



PRESPEKTIF KEAMANAN SIBER

DARI SUDUT PANDANG BSSN

Badung, 8 Oktober 2021



PUSAT OPERASI KEAMANAN SIBER NASIONAL
NATIONAL CSIRT OF INDONESIA
ID-SIRTI/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE
COORDINATION CENTER



Nama : **Ferdinand Mahulette**
Pangkat : **Brigjen TNI**
NRP : **1900026591265**
Status : **K3**
Jabatan : **Direktur Operasi
Keamanan Siber, BSSN**





Apa itu Cyber

- Dunia cyber (*Cyberspace*) adalah media elektronik dalam jaringan komputer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal-balik secara online.
- Dunia cyber merupakan integrasi dari berbagai peralatan teknologi komunikasi dan jaringan komputer yang dapat menghubungkan peralatan komunikasi yang tersebar di seluruh penjuru dunia secara interaktif.
- Dikarenakan akses media elektronik tanpa batas antara satu sama lainnya, maka rawan untuk terjadinya kejahatan.





PUSAT OPERASI KEAMANAN SIBER NASIONAL
NATIONAL CSIRT OF INDONESIA
Id-SIRTI/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE
COORDINATION CENTER

Cyberspace



PERINTAH PRESIDEN REPUBLIK INDONESIA

“Kita harus siaga menghadapi ancaman kejahatan siber, termasuk kejahatan penyalahgunaan data.”

Data adalah jenis kekayaan baru bangsa kita, kini data lebih berharga dari minyak. Dalam bidang pertahanan keamanan, kita juga harus tanggap dan siap menghadapi perang siber”



PERUBAHAN ANCAMAN NEGARA

KONVENSIIONAL = INVASI MILITER



- **Biaya Mahal**
- **Dikutuk Komunitas Dunia**
Contoh: Perang Vietnam, Irak dan Afghanistan

ANCAMAN BARU = LEBIH FATAL



Terorisme, Narkoba, Human Trafficking, dsb.



Radikalisme, Separatisme, pornografi



Illegal Lodging, Illegal Fishing,



Serangan Cyber, Kartel, Mafia perdagangan

MULTI DIMENSI DAN MELIPUTI SELURUH ASPEK KEHIDUPAN

EVOLUSI PEPERANGAN



G-1

Generasi 1
Padat Manusia

(1870 1918)

Generasi 2
Manuver dan
Tembakan

G-2

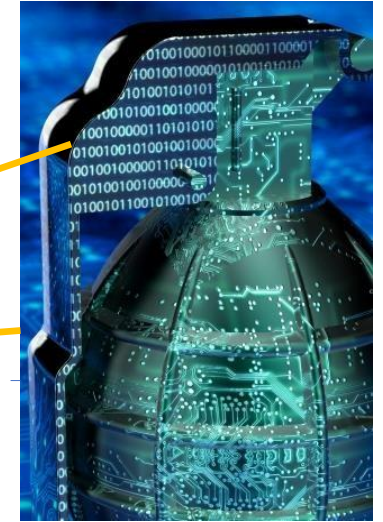
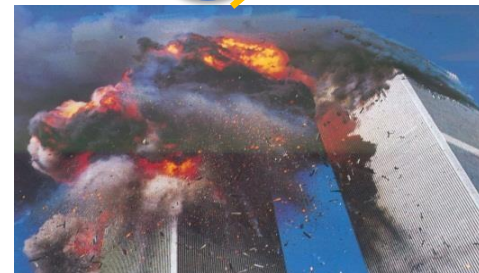


G-3

Generasi 3
Padat Teknologi

Generasi 4
Asimetris

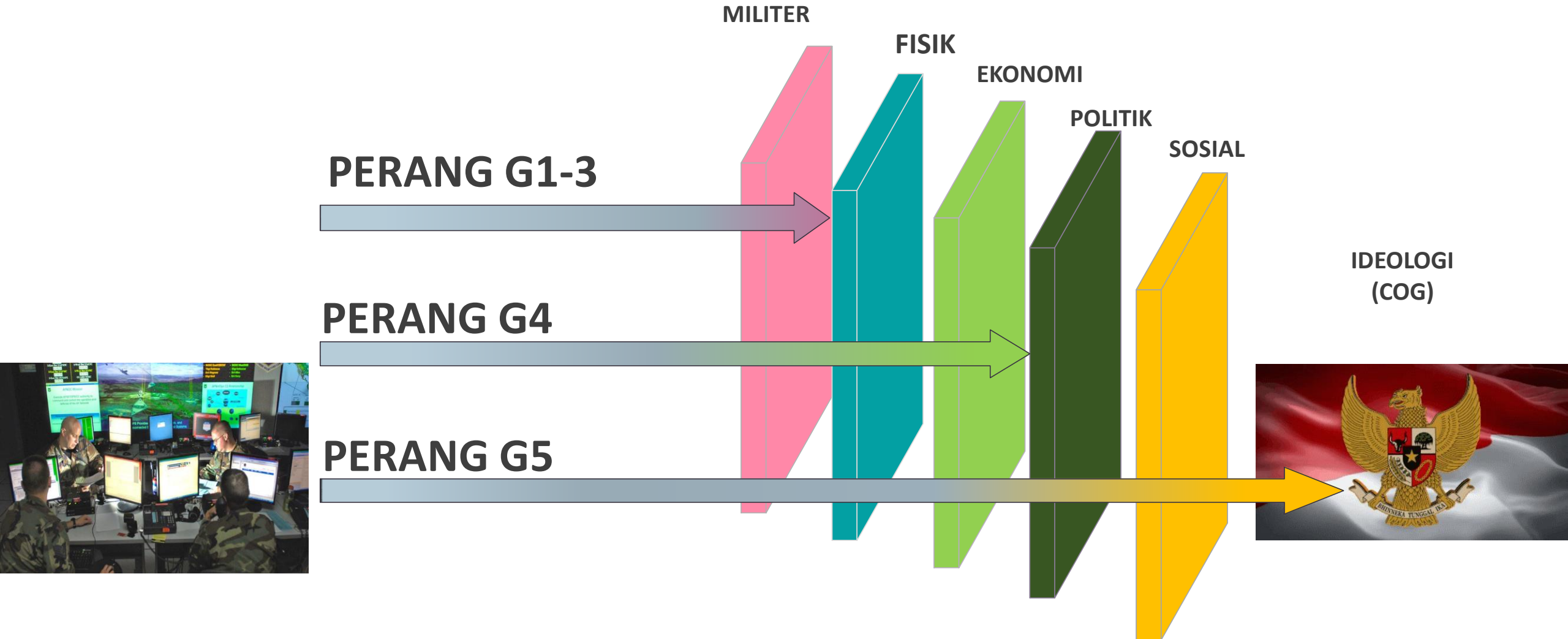
G-4



G-5

Generasi 5
Siber dan Informasi

DAYA TEMBUS STRATEGI SERANGAN SIBER / INFORMASI



SERANGAN SIBER PADA POSITIONAL ASSET

Mengubah Emosi, Sikap, Tingkah Laku, Opini, dan Motivasi



RUANG SIBER INDONESIA

Pembukaan
UUD NRI Tahun 1945

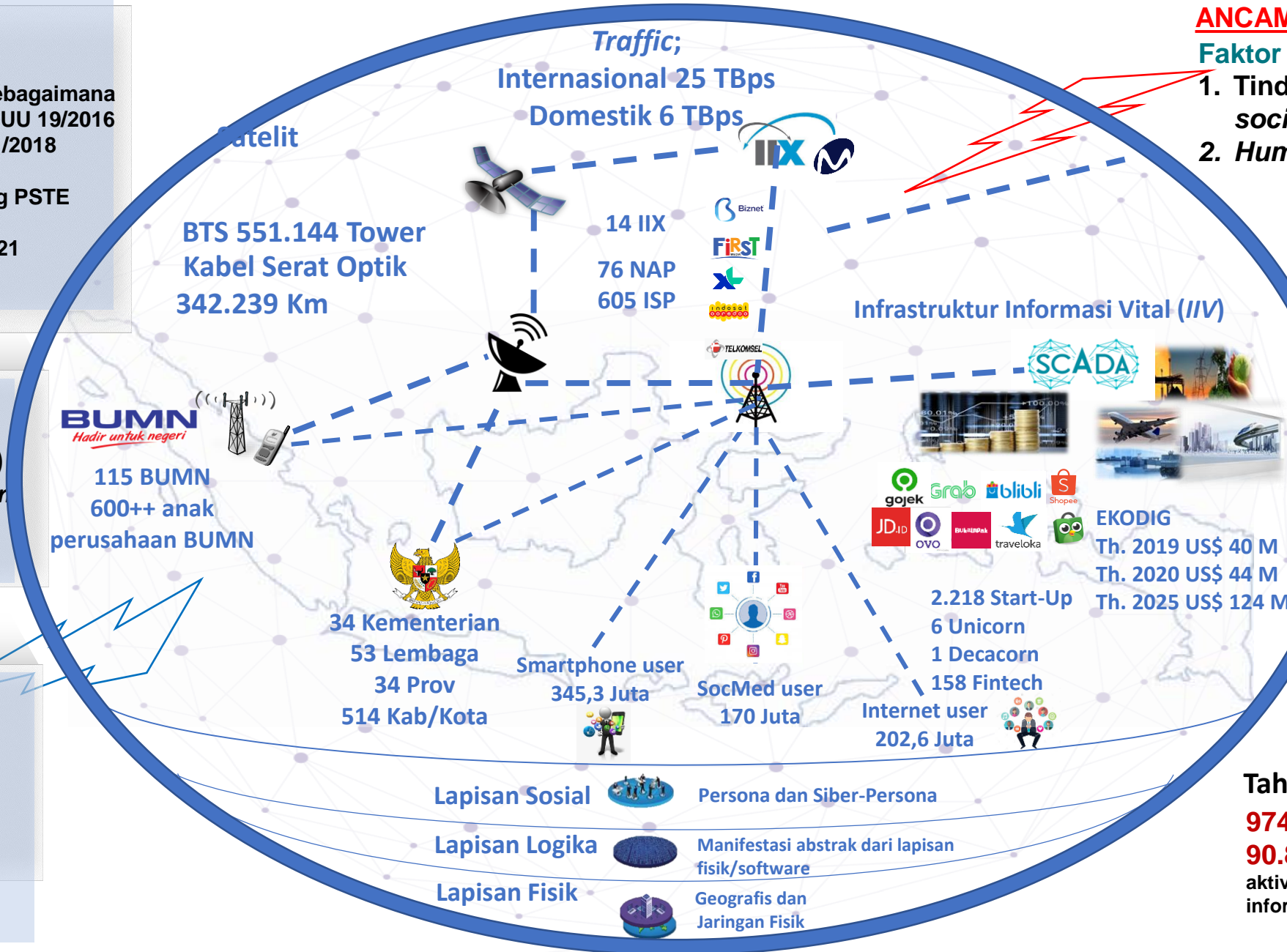
UU 11/2008 ttg ITE sebagaimana
telah diubah dengan UU 19/2016
ttg Perubahan UU 11/2018

