



BADAN SIBER
DAN SANDI
NEGARA

LANSKAP KEAMANAN SIBER INDONESIA

2022





LANSKAP KEAMANAN SIBER INDONESIA **2022**

LANSKAP KEAMANAN SIBER INDONESIA 2022

TIM REDAKSI

Pelindung:

Kepala Badan Siber dan Sandi Negara
Letnan Jenderal TNI (Purn) Hinsa Siburian

Pengarah:

Deputi Bidang Operasi Keamanan Siber dan Sandi
Mayor Jenderal TNI Domingus Pakel, S.Sos., M.M.S.I

Penanggung Jawab:

Direktur Operasi Keamanan Siber
Andi Yusuf, M.T.

Pemimpin Redaksi:

Taufik Arianto, S.ST., M.Kom

Editor:

Andi Yusuf, M.T.
Taufik Arianto, S.ST., M.Kom
Claudia Dwi Amanda, S.ST., M.Mhan
Tim Komunikasi Publik BSSN

Layout & Desain:

Apriza Noer Ramadhan, S. Tr. Kom
Riam Kristallia, S.Tr.Kom

Tim Penyusun:

Taufik Nurhidayat, S.ST
Novian Nur Cahya, S.ST, M.Kom.
Hendri Malaka, S.ST
Claudia Dwi Amanda, S.ST., M.Mhan
Frizka Ferina, S.ST., M.M.
Jeni Rahman, S.S.T.MP
Rizki Yigitama, S.S.T.TP., M.T.
Zegar Pradipta Putra, S.Tr.TP
Bintang Telaga Must, S.Tr.TP
Senja Putra Sundara, S.Tr.TP
Sion Rebeca Tamba, S.Tr.MP
Damar Apri Sudarmadi, S.S.T.MP., M.Si.
Ghina Fitriya, S.Tr.Kom
Damayani Suyitno, S.Tr.Kom
Dwi Novazrianto, S.Tr.Kom
Ghina Mariyah Fairuz, S.Tr.Kom
Meilita Karendra Putri, S.Tr.Kom
M. Daffi Alhafizh, S.Tr.Kom
Mohammad Fathul Ikhsan, S.Tr.Kom
Nadya Marta Matanggwan, S.Tr.Kom
Rakai Sandya Ardiansyah, S.Tr.Kom
Restu Dwi Putro, S.Tr.Kom
Rico Setyawan, S.Tr.Kom
Satrya Abdi Widjaya, S.ST
Basuki Erwin Setiyadi, S.S.T.TP., M.Si.
Chandra Andjar Putra, S.Tr.MP., M.Si.
Fatmil Dwi Pambudi, S.Tr.TP
Rycka Septiasari, S.Tr.Kom
Aprilia Kusuma Dewi, S.Tr.Kom

Nurul Hidayah, S.Tr.Kom
Muhammad Fadhillah Fajari, S.Tr.Kom
Madani Shafurah, S.Tr.Kom
Rindu Alifa Maharani, S.Tr.Kom
Rizqy Rionaldy, S.Tr.Kom
Wahyu Rendra Aditya, S.Tr.Kom
Imas Purbasari, S.Tr.Kom
Indra Adi Putra, S.ST., M.M.
Nilam Qolbi, S.Tr.Kom
Alsita Putri Iriana, S.Tr.Kom
Muhammad Subkhan Arif, S.Tr.Kom
Apriza Noer Ramadhan, S.Tr.Kom
Rahma Humaira Nugraha, S.Tr.Kom
Surya Perdana Hasibuan, S.Tr.TP
Renaltha Puja Bagaskara, S.Tr.TP
Candra Kurniawan, S.Tr.Kom
Yahya Dzaky Rahmansyah, S.Tr.Kom
Bintang Wahyudono, S.Tr.Kom
Muhammad Zidni Hakami, S.Tr.Kom
Muhammad Jamil Daulima, S.Tr.Kom
Gifni Hammam Muyasar P., S.Tr.Kom
Zen Iqbal Dhananjaya, S.Tr.Kom
Manda Lusyia Azhari, S.Tr.MP.
We Muftihaturrahmah Tenri Sau, S.Tr.Kom
Dessisiliya Nurlaila Ramadhani, S.Tr.Kom
Muhammad Adib Nursumirat, S.Tr.Kom
Muhammad Aqil Hilmi, S.Tr.Kom
Esa Egistian Hartadi, S.Tr.Kom

Alamat Redaksi:

Direktorat Operasi Keamanan Siber

Badan Siber Dan Sandi Negara

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

DKI Jakarta, Indonesia 12550



Ingatlah bahwa kechilafan satu orang sahaja tjukup sudah menjebabkan keruntuhan negara.

*dr. Roebiono Kertopati
Bapak Persandian Indonesia*





**Letjen TNI (Purn)
Hinsa Siburian**

Kepala Badan Siber dan Sandi Negara



BSSN juga mengampanyekan gerakan **'Jaga Ruang Siber'** melalui berbagai kegiatan literasi digital untuk mengoptimalkan pemanfaatan sekaligus menghindari terjadinya penyalahgunaan ruang siber Indonesia.

SAMBUTAN

Kepala Badan Siber dan Sandi Negara

Seiring dengan kemajuan di bidang Teknologi, Informasi dan Komunikasi (TIK), keamanan siber menjadi salah satu isu strategis di Indonesia, dilihat dari terbukanya berbagai peluang kesejahteraan manusia seperti kemudahan dalam berkomunikasi maupun urusan bisnis khususnya ekonomi digital. Namun, perlu disadari bahwa semakin tinggi tingkat pemanfaatan Teknologi Informasi dan Komunikasi, akan berbanding lurus dengan jumlah serangan siber yang ada.

Dalam rangka mengamankan ruang siber nasional dibutuhkan Strategi Keamanan Siber. Berkaitan dengan hal tersebut, BSSN telah melakukan berbagai cara, antara lain dengan menyempurnakan pelaksanaan tugas Badan Siber dan Sandi Negara melalui Perpres Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara serta menyusun pengaturan strategis. BSSN juga terus melakukan optimalisasi pelaksanaan tugas dan fungsi pokok BSSN, terutama dalam penyelenggaraan keamanan siber dan sandi. Tidak hanya itu, BSSN juga mengampanyekan gerakan 'Jaga Ruang Siber' melalui berbagai kegiatan literasi digital untuk mengoptimalkan pemanfaatan sekaligus menghindari terjadinya penyalahgunaan ruang siber Indonesia.

Untuk itu, saya mendukung penuh adanya Lanskap Keamanan Siber Indonesia Tahun 2022 sebagai salah satu upaya BSSN dalam meningkatkan literasi digital masyarakat Indonesia dengan memberikan gambaran kepada masyarakat terkait dengan kondisi keamanan siber Indonesia pada tahun 2022. Saya harap, dengan adanya Lanskap Keamanan Siber Indonesia Tahun 2022, seluruh pihak dapat terus berpartisipasi aktif dalam menjaga keamanan ruang siber Indonesia.

Demikian yang dapat saya sampaikan, semoga Tuhan Yang Mahakuasa selalu memberikan bimbingan, kesehatan, dan kekuatan kepada kita semua dalam menjalankan setiap aktivitas sehingga tugas dan fungsi BSSN dapat terus berjalan dengan baik.



**Major Jeneral TNI
Dominggus Pakel,
S.Sos., M.M.S.I**

Deputi Bidang Operasi
Keamanan Siber dan Sandi



Sepanjang tahun 2022, berbagai jenis ancaman siber telah banyak menargetkan ruang siber Indonesia. Berkaitan dengan hal tersebut, berbagai upaya telah kami lakukan dengan terus meningkatkan kompetensi dan inovasi di bidang teknologi keamanan siber.

SAMBUTAN

Deputi Bidang Operasi Keamanan Siber dan Sandi

Sepanjang Tahun 2022 banyak yang terjadi pada ruang siber di Indonesia yang tentunya menjadi perhatian seluruh Indonesia.

BSSN selaku penanggung jawab keamanan siber di Indonesia memiliki peran penting untuk menjaga ruang siber Indonesia. Berkaitan dengan hal tersebut, Deputi Bidang Operasi Keamanan Siber dan Sandi (Deputi II) memiliki tugas menyelenggarakan perumusan dan pelaksanaan kebijakan teknis di bidang operasi keamanan siber dan sandi.

Selama Tahun 2022, Deputi II telah banyak menyelenggarakan kegiatan operasi keamanan siber dan sandi dengan melakukan kolaborasi bersama institusi lainnya dalam rangka meningkatkan efektivitas penyelenggaraan ruang siber yang aman. Deputi II juga ikut berpartisipasi pada kegiatan nasional maupun internasional untuk meningkatkan keamanan siber di Indonesia dengan melaksanakan koordinasi, perumusan, dan pelaksanaan kebijakan teknis di bidang operasi keamanan siber, operasi keamanan dan pengendalian informasi, serta operasi sandi.

Oleh karenanya, sebagai pertanggung jawaban kami dalam menjalankan tugas, Deputi II telah menyusun lanskap keamanan siber Indonesia tahun 2022 yang diharapkan dapat menjadi gambaran dan informasi terkait kondisi keamanan ruang siber di Indonesia sepanjang tahun 2022 sekaligus dapat membangun situational awareness di bidang siber untuk seluruh masyarakat Indonesia. Kami sadar bahwa masih banyak kekurangan dan keterbatasan yang perlu dibenahi dalam membangun keamanan siber nasional. Untuk itu, Deputi II terus berupaya meningkatkan kapabilitas dalam memperkuat pertahanan dan ketahanan siber dan sandi nasional.

Kontribusi serta peran dari institusi pemerintah, komunitas, maupun masyarakat sangat penting dalam menjaga ruang siber Indonesia yang lebih aman. Saya mengucapkan terima kasih atas bantuan serta kerjasama yang diberikan kepada BSSN khususnya Deputi II dalam membantu mengamankan dan meningkatkan ruang siber yang lebih aman. Saya berharap Lanskap Keamanan Siber Indonesia Tahun 2022 ini dapat meningkatkan kewaspadaan seluruh lapisan masyarakat terhadap ancaman siber yang ada.



SAMBUTAN

DIREKTUR OPERASI KEAMANAN SIBER

Marilah kita panjatkan puji syukur kehadirat Tuhan Yang Maha Esa karena atas karunia-Nya, Direktorat Operasi Keamanan Siber dan Sandi dapat membantu BSSN menjalankan fungsinya sesuai amanah Presiden melalui Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.

Sepanjang tahun 2022, berbagai jenis ancaman siber telah banyak menargetkan ruang siber Indonesia. Berkaitan dengan hal tersebut, berbagai upaya telah kami lakukan dengan terus meningkatkan kompetensi dan inovasi di bidang teknologi keamanan siber. Segala bentuk koordinasi, perumusan, dan pelaksanaan kebijakan teknis di bidang operasi keamanan siber telah dijalankan sesuai Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara. Sebagai bentuk pertanggung jawaban, kami telah menyusun Lanskap Keamanan Siber Indonesia Tahun 2022 yang berisikan kondisi keamanan siber di Indonesia selama Tahun 2022.

Dengan adanya laporan tahunan tersebut, diharapkan kita dapat mengetahui serta memahami lanskap kondisi ruang siber Indonesia sepanjang tahun 2022. Hal ini dapat digunakan menjadi salah satu acuan penentuan kebijakan strategis negara, serta menjadi rambu-rambu masyarakat dalam beraktivitas di ruang siber. Kami juga mengajak seluruh elemen masyarakat untuk senantiasa berkolaborasi dan bersinergi menjaga keutuhan ruang siber nasional dari berbagai ancaman siber. Demikian sambutan saya, semoga Tuhan Yang Maha Kuasa senantiasa memberikan kekuatan kepada kita dalam melaksanakan pengabdian terbaik kepada bangsa dan negara.



Kami mengajak seluruh elemen masyarakat untuk senantiasa berkolaborasi dan bersinergi menjaga keutuhan ruang siber nasional dari berbagai ancaman siber.

Daftar Isi

SUMMARY	10
Profil Direktorat Operasi Keamanan Siber	12
Tren Trafik Anomali	14
• Trafik Anomali Serangan Siber di Indonesia	15
• Top 10 Trafik Anomali	16
• Top 10 Negara Sumber dan Tujuan	20
• Aktivitas Advanced Persistent Threat (APT)	21
Rekapitulasi Insiden Siber	23
• Web Defacement	24
• Aduan Siber dan Notifikasi	28
• Cyber Threat Intelligence	31
Top 5 Common Vulnerabilities and Exposures (CVE)	34
• Top 5 CVE Global	35
• Top 5 CVE Nasional	39



Kampanye Phishing

- Phishing via .APK
- Phishing Perbankan

Highlight IT Security Assessment (ITSA)

- ITSA pada Aplikasi Strategis
- Top 5 Kerentanan

Dukungan Keamanan Siber dan Sandi pada Event Nasional dan Internasional

Kolaborasi BSSN Pada Event Nasional dan Internasional

Lesson Learned Top 3 Insiden Siber

- Insiden Kebocoran Data
- Insiden Ransomware
- Insiden Web Defacement

Prediksi Ancaman Siber Tahun 2023

45

46

47

49

50

52

54

59

70

72

77

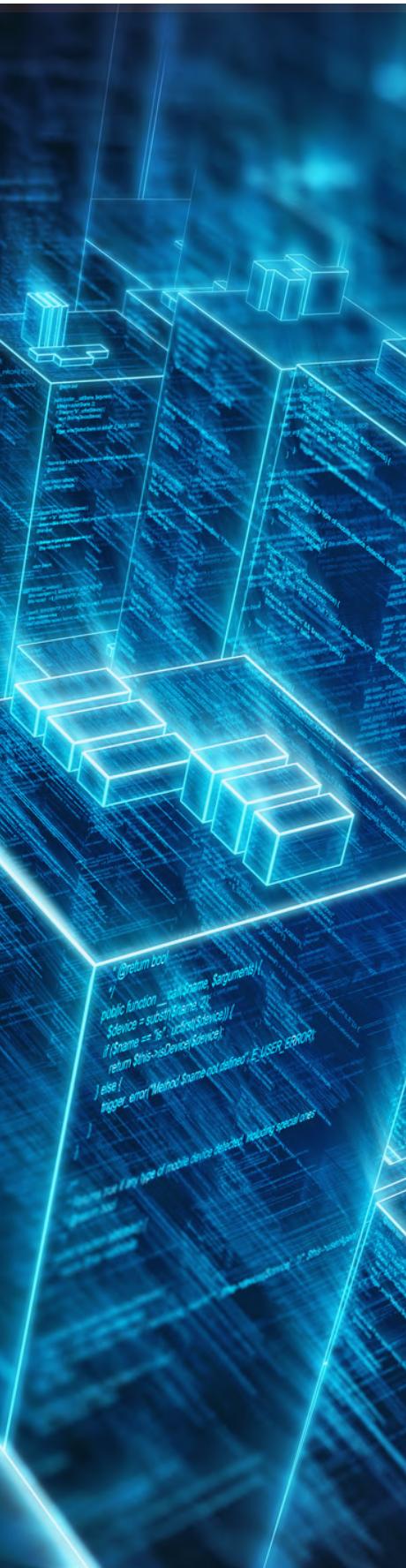
82

86



SUMMARY

Total trafik anomali di Indonesia selama tahun 2022 adalah **976.429.996 anomali** dengan jenis trafik anomali tertinggi yaitu **MyloBot Botnet** yang memungkinkan penyerang untuk mengambil kendali penuh atas sistem pengguna. Terdapat **4.421.992 aktivitas APT** serta **2.348 kasus Web Defacement** yang terjadi di Indonesia pada tahun 2022. Berdasarkan laporan yang diterima dari stakeholder pada layanan aduan siber, didapatkan sebanyak **236 aduan** selama tahun 2022 dengan sektor terbanyak pada aduan siber yang diterima adalah **sektor administrasi pemerintahan** dan kategori aduan berupa **Misconfiguration**. BSSN telah mengirimkan **1.433 notifikasi indikasi insiden** ke stakeholder dengan jenis notifikasi terbanyak dikirimkan adalah *Web Defacement*. Selain itu, melalui layanan *Cyber Threat Intelligence*, BSSN juga melakukan penelusuran dugaan insiden siber dengan jumlah total **399 dugaan insiden siber** dengan jumlah jenis dugaan insiden tertinggi yaitu **data breach**. Hasil penelusuran pada Darknet, ditemukan adanya *Credential Exposure* yang berdampak pada **427 stakeholder** di Indonesia. Adapun pengelompokan sektor dilakukan berdasarkan Peraturan Presiden No. 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV).



Pada tahun 2022, **CVE-2022-21907** merupakan jenis kerentanan yang perlu menjadi perhatian secara global karena memungkinkan penyerang dapat memperoleh akses ke Windows Server dan melakukan eksekusi kode secara *remote*. CVE-2022-22536 merupakan jenis kerentanan yang perlu menjadi perhatian di Indonesia karena memungkinkan penyerang dapat menambahkan *request* untuk menyamar sebagai pengguna atau manipulasi inputan *cache web*. Salah satu layanan yang dilakukan BSSN terhadap stakeholder adalah IT Security Assessment (ITSA). Hasil ITSA yang dilakukan oleh BSSN tahun 2022, ditemukan sebanyak **1.950 celah keamanan** dari **457 sistem elektronik** pada berbagai aplikasi yang digunakan oleh masyarakat secara luas. Jenis kerentanan tertinggi dengan tingkat risiko *critical* yang ditemukan selama pelaksanaan ITSA tahun 2022 adalah *Insecure Data Object Reference* (IDOR).

BSSN turut berperan aktif memberikan dukungan keamanan siber dan sandi pada *event* nasional serta internasional di Indonesia selama tahun 2022 dalam bentuk pengujian keamanan terhadap sistem elektronik, pemasangan perangkat deteksi dan monitoring pada perangkat jaringan pada ISP dan di *site event*, melakukan deteksi dini ancaman siber, melaksanakan upaya tanggap insiden dan *digital forensic incident response* (DFIR) ketika terjadi insiden siber, serta upaya perbaikan terhadap sistem elektronik yang memiliki celah keamanan. BSSN juga melakukan kolaborasi dengan berbagai *stakeholder* di Indonesia serta aktif mengikuti forum-forum Internasional untuk meningkatkan keamanan siber sebagai upaya untuk menjaga ruang siber Indonesia. Kerja sama yang dilakukan oleh BSSN meliputi kerja sama layanan Laboratorium Forensik Digital (LFD) BSSN dan Kolaborasi Internasional ID-SIRTII/CC. Total barang bukti yang diproses oleh LFD BSSN selama tahun 2022 adalah **406 barang bukti**.

Dalam rangka mengantisipasi dan mencegah terjadinya insiden siber, maka langkah yang dapat dilakukan di antaranya melakukan IT Security Assessment pada sistem informasi yang dimiliki, menerapkan kebijakan penggunaan *strong password*, melakukan edukasi terhadap pengguna sistem, melakukan reviu akun sistem dan aplikasi, dan lain-lain. Berdasarkan pencarian yang dilakukan melalui sumber pencarian terbuka dan analisis data *monitoring* lalu lintas jaringan pada tahun 2022, didapatkan adanya beberapa ancaman siber yang diprediksi akan muncul di tahun 2023. Ancaman siber tersebut meliputi *Ransomware*, Kebocoran Data, Serangan APT, *Phishing*, *Cryptojacking*, DDoS, Serangan RDP, *Web Defacement*, serta *Social Engineering*.



PROFIL

DIREKTORAT OPERASI KEAMANAN SIBER

Badan Siber dan Sandi Negara

Berdasarkan Peraturan Presiden No. 53 Tahun 2017

Badan Siber dan Sandi Negara (BSSN) merupakan transformasi peleburan Lembaga pemerintah yang telah ada sebelumnya, yaitu Lembaga Sandi Negara (Lemsaneg). Bersama dengan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika (Kemenkominfo) serta Indonesia Security Incident Response Team on Internet Infrastructure (Id-SIRTII) melalui Perpres Nomor 53 tahun 2017 tentang BSSN yang selanjutnya disempurnakan dengan Perpres Nomor 133 tahun 2017.

Direktorat Operasi Keamanan Siber

Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021

Presiden Republik Indonesia Joko Widodo pada tanggal 13 April 2021 menandatangani Peraturan Presiden (Perpres) Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (BSSN). Penerbitan Perpres tersebut dilandasi karena perlu dilakukannya penataan organisasi BSSN dalam rangka mewujudkan keamanan, perlindungan, dan kedaulatan siber nasional, serta meningkatkan pertumbuhan ekonomi nasional. Peraturan tersebut diterbitkan untuk mengoptimalkan pelaksanaan tugas dan fungsi organisasi BSSN di bidang keamanan siber dan sandi sehingga dapat dilakukan dengan lebih efektif dan efisien. Organisasi dan Tata Kerja BSSN kemudian diatur dalam Peraturan BSSN Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja BSSN.



Direktorat Operasi Keamanan Siber

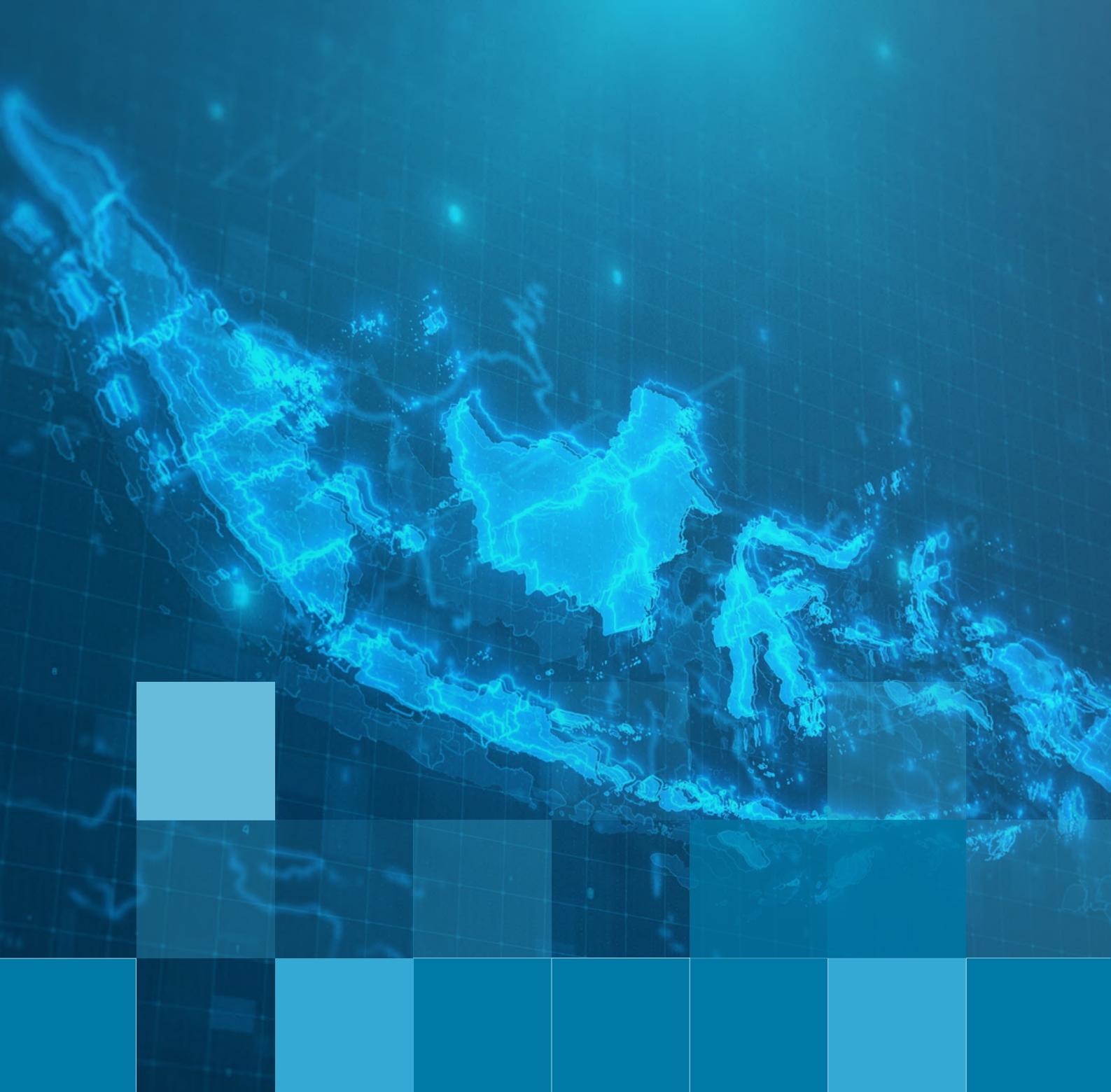
Direktorat Operasi Keamanan Siber mempunyai tugas melaksanakan koordinasi, perumusan, dan pelaksanaan kebijakan teknis di bidang operasi keamanan siber.

DIREKTORAT OPERASI KEAMANAN SIBER

Direktorat Operasi Keamanan Siber merupakan salah satu unit kerja yang berada di bawah Deputi Bidang Operasi Keamanan Siber dan Sandi, Badan Siber dan Sandi Negara. Unit kerja ini berdampingan dengan Direktorat Operasi Keamanan dan Pengendalian Informasi serta Direktorat Operasi Sandi. Direktorat Operasi Keamanan Siber mempunyai tugas melaksanakan koordinasi, perumusan, dan pelaksanaan kebijakan teknis di bidang operasi keamanan siber. Dalam melaksanakan tugasnya, Direktorat Operasi Keamanan Siber menyelenggarakan fungsi:



- Penyiapan perumusan kebijakan teknis operasional di bidang identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan;
- Penyiapan koordinasi dan pelaksanaan identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan;
- Pengelolaan tanggap insiden siber nasional dan sektor pemerintah, kontak siber nasional, serta pengelolaan krisis siber nasional;
- Pengelolaan informasi dini ancaman siber dan analisis *big data* serta analisis *malware*;
- Pelaksanaan dukungan penyidikan, forensik digital, dan pertolongan ahli;
- Pelaksanaan pemantauan, evaluasi, dan pelaporan di bidang operasi keamanan siber; dan
- Pelaksanaan urusan perencanaan, keuangan, rumah tangga, kepegawaian, ketatalaksanaan, persuratan, kearsipan, serta penyusunan evaluasi dan pelaporan Direktorat.



