



KEMENTERIAN HUKUM REPUBLIK INDONESIA
PUSAT DATA DAN TEKNOLOGI INFORMASI

Jalan H.R. Rasuna Said Kav. 6-7, Kuningan, Jakarta Selatan (Kotak Pos 46)
Telepon: (021) 5253004, Faksimile: (021) 5263082
Laman: <https://pusdatin.kemenkum.go.id>, Pos-el: pusdatin@kemenkum.go.id

Nomor : SEK.7-TI.06.01-11 25 Juni 2025
Sifat : Sangat Segera
Lampiran : Satu berkas
Hal : Penyampaian Hasil Monitoring Anomali Trafik
pada Jaringan Pusat Data Kementerian Hukum

Yth. Daftar Nama Terlampir
di tempat

1. Rujukan:

- a. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
 - b. Peraturan Presiden Republik Indonesia Nomor 155 Tahun 2024 tentang Kementerian Hukum (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 351);
 - c. Peraturan Menteri Hukum dan Hak Asasi Manusia Republik Indonesia Nomor 30 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia (Berita Negara Republik Indonesia Tahun 2021 Nomor 949);
 - d. Peraturan Menteri Hukum Nomor 1 Tahun 2024 tentang Organisasi dan Tata Kerja Kementerian Hukum (Berita Negara Republik Indonesia Tahun 2024 Nomor 832);
 - e. Keputusan Menteri Hukum dan Hak Asasi Manusia Nomor M.HH-02.TI.01 Tahun 2023 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintah Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintah Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia;
 - f. Keputusan Menteri Hukum dan Hak Asasi Manusia Nomor M.HH-06.TI.05.01 Tahun 2023 tentang Pedoman Manajemen Pusat Data Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia;
 - g. Surat Deputi Bidang Operasi Keamanan Siber dan Sandi Nomor 3607/BSSN/D2/OS.01.02/06/2025 tanggal 12 Juni 2025 hal Pemberitahuan Kegiatan Operasi Monitoring Keamanan Siber pada Kementerian Hukum.
 2. Sehubungan dengan surat Deputi Bidang Operasi Keamanan Siber dan Sandi nomor 3607/BSSN/D2/OS.01.02/06/2025 tanggal 12 Juni 2025 hal Pemberitahuan Kegiatan Operasi Monitoring Keamanan Siber pada Kementerian Hukum, bersama ini disampaikan hal-hal sebagai berikut:
 - a. bahwa Pihak BSSN telah menyampaikan hasil monitoring anomali trafik jaringan Kementerian Hukum periode 1 Januari s.d. 16 Juni 2025 yang mencakupi blok alamat IP publik 3 (tiga) jaringan Pusat Data yakni:
 - 1) 103.145.96.0/24 dan 103.163.21.0/24 dikelola Pusdatin;
 - 2) 103.200.128.0/22 dikelola Ditjen AHU; dan
 - 3) 103.150.168.0/23 dikelola Ditjen KI.

- b. bahwa hasil monitoring yang telah disampaikan oleh Pihak BSSN, ditemukan adanya anomali trafik pada alamat IP **103.200.128.66 milik Ditjen AHU** dan temuan kerentanan CVE-2021-1619 dengan level kritis (CVSS 9.8) pada asset **Router/Switch Cisco IOS XE milik Ditjen KI**;
 - c. adapun rekomendasi Tim BSSN terkait huruf b yakni:
 - 1) temuan pada alamat IP 103.200.128.66, agar dilakukan validasi terhadap temuan anomali trafik tersebut; dan
 - 2) temuan kerentanan pada asset Router/Switch Cisco IOS XE, agar dilakukan pembaruan sistem.
3. Berkaitan dengan hal tersebut, diharapkan kepada Bapak/Ibu sebagai berikut:
 - a. melaksanakan rekomendasi yang telah disampaikan oleh Pihak BSSN pada angka 2 huruf c dengan mengisi **formulir verifikasi dan validasi indikasi insiden** yang dapat diunduh pada link <https://s.id/FORM-VALIDASI-INSIDEN-SIBER>;
 - b. mengisi **formulir pendataan aset teknologi informasi** (lampiran II) untuk disampaikan ke Pihak BSSN dalam melakukan monitoring trafik pada aset yang terhubung secara publik;
 - c. formulir pada angka 3 huruf a dan huruf b dapat disampaikan secara resmi kepada Kepala Pusat Data dan Teknologi Informasi paling lambat **hari Jumat tanggal 4 Juli 2025**.
 4. Untuk informasi lebih lanjut dapat menghubungi Sdr. Puji Andreanto (+62 858-8115-5171).
- Atas perhatian dan kerja samanya diucapkan terima kasih.



Kepala Pusat Data dan Teknologi Informasi,



Ditandatangani secara elektronik oleh :

Rifqi Adrian Kriswanto

Tembusan:
Sekretaris Jenderal.

LAMPIRAN I
Surat Dinas Kepala Pusat Data
dan Teknologi Informasi
Nomor : SEK.7-TI.06.01-11
Tanggal : 25 Juni 2025

DAFTAR TUJUAN

1. Direktur Teknologi Informasi;
Direktorat Jenderal Administrasi Hukum Umum
2. Direktur Teknologi Informasi Kekayaan Intelektual;
Direktorat Jenderal Kekayaan Intelektual



Kepala Pusat Data dan Teknologi Informasi,



Ditandatangani secara elektronik oleh :
Rifqi Adrian Kriswanto

LAMPIRAN II
Surat Dinas Kepala Pusat Data dan
Teknologi Informasi
Nomor : SEK.7-TI.06.01-11
Tanggal : 25 Juni 2025

TEMPLATE FORMULIR PENDATAAN ASET TI

No.	OS	Jenis Aset	AS Number	IP Publik	Keterangan	Level Critical Aset (Low, Medium, High, Critical)
1	CentOS 7	Firewall	AS141583	103.158.20.1	F5	Critical
2		Web Server	AS141583	103.158.20.2	SI Ropog	Critical
3						
4						
Dst..						



Kepala Pusat Data dan Teknologi Informasi,



Ditandatangani secara elektronik oleh :

Rifqi Adrian Kriswanto



**BADAN SIBER
DAN SANDI
NEGARA**

ANOMALI TRAFIK NASIONAL DAN ANOMALI TRAFIK KEMENTERIAN HUKUM

Periode 1 Januari s.d 16 Juni 2025

KEMENTERIAN HUKUM



Limited disclosure, restricted to participant's organization

KLASIFIKASI DOKUMEN



TLP Amber+Strict: Hanya untuk kalangan terbatas, di mana penerima informasi hanya dapat membagi/meneruskan informasi kepada kalangan internal organisasi yang dianggap perlu mengetahui informasi tersebut.

Data dalam dokumen ini merupakan data bersifat terbatas yang hanya diperuntukkan kepada kalangan internal organisasi, apabila dokumen diterima oleh selain pihak yang berwenang maka tanggung jawab atas kebocoran data dalam dokumen ini ditanggung sepenuhnya oleh pemberi dokumen yang memberikan kepada pihak yang tidak berwenang

