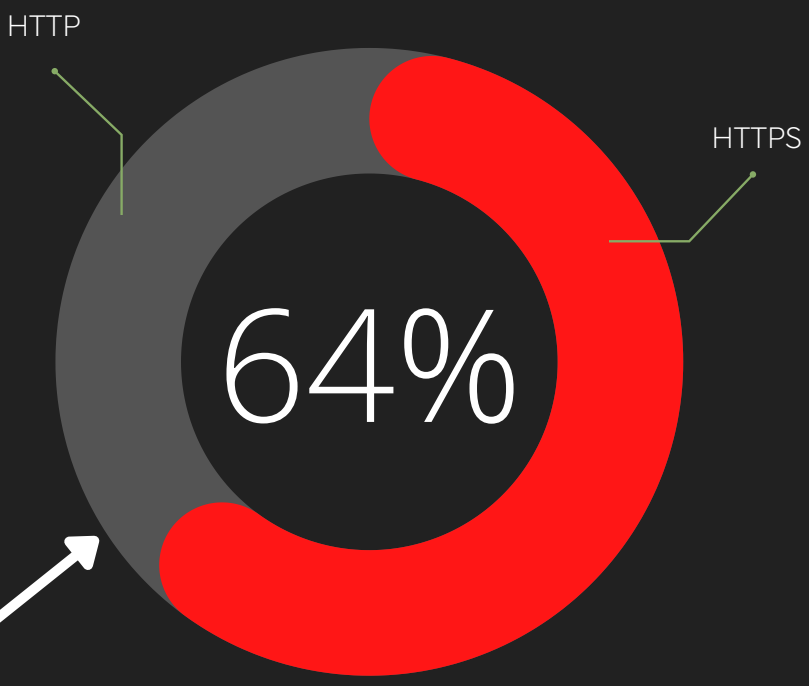
On July 19, 2021, the United States accused China of deliberately using contract hackers. According to the indictment, China targeted organizations from Indonesia and countries such as the USA, Canada, and Germany in the campaign between 2011-2018. The DOJ said that four Chinese nationals serving for the Department of State Security (MSS) orchestrated the campaign to seize confidential business information, trade secrets, and private technologies used for autonomous vehicles, specialty chemical formulas, commercial aircraft servicing, and proprietary software genetic-sequencing technology and data, and foreign information. Further, victims from aviation, defense, education, government, health care, pharmaceutical, and maritime sectors were involved in the attacks, aligning with APT17 and APT41 - well-known China-backed hacking groups.

Alleged Cyber Espionage Campaign Targeting BIN

On September 10th, the cybersecurity news portal, The Record, claimed that a threat actor group from China attacked computers belonging to the intelligence service of Indonesia - the Badan Intelijen Negara (BIN). According to The Record, the Chinese state-sponsored threat actors Mustang Panda hacked the primary intelligence agency and nine other agencies within the Indonesian government. After being informed, the victim intelligence agency examined the suspected breach with other organizations and associated stakeholders. However, they rejected the claim, and "our server is safe, and under control, there is no indication that suspected Chinese hackers hacked it," said a spokesman for the agency. The representative also stated that their computers are an attractive target for threat actors, and the agency conducts routine controls and maintenance on its systems.

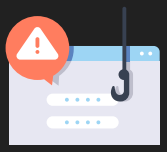
Phishing Threats

Email phishing remains the top ransomware attack vector. The typical tactic is to deliver malicious macro-enabled Office documents attached to the email. Combined with business email compromise (BEC) scams and social engineering methods, the effects can increase dramatically.



Attackers are increasingly using https to lure their victims into clicking malicious links

SOCRadar has detected almost 20,000 phishing attacks targeting Indonesia since the beginning of 2021, showing a 38% increase comparing to the last year. SOCRadar CTIA team is seeing a phishing trend targeting fast-growing digital industries, including e-commerce, FinTech, cryptocurrency exchange, and cloud/SaaS.



19,919
Total phishing attacks detected over the last 1 year

Microsoft
Top SaaS phishing scheme for credential harvesting

Most used TLDs

.tk | .id | .com

The Digital Industries Commonly Targeted by Phishing Attacks

Comman Platforms

Social Media /IM

Cloud / Webmail

E-commerce

Payment / Crypto

Attackers Objective

To distribute malware and steal the social media login credentials of individuals.

To steal the corporate email credentials to gain an initial foothold to the victim's communication channels.

To steal the credentials of individuals/companies and other personal info (PII) for using in fraudulent e-shopping activities

To steal the login accounts of individuals/businesses for financial gain or using them in illegal transactions.

