

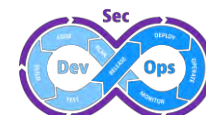


CyberDrill Exercise

“ Penanganan Insiden Keamanan Siber Pada Kasus Eksploitasi Aplikasi Web, Jaringan dan Data Breach ”

Kesiapsiagaan Teknis Insiden Keamanan Siber Pemerintah Pusat

Bandung, 19 dan 21 September 2022



1. LANSKAP ANCAMAN SIBER GLOBAL
2. LANSKAP ANCAMAN SIBER NASIONAL
3. EKSPLOITASI APLIKASI WEB DAN JARINGAN
4. DATA BREACH (KEBOCORAN DATA)
5. SOLUSI DAN TINDAKAN PREVENTIF
6. CYBERDRILL EXERCISE



LANSKAP ANCAMAN SIBER GLOBAL

LANSKAP ANCAMAN SIBER GLOBAL



GLOBAL CYBERSECURITY INDEX 2020

Published in Geneva, Switzerland 2022

Indonesia (Republic of)



Development Level:
Developing Country

Area(s) of Relative Strength
Cooperative, Capacity
Development Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
94.88	18.48	19.08	17.84	19.48	20.00

Source: ITU Global Cybersecurity Index v4, 2020

Table 3: GCI results: Global score and rank

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10

Indonesia	94.88	24
Viet Nam	94.59	25

Major Attack Types

you need to know
at least

Figure 1: ENISA Threat Landscape 2021 - Prime threats



Source : <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

Top cybersecurity threats facing the world in 2022

1. Social Engineering

Any network is hackable if an employee can be duped into sharing access

2. Third Party Exposure

Vendors, client, and app integrations with poor security can provide access to an otherwise well-protected network

3. Configuration Mistakes

Even the most cutting-edge security software only works if it's installed correctly

4. Poor Cyber Hygiene

Employee training is essential to ensure those with network access maintain safe cyber practices.

5. Cloud Vulnerability

Online data storage and transfer provides increased opportunities for a potential hack

6. Ransomware

Hackers can capture sensitive data or take down networks and demand payment for restored access.

7. Mobile Device Vulnerability

Devices that connect to multiple networks are exposed to more potential security threats.

8. Internet of Things

Smart technology users may not realize that any IoT device can be hacked to obtain network access.

9. Poor Data Management

When massive amounts of unnecessary data are kept, it's easier to lose and expose essential information.

10. Inadequate Post-Attack Procedures

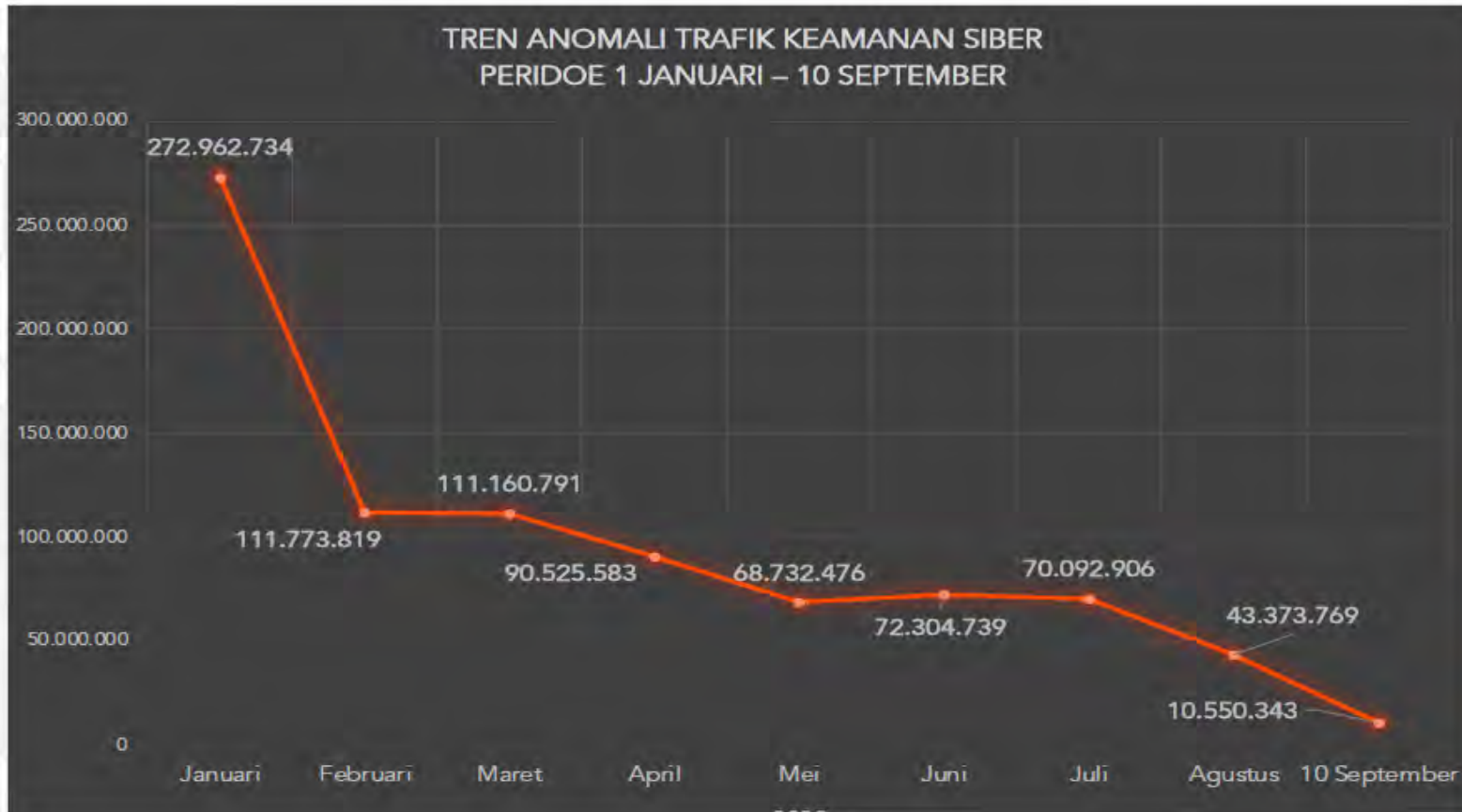
Security patches must be as strong as the rest of your cybersecurity protections.