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

TLP:AMBER+STRICT





ANOMALI TRAFIK NASIONAL

Periode 1 Januari s.d 15 Juni 2025

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



TREN ANOMALI TRAFIK KEAMANAN SIBER NASIONAL

> Periode 1 Januari – 15 Juni 2025



2.900.819.136

**ANOMALI TRAFIK PERIODE
1 JANUARI – 15 Juni 2025**

TOP #3 – JENIS ANOMALI TRAFIK

93,60%

**2.715.205.790
MALWARE ACTIVITY**

135.852.418

**UNAUTHORIZED ACCESS AND SYSTEM
MISCONFIGURATION**

4,68%

0,70%

**20.318.554
EXPLOIT**

KEMENTERIAN HUKUM



**BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA**

J. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



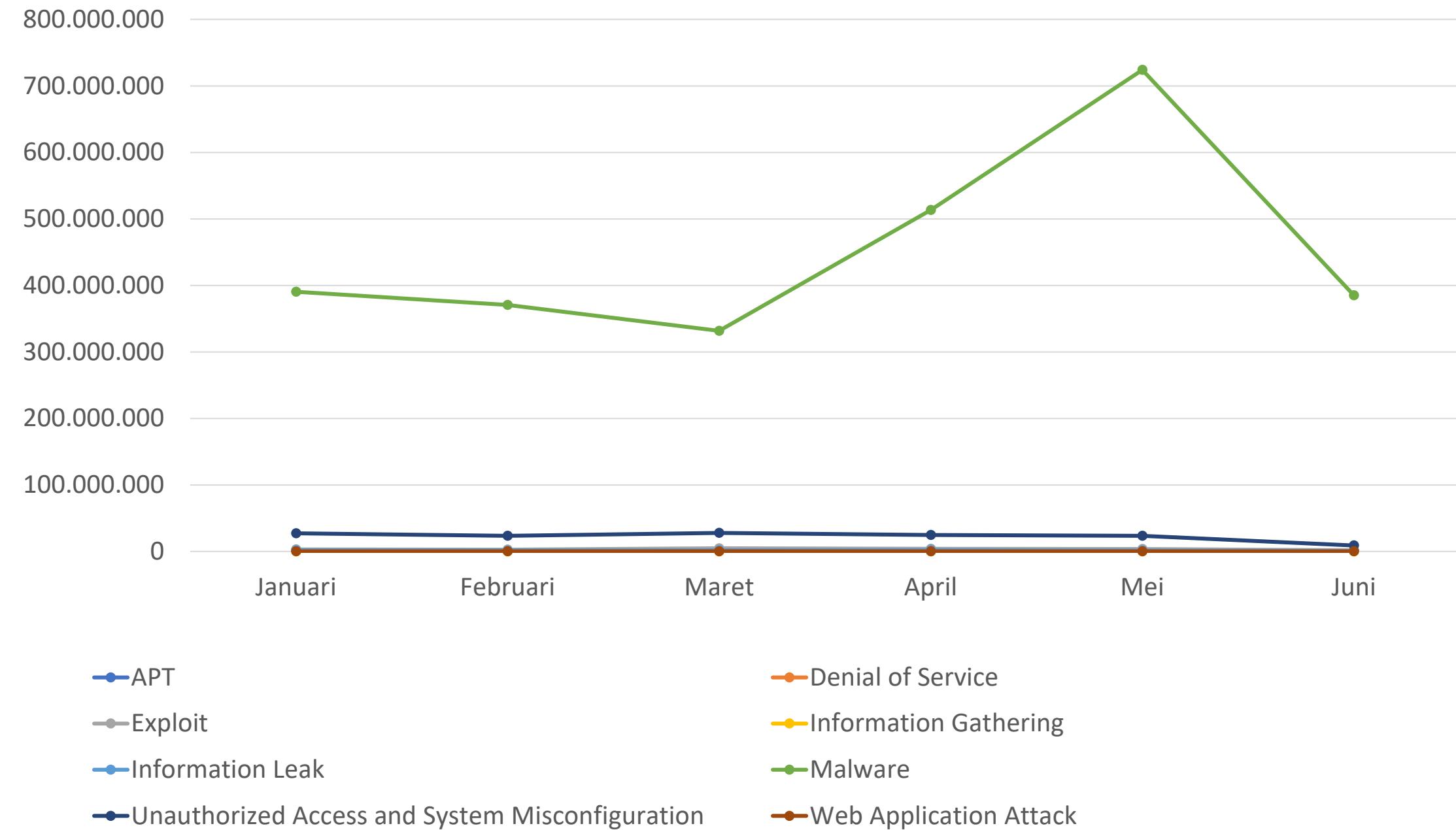
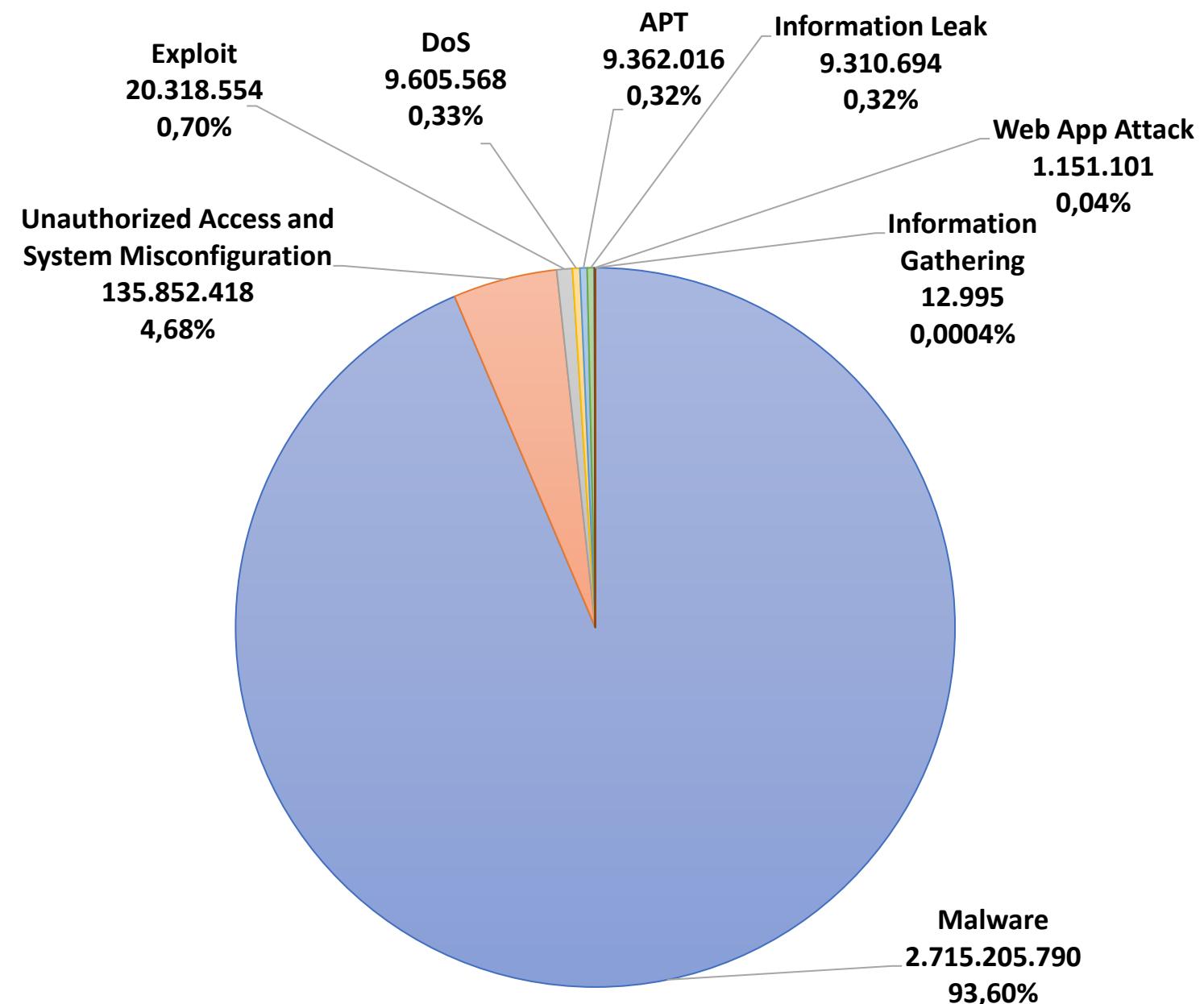
Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



KLASIFIKASI ANOMALI TRAFIK

> Periode 1 Januari – 15 Juni 2025



KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



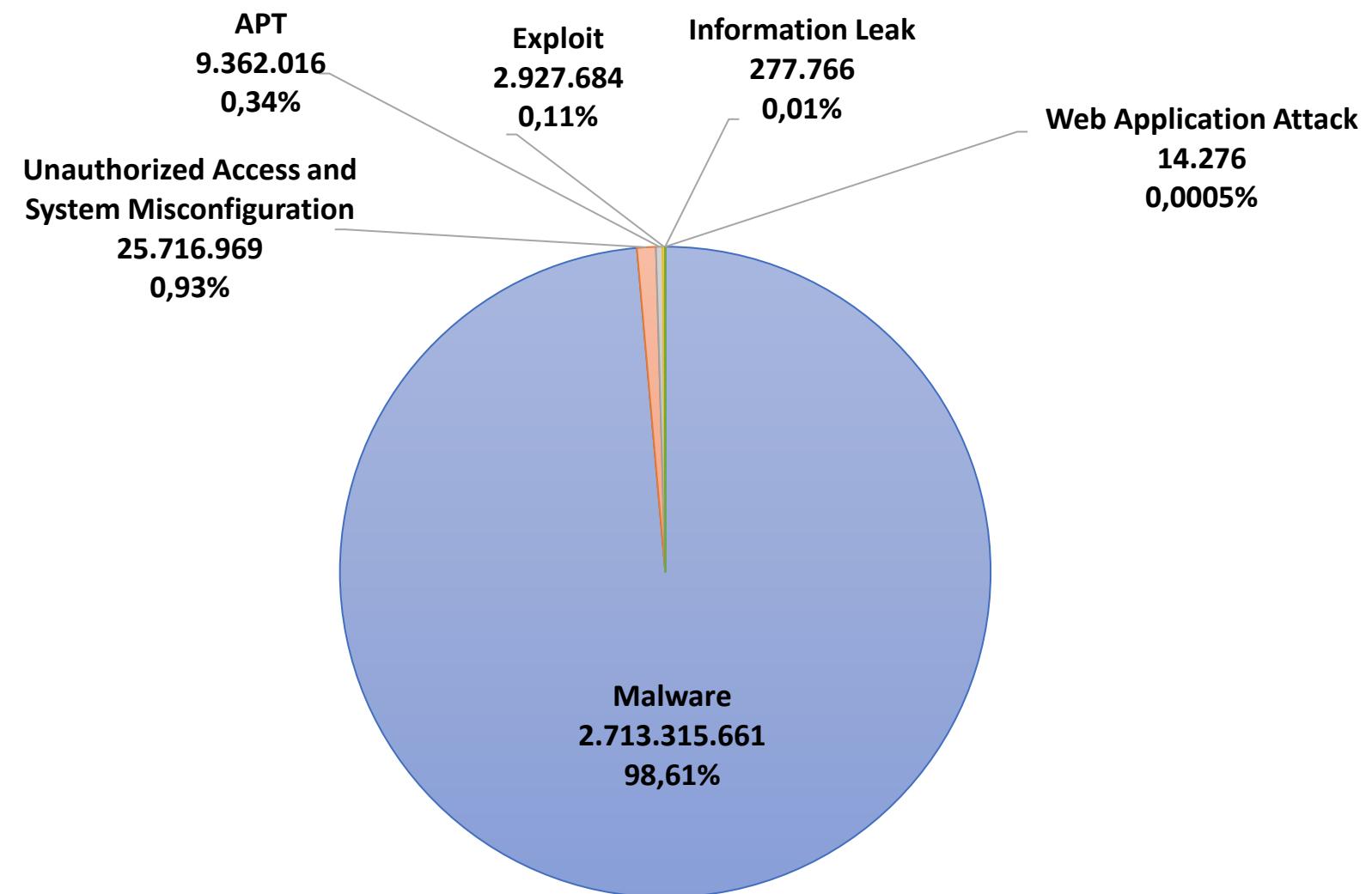
Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



ANOMALI COMPROMISE DAN ATTACK SUCCESSFUL

Pada periode 1 Januari – 15 Juni 2025, terdeteksi terdapat **2.900.819.136** anomali dengan **2.725.509.677** anomali diindikasikan berhasil menginfeksi dan telah melakukan komunikasi timbal balik dengan server yang digunakan penyerang (**Compromise**) dan **26.104.695** anomali diindikasikan sebagai upaya serangan yang berhasil dilakukan terhadap sistem elektronik dan penyerang mendapat respon berhasil dari sistem elektronik tersebut (**Attack Successful**).



Anomali dengan status **Compromise** dan **Attack Successful** berasal dari kategori **Malware** (98,61%), **Unauthorized Access and System Misconfiguration** (0,93%), **APT** (0,34%), **Exploit** (0,11%), **Information Leak** (0,01%), dan **Web Application Attack** (0,0005%).

Berikut daftar 3 anomali tertinggi dari setiap klasifikasi yang diindikasikan **Compromise** dan **Attack Successful**.