TREN TRAFIK ANOMALI

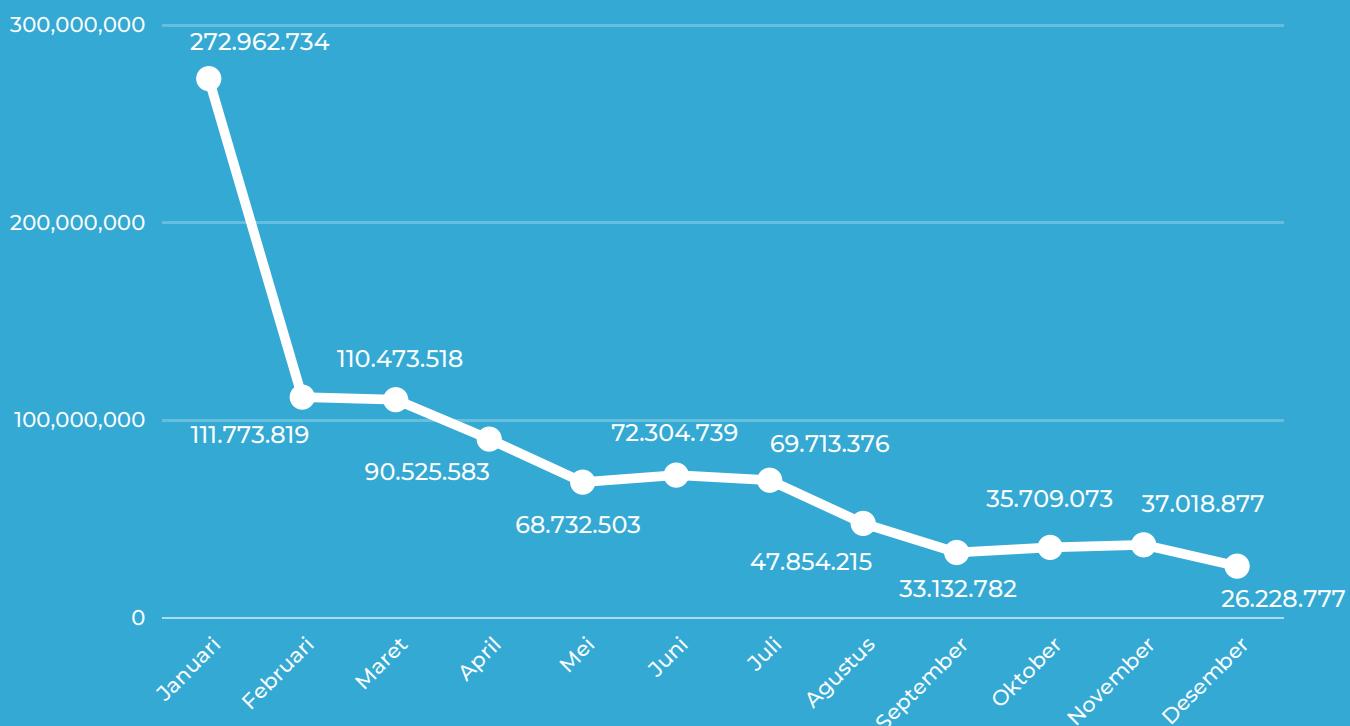
2022

Trafik Anomali Serangan Siber di Indonesia

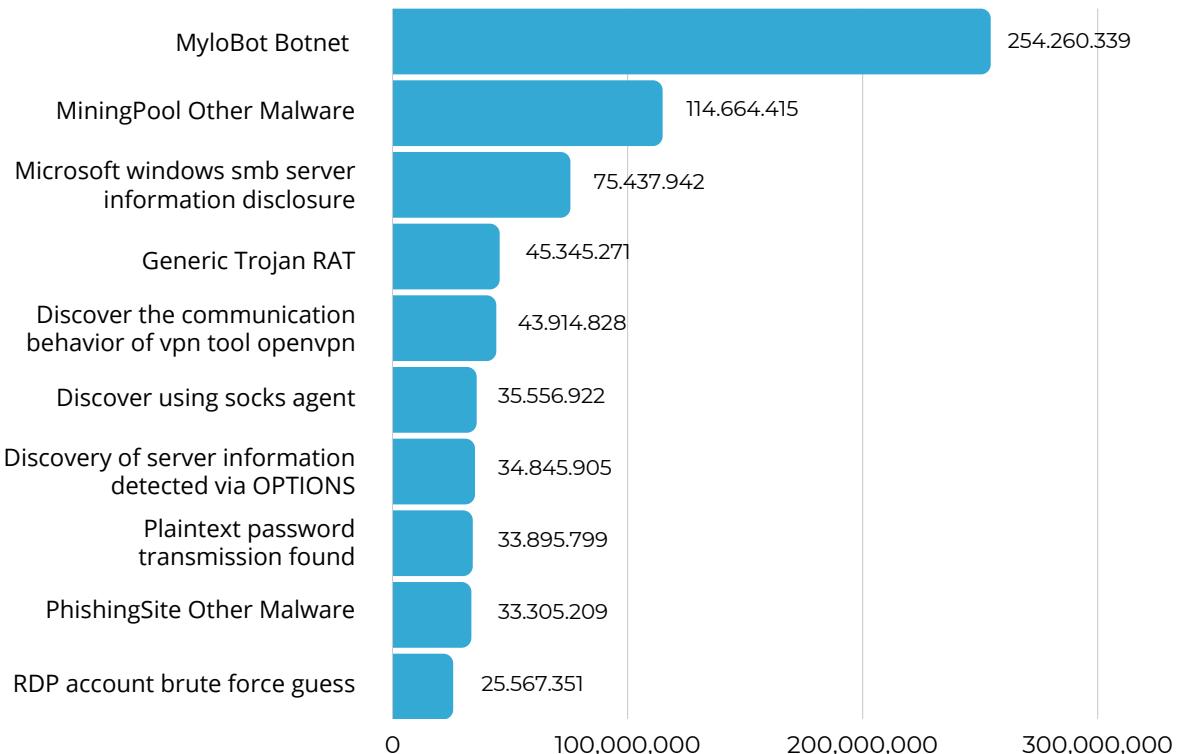
976.429.996

Total Trafik Anomali
Tahun 2022

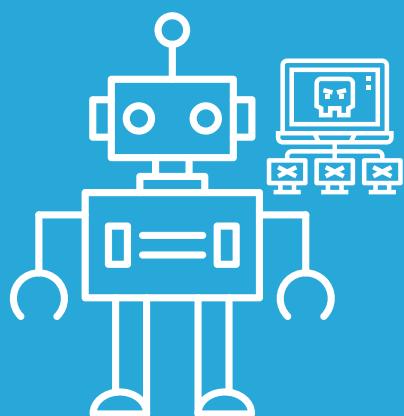
Total trafik anomali di Indonesia selama tahun 2022 adalah **976.429.996 anomali**. Jumlah anomali trafik pada tahun 2022 mengalami penurunan yang signifikan hingga 40% lebih dari tahun sebelumnya. Adapun penyebab penurunan trafik anomali disebabkan karena terjadinya penurunan trafik pada sensor yang dipasang di ISP dan penurunan jumlah *Indicator of Compromise* (IoC) yang terdeteksi. Grafik trafik anomali periode Januari - Desember 2022 dapat dilihat pada gambar berikut :



TOP 10 TRAFIK ANOMALI



#1 MyloBot Botnet



Mylobot Botnet adalah salah satu jenis *botnet* yang menargetkan dan dapat mengambil alih perangkat yang menjalankan sistem operasi Windows. *Botnet* ini menyebar melalui spam *e-mail* dan unduhan *file* yang telah terinfeksi. Mylobot sangat berbahaya karena memiliki kemampuan mengunduh dan mengeksekusi semua jenis muatan setelah berhasil menginfeksi. Fungsi utama *botnet* memungkinkan penyerang untuk mengambil kendali penuh atas sistem pengguna, salah satunya berfungsi sebagai gerbang untuk mengunduh muatan (*payload*) tambahan dari server *Command and Control*.

Perilaku umum Mylobot melakukan *callback* ke domain-domain yang dihasilkan dari *Domain Generation Algorithm* (DGA). DGA menjadi salah satu metode yang digunakan untuk mempersulit deteksi terhadap aktivitas *malware*, karena DGA merupakan algoritma yang digunakan oleh penyerang untuk membangkitkan nama domain yang berbeda-beda dengan karakteristik dan pola penamaan yang acak dalam jumlah besar, sehingga dapat dimanfaatkan oleh penyerang untuk berkomunikasi ke *Command and Control* (C&C). Mylobot juga memiliki teknik anti-VM dan anti-sandboxing yang canggih untuk menghindari deteksi dari proses analisis. Mylobot Botnet menargetkan sistem operasi Microsoft Windows yang menyebar melalui spam *e-mail* dan unduhan *file* yang telah terinfeksi. Setelah terinstal, Botnet mematikan Windows Defender dan Windows Update dan memblokir *port* tambahan di *firewall*.

#2 MiningPool

MiningPool adalah suatu program yang khusus digunakan untuk melakukan penambangan mata uang kripto (*cryptocurrency*) di perangkat komputer atau server secara diam-diam tanpa adanya otoritas yang sah dari pemilik perangkat. MiningPool biasanya menggunakan sumber daya (misalnya aktivitas CPU) dari korban untuk melakukan penambangan, sehingga bedampak perangkat korban akan mengalami penurunan kinerja seperti daya, memori, dan kegunaan operasional dari perangkat yang telah terinfeksi program tersebut. Metode penyebaran yang dilakukan penyerang adalah menggunakan *e-mail phishing*.

#3 Microsoft Windows SMB Server Information Disclosure

Kerentanan ini terdapat pada komponen SMBv1 pada Microsoft Windows SMB Server, sehingga mengakibatkan penyerang dapat mengambil informasi sensitif dari memori dengan mengirimkan *crafted packets*. Perangkat-perangkat yang terinfeksi diantaranya: Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10, Windows Server 2016.

#4 Generic Trojan RAT

Generic Trojan merupakan program berbahaya yang digunakan untuk mencuri informasi dari perangkat yang terinfeksi dengan melakukan *remote access*. *Trojan* dapat menyebar melalui lampiran *e-mail*, tautan berbahaya, *drive*, maupun dikirimkan dari *malware* lainnya. Tanda-tanda sistem yang terinfeksi Generic Trojan RAT adalah kinerja sistem yang melambat, konfigurasi sistem berubah, menampilkan pesan *error*, dan perilaku sistem yang mencurigakan. *Trojan* merupakan program berbahaya yang berkamuflase sedemikian rupa dalam bentuk aplikasi yang *legitimate* dan terkadang sulit bagi pengguna untuk dapat membedakannya, sehingga pengguna secara tidak sadar memasang aplikasi tersebut. Setelah aplikasi tersebut terpasang pada komputer pengguna, *trojan* akan menjalankan program-program pada *background process* tanpa diketahui oleh pengguna.

#5 Discover The Communication Behavior of VPN Tool OpenVPN

OpenVPN merupakan sebuah aplikasi/*software* berbasis *open-source* yang digunakan untuk melakukan koneksi ke internet dengan melalui *Virtual Private Network* (VPN). OpenVPN akan membuat koneksi dengan menggunakan *Point to Point* (PTP) *Tunnel* yang telah dienkripsi menggunakan *username* dan *password*. Aplikasi/*software* ini sebenarnya legal, namun saat ini *threat actor* dapat menyisipkan sebuah *malware* ke dalam aplikasi OpenVPN dan digunakan untuk memata-matai aset korban. Oleh karena itu, ketika menggunakan aplikasi OpenVPN perlu dipastikan aplikasi tersebut diunduh dari *market store* yang resmi dan menggunakan versi yang *update*.

#6 Discover Using Socks Agent

Socks (*Socket Secure*) proxy merupakan *framework* yang digunakan untuk melakukan *routing* dari berbagai jenis program ataupun protokol. Socks proxy akan melakukan *bypass* terhadap *firewall*, sehingga akan terjalin komunikasi *Transmission Control Protocol* (TCP) ataupun *User Datagram Protocol* (UDP) dari server di internet ke *endpoint*/perangkat yang berada setelah *firewall*. Socks proxy juga dapat dimanfaatkan untuk melakukan kejahatan siber, seperti pemanfaatan socks proxy untuk melakukan serangan DDoS (*Distributed Denial of Service*) dan membuat koneksi untuk melewati *firewall*.

#7 Discovery of Server Information Detected via OPTIONS

Penyerang menggunakan metode HTTP OPTIONS agar dapat melakukan komunikasi yang didukung oleh sumber daya tujuan, seperti informasi versi server, *request method* oleh server, dan lain-lain. Kegiatan ini dilakukan agar diperoleh informasi terkait server, sehingga memudahkan penyerang untuk melakukan eksplorasi selanjutnya.

#8 Plaintext Password Transmission Found

Anomali ini terkait dengan perolehan transmisi kata sandi dalam bentuk teks *plain* (tidak dienkripsi), hal ini dapat memungkinkan penyerang dapat masuk dan mengakses ke dalam sistem korban. Oleh karena itu, diperlukan penggunaan protokol yang terenkripsi seperti *Hypertext Transfer Protocol Secure* (HTTPS).

#9 PhishingSite Other Malware

PhishingSite merupakan salah satu aktivitas infeksi *malware* dengan memanfaatkan metode *phishing* dalam menyebarluaskan atau melakukan infeksi *malware* pada perangkat korban, seperti mengirimkan *e-mail phising* berisi dokumen yang didalamnya telah disisipkan *malware* tertentu.

#10 Remote Desktop Protocol (RDP) Account Brute Force Guess

Dalam serangan *brute force* RDP, penyerang menggunakan pemindai jaringan untuk mengidentifikasi rentang *port IP* dan TCP yang digunakan oleh server RDP. Setelah melakukan pemindaian, penyerang mencoba mendapatkan akses ke sistem (biasanya sebagai administrator) dengan menggunakan program yang secara otomatis mencoba untuk *login* berulang kali dengan menggunakan segala kemungkinan kombinasi *username* dan *password* yang ada. Setelah penyerang memiliki akses melalui RDP, penyerang dapat melakukan aktivitas yang sesuai dengan hak akun yang diretasnya. Penyerang yang telah mendapatkan akses administrator dapat melakukan penonaktifan perangkat lunak antivirus, melakukan instalasi *malware*, mencuri data/informasi pribadi, melakukan enkripsi *file*, dan lainnya.



Berdasarkan anomali yang dideteksi melalui monitoring yang dilakukan, didapatkan alamat IP sumber dan tujuan anomali. Alamat IP tersebut dapat menunjukkan dari negara mana anomali berasal dan ke negara mana anomali ditujukan.

Adapun negara-negara yang terdeteksi sebagai sumber anomali, belum dapat dipastikan sebagai negara asal anomali karena penyerang berpotensi menggunakan proxy yang bertujuan menyembunyikan atau menyamarkan alamat IP asli penyerang.

TOP 10 NEGARA SUMBER DAN TUJUAN



TOP 10 SUMBER ANOMALI

	Amerika Serikat	213.451.490
--	-----------------	-------------

	Singapura	11.193.352
--	-----------	------------

	Indonesia	193.250.972
--	-----------	-------------

	Britania Raya	10.894.478
--	---------------	------------

	Belanda	27.857.574
--	---------	------------

	Jerman	8.809.948
--	--------	-----------

	Tiongkok	22.894.253
--	----------	------------

	Korea Selatan	8.712.496
--	---------------	-----------

	Rusia	13.111.832
--	-------	------------

	Perancis	7.705.614
--	----------	-----------

TOP 10 TUJUAN ANOMALI

	Indonesia	539.933.976
--	-----------	-------------

	Belanda	6.669.047
--	---------	-----------

	Amerika Serikat	117.504.939
--	-----------------	-------------

	Rusia	6.449.615
--	-------	-----------

	Jerman	13.960.055
--	--------	------------

	Tiongkok	4.657.653
--	----------	-----------

	Singapura	12.226.894
--	-----------	------------

	Britania Raya	3.793.598
--	---------------	-----------

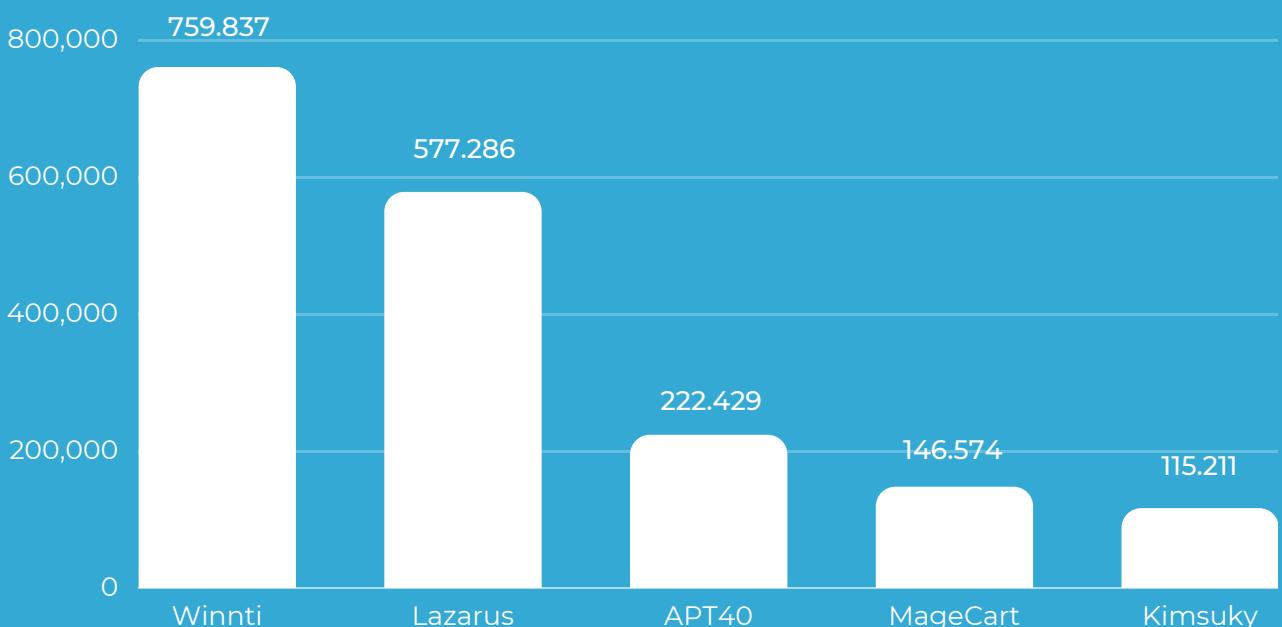
	Kanada	8.463.939
--	--------	-----------

	Perancis	3.785.477
--	----------	-----------

Aktivitas Advanced Persistent Threat

4.421.992 Aktivitas APT di Indonesia
Tahun 2022

Advanced Persistent Threat (APT) merupakan *attack campaign* yang dilakukan oleh *threat actor*, dapat bersifat *state-sponsored actor* maupun *non-state sponsored actor*. *Threat actor* ini menggunakan berbagai metode/teknik canggih yang dirancang untuk melakukan serangan siber secara *persistent*, *sophisticated*, dan *clandestine* untuk mendapatkan akses ke sistem dan bertahan dalam sistem tersebut dalam jangka waktu yang lama. APT memiliki dampak, seperti pencurian data, perolehan akses masuk ke sistem, merusak sistem, maupun spionase. Terdapat **4.421.992 aktivitas APT** di Indonesia selama tahun 2022. Berikut adalah tabel yang memperlihatkan aktivitas APT yang paling banyak menyerang di Indonesia:





Advanced Persistent Threat

Pelaku ancaman siber berupa kelompok yang biasanya disponsori oleh negara atau organisasi besar lain dengan tujuan untuk memperoleh akses tidak sah ke jaringan komputer target dan tetap tidak terdeteksi untuk jangka waktu yang lama.

Winnti

Winnti atau disebut dengan Blackfly atau Wicked Panda, merupakan grup / *threat actor* berasal dari Tiongkok yang memiliki tujuan untuk mencuri informasi dan melakukan mata-mata dan diketahui mulai aktif sejak tahun 2010.

Lazarus

Lazarus atau disebut Hidden Cobra, Labyrinth Chollima merupakan grup / *threat actor* berasal dari Korea Utara yang memiliki tujuan untuk pencurian informasi, spionase, sabotase, dan beberapa kejahatan finansial.

APT40

APT 40 atau disebut Leviathan, Bronze Mohawk, merupakan grup / *threat actor* berasal dari Cina yang memiliki tujuan untuk melakukan pencurian informasi dan spionase. *Threat actor* ini diketahui mulai aktif beroperasi dari tahun 2009.

MageCart

MageCart atau disebut FIN 6, Skeleton Spider, merupakan grup / *threat actor* yang memiliki tujuan untuk melakukan pencurian informasi khususnya terkait sektor finansial.

Kimsuky

Kimsuky atau disebut dengan Thallium, Black Banshee, Velvet Chollima, merupakan grup / *threat actor* yang berasal dari Korea Utara dengan tujuan untuk melakukan pencurian informasi dan mata-mata. Dugaan *threat actor* ini berasal dari Korea Utara berdasarkan ditemukannya *string* dengan berbahasa Korea pada *malware* yang digunakan dalam *campaign* ini.



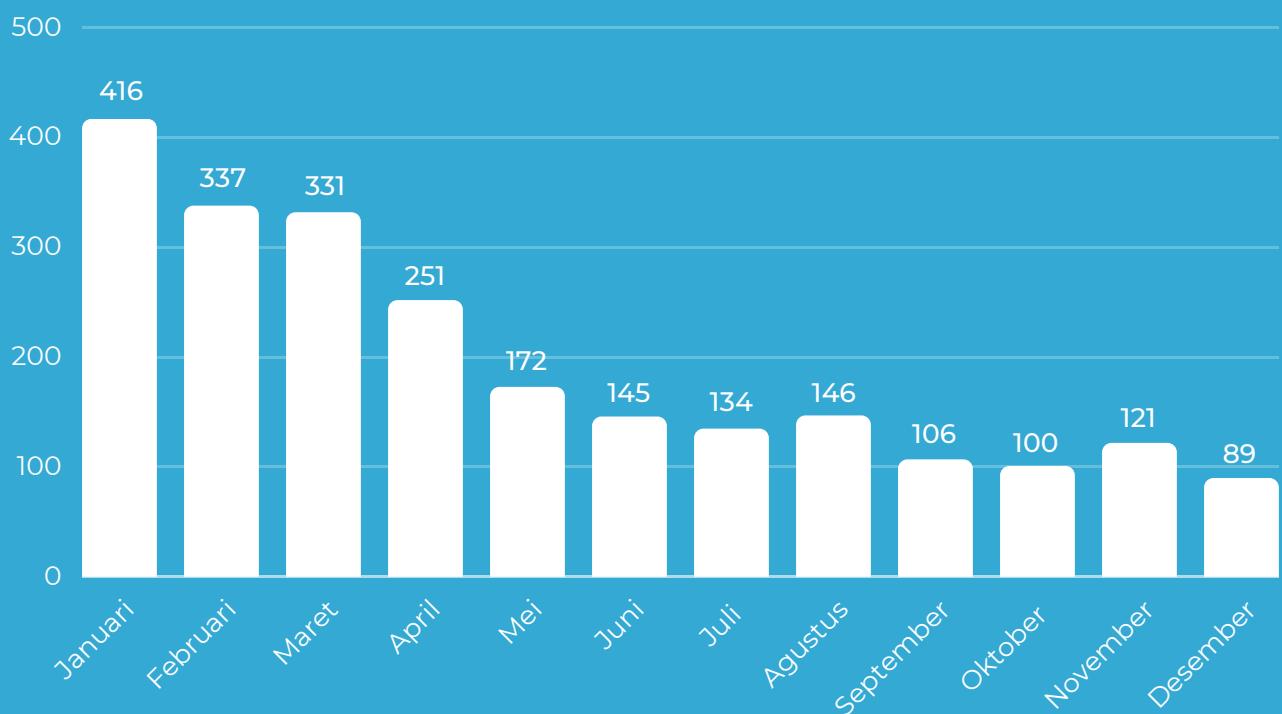
REKAPITULASI INSIDEN SIBER

2022

WEB DEFACEMENT

2.348 kasus

Serangan *web defacement* merupakan serangan yang dilakukan untuk mengeksloitasi situs web atau server web yang rentan dengan memanfaatkan kerentanan dari sistem sehingga penyerang dapat merusak, memodifikasi, atau menghapus konten halaman web yang telah diretas. Pelaku serangan *web defacement* disebut sebagai *defacer*. Selama tahun 2022, BSSN telah mencatat terdapat **2.348 kasus** *web defacement* yang terjadi di situs-situs Indonesia dengan kasus terbanyak terjadi pada bulan Januari dengan jumlah kasus sebanyak **416 kasus** *web defacement*.