PP 71 Tahun 2019 Ttg PSTE

Perpres 28 Tahun 2021
ttg BSSN

National CSIRT
CSIRT Sectoral
(GOV, IIV, EKODIG)
CSIRT Organization
(K/L/D/I)

POLRI
Kejaksaan RI
BNPT
BNN
BIN
TNI
KEMHAN
KEMENKOMINFO



ANCAMAN PADA RUANG SIBER

Faktor penyebab ancaman siber:

1. Tindak kejahatan (*hacking & social engineering*)
2. Human error

Sifat Serangan

1. Teknis:

- DDoS
- Phishing
- Malware
- Brute Force, dll.

2. Sosial:

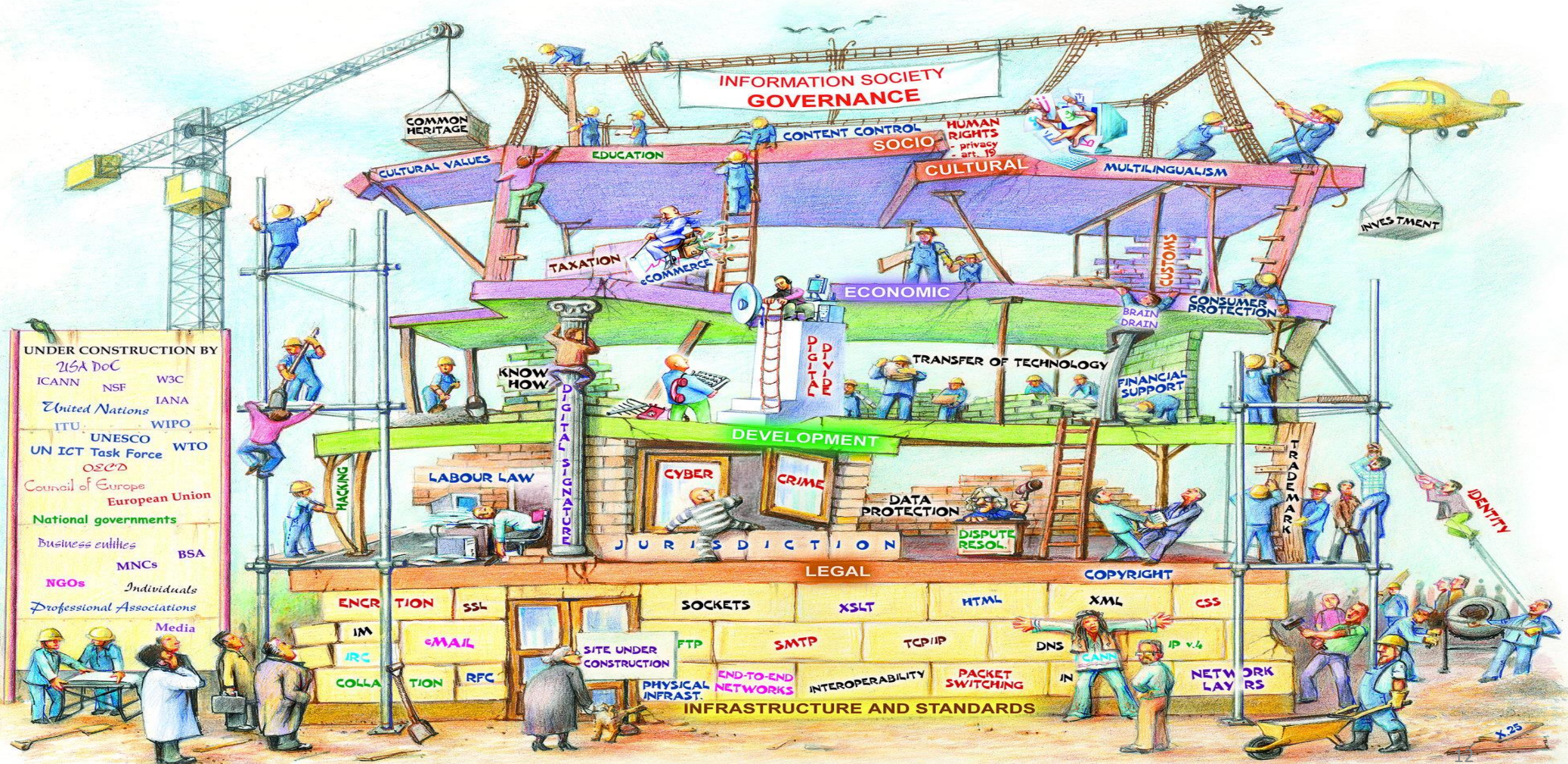
- Propaganda hitam
- Point and shriek
- Pembajakan informasi, dll.

Tahun 2020 : ± 495 juta

9749 Kasus peretasan situs

90.887 Kebocoran data dari aktivitas *malware* pencuri informasi di Indonesia

Cyber Security Master Plan ???



Manfaat Siber

- ✓ 2.218 Start-Up
- ✓ 6 Unicorn
- ✓ 1 Decacorn
- ✓ 158 Fintech

EKODIG

- ✓ Th. 2019 US\$ 40 M
- ✓ Th. 2020 US\$ 44 M
- ✓ Th. 2025 US\$ 124 M

Kejahatan Siber



DUA SISI MATA UANG



Prinsip Penting Keamanan Siber

1. In IT, everything is evolving

- ✓ Space
- ✓ Connectivity
- ✓ Potential benefit
- ✓ Threat

2. IT / ICT - 2 Sisi Mata Uang

- | | |
|------------------|-----------------------|
| ✓ 2.218 Start-Up | EKODIG |
| ✓ 6 Unicorn | ✓ Th. 2019 US\$ 40 M |
| 1 Decacorn | ✓ Th. 2020 US\$ 44 M |
| ✓ 158 Fintech | ✓ Th. 2025 US\$ 124 M |