LANSKAP ANCAMAN SIBER NASIONAL 2022

Tren Anomali Trafik Keamanan Siber

> Periode 1 Januari – 10 September 2022



TERCATAT TERDAPAT
851.477.160
ANOMALI TRAFIK PADA
TAHUN 2022

TOP #3 – JENIS ANOMALI TRAFIK

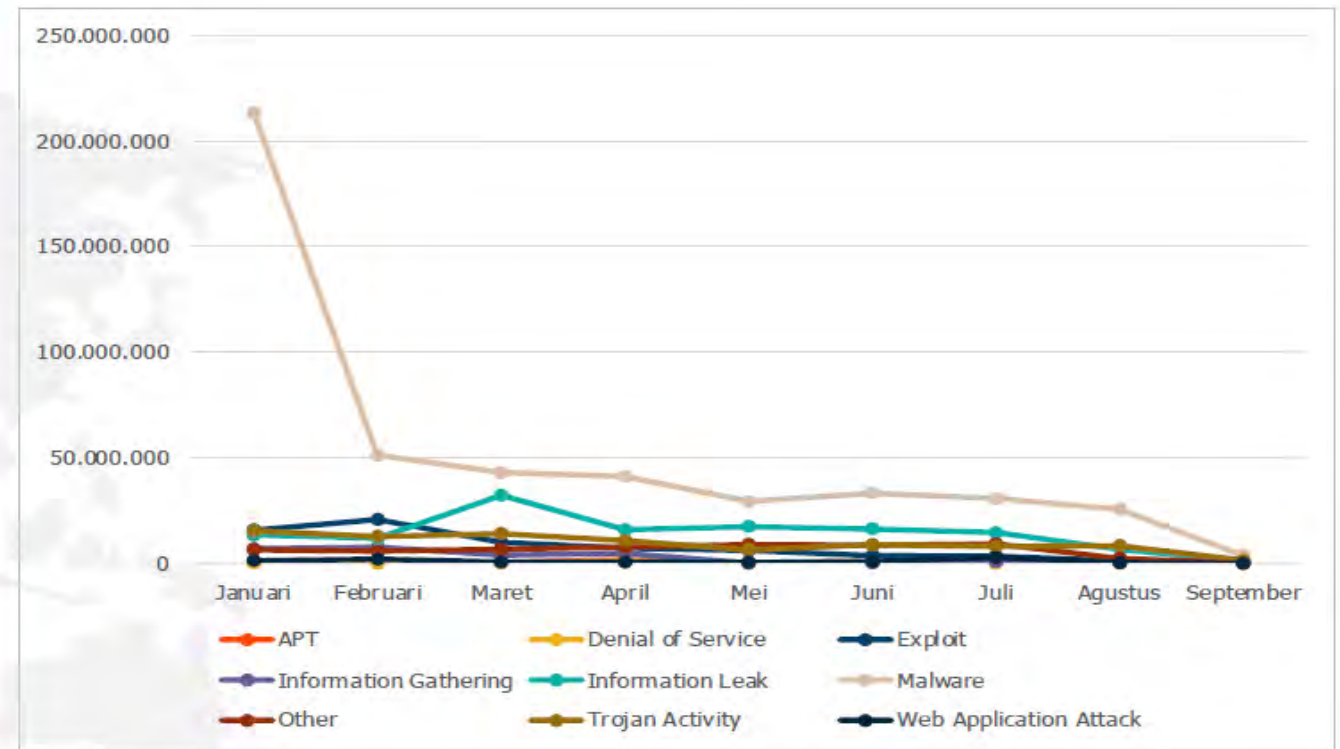
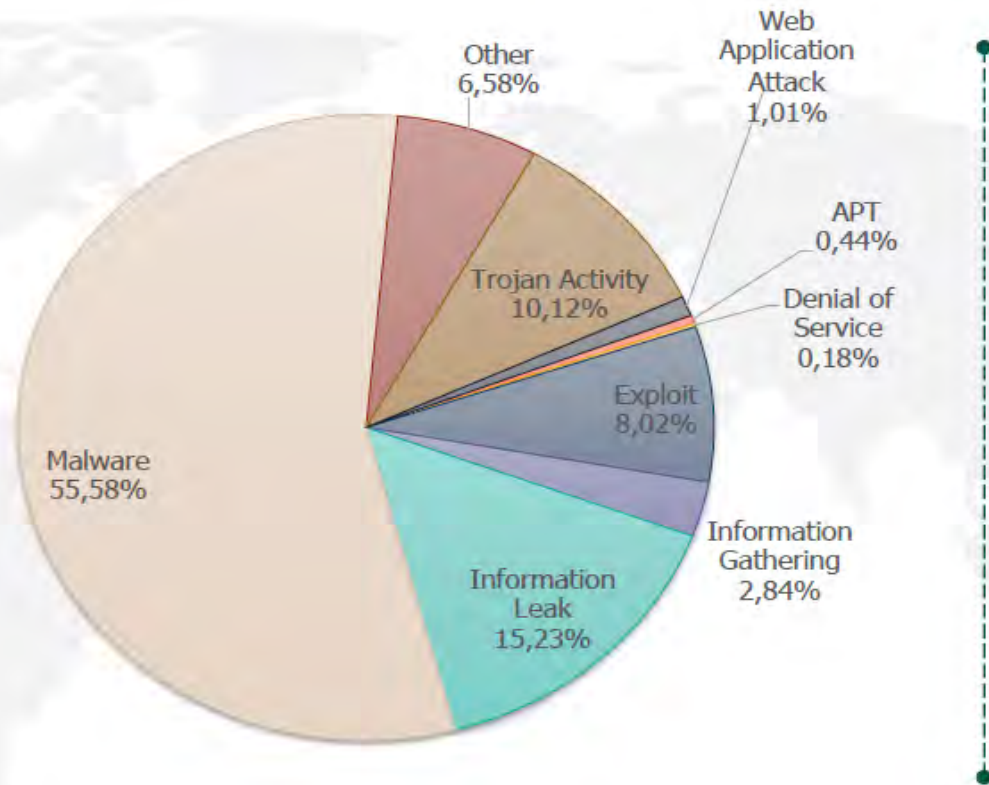
55,58% INFEKSI MALWARE

INFORMATION LEAK **15,23%**

10,12% TROJAN

Tren Anomali Trafik Keamanan Siber

> Periode 1 Januari – 10 September 2022



ADVANCED PERSISTENT THREAT (APT) DI INDONESIA PERIODE JANUARI – 4 SEPTEMBER 2022

Selama periode Januari – 4 September 2022 terdeteksi adanya aktivitas APT di Indonesia sebanyak **1.887.351** yang tersebar pada sektor IIVN.



APT	Count	Percent from Total
Lazarus	537,073	28.46%
Winnti	463,492	24.56%
APT40	160,107	8.48%
MageCart	100,062	5.30%
DangerousPassword	92,218	4.89%
SilverTerrier	76,546	4.06%
OceanLotus	58,256	3.09%
APT10	40,690	2.16%
Kimsuky	36,021	1.91%
Lockbit2	35,716	1.89%

TREN SERANGAN SIBER INDONESIA 2022

Data Breach

Data menjadi salah satu komoditas yang paling dicari saat ini. Selain memiliki nilai jual, data juga merupakan aset informasi yang menjadi target penyanderaan.

(target: Infrastruktur, end-user)

Web Defacements

Kasus peretasan di Indonesia menjadi salah satu hal yang masih marak terjadi. Situs yang teretas kemudian dimanfaatkan untuk tindak kejahatan lainnya (Judi Online, crypto-mining, fake online-shop, dll)



Human Operated Ransomware

Pada kasus ini pelaku serangan tidak melakukan penyanderaan terhadap seluruh data, namun hanya pada data tertentu yang memiliki nilai ekonomis dan memberikan peluang lebih besar korban untuk melakukan pembayaran.

(Ransomware Gang, Ransomware as a Service)

Advance Persistent Threat

Aktifitas kejahatan siber yang dilakukan oleh pelaku kejahatan siber dengan Taktik, Teknik dan Prosedur yang cukup kompleks.

(Umumnya dilakukan oleh *State-sponsored actor*)



EKSPLOITASI APLIKASI WEB DAN JARINGAN

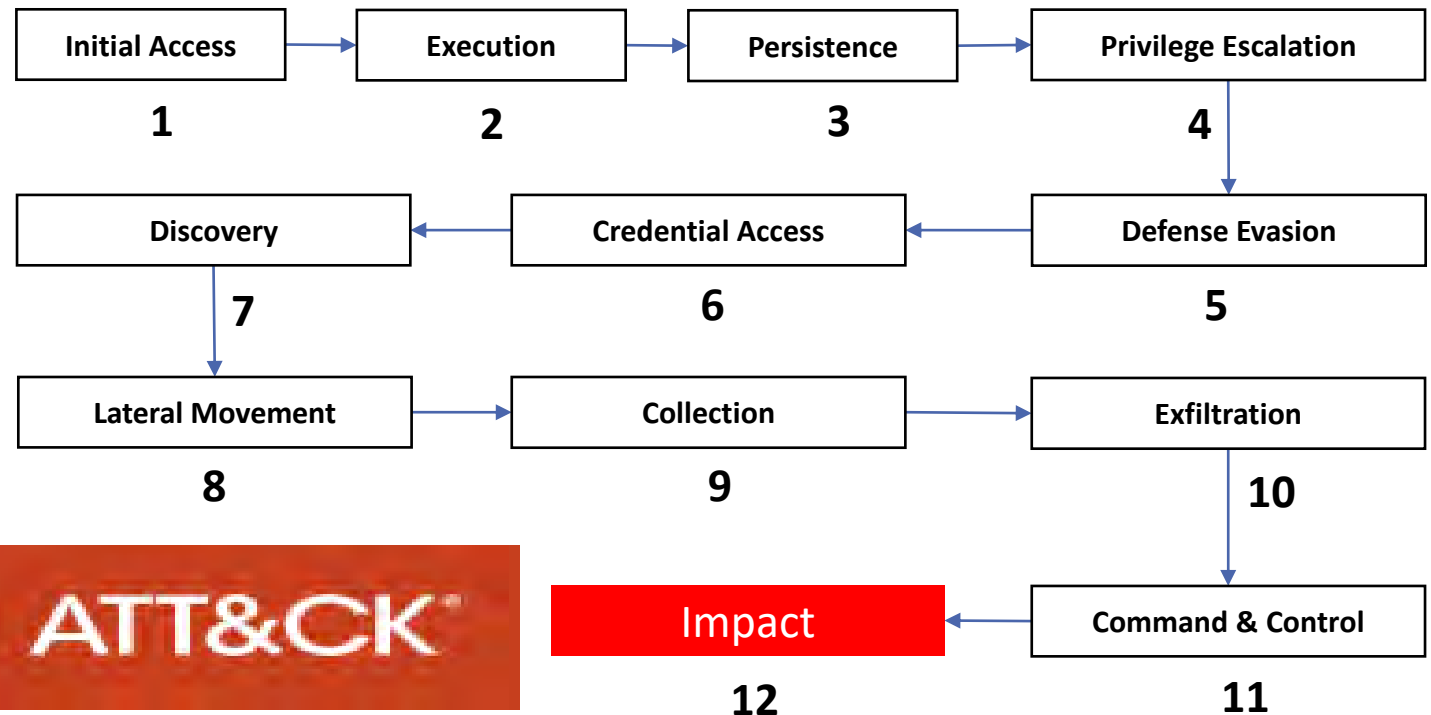
MITRE ATT&CK threat models and methodologies

