LANSKAP
KEAMANAN SIBER INDONESIA
2023

Id-SIRTII/CC – BSSN

Jalan Harsono RM No. 70 Ragunan.
Jakarta Selatan, 12550, Indonesia

TLP: CLEAR

LANSKAP
KEAMANAN SIBER INDONESIA
2023


Ingatlah bahwa kechilafan satu orang sahaja tjukup sudah menjebabkan keruntuhan negara.
dr. Roebiono Kertopati
Bapak Persandian Indonesia
BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

SAMBUTAN
KEPALA BADAN SIBER DAN SANDI NEGARA

LETJEN TNI (PURN)
HINSA SIBURIAN

Kepala Badan Siber dan
Sandi Negara

> *BSSN berkomitmen untuk mendorong gerakan 'Jaga Ruang Siber' dengan melibatkan masyarakat melalui berbagai kegiatan literasi digital.*

Pada tahun 2023, berbagai dinamika ruang siber global dan nasional yang melibatkan Teknologi Informasi dan Komunikasi (TIK) membuktikan bahwa keamanan siber semakin hari menjadi semakin krusial, tidak hanya berkaitan dengan isu pelindungan data pribadi dan informasi sensitif, tetapi juga berkaitan dengan upaya menjaga stabilitas ekosistem digital untuk memperoleh manfaat maksimal dari potensi ekonomi digital Indonesia.

BSSN sebagai garda terdepan dalam menghadapi ancaman di ruang siber, terus mengambil langkah-langkah strategis untuk memperkuat keamanan siber negara. Dalam hal ini, BSSN merumuskan kebijakan dan strategi keamanan yang adaptif sesuai dengan perkembangan teknologi dan ancaman siber yang semakin kompleks. Melalui upaya ini, BSSN berkomitmen untuk memberikan pemahaman yang lebih dalam kepada masyarakat mengenai pentingnya keamanan siber dalam kehidupan sehari-hari dan kemajuan negara.

Adapun Lanskap Keamanan Siber 2023 yang disajikan merupakan gambaran komprehensif tentang tantangan, tren, dan langkah-langkah pencegahan yang menjadi fokus utama BSSN. Dokumen ini tidak hanya mencerminkan kerja keras tim BSSN dalam menjaga keamanan siber, atau sekadar laporan tahunan. Dokumen ini adalah ajakan untuk bertindak bagi seluruh pemangku kepentingan untuk bersama-sama berpartisipasi aktif dan bertanggung jawab dalam menjaga integritas ruang siber Indonesia. Keamanan siber adalah tanggung jawab kita bersama.

Mari gunakan teknologi digital dengan cerdas dan bertanggung jawab. Jangan biarkan ruang siber menjadi arena kejahatan, melainkan menjadi jembatan kemajuan dan kolaborasi. Percayalah, dengan kesadaran dan kolaborasi bersama, kita dapat menciptakan ruang siber yang aman, tepercaya, dan berkembang.Semoga Lanskap Keamanan Siber 2023 ini memberikan panduan yang berharga, bahan evaluasi, dan sebagai pertimbangan utama untuk memprediksi dan mempersiapkan diri menghadapi ancaman siber di tahun 2024 dan seterusnya demi Indonesia yang kuat, aman, dan sejahtera. Mari jadikan tahun 2024 ini sebagai tahun kebangkitan kesadaran keamanan siber nasional.

Demikian yang dapat saya sampaikan, semoga Tuhan Yang Maha Kuasa senantiasa memberikan petunjuk, kesehatan, dan kekuatan kepada kita semua dalam menjalankan setiap tugas, sehingga fungsi dan kinerja BSSN dapat terus berjalan dengan baik.