3. Threat follow asset, Attack follow vulnerability

4. Everything is recorded and trackable

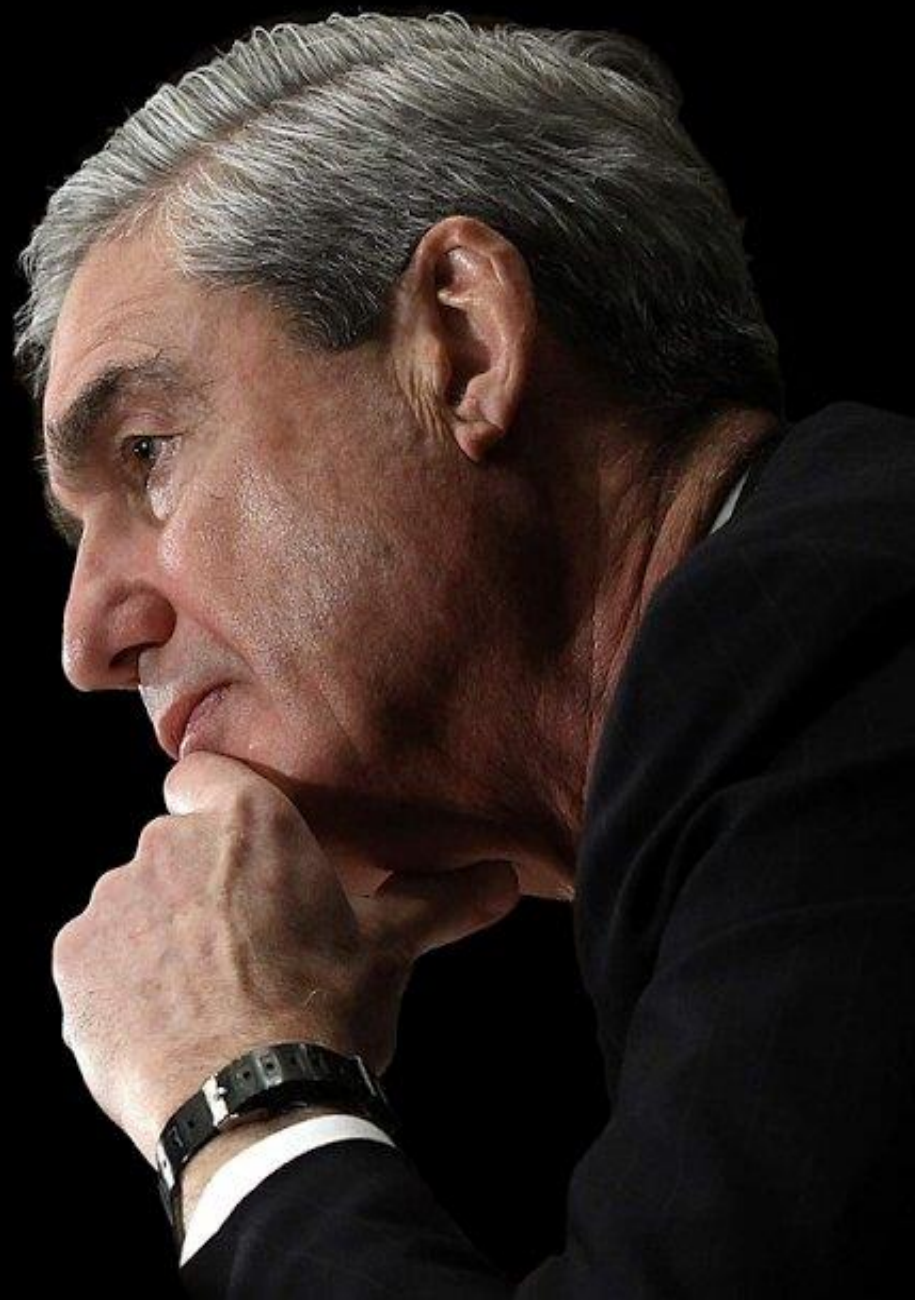
5. No 100% protection

6. Empowering PPT

- ✓ PEOPLE – aware people
- ✓ PROCESS -- standard process
- ✓ TECHNOLOGY -- trusted technology

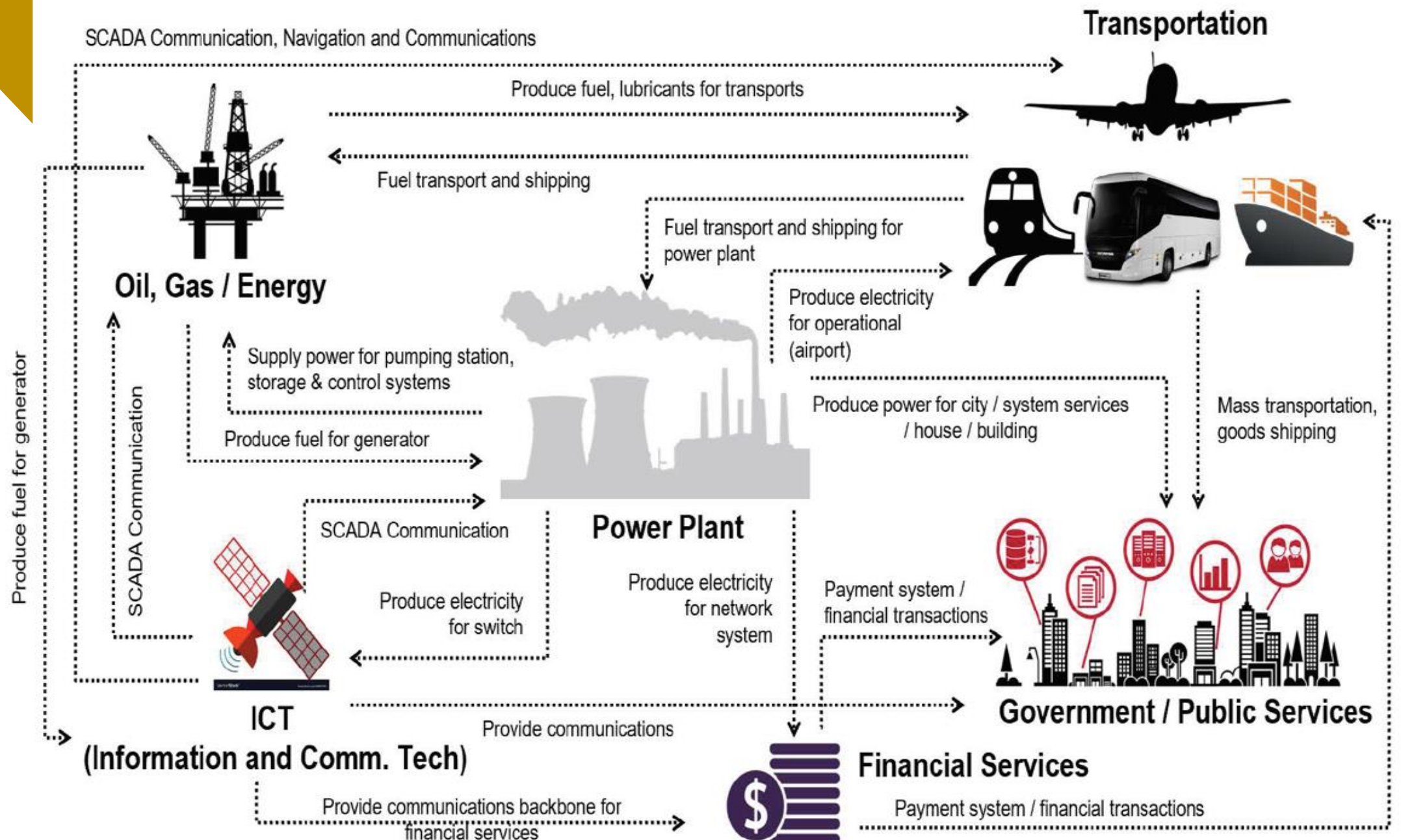
***“There are only two types of companies:
those that have been hacked,
and those that will be.”***

*Robert Mueller
FBI Director, 2001-2013*





Interdependensi Sektor Infrastruktur Informasi Vital (IIV)





BADAN SIBER DAN SANDI NEGARA

TANTANGAN KEAMANAN SIBER 2021



**ISU KEAMANAN PENGGUNAAN
PERANGKAT PRIBADI**



**PEKERJA REMOTE TETAP
MENJADI TARGET UTAMA
PENYERANG**



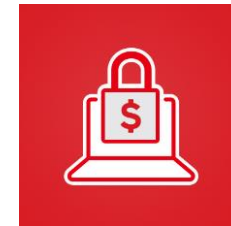
**ISU KEAMANAN DATA PADA
TRANSORMASI DIGITAL**



