Increased Cyber Attacks on the Government Sector in Indonesia

Author: Bablu Kumar

Co-Authors: Vikas Kundu and Noel Varghese

Threat Research and Information Analytics Division (TRIAD)

CloudSEK

Table of Contents

Home to 275 million people, Indonesia is fostering a start-up ecosystem with new government-led initiatives such as the **#1000StartupDigital** movement, encouraging new and existing businesses to 'Go Digital and Go Global'. This can potentially take Indonesia's digital economy closer to reaching USD 124 billion by the end of 2025, according to a study by Google, Temasek, and Bain & Company.

CloudSEK's contextual AI digital risk platform XVigil is closely monitoring underground cybercrime forums for cyberattacks against Indonesia. We have noticed a sharp spike in cyberattacks against Indonesian entities. Therefore, our focus in this blog is to understand threat actors' motivation and TTPs (tactics, techniques, and procedures) by comparing our data from 2021 and 2022.

Most Common TTPs

Now let's look at the common TTPs we have observed in the wild and the motivation behind these cyber threats.

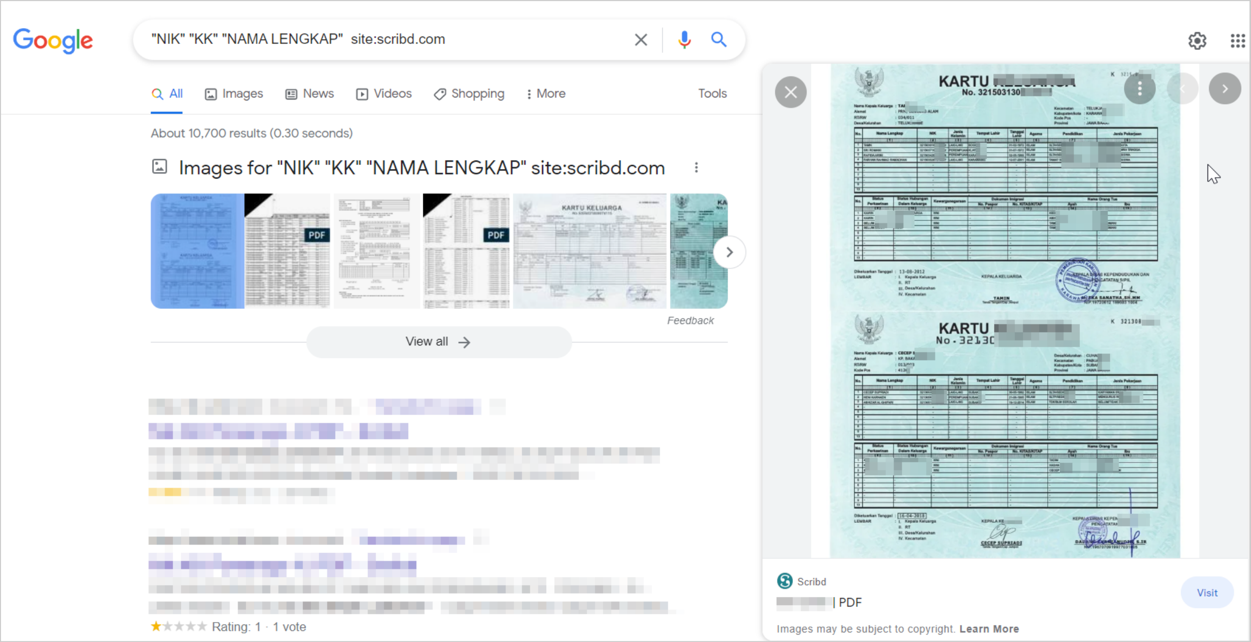
Ongoing Indonesian Gambling WordPress/cPanel Campaign

- A widespread campaign is targeting education, government, and nonprofit sector sites.
- Threat actors upload an obfuscated version of the ALFA TEAM web shell.
- The initial PHP dropper uses eval() and gzinflate() to produce at-runtime PHP, so the cleartext web shell never touches the filesystem.
- The web shell has the ability to clone and spoof login pages, including cPanel admin portals.
- This feature can help pivot from a single WordPress site compromise to an entire cPanel instance.
- Fake pages can be configured to "fail" 3 times to confirm password capture.
- This technique could also be used to attempt the capture of SSO credentials from unwitting users.
- It's anticipated that there are 240,000 potentially compromised sites in the public sector according to a blog post.