KLASIFIKASI	THREAT NAME	TOTAL
Malware	<i>Mirai Botnet activity</i>	1.158.889.145
	<i>Remcos RAT activity</i>	785.899.835
	<i>Generic Trojan RAT activity</i>	321.342.119
Unauthorized Access and System Misconfiguration	<i>Discover using socks agent</i>	14.156.070
	<i>The remote connection tool AnyDesk is active</i>	11.031.236
	<i>Website Automatic Directory Listing Detection</i>	333.038
APT	<i>SilverTerrier</i>	1.757.801
	<i>Bluenoroff</i>	1.643.890
	<i>UNC2452</i>	689.174
Exploit	<i>w2km ExploitKit activity</i>	1.547.843
	<i>Microsoft windows doublepulsar (double pulsar) smb remote code execution</i>	505.156
	<i>DCRat ExploitKit activity</i>	151.280
Information Leak	<i>Find the robots.txt file</i>	112.958
	<i>Crossdomain information disclosure vulnerability</i>	52.033
	<i>Cacti info leak vulnerability</i>	36.485
Web Application Attack	<i>SQL injection</i>	12.867
	<i>Cross-site scripting vulnerability (suspected)</i>	1.080
	<i>General arbitrary file reading (successful)</i>	235



TREN ANCAMAN SIBER RANSOMWARE DAN APT NASIONAL

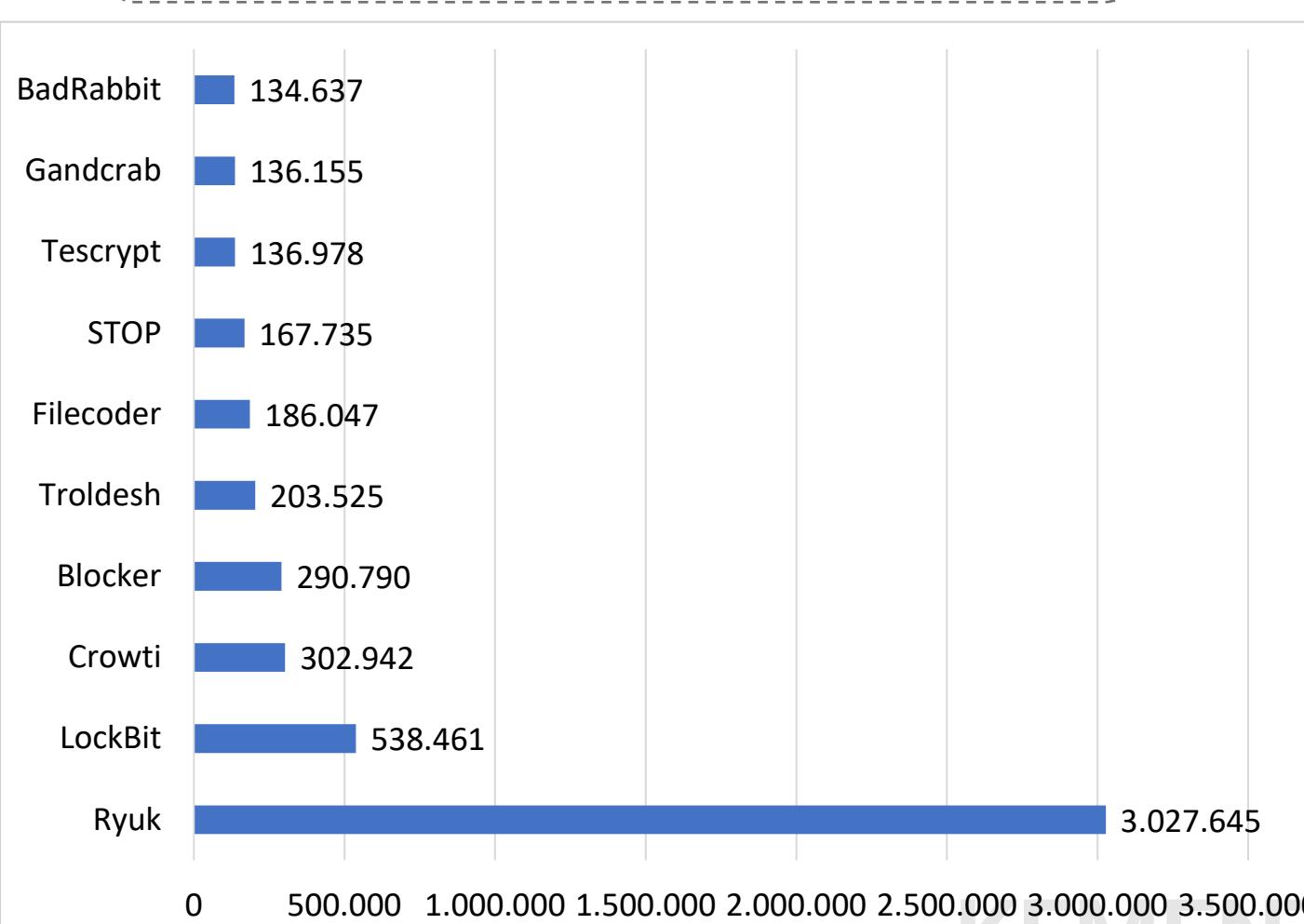
> Periode 1 Januari – 15 Juni 2025

Ransomware



5.886.631

Anomali Trafik Berjenis Ransomware

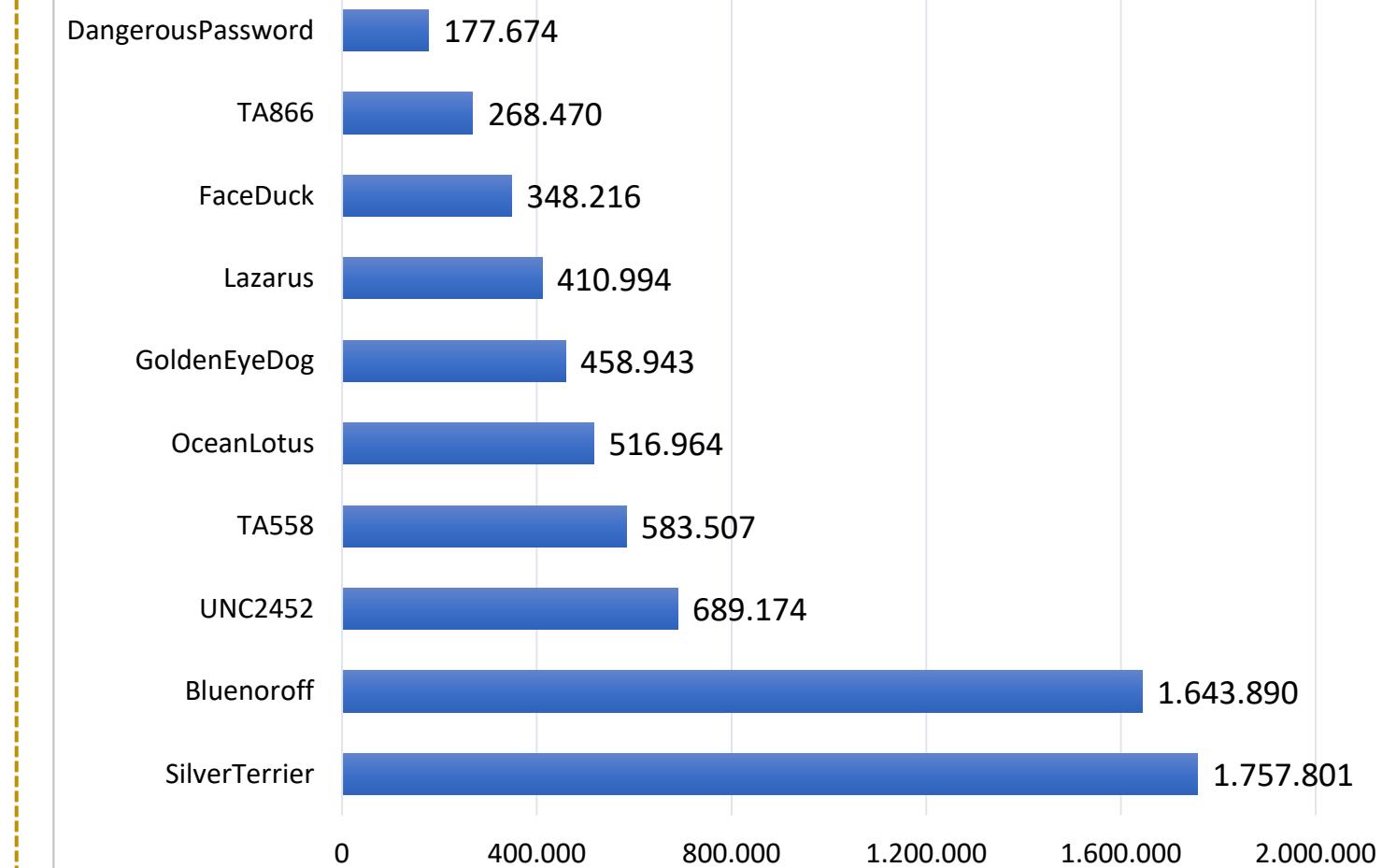


Advanced Persistent Threat



9.362.016

Anomali Trafik Berjenis APT



**BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA**

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

TLP:AMBER+STRICT





ANOMALI TRAFIK KEMENTERIAN HUKUM

Periode 1 Januari s.d 16 Juni 2025

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



DAFTAR ASET KEMENTERIAN HUKUM

> Periode 1 Januari – 16 Juni 2025

Berikut adalah daftar aset Kementerian Hukum yang di jadikan sebagai ruang lingkup pemonitoran:

Segmen IP	AS Number	Pengelola Aset
103.150.168.0/24	AS 140394	Direktorat Jenderal Kekayaan Intelektual
103.200.128.0/22	AS 134633	Direktorat Jenderal Administrasi Hukum Umum
103.145.96.0/24	AS 139442	Kementerian Hukum dan Hak Asasi Manusia
103.163.21.0/24		

13

Alamat IP Terdapat
Anomali Trafik

Berdasarkan hasil pemonitoran periode 1 Januari s.d 16 Juni 2025, diketahui terdapat anomali trafik pada satu Alamat IP milik Kementerian Hukum.

*Informasi terkait aset didapatkan dari sumber terbuka, sehingga apabila terdapat ketidaksesuaian berkenan untuk diinformasikan agar dapat diperbarui

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

J. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

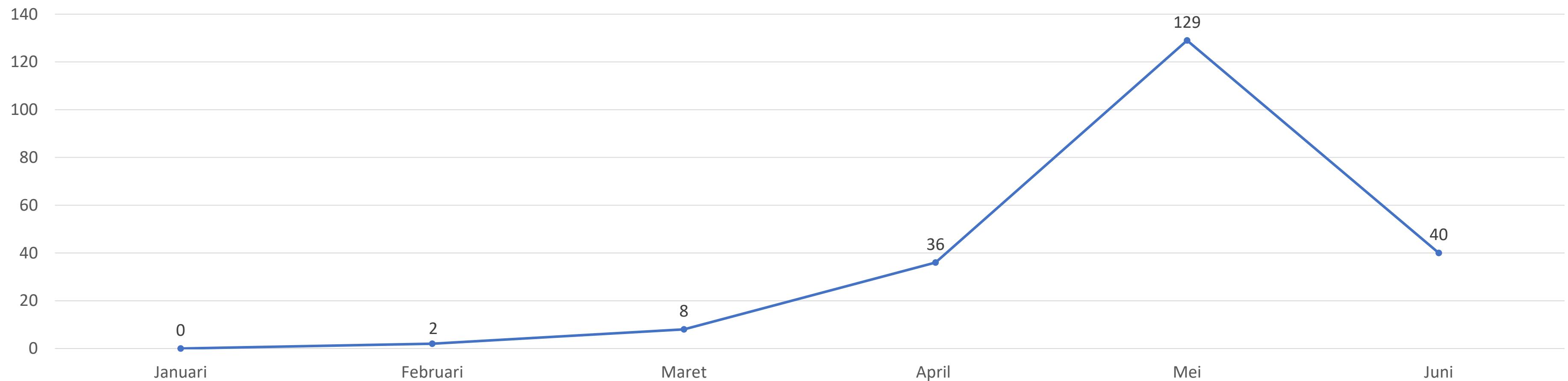
TLP:AMBER+STRICT



ANOMALI TRAFIK KEMENTERIAN HUKUM

> Periode 1 Januari – 16 Juni 2025

TREN ANOMALI TRAFIK BULANAN



Berikut merupakan grafik tren anomali trafik sejak tanggal 1 Januari – 16 Juni 2025 pada aset Kementerian Hukum dengan jumlah **215** anomali.