**MALWARE INFO STEALER (TETAP
MENINGKAT)**



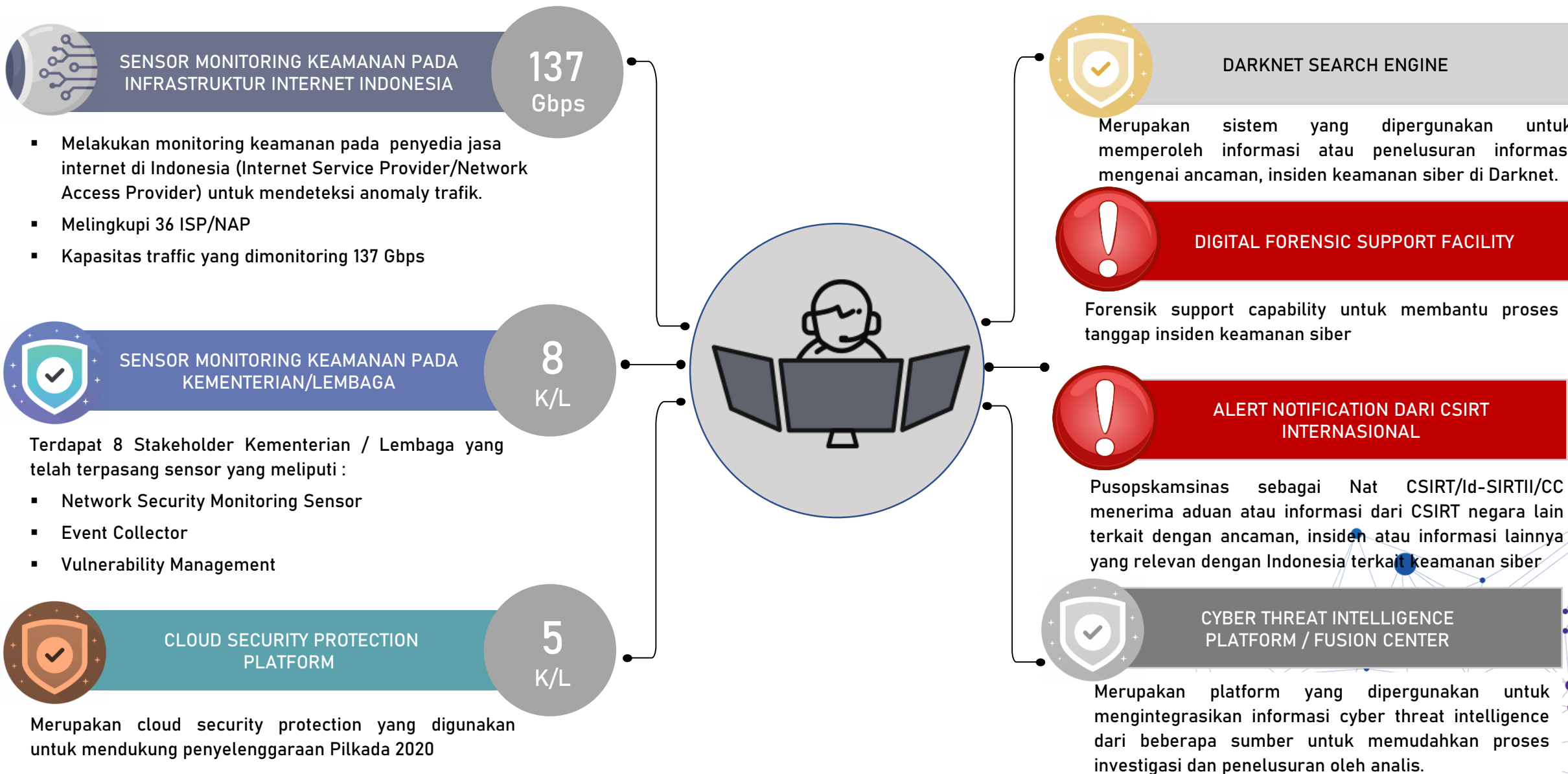
**DATA TETAP MENJADI KOMODITI
YANG DIINCAR OLEH PENYERANG**



**RANSOMWARE DOUBLE
EXTORTION
(RANSOM, LEAK, & AMPLIFY)**



SISTEM MONITORING KEAMANAN SIBER NASIONAL



URGENSI SISTEM MONITORING KEAMANAN SIBER NASIONAL



PUSAT OPERASI KEAMANAN SIBER NASIONAL
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE
COORDINATOR CENTER

Pendekatan Keamanan Kolaboratif

Why?
PERKEMBANGAN
ANCAMAN
SEMAKIN
KOMPLEKS DAN
SERANGAN SIBER
SEMAKIN MASIF

How?
PEMBANGUNAN
MEKANISME
KEAMANAN
KOLABORATIF

What?
BERBAGI
INFORMASI
ANCAMAN
KEAMANAN
SIBER

Meningkatkan postur keamanan dan ketahanan siber

Membangun kapabilitas bersama

Meningkatkan kemampuan bertahan secara proaktif.

Mengetahui Gambaran Komprehensif Mengenai Ancaman Siber Tingkat Nasional

Monitoring Trafik Internet Nasional

Gambaran Utuh Ancaman dan Serangan Siber di Indonesia

ISP

IKN

PEMERINTAH

PUBLIK

MSSP

TIM KOORDINASI SPBE

- ❖ Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik
- ❖ Permenpanrb Nomor 5 Tahun 2018 tentang Pedoman Evaluasi Sistem Pemerintahan Berbasis Elektronik



Website: www.bssn.go.id



Profesional



INtegritas



adapTAbilitas teknologi



tepeRcaya



BADAN SIBER DAN SANDI NEGARA



Peran BSSN dalam SPBE Nasional

PERPRES NO 95 TAHUN 2018

SPBE

UNSUR SPBE

1. Rencana Induk SPBE Nasional
2. Arsitektur
3. Peta Rencana
4. Rencana dan Anggaran
5. Proses Bisnis
6. Data dan Informasi
7. Infrastruktur
8. Aplikasi
9. Keamanan
10. Layanan

1 ARSITEKTUR SPBE NASIONAL

BSSN bertanggung jawab dalam penyusunan domain arsitektur keamanan SPBE

2 INFRASTRUKTUR SPBE NASIONAL

Memberikan pertimbangan kelaikan keamanan dalam pembangunan Pusat Data Nasional/Sementara, Jaringan Intra Pemerintah, dan Sistem Penghubung Layanan

3 AUDIT KEAMANAN SPBE

- Melakukan Audit Keamanan pada Infra SPBE Nasional dan Aplikasi Umum.
- Menyusun Standar dan tata laksana audit keamanan SPBE

4 MANAJEMEN KEAMANAN SPBE

- Melaksanakan Manajemen Keamanan Informasi, KLDI dapat berkonsultasi dengan BSSN
- Menyusun pedoman Manajemen Keamanan Informasi SPBE

5 KEAMANAN SPBE

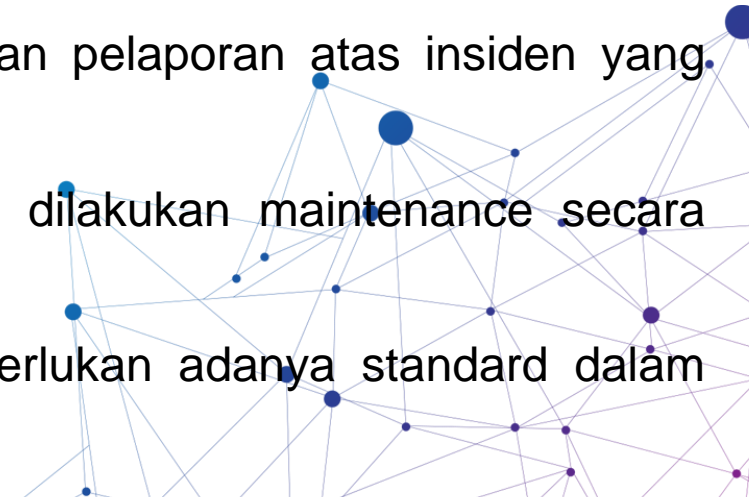
- Penerapan Keamanan SPBE dan penyelesaian permasalahan Keamanan SPBE, KLDI berkoordinasi dan berkonsultasi dengan BSSN
- Menyusun standar teknis dan prosedur keamanan SPBE

TANTANGAN PENYELESAIAN PENANGANAN INSIDEN



DIREKTORAT OPERASI KEAMANAN SIBER
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE
COORDINATION CENTER

- Tidak semua institusi memiliki Tim Tanggap Insiden sendiri, sehingga notifikasi yang disampaikan responsnya bervariasi.
- Pada kasus tertentu, institusi lebih cenderung tertutup atau melakukan penanganan insiden secara mandiri. Sehingga situational awareness yang diharapkan dari lesson learned proses tanggap insiden pemangku kepentingan yang terdampak belum dapat terbangun dengan baik.
- Penyelesaian kasus peretasan kecenderungannya hanya mengembalikan ke halaman situs sebelumnya, namun tidak dilakukan secara tuntas.
- Kendala birokrasi dalam proses tanggap insiden, dikarenakan insiden terjadi pada unit kerja yang berbeda.
- Belum ada payung hukum/regulasi yang bersifat mewajibkan untuk melakukan pelaporan atas insiden yang terjadi atau perkembangan penanganan insiden yang terjadi.
- Sistem Elektronik yang terdampak telah habis masa supportnya atau tidak dilakukan maintenance secara mandiri, sehingga terkendala dalam proses perbaikan.
- Log yang diperlukan dalam proses tanggap insiden tidak ada sehingga diperlukan adanya standard dalam logging terhadap sistem elektronik untuk mendukung tanggap insiden.



Insiden Ransomware pada Colonial Pipeline



Colonial Pipeline merupakan sebuah perusahaan bahan bakar yang bertanggung jawab terhadap hampir separuh pasokan bahan bakar untuk wilayah pantai timur Amerika Serikat.