Harvesting PII & PHI of Indonesian Citizens using Google Dorks

- Recently threat actors were observed allegedly making use of Google Dorking and filters to harvest the PII and PHI of Indonesian citizens from Scribd, a document hosting platform that allows anyone to view public documents.
- The motive for uploading such sensitive documents on the platform is still unknown.

- Using Google Dorks (see appendix), they could narrow down their search to uncover the following sensitive information:
  - NIK Number (Indonesian National ID Number)
  - Name
  - Date of Birth
  - Phone Number
  - Address
  - Health Card Number
- By using appropriate dorks, anyone can find similar sensitive docs on other websites. These documents get indexed by the Google Search engine as well.



"NIK" "KK" "NAMA LENGKAP" site:scribd.com

About 10,700 results (0.30 seconds)

Images for "NIK" "KK" "NAMA LENGKAP" site:scribd.com

[redacted]

Rating: 1 · 1 vote

KARTU [redacted]

No. 321503130[redacted]

KARTU [redacted]

No - 3213C[redacted]

Scribd

[redacted] | PDF

Images may be subject to copyright. Learn More

Figure 0: Screenshot depicting how threat actors collect PII using simple Google Dorks

Exploiting SQL Injection Vulnerability

In a recent cyber attack, 26 million confidential records of police membership data and sensitive documents were exfiltrated and put on sale for a price of EUR 200,000 (to be paid in cryptocurrency).

- A SQL injection vulnerability was potentially exploited to gain access to the database.
- The actor possibly used hexadecimal encoded payload.
- The open source sqlmap tool was used to dump the contents of 10 databases via SQL injection.

Motivation

- Some threat actors like Strovian often expose these data breaches to highlight the lack of security measures enforced by Indonesian organizations, thus putting the privacy of Indonesian citizens at risk.
- In one instance, a threat actor previously disclosed security vulnerabilities to the Indonesian Government, but the vulnerabilities remained unpatched due to the lack of response from the concerned authorities.
- Cyber-protest is yet another political reason for government entities to be breached. For instance, a threat actor has recently leaked 1.4 GB worth of files regarding the nuclear power authority for free in response to police brutality and corruption by the Indonesian government. This is signaling a spike in cyber threats against the country due to the lack of police accountability and citizens' continued indignation.
- In other cases, the motivation behind the breaches was purely financial.

Monthly Distribution of Cyber Attacks in 2021 & 2022

Looking at the graph (**Figure 1**), we can deduce that while the service sector observed the highest number of cyber threats in 2021, we also notice a steep rise in cyber threats against the government sector starting from December 2021. Following this trend, the government sector became the most-targeted sector in 2022 (**Figure 2**).

Comparing both graphs, we can see that 2022 has seen a whopping 32.5% upsurge in the number of cyber threats in the first three quarters than the entire year in 2021.