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

J. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

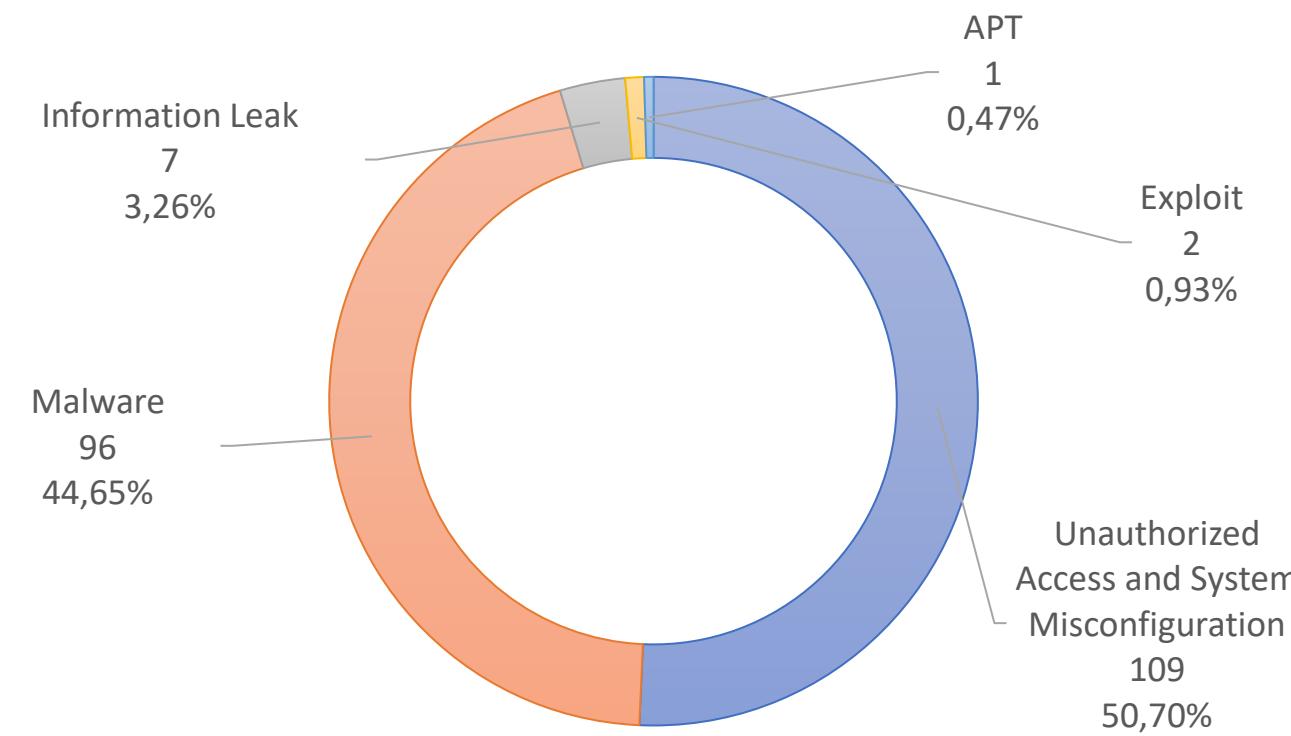
TLP:AMBER+STRICT



ANOMALI TRAFIK ASET KEMENTERIAN HUKUM

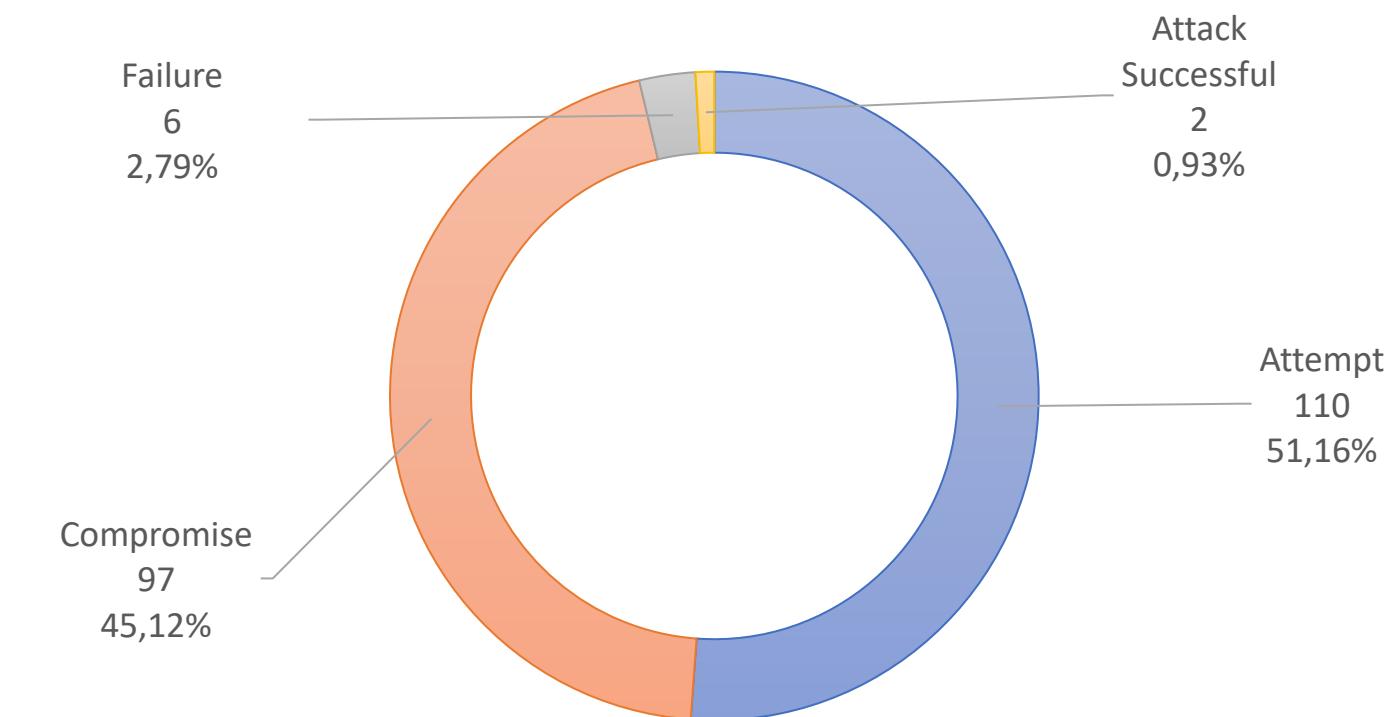
> Periode 1 Januari – 16 Juni 2025

KATEGORI ANOMALI TRAFIK



Sejak tanggal Periode 1 Januari – 16 Juni 2025, anomali trafik yang paling banyak terdeteksi pada aset Kementerian Hukum berasal dari kategori **Unauthorized Access and System Misconfiguration** dengan persentase sebanyak 50,70%.

STATUS ANOMALI TRAFIK



Status dari anomali trafik yang terdeteksi adalah :

- 51,16% Upaya percobaan (*Attempt*)
- 45,12% Serangan berhasil menginfeksi (*Compromise*)
- 2,79% Percobaan gagal (*Failure*)
- 0,93% Serangan berhasil (*Attack Successful*)

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



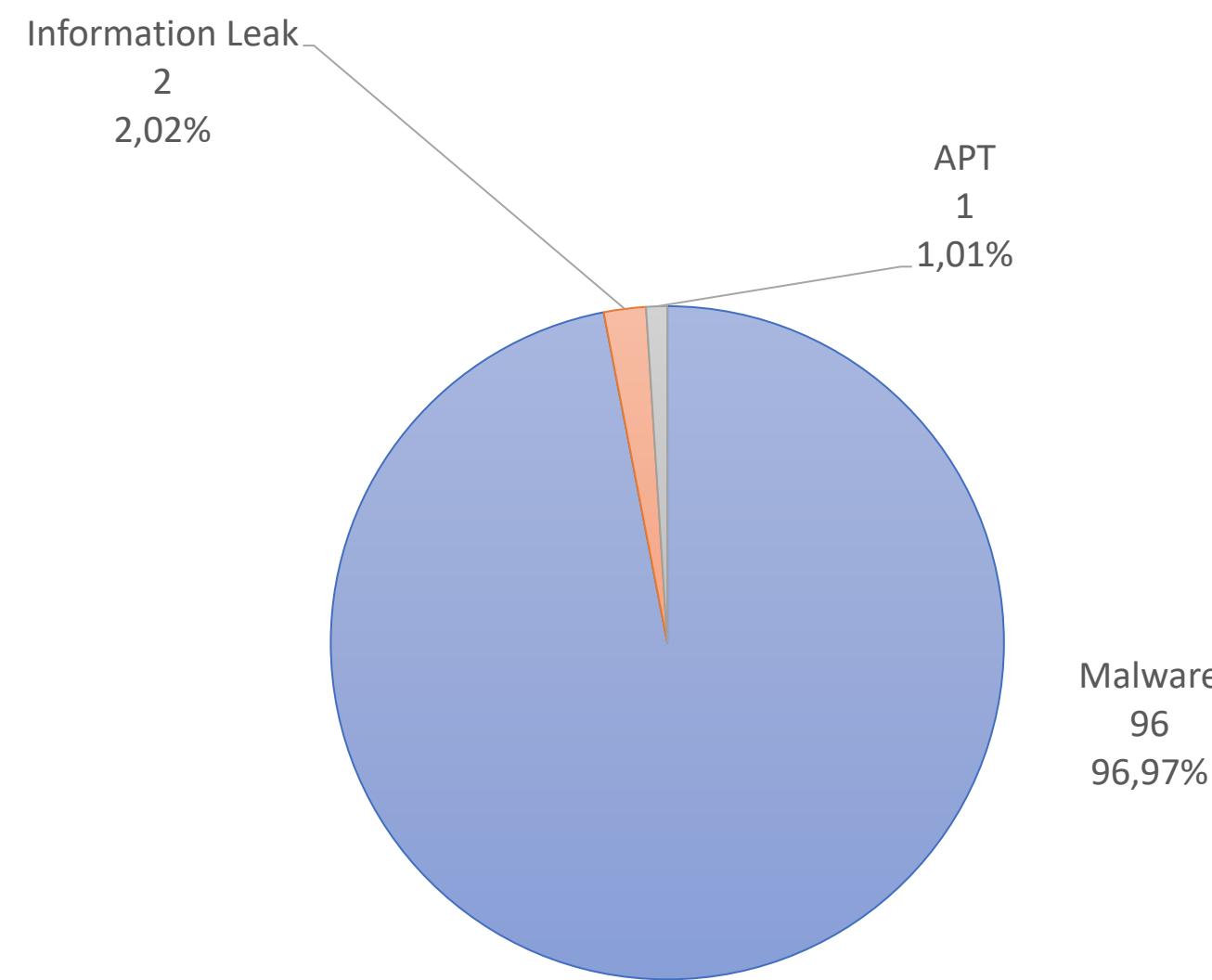
Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



ANOMALI COMPROMISE DAN ATTACK SUCCESSFUL

Pada periode 1 Januari – 16 Juni 2025 terdeteksi terdapat **99** anomali dengan **97** anomali diindikasikan berhasil menginfeksi dan telah melakukan komunikasi timbal balik dengan server yang digunakan penyerang (*Compromise*) dan **2** anomali diindikasikan sebagai upaya serangan yang berhasil dilakukan terhadap sistem elektronik dan penyerang mendapat respon berhasil dari sistem elektronik tersebut (*Attack Successful*).