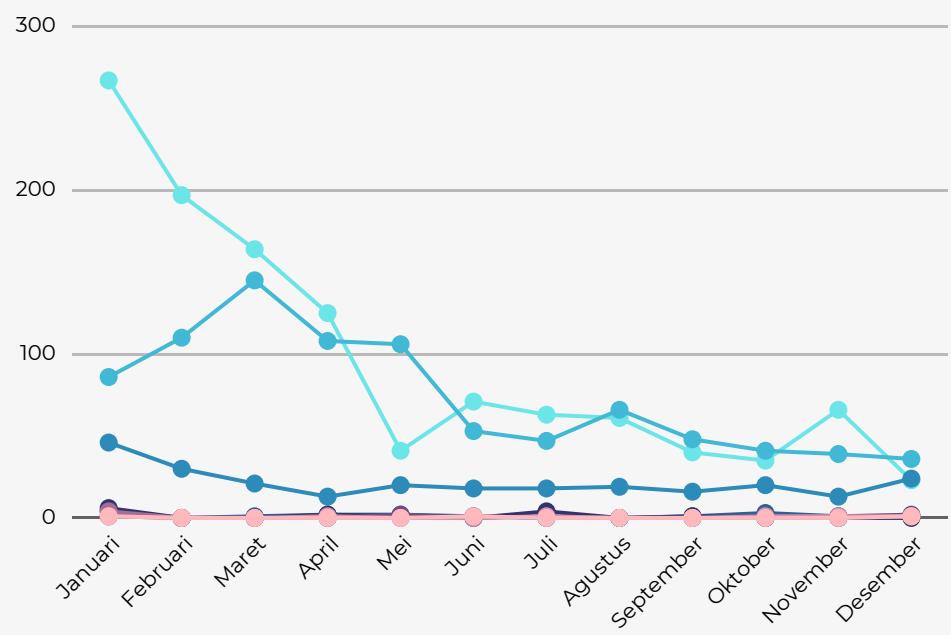
Sektor Terdampak Web Defacement

Selama tahun 2022, sektor yang paling banyak terkena serangan *web defacement* adalah sektor **Administrasi Pemerintahan** dengan jumlah kasus sebanyak **885 kasus**.



Legend:

Lainnya	Adm. Pemerintahan	Pertahanan	Kesehatan	TIK	Pangan	Keuangan	ESDM	Transportasi
---------	-------------------	------------	-----------	-----	--------	----------	------	--------------



Pengelompokan kasus *web defacement* berdasarkan sebaran waktu bertujuan untuk mengetahui waktu terbanyak terjadinya *web defacement*. Berdasarkan hasil pengelompokan tersebut diketahui bahwa kasus *web defacement* paling banyak terjadi pada **Weekdays (Senin-Jumat) pada pukul 18.00 - 06.00 WIB** dengan jumlah kasus sebanyak **1045 kasus**.

SEBARAN WAKTU

Weekdays

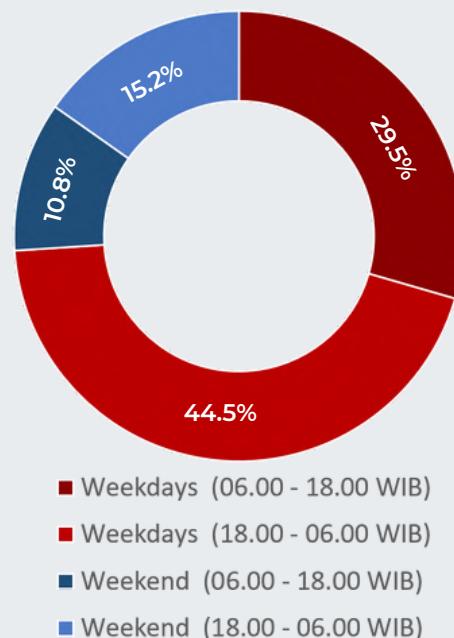
692 KASUS — 06.00 - 18.00 WIB

1045 KASUS — 18.00 - 06.00 WIB

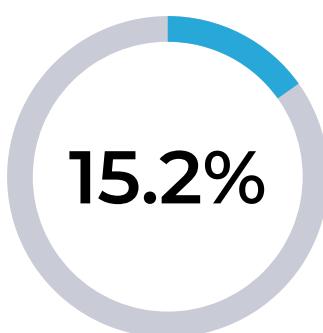
Weekend

253 KASUS — 06.00 - 18.00 WIB

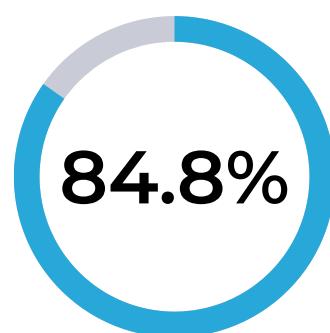
358 KASUS — 18.00 - 06.00 WIB



Secara umum, kasus *web defacement* terjadi pada *homepage* dan *hidden page* (tersembunyi). Dalam tahun 2022, kasus yang paling banyak ditemukan adalah kasus *web defacement* tersembunyi sebanyak 1992 kasus. Kasus *web defacement* pada *homepage* berarti lokasi *defacement* terletak di halaman utama web sehingga ketika pengguna mencoba mengakses situs tersebut maka web akan menampilkan halaman *defacement* tersebut. Sedangkan untuk *web defacement* yang *hidden* berarti *defacement* terletak di lokasi tertentu selain halaman utamanya. Oleh karena itu, ketika pengguna mengakses web terinfeksi belum tentu menemukan halaman *defacement* tersebut.



Homepage
356 kasus

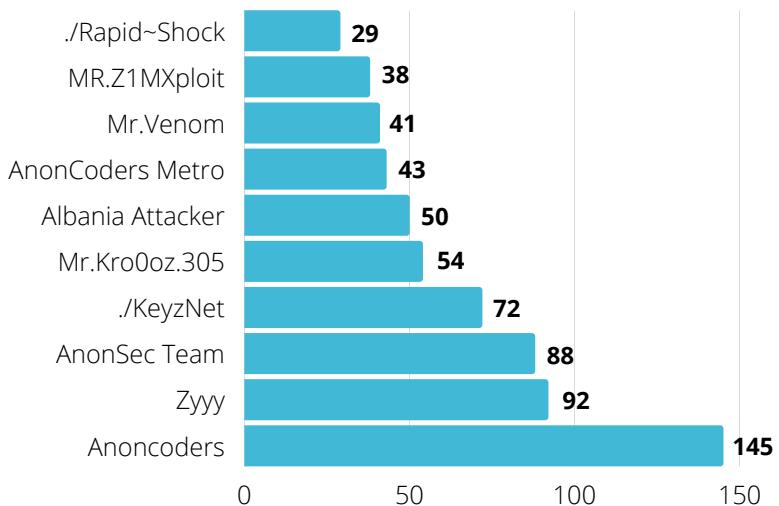


Tersembunyi
1992 kasus



NOTIFIER WEB DEFACEMENT

Berdasarkan data yang tercatat, *notifier web defacement* terbanyak selama tahun 2022 adalah Anoncoders dengan jumlah kasus sebanyak **145 kasus**.



PENCEGAHAN WEB DEFACEMENT



Menerapkan kebijakan pembuatan *password* sesuai dengan kriteria *strong password* kepada setiap pengguna serta tidak menggunakan *default username* dan *password*.



Melakukan pembaruan sistem secara berkala



Melakukan pemeriksaan terhadap konfigurasi yang telah diterapkan. Selain itu, melakukan audit atau *penetration testing* juga dapat membantu pemilik sistem elektronik untuk mengidentifikasi kerentanan termasuk kesalahan konfigurasi.

Aplikasi seharusnya dibangun dengan memperhatikan keamanannya, misalnya melakukan sanitasi input pengguna. Selain itu, sebagai pengamanan tambahan seharusnya server menerapkan *Web Application Firewall* (WAF).

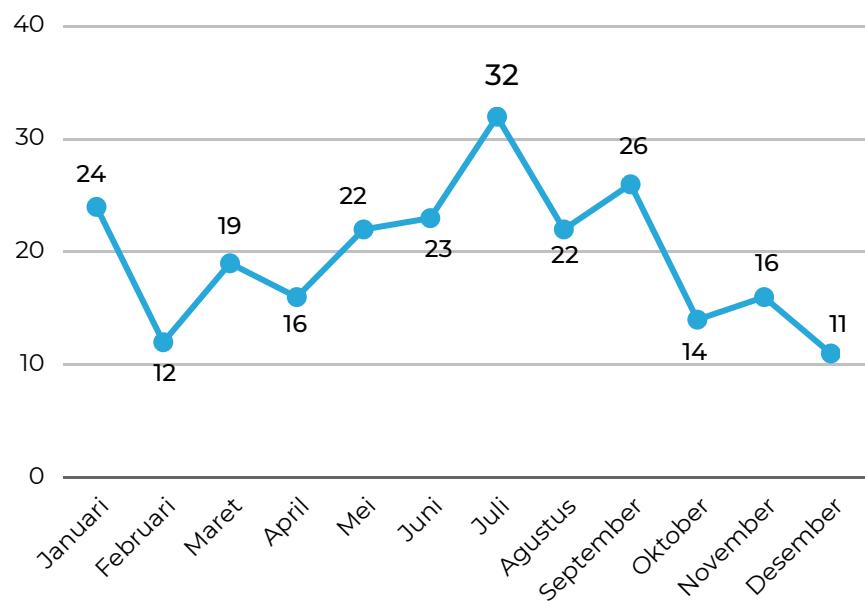


Aduan Siber

236
Aduan

Aduan siber yang diterima oleh BSSN selama 2022

Aduan siber paling banyak diterima BSSN pada bulan **Juli 2022** yaitu sebanyak **32 aduan**



Rekapitulasi Aduan Siber Berdasarkan Sektor

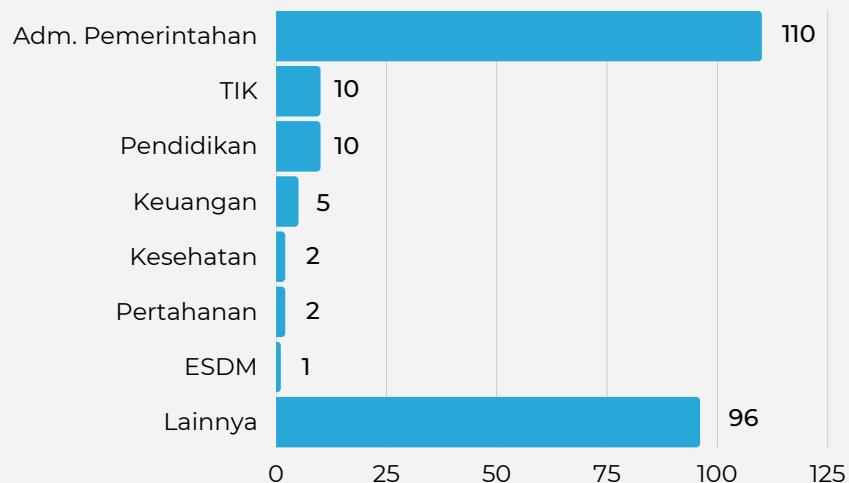


Puskober

Media yang dapat digunakan oleh masyarakat untuk melakukan pelaporan aduan siber, yaitu melalui telepon, surat elektronik (*e-mail*), ataupun datang secara langsung ke Kantor BSSN.

+6281281354598

bantuan70@bssn.go.id



Kategori Aduan Siber

Aduan siber yang diterima oleh BSSN terdiri dari 13 kategori aduan dengan 3 kategori tertinggi yaitu sebagai berikut:

37%

Misconfiguration

aduan dari masyarakat terkait laporan kesalahan konfigurasi yang menyebabkan kerentanan pada sistem elektronik

21%

Cybercrimes

aduan dari masyarakat yang menjadi korban kejahatan siber seperti penipuan, pemerasan, dan judi *online*

15%

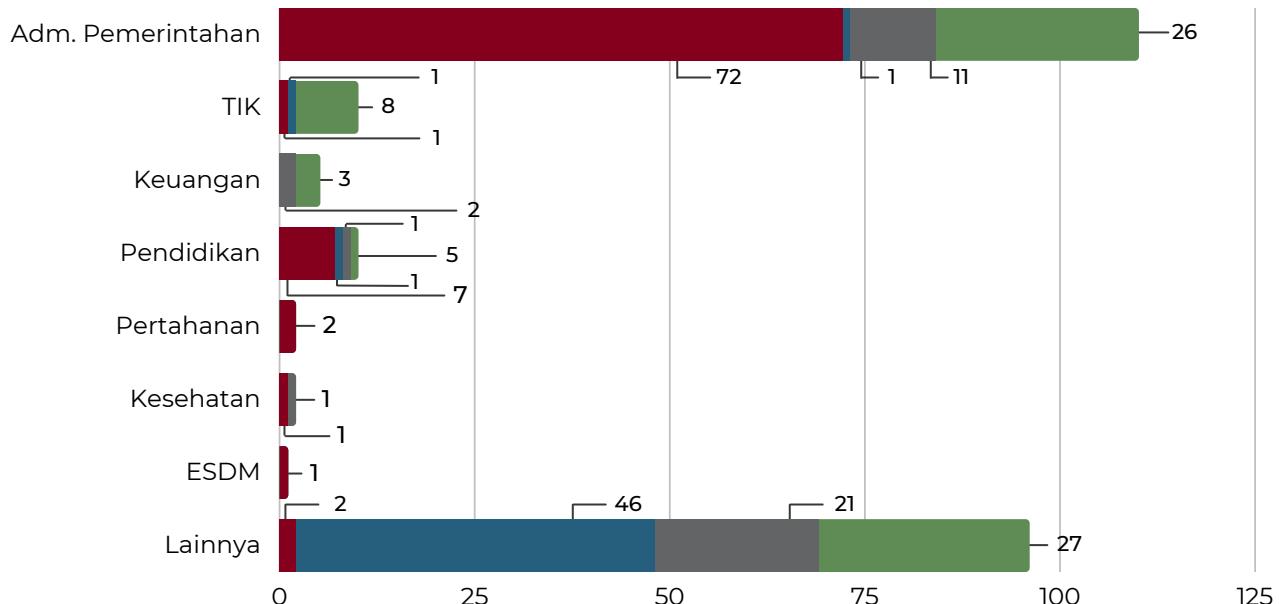
Ransomware

aduan dari masyarakat yang terkena insiden keamanan siber berupa ransomware

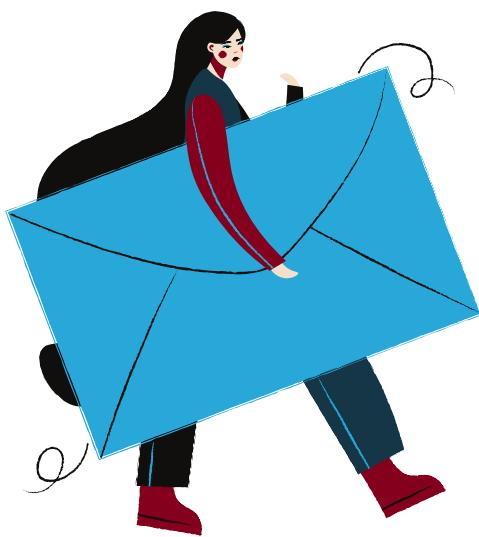
27%

Lainnya

aduan dari masyarakat yang mengalami insiden keamanan siber seperti *phising*, *web defacement*, DoS dan lain-lain



Pada Sektor Administrasi Pemerintahan aduan tentang *misconfiguration* sebanyak 72 aduan menjadi kategori insiden paling banyak, pada Sektor TIK aduan insiden DoS menjadi paling banyak yaitu 7 aduan, pada Sektor Keuangan aduan paling banyak terdapat pada jenis insiden *phising* dan *ransomware* masing-masing berjumlah 2 aduan, pada Sektor Pendidikan aduan *misconfiguration* menjadi aduan paling banyak sebanyak 7 aduan. Pada Sektor Pertahanan terdapat 2 aduan tentang *misconfiguration*, pada Sektor Kesehatan terdapat aduan terkait *ransomware* dan *misconfiguration* dengan jumlah masing-masing 1 aduan, pada Sektor ESDM terdapat 1 aduan terkait *misconfiguration* dan pada Sektor Lainnya seperti aduan dari individu terdapat 46 aduan terkait *cybercrimes*, dan 21 aduan *ransomware*.



TREN PENGIRIMAN NOTIFIKASI INDIKASI INSIDEN

1.433

Notifikasi

**TOTAL NOTIFIKASI
DIKIRIMKAN**



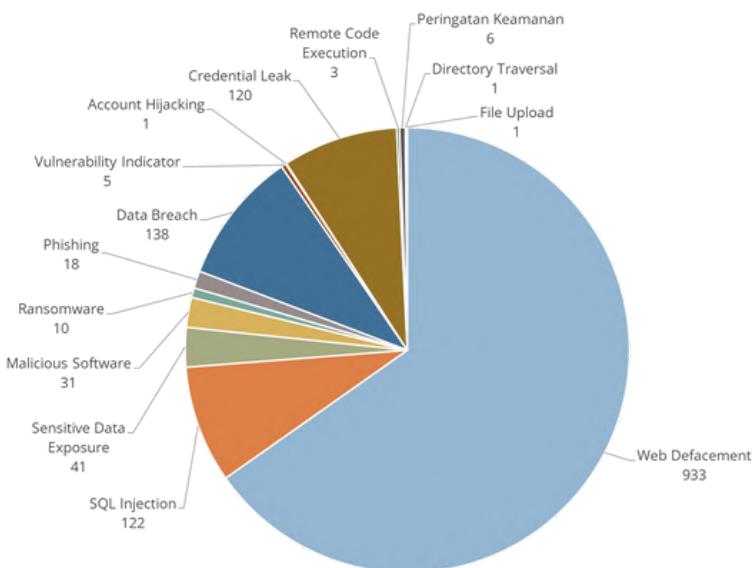
**126 NOTIFIKASI
DIRESPO**



**1307 NOTIFIKASI
TIDAK DIRESPO**



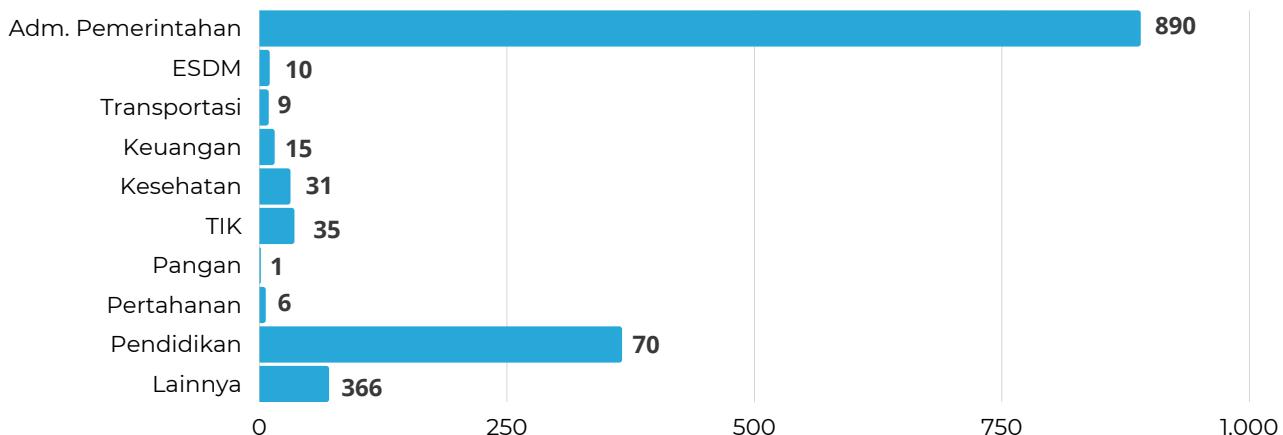
JENIS NOTIFIKASI

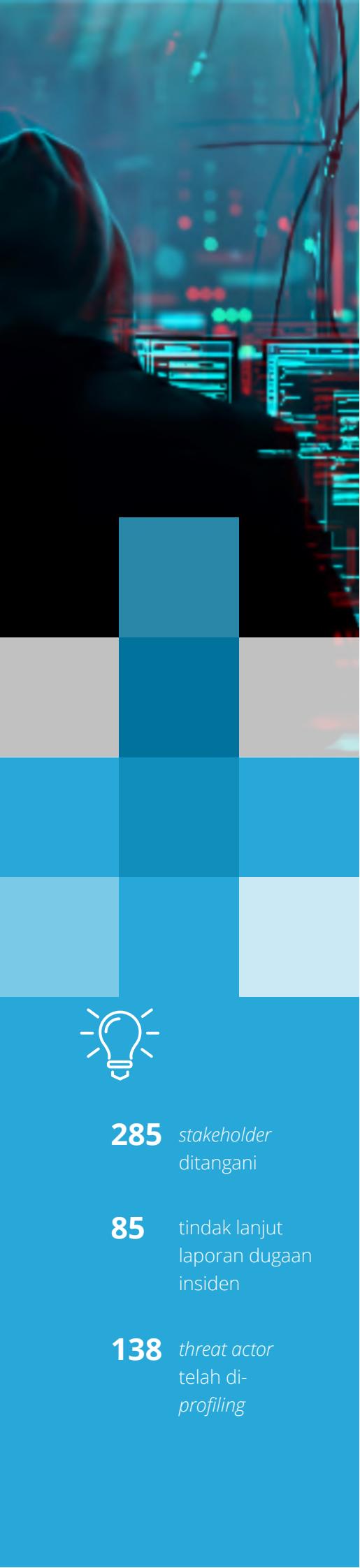


Jenis indikasi insiden pada notifikasi yang terbanyak dikirimkan adalah *Web Defacement* sebanyak 933, yang kemudian terbanyak lainnya yaitu *Data Breach* sebanyak 138 dan Kerentanan *SQL Injection* sebanyak 122. Terdapat gap yang besar antara top 3 jenis indikasi insiden pada notifikasi yang dikirimkan, hal ini menunjukkan bahwa masih **tingginya indikasi serangan siber yang mengarah pada aplikasi web.**



SEKTOR NOTIFIKASI





Cyber Threat Intelligence

399 Dugaan
Insiden Siber

dengan berbagai jenis insiden, diantaranya yaitu: kebocoran data, kerentanan, *malicious activity*, isu IPOLEKSOSBUDHANKAM, *malware*, *phising*, penanganan proaktif insiden, *profiling*, *ransomware*, *web defacement*, dan APT.

Sebaran *Stakeholder* (Sektor)

120	Adm. Pemerintahan	14	Keuangan
20	ESDM	11	Kesehatan
25	TIK	3	Pangan
20	Pertahanan	59	Lainnya
13	Transportasi		



285 *stakeholder*
ditangani

85 tindak lanjut
laporan dugaan
insiden

138 *threat actor*
telah di-
profiling

DARKNET EXPOSURE

427
Instansi

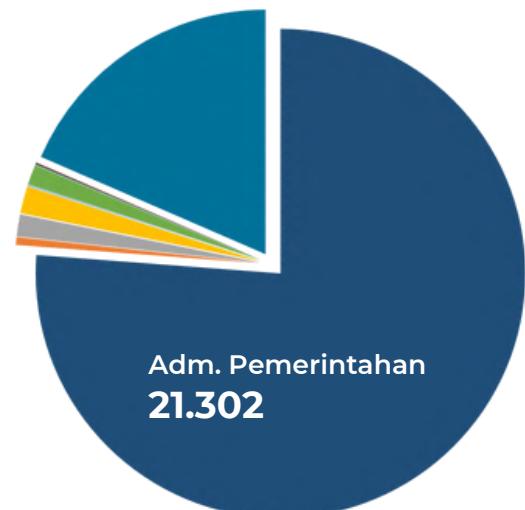
di Indonesia yang
terdampak darknet
exposure

Darknet exposure merupakan kondisi ketika terdapat data/infomasi kredensial akun pada suatu instansi tertentu yang terekspos di *darknet* sehingga berpotensi untuk dieksplorasi atau dicuri oleh pihak lain yang tidak bertanggungjawab serta dimanfaatkan untuk kepentingan mereka.

Dari data temuan tersebut, persentase paling tinggi yaitu pada Sektor Administrasi Pemerintahan sebesar 76,20%, Sektor Lainnya sebesar 18,49%, Sektor Keuangan sebanyak 1,799%, Sektor Transportasi sebanyak 1,45%, Sektor TIK sebanyak 1,34%, Sektor Pangan sebanyak 0,1%, dan Sektor Pertahanan 0,05%, Sektor ESDM sebanyak 0,51%. Oleh karena itu, diharapkan pengguna dapat menerapkan manajemen akun pengguna, *Restrict File and Directory Permissions*, kebijakan *password* terkait kombinasi karakter, tidak menggunakan akun/kredensial dinas untuk kepentingan selain kedinasan, dan segmentasi jaringan, serta melakukan himbauan pergantian *password* kepada setiap pegawai di masing-masing instansi.

REKAPITULASI DARKNET EXPOSURE 2022

Sektor	Jumlah Data Exposure	Jumlah Instansi
Adm. Pemerintahan	21.302	133
ESDM	143	25
Transportasi	406	63
Keuangan	503	53
Kesehatan	17	42
TIK	375	29
Pangan	28	17
Pertahanan	14	8
Lainnya	5.168	57
Total	27.956	427



- Adm. Pemerintahan
- ESDM
- Transportasi
- Keuangan
- Kesehatan
- Pangan
- Pertahanan
- Lainnya

REKAPITULASI DUGAAN KEBOCORAN DATA

Sepanjang tahun 2022, BSSN telah berhasil melakukan deteksi terjadi **311 dugaan insiden *data breach*** pada **248 stakeholder**. Dugaan insiden *data breach* **terbanyak yaitu terjadi pada bulan September 2022 sebanyak 119 insiden** dari total keseluruhan insiden sebanyak 311 dugaan insiden *data breach*.