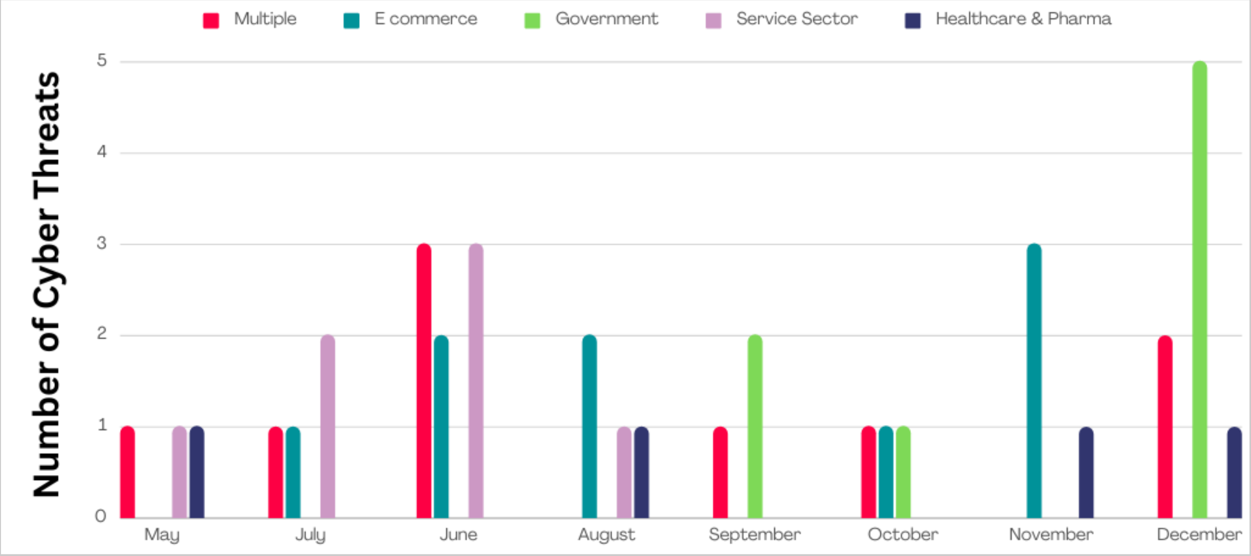


Figure 1: Monthly distribution of cyber threats in 2021

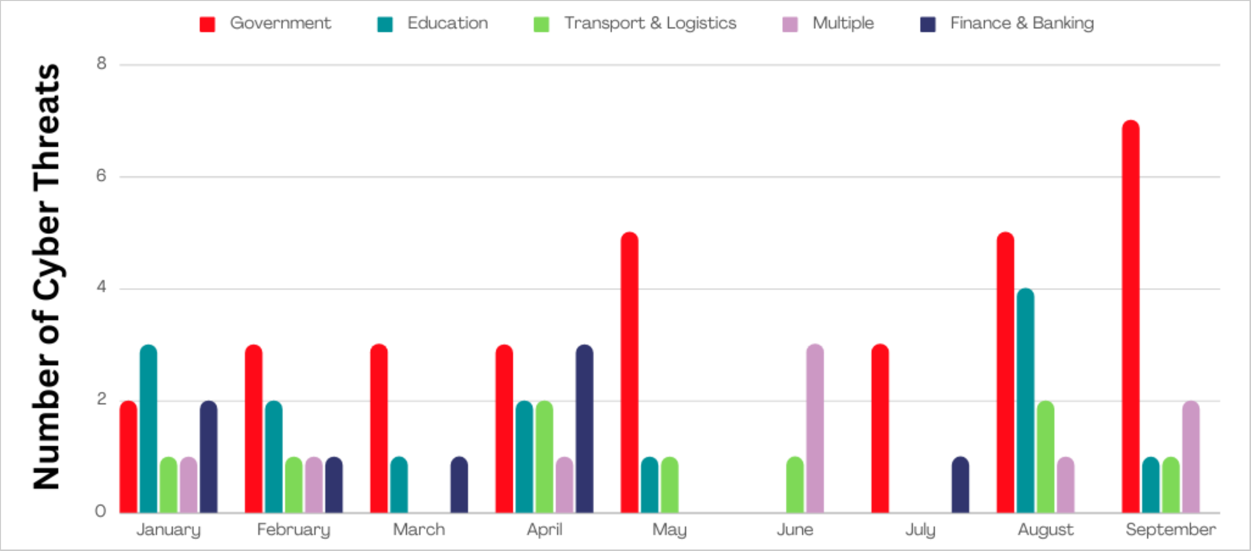


Figure 2: Monthly distribution of cyber threats in 2022

As depicted in **Figure 3**, the government sector recorded almost 4 times more cyber incidents in 2022. The highest number of cyber threats in 2021 and 2022 was observed in June and August respectively.