Critical Asset Exposures & Vulnerabilities

When SOC analysts, vulnerability management teams, and security leaders have limited time and budget, prioritizing vulnerabilities to reduce the public attack surface becomes paramount. Following is a high-level statistical view of the critical ports and vulnerabilities on the internet-facing infrastructure and technologies.

Ransomware gangs heavily exploit these as they are exposed, but we can still observe them unpatched or exposed to any remote actors. It is highly recommended to check the technologies listed so far for unpatched, critical, exploited vulnerabilities. (Source: Shodan)

Vulnerable Hosts | Code: ID

The number of highly-exploited vulnerabilities in Indonesia is given below.

318	Microsoft Exchange Server Unauthenticated Remote Code Execution Vulnerability	CVE-2021-31206 #ProxyShell	CVSS: 9.2
59	VMware vCenter Server Unauthenticated Remote Code Execution Vulnerability	CVE-2021-21972 #vSphere	CVSS: 9.8
38	Palo Alto Networks SSLVPN PreAuth Remote Code Execution Vulnerability	CVE-2019-1579 #GlobalProtect	CVSS: 9.8
19	Citrix ADC / Gateway Remote Code Execution Vulnerability	CVE-2019-19781 #NetScaler	CVSS: 9.8

Other Critical Findings

16,271
Exim Server v4.92

13,782
Open RDP 3389

2093
CVE-2014-0160
#Heartbleed

531
CVE-2019-0708
#BlueKeep

Credentials Leaked on the Dark Web

Using stolen credentials is one of the most common initial access techniques leveraged by your adversaries. C-level credentials are significantly more helpful for BEC attackers. Last year, SOCRadar detected more than 1 billion exposed credentials by analyzing the breach datasets shared on the deep and dark web forums, most of which are tied to plain-text passwords.

Password reuse is continuing to be a pain for all security professionals. When it merges with the lack of MFA mechanisms, it becomes a bigger problem. Ransomware and APT actors continuously seek access to sensitive information, intellectual property, confidential business data through stolen credentials. Following are the statistics about Indonesia's current risk situation.

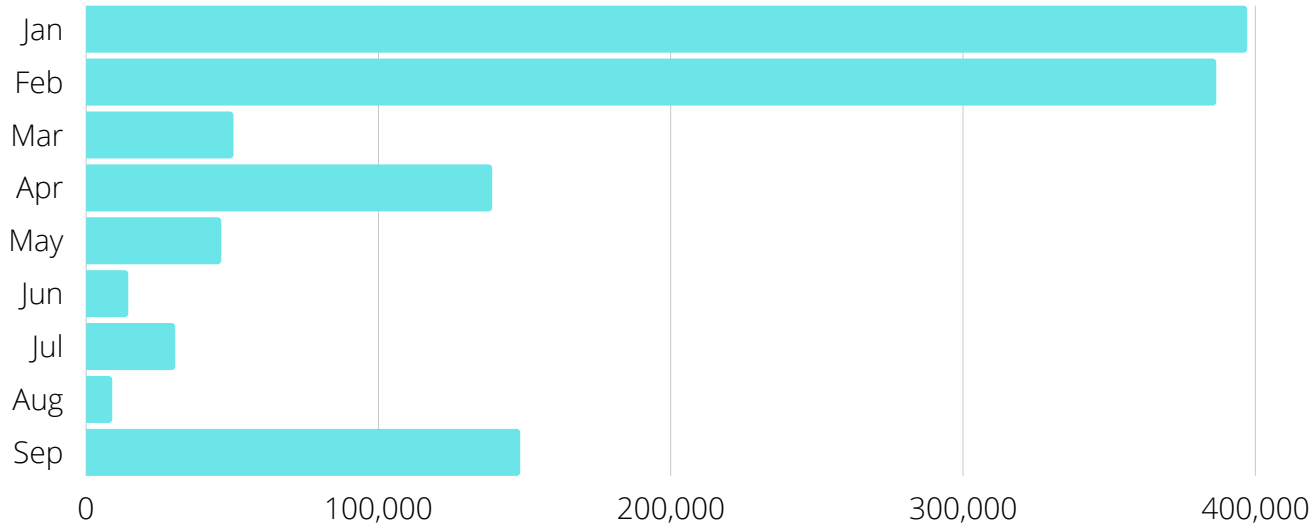


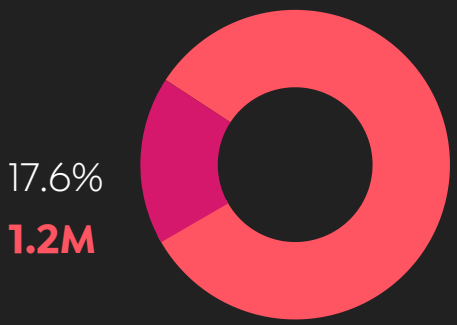
Figure 4. Month-over-month number of leaked credentials from Indonesia in 2021

6.9 Million

stolen credentials from Indonesia

24748

stolen credentials from government agencies



In 2021 alone, SOCRadar analysts found 1.2 million stolen credentials from Indonesia, which added up to a total of 5.7 million credentials found before 2021.