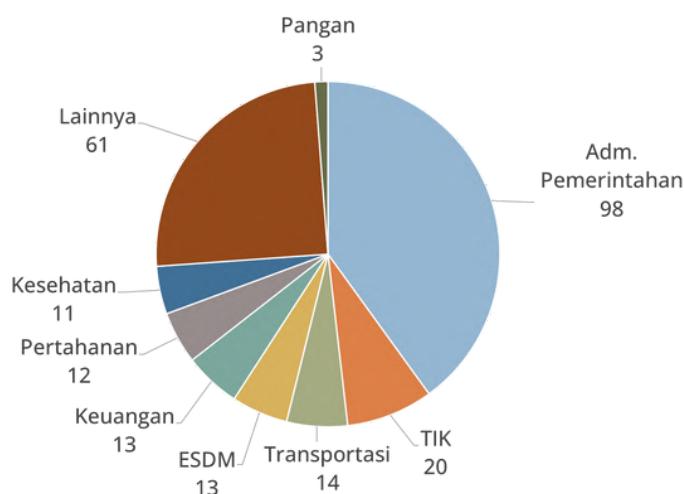
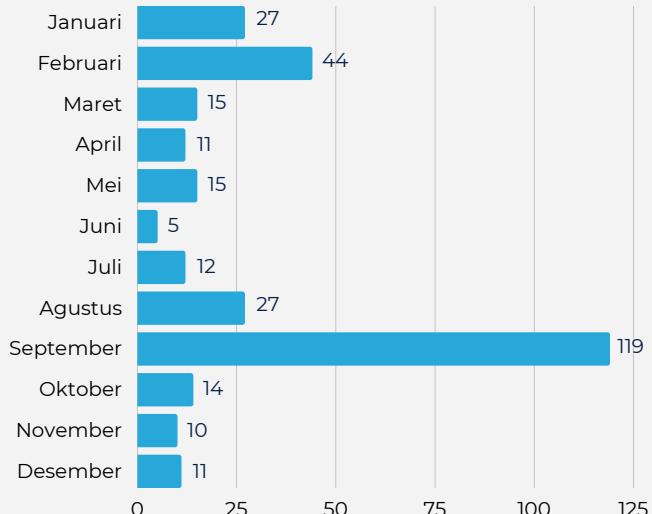
ASISTENSI TINDAK LANJUT

Terdapat **35 stakeholder** yang telah melakukan tindak lanjut dan asisten bersama dengan BSSN



RESPONS

Terdapat **85 stakeholder** yang telah merespons notifikasi



SEKTOR TERDAMPAK

Jumlah *stakeholder* yang kurang dari jumlah insiden disebabkan karena adanya lebih dari satu insiden yang terjadi pada *stakeholder* yang sama. Sektor yang paling banyak terjadi dugaan insiden *data breach* adalah Sektor Administrasi Pemerintahan, Sektor Lainnya, dan Sektor Teknologi Informasi dan Komunikasi (TIK).



TOP 5 CVE

2022



TOP 5 CVE GLOBAL

Common Vulnerability Exposure (CVE) merupakan daftar kerentanan aset keamanan informasi berlaku secara global yang terdiri dari nomor identifikasi, deskripsi, dampak untuk memudahkan dalam berbagi informasi antar organisasi.

Top 5 CVE Global merupakan 5 jenis kerentanan pada sistem maupun aplikasi dengan pengguna di seluruh dunia/global yang perlu menjadi perhatian. Top 5 CVE global yang terdapat pada tahun 2022 memiliki tingkat dampak High hingga Critical. Pada bab ini akan menjelaskan rincian penjelasan, dampak, dan panduan mitigasi dari setiap Top 5 CVE Global.

CVE-2022-21907

CVE-2022-21907 memiliki nilai **9,8** dengan tingkat dampak **CRITICAL**. Kerentanan ini terdapat pada layanan HTTP Protocol Stack (http.sys) Microsoft yang merupakan protokol pada Windows Server. Windows Server merupakan sistem operasi versi Windows yang khusus digunakan untuk server atau *data center*. Windows Server digunakan sebagai *server networking* perusahaan, berbagai layanan berbasis *cloud*, sebagai server *website*, *web app*, dan lain sebagainya.

Produk yang memiliki kerentanan CVE-2022-21907 adalah Windows Server 2019, Windows Server versi 20H2, Windows Server 2022, Windows 10 versi 21H2, Windows 11, dan Windows 10 versi 20H2. CVE-2022-21907 yang memiliki kerentanan terhadap serangan *Remote Code Execution* (RCE) yang dilakukan dengan mengirim paket yang dibuat khusus ke sistem yang menggunakan HTTP Protocol Stack (http.sys) untuk memproses paket. Tidak diperlukan interaksi pengguna dan hak istimewa untuk melakukan eksploitasi pada kerentanan ini.

DAMPAK

Dampak dari kerentanan ini yaitu memungkinkan penyerang dapat memperoleh akses ke Windows Server dan melakukan eksekusi kode secara *remote*.

PANDUAN MITIGASI

- Melakukan pembaruan Windows Server ke versi terbaru.
- Melakukan konfigurasi di fitur HTTP Trailer Support untuk mendeteksi kerentanan pada Sistem Operasi Windows Server 2019 dan Windows 10 versi 1809.

CVE-2022-22587

CVE-2022-22587 memiliki nilai **9,8** dengan tingkat dampak **CRITICAL**. Kerentanan ini muncul karena adanya *memory corruption* pada Apple. Aplikasi *malicious* dapat mengeksekusi kode arbitrer pada kernel. Kerentanan ini terdapat pada iOS dan iPadOS versi sebelum 15.3, macOS Big Sur versi sebelum 11.6.3, dan macOS Monterey dibawah versi 12.2.

DAMPAK

Dampak dari kerentanan ini yaitu memungkinkan penyerang dapat melakukan serangan kode arbitrer dengan memanfaatkan aplikasi *malicious*. Kode arbiter adalah kemampuan penyerang untuk menjalankan perintah atau kode pilihan penyerang pada mesin target, sehingga menyebabkan kegagalan pada memori Apple.

PANDUAN MITIGASI

Cara mitigasi yang dapat dilakukan yaitu melakukan pembaharuan versi menggunakan versi yang telah diperbarui antara lain iOS 15.3 dan iPadOS 15.3, macOS Big Sur 11.6.3, macOS Monterey 12.2.

CVE-2022-36934

CVE-2022-36934 memiliki nilai **9,8** dengan tingkat dampak **CRITICAL**. Kerentanan ini muncul karena adanya *integer overflow* pada aplikasi WhatsApp saat membuat panggilan video. Produk yang memiliki kerentanan CVE-2022-36934 adalah aplikasi WhatsApp dan WhatsApp Business versi sebelum v2.22.16.12 untuk tipe Android dan iOS. CVE-2022-36934 yang memiliki kerentanan terhadap serangan RCE yang dilakukan ketika melakukan *video call*. Tidak memerlukan interaksi pengguna dan hak istimewa untuk melakukan eksloitasi pada kerentanan ini.

DAMPAK

Dampak dari kerentanan ini adalah penyerang dapat memperoleh akses kedalam perangkat korban dan melakukan eksekusi kode secara *remote*. Hal tersebut dapat dimanfaatkan penyerang untuk mempengaruhi sistem pada perangkat korban dan menjalankan kode berbahaya.

PANDUAN MITIGASI

- Melakukan pembaruan aplikasi WhatsApp ke versi terbaru.
- Tidak menerima *video call* dari orang yang tidak dikenal.

CVE-2022-30136

CVE-2022-30136 memiliki nilai **9,8** dengan tingkat dampak **CRITICAL**. Kerentanan ini terdapat pada Windows Server 2012 R2, Windows Server 2016, Windows Server 2019.

DAMPAK

Dampak apabila kerentanan ini berhasil dieksploitasi adalah penyerang dapat melakukan eksekusi kode secara *remote* (RCE).

PANDUAN MITIGASI

- Melakukan *update* versi NFSV2.0 atau NFSV3.0.
- Menonaktifkan NFSV4.1.
- Mengimplementasikan Windows Security Update secara berkala.

CVE-2022-26923

CVE-2022-36934 memiliki nilai **8,8** dengan tingkat dampak **HIGH**. Kerentanan ini disebut juga sebagai kerentanan *Elevation Of Privilege* pada ADCS. ADCS adalah server *role* yang berfungsi sebagai implementasi *Public Key Infrastructure* (PKI) Microsoft yang erat kaitannya dengan Active Directory dan memungkinkan penerbitan sertifikat yang merupakan dokumen elektronik berformat X.509 yang ditandatangani secara digital yang dapat digunakan untuk enkripsi, penandatanganan pesan, dan/atau autentikasi.

DAMPAK

Pada CVE-2022-26923, penyerang dapat memanipulasi atribut DnsHostName, yang menentukan nama komputer seperti yang terdaftar di DNS, kemudian memungkinkan penyerang untuk mendapatkan sertifikat dari layanan ADCS yang berpotensi mengarah pada *privilege escalation*.

PANDUAN MITIGASI

Melakukan pembaruan server yang menjalankan layanan ADCS dan Windows Domain Controller yang mengoperasikan autentikasi berbasis sertifikat ke versi terbaru.



TOP 5 CVE NASIONAL

Top 5 CVE Nasional merupakan 5 jenis kerentanan pada sistem maupun aplikasi yang berpotensi terdampak terhadap pengguna di Indonesia. Top 5 CVE Nasional yang terdapat pada tahun 2022 memiliki tingkat dampak High hingga Critical. Pada bab ini akan menjelaskan rincian penjelasan, dampak, cara mendekripsi, panduan mitigasi, dan kategori sektor berpotensi terdampak dari setiap Top 5 CVE Nasional.

CVE-2022-22536

CVE-2022-22536 memiliki nilai **10,0** dengan tingkat dampak **CRITICAL**. Kerentanan ini terdapat pada SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53, dan SAP Web Dispatcher.

DAMPAK

Penyebab utama CVE-2022-22536 berkaitan dengan adanya kerawanan terhadap *smuggling request* dan *concatenation request* yang menyebabkan penyerang yang tidak diautentikasi dapat menambahkan *request* untuk menyamar sebagai pengguna atau manipulasi inputan *cache web*. Keberhasilan serangan ini mengakibatkan *compromised* secara penuh pada kerahasiaan, integritas, dan ketersediaan sistem.

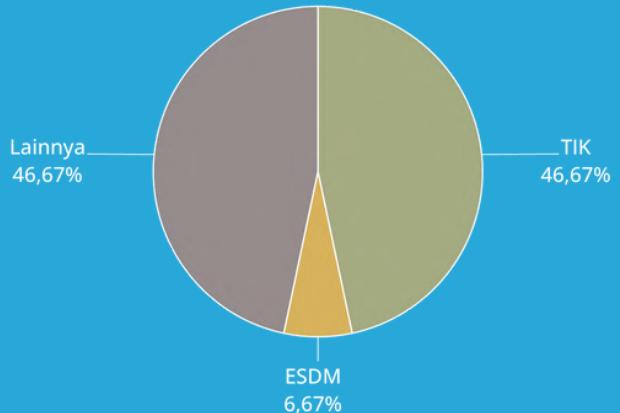
CARA DETEKSI

Menjalankan program pemindaian kerentanan yang terdapat pada https://github.com/Onapsis/onaps_is_icmad_scanner

PANDUAN MITIGASI

- Menerapkan pembaruan sistem SAP ke versi terbaru dan memastikan sistem selalu *up to date*.
- Membatasi jenis akses pengguna *root* ketika menjalankan perangkat lunak di perangkat tersebut untuk mengurangi potensi berhasilnya serangan.
- Tidak mengakses situs web yang berasal dari sumber tidak terpercaya.
- Menerapkan hak akses terendah ke semua sistem bagi pengguna biasa.
- Menggunakan *Web Application Firewall* (WAF).
- Menonaktifkan *connection refuse* pada server *back-end*.
- Melakukan konfigurasi server *front-end* untuk menormalisasikan *request* yang memiliki karakter khusus.

KATEGORI SEKTOR BERPOTENSI TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 46.67%, Sektor Lainnya sebesar 46.67%, dan Sektor Energi dan Sumber Daya Mineral sebesar 6.67%.

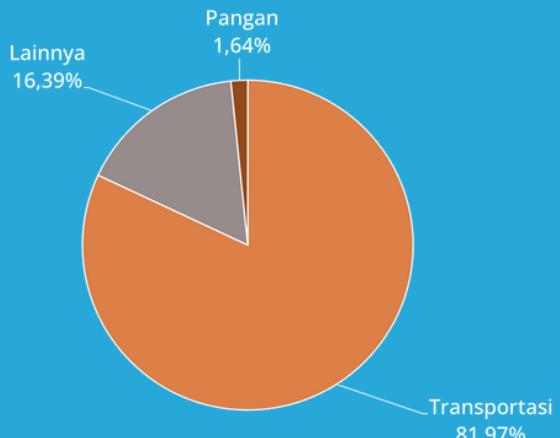
CVE-2022-32548

CVE-2022-32548 memiliki nilai **9,8** dengan tingkat dampak **CRITICAL**. Kerentanan ini terdapat pada DrayTek Vigor yang merupakan salah satu produk sistem operasi router dari DrayTek Corporation.

DAMPAK

Penyebab utama CVE-2022-32548 ini berkaitan dengan adanya *buffer overflow* pada antarmuka manajemen web perangkat DrayTek, khususnya pada halaman *login* di `/cgi-bin/wlogin.cgi`. Kerentanan keamanan ini dapat dimanfaatkan oleh penyerang untuk mendapatkan kendali (*remote access*) dari sebuah *host*, melakukan *privilege escalation*, dan melakukan eksekusi kode arbitrer.

KATEGORI SEKTOR BERPOTENSI TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 81.97%, Sektor Lainnya sebesar 16.39%, dan Sektor Pangan sebesar 1.64%.

CARA DETEKSI

Upaya eksplorasi dapat dideteksi pada **log/alert** ketika *string base64* yang rusak dikirim melalui permintaan POST ke **endpoint /cgi-bin/wlogin.cgi** pada router *interface* manajemen web. *String* yang disandikan Base64 diharapkan dapat ditemukan di bidang aa dan ab dari permintaan POST. *String* base64 yang rusak mengindikasikan serangan akan memiliki jumlah **padding %3D** yang sangat tinggi, sehingga angka apa pun di atas tiga harus dianggap mencurigakan.

PANDUAN MITIGASI

- Menerapkan *patch* yang telah dirilis oleh DrayTec Corp dan memastikan *firmware* pada perangkat selalu *up to date* pada tautan berikut <https://www.draytek.com/support/latest-firmwares/>.
- Melakukan verifikasi pada antarmuka manajemen seperti pada *port mirroring*, pengaturan DNS, dan akses VPN.
- Tidak melakukan *expose* pada antaramuka manajemen ke internet kecuali benar-benar diperlukan. Apabila iya, pastikan untuk mengaktifkan pembatasan *two-factor authentication* (2FA) untuk meminimalisir risiko serangan.
- Mengubah *password* perangkat yang terdampak dan menghapus data rahasia yang tersimpan di router.
- Menonaktifkan akses jarak jauh dan SSL VPN pada router serta menggunakan daftar kontrol akses dan 2FA jika memungkinkan.

CVE-2022-30136

CVE-2022-30136 memiliki nilai **9,8** dengan tingkat dampak **CRITICAL**. Kerentanan ini terdapat pada Windows Server 2012 R2, Windows Server 2016, Windows Server 2019.

DAMPAK

Dampak apabila kerentanan ini berhasil dieksploitasi adalah penyerang dapat menjalankan perintah pada sistem terdampak secara *remote* atau *Remote Code Execution* (RCE).

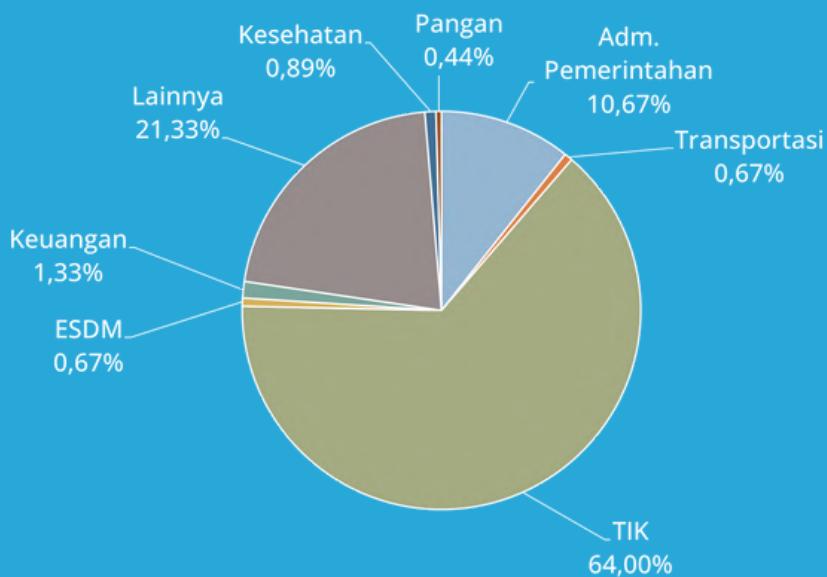
CARA DETEKSI

Kerentanan ini dapat dideteksi dengan melakukan pemeriksaan versi *Network File System* untuk melihat versi terdampak.

PANDUAN MITIGASI

- Melakukan *update* versi NFSV2.0 atau NFSV3.0 ketika sudah melakukan Windows Security Update Mei 2022
- Menonaktifkan NFSV4.1.
- Mengimplementasikan Windows Security Update secara berkala.

KATEGORI SEKTOR BERPOTENSI TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 64%, Sektor Administrasi Pemerintah sebesar 10.67%, dan Sektor Lainnya 21.33%.

CVE-2022-30190

CVE-2022-30190 memiliki nilai **7,8** dengan tingkat dampak **HIGH**. Kerentanan ini terdapat pada layanan Microsoft Support Diagnostic Tool (MSDT) yang merupakan salah satu produk dari Microsoft Corporation mulai dari 2013 hingga yang terbaru, pada semua sistem operasi Windows yang menyediakan layanan MSDT.

DAMPAK

Dampak dari kerentanan ini adalah penyerang dapat menjalankan perintah dengan izin aplikasi yang digunakan untuk membuka dokumen berbahaya. Kerentanan ini memungkinkan penyerang dapat melakukan instalasi program, melakukan modifikasi data, membuat akun baru, menjalankan kode arbitrer dengan hak istimewa *calling application*.



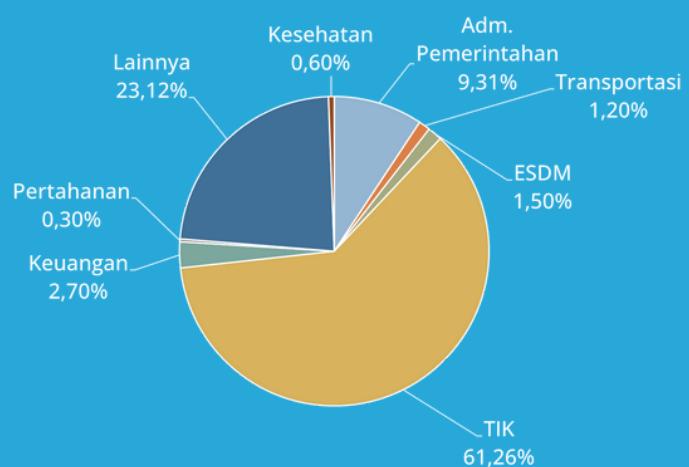
CARA DETEKSI

Cara yang digunakan untuk dapat melakukan deteksi terkait sistem terdampak melalui konfigurasi pada *command line parameter "/dt"*.

PANDUAN MITIGASI

- Menonaktifkan protokol URL MSDT dan **"ms-search"**
- Melakukan perlindungan dengan menggunakan Microsoft Defender Antivirus (MDAV).
- Menggunakan Microsoft Defender for Endpoint untuk deteksi dan perlindungan pada aplikasi Office dan Msdt.exe.
- Melakukan pemeriksaan hubungan *parent-child*, yaitu proses msdt.exe yang dimulai oleh proses induk seperti word.exe atau excel.exe.
- Melakukan pencegahan Office membuat child process dengan membuat *Attack Surface Reduction (ASR) rule*.

KATEGORI SEKTOR BERPOTENSI TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 61.26%, Sektor Lainnya sebesar 23.12%, Sektor Administrasi Pemerintahan sebesar 9.31%, dan Sektor Keuangan sebesar 2.7%

CVE-2022-26148

CVE-2022-26148 memiliki nilai **9,8** dengan tingkat dampak **CRITICAL**. Kerentanan ini terdapat pada layanan Grafana versi sebelum 7.3.4 yang merupakan perangkat lunak analisis data. Penyebab dari kerentanan ini adalah *password* Zabbix dapat ditemukan di *source code* HTML api_jsonrpc.php.

DAMPAK

Dampak dari kerentanan ini dapat memungkinkan penyerang untuk menemukan *password* akun Zabbix dan alamat URL. Selain itu, dengan melakukan pendekatan pencarian inurl:api_jsonrpc.php, dimungkinkan untuk menemukan target yang rentan dengan Google Hacking. Eksloitasi kerentanan dapat menyebabkan pengungkapan informasi sensitif, penambahan atau modifikasi data, dan *Denial of Service* (DoS).

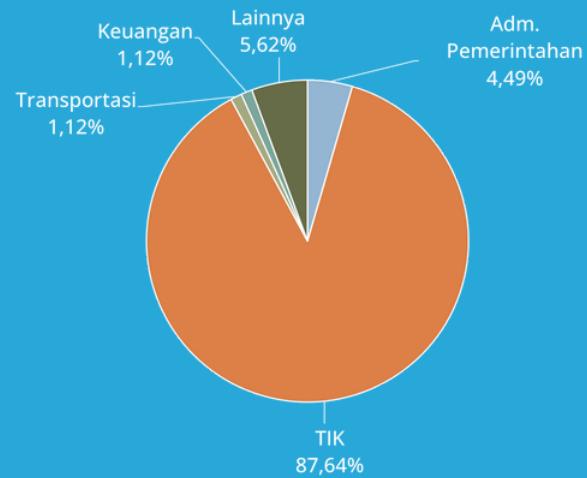
CARA DETEKSI

Melakukan pemeriksaan versi Grafana jika versi berada di bawah 7.3.4 hal ini mengindikasi aplikasi tersebut masih terdampak kerentanan CVE-2022-26148.

PANDUAN MITIGASI

- Melakukan klasifikasi data yang diproses, disimpan, atau dikirimkan oleh suatu aplikasi.
- Melakukan identifikasi data yang sensitif sesuai peraturan/kebijakan yang dimiliki, kemudian menerapkan kontrol sesuai klasifikasi.
- Menggunakan sistem token yang sesuai dengan PCI DSS.
- Menggunakan algoritma enkripsi terbaru dan memastikan algoritma, protokol, serta kunci standar yang mutakhir dan kuat tersedia dengan menggunakan manajemen kunci yang tepat.
- Menerapkan enkripsi pada semua transit data dengan protokol keamanan seperti *Transport Layer Security* (TLS) dengan *Cipher Perfect Forward Secrecy* (PFS), prioritas *cipher* oleh server, dan parameter yang aman.
- Menerapkan metode pengamanan transit data yang bersifat *strict*, seperti *HTTP Strict Transport Security* (HSTS).
- Melakukan penyimpanan *password* menggunakan fungsi *hashing* adaptif dan *salted* yang kuat dengan *delay factor*, seperti Argon2, scrypt, bcrypt atau PBKDF2.
- Menonaktifkan *caching* untuk respons yang berisi data sensitif.
- Menghapus *cookies* secara berkala.
- Menonaktifkan fitur *Autocomplete*.

KATEGORI SEKTOR BERPOTENSI TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 87.64%, Sektor Lainnya sebesar 5.62%, dan Sektor Administrasi Pemerintahan sebesar 4.49%.

```
state = true
else
    on trigger
    state = false
end if
2(false)
e <> oldstate then
    state = true then
        else below depending on whether
        pins high or low on triggering.
        transmit2(false)
        oldstate = state
        end if
    else then
        state = false then
            opposite of above (change
            transmit2(true)
            oldstate = state
            end if
        end if
    end if
end sub
state
main:
    assign prescaler to TMRO
    designate gpio as output
    configure pin 5 of GPIO as input
        initialize gpio
        initialize cnt
TMR0 = 96
```

ACCESS DENIED

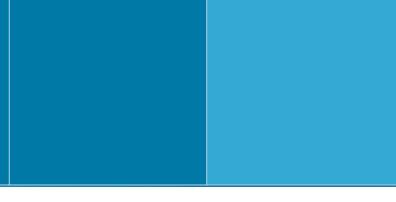
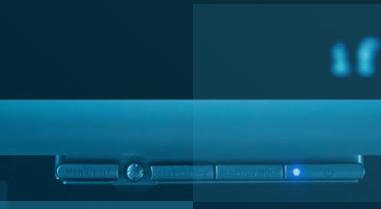
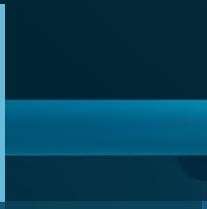
```
secs = secs + 1
increment second
ingCounter = 0
end if

if secs = 60 then
    secs = 0
    minutes = minutes + 1
    end if

if minutes = 10 then
    if state = binAlarmState then
        STILL in the 'alarm' state, so send
        signal every 10 minutes...
        transmit(binAlarmSignal)
        end if
    end if

hours = hours + 1
minutes = 0
end if
if hours > 12 then
    hours = 0
    <> binAlarmState then
        alarmSignal = true) then
            transmit(false)
            else
                transmit(true)
            end if
        oldstate = state
        end if
    end if

loop until 0 = 1
if minutes = 60 then
```



KAMPANYE PHISHING

2022

PHISING VIA .APK

Kasus: Jasa Ekspedisi

Modus penipuan melalui pengiriman paket pada salah satu aplikasi jasa ekspedisi viral di media sosial pada Desember tahun 2022. Modus penipuan ini dilakukan oleh penyerang dengan mengirimkan pesan singkat kepada korban dengan alasan untuk memastikan status paket yang akan dikirimkan. Pelaku mengirimkan sebuah file berekstensi .APK dengan nama "LIHAT Foto Paket".