1 Reconnaissance 2 Weaponize 3 Deliver 4 Exploit 5 Control 6 Execute 7 Maintain

PRE-ATT&CK

- Priority Definition
 - Panning Direction
- Target Selection
- Information Gathering
 - Technical, People, Organizational
- Weakness Identification
 - Technical, People, Organizational
- Adversary OpSec
- Establish Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK for Enterprise



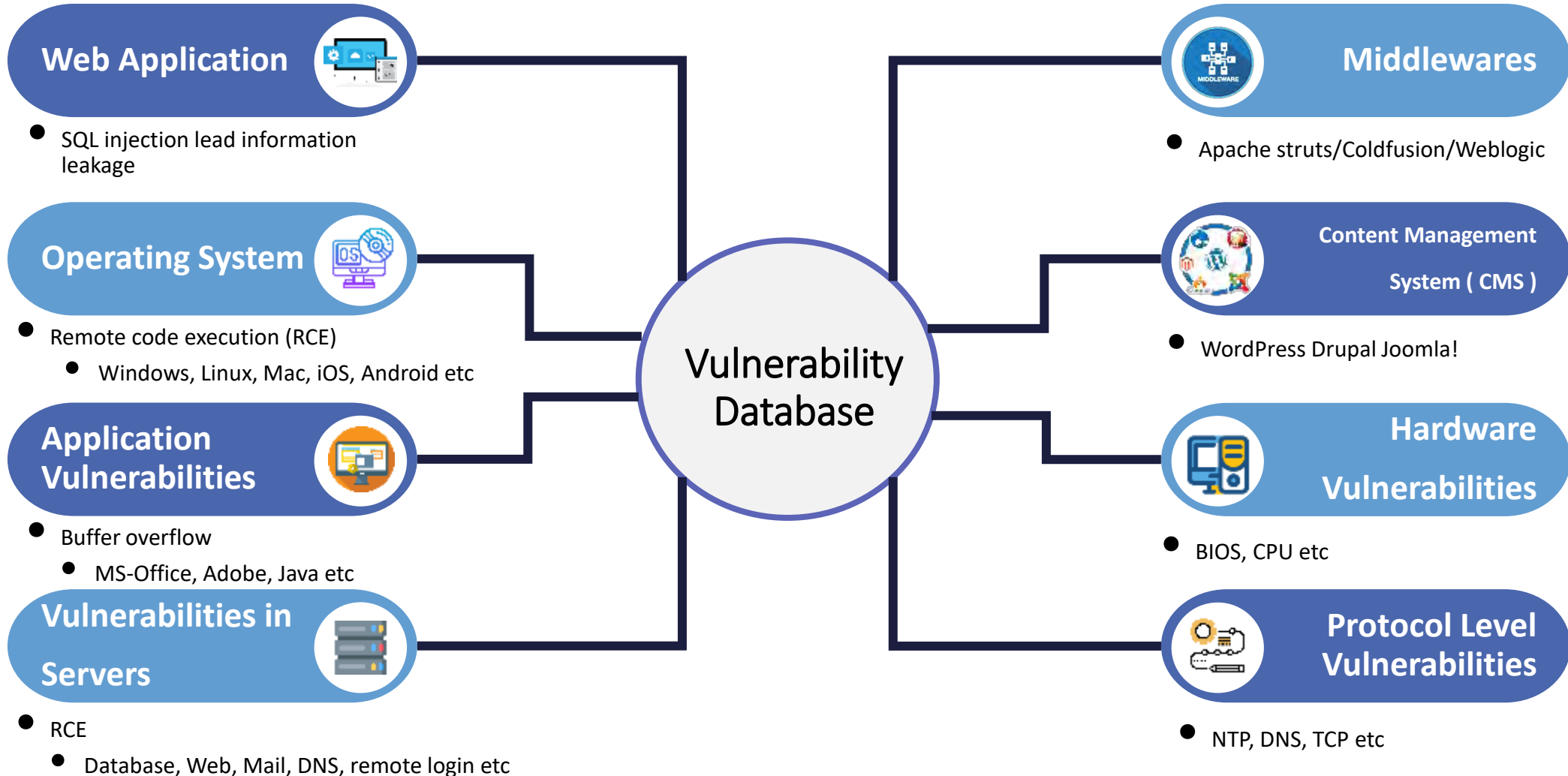
MITRE | ATT&CK

Latest Web Application risk based on OWASP Top 10 2021



Reference:

- <https://owasp.org/>
- <https://owasp.org/www-project-top-ten/>



Major Vulnerability Database and Standards

**CISA KNOWN EXPLOITED
VULNERABILITIES
CATALOG**

Now available
in the NVD



NIST NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

National Vulnerability Database : NVD

The NVD is the U.S. government repository of standards based vulnerability management data

<https://nvd.nist.gov/>



Common Vulnerability Exposure :CVE

CVE is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

<https://cve.mitre.org/>



Common Weakness Enumeration: CWE

CWE is a community-developed list of common software and hardware security weaknesses.

<https://cwe.mitre.org/>

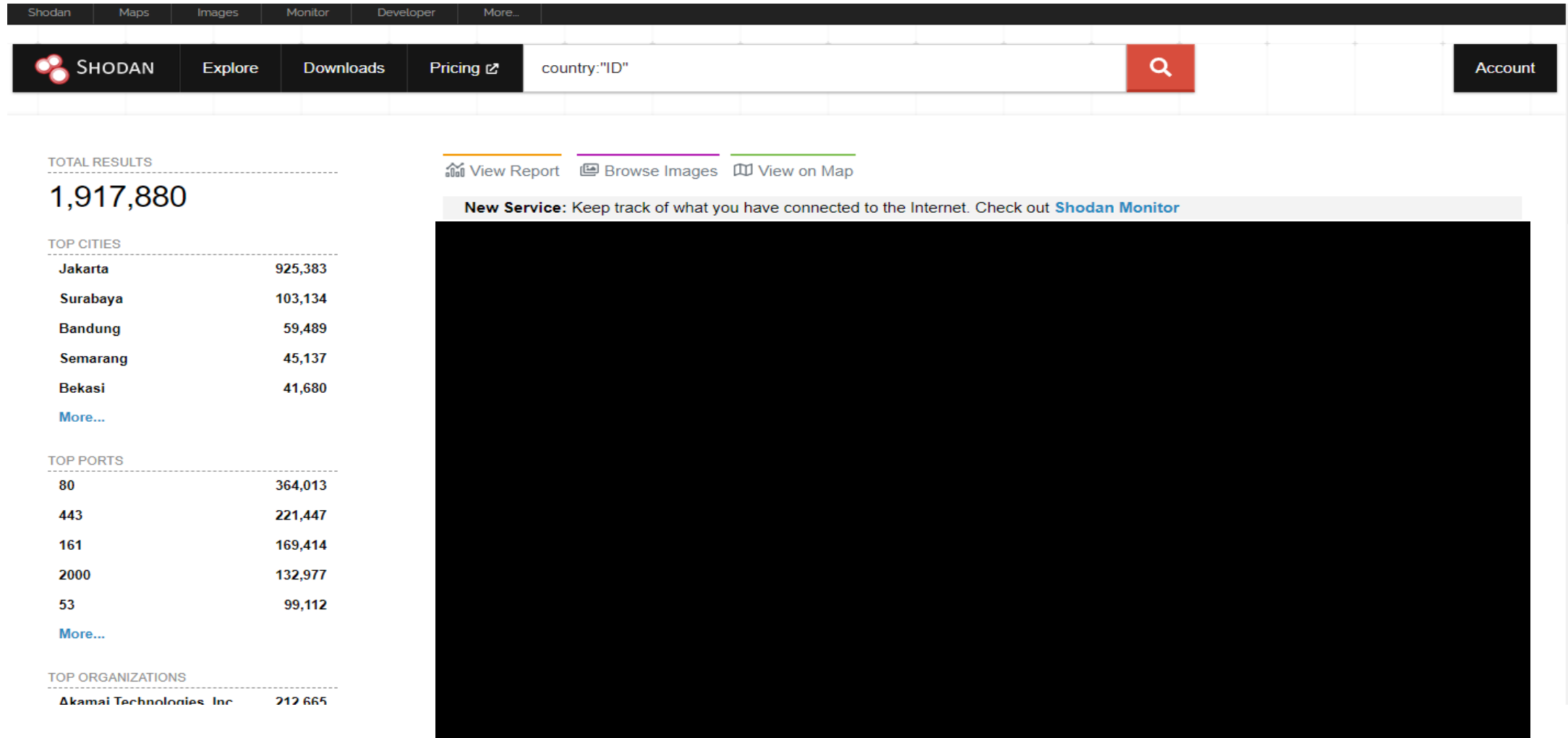


Common Vulnerability Scoring System: CVSS

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.