Anomali dengan status *compromise* dan *attack successful* berasal dari kategori **Malware** (96,97%), **Information Leak** (2,02%), dan **APT** (1,01%).

Berikut daftar 3 anomali tertinggi dari setiap klasifikasi yang diindikasikan *compromise* dan *attack successful*.

KLASIFIKASI	THREAT NAME	TOTAL
Malware	PhishingSite Other Malware activity	61
	Generic Trojan RAT activity	21
	Phishing&Fraud Other Malware activity	3
Information Leak	PhpMyAdmin information disclosure vulnerability	2
APT	APT29	1

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri

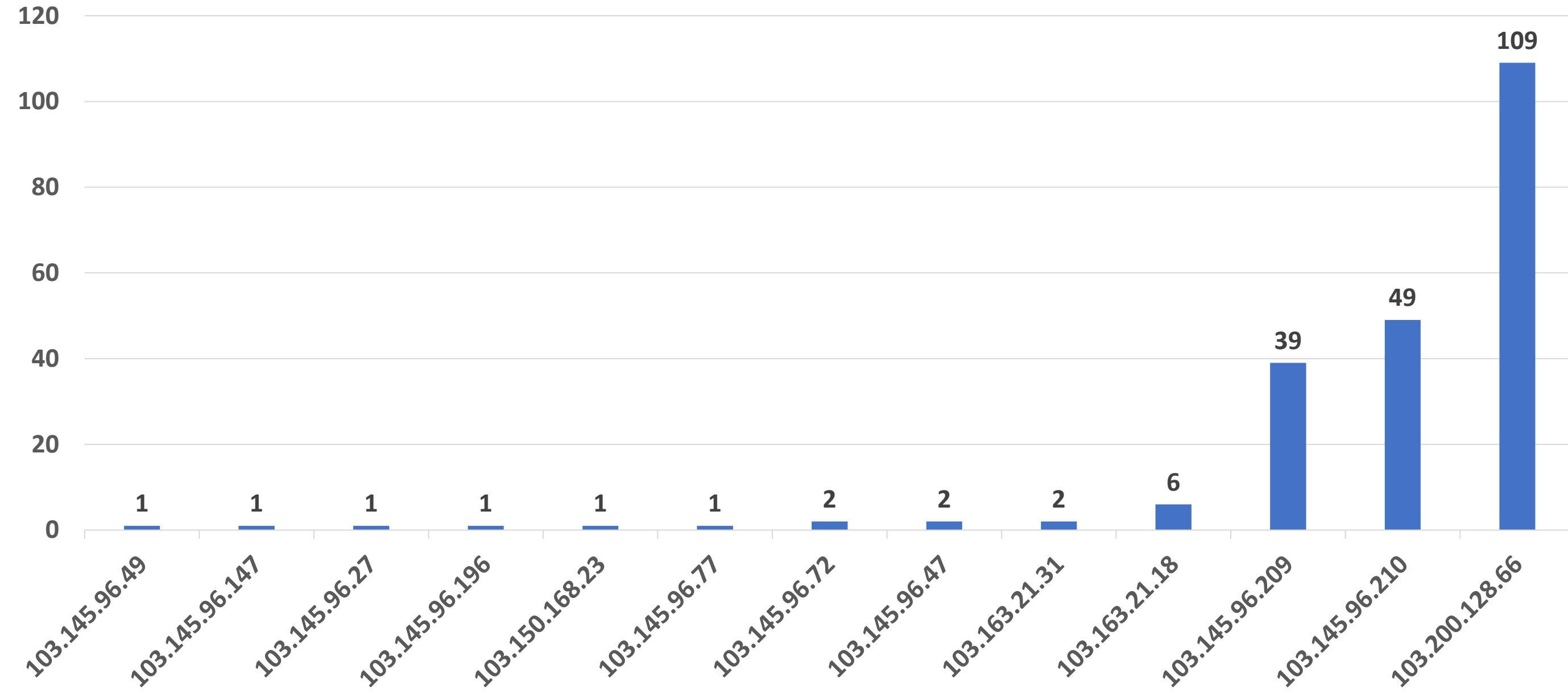


Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



ANALISIS ANOMALI TRAFIK



Anomali trafik didominiasi oleh alamat IP 103.200.128.66, 103.145.96.210, dan 103.145.96.209

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

J. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri

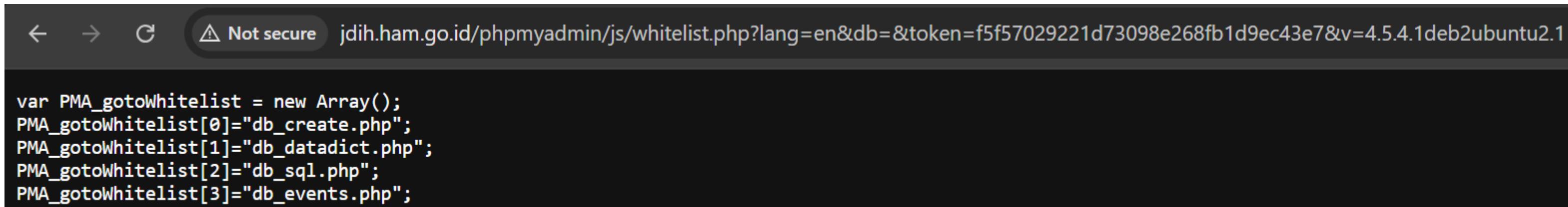


Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



PhpMyAdmin information disclosure vulnerability



A screenshot of a web browser window. The address bar shows a URL starting with "jdih.ham.go.id/phpmyadmin/js/whitelist.php?lang=en&db=&token=f5f57029221d73098e268fb1d9ec43e7&v=4.5.4.1deb2ubuntu2.1". A "Not secure" warning icon is present. The main content area displays the following JavaScript code:

```
var PMA_gotoWhitelist = new Array();
PMA_gotoWhitelist[0] = "db_create.php";
PMA_gotoWhitelist[1] = "db_datadict.php";
PMA_gotoWhitelist[2] = "db_sql.php";
PMA_gotoWhitelist[3] = "db_events.php";
```

PhpMyAdmin Information Disclosure Vulnerability adalah jenis kerentanan keamanan di mana *phpMyAdmin*, sebuah tool berbasis web untuk mengelola database MySQL/MariaDB, secara tidak sengaja mengekspos informasi sensitif kepada pengguna yang tidak berwenang.

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



ANALISIS ANOMALI TRAFIK

103.163.21.31

// TAGS: self-signed

General Information

Country: Indonesia
City: Manado
Organization: KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
ISP: KEMENKUMHAM
ASN: AS139

Open Ports

53, 2000, 8085, 8443 // 2000 / TCP

103.163.21.18

103.145.96.210

General Information

Hostnames: ns4.kemenkum.go.id
Domains: kemenkum.go.id
Country: Indonesia
City: Jakarta

Open Ports

53 // 53 / UDP

none
Recursion: enabled
Resolver name: F502.kemenkumham.go.id

103.145.96.209

General Information

Hostnames: ns3.kemenkum.go.id
Domains: kemenkum.go.id
Country: Indonesia
City: Jakarta
Organization: KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
ISP: KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
ASN: AS139442

Open Ports

53 // 53 / UDP

none
Recursion: enabled
Resolver name: F501.kemenkumham.go.id

Port 53 (DNS) yang terbuka untuk publik

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



ANALISIS ANOMALI TRAFIK

Open recursive resolver detected on 103.163.21.31

IP address 103.163.21.31 is **vulnerable** to DNS Amplification attacks.

Open recursive resolver detected on 103.163.21.18

IP address 103.163.21.18 is **vulnerable** to DNS Amplification attacks.

Open recursive resolver detected on 103.145.96.209

IP address 103.145.96.209 is **vulnerable** to DNS Amplification attacks.

Open recursive resolver detected on 103.145.96.210

IP address 103.145.96.210 is **vulnerable** to DNS Amplification attacks.

```
PS C:\Users\glgpu> nslookup google.com 103.163.21.31
Server: Unknown
Address: 103.163.21.31
```

Non-authoritative answer:

```
Name: google.com
Addresses: 2404:6800:4003:c04::8b
           2404:6800:4003:c04::66
           2404:6800:4003:c04::65
           2404:6800:4003:c04::8a
           172.217.194.101
           172.217.194.100
           172.217.194.102
           172.217.194.138
           172.217.194.139
           172.217.194.113
```

Sumber: openresolver.com

PoC DNS Server terbuka dan dapat digunakan oleh semua orang

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



REKOMENDASI

1. Melakukan *scanning* secara berkala pada aset milik Kementerian Hukum serta melakukan pembaharuan terhadap antivirus dan sistem secara berkala.
2. Menerapkan protokol HTTPS pada sistem layanan aplikasi Web
3. Batasi agar DNS server hanya dapat diakses oleh jaringan internal Kementerian Hukum dengan menerapkan *access control list* pada *firewall*.
4. Mengubah akun pengguna dan password yang digunakan dengan asumsi seluruh informasi tersebut telah berhasil diperoleh oleh pihak yang tidak bertanggung jawab.
5. Melakukan pemblokiran terhadap IoC dari aktivitas anomali.
6. Melakukan pemantauan jaringan secara proaktif untuk setiap aktivitas yang mencurigakan.
7. Menyusun regulasi terkait penggunaan *password* sesuai standar keamanan, penggantian *password* secara berkala serta pemasangan antivirus pada perangkat pegawai.

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



PROFIL KERENTANAN UMUM (CVE) KEMENTERIAN HUKUM JUNI 2025

Direktorat Operasi Keamanan Siber

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



RINGKASAN

1. Hasil analisis kerentanan pada Kementerian Hukum ditemukan sebanyak 2.014 hit kerentanan dengan 318 jenis kerentanan. Jenis kerentanan yang memiliki CVSS tertinggi dan hit terbanyak yaitu kerentanan pada fungsi AAA (*Authentication, Authorization, and Accounting*) di Cisco IOS XE dengan level CRITICAL (CVSS 9.8) berupa CVE-2021-1619.
2. Alamat IP dengan jumlah hit terbanyak yaitu 103.150.169.122 yang merupakan alamat IP dari website SIMPAKI Direktorat Jenderal Kekayaan Intelektual Kementerian Hukum dan HAM Republik Indonesia dengan jumlah hit 140.