SAMBUTAN

Deputi Bidang Operasi Keamanan Siber dan Sandi

MAYOR JENDERAL TNI DOMINGGUS PAKEL, S.Sos., M.M.S.I

Deputi Bidang Operasi
Keamanan Siber dan Sandi

> *Seiring perjalanan tahun 2023, ruang siber Indonesia menjadi target berbagai jenis ancaman siber. Dalam menghadapi tantangan ini, kami terus berupaya meningkatkan kompetensi dan mendorong inovasi di sektor teknologi keamanan siber.*

Selama tahun 2023, banyak peristiwa signifikan terjadi di ruang siber Indonesia yang menjadi perhatian utama bagi seluruh masyarakat. Sebagai instansi yang bertanggung jawab atas keamanan siber di Indonesia, BSSN memiliki peran sesuai Peraturan Presiden Nomor 53 Tahun 2017. Dalam peraturan presiden tersebut, Deputi Bidang Operasi Keamanan Siber dan Sandi (Deputi II) memiliki tugas utama yaitu menyusun dan melaksanakan kebijakan teknis di bidang operasi keamanan siber dan sandi. Deputi II telah aktif mengoordinasikan berbagai kegiatan operasi keamanan siber dan sandi, menjalin kerja sama dengan lembaga lain untuk meningkatkan efektivitas penyelenggaraan ruang siber yang aman. Deputi II juga terlibat dalam kegiatan nasional dan internasional, memberikan kontribusi dalam meningkatkan keamanan siber di Indonesia melalui koordinasi, perumusan, dan pelaksanaan kebijakan teknis di bidang operasi keamanan siber, operasi keamanan dan pengendalian informasi, serta operasi sandi.

Sebagai bagian dari tanggung jawab kami, Deputi II telah menyusun Lanskap Keamanan Siber Indonesia tahun 2023. Dokumen ini diharapkan dapat memberikan pandangan dan informasi terkait situasi keamanan ruang siber di Indonesia sepanjang tahun tersebut, sekaligus membangun kesadaran situasional melalui prediksi ancaman siber 2024 yang disajikan. Kami menyadari adanya kekurangan dan batasan yang perlu diperbaiki guna memperkuat keamanan siber nasional. Oleh karena itu, Deputi II terus berupaya meningkatkan kapabilitas untuk memperkuat pertahanan dan ketahanan siber serta sandi nasional.

Peran serta kontribusi yang proaktif dari berbagai sektor, termasuk institusi pemerintah, komunitas, dan masyarakat, memberikan dampak yang signifikan dalam menjaga kestabilan dan keamanan ruang siber Indonesia. Kami ingin menyampaikan apresiasi tinggi atas dukungan serta kerja sama yang telah diberikan kepada BSSN, terutama kepada Deputi II, dalam usaha bersama menjaga dan meningkatkan keamanan ruang siber. Semoga Lanskap Keamanan Siber Indonesia Tahun 2023 ini dapat meningkatkan kesadaran seluruh masyarakat Indonesia terhadap potensi ancaman siber yang dapat muncul di masa mendatang.

SAMBUTAN
Direktur Operasi Keamanan Siber

ANDI YUSUF, M.T.
Direktur Operasi Keamanan Siber

> *Marilah kita bersama-sama aktif berpartisipasi dan bekerja sama erat untuk melindungi ruang siber nasional dari berbagai potensi ancaman siber. Dengan bersatu padu, kita dapat menciptakan lingkungan siber yang aman dan dapat dipercaya bagi seluruh masyarakat.*

Marilah kita bersama-sama menyampaikan rasa syukur kepada Tuhan Yang Maha Esa atas berkat dan anugerah-Nya. Kehadiran Direktorat Operasi Keamanan Siber menjadi bagian yang signifikan mendukung BSSN dalam menjalankan tugasnya sesuai dengan mandat Presiden, sebagaimana tertera dalam Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 mengenai Badan Siber dan Sandi Negara.

Beragam ancaman siber telah terjadi di ruang siber Indonesia seiring dengan perjalanan tahun 2023. Dalam konteks ini, kami telah aktif melakukan upaya peningkatan kompetensi dan inovasi di bidang teknologi keamanan siber. Koordinasi, perumusan, dan pelaksanaan kebijakan teknis di sektor operasi keamanan siber telah kami jalankan sesuai dengan ketentuan Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara. Sebagai bentuk pertanggungjawaban, kami dengan penuh dedikasi menyusun Lanskap Keamanan Siber Indonesia Tahun 2023 yang memberikan gambaran rinci mengenai kondisi keamanan siber di Indonesia sepanjang tahun tersebut.

Melalui Lanskap Keamanan Siber Indonesia Tahun 2023, kami berharap dapat memberikan pemahaman yang lebih mendalam mengenai lanskap kondisi ruang siber Indonesia sepanjang tahun 2023. Informasi ini menjadi dasar yang penting untuk menentukan kebijakan strategis negara dan memberikan panduan bagi masyarakat dalam beraktivitas di ruang siber. Kami mengajak seluruh elemen masyarakat untuk terus berkolaborasi dan bersinergi dalam menjaga integritas ruang siber nasional dari berbagai ancaman siber.