<https://www.first.org/cvss/>

Threat Intelligent Online



The screenshot displays the Shodan search engine interface. At the top, there is a navigation bar with links for Shodan, Maps, Images, Monitor, Developer, and More... Below this is a search bar containing the query 'country:"ID"' and a search button. The search results are categorized into several sections:

- TOTAL RESULTS:** 1,917,880
- TOP CITIES:** A list of cities and their corresponding result counts.
- TOP PORTS:** A list of ports and their corresponding result counts.
- TOP ORGANIZATIONS:** A list of organizations and their corresponding result counts.

Additional features include a 'New Service' banner for Shodan Monitor and navigation options like 'View Report', 'Browse Images', and 'View on Map'. The interface also includes a navigation menu with 'SHODAN', 'Explore', 'Downloads', 'Pricing', and 'Account'.

City	Count
Jakarta	925,383
Surabaya	103,134
Bandung	59,489
Semarang	45,137
Bekasi	41,680

Port	Count
80	364,013
443	221,447
161	169,414
2000	132,977
53	99,112

Organization	Count
Akamai Technologies, Inc	212,665

Exploit-DB Online



The screenshot displays the Exploit-DB website interface. At the top, the logo "EXPLOIT DATABASE" is visible. Below the header, there are filter options for "Verified" and "Has App", a "Filters" button, and a "Reset All" button. A search bar is present on the right. The main content is a table of exploits with columns for Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2022-09-15	↓	×	×	Gitea 1.16.6 - Remote Code Execution (RCE) (Metasploit)	WebApps	Multiple	samguy
2022-09-02	↓	×	×	WordPress Plugin Netroids Blog Posts Grid 1.0 - Stored Cross-Site Scripting (XSS)	WebApps	PHP	Luqman Hakim Zahari
2022-09-02	↓	×	×	WordPress Plugin Testimonial Slider and Showcase 2.2.6 - Stored Cross-Site Scripting (XSS)	WebApps	PHP	Luqman Hakim Zahari
2022-09-02	↓	×	×	Sophos XG115w Firewall 17.0.10 MR-10 - Authentication Bypass	WebApps	Hardware	Aryan Chehreghani
2022-08-09	↓	×	×	PAN-OS 10.0 - Remote Code Execution (RCE) (Authenticated)	Remote	Multiple	UnD3sc0n0c1d0
2022-08-09	↓	×	×	ThingsBoard 3.3.1 'description' - Stored Cross-Site Scripting (XSS)	WebApps	Multiple	Steffen Langenfeld
2022-08-09	↓	×	×	ThingsBoard 3.3.1 'name' - Stored Cross-Site Scripting (XSS)	WebApps	Multiple	Steffen Langenfeld
2022-08-09	↓	×	×	Feehi CMS 2.1.1 - Stored Cross-Site Scripting (XSS)	WebApps	PHP	Shivam Singh
2022-08-09	↓	×	×	Prestashop blockwishlist module 2.1.0 - SQLI	WebApps	PHP	Karthik UJ
2022-08-02	↓	×	×	uftpd 2.10 - Directory Traversal (Authenticated)	Remote	Linux	Aaron Esau
2022-08-01	↓	☑	×	Easy Chat Server 3.1 - Remote Stack Buffer Overflow (SEH)	Remote	Windows	r00tppg
2022-08-01	↓	×	×	Webmin 1.996 - Remote Code Execution (RCE) (Authenticated)	WebApps	Linux	Emir Polat

Contoh : Google Dork



Google

"Index Of" | .sql site:*.go.id



Semua Gambar Buku Video Berita Lainnya Alat

Sekitar 194.000 hasil (0,40 detik)

Index of /v.2/DB

Index of /v.2/DB. Name · Last modified · Size · Description · Parent Directory, -, v_2.sql, 2019-01-25 15:59, 491K.

Name	Last modified	Size
Parent Directory		
anggota_poktan_sumbawa.sql	26-Oct-2014 19:03	2.2M
bpp_16_oktober_2014.sql	17-Oct-2014 09:05	3.4M
data.sql	2020-02-14 08:26	114K
data_56.sql	2020-02-14 08:27	9.6M

Google

"Hacked By" site:*.go.id



Semua Gambar Berita Video Shopping Lainnya Alat

Sekitar 15.000 hasil (0,28 detik)

<https://jdih.kendalkab.go.id/perpustakaan>

Hacked By ArdhyanX - AlwaysCrew - JDih Kabupaten Kendal

AlwaysCrew | **Hacked By** ArdhyanX - AlwaysCrew.

<https://tulangbawangbaratkab.go.id/hacked-by-zin>

Hacked By Zin - Kabupaten Tulang Bawang Barat

Hacked By Zin. 07 September 2022. dibaca 10 kali. Gabut. **Hacked By** Mr.Heckers ft Kuncen Haxor. memek12345. berita. read more ...

<https://jdih.kendalkab.go.id/perpustakaan>

TIPIKOR | Hacked By ArdhyanX - AlwaysCrew

Hacked By ArdhyanX - AlwaysCrew. AlwaysCrew. Menu. Beranda depan · Warta Perpustakaan · Info Perpustakaan · Lokasi Perpustakaan · Area Anggota · Pustakawan ...

No. Panggil: 343.2 DEW t

Bahasa: Indonesia

<https://inspektorat.tegalkab.go.id/2022/08/27/hacke...>

Hacked by find.eda ft firatke - Inspektorat Kabupaten Tegal

Hacked by find.eda ft firatke. Posted By: admin 27/08/2022. **Hacked by** find.eda ft firatke. Previous post · Next post.

<http://tanjunganom.nganjukkab.go.id/tmp/indo>

Hacked By MR.5T1Y0

HACKED BY MR.5T1Y0.