KEMENTERIAN HUKUM



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri

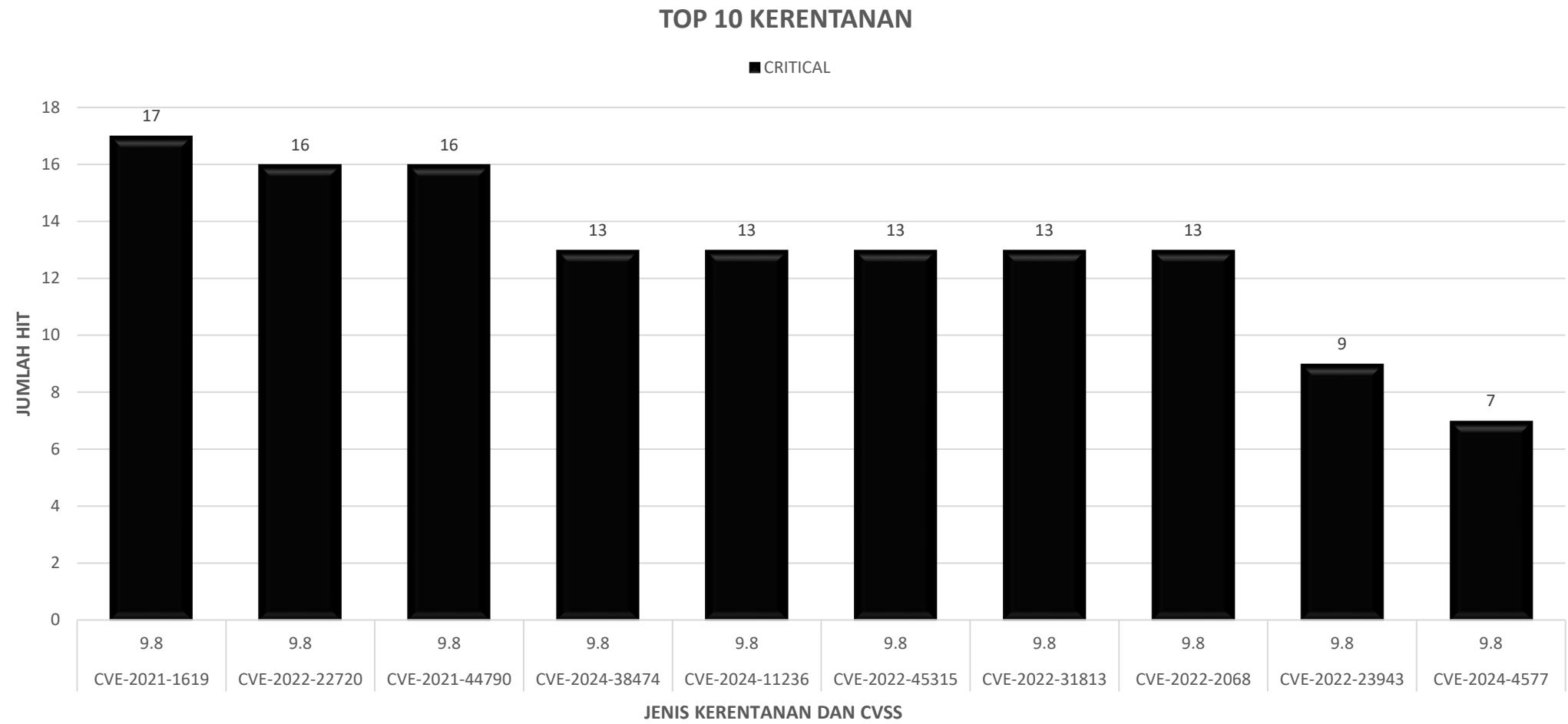
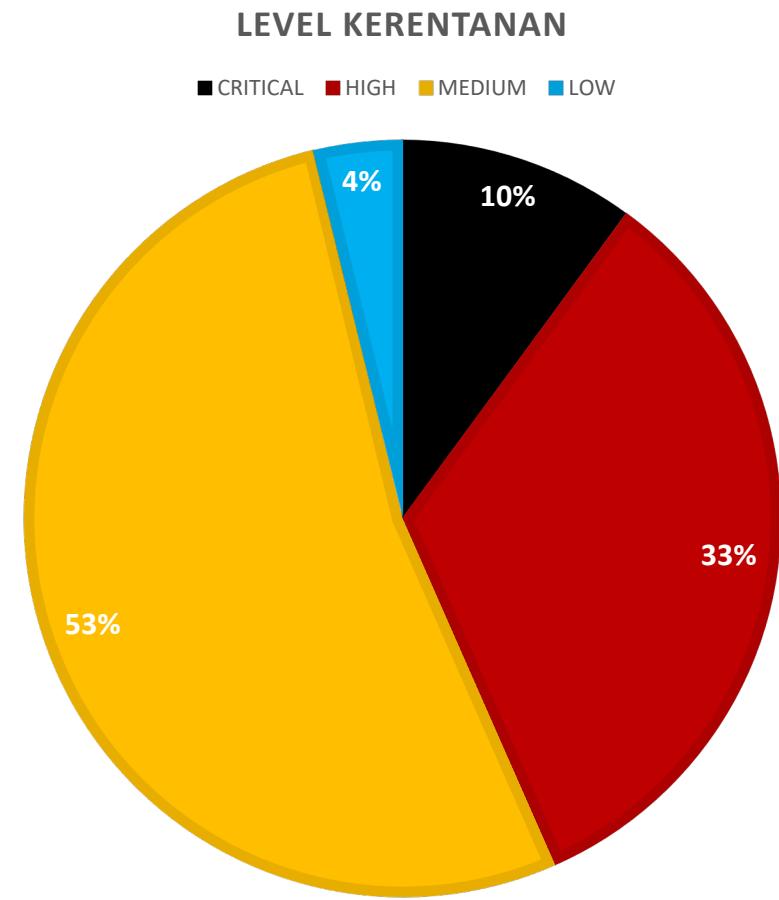


Badan Siber dan Sandi Negara

TLP:AMBER+STRICT



KERENTANAN UMUM KEMENTERIAN HUKUM



Berdasarkan 318 jenis kerentanan ditemukan bahwa 10% termasuk kategori CRITICAL, 33% termasuk kategori HIGH, 53% termasuk kategori MEDIUM, dan 4% termasuk kategori LOW. Berikut merupakan grafik skala kerentanan dari CVE yang berhasil diperoleh pada Kementerian Hukum.

Berdasarkan hasil pengumpulan jenis kerentanan, diperoleh informasi bahwa jenis kerentanan dengan severity tertinggi adalah **CVE-2021-1619** dengan level CRITICAL (CVSS 9.8) serta jumlah hit 17 kali. Kerentanan tersebut merupakan kerentanan pada fungsi AAA (*Authentication, Authorization, and Accounting*) di Cisco IOS XE yang memungkinkan penyerang jarak jauh yang tidak terautentikasi untuk melewati proses otentikasi pada layanan NETCONF atau RESTCONF.

KEMENTERIAN HUKUM



**BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA**

J. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara

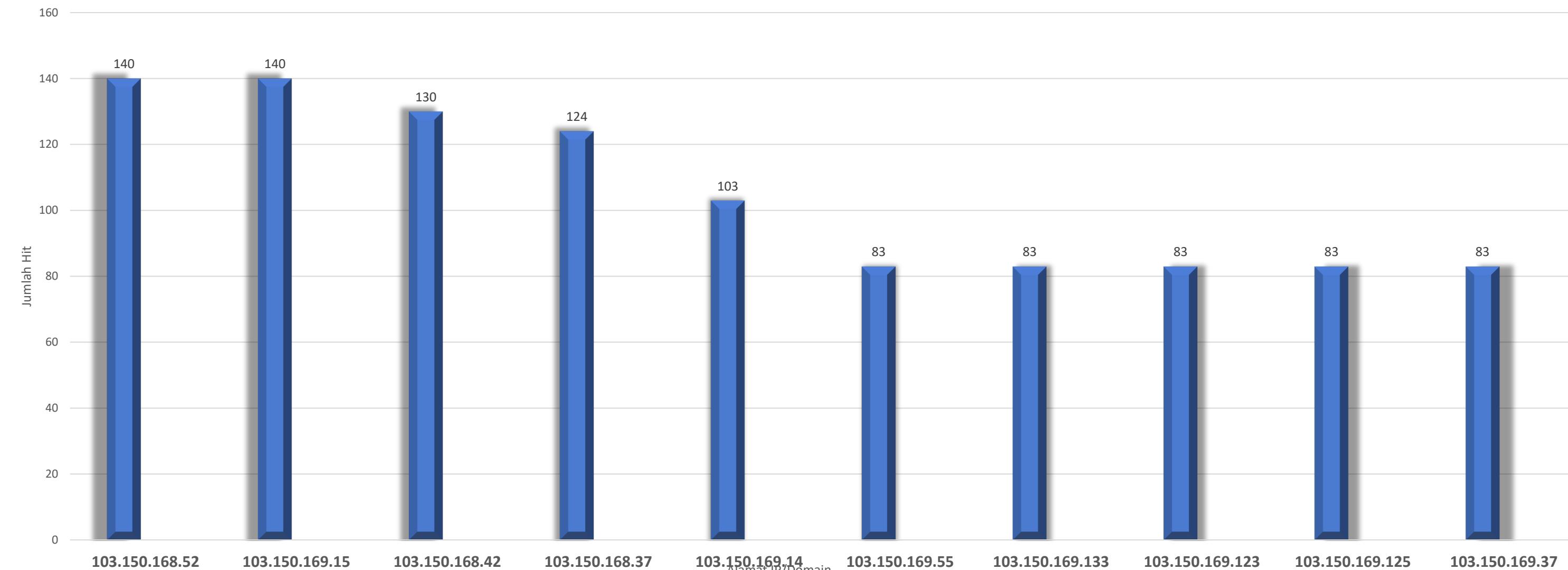
TLP:AMBER+STRICT



ASET TERDAMPAK KEMENTERIAN HUKUM

Berdasarkan informasi aset terdampak pada Kementerian Hukum, terdapat 28 aset yang terdampak, berikut adalah informasi keterkaitan antara top 10 aset dengan kerentanan yang dimiliki:

TOP 10 ALAMAT IP KEMENTERIAN HUKUM





TEMUAN DARKNET EXPOSURE BERKAITAN DENGAN ASET MILIK KEMENTERIAN HUKUM REPUBLIK INDONESIA

KEMENTERIAN HUKUM TERBATAS

Limited disclosure, restricted to participants' organization (Hanya untuk Internal Organisasi (Kementerian Hukum Republik Indonesia))
Tanggung jawab distribusi file ini diserahkan kepada pemegang file



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



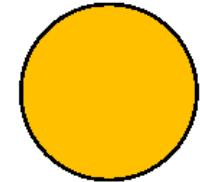
@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara



TLP: AMBER+STRICT : Informasi yang sensitive dan dibatasi hanya untuk kalangan terbatas, di mana penerima informasi hanya dapat membagi/meneruskan informasi kepada kalangan internal organisasi yang dianggap perlu mengetahui informasi dan tidak dibagikan ke pihak lainnya.