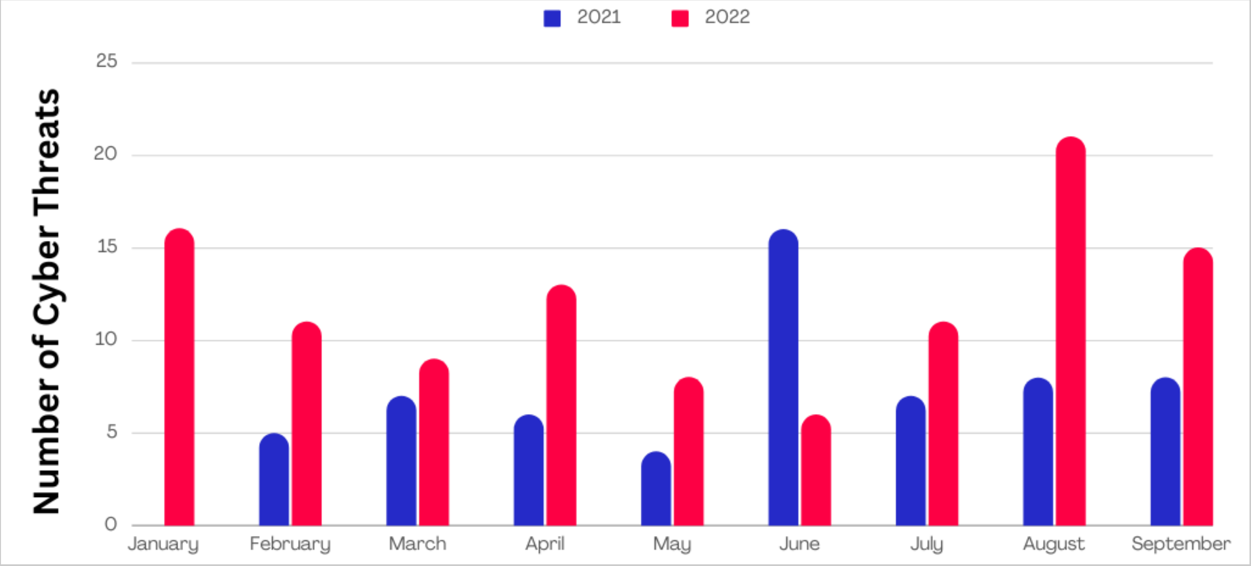


Figure 3: Monthly distribution of cyber attacks on Indonesian entities in the first nine months of 2021 and 2022.

Threat Actors Prime Targets

In 2021, the service sector followed by the multiple and education sectors was the most affected.