Operating System for Hacking



Kali Linux OS



ParrotOS



Backbox OS



BlackArch



Fedora Security



Dracos OS

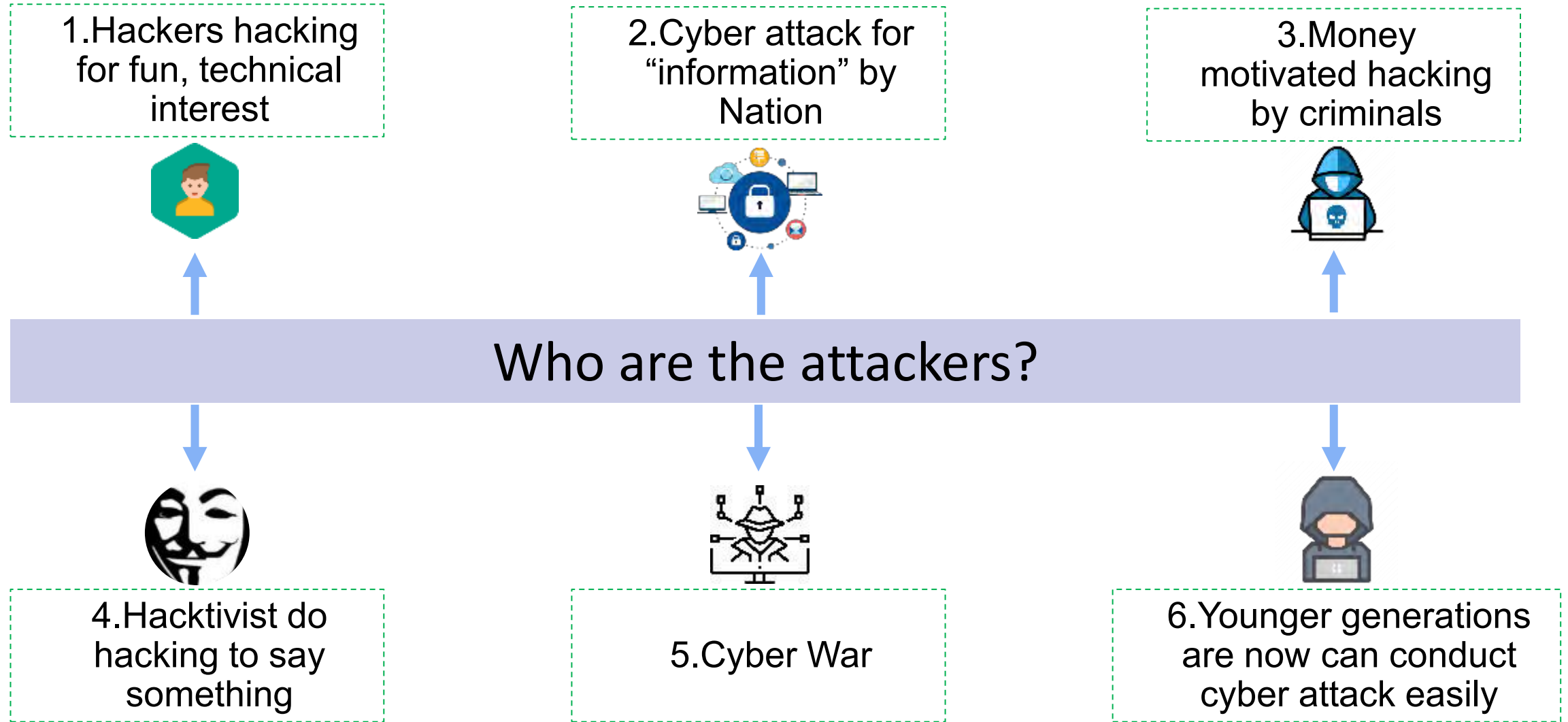


Caine OS



Network Security Toolkit

Samurai Web Testing Framework



Better Chance
for Attackers



Latest technology
trend changes
attackers' chance of
successful
exploitation



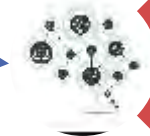
Cloud



API / Fintech



IoT (Physical)



Data connection



Cryptocurrency



DevOps / DevSecOps

Reference :

<https://cybersecurityforme.com/cybersecurity-and-latest-technology-trends/>



DATA BREACH (KEBOCORAN DATA)

Data Breach



ISO/IEC 27040 / GDPR

mendefinisikan *Data Breach* sebagai:

“compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed”.

Tindakan atau kegiatan yang mengarah pada perusakan, kehilangan, perubahan, pengungkapan yang tidak sah atau tidak disengaja, atau akses ke data yang dilindungi yang dikirimkan, disimpan, atau diproses

DATA BREACH INFORMATION :



Personal Health
Information (PHI)



Personal Identifiable
Information (PII)



Intellectual
Property



Sensitive
Information



Financial
Information



Government
Information



Rekapitulasi Notifikasi Data Breach

> Laporan Data Breach Tahun 2022 Per 13 September 2022

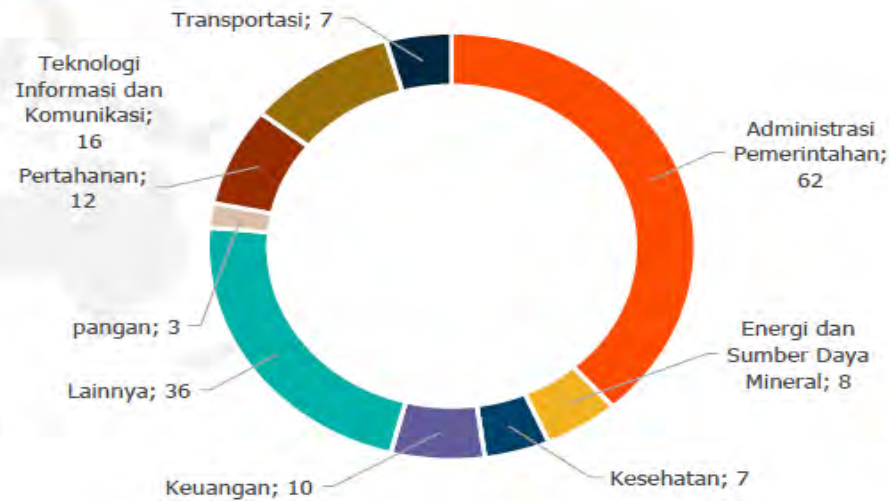


Penyebab

52 Malware Stealer

130 Anonymous Threat Actor (Breach Forum)

52 Kasus disebabkan oleh Malware Stealer, dan dari 95 Kasus yang terpublikasi disebabkan oleh 57 Threat Actor unik pada Breach Forum



Lanskap Digital Indonesia

mendorong pertumbuhan inklusif dengan tetap memperhatikan mitigasi risiko

Peluang

Demografi



Potensi pasar yang besar

51%
unbanked people

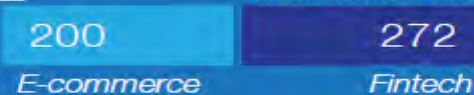
Sumber: World Bank, 2017

Lanskap Digital

Pengguna



Pelaku



Tantangan



Data is the "New Oil"