Data dalam dokumen ini merupakan data bersifat sensitive dan rahasia yang hanya diperuntukkan kepada internal organisasi (Kementerian Hukum Republik Indonesia), apabila dokumen diterima oleh selain internal organisasi maka tanggung jawab atas kebocoran data dokumen ini ditanggung sepenuhnya oleh pemberi dokumen yang memberikan kepada pihak yang tidak berwenang.

KEMENTERIAN HUKUM TERBATAS



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



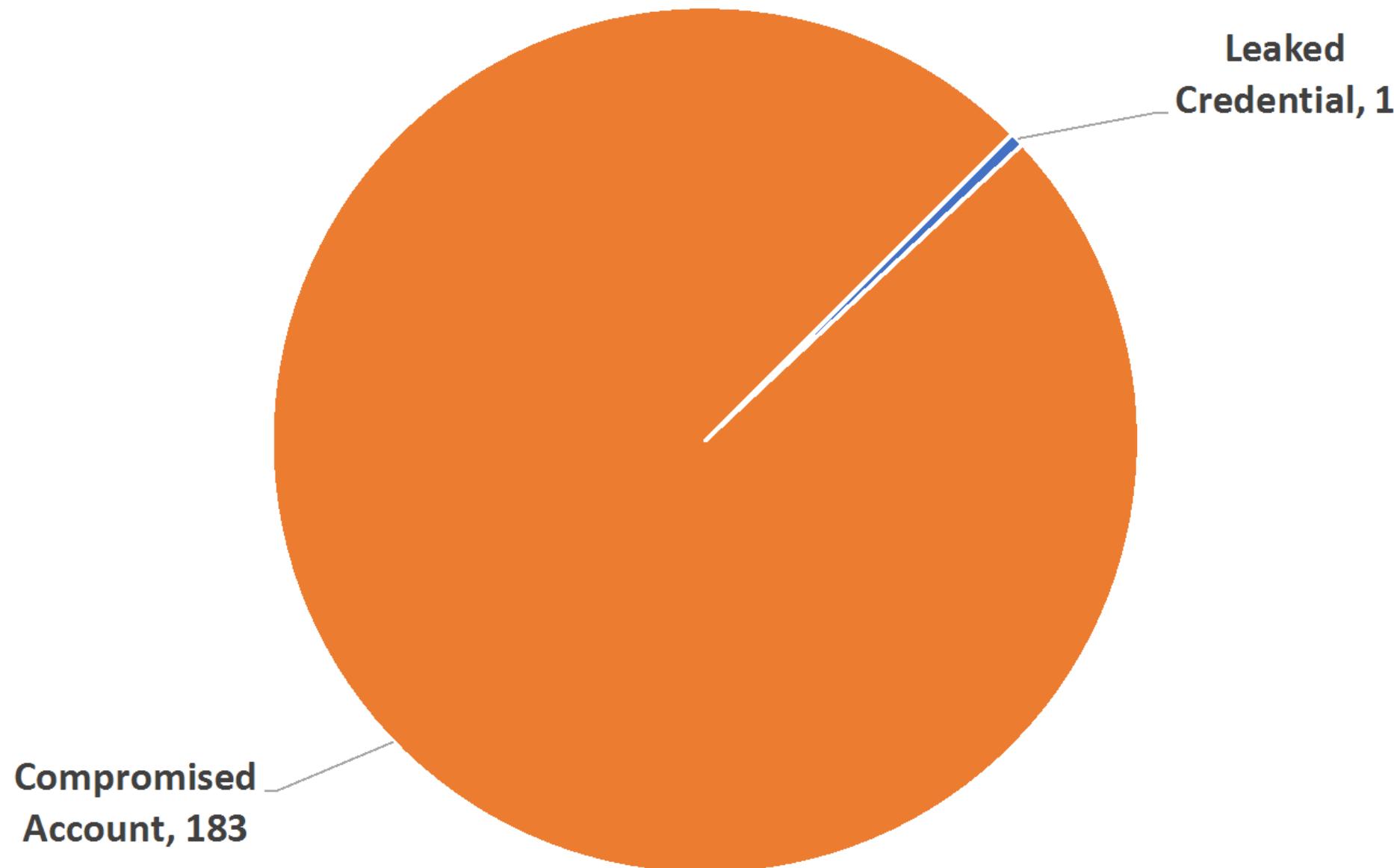
@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara



Rentang Waktu Temuan
1 Januari 2025 – 12 Maret 2025

Leaked Credential

Kebocoran yang terjadi pada aplikasi pihak ketiga (seperti e-commerce, aplikasi booking tiket, aplikasi booking penginapan dan lain-lain) akibat penggunaan email dinas Kondisi dimana email dinas digunakan untuk keperluan lain diluar kegiatan kedinasan.

Total 183

Rentang Waktu Temuan
1 Januari 2025 – 12 Maret 2025

Compromised Account

Kondisi dimana kebocoran data pada end user disebabkan oleh malware stealer. Adapun kebocoran username dan password pada web service tertentu, sehingga dapat disalahgunakan oleh pihak lain.