Berdasarkan penamaan Microsoft, file APK tersebut terdeteksi sebagai *malware* bernama ANDROID/SMSStealer.ZZ16.Gen dengan nilai *hash* 5582dfd9f5d8c10df1aba661be532695. File .APK yang diinstal oleh korban selanjutnya akan terlihat mirip seperti aplikasi salah satu ekspedisi yang akan meminta beberapa *permission* agar dapat melihat dan mencuri data SMS dari perangkat korban. *Malware* ANDROID/SMSStealer.ZZ16.Gen merupakan *malware* yang menargetkan pengguna *mobile device/smartphone* berbasis sistem operasi Android dan menyebar melalui aplikasi *instant messaging*. *Malware* ini melakukan pencurian data dari perangkat terinfeksi terutama data SMS dari perangkat yang kemudian akan dikirimkan pada *Command and Control* (CnC).



Malicious Permission

Sampel yang dianalisis memiliki beberapa permintaan *permission* yang diberikan kepada korban, yaitu READ_SMS, RECEIVE_SMS, dan SEND_SMS. Beberapa *permission* ini memungkinkan penyerang untuk dapat menerima, mengirim dan membaca SMS dari perangkat korban.



Code Review

Setelah aplikasi terpasang maka sebuah *script* akan berjalan secara otomatis untuk mengirimkan data SMS dari perangkat korban menuju pada sebuah server C&C mencurigakan. Setelah dilakukan pengecekan terhadap domain yang diduga sebagai C&C, diketahui sejak berita tersebut menjadi viral di beberapa media diketahui domain tersebut telah di-suspend.

Rekomendasi

- Mengunduh dan menginstal aplikasi hanya dari *official app store* seperti Play Store atau iOS App Store
- Berhati-hati setiap kali membuka tautan ataupun file yang didapatkan dari seseorang yang tidak dikenali
- Mematikan pengaturan otomatis unduh media pada aplikasi messenger
- Teliti dalam memberikan ijin (*permission*) untuk aplikasi yang diinstalasi.

PHISING PERBANKAN

Phishing merupakan kejahatan siber dengan memanfaatkan aplikasi website/mobile palsu yang dibuat seolah-olah mirip dengan aplikasi resmi yang bertujuan untuk menipu calon korban. Tujuan dari threat actor membuat aplikasi phising untuk menipu calon korban agar memasukkan data sensitif seperti username dan password, nomor PIN, data diri pribadi, menipu korban untuk melakukan instalasi suatu aplikasi tertentu, dan lain-lain.

Selama tahun 2022, semakin marak kasus aplikasi *phishing* perbankan yang menargetkan nasabah bank untuk mendapatkan PIN rekening ataupun kode OTP milik korban. Pada kasus di sektor perbankan, mayoritas aplikasi *phising* disebarluaskan melalui pesan *broadcast Whatsapp*, undian berhadiah di media sosial, penyebaran *spam message* kepada e-mail calon korban dan potongan tarif transfer serta biaya admin.

Aktivitas Phishing

SOCIAL ENGINEERING



Threat actor melakukan *social engineering* yang menargetkan pengguna *online banking* untuk mencuri data kredensial *banking* (username, password, OTP). Threat actor biasanya akan mengaku sebagai pegawai dari salah satu bank dan meyakinkan calon korban untuk langsung mempercayai instruksi mereka agar membagikan data sensitif milik calon korban.

PHISHING



Threat actor melakukan *phishing* menggunakan aplikasi *mobile banking* untuk update tarif transaksi atau promo gratis biaya transfer antar bank, sehingga threat actor dapat mengumpulkan data kredensial milik pengguna.

PENCURIAN INFORMASI

Threat actor menggunakan SMS Stealer Android *malware* yang dapat mengakses pesan milik *device* pengguna untuk mencuri informasi OTP yang digunakan untuk *login* pada aplikasi *mobile banking*, kemudian dikirimkan melalui server *Command and Control* (C&C). Kemudian, C&C milik threat actor menerima pesan/SMS dari *device* milik korban.



PEROLEHAN KREDENSIAL

Threat actor berhasil memperoleh data kredensial milik korban dan digunakan untuk masuk ke dalam akun korban.

REKOMENDASI

Pada kasus *phishing* perbankan, informasi yang dicuri oleh *threat actor* antara lain: *username*, *password*, mengumpulkan pesan yang diterima pada *device* korban (termasuk OTP *Mobile banking* yang dikirimkan melalui SMS), informasi *device* yang digunakan (nama *device*, nomor model, dll). Pengguna diharapkan untuk dapat meningkatkan kewaspadaan terhadap upaya *phising* yang dilakukan oleh *threat actor*, berikut adalah rekomendasi tindakan yang dapat dilakukan untuk pencegahan *phising*:



Berhati-hati dalam membuka tautan dalam *e-mail*, SMS dan *broadcast chat* yang menawarkan promo, undian, atau meng-update aturan tertentu.



Tidak langsung mempercayai dan menjalankan instruksi dari seseorang (via telepon) yang mengaku sebagai pegawai sebuah perusahaan/bank. Sebaiknya juga tidak mengangkat telefon dari nomor yang tidak dikenal, tanpa pemberitahuan terlebih dahulu.



Tidak memasukkan *username* dan *password* pada *website*/aplikasi yang tidak terpercaya.



Tidak memberikan *password* dan OTP kepada siapapun.



Menggunakan *password* yang berbeda-beda pada tiap aplikasi yang dimiliki.



Menggunakan *password* yang memenuhi kriteria *strong password*.



Menerapkan 2FA untuk *login* pada layanan aplikasi tertentu.



Mengaktifkan pengaturan keamanan dan privasi aplikasi *browser* dan perangkat untuk memblokir *phishing*, *malware*, dan situs *malicious* lainnya.



Melakukan pembaruan untuk sistem operasi, aplikasi, antivirus dan *browser* secara berkala.



Mengkonfirmasi kepada pihak bank melalui *call center* jika terdapat permintaan yang mencurigakan.

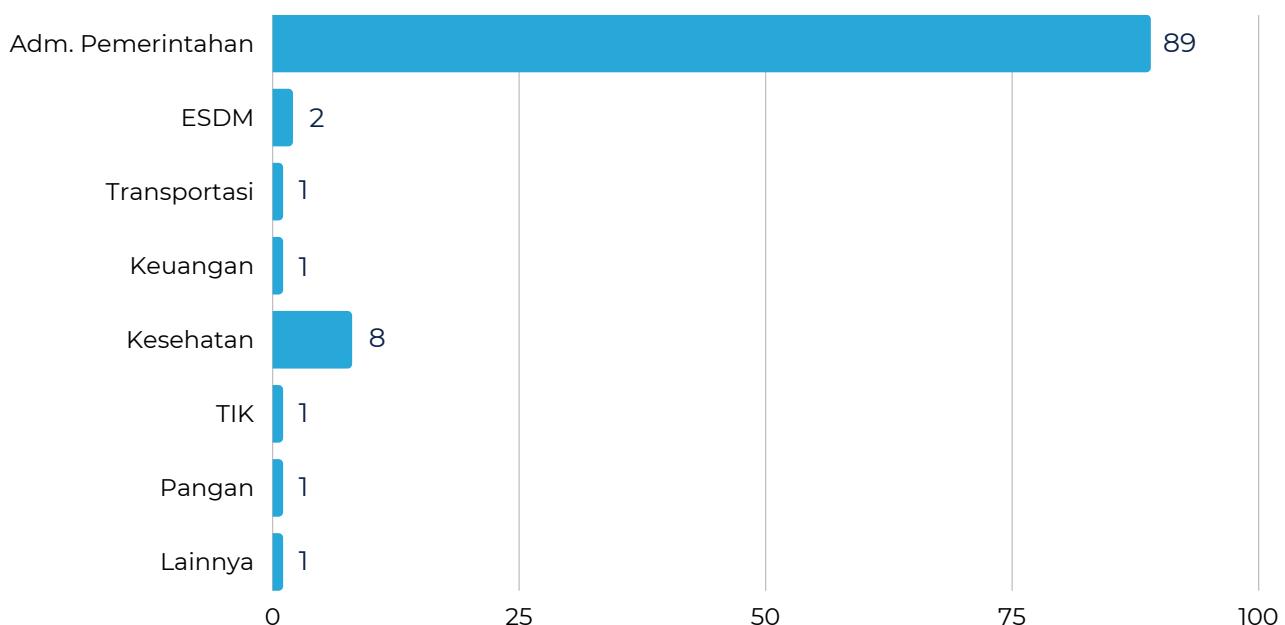


HIGHLIGHT IT SECURITY ASSESSMENT

2022

ITSA Pada Aplikasi Strategis

Information Tecnhonlogy Security Assessment (ITSA) merupakan layanan publik BSSN dengan rangkaian kegiatan berupa identifikasi celah keamanan, uji penetrasi, validasi kerentanan, serta pemberian rekomendasi perbaikan guna remediasi, pengamanan, dan meminimalkan celah keamanan yang dapat dieksloitasi pada sistem elektronik. Salah satu tujuan ITSA yaitu untuk mengidentifikasi celah keamanan pada sistem elektronik untuk menanggulangi adanya potensi kerentanan yang dapat dimanfaatkan oleh pihak eksternal maupun internal untuk melanggar kebijakan keamanan atau perusakan sistem elektronik. Salah satu tujuan ITSA yaitu untuk mengidentifikasi celah keamanan pada sistem elektronik untuk menanggulangi adanya potensi kerentanan yang dapat dimanfaatkan oleh pihak eksternal maupun internal yang tidak berhak dan berkepentingan untuk melanggar kebijakan keamanan atau perusakan sistem elektronik.



Pada Tahun 2022, telah dilaksanakan kegiatan ITSA sebanyak **169 operasi** pada **104 instansi** dengan jumlah **457 sistem elektronik** yang terdiri atas infrastruktur, aplikasi umum dan aplikasi khusus. Aplikasi umum merupakan aplikasi Sistem Pemerintahan Berbasis Elektronik (SPBE) yang sama, standar, dan digunakan secara bagi pakai oleh instansi pusat dan/atau pemerintah daerah, sedangkan aplikasi khusus adalah aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh instansi pusat atau pemerintah daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain (sumber: Peraturan Presiden Nomor 95 Tahun 2018).

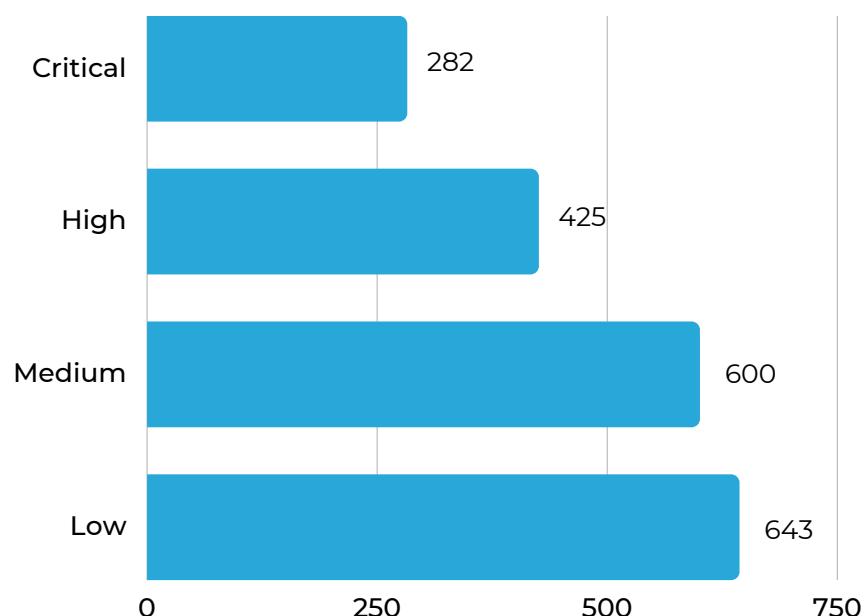


Hasil ITSA Tahun 2022

1.950
Celah Keamanan

ditemukan dari 457
Sistem Elektronik

Celah keamanan dibagi berdasarkan tingkat risiko (*risk severity*) yaitu *Critical*, *High*, *Medium*, dan *Low*.



Kontak ITSA

Media yang dapat digunakan untuk mendapatkan layanan publik ITSA, yaitu melalui telepon, surat elektronik (*e-mail*), ataupun datang secara langsung ke Kantor BSSN.

 +6282122230970

 itsa@bssn.go.id

- Tingkat risiko **Critical**, mayoritas dapat menyebabkan kebocoran data, pengambilalihan akun admin, dan kemungkinan untuk mengunggah (*upload*) *malicious file* seperti *malware* ataupun *backdoor webshell* tersembunyi.
- Tingkat risiko **High**, sebagian besar mengakibatkan penyerang dapat melihat data akun lain yang cukup sensitif, pengambilalihan akun pengguna lain, dan kemungkinan dapat mengunggah *pop-up script* berbahaya tertentu yang tersimpan di server.
- Tingkat risiko **Medium**, dapat menyebabkan *brute force password*, memasukan *script* pada *path* tertentu, tetapi tidak tersimpan di server, serta melakukan pencurian *cookie user*.
- Tingkat risiko **Low**, dapat menyebabkan serangan *clickjacking*, *system error* karena penggunaan modul yang tidak *update*, dan dapat mencoba masuk ke *port-port* tertentu.

Top 5 Kerentanan

Celah keamanan yang ditemukan dari hasil pelaksanaan ITSA, dibagi menjadi 4 (empat) tingkat risiko (*risk severity*), yaitu *low*, *medium*, *high*, dan *critical*. Tingkat risiko didasarkan oleh besarnya dampak yang ditimbulkan dan kemungkinan keberhasilan terjadinya suatu celah keamanan yang dapat menghambat pencapaian tujuan atau sasaran organisasi. Berdasarkan hasil ITSA selama tahun 2022, ditemukan sebanyak **1.950 celah keamanan** yang memiliki tingkat risiko yang berbeda-beda. Berikut merupakan 5 (lima) kerentanan dengan tingkat risiko *critical* yang memiliki dampak yang besar terhadap keamanan aplikasi yang ditemukan selama pelaksanaan ITSA tahun 2022.

Insecure Data Object Reference (IDOR)

IDOR merupakan jenis kerentanan *access control* yang memanfaatkan parameter-parameter tertentu sehingga penyerang dapat mengakses secara langsung objek yang sifatnya terbatas. Kerentanan ini banyak ditemukan pada aplikasi web yang menggunakan parameter sederhana dan/atau tidak dienkripsi, hal ini menyebabkan penyerang dapat menginputkan nilai parameter secara sembarang ataupun tertentu untuk mengetahui data lainnya. Kerentanan IDOR paling sering dikaitkan dengan *privilege escalation* atau eskalasi hak istimewa yang memungkinkan pengguna biasa dapat meningkatkan hak aksesnya menjadi lebih tinggi dengan memanfaatkan IDOR. Sebagian besar aplikasi web menggunakan ID sederhana untuk mereferensikan objek dengan parameter. Misalnya: ID pengguna, NIK, ataupun NIP.

SQL Injection

SQL *Injection* merupakan salah satu teknik pemanfaatan celah keamanan yang terdapat pada *database* aplikasi. Celah keamanan tersebut terjadi karena adanya kesalahan dalam pemfilteran input sehingga penyerang dapat melakukan injeksi kode (*query*) SQL pada situs web maupun aplikasi. Umumnya, penyerang menggunakan perintah atau *query* SQL untuk melakukan *bypass* mekanisme autentikasi pada *database*. Injeksi kode yang dilakukan menyebabkan penyerang dapat masuk dan mengakses *database* tanpa proses autentikasi. Selain itu, penyerang bebas untuk mengubah, menambah, dan menghapus data-data pada *database* situs web atau aplikasi, dan dapat menyebabkan kebocoran data.

Privilege Escalation

Privilege escalation merupakan serangan yang bertujuan untuk mendapatkan izin atau hak akses dengan tingkat yang lebih tinggi pada sistem atau jaringan. Semakin tinggi hak akses yang didapatkan, semakin mudah bagi penyerang untuk melakukan eksloitasi pada sistem atau jaringan. Penyerang memanfaatkan kelemahan sistem dan kesalahan konfigurasi dalam melakukan serangan ini.



Broken Access Control

Broken access control adalah suatu kerentanan dimana mekanisme autentikasi dan pembatasan akses tidak diterapkan dengan baik, sehingga penyerang yang tidak memiliki hak dapat mengakses sebuah target sistem dengan level hak akses yang sama atau lebih tinggi. Hal-hal yang dapat dilakukan penyerang dengan memanfaatkan kerentanan ini antara lain:

1. Melewati pemeriksaan akses kontrol dengan memodifikasi URL, *internal application state*, *HTML page*, atau menggunakan *custom API attack tool*.
2. Memperbolehkan setiap pengguna untuk melihat atau mengubah akun pengguna lain.
3. Menaikkan *privilege level* sehingga penyerang bisa mendapatkan hak akses yang lebih tinggi tanpa melakukan *login*.
4. Melakukan manipulasi metadata seperti memanipulasi token kontrol akses, atau memanipulasi *cookie* atau *hidden field* untuk melakukan peningkatan *privilege (elevation privilege)*.
5. Mengakses API yang tidak memiliki akses kontrol untuk melakukan fungsi POST, PUT, dan DELETE.

XSS (Stored, Reflected dan DOM-Based)

Cross Site Scripting atau yang sering disebut dengan XSS merupakan jenis celah keamanan yang dapat digunakan untuk melakukan pencurian data sensitif milik korban, mengendalikan sesi pengguna, menjalankan kode berbahaya, atau sebagai rangkaian untuk melakukan *phishing* yang ditujukan kepada korban. XSS merupakan serangan injeksi kode yang dilakukan pada sisi klien dengan memanfaatkan fitur input yang tidak difilter atau divalidasi terlebih dahulu oleh sistem pada halaman situs web. Penyerang dapat menginjeksikan kode berbahaya ke halaman situs web dengan bahasa pemrograman yang biasa digunakan adalah VBScript, ActiveX, Flash, JavaScript, dan bahasa sisi klien lainnya. XSS sering digunakan untuk mencuri sesi korban yang kemudian dimanfaatkan untuk mengetahui data-data sensitif milik korban, seperti *username* dan *password login*, sampai dengan data pribadi lainnya yang dapat digunakan penyerang untuk melakukan serangan lanjutan.



DUKUNGAN KEAMANAN SIBER DAN SANDI PADA EVENT NASIONAL DAN INTERNASIONAL

BSSN berperan aktif dalam mendukung keamanan siber dan sandi pada penyelenggaraan *event* Nasional dan Internasional pada Tahun 2022. Proses pengamanan siber pada *event* nasional dan internasional dilakukan sejak pra pelaksanaan hingga pasca-pelaksanaan. BSSN melakukan beberapa upaya pengamanan siber dalam bentuk pengujian keamanan terhadap sistem elektronik, pemasangan perangkat deteksi dan *monitoring* pada perangkat jaringan pada *Internet Service Provider* (ISP) dan di *site event*, melakukan deteksi dini ancaman siber, melaksanakan upaya tanggap insiden dan *digital forensic incident response* (DFIR) ketika terjadi insiden siber, serta upaya perbaikan terhadap sistem elektronik yang memiliki celah keamanan.

Seleksi CASN PPPK



BSSN melakukan pemantauan pada kegiatan CASN yang diadakan oleh BKN pada bulan Maret 2022 sampai dengan saat laporan ini disusun (Januari 2023) yaitu kegiatan Seleksi Kompetensi Dasar (SKD) CASN Sekolah kedinasan dan pemantauan kegiatan Seleksi PPPK Teknis dan Non Teknis. Pemantauan dilakukan pada sisi *endpoint* / server milik Kemdikbud dan BKN yang digunakan untuk kegiatan CASN. Pada pelaksanaan *Computer Assisted Test* (CAT) CASN beberapa hal yang menjadi perhatian untuk dilakukan pemantauan yaitu akun aplikasi, akun *Virtual Private Network* (VPN), serta aktivitas yang mencurigakan pada *database*.

Seleksi POLRI

BSSN telah berkolaborasi dengan Kepolisian Negara Republik Indonesia (POLRI) dalam melaksanakan pengamanan rangkaian seleksi penerimaan dan kenaikan pangkat anggota POLRI yang dilaksanakan pada tahun 2022 secara luring dan daring. BSSN telah melaksanakan rangkaian pengamanan pada tingkat seleksi daerah hingga Nasional dalam upaya meningkatkan keamanan siber pada rangkaian kegiatan seleksi anggota POLRI. Kegiatan pengamanan rangkaian kegiatan seleksi anggota POLRI meliputi kegiatan pemeriksaan keamanan *device* pembuat soal, pemeriksaan keamanan *device* pengunduh soal, pengawas ujian, pemeriksaan aktivitas lalu lintas jaringan utama dan *back up venue* kegiatan, hingga menjadi saksi dalam sidang kelulusan.

Kegiatan pengamanan rangkaian kegiatan seleksi anggota POLRI menghasilkan keamanan perangkat yang digunakan pada saat seleksi dan *venue* kegiatan yang lebih baik untuk pelaksanaan seleksi anggota POLRI baik secara luring maupun daring. Kegiatan pengamanan seleksi ini telah mengamankan lebih dari 123 rangkaian acara seleksi POLRI, dengan hasil bahwa kegiatan dapat berjalan baik dan lancar.



Sidang Tahunan MPR dan DPR

BSSN berkolaborasi dengan Dewan Perwakilan Rakyat Republik Indonesia (DPR RI) dalam melaksanakan kegiatan pengamanan Sidang Tahunan Majelis Permusyawaratan Rakyat Republik Indonesia (MPR RI) dan Sidang Paripurna DPR RI yang dilaksanakan pada Hari Selasa, Tanggal 16 Agustus 2022. BSSN telah melaksanakan rangkaian pengamanan selama 1 (satu) bulan dalam upaya meningkatkan keamanan siber guna mendukung berjalannya Sidang Tahunan MPR RI dan Sidang Paripurna DPR RI yang dihadiri secara luring dan daring.

Kegiatan pengamanan Sidang Tahunan MPR RI dan Sidang Paripurna DPR RI meliputi kegiatan pengujian keamanan infrastruktur jaringan melalui layanan *Information Technology Security Assessment* (ITSA) pada Ruang Rapat Komisi I DPRI RI dan Gedung Nusantara DPR RI, *monitoring* media sosial, *monitoring* aktivitas lalu lintas jaringan, serta pengamanan jaringan dan sinyal komunikasi di hari pelaksanaan Sidang Tahunan MPR RI dan Sidang Paripurna DPR RI yang bertempat di Gedung Nusantara DPR RI. Kegiatan pengamanan Sidang Tahunan MPR RI dan Sidang Paripurna DPR RI memiliki tujuan untuk kelancaran dan keamanan jaringan dalam pelaksanaan Sidang Tahunan MPR RI dan Sidang Paripurna DPR RI.



HUT RI



Pada periode 8 s.d. 17 Agustus 2022, BSSN melakukan pemantauan terhadap *web server* terkait Kegiatan Hari Ulang Tahun Republik Indonesia Ke-77. Pemantauan dilakukan menggunakan sistem *monitoring Internet Exchange* (IIX), *International Gateway* dan *Security Information and Event Management* (SIEM) Kementerian Sekretariat Negara RI. Terdapat anomali berupa upaya percobaan serangan terhadap aplikasi berbasis web seperti mencoba mengeksploitasi kerentanan, mengakses URL yang terbatas, dan melakukan injeksi kode pada halaman *website*. Kondisi tersebut dapat segera dideteksi dan diatasi, sehingga sampai dengan akhir pelaksanaan kegiatan berlangsung, kegiatan HUT RI dapat berjalan dengan baik dan tidak ditemukan aktivitas serangan yang berhasil menyerang infrastruktur jaringan yang terdapat pada Kegiatan HUT RI.

ASEAN Para Games 2022



Kegiatan ASEAN Para Games 2022 dilaksanakan pada tanggal 31 Juli - 7 Agustus 2022 di Solo. Kegiatan Operasi Keamanan Siber pada Penyelenggaraan ASEAN Para Games 2022 dilakukan dalam 2 (dua) metode, yaitu: Pengamanan *On-Site* dan Pemantauan oleh BSSN. Tim Satgas Pengamanan *On-Site* beroperasi di Ruang *Technical Operation Center* (TOC) Stadion Manahan. Berdasarkan hasil *monitoring* aset, terdapat anomali yang didominasi oleh serangan web dan pemindai jaringan. Dari seluruh anomali yang terjadi, tidak ada yang menyebabkan insiden siber karena semua serangan berhasil diblok oleh *security perimeter*.

Tim Satuan Tugas di BSSN tidak menemukan anomali yang berkaitan dengan kegiatan. Secara teknis operasi keamanan siber, tidak ditemukan aktivitas serangan yang berhasil menyerang infrastruktur jaringan yang terkait dengan kegiatan ASEAN Para Games 2022.