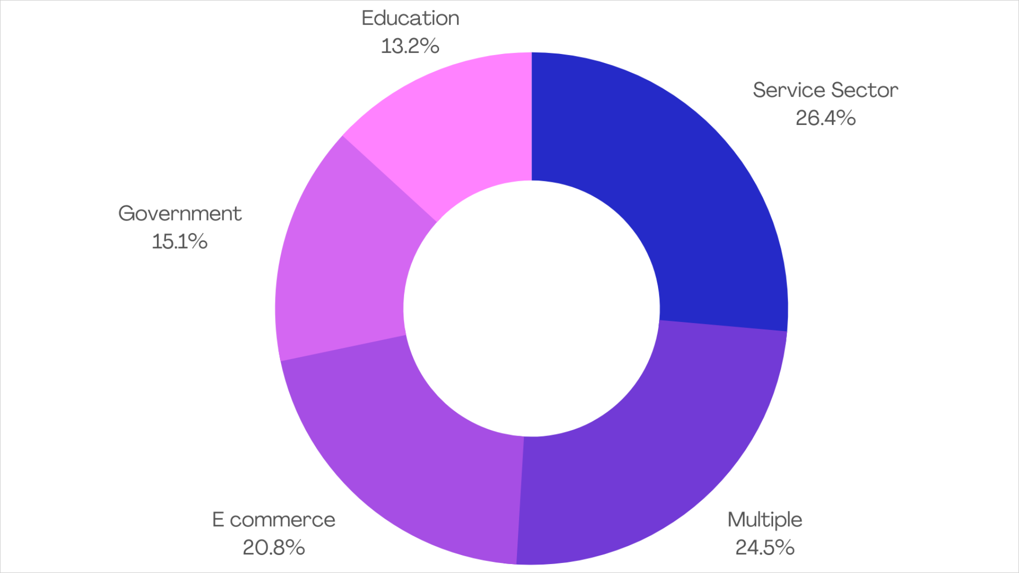


Figure 4: Most affected sectors in 2021

It should also be noted that the government sector wasn't a prime target back in 2021 but we observed an opposite trend in 2022 (**Figure 5**).

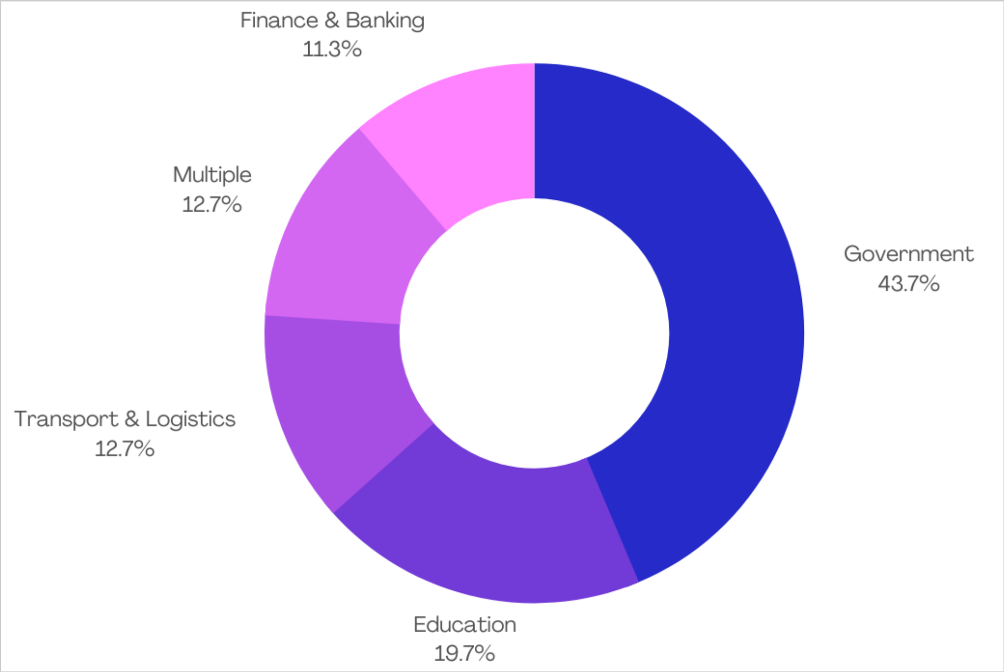


Figure 5: Most affected sectors in 2022

Major Threat Actors

The threat actors that have jolted the entire nation are highly reputed on the dark web forums.