KEMENTERIAN HUKUM
TERBATAS

Total 1



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



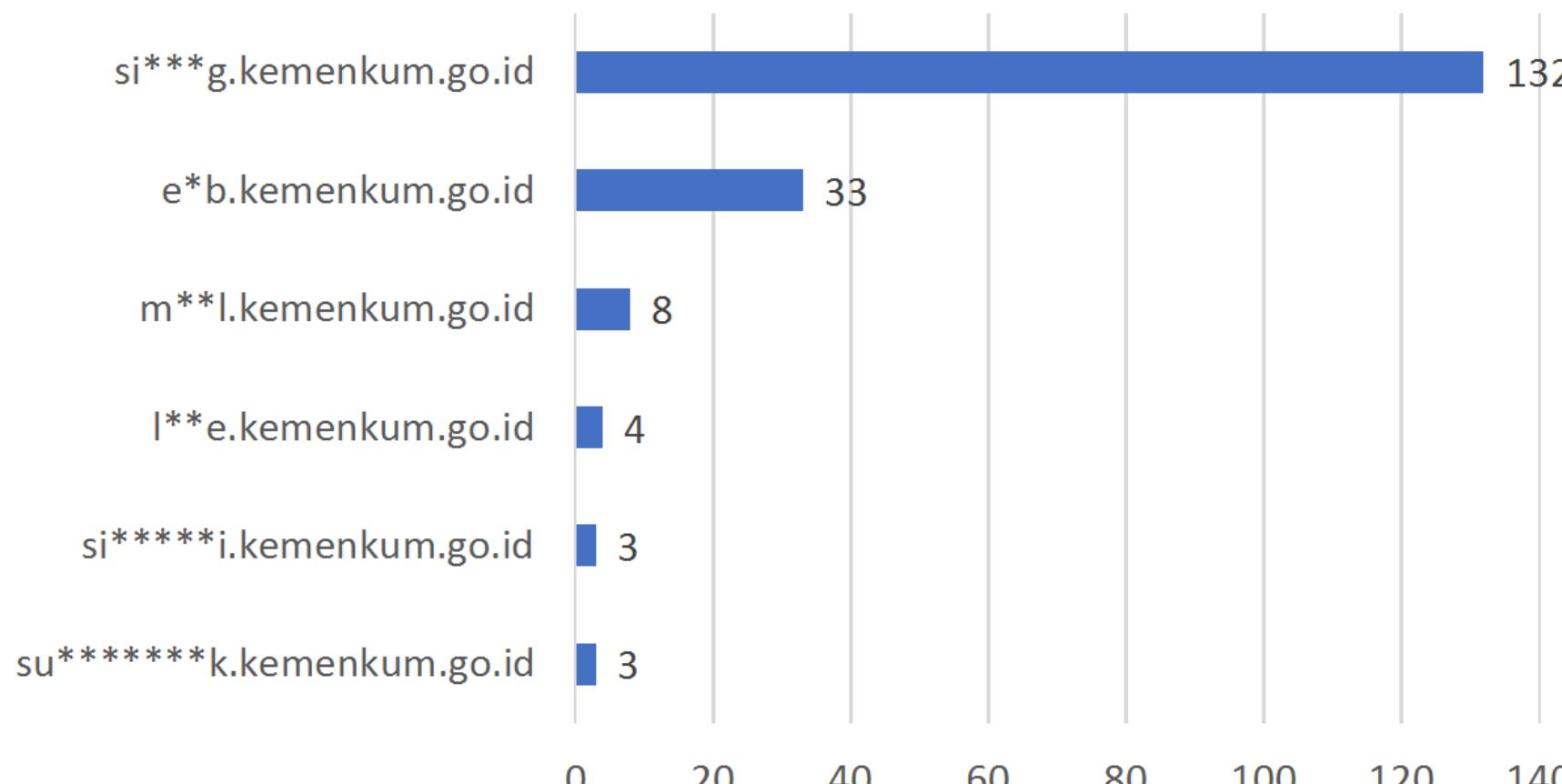
Badan Siber dan Sandi Negara



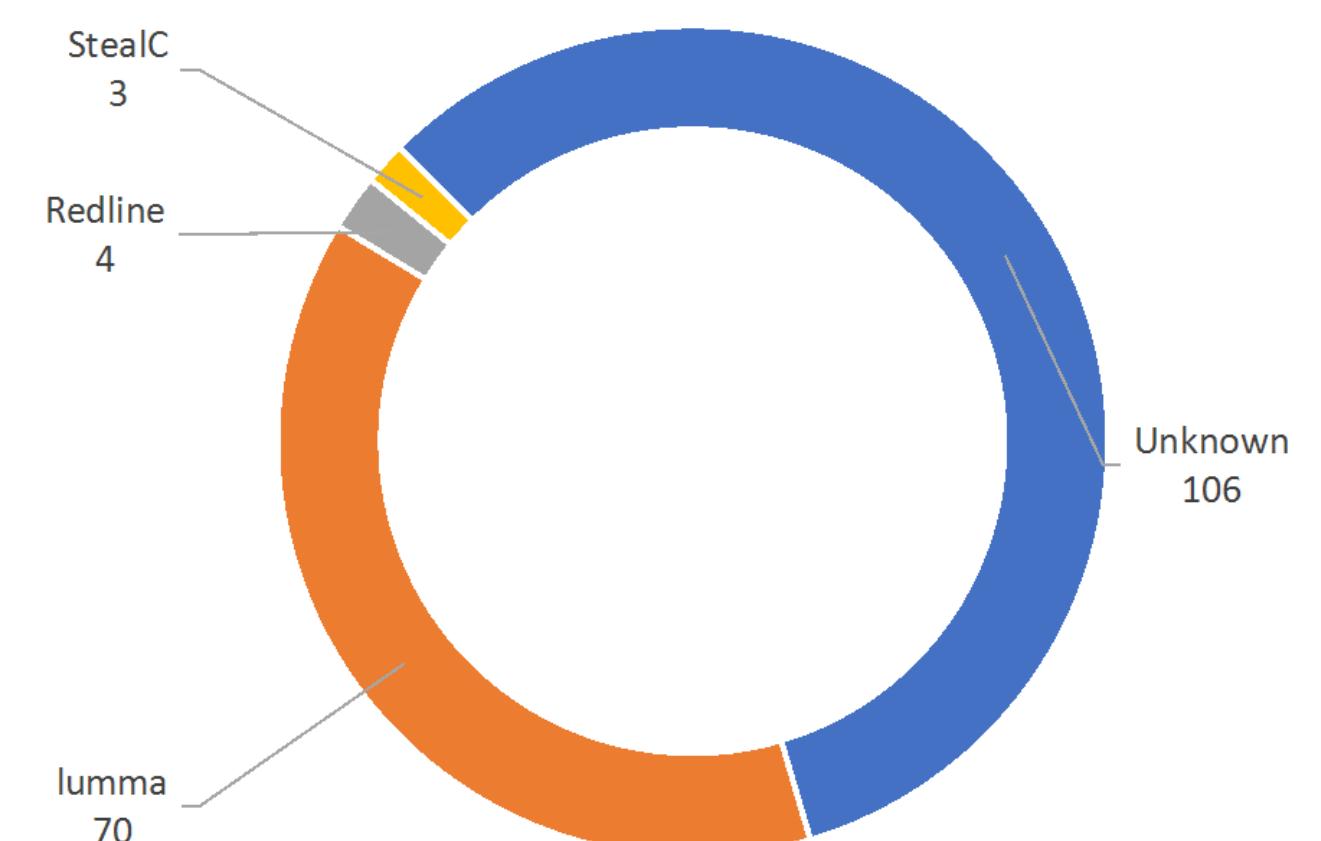
Compromised Account

Kondisi dimana kebocoran data pada end user disebabkan oleh malware stealer. Adapun kebocoran username dan password pada web service tertentu, sehingga dapat disalahgunakan oleh pihak lain.

Web Service Terdampak



Malware Stealer



KEMENTERIAN HUKUM
TERBATAS



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



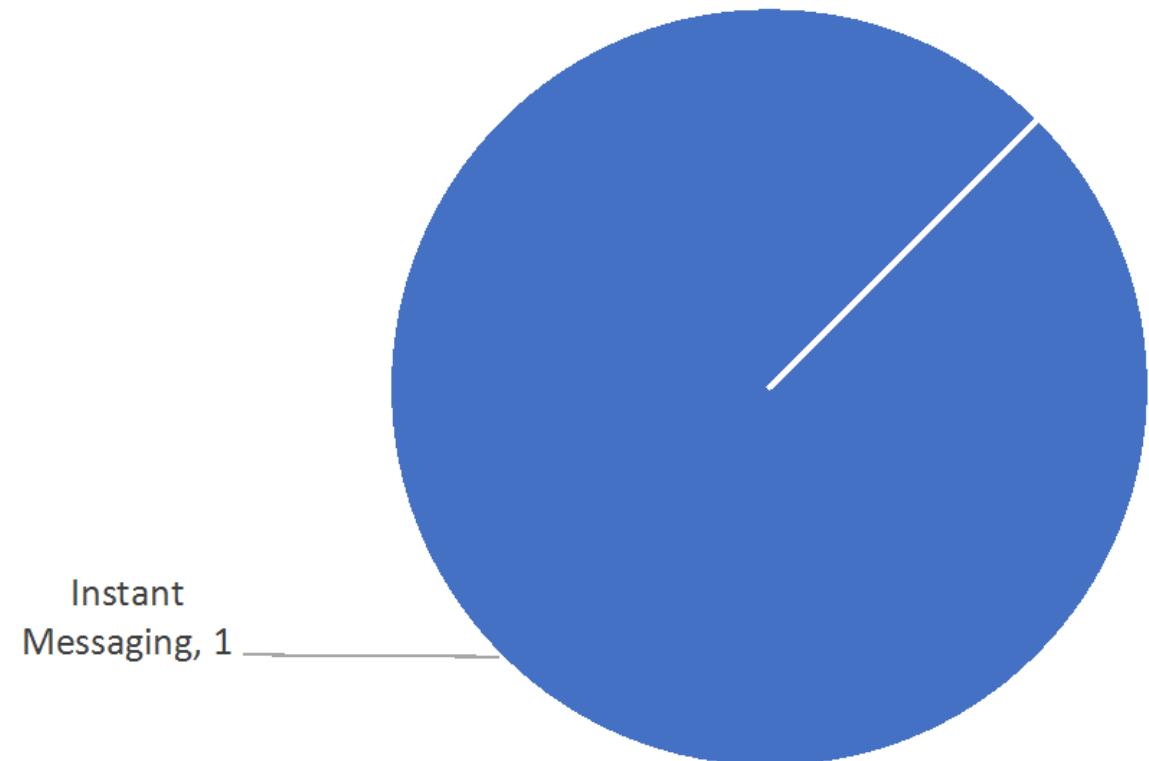
Badan Siber dan Sandi Negara



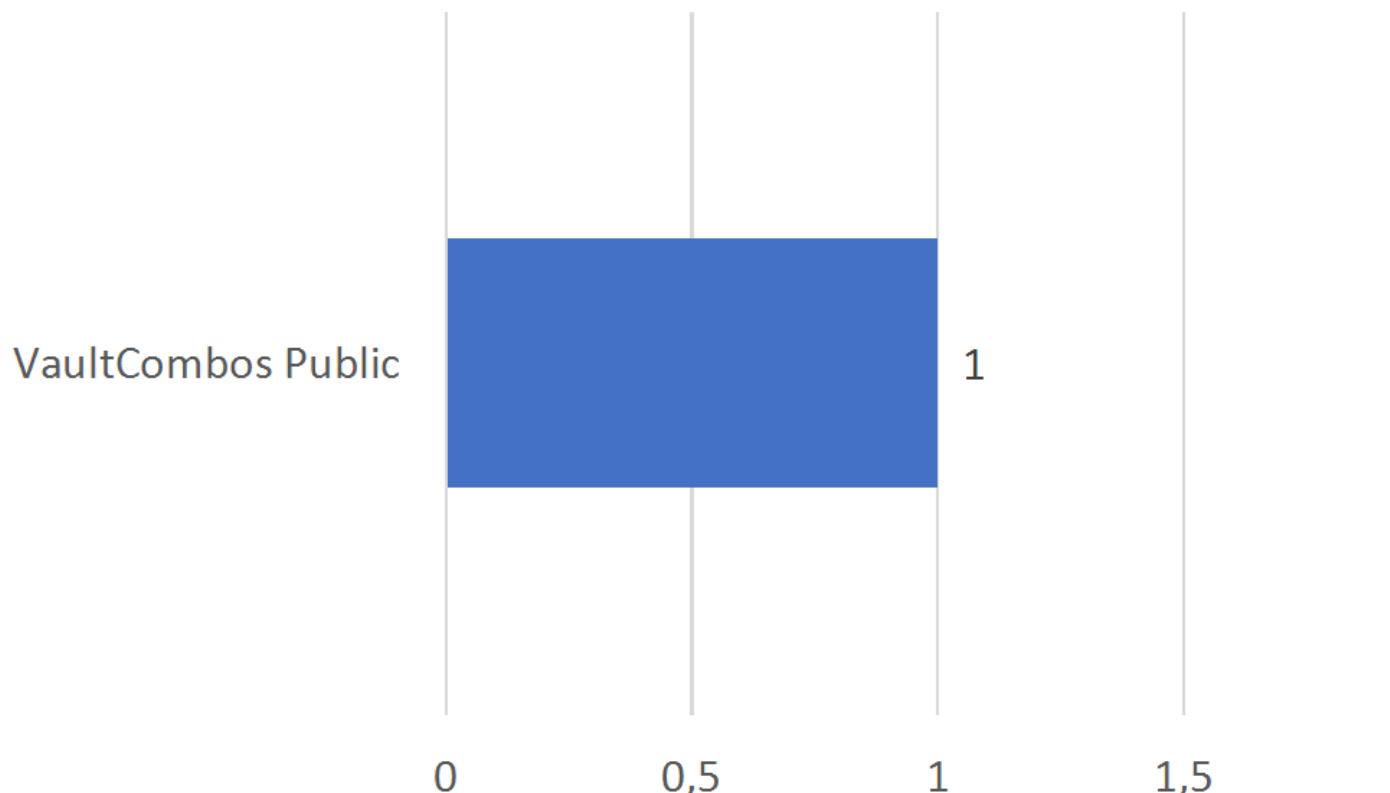
Leaked Credentials

Kebocoran yang terjadi pada aplikasi pihak ketiga (seperti e-commerce, aplikasi booking tiket, aplikasi booking penginapan dan lain-lain) akibat penggunaan email dinas Kondisi dimana email dinas digunakan untuk keperluan lain diluar kegiatan kedinasan.

Kategori Sumber Kebocoran Data



Sumber Kebocoran Data



KEMENTERIAN HUKUM
TERBATAS



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550



<https://bssn.go.id>



@bssn_ri



@bssn_ri



Badan Siber dan Sandi Negara



Melakukan validasi terhadap temuan kebocoran data kredensial (yang ditemukan pada darknet exposure) milik pegawai / pengguna.

1

2

Tidak Menggunakan software bajakan serta rutin update software serta menggunakan antivirus pada perangkat.



Mewajibkan update password secara berkala serta membuat tata kelola / peraturan sebagai upaya memitigasi risiko insiden kebocoran data.

3

4

Memberlakukan multi-factor authentication pagi para pengguna.



Tidak menggunakan email dinas diluar kepentingan kedinasan

5

6

Memberikan *security awareness* kepada sumber daya manusia atau pegawai agar waspada terhadap adanya upaya akses tidak sah atau manipulasi oleh penyerang. Hal ini dilakukan untuk mengurangi keberhasilan *spearphishing*, rekayasa sosial, dan teknik lain yang melibatkan interaksi pengguna yang seringkali menjadi rantai terlemah.



Melakukan koordinasi dan reaksi cepat tanggap kepada tim BSSN untuk meminimalkan dampak insiden siber.

7

KEMENTERIAN HUKUM





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

Mayjen TNI (Purn) dr. Roebiono Kertopati
(1914 – 1984)
Bapak Persandian Republik Indonesia