Inter-Parliamentary Union (IPU)

Kegiatan IPU dilaksanakan pada tanggal 18-24 Maret 2022 di Nusa Dua, Bali. Seluruh aktivitas yang terindikasi sebagai aktivitas anomali yang terdeteksi telah dilakukan verifikasi dan langkah mitigasi awal dari aktivitas yang terjadi tersebut, sehingga tidak mengganggu pelaksanaan kegiatan Pengamanan IPU Assembly & Related Meetings ke 144. Adapun tindakan mitigasi yang dilakukan, antara lain dengan melakukan isolasi dari jaringan terhadap PC yang terdampak, menerapkan daftar *Indicator of Compromised* (IOC) pada perangkat *security perimeter*, dan berkoordinasi dengan pemangku kepentingan.



Satuan Tugas Pelindungan Data



BSSN berperan aktif dalam melaksanakan tugasnya sebagai Tim Satuan Tugas Pelidungan Data pada Tahun 2022 untuk mendukung pelaksanaan pelindungan data terhadap 8 Kementerian/Lembaga Prioritas yang telah ditentukan. Adapun Satgas Pelindungan Data terdiri dari 5 (lima) tim, antara lain: Tim Tata Kelola dan Manajemen Risiko, Tim Operasi Keamanan Siber, Tim Operasi Pengendalian Informasi, Tim Operasi Sandi, dan Tim Komunikasi Publik.

Konferensi Tingkat Tinggi G20

Kegiatan Konferensi Tingkat Tinggi G20 dilaksanakan pada Bulan Juli-November 2022 di Bali. BSSN sebagai *leading sector* pada pengamanan Siber G20 berperan aktif dalam pengamanan siber pada 17 event serangkaian event KTT G20 , diantaranya: 3rd DEWG, SAI, 4th DEWG & DEMM, S20, FMM, TIIWG & TIIIMM, TWG & TMM, P20, C20, RIIG & RIMM, Space 20, HMM, 4th Sherpa Meeting, B20, Media Center, JHFMM, dan KTT G20. Tim BSSN menemukan celah keamanan dan potensi insiden berupa:

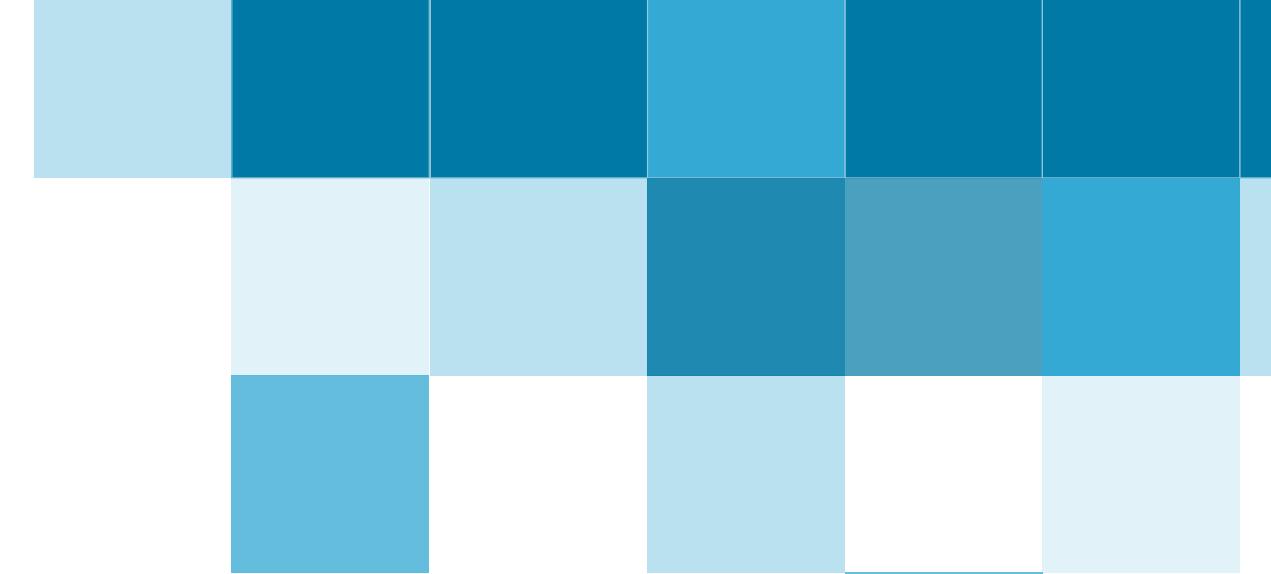
- Terdapat beberapa kerentanan kritis berdasarkan hasil *Vulnerability Assessment* (VA) pada infrastruktur dan situs-situs yang digunakan pada event KTT G20.
- Terdapat aplikasi terindikasi berbahaya dari komputer yang digunakan di hotel yang menjadi tempat penyelenggaraan acara KTT G20.
- Terdapat anomali trafik yang terdeteksi di IIX dan *International Gateway* pada asset yang berkaitan dengan kegiatan G20.
- Dilakukan kegiatan tanggap insiden siber sebagai langkah tindak lanjut dari hasil *monitoring* dan VA.
- Telah dikirimkan sejumlah 19 dokumen notifikasi kepada pemilik asset seperti pihak hotel selaku *venue* kegiatan, instansi sebagai penyelenggara kegiatan, dan pemangku kepentingan lainnya.
- Seluruh temuan tersebut telah berhasil dilakukan tindak lanjut melalui upaya tanggap insiden siber dan seluruh insiden berhasil dipulihkan.





KOLABORASI BSSN PADA EVENT NASIONAL DAN INTERNASIONAL

Era digital yang terus berkembang membuat banyak organisasi khususnya pada Sektor Pemerintah menerapkan berbagai teknologi untuk melakukan transformasi digital menjadi Sistem Pemerintahan Berbasis Elektronik (SPBE). Implementasi teknologi yang terus meningkat ini kemudian juga meningkatkan risiko ancaman keamanan siber. Dalam mewujudkan keamanan siber dengan cakupan yang lebih luas, BSSN melalui layanan yang ada melakukan kolaborasi dengan Sektor Pemerintah lainnya dan aktif mengikuti forum-forum Internasional untuk meningkatkan keamanan siber sebagai upaya untuk menjaga ruang siber Indonesia.



Forum Komunikasi dan Koordinasi Nat-CSIRT

BSSN telah menyelenggarakan kegiatan Forum Komunikasi dan Koordinasi Nat-CSIRT pada tanggal 19 s.d. 21 September 2022 bertempat di Gets Hotel, Semarang, Jawa Tengah. Forum Komunikasi dan Koordinasi NAT-CSIRT merupakan wujud dari salah satu dari kerja sama nasional berupa penyediaan wadah kolaborasi dan koordinasi serta pelaksanaan layanan bimbingan teknis penanganan insiden pada CSIRT Organisasi pada Tahun 2022. Forum Komunikasi dan Koordinasi Nat-CSIRT diselenggarakan oleh BSSN yang memiliki tugas dan fungsi sebagai pengelola tanggap insiden nasional atau *National Computer Security Incident Response Team* (Nat-CSIRT) yang dijalankan melalui ID-SIRTII/CC.



Kegiatan ini dihadiri oleh 39 peserta yang merupakan gabungan dari 22 CSIRT Pemerintah dan CSIRT Sektoral. Secara keseluruhan pelaksanaan Forum Komunikasi dan Koordinasi Nat-CSIRT terselenggarakan dengan tertib dan lancar. Kegiatan ini diharapkan menciptakan komunikasi dan kolaborasi antar para personel CSIRT Organisasi, serta peserta diharapkan mampu melakukan proses tanggap insiden secara mandiri sehingga dapat tercipta tingkat kematangan, level kompetensi teknis yang merata, dan kesamaan pola tindak dalam menangani insiden siber di setiap CSIRT Organisasi.

Pilot Project Voluntary Vulnerability Identification and Protection Program (VVIP-Program)

Direktorat Operasi Keamanan Siber, Badan Siber dan Sandi Negara (BSSN) menggelar kegiatan Pilot Project *Voluntary Vulnerability Identification and Protection Program* (VVIP-Program) yang diselenggarakan di Provinsi Bali pada September 2022. VVIP-Program melibatkan masyarakat untuk berkolaborasi secara sukarela dengan BSSN dalam melakukan pengidentifikasi kerentanan serta proteksi pada sistem elektronik milik Pemerintah. Kegiatan VVIP-Program Bali melibatkan beberapa kampus dan komunitas *Bug Hunter* se-Bali dan difasilitasi oleh Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali.



Bug Bounty Kemendikbud Ristek 2022

Badan Siber dan Sandi Negara (BSSN) bersama dengan Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbud Ristek) menyelenggarakan kegiatan *Bug Bounty* Kemendikbud Ristek 2022 yang berlangsung dari Juni hingga pertengahan Juli 2022, kegiatan uji keamanan pada 15 aplikasi yang dimiliki 7 unit kerja di lingkungan Kemendikbud. Kegiatan tersebut merupakan wujud aktif kerja sama BSSN

dengan kementerian dan lembaga negara, terkait pengembangan minat dalam lingkup ruang siber dan peningkatan kompetensi sumber daya manusia keamanan siber di Indonesia. Perwakilan BSSN berperan sebagai juri pada kegiatan *Bug Bounty* Kemendikbud Ristek yang diikuti oleh 275 peserta yang sebagian besar berasal dari kalangan akademisi.



Cybersecurity Hackathon & JobFair 2022



BSSN terlibat aktif dalam kegiatan Cybersecurity Hackathon & JobFair 2022 sebagai dewan juri yang diselenggarakan oleh MasterCard dan InfraDigital Foundation yang berkolaborasi dengan Kemendikbud Ristek guna melakukan pengawasan *capacity building* (pelatihan dan sertifikasi). Kegiatan berlangsung pada tanggal 28-29 November 2022 bertempat di Kemendikbud Ristek Gedung D dan Hotel Aryaduta Jakarta. Kegiatan Cybersecurity Hackathon & JobFair 2022 ini melibatkan mahasiswa perguruan tinggi dan siswa sekolah menengah kejuruan se-Indonesia.

Assessment Teknis Operasional dan Keamanan

Dalam rangka mendukung kinerja Kementerian Luar Negeri di KBRI Seoul serta upaya memitigasi berbagai ancaman dan kerentanan pada data center, pihak Kementerian Luar Negeri di KBRI Seoul melalui Kementerian Komunikasi dan Informatika melakukan kolaborasi dengan BSSN. Kolaborasi dilakukan melalui kegiatan Assessment Teknis Operasional dan Keamanan pada data center Kementerian Luar Negeri di KBRI Seoul. Assessment dilakukan sebagai upaya untuk memenuhi Perpres 95 Tahun 2018 tentang Sistem Pemerintahan

Berbasis Elektronik (SPBE) Pasal 30 yang mengamanatkan Kementerian/Lembaga harus melakukan audit sistem elektronik dan audit keamanan terhadap Data Center atau ruang server yang dikelolanya. BSSN berperan sebagai assessor pada kegiatan Assessment Teknis Operasional dan keamanan yang dilakukan secara langsung pada tanggal 23 s.d 26 November 2022 yang berlokasi di Seoul, Korea Selatan.

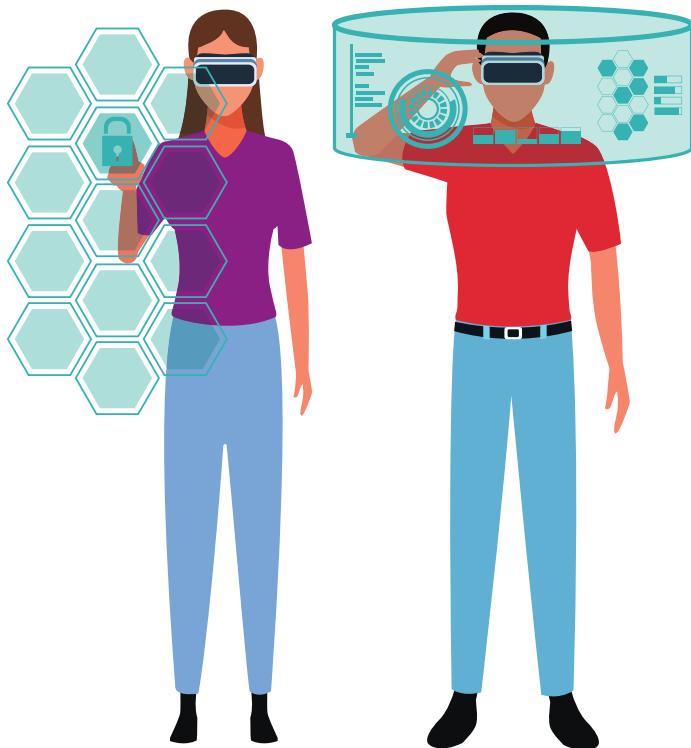


Kerjasama Layanan HONEYNET

ISIF Project

Honeynet BSSN juga telah berkolaborasi dengan Swiss German University (SGU) dan komunitas Indonesia Honeynet Project (IHP) yang berfokus pada siklus deteksi dalam *Framework Cyber Security*. Hal ini salah satunya diimplementasikan dalam bentuk kerjasama riset yang dilakukan bersama SGU dan IHP dalam penelitian ISIF (*The Information Society Innovation Fund*) ASIA.

Tujuan dari ISIF Project ini adalah untuk menyediakan *platform sharing* bagi setiap organisasi di Indonesia (nantinya dapat diterapkan di negara-negara ASEAN atau Asia Pasifik) untuk berbagi informasi ancaman keamanan yang dikumpulkan melalui *honeypot* pada organisasi disuatu negara. Selain itu, *project* ini juga menjadi sebuah inovasi dan pertama kali dilakukan dengan menggabungkan upaya penelitian antara pemerintah (BSSN), lembaga pendidikan (SGU), dan komunitas keamanan siber (IHP) untuk membangun *platform threat information sharing*.



Dalam rangka memperluas cakupan sistem *Honeynet* BSSN, serta memperkaya data serangan siber di Indonesia, *Honeynet* BSSN setiap tahunnya selalu menjalin kerja sama baru dengan berbagai *stakeholder* di Indonesia. Pada tahun 2022, terdapat penambahan sebanyak 15 titik pemasangan *honeypot*, sehingga jumlah *Honeypot* BSSN yang terpasang mencapai

93 titik
yang tersebar
di 26 provinsi

Penambahan titik *Honeypot* ini tentunya semakin memperkaya informasi data serangan siber yang menyerang Indonesia berdasarkan sistem *Honeynet* BSSN. Informasi serangan siber yang diperoleh dari sistem *Honeynet* BSSN selanjutnya dapat digunakan sebagai salah satu referensi peningkatan *security perimeter* milik Mitra *Honeynet* sekaligus meningkatkan *cyber security awareness* bagi masyarakat.

National Cybersecurity Connect 2022



Sepanjang tahun 2022, Honeynet BSSN telah mengikuti beberapa kegiatan dan pameran keamanan siber yang diperuntukkan bagi komunitas keamanan siber dan masyarakat umum. Beberapa kegiatan yang diikuti oleh Honeynet BSSN yaitu National Cybersecurity Connect 2022 yang dilaksanakan pada tanggal 26 s.d. 27 Oktober 2022 di Birawa Assembly Hall, Bidakara, Jakarta. Kegiatan NCC adalah kegiatan keamanan siber terbesar pertama dan dihadirkan untuk menjadi solusi dan wadah bagi seluruh pemangku kepentingan untuk berkumpul, berdiskusi, dan berkontribusi bagi ekosistem keamanan siber nasional Indonesia.

Indo Defence Expo & Forum 2022

Honeynet BSSN juga telah mengikuti kegiatan pameran Indo Defence Expo & Forum 2022 yang diselenggarakan oleh Kementerian Pertahanan. Kegiatan ini dilaksanakan pada tanggal 2 s.d. 5 November di JIEXPO Kemayoran, Jakarta. Indo Defence Expo & Forum merupakan kegiatan pameran industri pertahanan terbesar di Asia Tenggara. Dalam kedua kegiatan tersebut, tim Honeynet BSSN memperkenalkan dan mensosialisasikan tentang Honeynet BSSN sebagai salah satu teknologi keamanan siber yang dapat dimanfaatkan dalam rangka pengelolaan informasi dini serangan siber.



Untuk informasi lebih lanjut terkait Layanan Honeynet BSSN, termasuk didalamnya terdapat Laporan Tahunan Honeynet BSSN sejak tahun 2018, dapat diakses melalui tautan berikut:

<https://bssn.go.id/honeynet>



Kerjasama Layanan DIGITAL FORENSIK

Laboratorium Forensik Digital (LFD) BSSN merupakan laboratorium yang mendukung pelayanan forensik digital pada bidang insiden keamanan siber seperti *web defacement*, kebocoran data, *ransomware*, pemalsuan, penghapusan data, kehilangan, serta insiden lainnya.

KERJASAMA



Laboratorium Forensik Digital BSSN telah bekerjasama dengan
22 stakeholder

- 17** Pemerintah Pusat
- 4** Pemerintah Daerah
- 1** BUMN

KASUS



5 kasus

dengan 45 lokus pengambilan barang bukti telah ditangani.

BARANG BUKTI

Total barang bukti yang diproses oleh **LFD BSSN** :
406 barang bukti



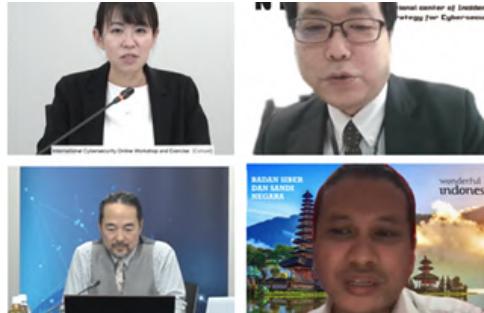
Kegiatan pemeriksaan yang dilakukan pasca terjadinya insiden keamanan siber. Analisis dilakukan pada barang bukti digital berupa perangkat elektronik seperti server, laptop, PC desktop, *handphone*, *hard drive* eksternal serta perangkat lainnya. *Output* yang dihasilkan berupa Laporan Hasil Pemeriksaan Laboratorium Forensik Digital BSSN.



Kolaborasi Internasional ID-SIRTII/CC

NISC International Cybersecurity Online Workshop & TTX

Workshop dan Table Top Exercise (TTX) ini diselenggarakan oleh NISC Jepang dan diikuti oleh Indonesia, Jepang Jerman, Malaysia, Singapura Amerika Serikat, dan Inggris. Kegiatan ini berfokus pada pengembangan ketepatan pengambilan keputusan di kalangan pimpinan organisasi, dalam menganalisis dan menanggapi insiden siber yang mungkin terjadi.



Cyber Bootcamp (National Security College, The Australian National University)

Program Cyber Bootcamp yang diselenggarakan oleh pemerintah Australia memberikan pelatihan keterampilan kepada pejabat pemerintah dari negara-negara ASEAN dan Pasifik. Program ini bertujuan untuk membangun pengetahuan dan kesadaran keamanan siber kepada peserta di berbagai aspek di dunia maya — mulai dari teknologi dan ancaman hingga pengambilan keputusan.



United Nations Office on Drugs and Crime (UNODC) Bilateral Meeting on Ransomware

Dalam upaya mengatasi kejahatan siber berupa serangan ransomware, UNODC bekerja sama dengan negara-negara di Asia Pasifik dalam berdiskusi dan berbagi pengalaman dalam menghadapi serangan siber berupa ransomware. Tidak hanya BSSN, kegiatan ini juga diikuti oleh Tippidsiber POLRI, CSIRT.ID, dan partisipan dari negara lain yaitu Malaysia, Filipina, Singapura, Thailand, dan Vietnam.



English Communication for Cybersecurity Professional, MIIS, Embassy of US

Atas kerjasama BSSN dan Kedutaan Amerika Serikat di Indonesia, BSSN menyelenggarakan pelatihan English Communication for Cybersecurity Professional yang diampu oleh Middlebury Institute of International Study. Kegiatan ini bertujuan untuk meningkatkan kemampuan dan kompetensi personel BSSN dalam bidang keamanan siber.



ASEAN-Japan Policy Meeting & TTX, Jepang dan Indonesia

Kegiatan ini sebagai platform untuk bertukar pandangan, berbagi pengalaman, dan *best practice* setiap negara mengenai tantangan keamanan siber yang dihadapi baik dalam serangan *ransomware* yang menargetkan infrastruktur penting dan tren digitalisasi. Kegiatan ini dihadiri oleh negara-negara di ASEAN dan Jepang.

ITU – UAE "Cyber Protective Shield" Cyber Drill

Bersamaan dengan EXPO2020 DUBAI, ITU bekerjasama dengan Uni Emirat Arab menggelar kegiatan Cyber Drill bertema "Cyber Protective Shield". Bersama dengan negara-negara lain, Indonesia berpartisipasi sebagai peserta *Capture The Flag* (CTF) dan melakukan simulasi serangan siber.

UNODC Bilateral Meeting on Ransomware UN

PBB bersama negara-negara di Asia Pasifik melakukan pembahasan yang memiliki fokus terkait penanganan *ransomware*. Adapun kegiatan ini diselenggarakan di Kuala Lumpur, Malaysia yang dihadiri oleh negara Singapura, Thailand, Filipina, Laos, Samoa, Vanuatu, Fiji, dan PNG.

ASEAN-Japan (NISC) TTX JEPANG

National Center of Incident Readiness and Strategy for Cybersecurity (NISC) Jepang merupakan salah satu anggota FIRST yang menyelenggarakan kegiatan Cyber-Exercise Workshop di Tokyo, Jepang. Kegiatan ini diikuti oleh berbagai negara yaitu: Indonesia, Jepang, Thailand, India, Irlandia, Republik Ceko, dan Singapura.

International Law Enforcement Academy (ILEA) Computer and Network Intrusion Course (CNIC)

ILEA Bangkok merupakan lembaga pendidikan yang beroperasi atas kerjasama pemerintah kerajaan Thailand dan pemerintah Amerika Serikat. ILEA bersama United States Secret Service (USSS) menyelenggarakan CNIC pada Agustus 2022 untuk negara di kawasan ASEAN dan berlangsung di Kantor ILEA Bangkok, Thailand. Negara yang mengikuti kegiatan ini antara lain Indonesia, Malaysia, Filipina, Thailand, dan Singapura.

34th Annual FIRST Conference dan 17th Nat-CSIRT Annual Technical Meeting

Indonesia telah menjadi anggota Forum of Incident Response and Security Teams (FIRST) sejak tahun 2010, dan sebagai pengelola tim tanggap insiden siber nasional, BSSN menjadi anggota dari Nat-CSIRT. Pertemuan tahunan ini dilaksanakan di Irlandia dalam rangka peningkatan kapasitas personel, pemilihan kepengurusan periode baru, hingga sosialisasi hasil penelitian dan *working group* yang dilaksanakan oleh negara-negara anggota.





Industrial Control Systems (ICS) 301L and Cyber Security Evaluation Tool (CSET) oleh Kedutaan Besar Amerika Serikat

BSSN berpartisipasi dalam pelatihan yang mengusung keamanan siber pada ICS yang dilaksanakan atas kerjasama dengan Kedutaan Besar Amerika Serikat. Kegiatan ini berupa intensive training terkait pelindungan dan pengamanan ICS dari ancaman inisiden siber dan pelatihan secara berkelompok *Red Team/Blue Team* yang disesuaikan dengan lingkungan sistem kontrol yang sebenarnya.

Singapore ACID Drill Test

ASEAN CERT Incident Drill (ACID) kembali dilaksanakan dan merupakan ACID ke-16 yang diselenggarakan dengan tema yang diangkat dalam kegiatan tersebut adalah "*Dealing with Disruptive Cyber-Attacks Arising from Exploitation of Vulnerabilities*".

24th AJCCBC Cybersecurity Technical Training ASEAN-Japan Cybersecurity Capacity Building Centre

ASEAN-Japan Cybersecurity Capacity Building Centre atau AJCCBC adalah sebuah pusat pelatihan keamanan siber yang ditujukan untuk anggota negara-negara ASEAN untuk meningkatkan kapabilitas mereka dalam bidang keamanan siber.

China Network Security Conference and Seminar (CNCERT)

Kerjasama Indonesia dengan CN-CERT Tiongkok terus berlanjut dengan terus dilakukannya peningkatan kapasitas dan pengetahuan melalui program edukasi berupa seminar dan konferensi.

Singapore Sharing Session on Ransomware

Singapura mengundang negara-negara ASEAN dalam pembahasan aktivitas serangan siber *ransomware* yang terjadi di lingkup ASEAN.

Arab Drill Test Arab Saudi

ITU-ARAB Regional Cybersecurity Center ikut mendukung kegiatan OIC-CERT Annual General Meeting dengan menyelenggarakan *cyber drill* pada rangkaian kegiatan tahunan tersebut. Indonesia bersama beberapa negara anggota OIC-CERT mengikuti kegiatan ini secara daring.

Africa-CERT Annual Cyber Security Drill 2022

ITU-ARAB Regional Cybersecurity Center ikut mendukung kegiatan OIC-CERT Annual General Meeting dengan menyelenggarakan *cyber drill* pada rangkaian kegiatan tahunan tersebut. Indonesia bersama beberapa negara anggota OIC-CERT mengikuti kegiatan ini secara daring.

ITU-ASEAN CyberDrill

Indonesia berpartisipasi dalam kegiatan ITU-ASEAN Cyber Drill dalam rangka peningkatan kapasitas di bidang penanganan insiden keamanan siber.

OIC-CERT 10th GENERAL MEETING & 14th ANNUAL CONFERENCE 2022

OIC-CERT atau *Organization of Islamic Cooperation Computer Emergency Response Team* merupakan organisasi untuk koordinasi dan kerjasama CSIRT pada negara-negara Islam. Id-SIRTII/CC aktif mengikuti beberapa program capacity building yang diselenggarakan oleh OIC-CERT seperti *Table top exercise*, *cyber drill test*, *workshop* dan *webinar*. Pada kegiatan OIC-CERT 10th GENERAL MEETING & 14th ANNUAL CONFERENCE Tahun 2022, Indonesia terpilih kembali sebagai Board Committee dan Deputy Chair of OIC-CERT untuk periode 2022-2024.