Data adalah kunci daya saing



Trafik Internet/detik



Adopsi Cloud Computing



Media Sosial/Menit



Transaksi Pembayaran

2rb /detik

Digital Banking



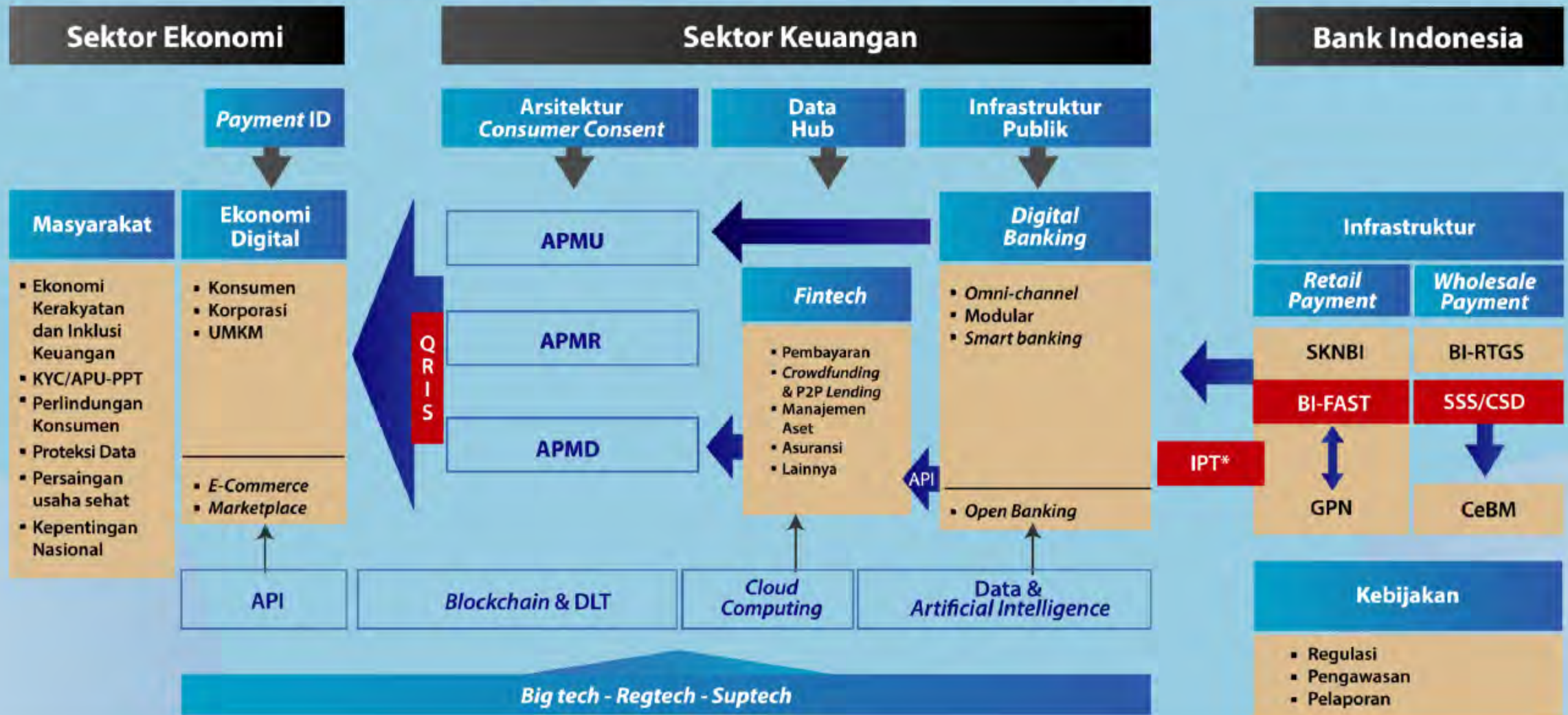
ecommerce



Sumber: Unctad, Cisco, Bank Indonesia, Lorilewis

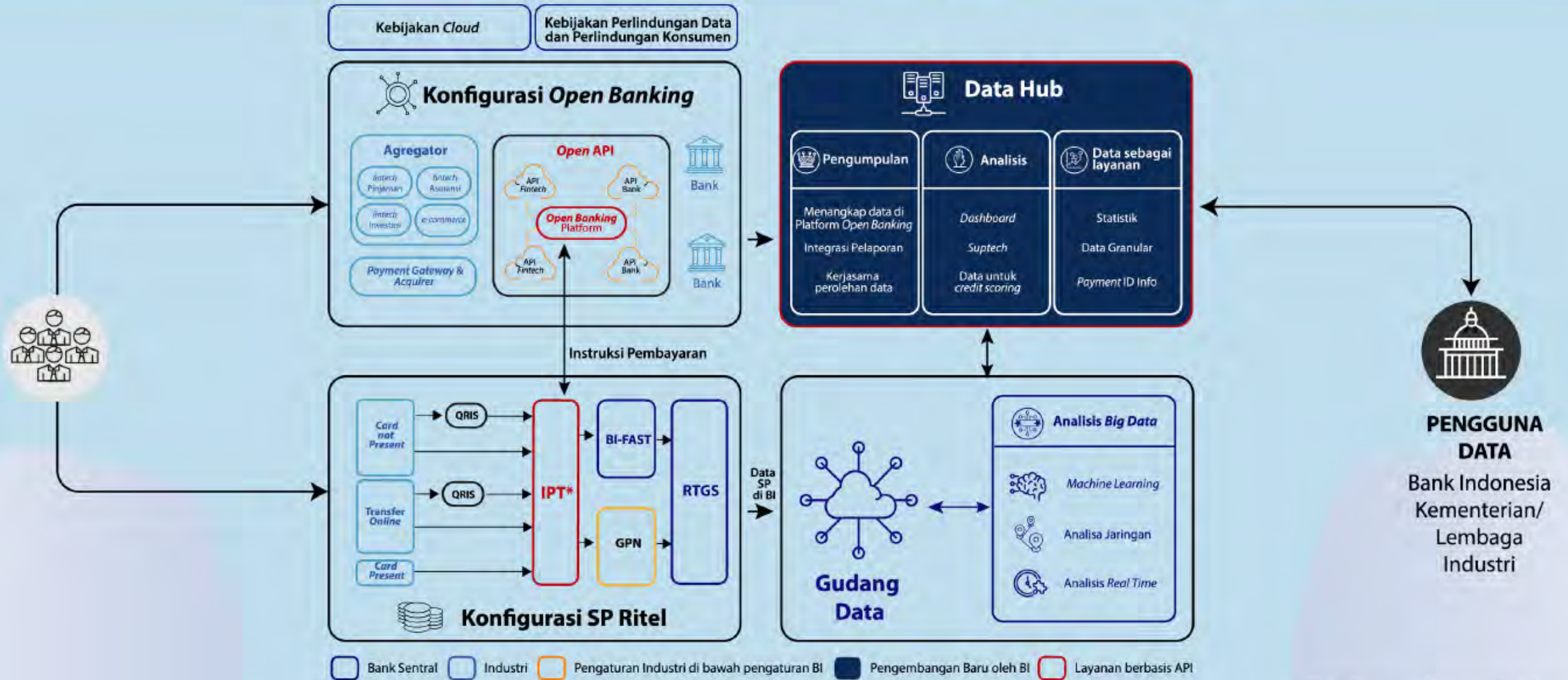
Konfigurasi Ekonomi dan Keuangan Digital Indonesia

SPI 2025 mendukung integrasi ekonomi-keuangan digital nasional sehingga menjamin fungsi bank sentral dalam proses peredaran uang, kebijakan moneter, dan stabilitas sistem keuangan.



Konfigurasi Data Hub

Pengembangan infrastruktur publik untuk menjamin keterbukaan terhadap akses data dan informasi dengan tetap memperhatikan proteksi data pribadi konsumen dan prinsip persaingan usaha yang sehat



*Interface pembayaran terintegrasi

Cyber attacks on Nvidia



11:45 nachm. - 25. Feb. 2022 - Twitter Web App

Source : [https://twitter.com/tomwarren/status/1497341983127445506](\"https://twitter.com/tomwarren/status/1497341983127445506\")



Source : [https://www.reuters.com/technology/nvidia-says-employee-company-information-leaked-online-after-cyber-attack-2022-03-01/](\"https://www.reuters.com/technology/nvidia-says-employee-company-information-leaked-online-after-cyber-attack-2022-03-01/\")

Created: Feb 25, 2022 07:08 PM
Updated: Feb 25, 2022 07:10 PM



McDonald's

<https://www.mcdonalds.com/>

500 GB

Back in 1954, a man named Ray Kroc discovered a small burger restaurant in California, and wrote the first page of our history. From humble beginnings as a small restaurant, we're proud to have become one of the world's leading food service brands with more than 36,000 restaurants in more than 100 countries.

Ransomware McDonald's

[https://pbs.twimg.com/media/FMd_r9bXIAYIGG7?format=jpg&name=900x900;](https://pbs.twimg.com/media/FMd_r9bXIAYIGG7?format=jpg&name=900x900)

<https://borncity.com/win/2022/02/26/nvidia-von-cyberangriff-betroffen-25-feb-2022/>

← Windows 10/11 (21H2): Wipe does not delete user data

Linux vulnerabilities patched fastest (Feb. 2022) →

axis.com (IP security camera vendor) is down (Feb. 21, 2022)

Posted on 2022-02-21 by guenni



[[German](#)] Brief note for people dealing with security cameras from vendor Axis. A German blog reader informed me, that the website of this vendor is currently down. There seems to be massive technical issues causing a major outage. Whether it is the result of a cyber attack, or just the technology, I can not currently answer. Means that customers (banks, supermarkets, etc.) can no longer access their security cameras remotely because the cloud is down. Here is some information. **Addendum:** It looks like a cyberattack –

because after my inquiry on Twitter, there is a new reference to an "IT-related intrusion" on the status page – see addendum in the text. **Addendum 1:** It's was a cyberattack that has taken place.

<https://borncity.com/win/2022/02/21/webseite-von-ip-sicherheitskamera-hersteller-axis-com-ist-down-21-2-2022/>

[Axis Communications](#) AB is a Swedish manufacturer of network cameras, access control and network audio devices for physical security and video surveillance. The manufacturer considers itself a technology leader in network cameras and other IP network solutions.

The websites are down

I received a private message from a reader via Facebook (thanks for that) on 2/21/2022 at mid-afternoon, asking if I knew anything about axis.com, because their website was dead. In deed – whoever tries to access the site *axis.com* in a browser is greeted with a simple error message that the page is not accessible. Here is the German version of this browser message.

[Home](#) > [Cryptocurrency](#) > [News](#) » Solana Hack That Drained \$8 Million Is Linked To The Slope Mobile

Solana hack that drained \$8 million is linked to the Slope mobile wallet

■ IANS | AUG 5, 2022, 11:38 IST



Source :

<https://www.businessinsider.in/cryptocurrency/news/solana-hack-that-drained-8-million-is-linked-to-the-slope-mobile-wallet/articleshow/93363977.cms>

The multi-million Solana crypto hack, that drained more than 8,000 wallets worth around \$8 million, has been linked to accounts tied with the Slope mobile wallet app.

Slope Finance said in a statement that a cohort of Slope wallets were compromised in the breach, advising users to create "a new and unique seed phrase wallet, and transfer all assets to this new wallet."

"We have some hypotheses as to the nature of the breach, but nothing is yet firm. We feel the community's pain, and we were not immune. Many of our own staff and founders' wallets were drained," the company said late on Thursday.

tempo.co
BICARA FAKTA

Cari Berita

TEMPO EKSKLUSIF ▾

Terbaru Terpopuler News ▾ Multimedia ▾ Olahraga ▾ Nusantara ▾ Otomotif ▾

Beranda > Tekno

Sampel 2 Juta Data SIM Card Diduga Bocor dari Kominfo, Apakah ada Nomor Anda?

Reporter: Maria Fransisca Lahur
Editor: Zacharias Wuragil

Senin, 5 September 2022 15:31 WIB





"BANK OF INDONESIA"

<https://www.bi.go.id>

Jl. MH. Thamrin 2, Jakarta, Jakarta, Indonesia

In its capacity as central bank, Bank Indonesia is mandated with one overarching goal, namely to create and maintain rupiah stability. Towards that goal, Bank Indonesia is tasked with managing the Monetary sector, Payment System and Financial System Stability, which are integrated to ensure the overarching goal is achieved effectively and efficiently.