Demikianlah sambutan ini, semoga kita senantiasa diberikan kekuatan oleh Tuhan Yang Maha Kuasa dalam menjalankan tugas pengabdian terbaik bagi bangsa dan negara. Terima kasih atas perhatian dan kerja sama yang telah diberikan.

LANSKAP KEAMANAN SIBER INDONESIA 2023

Oleh Direktorat Operasi Keamanan Siber

Dokumen Lanskap Keamanan Siber Indonesia 2023 merupakan kajian komprehensif di berbagai aspek penting dalam keamanan siber di Indonesia selama 2023. Dokumen ini memberikan wawasan dan membantu pemangku kepentingan dapat proaktif dalam membangun strategi pertahanan siber yang efektif.

DAFTAR ISI

RINGKASAN

Total trafik anomali di Indonesia selama tahun 2023 adalah **403.990.813 anomali** dengan jenis trafik anomali tertinggi yaitu ***Generic Trojan RAT*** yang mengindikasikan adanya aktivitas *backdoor communication* menuju domain *malicious* yang terindikasi sebagai *command and control server* milik *threat actor*. Terdapat **4.001.905 aktivitas *Advanced Persistent Threat* (APT)** dan **1.011.209 aktivitas *ransomware***. BSSN telah mengirimkan **1.762 notifikasi** indikasi insiden ke *stakeholder* dengan jenis notifikasi terbanyak dikirimkan adalah Anomali Trafik. Adapun pengelompokan sektor dilakukan berdasarkan Peraturan Presiden No. 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV). Berdasarkan hasil pemantauan dan analisis *Cyber Threat Intelligence*, BSSN juga melakukan penelusuran dugaan insiden siber dengan jumlah total **347 dugaan insiden siber** dengan jumlah jenis dugaan insiden tertinggi yaitu *Data Breach*. Hasil penelusuran pada *darknet*, ditemukan adanya **1.674.185 temuan *data exposure*** yang berdampak pada 429 *stakeholder* di Indonesia. Pada kasus *web defacement* ditemukan sebanyak **189 kasus** yang telah dinotifikasi oleh BSSN dengan klasifikasi kasus paling banyak adalah *web defacement* pada halaman tersembunyi (*hidden*). Berdasarkan laporan yang diterima dari *stakeholder* pada layanan aduan siber, diperoleh sebanyak **1.417 aduan** dengan kategori aduan terbanyak adalah ***Cybercrime*** sebanyak 86%.

BSSN telah mempublikasikan 66 imbauan keamanan terkait *Common Vulnerabilities and Exposures* (CVE) maupun potensi insiden lainnya pada website idsirtii. Salah satu Top CVE global berdasarkan skor *Common Vulnerability Scoring System* (CVSS) yang memiliki tingkat dampak *Critical* yaitu **CVE-2023-20198** yang memungkinkan *threat actor* dapat masuk dengan akses *user* untuk menjalankan perintah untuk membuat kombinasi *user* dan *password* lokal. Sedangkan, salah satu Top CVE nasional berdasarkan jumlah *hit* terbanyak di Indonesia yaitu **CVE-2022-22721** yang menyebabkan *buffer overflow* dengan ukuran *request body* yang sangat besar atau tak terbatas. Selain itu, berdasarkan pengujian kerentanan sistem elektronik melalui kegiatan *IT Security Assessment* (ITSA) yang dilakukan oleh BSSN ditemukan sebanyak **2.860 celah keamanan** pada **586 sistem elektronik**.

Jenis kerentanan tertinggi dengan tingkat risiko *Critical* adalah *Insecure Data Object Reference* (IDOR) yang memungkinkan *threat actor* dapat dengan mudah mengakses atau memodifikasi data tanpa memerlukan validasi atau otorisasi yang memadai.