TOP 3 INSIDEN SIBER

LESSON LEARNED

LESSON LEARNED

Respon dari Pemilik Sistem Elektronik (PSE) dan/atau CSIRT Organisasi terhadap Layanan Asistensi Tanggap Insiden dikelompokkan menjadi 4 (empat) kategori respons yaitu *Handle BSSN*, Kolaborasi, *Handle PSE/CSIRT*, dan Tidak Respon, berikut merupakan detail respons asistensi pada tahun 2022:

			
HANDLE BSSN 25 Insiden Proses asistensi penanganan insiden dilakukan secara penuh oleh BSSN.	KOLABORASI 7 Insiden Proses penanganan insiden dilakukan oleh PSE dan/atau CSIRT yang bekerja sama dengan BSSN	HANDLE PSE/CSIRT ORGANISASI 34 Insiden Proses penanganan insiden yang dilakukan secara penuh oleh PSE/CSIRT.	TIDAK RESPON 2 Insiden Tidak melakukan konfirmasi atas kelanjutan penanganan.

Layanan Asistensi Tanggap Insiden sepanjang 2022 terdapat 68 penanganan yang terdiri dari beberapa sektor yaitu sebagai berikut:

			
ADMINISTRASI PEMERINTAH 47 insiden	SEKTOR ESDM 2 insiden	SEKTOR KESEHATAN 2 insiden	SEKTOR KEUANGAN 2 insiden
			
SEKTOR PENDIDIKAN 3 insiden	SEKTOR TIK 5 insiden	SEKTOR TRANSPORTASI 2 insiden	SEKTOR LAINNYA 4 insiden



Pasca Layanan Asistensi Tanggap Insiden, diketahui bahwa Top 3 insiden yang terjadi yaitu kebocoran data, *ransomware*, dan *web defacement*.



MASSIVE DATA BREACH

INSIDEN KEBOCORAN DATA

Insiden kebocoran data merupakan insiden siber dimana data atau rahasia milik organisasi telah diakses dan diungkap ke publik oleh *threat actor* tanpa sepengetahuan dari pemilik sistem. Data-data yang diambil oleh penyerang umumnya bersifat sensitif, seperti *Personal Identifiable Information* (PII), data sensitif organisasi, dan data lainnya yang seharusnya hanya diketahui oleh pihak yang memiliki hak. Berdasarkan hasil asistensi tanggap insiden diperoleh informasi terkait dengan *attack vector* insiden kebocoran data, skema insiden kebocoran data, dan *lesson learned* yang dapat diambil dari insiden kebocoran data.

Top 5 Attack Vector Kebocoran Data

Berikut ini pemetaan ke *Framework MITRE ATT&CK* pada Top 5 *attack vector* yang teridentifikasi digunakan oleh penyerang pada insiden Kebocoran Data

A **Compromised Account (T1586)**

Threat actor memanfaatkan akun-akun yang telah terkompromi oleh *malware stealer* atau dari *social engineering* untuk masuk ke sistem. *Threat actor* biasanya menggunakan beberapa metode untuk melakukan kompromi akun seperti menggunakan *phishing*, *malware stealer*, ataupun membeli dari pihak ketiga. *Compromised account* biasanya terjadi pada *end-user* yang dengan menimbulkan tingkat kepercayaan untuk mengunjungi atau mengakses suatu *link malicious*.

B **Valid Accounts (T1078)**

Threat actor dapat memanfaatkan akun yang telah terkompromi untuk masuk ke sistem yang merupakan akun pengguna yang *legitimate*. *Threat actor* dapat memilih menggunakan *valid accounts* yang telah terkompromi dari pada menggunakan *malware* yang kemungkinan akan terdeteksi perimeter keamanan. Dengan menggunakan *valid accounts* akan memudahkan *threat actor* untuk masuk ke sistem dan melakukan *persistence*, *privilege escalation*, atau *defense evasion*. Biasanya *threat actor* memanfaatkan akun-akun VPN, Remote Desktop, dan Outlook Web Access.

C **Exploit Public-Facing Application (T1190)**

Threat actor memanfaatkan kelemahan yang terdapat pada situs web untuk melakukan berbagai percobaan serangan seperti *SQL Injection*, *File Upload*, *XSS*, exploitasi CVE dan lain sebagainya. Dengan melakukan eksplorasi pada sistem tersebut *threat actor* dapat masuk ke sistem dan mengakses *database*.

D **Compromise Infrastructure (T1584)**

Threat actor memanfaatkan infrastruktur yang telah terkompromi untuk melakukan serangan pada infrastruktur atau sistem lain. *Threat actor* menggunakan infrastruktur pihak lain sebagai *proxy* untuk menghindari deteksi atau mengaburkan keberadaan *threat actor*.

E **Active Scanning (T1595)**

Threat actor melakukan *scanning* secara aktif pada sistem target untuk mengumpulkan informasi yang dapat dilakukan eksplorasi. Aktivitas ini akan dilakukan pada sistem informasi yang dapat diakses secara publik, bahkan *threat actor* juga akan melakukan *scanning* melalui perangkat korban untuk mengetahui informasi infrastruktur jaringan dalam satu segment dengan korban.



Skema Insiden Kebocoran Data

A **Information Gathering**

Threat actor akan menentukan target, melakukan pemindaian untuk mencari informasi pada sistem yang dapat dimanfaatkan untuk eksploitasi. *Threat actor* juga akan berusaha untuk mendapatkan informasi terkait *user-user* untuk selanjutnya menjadi target serangan *phishing*.

B **Attack**

Threat actor memanfaatkan informasi sistem yang telah diperoleh untuk melakukan eksploitasi sistem, dan berupaya untuk dapat *persistence* dan bahkan *lateral movement* ke administrator ataupun dengan mengirimkan *phishing* terhadap pengguna-pengguna yang telah diketahui sebelumnya untuk mengirimkan *malware*.

C **Exfiltrasi Data**

Setelah *threat actor* berhasil masuk ke sistem, *threat actor* akan mengakses dan melakukan ekspor *database* atau dokumen-dokumen penting lainnya. Data-data tersebut biasanya akan diperjualbelikan pada *darkweb*.



Kevin Mitnick

You can never protect yourself 100%. What you do is protect yourself as much as possible and mitigate risk to an acceptable degree. You can never remove all risk

Lesson Learned

Kebocoran Data

Indonesia telah memiliki peraturan terkait data pribadi yaitu tertuang dalam Undang-Undang No 27 Tahun 2022 tentang Pelindungan Data Pribadi. UU tersebut mengatur terkait persetujuan pemilik data hingga konsekuensi hukum termasuk sanksi pidana bagi pelanggar aturan. Dengan adanya UU tersebut memberikan landasan hukum bagi Indonesia dalam keamanan dan perlindungan terhadap data pribadi warga negara Indonesia. Berdasarkan insiden kebocoran data yang pernah terjadi, berikut terdapat beberapa upaya yang dapat dilakukan untuk mencegah kebocoran data:

A Melakukan IT Security Assessment pada sistem informasi yang dimiliki

Threat actor memanfaatkan akun-akun yang telah terkompromi oleh *malware stealer* atau dari *social engineering* untuk masuk ke sistem. *Threat actor* biasanya menggunakan beberapa metode untuk melakukan kompromi akun seperti menggunakan *phishing*, *malware stealer*, ataupun membeli dari pihak ketiga. *Compromised account* biasanya terjadi pada *end-user* yang dengan menimbulkan tingkat kepercayaan untuk mengunjungi atau mengakses suatu *link malicious*.

B Menerapkan kebijakan penggunaan strong password

Pemilik sistem sebaiknya menerapkan kebijakan penggunaan *password* yang kompleks dan melakukan penggantian *password* secara berkala. Hal ini bertujuan untuk mengurangi risiko terjadinya akun yang terkompromi serta mempersulit *bruteforce attack*.

C Melakukan edukasi terhadap pengguna sistem

Pengguna sering kali menjadi titik terlemah dalam keamanan jaringan yang dapat dimanfaatkan oleh *threat actor* sebagai pintu masuk. *Threat actor* dapat melakukan *social engineering* atau dengan mengirimkan *phishing* kepada korban. Pengguna sistem diimbau untuk tidak membuka tautan/file/e-mail/URL dari sumber yang tidak diketahui kebenarannya serta tidak mengakses situs ilegal.

D Melakukan reviu akun sistem dan aplikasi

Akun pengguna menjadi hal yang krusial dalam beberapa kasus kebocoran data, hal tersebut karena *threat actor* memanfaatkan akun pengguna yang telah terkompromi untuk masuk secara sah ke sistem untuk selanjutnya melakukan *lateral movement* ke sistem lain. Oleh karena itu, perlu dilakukan reviu secara berkala daftar akun pengguna.



Bruce Schneier

If someone steals your password, you can change it. But if someone steals your thumbprint, you can't get a new thumb.

E Melakukan penonaktifan port layanan

Layanan sistem atau *port* sering kali dimanfaatkan *threat actor* untuk dapat masuk ke sistem. Layanan sistem yang sering dimanfaatkan *threat actor* sebagai *initial access* dan bahkan untuk melakukan *lateral movement* antara lain layanan SMB, SSH, FTP, dan RDP, sehingga diperlukan penutupan layanan yang tidak digunakan.

F Melakukan Validasi Data terhadap Insiden yang terjadi

Beberapa insiden yang terjadi diketahui bahwa data yang dibocorkan oleh *threat actor* merupakan data hasil penggabungan dengan data-data lain dengan penambahan beberapa *database field*. Oleh karena itu pemilik sistem perlu melakukan validasi terhadap data yang dibocorkan oleh *threat actor* untuk memastikan kesesuaian data tersebut.

F Melakukan penyampaian kepada pemilik data atau masyarakat

Berdasarkan Undang-Undang No 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 46 disebutkan bahwa Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis yang mencakup data pribadi yang terungkap, kapan dan bagaimana data pribadi terungkap, serta upaya penanganan dan pemulihan terkait kegagalan Pelindungan Data Pribadi. Hal tersebut disampaikan paling lambat 3x24 jam kepada Subjek Data, dan Lembaga, serta wajib memberitahukan kepada masyarakat.

G Melakukan *hardening* atau *patching* pada sistem yang terdampak

Setelah dilakukan analisis terhadap hasil *imaging*, maka akan dimungkinkan ditemukan *initial access threat actor* masuk ke sistem. Dengan hal tersebut maka dapat dilakukan *hardening* sistem operasi serta *patching* seluruh teknologi yang digunakan seperti *framework*, *Content Management System (CMS)*, *plugins*, dan *theme*.



RANSOMWARE

INSIDEN RANSOMWARE

Insiden *ransomware* merupakan insiden siber yang disebabkan oleh *malware* yang menyerang perangkat dan melakukan enkripsi pada data yang terdapat pada perangkat serta melakukan eksfiltrasi data yang bertujuan untuk mengancam korban supaya membayar tebusan atas data tersebut. Saat ini metode *ransomware* mengarah pada *multiple extortion*, yaitu selain melakukan penyaderaan data dalam enkripsi, *threat actor* juga mengancam untuk mempublikasikan data sensitif apabila tebusan tidak diberikan oleh pemilik sistem.

Insiden serangan *ransomware* pada berbagai organisasi lintas sektor turut mewarnai lanskap ancaman siber di Indonesia sepanjang 2022. Berdasarkan pemantauan yang dilakukan BSSN terhadap situs *darkweb*, setidaknya telah terjadi 17 serangan *ransomware* yang disertai dengan publikasi data sensitif pada berbagai organisasi di Indonesia. Berdasarkan hasil Asistensi Tanggap Insiden, diketahui Top 3 jenis ransomware beserta attack vector yang dimanfaatkan threat actor sebagai berikut:

TOP 3 RANSOMWARE

Ransomware LockBit

LockBit tercatat sebagai kelompok *ransomware* yang paling aktif melakukan serangan sepanjang 2022. Diperkirakan telah terjadi 836 insiden serangan *ransomware* global yang dikaitkan dengan kelompok *ransomware* LockBit (2022 Ransomware Statistics – DeepWeb intelligence Feed (darkfeed.io)). Terhadap organisasi di Indonesia, BSSN mencatat LockBit telah menyerang beberapa organisasi yang berasal dari sektor industri, transportasi, dan energi. LockBit diketahui telah melakukan sejumlah perubahan radikal setelah ditemukannya *critical bug* pada proses enkripsi oleh *ransomware* LockBit 2.0 (Part 1: LockBit 2.0 *ransomware bugs and database recovery attempts* - Microsoft Community Hub). Perubahan radikal tersebut mencakup perubahan dan pemutakhiran struktur kode *ransomware*, peningkatan ancaman dengan teknik ekstorsi baru, serta mengeluarkan program *bounty reward* bagi yang ingin bekerja sama dengan kelompok *ransomware* LockBit (LockBit 3.0 Update | *Unpicking the Ransomware's Latest Anti-Analysis and Evasion Techniques* - SentinelOne).

<https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/>

Ransomware BlackCat

Ransomware BlackCat merupakan kelompok *ransomware* yang menjalankan bisnis *ransomware-as-a-service* (RaaS) seperti kelompok *ransomware* pada umumnya dan telah aktif menyerang sejak November 2021. BlackCat diketahui telah melakukan sejumlah serangan yang ditargetkan dan terkenal karena menjadi kelompok *ransomware* pertama yang menggunakan bahasa pemrograman Rust *The many lives of BlackCat ransomware - Microsoft Security Blog*. Bahasa pemrograman Rust membuat BlackCat mampu mengurangi kemungkinan adanya *bug* yang dapat dieksplorasi oleh para ahli keamanan siber dalam mencari *decryptor*. Serangan *ransomware* BlackCat pada organisasi di Indonesia dalam periode tahun 2022 diidentifikasi terjadi pada sektor TIK dan Konstruksi.

<https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/>

Ransomware Vice Society

Serangan *ransomware* pada organisasi di Indonesia pada tahun 2022 juga dilakukan oleh kelompok *ransomware* Vice Society yang berdampak pada sektor Pemerintah dan Transportasi. Kemunculan *ransomware* Vice Society terdeteksi sejak 2021. Pada tahun 2022 Vice Society dikenal aktif melakukan serangan pada sektor pendidikan terutama pada organisasi pendidikan yang berlokasi di Amerika Serikat. Hal tersebut mendapat perhatian khusus oleh otoritas keamanan siber Amerika Serikat hingga mengeluarkan peringatan khusus *Joint Cybersecurity Advisory* (CSA) dari FBI, CISA, dan *Multi-State Information Sharing and Analysis Center* (MS-ISAC) berupa ancaman kelompok *ransomware* Vice Society di tahun mendatang #StopRansomware: Vice Society | CISA.

<https://www.cisa.gov/uscert/ncas/alerts/aa22-249a>

Top 5 Attack Vector Ransomware

Besarnya potensi daya kerusakan dan kerugian yang dapat ditimbulkan oleh serangan *ransomware* perlu menjadi perhatian khusus bagi seluruh PSE. BSSN mengidentifikasi sejumlah *attack vector* yang umumnya digunakan oleh kelompok *ransomware*.

A ***Spearphishing Attachment (T1566.001)***

Untuk mendapatkan akses awal ke sistem korban, *threat actor* memanfaatkan *e-mail* dengan lampiran yang berisi kode berbahaya. Lampiran *spearphishing* adalah jenis *spearphishing* dengan target spesifik/khusus yang menggunakan metode pengiriman *e-mail* dengan lampiran *malware* yang bertujuan untuk menjalankan kode berbahaya pada sistem korban. Taktik ini juga melibatkan teknik *social engineering*, yakni *threat actor* menyamar sebagai sumber yang terpercaya untuk menipu korban agar membuka lampiran tersebut.

B ***Exploit Public-Facing Application (T1190)***

Threat actor memanfaatkan kelemahan pada komputer atau program yang terhubung ke internet menggunakan perangkat lunak, data, atau perintah untuk menyebabkan dampak yang tidak diinginkan atau tidak terduga. Terdapat sejumlah kerentanan aplikasi yang diketahui dieksplorasi oleh kelompok *ransomware* untuk mendapatkan akses awal ke perangkat korban.

C ***Drive-by Compromise (T1189)***

Threat actor memanfaatkan situs web terinfeksi yang dirancang agar dapat menginfeksi perangkat korban ketika korban mengunduh suatu program dari *website* yang sudah diinfeksi.

D ***Valid Accounts (T1078)***

Dalam menginfeksi perangkat korban, *threat actor* memanfaatkan akun kredensial organisasi yang telah terkompromi dan dijual di *darkweb*. Akun kredensial yang valid digunakan *threat actor* untuk melakukan *bypass perimeter* sistem keamanan yang dimiliki organisasi korban.

E ***External Remote Services (T1133)***

Threat actor memanfaatkan kerentanan pada konfigurasi aplikasi *remote* yang digunakan oleh organisasi seperti layanan RDP dan aplikasi VPN untuk masuk ke dalam sistem organisasi korban.

Lesson Learned

Ransomware

BSSN merekomendasikan seluruh organisasi PSE untuk berkoordinasi dan membangun kolaborasi yang kuat dengan BSSN guna meningkatkan postur keamanan siber organisasi dalam melindungi dan merespons terjadinya insiden siber khususnya yang diakibatkan oleh *ransomware*. Berdasarkan insiden *ransomware* yang pernah terjadi, berikut terdapat beberapa upaya yang dapat dilakukan untuk mencegah terjadinya *ransomware*.

A Melakukan implementasi *security perimeter* di level jaringan

Implementasi *security perimeter* di level jaringan bertujuan agar organisasi dapat secara cepat melakukan identifikasi, deteksi, dan investigasi aktivitas abnormal dan potensi aktivitas *ransomware* sebelum serangan *ransomware* pada organisasi terjadi. Penggunaan *security perimeter* seperti *firewall* diperlukan untuk memblokir lalu lintas berbahaya yang diketahui pada jaringan organisasi.

B Melakukan implementasi segmentasi jaringan untuk mencegah penyebaran *ransomware*

Segmentasi jaringan dapat membantu mencegah penyebaran *ransomware* yang telah menginfeksi perangkat organisasi dengan mengendalikan arus lalu lintas antara-dan akses ke-berbagai subjaringan dan dengan membatasi *lateral movement* oleh *threat actor*.

C Melakukan implementasi *end-point security* dengan kemampuan *behavior analysis*

Perangkat lunak *endpoint security* dengan kemampuan *behavior analysis* dapat membantu melindungi perangkat hingga titik *endpoint* terhadap infeksi *ransomware* dengan mendeteksi dan memblokir *malware* sebelum berhasil mengenkripsi *file-file* pada perangkat. Oleh karena itu, diperlukan untuk selalu memperbarui perangkat lunak *end point security* dan menjalankan pemindaian secara berkala untuk memastikan bahwa sistem senantiasa terlindungi.

D Melakukan penerapan kebijakan keamanan

Organisasi perlu mereviu kembali seluruh kebijakan keamanan yang dimiliki oleh organisasi terutama terkait dengan Kebijakan Penggunaan Perangkat Pribadi untuk Pekerjaan ataupun Akses ke *Corporate Network*, Kebijakan Instalasi Piranti Lunak, Kebijakan Penggunaan Internet, Kebijakan *Teleworking*, dan Kebijakan Penggunaan *Removable Media*. Pastikan seluruh kebijakan keamanan telah teridentifikasi dan diterapkan secara menyeluruh dengan dukungan penerapan yang kuat.

E

Melakukan prosedur *backup* data secara dan berkala, kemudian lakukan uji coba *restore* secara periodik guna memastikan prosedur *backup-restore* dapat berjalan dengan baik

Dengan menerapkan kegiatan ini ini, organisasi dapat memastikan bahwa mereka tidak akan terganggu jika serangan *ransomware* terjadi. Oleh karena itu, perlu dipisahkan lokasi penyimpanan utama dan lokasi penyimpanan *backup* guna menghindari infeksi *ransomware* pada penyimpanan *backup*.

F

Isolasi host terdampak dari jaringan

Organisasi perlu dapat melakukan respons cepat terhadap aktivitas mencurigakan yang berjalan dengan mengisolasi host terdampak dari segmen jaringan yang dimiliki organisasi untuk dapat mengurangi dampak dari serangan *ransomware* yang sedang berlangsung.

G

Tidak melakukan *shutdown* host terdampak dan melakukan *imaging* host terdampak

Berdasarkan asistensi tanggap insiden serangan *ransomware* sepanjang 2022, sejumlah organisasi ditemukan langsung mematikan perangkat host terdampak saat insiden terjadi yang bertujuan untuk meminimalisir dampak serangan. Langkah tersebut kemudian berdampak pada hilangnya sejumlah artifak dan bukti digital yang diperlukan dalam melakukan investigasi dan pemulihan setelah insiden terjadi.

H

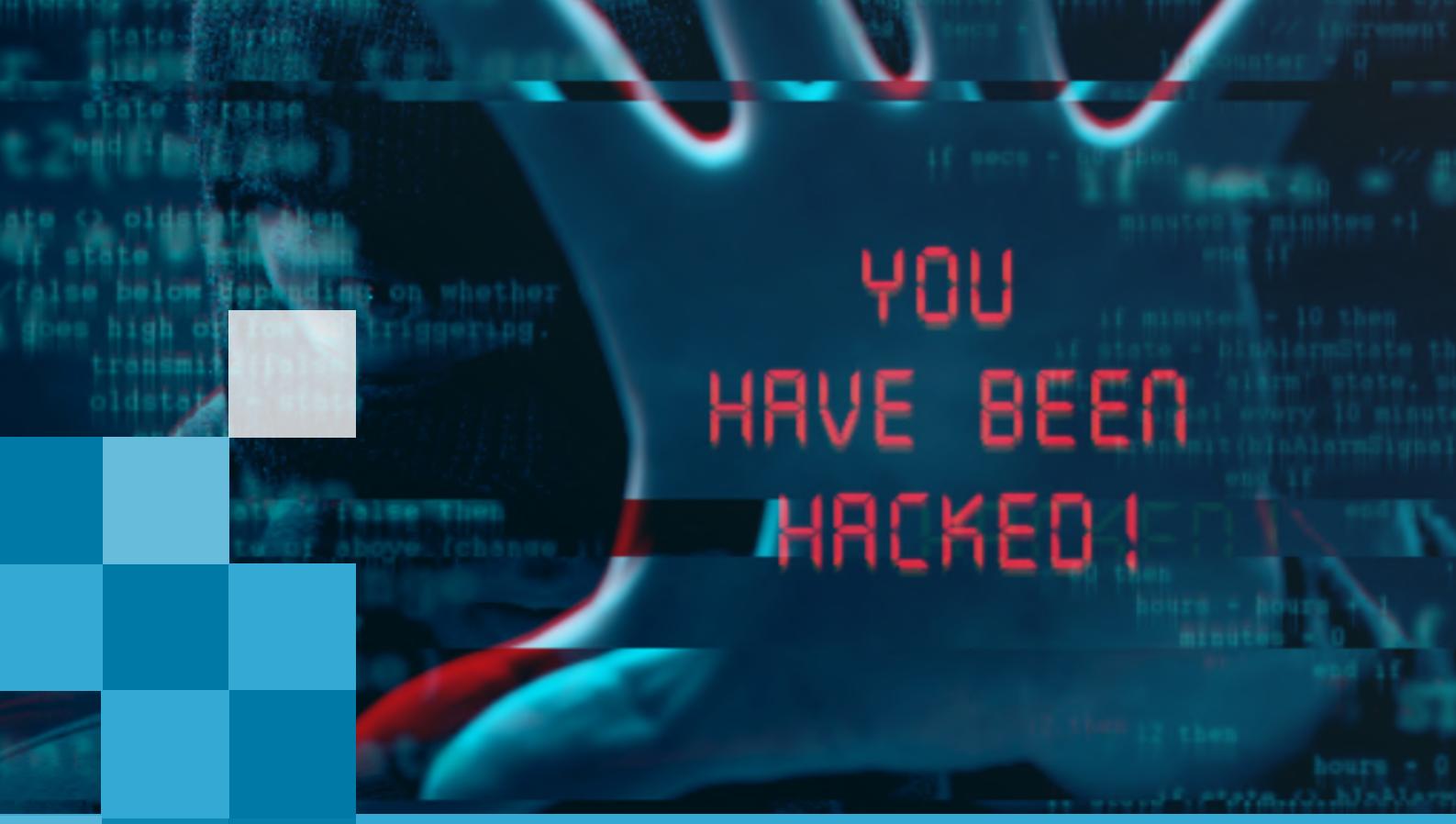
Melakukan prosedur mitigasi sesuai dokumen perencanaan tindak lanjut insiden

Penting bagi organisasi menjalankan skenario mitigasi yang telah tertuang dalam dokumen *Incident Response Plan* (IRP), *Disaster Recovery Plan* (DRP), dan *Business Continuity Plan* (BCP) guna memastikan prosedur pemulihan telah berjalan sesuai dengan prosedur yang ditetapkan oleh organisasi.

I

Melakukan *Compromise Assessment* (CA) untuk mencegah artefak yang tertinggal pada host terdampak

Investigasi mendalam perlu dilakukan organisasi untuk memastikan tidak ada artefak berupa *backdoor* ataupun *shell payload* masih tersisa di perangkat terdampak.



YOU
HAVE BEEN
HACKED!