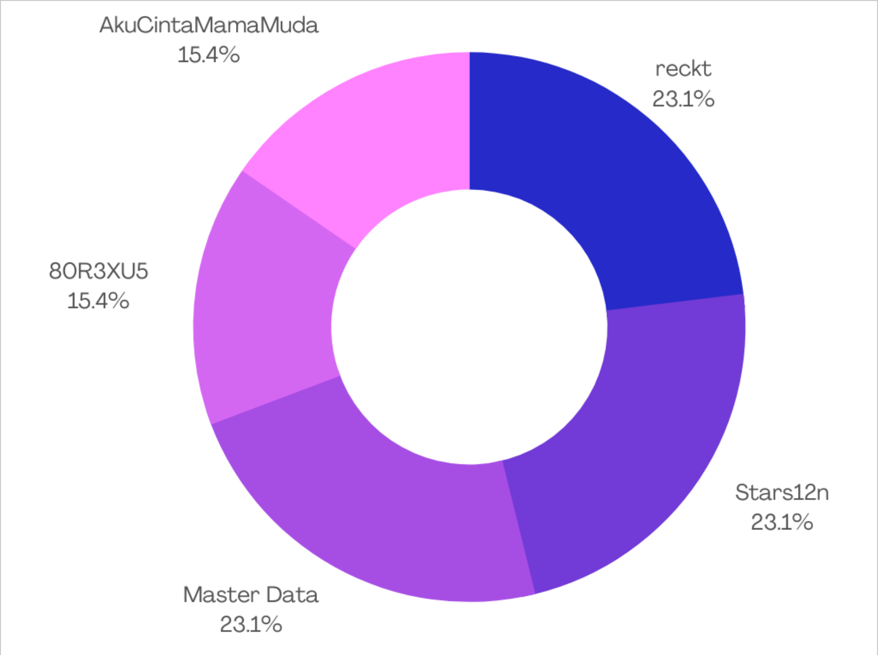


Figure 6: Top 5 threat actors targeting Indonesian entities in 2021

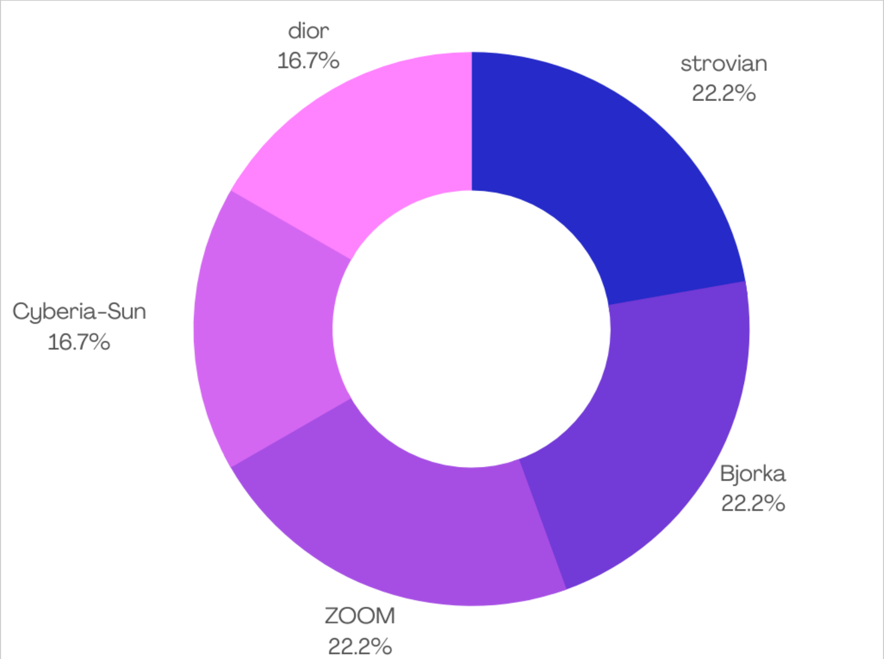


Figure 7: Top 5 threat actors targeting Indonesian entities in 2022

Master Data

- Master data is a threat actor group that actively operated on a now-dead English-speaking cybercrime forum. They actively post data that target various sectors and regions.
- Since most of their advertisements contained samples as proof to substantiate his claims, it was concluded that the actor did possess the data.

- On multiple occasions, the threat actor was found accessing and downloading databases from open databases, databases present in open web directories, or exploiting vulnerabilities on third-party vendors associated with an organization.
- The actor has been consistent in selling data and has been primarily data that contains PII such as phone numbers, email addresses, and passwords.

Bjorka

- A threat actor, Bjorka, has made Indonesia its primary attack target.
- The motivation behind the attacks is both financial and political.
- Bjorka's attacks had a significant impact, leading Indonesia to push a Personal Data Protection bill into law. The absence of such a law did not give clarity on who would handle and store the PII and PHI of Indonesian citizens.
- Among other hacking activities, Bjorka used to manage a leaked credentials DB engine - titled **leaks.sh**, in 2021. The site is currently unavailable.