BSSN telah melaksanakan **83 kegiatan asistensi** tanggap insiden siber di 74 *stakeholder*. Kategori pelaksanaan asistensi tanggap insiden siber yaitu proses asistensi dilakukan secara penuh oleh BSSN, proses asistensi dilakukan secara penuh oleh PSE/CSIRT, dan proses asistensi dilakukan oleh PSE/CSIRT bekerja sama dengan BSSN. Oleh karena itu, disusun *lesson learned* 3 (tiga) jenis kasus terbanyak berdasarkan asistensi tanggap insiden siber yaitu *Web Defacement*, *Ransomware*, dan *Data Breach*. Secara umum, dalam rangka mengantisipasi dan mencegah terjadinya insiden siber, maka langkah yang dapat dilakukan di antaranya *security hardening* pada sistem operasi server, pembaruan sistem dan perangkat lunak, menetapkan kebijakan penggunaan *password* yang kuat sesuai standar, edukasi *security awareness* kepada pengguna, dan lain-lain.

BSSN secara aktif melaksanakan pengamanan siber pada *event* nasional serta internasional di Indonesia dalam bentuk pengujian keamanan terhadap sistem elektronik, pemasangan perangkat deteksi keamanan siber yang berkolaborasi dengan *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. 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 Honeynet antara BSSN dengan Swiss-German University (SGU) dan Komunitas Indonesia Honeynet Project (IHP). Selain itu, BSSN juga melaksanakan kerjasama Laboratorium Forensik Digital untuk mendukung pelaksanaan forensik digital pada bidang insiden keamanan siber. Laboratorium Forensik Digital tersebut berhasil meraih Sertifikat Akreditasi ISO/IEC 17025:2017 pada tahun 2023. Berdasarkan analisis BSSN diperoleh beberapa potensi ancaman siber yang diprediksi akan muncul di tahun 2024. Ancaman siber tersebut meliputi *Web Defacement*, *Ransomware*, *Cyber Threats Based Artificial Intelligence* (AI), *Internet of Things* (IoT) *Attack*, *Advanced Persistent Threat* (APT), *Phishing*, dan *Distributed Denial of Service* (DDoS).

PROFIL
DIREKTORAT OPERASI KEAMANAN SIBER

BADAN SIBER DAN SANDI NEGARA

Berdasarkan Peraturan Presiden Nomor 53 Tahun 2017

Badan Siber dan Sandi Negara (BSSN) merupakan hasil dari penggabungan beberapa entitas pemerintah sebelumnya, antara lain Lembaga Sandi Negara (Lemsaneg), Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika (Kemenkominfo), serta Indonesia *Security Incident Response Team on Internet Infrastructure* (Id-SIRTII). Proses penggabungan ini diwujudkan melalui Peraturan Presiden Nomor 53 tahun 2017 tentang BSSN.

DIREKTORAT OPERASI KEAMANAN SIBER

Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021

Presiden Republik Indonesia, Joko Widodo, menandatangani Peraturan Presiden (Perpres) Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (BSSN) pada tanggal 13 April 2021. Penerbitan Perpres ini didasarkan pada kebutuhan untuk merancang kembali struktur organisasi BSSN, dengan tujuan mencapai keamanan, perlindungan, dan kedaulatan siber nasional. Selanjutnya, organisasi dan tata kerja BSSN dijelaskan lebih lanjut dalam Peraturan BSSN Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja BSSN.

Direktorat Operasi Keamanan Siber merupakan bagian dari Deputi Bidang Operasi Keamanan Siber dan Sandi di lingkungan Badan Siber dan Sandi Negara. Direktorat Operasi Keamanan Siber bertanggung jawab untuk melakukan koordinasi, merumuskan, dan melaksanakan kebijakan teknis di sektor operasi keamanan siber. Direktorat Operasi Keamanan Siber melaksanakan fungsi-fungsi berikut:

- Penyiapan perumusan kebijakan teknis operasional di bidang identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan
- Penyelenggaraan koordinasi dan implementasi identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan
- Pengelolaan tanggap insiden siber nasional dan sektor pemerintah, kontak siber nasional, serta pengelolaan krisis siber nasional
- Pengelolaan informasi mengenai ancaman siber secara proaktif dan analisis big data serta analisis malware
- Pendukung penyidikan, forensik digital, dan memberikan bantuan sebagai ahli dalam kasus keamanan siber
- Pelaksanaan pemantauan, evaluasi, dan pelaporan di bidang operasi keamanan siber
- Pelaksanaan urusan perencanaan, keuangan, rumah tangga, kepegawaian, ketatalaksanaan, persuratan, kearsipan, serta penyusunan evaluasi dan pelaporan.