INSIDEN WEB DEFACEMENT

Insiden *web defacement* merupakan insiden yang terjadi pada tampilan *website* dimana *threat actor* melakukan perubahan tampilan *website* sehingga dapat merusak reputasi pemilik sistem. Umumnya web defacement memanfaatkan kerentanan pada sistem website seperti CMS, Plugin, dan Web Engine yang tidak dilakukan *update*. Walaupun metode serangan yang digunakan dikategorikan sederhana dan mudah, namun insiden *web defacement* dapat dimanfaatkan sebagai awalan pintu masuk insiden lainnya dan bahkan server yang terkompromi dapat digunakan sebagai *botnet* untuk melakukan serangan ke sistem/infrastruktur lainnya.

Top 3 Attack Vector Web Defacement

Berdasarkan hasil Asistensi Tanggap Insiden, diketahui *attack vector* yang dimanfaatkan *threat actor* sebagai berikut:

A

Exploit Public-Facing Application (T1190)

Threat actor memanfaatkan kelemahan yang terdapat pada situs web untuk melakukan berbagai percobaan serangan seperti SQL Injection, File Upload, XSS, dan lain sebagainya.

B

Active Scanning (T1595)

Threat actor melakukan scanning untuk mengumpulkan informasi yang dapat dilakukan eksplorasi dari sistem target.

C

Compromised Account (T1586)

Threat actor memanfaatkan akun-akun yang telah terkompromi oleh malware stealer untuk masuk ke sistem.

Lesson Learned

Web Defacement

Berdasarkan insiden *web defacement* yang pernah terjadi, berikut terdapat beberapa upaya yang dapat dilakukan untuk mencegah terjadinya *web defacement*:

A

Melakukan **security hardening** pada OS Server

Hal tersebut dilakukan untuk mengurangi kemungkinan vektor serangan pada OS server baik pada server yang digunakan sehingga semakin sulit bagi para *hacker* untuk menyerang server tersebut. Hal ini juga dapat dilakukan dengan penambahan antivirus atau *End-Point Detection and Response* (EDR) pada server.

B

Memperkuat mekanisme dan manajemen autentikasi pengguna yang mengakses server secara remote

Sebaiknya melakukan pembatasan akses pada autentikasi akun yang melakukan SSH dengan cara konfigurasi pada SSH *whitelist/blacklist* pengguna SSH, kustomisasi *port* SSH (diusahakan tidak menggunakan *port* umum), menerapkan penggunaan sertifikat untuk proses autentikasi SSH, menentukan pengguna yang mendapatkan hak akses *root*, melakukan *review* terhadap akses pengguna secara berkala.

C

Melakukan pengumpulan *log* secara tersentralisasi

Pemilik sistem dapat melakukan pengumpulan *log* secara tersentralisasi untuk memudahkan dalam proses *monitoring* secara analisa ketika terjadi suatu insiden. Beberapa *tools opensource* yang dapat digunakan untuk sentralisasi *log* adalah salah satunya Elasticsearch, Logstash, dan Kibana (ELK).

D

Melakukan penonaktifan layanan sistem yang tidak digunakan

Sistem layanan yang tidak digunakan sebaiknya untuk dinonaktifkan karena dapat menjadi risiko untuk disalahgunakan oleh penyerang. Selain itu, pemilik sistem disarankan untuk menutup *port* yang tidak digunakan. Hal ini diakibatkan karena layanan sistem dan *port* dapat digunakan oleh penyerang, seperti *port* SMB, SSH dan RDP untuk melakukan *lateral movement* dari salah satu yang terinfeksi kedalam sistem lainnya untuk menimbulkan dampak yang lebih besar.

E

Melakukan penggantian halaman terdampak dengan halaman perbaikan

Untuk pemberitahuan secara umum pada pengunjung *website*, perlu segera dibuatkan halaman perbaikan untuk memberitahukan bahwa pada saat ini *website* sedang dalam perbaikan karena suatu hal, supaya pengunjung tahu bahwa *website* yang sedang dituju masih *available* namun sedang dalam proses pemeliharaan/perbaikan.



David Bernstein

For every lock, there is someone out there trying to pick it or break in.

F Melakukan security hardening pada CMS yang digunakan

Menerapakan *best practice* pada CMS dan selalu melakukan *update* secepatnya pada CMS. Hal ini dilakukan untuk mengurangi kemungkinan vektor serangan melalui kerentanan pada CMS yang dapat di eksplorasi oleh penyerang.

G Melakukan pemindaian kerentanan pada server

Pemindaian kerentanan ini ditujukan untuk memeriksa kerentanan yang diindikasikan masih ada pada sistem terdampak sehingga jika ditemukan maka dapat dilakukan penutupan celah oleh pemilik sistem.

H Memastikan konten kembali seperti semula

Untuk menghindari adanya *file-file malicious* yang ada pada direktori website, pemilik sistem harus memeriksa apakah konten yang asli sudah sesuai atau adakah perubahan yang dilakukan oleh penyerang, guna untuk melakukan penanggulangan dari insiden yang terjadi supaya layanan *website* dapat berjalan kembali secara normal.

G Melakukan penanggulangan terhadap celah yang ada dan menjalankan layanan web kembali

Setelah analisis dilakukan dan ditemukan celah kerentanan serta *malicious file*, perlu dilakukan penanggulangan hal tersebut seperti penghapusan *malicious file* yang ada, mengganti index.php yang baru, melakukan *patching* aplikasi terbaru supaya layanan website dapat berjalan seperti sediakala. Pemulihan sistem layanan website harus segera dilakukan supaya tidak mengganggu jalannya proses bisnis yang ada.



PREDIKSI ANCAMAN SIBER TAHUN 2023

Berdasarkan pencarian yang dilakukan melalui sumber pencarian terbuka dan analisis data monitoring lalu lintas jaringan pada tahun 2022, didapatkan adanya beberapa ancaman siber yang diprediksi akan muncul di tahun 2023. Ancaman siber tersebut meliputi *Ransomware*, Kebocoran Data, Serangan APT, *Phishing*, *Cryptojacking*, *Distributed denial of service* (DDoS), Serangan RDP, serta *Social Engineering*, *Artificial Intelligence* (AI), IoT Cybercrime, dan *Web Defacement*. Peningkatan jumlah yang signifikan di beberapa tahun terakhir menyebabkan beberapa ancaman tersebut diprediksi akan tetap banyak terjadi di tahun 2023. Langkah yang dapat dilakukan untuk terhindar dari beberapa ancaman tersebut antara lain melakukan *backup data* secara berkala, menerapkan pembatasan hak akses, melakukan pembaruan sistem operasi, dan lain sebagainya.

Ransomware



Ransomware is more about manipulating vulnerabilities in human psychology than the adversary's technological sophistication

-- James Scott

Ransomware merupakan salah satu bentuk ancaman siber yang dapat mengunci akses terhadap aset (sistem ataupun data), kemudian meminta sejumlah biaya untuk menebus akses tersebut kepada pemilik aset. Berdasarkan survei *ransomware* global yang dilakukan oleh Fortinet, didapatkan terdapat 67% organisasi terdampak serangan *ransomware*. Maraknya perkembangan *ransomware* secara global juga sejalan dengan tingginya jumlah serangan *ransomware* yang terjadi di Indonesia.

Pada Laporan Tahunan Monitoring Kemanan Siber BSSN tahun 2022, tercatat *ransomware* menduduki peringkat ketiga sebagai jenis serangan yang paling banyak dilaporkan setelah *Misconfiguration*. Dari 506.185 *ransomware submissions* yang dicatat oleh Emsisoft, sebanyak 13,80% submissions berasal dari Indonesia. Oleh karena itu, Indonesia masuk ke dalam kategori 10 besar negara yang melaporkan insiden *ransomware*. Penyerang dapat menaikkan harga tebusan dengan menambahkan *malware wiper* ke serangan *ransomware* yang dilakukan. *Malware wiper* menambah kemampuan penyerang untuk menghapus data dan melumpuhkan ketersediaan sistem penting, seperti *Operational Technology* (OT) atau peralatan manufaktur dan server. Teknik *malware wiper* juga dimanfaatkan dalam perang di Ukraina untuk menyerang infrastruktur vital pada tahun 2022.



John David McAfee

A hacker is someone who uses a combination of high-tech cyber tools and social engineering to gain illicit access to someone else's data.

Selain itu, FortiGuard Labs juga mengidentifikasi setidaknya 7 varian *wiper* baru dalam 6 bulan pertama tahun 2022 yang digunakan dalam berbagai gerakan melawan pemerintah, militer, dan organisasi swasta. Peningkatan jumlah insiden serangan *ransomware* di tahun 2021 dan 2022, ditambah dengan adanya *malware wiper* yang membuat *ransomware* lebih merusak dan canggih, memungkinkan *ransomware* menjadi salah satu jenis serangan yang akan tetap dimanfaatkan penyerang pada tahun 2023. Peluang ini akan dimanfaatkan oleh *Ransomware-as-a-Service* (Raas) provider maupun pelaku *double extortion* untuk melakukan modernisasi perangkat lunak yang dimiliki dan fokus pada eksfiltrasi data dan "leak sites" untuk memperjual belikan data dan mempermalukan publik.



Kebocoran Data

“ Data is the pollution problem of the information age, and protecting privacy is the environmental challenge.

-- Bruce Schneier

Insiden kebocoran data merupakan upaya penyerang untuk melakukan pencurian data untuk selanjutnya dipublikasikan secara publik tanpa sepengetahuan dari pemilik sistem. Data-data yang diambil oleh penyerang umumnya bersifat sensitif, seperti *Personal Identifiable Information* (PII), data sensitif organisasi, dan data lainnya yang seharusnya hanya diketahui oleh pihak yang memiliki hak. Berdasarkan pada artikel "Lesson Learned from A Decade Data Breach" oleh F5 Labs, disebutkan bahwa penyebab utama dari insiden kebocoran data adalah *Web Application Vulnerability* dan *Phishing*.

Kerawanan pada *web application* menjadi penyebab utama terbesar dalam insiden kebocoran data yang diakibatkan adanya kesalahan konfigurasi pada web atau adanya fitur pendukung seperti tema, *plugin*, atau *framework* dari *web application* yang dapat dieksloitasi. Kesalahan konfigurasi dapat menyebabkan data sensitif pada web diakses secara publik. Sedangkan pada *phishing*, umumnya penyerang akan menyiapkan kode-kode berbahaya pada dokumen atau *e-mail*, sehingga ketika korban membuka dokumen tersebut, kode akan dieksekusi. Lemahnya sistem keamanan yang menyebabkan kerentanan sistem TI, perilaku pengguna yang kurang cermat dalam mengelola informasi, serta tersedianya platform untuk melakukan jual beli data menjadikan serangan dengan tujuan pencurian data memiliki daya tarik yang cukup tinggi bagi penyerang untuk mendapatkan keuntungan.



Serangan APT



For every lock, there is someone out there trying to pick it or break in.

-- David Bernstein

Fortinet sebagai perusahaan keamanan siber memprediksi bahwa akan terdapat peningkatan aktivitas *Advanced Persistent Threat* (APT) pada tahun 2023. Aktivitas tersebut berupa pengintaian (*reconnaissance*) maupun persenjataan praserangan (*Weaponization*). Peningkatan aktivitas APT tersebut berpotensi membuka jalan untuk peningkatan *Crime-as-a-Service* (CaaS). Berdasarkan data *ransomware* pada tahun 2022, terjadi peningkatan varian *ransomware* yang mencapai hampir 100% hanya pada paruh pertama tahun 2022. Pada 6 bulan pertama ditahun 2022, Fortinet menemukan 10,666 *ransomware*. Sedangkan pada tahun 2021 hanya ditemukan sebanyak 5,400 *ransomware* baru. Berbagai jenis *ransomware* inilah yang digunakan oleh kelompok APT untuk memperkaya teknik serangan mereka.

Seiring dengan pernyataan Fortinet, dalam Laporan Tahunan Monitoring Keamanan Siber tahun 2021 BSSN menyatakan bahwa terdapat 1.676.286 aktivitas APT di Indonesia. Berdasarkan laporan tersebut, APT atau *Advanced Persistent Threat* dapat diartikan sebagai pelaku ancaman siber berupa kelompok yang biasanya disponsori oleh negara atau organisasi besar lain dengan tujuan untuk memperoleh akses tidak sah ke jaringan komputer target dan tetap tidak terdeteksi untuk jangka waktu yang lama. Dari total aktivitas APT di Indonesia tersebut, OceanLotus menjadi APT dengan jumlah aktivitas terbanyak di Indonesia dengan total 527.239 aktivitas, diikuti dengan APT Winnti dengan total 300.327 aktivitas dan APT Kimsuky dengan total 228.140 aktivitas. Tren aktivitas APT ini mengalami peningkatan signifikan pada tahun 2022, yaitu terdapat sebanyak 4.421.992 aktivitas APT di Indonesia. Peningkatan Tren aktivitas APT inilah yang memproyeksikan aktivitas APT menjadi salah satu ancaman siber yang akan dihadapi oleh Indonesia di Tahun 2023.



A.J. Darkholme

The weakest link in any chain of security is not the technology itself, but the person operating it.

Phishing

Phishing merupakan salah satu tipe serangan *social engineering* yang menargetkan pada kelemahan manusia dengan cara mengelabuhi korban. Serangan ini biasanya dilakukan menggunakan *e-mail*, SMS, atau telepon yang bersifat menarik perhatian korban sehingga korban akan terpancing untuk membuka, mengakses, atau menerima *e-mail*, SMS atau telepon tersebut yang bertujuan untuk perolehan informasi dari korban kepada penyerang. *Phishing* memanfaatkan kelemahan manusia untuk mendapatkan informasi rahasia seperti kredensial akun korban. Serangan *phishing* juga dapat menjadi inisiatör untuk serangan-serangan siber yang lain dengan cara seperti pendistribusian *malware* ke dalam sistem korban melalui *e-mail* atau tautan URL yang *malicious*. Serangan *phishing* semakin menjadi isu kritis semenjak adanya pandemi Covid-19. *Threat actor* memanfaatkan situasi pandemi untuk menyebarkan ketakutan dan menipu individu sehingga memberi penyerang akses ke informasi sensitif.



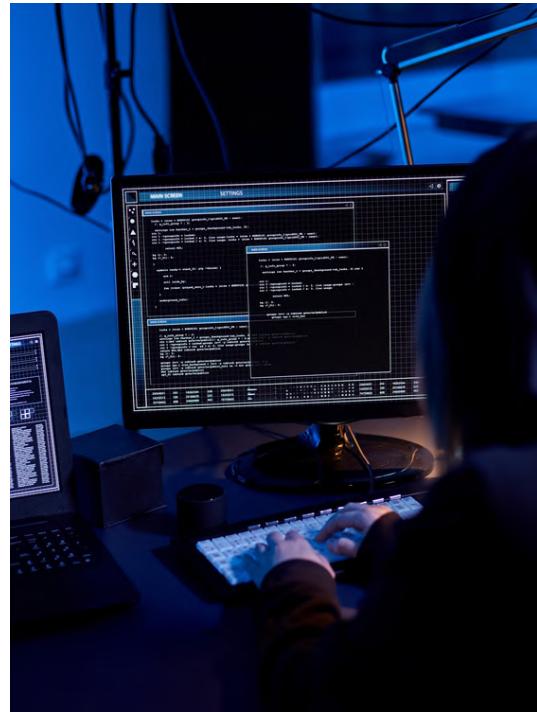
Cryptojacking

Cryptojacking adalah kejahatan dunia maya yang memanfaatkan sumber daya komputasi pihak lain secara ilegal untuk menambang mata uang kripto. *Cryptojacking* yang disebut juga *malicious cryptomining* memungkinkan peretas menambang mata uang digital tanpa membayar listrik, perangkat keras dan sumber daya lainnya untuk menambang mata uang digital. Jenis mata uang digital yang ditambang kebanyakan adalah Monero karena sulit untuk dilakukan pelacakan. Tren *cryptojacking* cenderung mengalami peningkatan berbanding lurus dengan meningkatnya nilai mata uang digital khususnya Bitcoin dan Monero. Serangan ini dapat menyerang ke semua sektor khususnya pada sektor Keuangan dan sektor Industri.



Serangan Remote Desktop Protocol (RDP)

RDP merupakan protokol komunikasi milik Microsoft yang memungkinkan perangkat yang menjalankan sistem operasi apapun untuk dapat terhubung secara jarak jauh. Selama beberapa tahun terakhir, terdapat serangan yang menyerang kerentanan dari RDP yang meningkat secara signifikan dengan threat actor mengeksplorasi port yang terbuka untuk memasang *ransomware* pada jaringan. Kontrol koneksi dari protokol RDP menggunakan port 3389. Port default ini digunakan untuk semua koneksi RDP yang menyediakan akses jaringan untuk pengguna jarak jauh melalui saluran terenkripsi. Peneliti Kaspersky melihat lonjakan besar pada pertengahan 2022 ketika serangan *brute-force* yang ditargetkan terhadap protokol RDP meningkat secara signifikan. Pada Februari 2022 terdapat 377,5 Juta serangan *brute-force* yang meningkat empat kali lipat dibandingkan tahun 2020. Serangan ini dapat mempengaruhi proses bisnis pada organisasi dari berbagai sektor.



Distributed Denial of Service (DDoS)

DDoS merupakan ancaman siber yang dapat melumpuhkan layanan suatu situs dengan mengirimkan permintaan dalam jumlah banyak. Selain jumlahnya, kecanggihan, kerumitan, dan durasi serangan DDoS juga semakin meningkat. Selain masalah kompleksitas dan sulitnya deteksi terhadap serangan DDoS, kekhawatiran terhadap lonjakan aktivitas serangan DDoS juga diakibatkan oleh tingginya angka pertumbuhan *Internet of Things* (IoT) di Indonesia. Tren pertumbuhan IoT tersebut perlu diiringi dengan penerapan keamanan yang mumpuni untuk pencegahan DDoS seperti penggunaan Anti DDos.

```
attack()

import socket, sys, os
print "[TARGET ATTACKING ADDRESS" + sys.argv[1]
print "injecting " + sys.argv[2];
def attack():
#pid = os.fork()
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((sys.argv[1], 80))
s.send("GET / HTTP/1.1\r\nHost: "+sys.argv[2]+"\r\n\r\n")
s.close()
```



Social Engineering

Social engineering merupakan serangan yang menggunakan manusia sebagai objek utama target serangan. Serangan ini dapat dilakukan dengan cara berkomunikasi dengan target secara langsung atau tidak langsung. Secara umum, tujuan dari serangan ini adalah untuk mendapatkan informasi tertentu dari target serangan. Namun, serangan ini juga dapat digunakan untuk mempengaruhi korban agar melaksanakan perintah dari penyerang. *Social engineering* sebenarnya berfokus pada manipulasi psikologis manusia dengan berbagai media yang bertujuan untuk mempengaruhi pikiran korban.

Artificial Intelligence (AI) dan IoT Cybercrime

AI dapat membawa keuntungan dan juga ancaman bagi dunia siber. Dengan peningkatan jenis perangkat IoT, AI diprediksi juga akan lebih banyak dimanfaatkan untuk melakukan kejahatan siber. AI dapat digunakan untuk mendeteksi perilaku IoT yang tidak biasa dan dapat dimanfaatkan untuk melakukan penipuan seperti *deepfake* (teknologi pertukaran wajah).



Edward Snowden

It is not data that is being exploited, it's people that are being exploited



Web Defacement

Web defacement merupakan suatu serangan pada website yang mengubah tampilan asli atau konten dari sebuah website. Pelaku serangan *web defacement* disebut sebagai defacer. *Web defacement* seringkali dimanfaatkan untuk menguji kemampuan defacer dan sebagai tindakan graffiti elektronik. Namun, *web defacement* akhir-akhir ini bukan hanya sebagai tindakan graffiti elektronik tetapi juga dapat dimanfaatkan untuk kepentingan agenda politik, karena dapat menurunkan reputasi atau kredibilitas dari pihak tertentu.

Serangan *web defacement* dapat dilakukan dengan memanfaatkan sebuah kelemahan dari sistem sehingga memungkinkan pelaku memiliki akses masuk hingga ke server dan memiliki kewenangan untuk mengganti atau menghapus konten suatu website. Terdapat berbagai metode untuk melakukan *web defacement*, tetapi cara yang paling umum digunakan adalah melalui *SQL Injection* yang memungkinkan akses administratif. Metode lain yang cukup efektif untuk digunakan adalah DDoS dan Port Scan.

Berdasarkan Laporan Tahunan Monitoring Kemanan Siber Tahun 2021, terdapat 5.940 kasus *web defacement* yang terjadi di Indonesia. Begitu pula pada tahun 2022, web defacement selalu masuk ke dalam tiga teratas insiden yang masuk dalam layanan BSSN, seperti pengiriman notifikasi insiden, Asistensi penanganan insiden siber, layanan *cyber threat intelligence*, dan layanan *digital forensic*. Hal tersebut memungkinkan adanya jumlah tinggi dari *web defacement* yang terjadi di tahun 2023.

Rekomendasi Menghadapi Ancaman Siber Tahun 2023

Dalam rangka upaya menghadapi prediksi ancaman siber pada tahun 2023, maka berikut disampaikan rekomendasi yang dapat dilakukan:

A Ancaman Ransomware

Langkah awal yang dapat dilakukan yaitu melakukan *backup data* secara berkala khususnya pada data yang memiliki nilai strategis. Langkah lengkapnya dapat dilihat pada dokumen di tautan berikut <https://cloud.bssn.go.id/s/T8mMqef6JoFx2MQ> <https://cloud.bssn.go.id/s/rtT5n4twbGLcaPW>

B Ancaman Kebocoran Data

Langkah awal yang dapat dilakukan untuk mencegah terjadinya insiden tersebut yaitu dengan melakukan pembatasan terhadap hak akses pengguna baik pada sistem maupun data. Panduan lengkap mengenai mitigasi ancaman kebocoran data dapat dilihat pada dokumen di tautan berikut (<https://cloud.bssn.go.id/s/QKwjMjj4rwoneJ9>).

C Ancaman APT

Langkah yang dapat dilakukan untuk mendeteksi ancaman tersebut diantaranya:

- Menerapkan sistem *monitoring* keamanan berupa IPS/IDS untuk memberikan *alert* jika ada indikasi aktivitas berbahaya.
- Melakukan pemantauan secara berkelanjutan terhadap aktivitas anomali pada jaringan maupun sistem.
- Melakukan pembarian terhadap aplikasi, sistem operasi dan *framework* yang digunakan pada sistem dan infrastruktur TI.
- Melakukan VA dan TSA secara berkala.

D Ancaman Phishing

Langkah awal yang dapat dilakukan untuk mencegah terjadinya insiden tersebut yaitu cermat dalam mengakses suatu *website* dan tidak mengakses tautan yang diberikan oleh pihak yang tidak dikenal. Panduan lengkap mengenai mitigasi ancaman *phishing* dapat dilihat pada dokumen di tautan berikut (<https://cloud.bssn.go.id/s/ewBFxn8g8jdBjDG>)



Ted Schlein

There are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don't know it.

E Ancaman *Cryptojacking*

Langkah awal yang dapat dilakukan untuk mencegah terjadinya insiden tersebut yaitu selalu melakukan *update* pada *database* anti *malware* dan melakukan pemindaian *malware* secara berkala. Panduan lengkap mengenai mitigasi ancaman *cryptojacking* yang memanfaatkan *malware* dapat dilihat pada dokumen di tautan berikut (<https://cloud.bssn.go.id/s/8K4EoNtrs3Ck3kq>)

F Ancaman DDoS

Langkah awal yang dapat dilakukan untuk mencegah terjadinya insiden tersebut yaitu mengontrol lalu lintas data dengan menghentikan dan membatasi koneksi atau proses yang tidak diinginkan pada server/router. Panduan lengkap mengenai mitigasi ancaman DDOS dapat dilihat pada dokumen di tautan berikut (<https://cloud.bssn.go.id/s/HNo4BmAppRix2e7>, <https://cloud.bssn.go.id/s/6ca8R2s2iiBQZrs>, <https://cloud.bssn.go.id/s/cYKeLwSHH3QNWP9>)

G Ancaman RDP

langkah awal yang dapat dilakukan untuk mencegah terjadinya insiden tersebut yaitu menonaktifkan layanan remote desktop apabila tidak diperlukan dan menutup port 3389. Panduan lengkap mengenai mitigasi ancaman RDP dapat dilihat pada dokumen di tautan berikut (https://bssn.go.id/wp-content/uploads/2019/05/imbauan_Layanan-Remote-Desktop.pdf).

H Ancaman *Social Engineering*

Langkah awal yang dapat dilakukan untuk mencegah terjadinya insiden tersebut yaitu meningkatkan kewaspadaan terhadap keamanan siber, tidak mudah tertipu oleh tawaran yang menggiurkan dari pihak yang belum dipastikan kebenarannya dan tidak memberikan informasi mengenai kredensial ke pihak siapapun. Panduan lengkap mengenai mitigasi ancaman *social engineering* dapat dilihat pada dokumen di tautan berikut (<https://bssn.go.id/wp-content/uploads/2019/05/Buku-Tips-BSSN-2019-tte.pdf>).

I Ancaman *Web Defacement*

Langkah awal yang dapat dilakukan untuk mencegah terjadinya insiden tersebut yaitu menerapkan secure development dalam membuat suatu website. Panduan lengkap mengenai mitigasi ancaman Web Defacement dapat dilihat pada dokumen di link berikut (<https://cloud.bssn.go.id/s/WrczsGWHKjpdPea>).



**BADAN SIBER
DAN SANDI
NEGARA**



Badan Siber dan Sandi Negara
Jl. Harsono R. M. No. 70,
Ragunan, Jakarta 12550



Whatsapp
+62 812-8135-4598



Telegram
t.me/id_SIRTII



Email
bantuan70@bssn.go.id