- 6 Mei 2021, Grup Hacker melakukan pencurian lebih dari 100GB data sebelum melakukan serangan ransomware
- 7 Mei 2021, sebuah serangan ransomware memaksa Colonial Pipeline untuk menghentikan operasinya guna mencegah kerusakan yang lebih luas
- 8 Mei 2021, colonial Pipeline membayar 75 Bitcoin atau setara 5 Juta USD ke Pelaku Serangan
- 9 Mei 2021, Presiden Joe Biden menyatakan kondisi darurat terkait dengan insiden siber ini.
- 10 Mei 2021, FBI mengkonfirmasi bahwa pelaku serangan adalah Grup DARKSIDE ransomware
- 11 Mei 2021, Colonial Pipeline website offline
- 13 Mei 2021, Grup DARKSIDE mengklaim bahwa sebagai infrastruktur mereka dilumpuhkan oleh aparat penegak hukum yang belum diketahui asalnya



SITUASI KEAMANAN SIBER NASIONAL

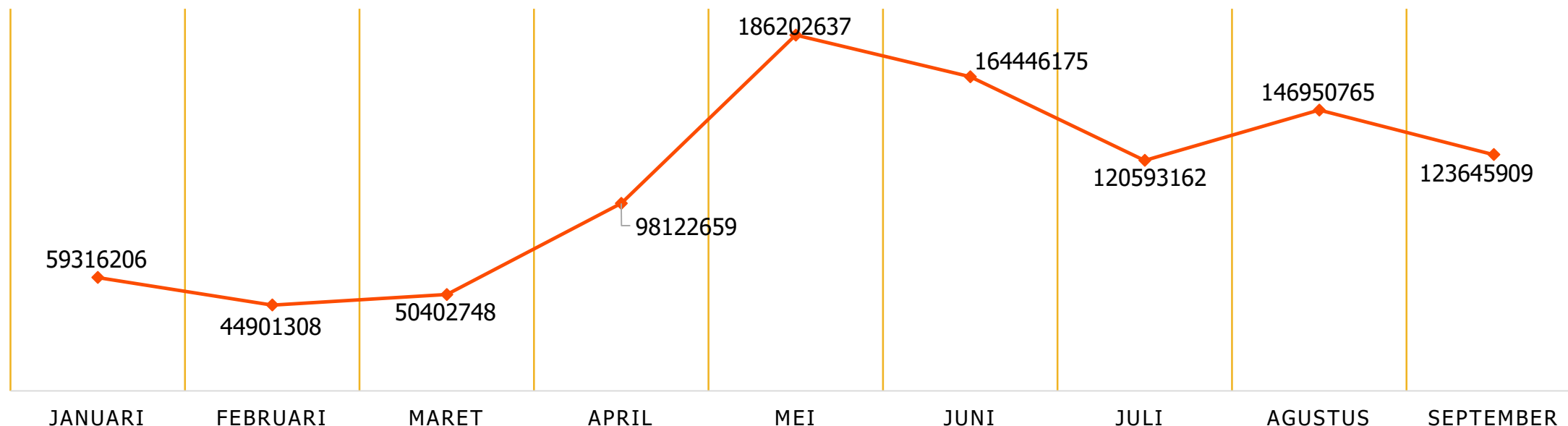
Januari sd September 2021



PUSAT OPERASI KEAMANAN SIBER NASIONAL
NATIONAL CSIRT OF INDONESIA

Id-SIRTI/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE
COORDINATION CENTER

Total Anomali Trafik



994.581.569

ANOMALI TRAFIK/SERANGAN SIBER
DI TAHUN 2021 (1 Januari – 30 September)

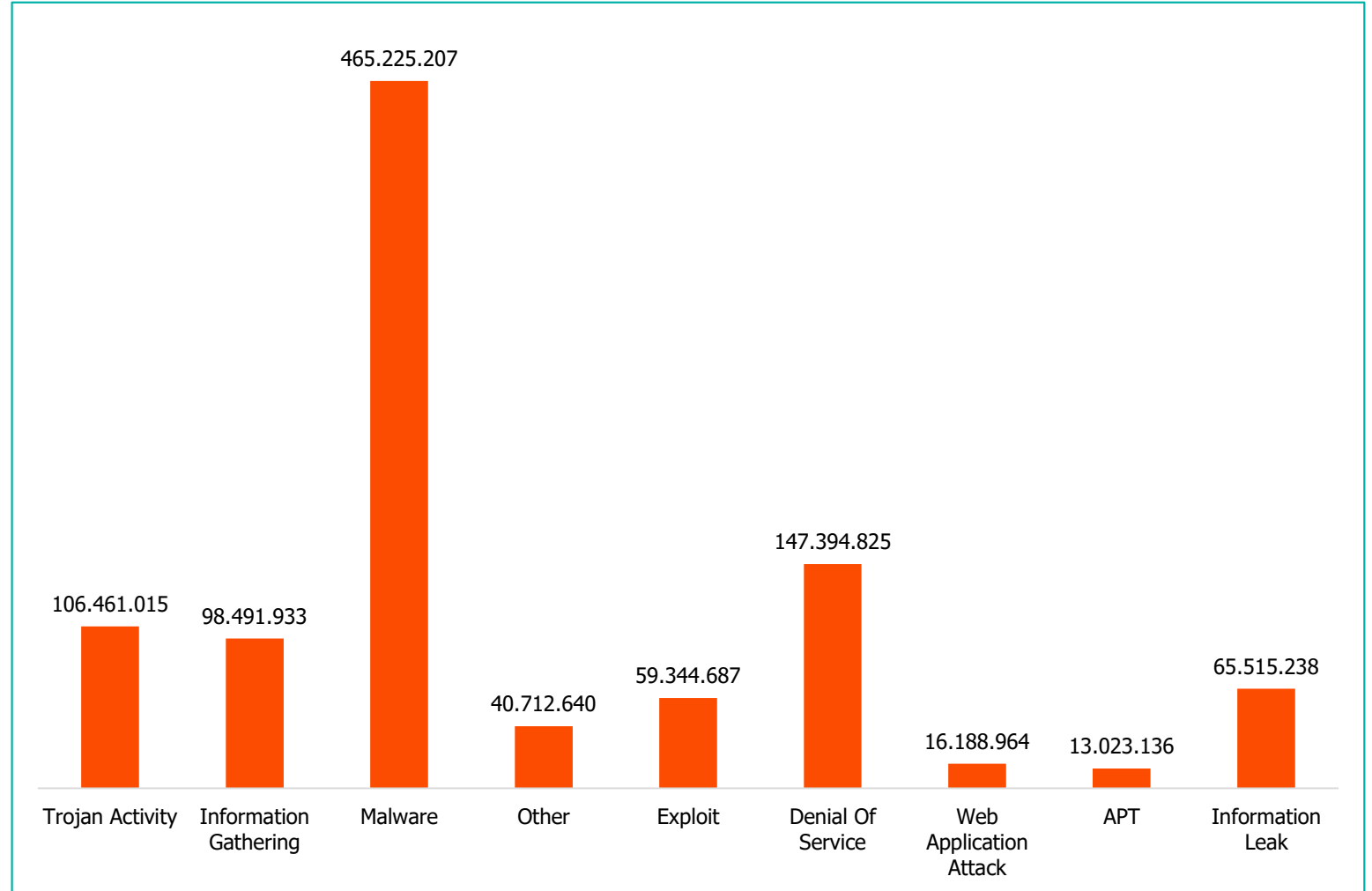
Direktorat Operasi Keamanan Siber BSSN melakukan monitoring serangan siber terhadap Indonesia selama 7/24 jam. Berdasarkan statistik hasil monitoring yang dilakukan mulai 1 Januari 2021 pukul 00:00:00 hingga 30 September 2021 pukul 23:59:59, anomaly trafik tertinggi terjadi pada bulan **Mei 2021** dengan jumlah mencapai **186.202.637** anomali.



■ Top Kategori Anomali Trafik

➤ Januari – September 2021

- **Malware** menjadi anomali dengan **jumlah tertinggi** selama bulan Januari hingga September 2021.
- **Malware** merupakan perangkat lunak yang dibuat dan bertujuan untuk memasuki dan merusak sistem tanpa diketahui oleh pemiliknya.
- **Malware** biasanya digunakan untuk mencuri data di dalam sistem, memanipulasi data, atau memata-matai sistem yang telah disusupi. Kebanyakan malware didistribusikan melalui email, pesan pribadi, maupun situs web.