Cybersecurity is a shared responsibility. We all have a role to play in protecting ourselves and our systems.

- Chris Krebs

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

TREN TRAFIK ANOMALI 2023

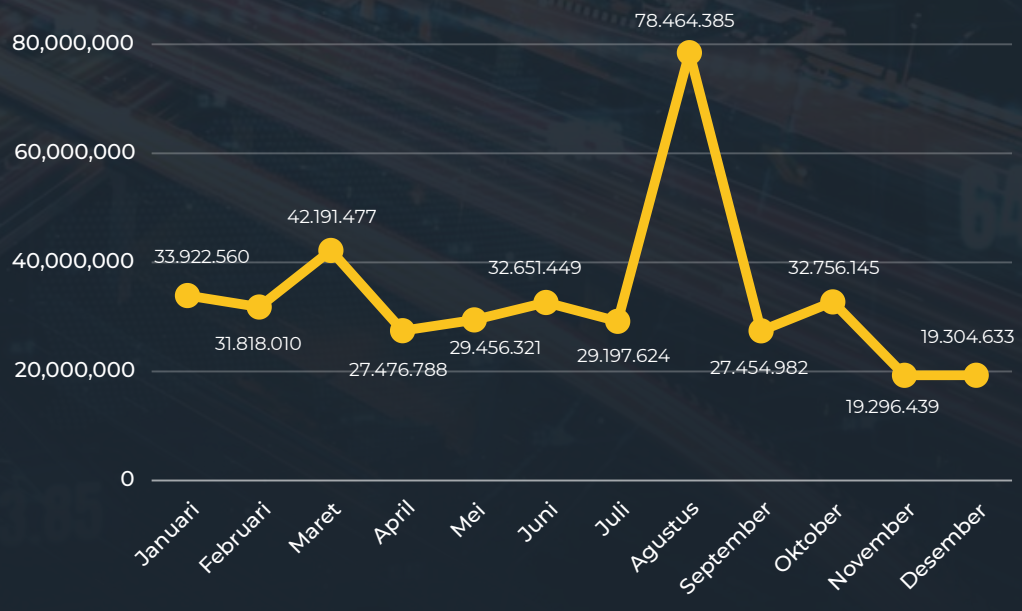
1

TRAFIK ANOMALI SERANGAN SIBER DI INDONESIA

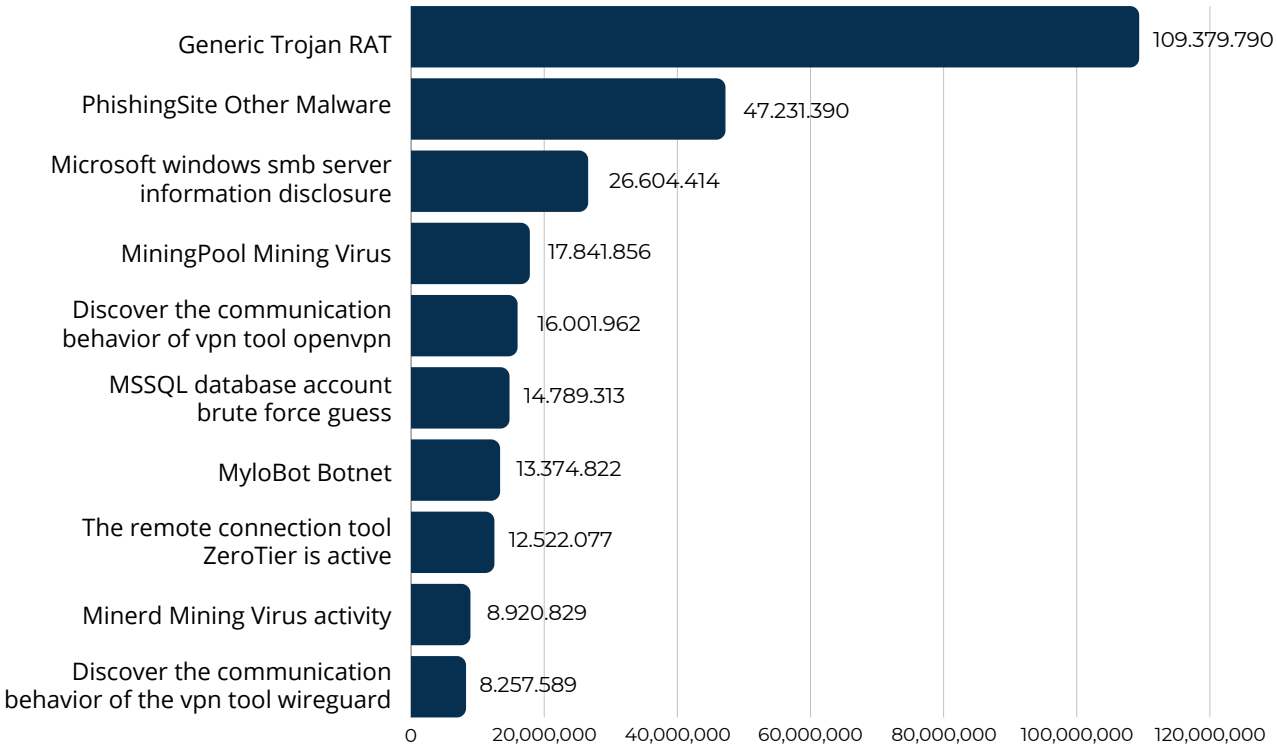
403.990.813

Total Trafik Anomali

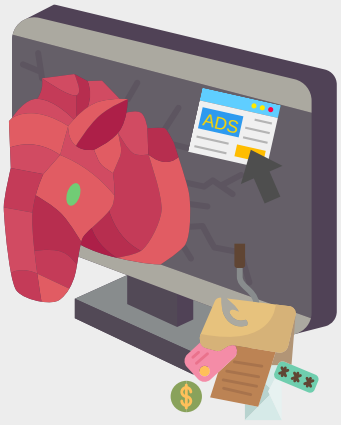
Total trafik anomali di Indonesia selama tahun 2023 adalah **403.990.813 anomali**. Anomali trafik tertinggi terjadi pada bulan Agustus dengan jumlah 78.464.385 anomali, sedangkan anomali terendah terjadi pada bulan November dengan jumlah 19.296.439 anomali. Aktivitas anomali trafik ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi. Berikut merupakan grafik trafik anomali periode Januari - Desember 2023:



TOP 10 TRAFIK ANOMALI

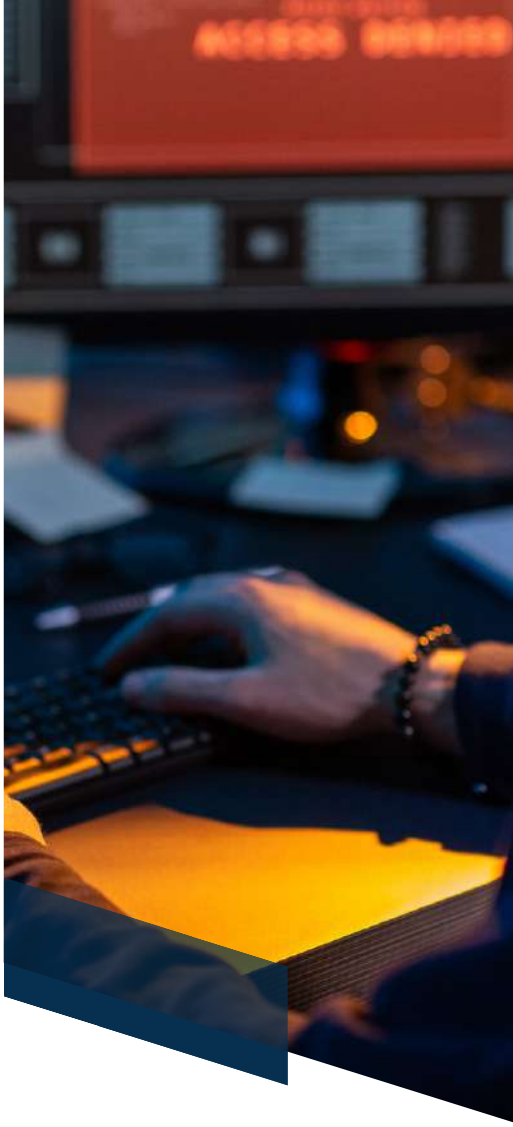


01 GENERIC TROJAN RAT



Generic Trojan RAT adalah *signature* yang mengindikasikan adanya aktivitas *backdoor communication* menuju domain *malicious* yang terindikasi sebagai *command and control server* milik *threat actor*. Aktivitas ini berpotensi digunakan untuk melakukan berbagai kegiatan mencurigakan seperti pencurian informasi, penghapusan data, pemblokiran, penyalinan informasi, serta menjalankan program pada perangkat yang terinfeksi di luar kehendak pengguna. Generic Trojan RAT menargetkan komputer dengan sistem operasi Windows dan dapat menyebar melalui tautan pada e-mail, tautan pada pesan singkat, pengunduhan melalui *drive*, ataupun dibawa oleh *malware* yang lebih dahulu menginfeksi perangkat. Perangkat yang terinfeksi Generic Trojan RAT akan menjalankan program pada *background process* tanpa diketahui oleh pengguna. Hal ini dapat berdampak pada pelambatan kinerja sistem, pengubahan konfigurasi, dan perangkat akan lebih sering menampilkan pesan *error*. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk melakukan pembaruan sistem operasi dan semua perangkat lunak yang diinstal, menggunakan perangkat antivirus yang selalu diperbarui secara berkala, menggunakan aplikasi asli yang diunduh dari sumber resmi, serta selalu berhati-hati saat membuka lampiran atau menerima *file* dan saat mengklik tautan dari suatu halaman situs web.

02 PHISHINGSITE OTHER MALWARE



PhishingSite merupakan salah satu aktivitas infeksi *malware* yang dilakukan dengan memanfaatkan situs *phishing*. Situs *phishing* merupakan situs web palsu yang diciptakan untuk menipu pengguna agar memberikan informasi pribadi, seperti password atau rincian keuangan. Situs palsu ini sering kali menggunakan tautan yang didistribusikan melalui *e-mail phising* yang tampak meyakinkan. PhishingSite meningkatkan risiko keamanan dengan menggabungkan serangan *phishing,* potensi pengunduhan, dan instalasi *malware* pada perangkat korban. Pihak-pihak yang ditargetkan adalah individu, perusahaan, dan organisasi yang tidak waspada terhadap ancaman siber yang dapat mengekspos data sensitif dan merusak integritas sistem. Dampak dari PhishingSite Other Malware adalah pencurian identitas, akses ilegal ke akun korban, pencurian informasi akun keuangan, dan potensi kerusakan pada perangkat atau jaringan yang terinfeksi *malware*. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk tidak sembarang mengklik tautan dari *e-mail* yang mencurigakan, selalu melakukan verifikasi keaslian situs web sebelum memasukkan informasi sensitif, dan melakukan pembaruan perangkat antivirus secara berkala.

03 MICROSOFT WINDOWS SMB SERVER INFORMATION DISCLOSURE

Trafik anomali ini berkaitan dengan pendeteksian penggunaan komponen SMBv1 pada Microsoft Windows SMB (*Server Message Block*) *Server*. SMB adalah protokol jaringan yang digunakan untuk berbagi file, pencetakan, dan komunikasi antar perangkat dalam suatu jaringan. Dalam hal ini, SMBv1 merupakan versi SMB yang *obsolete* dan memiliki kerentanan yang dapat menyebabkan pengungkapan informasi sensitif akibat kesalahan pemrosesan *request*, sehingga mengakibatkan *threat actor* dapat memperoleh akses ke informasi sensitif yang disimpan atau ditransmisikan dengan mengirimkan paket tertentu (*crafted packet*). Informasi sensitif ini dapat berupa data pengguna, struktur direktori, hingga rincian sistem operasi yang dapat digunakan untuk merencanakan serangan lebih lanjut. Kerentanan ini dapat dieksploitasi oleh *malware* yang menggunakan modul EternalBlue, diantaranya WannaCry, Trickbot, CoinMiner, dan WannaMine. Modul EternalBlue memungkinkan *malware* mengeksploitasi kerentanan CVE-2017-0147, menyebar di jaringan korban, menginfeksi semua perangkat yang terhubung dengan jaringan, dan menanamkan *payload crypto-ransomware*. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk melakukan pembaruan terhadap sistem operasi Microsoft Windows, menonaktifkan SMBv1 dan menggunakan SMB versi terbaru, menyesuaikan *Group Policy Objects* untuk membuat Windows *Firewall* membatasi koneksi SMB yang masuk ke sistem pengguna, mengaktifkan enkripsi pada komunikasi SMB untuk melindungi data yang ditransmisikan, serta menerapkan pembatasan otorisasi dari setiap sistem, layanan, dan perangkat lunak yang berjalan menggunakan *non-privileged user*.