Strovian

- The Indonesian entities are Strovian's primary target.
- The actor doesn't appear to be financially motivated.
- Strovian is one of the highly reputed threat actors on an infamous dark web forum.
- The actor is infamous for having leaked police and intelligence services' documents and the database of the Indonesian Police.
- Data breaches exposed by him are to show how weak Indonesian web-facing assets are in general.

Most Common Attack Vectors

Figure 8 and **Figure 9** highlight the three common attack vectors employed by threat actors to carry out attacks in 2021 and 2022.

While **data breaches** remained one of the most common attack vectors in both years, a steep rise in compromised **PII** has doubled this year.

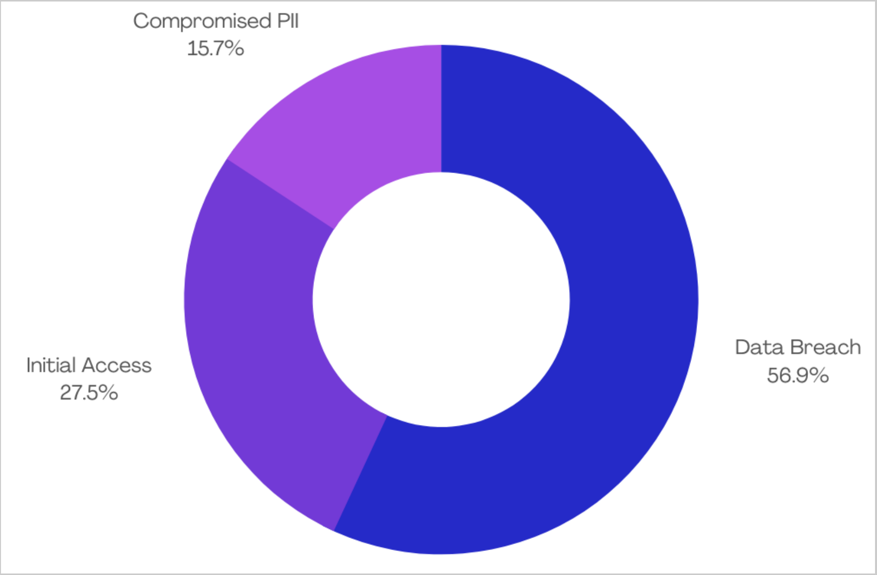


Figure 8: Most common attack vectors in 2021

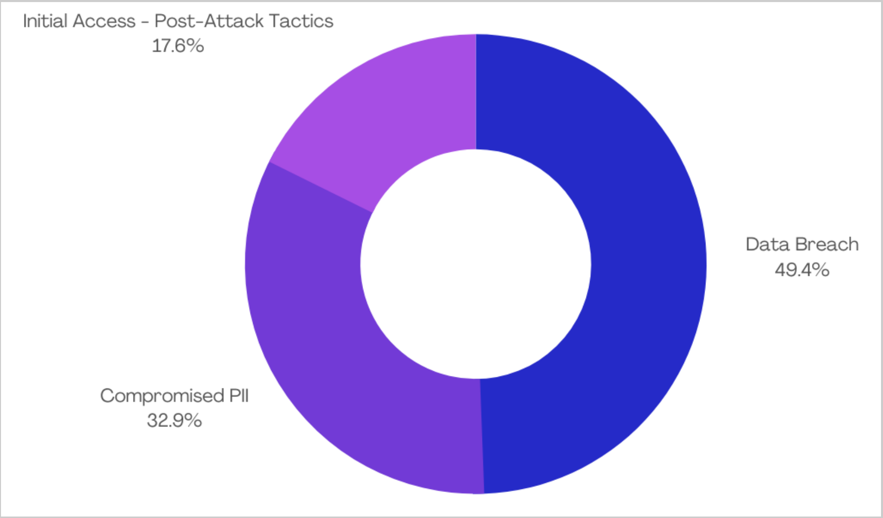


Figure 9: Most common attack vectors in 2022

Commonly Sought-After Data Types

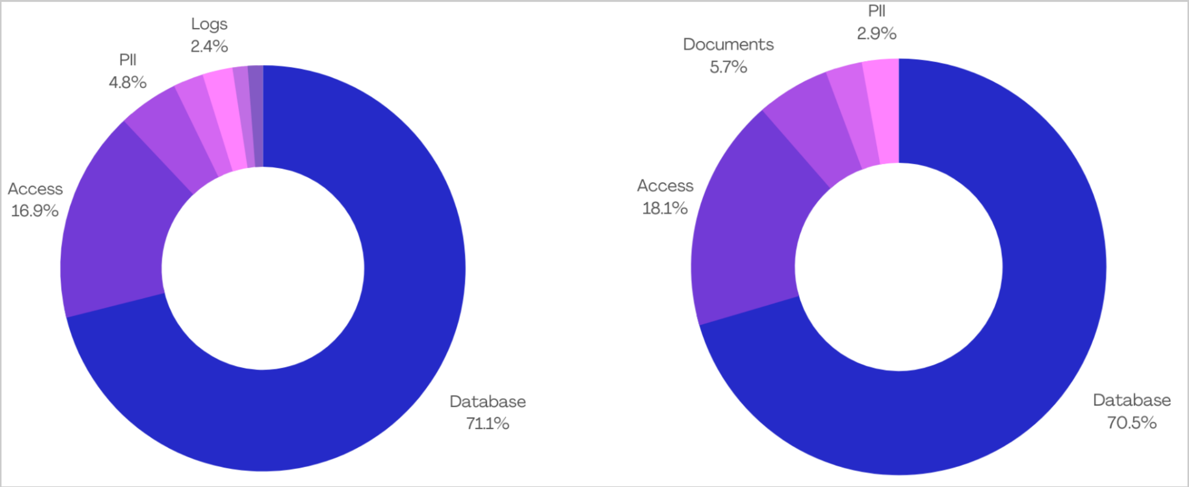


Figure 10: Data type exploited in 2021 (left) and 2022 (right)

In both 2021 and 2022, databases and access were the most commonly sought-after data type, with 71.2% of reported cases involving the leak or sale of databases from Indonesian entities in 2021. While this figure is 70.5% in the first nine months of 2022 alone, our data suggests the trend is ongoing.

The exploited databases include Personally Identifiable Information (PII) of victims such as:

- NIK (National ID Card Number)
- KK (Family Card Number)
- Full Name
- Residential Address
- Email Id
- Phone Number
- Gender, etc.

Conclusion

As noted, adversaries are actively targeting government and corporate websites, signaling that the current cybersecurity system is ineffective and subject to frequent attacks.