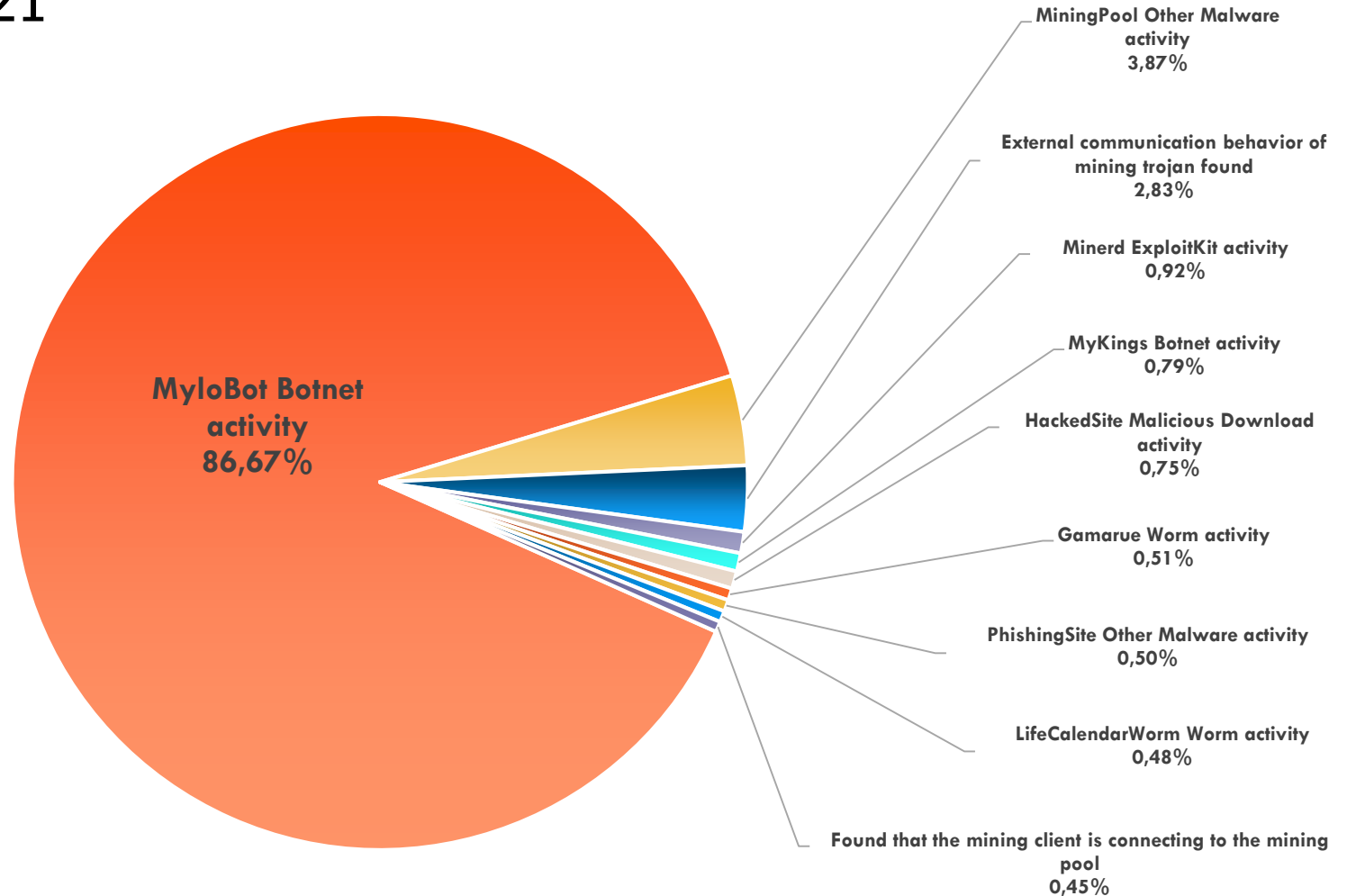
■ Top 10 Jenis Malware

• Januari – September 2021

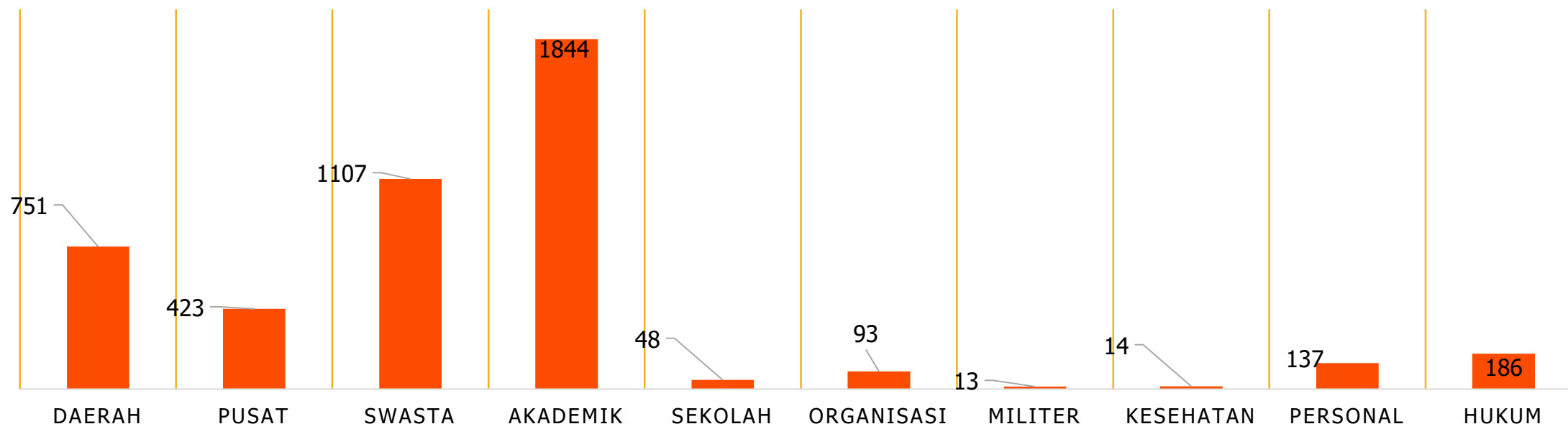
MyloBotnet

Hasil monitoring BSSN menunjukkan bahwa *malware* yang paling banyak digunakan dalam serangan siber selama Januari – Mei 2021 adalah berjenis MyloBotnet.

MyloBotnet memiliki kemampuan teknik untuk menghindari deteksi dari perangkat keamanan seperti anti-virus, dan dapat menonaktifkan "Windows Defender" dan memblokir port pada *firewall*.



Tren Serangan Siber di Indonesia

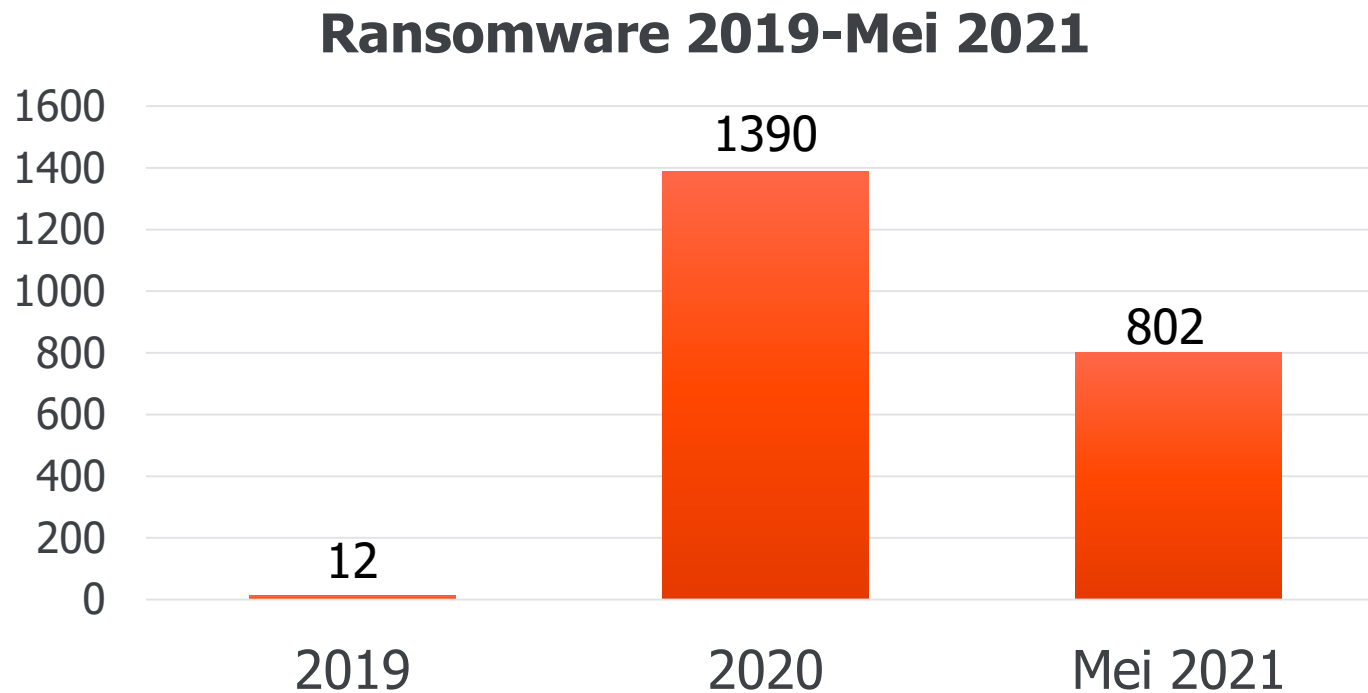


4.616
INSIDEN WEB DEFACEMENT
DI TAHUN 2021 (1 Januari – 30 September)

- Subdomain website fakultas dan Lembaga di **sektor akademik** memiliki intensitas serangan *defacement* **paling banyak** pada tahun 2021 (Januari – 30 September 2021)
- Subdomain di **sektor swasta** memiliki intensitas serangan *defacement* **paling banyak kedua** pada tahun 2021 (Januari – 30 September 2021)

■ Data Serangan Ransomware

- Berdasarkan publikasi dari akun **@darktracer_int**, telah terdeteksi berbagai serangan grup ransomware sepanjang tahun 2019 sampai dengan Bulan Mei tahun 2021 yang terus meningkat, baik jumlah maupun jenis serangannya.



Jenis Grup Ransomware di Seluruh Dunia

- Rekap serangan grup ransomware sepanjang tahun 2019 sampai dengan Mei tahun 2021.