PUBLISHED 1%

1/19/2022 9014 83803 [130.96 GB]

/ ROOT

corp.bi.go.id	12002
corp.bi.go.id	1706
corp.bi.go.id	1707
corp.bi.go.id	2101
corp.bi.go.id	2301
corp.bi.go.id	KPK1201
corp.bi.go.id	906
corp.bi.go.id	527
corp.bi.go.id	JV-001
corp.bi.go.id	JV-002
corp.bi.go.id	073
corp.bi.go.id	074
corp.bi.go.id	102
corp.bi.go.id	104
corp.bi.go.id	110
corp.bi.go.id	112
corp.bi.go.id	117
corp.bi.go.id	1821
corp.bi.go.id	0

<https://www.viva.co.id/digital/digilife/1444068-kebocoran-data-bank-indonesia-terus-bertambah>

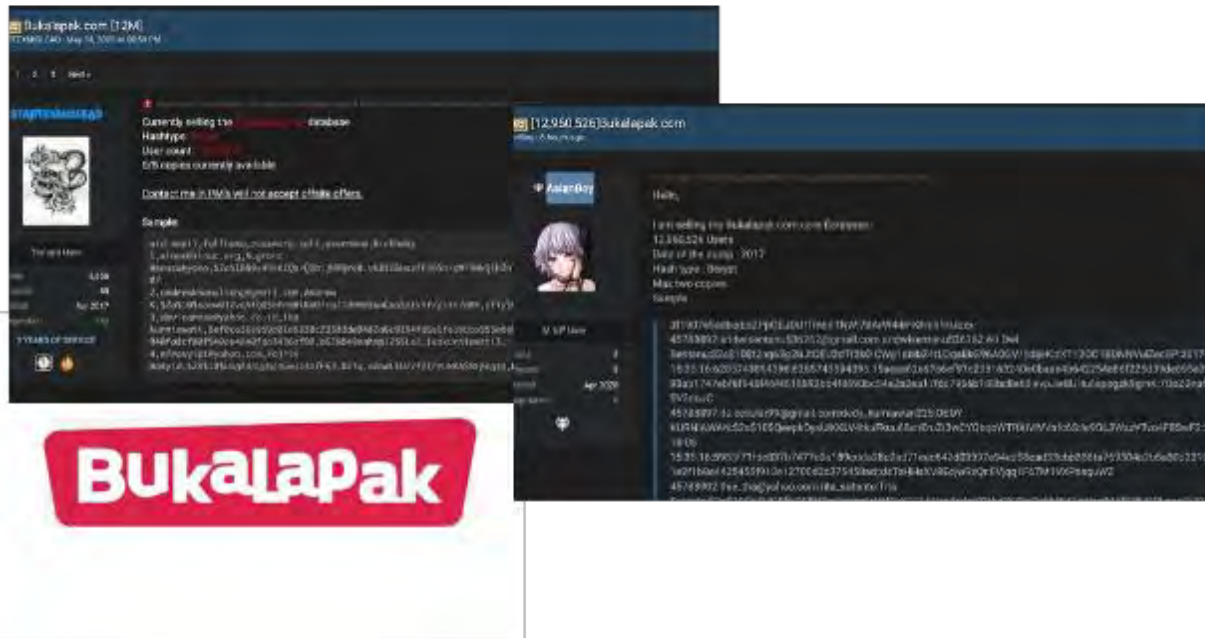


Tokopedia 91M
Contact: XMPP [redacted] Twitter: [redacted]
Sold by [redacted] - 0 sold since May 03, 2020 Vendor Level 1 Trust level 1
Unlimited items available for auto-dispatch

Product Class	Features	Origin Country	Features
Digital	Unlimited	World Wide	World Wide
Quantity Left	Never	Ships to	Escrow
Ends In		Payment	

default - 1 day - USD + 0.00
Purchase price: **USD 5,000.00**
Qty: 1
0.561030 ETC / 77.990953 XMR

Data Breaches Indonesia



Bukalapak.com [12M]
STARTERPACKS
Currently selling the starterpacks
User: [redacted]
576 copies currently available
Contact me in DM's will not accept chats offers

Sample

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]

Bukalapak

Data 279 Juta Penduduk Bocor di Internet, BPJS Kesehatan: Server Aman

Liberty Jemadu | Dicky Prasetya

Kamis, 20 Mei 2021 | 18:47 WIB



Ilustrasi kantor BPJS Kesehatan. (ANTARA FOTO/Aditya Pradana Putra)



SOLUSI DAN TINDAK PREVENTIF

SOLUSI DAN TINDAKAN PREVENTIF



Governance



- Corporate board
- Executive leadership
- Risk management
- 3rd party policies
- Zero-trust model

People



- SOC (Security Operation Center)
- Cyber security talent
- Employee awareness
- Adaptive trust model
- Secure remote environment

Process



- Identify
- Protect
- Detect
- Respond
- Recover

Technology



- DevSecOps
- AI & ML
- Zero trust architecture
- Hybrid cloud security
- SOAR (Security Orchestration, Automation and Response)

Build *Computer Security Incident Response Team (CSIRT)* is a must

What are Common Cyber Hygiene Problems?

Why is Cyber Hygiene Important?

Every employee needs to understand basic cyber hygiene practices and their role in protecting and maintaining your IT systems and devices. This will enable better incident response and provide immediate and effective defenses against cyber attacks.

Reference :

<https://www.upguard.com/blog/cyber-hygiene>

Loss of Data

Hard drives, online cloud storage and SaaS apps that store sensitive data that isn't backed up or maintained can be vulnerable to hacking, corruption, data leaks, and data breaches.

Misplaced data

Poor cyber hygiene could mean losing data in other ways, while it may not be corrupted or gone for good, it's increasingly common to misplace data due to the myriad of places it can be stored. This is why robust data classification is important.

Security breaches

Data breaches are becoming increasingly common, and costly. Spear phishing, whaling attacks, lack of configuration management, and poor network security can all lead to exposure of trade secrets, PII, and PHI. This can result in customer identity theft, industrial espionage, and a loss of market position.

Outdated software

Software applications must have security patches applied regularly to prevent known vulnerabilities. The success of the WannaCry ransomware computer worm is a great example of why patching operating systems is an important part of good cyber hygiene

Old security software

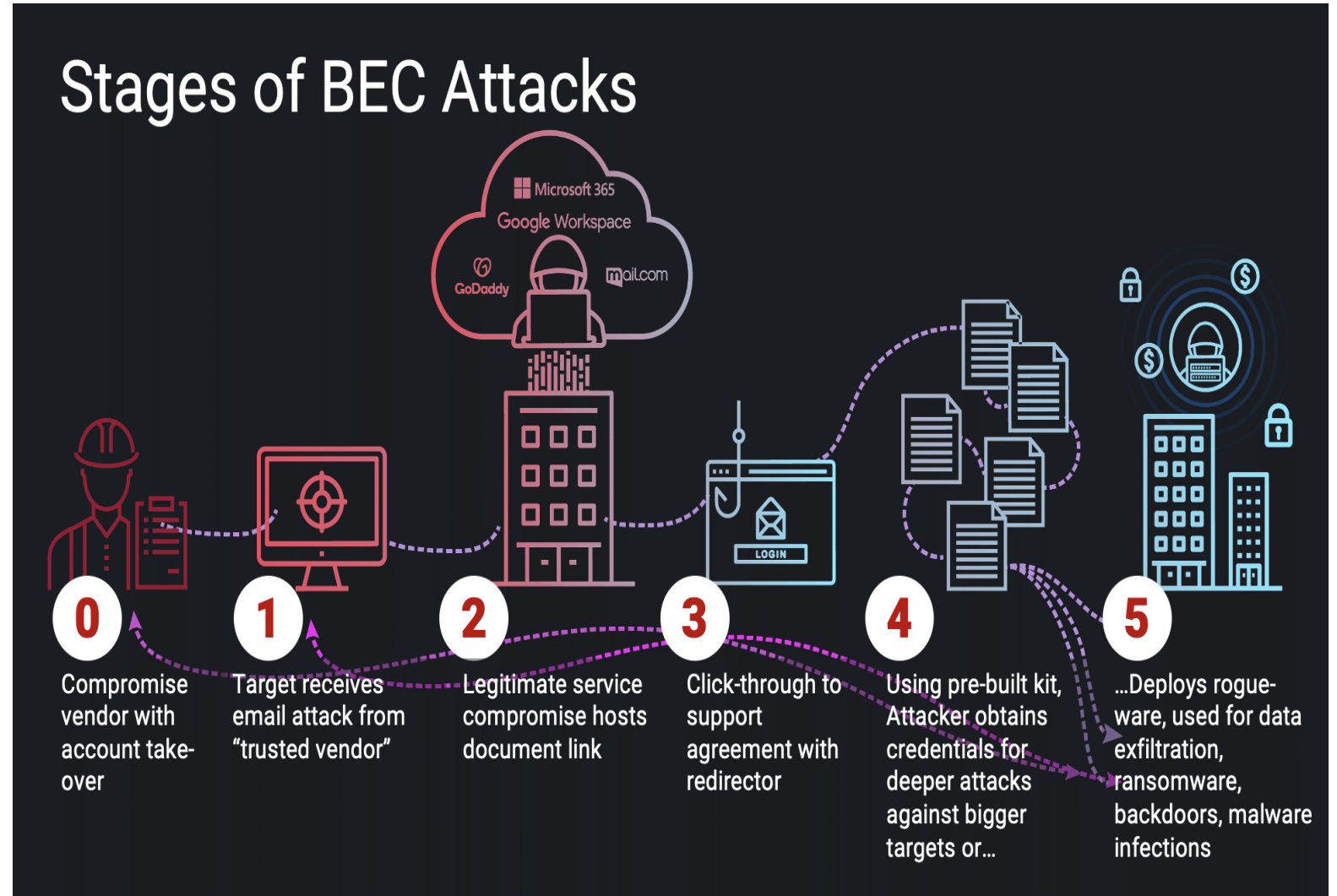
Antivirus software and other security software must be kept up to date to keep pace with the ever-changing threat landscape