Some government institutions that have become targets are

- the General Elections Commission
- the Defence Ministry
- the Indonesian Child Protection Commission
- the Indonesian Association of Muslim Intellectuals

- Indonesian Police, etc.

To fill up the gap, the government needs to push for the passing of a cyber security bill in the House of Representatives.

Additionally, it has become crucial that the government and corporate should opt for comprehensive intelligence methods to proactively eliminate threats to keeping businesses up and running.

References

- security-research/reports/20221013-slot-wordpress at main · uclahs-secops/security-research · GitHub
- Deadly Soccer Clash in Indonesia Puts Police Tactics in Spotlight - The New York Times
- Cybersecurity for Indonesia: what needs to be done? (theconversation.com)

Appendix

Police beat soccer fans with sticks and shields and fired tear gas at tens of thousands of spectators. Source: nytimes.com

Google Dork	
1	"COVID 19 VACCINATION CARD" "NIK" site:scribd.com
2	"NIK" "KK" "NAMA LENGKAP" site:scribd.com
3	"Kartu Vaksinasi Covid-19" site:scribd.com

Google dorks used by threat actors to harvest sensitive information from documents

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats even before they occur. We combine the power of Cyber Crime monitoring, Brand Monitoring, Attack Surface monitoring, and Supply chain intelligence to provide context to our customer's digital risks. Our unified dashboard allows customers to triage and visualize all digital threats in one place. We also offer workflows and integrations to manage and remediate the identified threats. To learn more about CloudSEK, visit cloudsek.com.