DDoS | Risk-to-others

The global internet ecosystem is currently vulnerable and carrying high malicious traffic. Sophisticated threat actors take advantage of these weak points for amplifying disruptive DDoS attacks against businesses, resulting in financial losses and critical service disruptions.

Based on the global risk condition dataset provided by Cyber Green Initiative, Indonesia can generate ~30TBit/sec DDoS traffic, ranking 28th in the world.

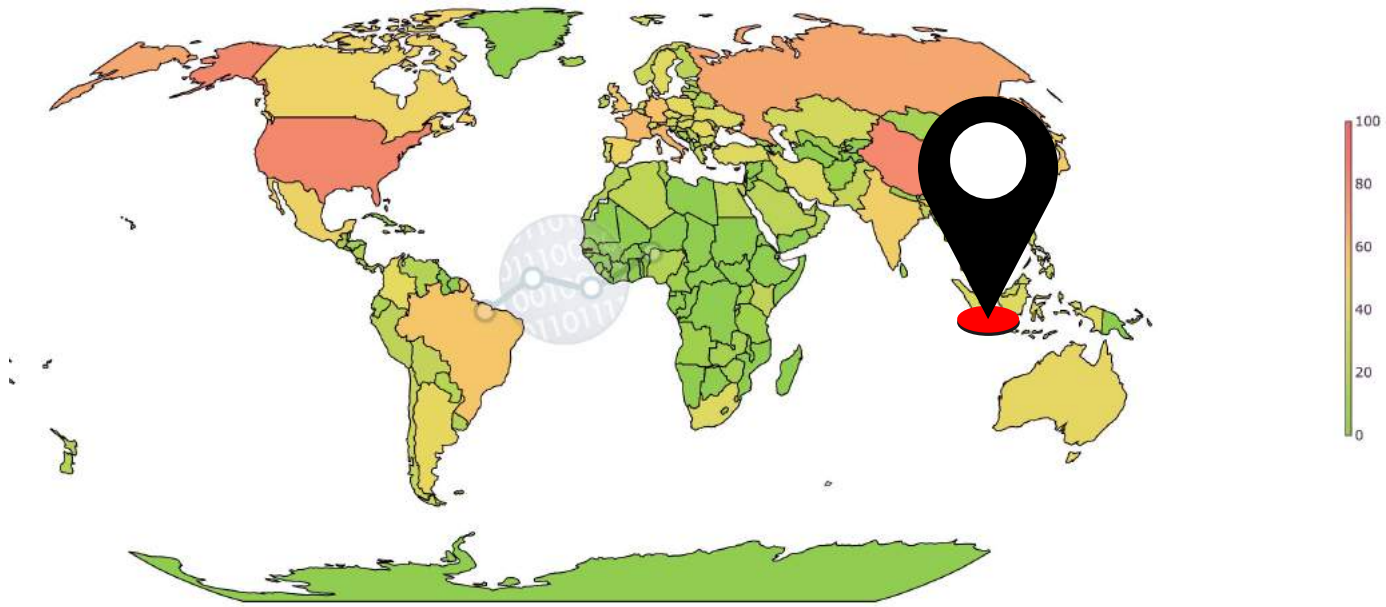


Figure 5. Global heatmap view of total potential DDoS bandwidth by country

Data source: CyberGreen

31 TBit/Sec

Indonesia | Total DDoS Potential

74,722
Open Recursive DNS

56,584
Open SNMP

49,294
Open NTP

37
Open CHARGEN

314
Open SSDP

ABOUT SOCRadar®

SOCRadar platform is an all-in-one solution that provides Extended Threat Intelligence, Digital Risk Protection, and External Attack Surface Management . Its false-positive free platform helps companies proactively defend themselves against cyber incidents. SOCRadar is empowered with strong AI algorithms and a highly talented analyst team, together they eliminate false positives.

FOLLOW US!

RECEIVE A FREE DEEP WEB REPORT FOR YOUR ORGANIZATION

SOCRadar, the early warning system for information security, analyzes thousands of deep web resources including hacker forums and social channels every day.

- **Deep web mentions**
- **Compromised credentials**
- **Malware/bot-infected users**
- **Highly critical data exposure findings**
- **Date of the latest exposure**

RECEIVE A FREE REPORT

CONTACT US info@socradar.io +1 (571) 249-4598 4000 Legato Road, Suite 1100 Fairfax, VA 22033 USA