Poor or lack of vendor risk management

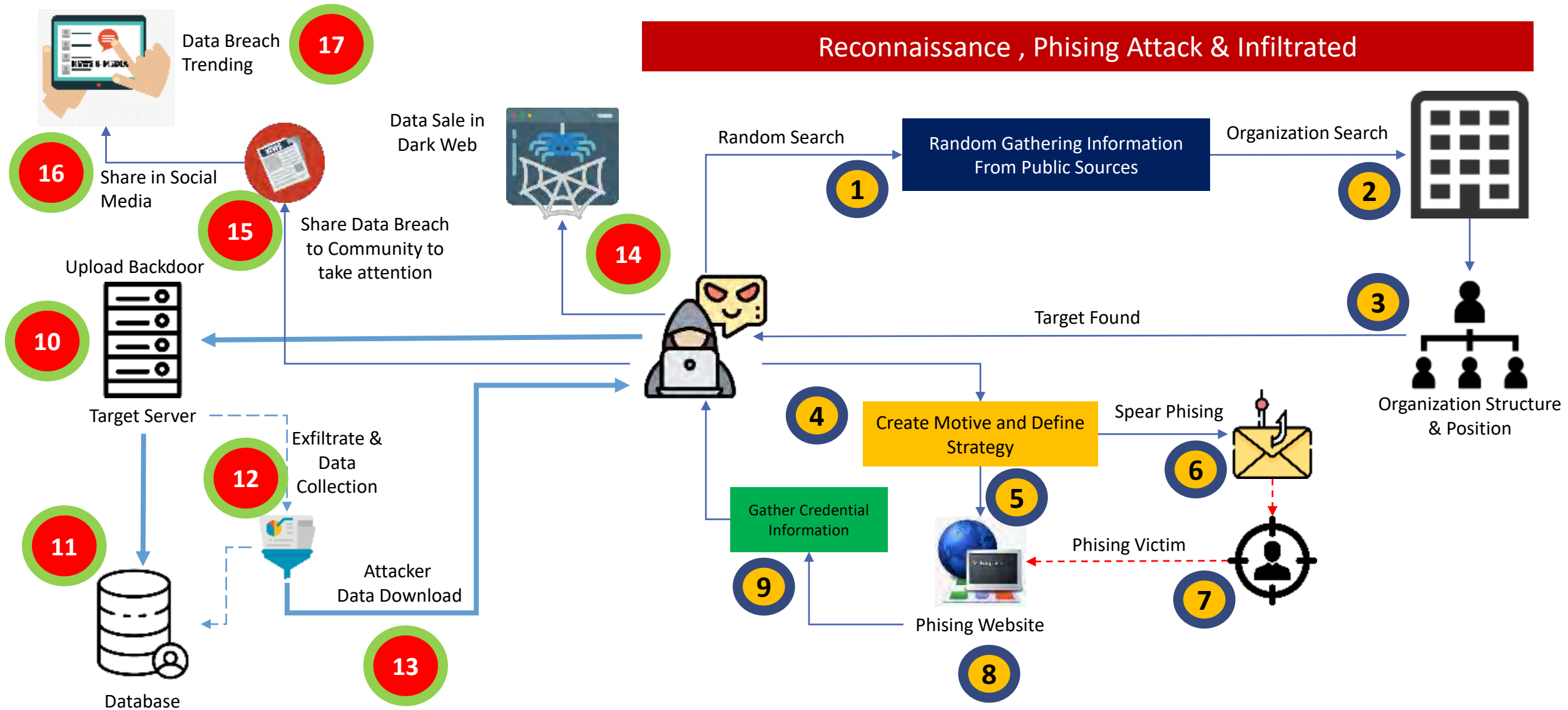
Number of your third-party vendors and service providers have access to your Wi-Fi networks or process sensitive data on your behalf

What is Business Email Compromises (BEC) ?

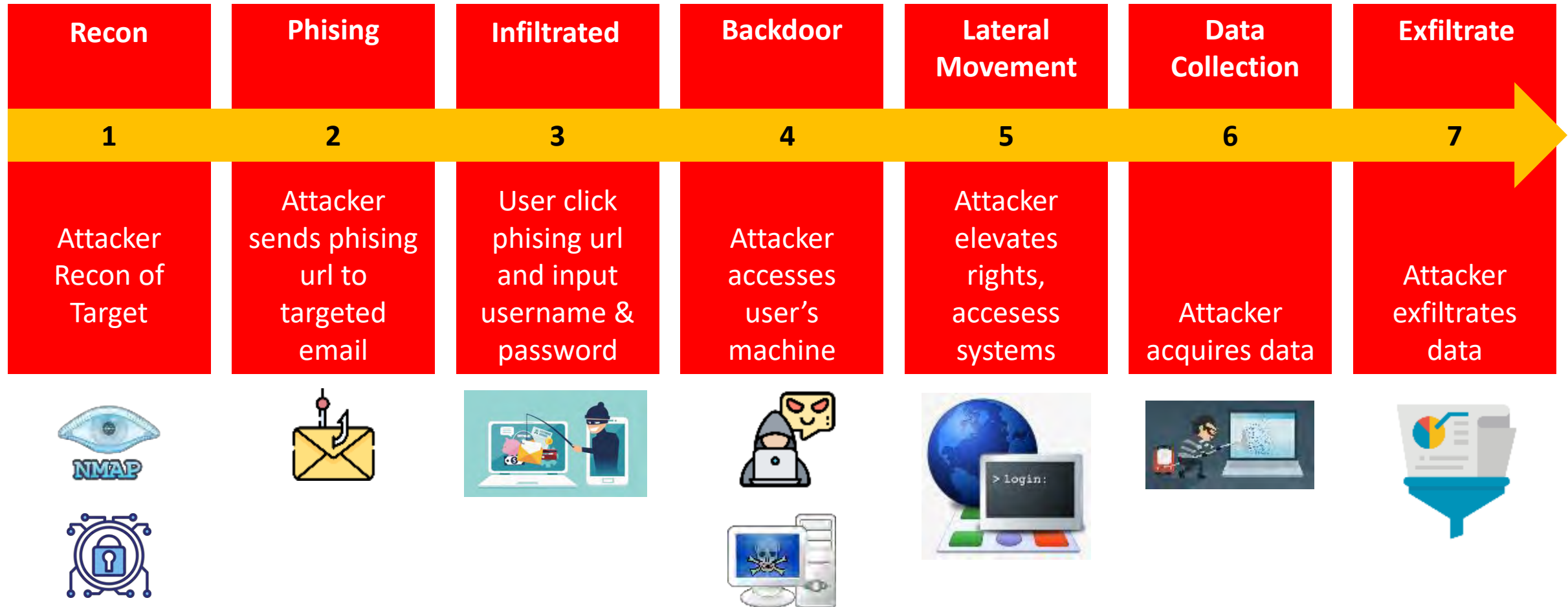
Business email compromise (BEC) is a type of phishing scam targeting companies for financial gain. These scams typically target executive-level employees or individuals involved in finance that could request or initiate wire transfers or other types of money transfer scams. Cybercriminals sometimes spoof an email address with a similar name of an executive or a vendor familiar with the company.



CYBERDRILL EXERCISE



Case Study Cyber Attack Anatomy of Data Breach





TERIMA KASIH