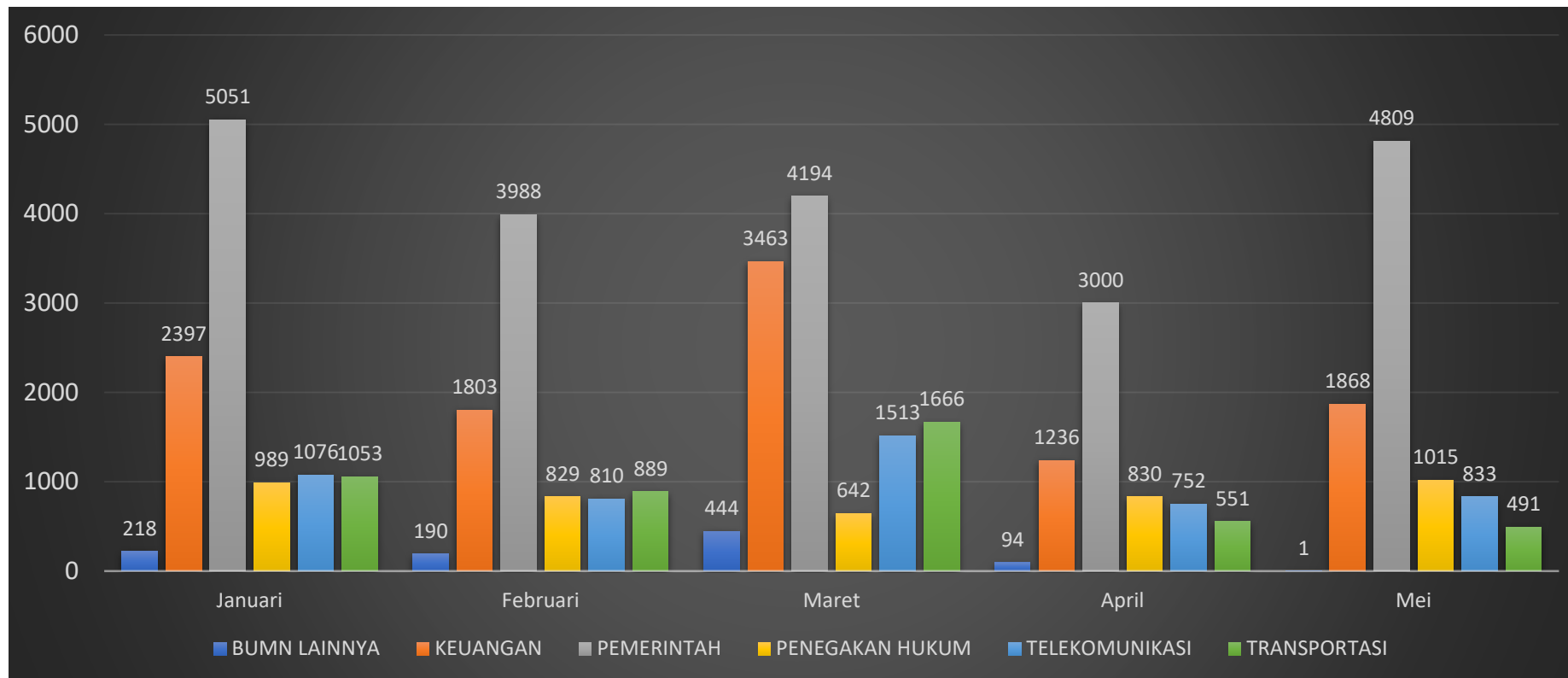
Tahun 2019	
Ransomware Gang	Jumlah
MAZE	6
Team Snatch	6
Total	12

Tahun 2020	
Ransomware Gang	Jumlah
AKO	9
Avaddon	21
CL0P	21
Conti	188
Cuba	1
DarkSide	24
DoppelPaymer	140
Egregor	206
Everest	21
LockBit	8
Lorenz	1
MAZE	260
Mount Locker	12
Nefilim	23
NEMTY	1
NetWalker	122
Pay2Key	6
Pysa	122
Ragnar_Locker	20
Ragnarok	10
RansomEXX	7
Ranzy Locker	3
Sekhmet	6
Sodinokibi (REvil)	138
Suncrypt	20
Total	1390

Mei 2021	
Ransomware Gang	Jumlah
Astro Team	16
Avaddon	114
BABUK LOCKER	43
CL0P	44
Conti	153
Cuba	8
DarkSide	75
DoppelPaymer	60
Everest	11
File Leaks	6
LockBit	1
Lorenz	11
LV	27
Marketo	16
Mount Locker	8
N3twOrm	3
Nefilim	13
NetWalker	22
Noname	3
Pysa	28
Ragnar_Locker	4
Ragnarok	23
RansomEXX	12
Sodinokibi (REvil)	89
Suncrypt	2
XING LOCKER	10
Total	802

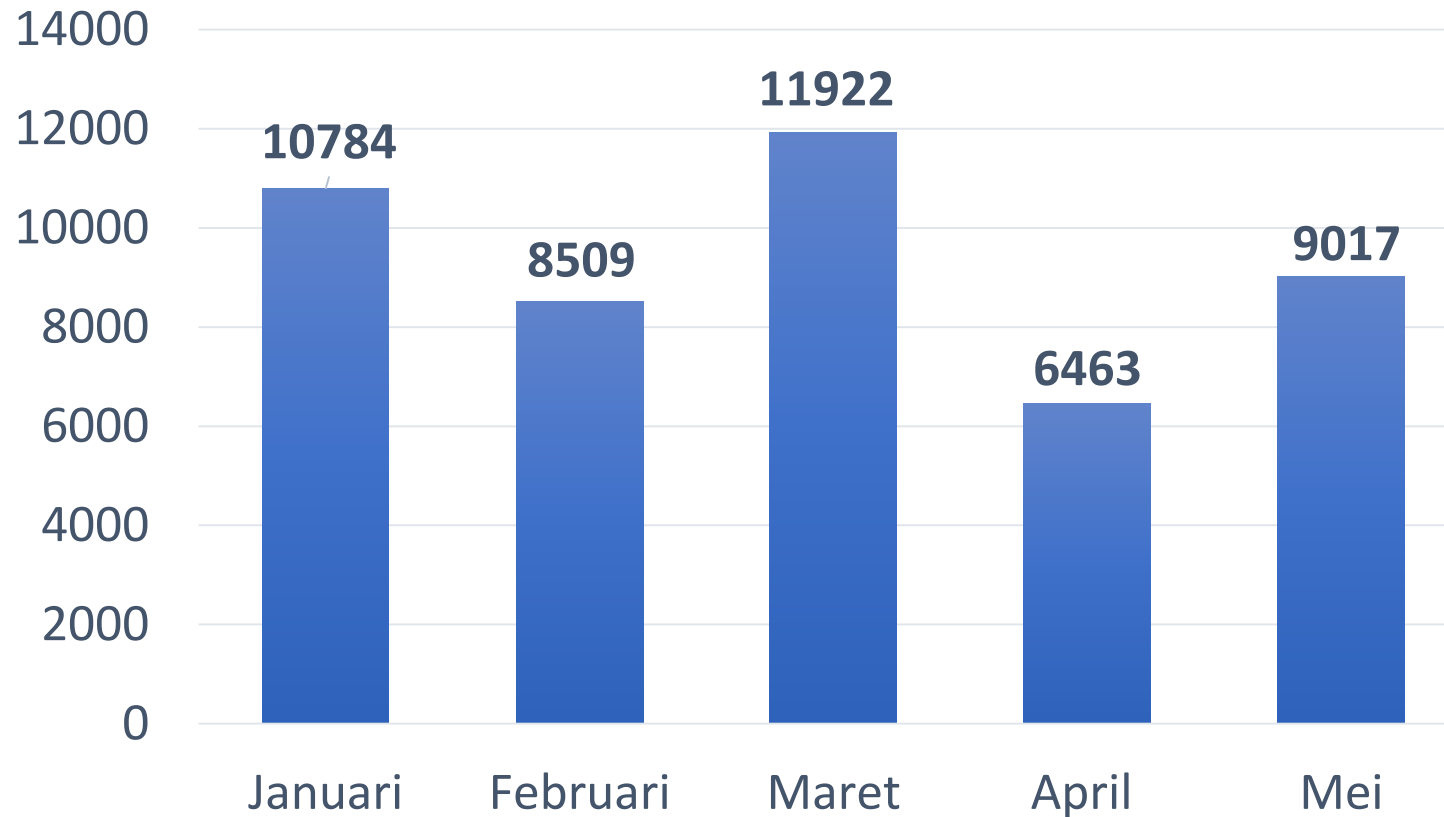
■ Compromised Account 2021

- Data jumlah compromised Account beberapa instansi yang terdeteksi oleh Threat Intelligence Platform yang dimiliki oleh Direktorat Operasi Keamanan Siber.
- Compromised Account tersebut sebagian besar disebabkan oleh Malware Information Stealer, atau didapatkan dari data broker.



Data Breach

JUMLAH KEBOCORAN AKUN TIAP BULAN YANG MENGALAMI INSIDEN DATA BREACH TAHUN 2021

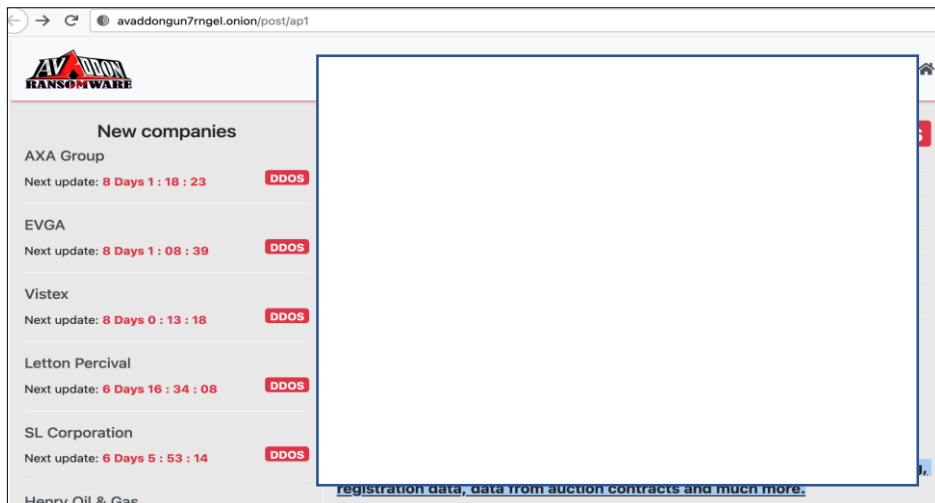


Total Data Breach

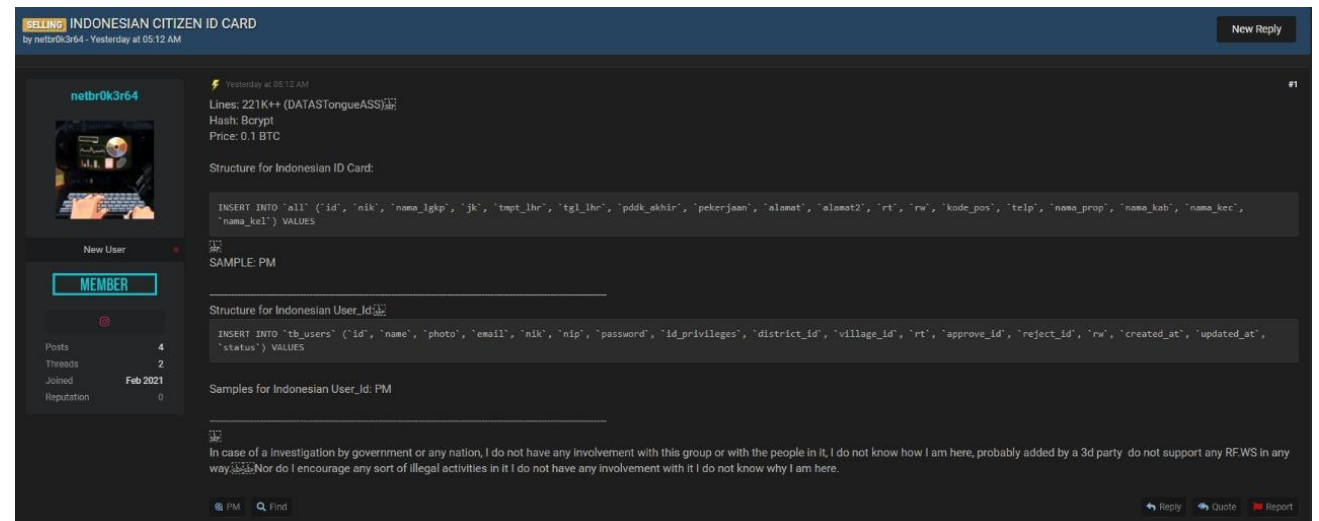
46.695

Tren Serangan Siber

Berdasarkan penelusuran Pusopskamsinas BSSN sepanjang tahun 2021, serangan siber yang menjadi perhatian dan terus mengalami peningkatan yaitu banyaknya **serangan grup ransomware** serta **data leaks** yang dilakukan oleh *threat actor* yang mayoritas dilatar belakangi oleh motif untuk mendapatkan keuntungan finansial.



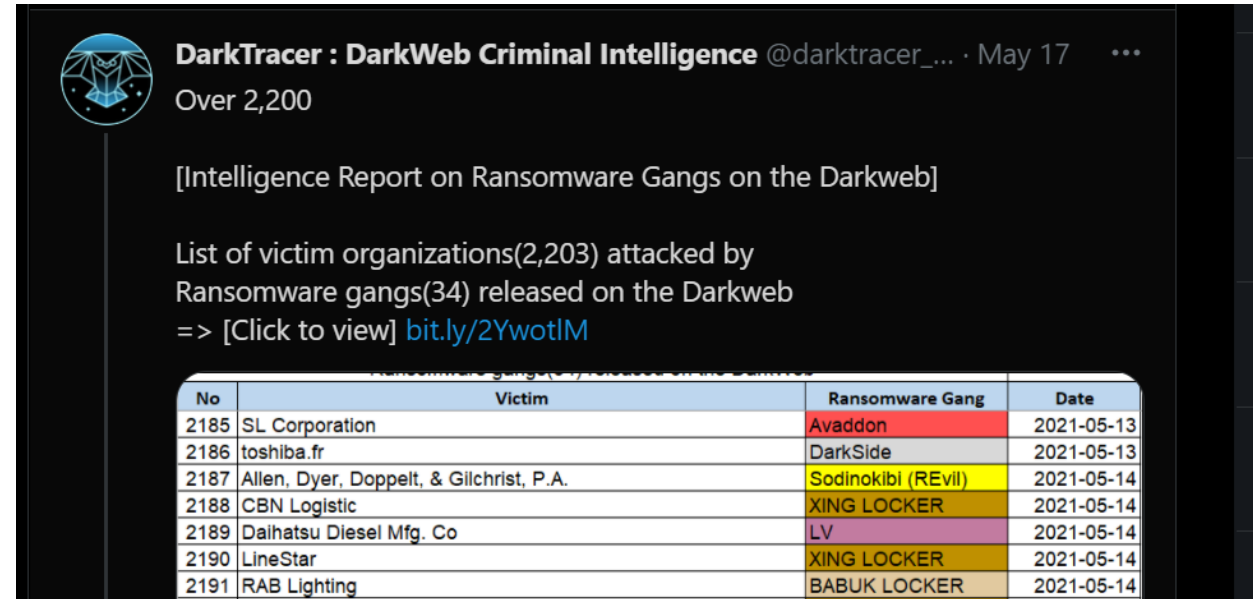
Serangan ransomware dilakukan dengan cara mengenkripsi file milik korban dan meminta sejumlah tebusan. Pelaku menjanjikan korban akan mendapatkan kunci dekripsi untuk membuka file tersebut, dan apabila korban tidak membayar, maka data akan dipublikasi.



Insiden data leaks banyak ditemukan telah di beberapa forum *deepweb* (seperti Raidforums), di mana data dijual-belian atau dipublikas. Biasanya pelaku mempublikasi data tersebut hanya berupa sampelnya saja. Sedangkan untuk mendapatkan keseluruhan data, kita harus membayarkan sejumlah uang / membeli dalam bentuk *bitcoin*.

Tren Ransomware

- BSSN melalui Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) menemukan informasi banyaknya serangan **Ransomware** yang menargetkan berbagai sektor di seluruh dunia.
- Serangan ransomware ini juga telah di publikasi oleh sebuah akun Twitter **@darktracer_int** (**DarkTracer : DarkWeb Criminal Intelligence**). @darktracer_int ini merupakan akun yang memiliki focus penelusuran terkait *Darkweb Criminal Intelligence Profiling Investigation*.
- Berdasarkan data yang dipublikasi akun ini pada tanggal 17 Mei 2021, terdapat 2203 instansi telah mengalami serangan dari **34 jenis Ransomware** yang terdeteksi diseluruh dunia.



DarkTracer : DarkWeb Criminal Intelligence @darktracer_... · May 17 · ...
Over 2,200

[Intelligence Report on Ransomware Gangs on the Darkweb]

List of victim organizations(2,203) attacked by Ransomware gangs(34) released on the Darkweb
=> [Click to view] bit.ly/2YwotlM

No	Victim	Ransomware Gang	Date
2185	SL Corporation	Avaddon	2021-05-13
2186	toshiba.fr	DarkSide	2021-05-13
2187	Allen, Dyer, Doppelt, & Gilchrist, P.A.	Sodinokibi (REvil)	2021-05-14
2188	CBN Logistic	XING LOCKER	2021-05-14
2189	Daihatsu Diesel Mfg. Co	LV	2021-05-14
2190	LineStar	XING LOCKER	2021-05-14
2191	RAB Lighting	BABUK LOCKER	2021-05-14

Sumber:
https://twitter.com/darktracer_int/status/1394189875096657921



PUSAT OPERASI KEAMANAN SIBER NASIONAL
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE
COORDINATION CENTER

***“(Ingatlah) Kechilafan
Satu Orang Sahaja Tjukup
Sudah Menjebabkan
Keruntuhan Negara”***



Mayjen TNI Dr. Roebiono Kertopati
(1914 - 1984)
Bapak Persandian Republik Indonesia



PUSAT OPERASI KEAMANAN SIBER NASIONAL
NATIONAL CSIRT OF INDONESIA

Id-SIRTI/CC

INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE
COORDINATION CENTER

Terima Kasih

Pusopskamsinas BSSN