04 MININGPOOL MINING VIRUS

MiningPool Mining Virus atau yang juga dikenal sebagai *crypto mining malware* adalah jenis *malware* yang menggunakan sumber daya komputer korban untuk melakukan penambang mata uang kripto. *Threat actor* biasanya menyebarkan *malware* ini melalui teknik seperti *phishing* atau melalui situs web yang telah dikendalikan oleh *threat actor*. Aktivitas MiningPool mengakibatkan adanya peningkatan penggunaan sumber daya komputasi untuk melakukan proses *mining* tanpa adanya otorisasi dari pemilik perangkat. Hal ini mengakibatkan perangkat korban akan mengalami penurunan daya, memori, penurunan kinerja operasional perangkat, dan dalam beberapa kasus dapat merusak perangkat keras korban. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk menonaktifkan layanan yang tidak digunakan, menerapkan *two-factor authentication* pada layanan yang digunakan, melakukan pembaruan antivirus serta sistem operasi secara berkala, menghindari mengunduh maupun membuka *e-mail* dari alamat pengirim yang tidak dikenal, dan selalu menggunakan aplikasi asli yang diunduh dari sumber resmi.

05 DISCOVER THE COMMUNICATION BEHAVIOR OF VPN TOOL OPENVPN

Trafik anomali ini berkaitan dengan pendeteksian penggunaan protokol *Virtual Private Network* (VPN) pada aplikasi OpenVPN. OpenVPN merupakan aplikasi berbasis *open-source* yang menggunakan protokol VPN untuk menciptakan *private tunnel* terenkripsi untuk terhubung ke internet. OpenVPN akan membuat koneksi dengan menggunakan *Point to Point* (PTP) *Tunnel* yang telah dienkripsi menggunakan *username* dan *password*. Aplikasi ini sebenarnya legal, namun saat ini *threat actor* dapat menyisipkan *malware* ke dalam aplikasi OpenVPN dan memanfaatkannya untuk melakukan spionase pada perangkat korban. Selain itu, node pada jaringan publik yang digunakan sebagai relay agent VPN seringkali merupakan Alamat IP yang memiliki reputasi buruk. Sebagai bentuk upaya pencegahan, pengguna diharapkan dapat melakukan pemantauan aktif terhadap lalu lintas jaringan OpenVPN, melakukan konfigurasi *firewall* yang baik dan *logging* yang intensif, menerapkan kebijakan otorisasi pengguna yang ketat, melakukan segmentasi jaringan serta audit keamanan secara rutin, dan menggunakan aplikasi OpenVPN versi terbaru yang diunduh dari sumber resmi.

06 MSSQL DATABASE ACCOUNT BRUTE FORCE GUESS

MSSQL *Database Account Brute Force Guess* merujuk pada ancaman siber yang menargetkan keamanan basis data. Serangan ini merambah jaringan dengan mencoba berbagai kombinasi password secara acak untuk mendapatkan akses ke akun basis data MSSQL. Dalam serangan ini, mengirimkan banyak permintaan *login* ke *server* dengan berbagai kombinasi password, dengan harapan menemukan kombinasi yang benar. Apabila percobaan yang dilakukan berhasil, serangan ini dapat membuka pintu bagi untuk mengakses, mengubah, bahkan melakukan pencurian data berharga pada basis data untuk melakukan berbagai aktivitas berbahaya, seperti melakukan instalasi perangkat lunak berbahaya atau merusak data. Sebagai bentuk upaya pencegahan, pengguna diharapkan dapat menerapkan kebijakan keamanan password yang kuat, mengkonfigurasi penguncian otomatis pada akun setelah beberapa kali percobaan *login* yang gagal, menggunakan layanan VPN untuk mengakses basis data, dan melakukan pembaruan rutin untuk melindungi integritas serta kerahasiaan data yang disimpan dalam basis data.

07 MYLOBOT BOTNET

Mylobot Botnet adalah salah satu jenis *botnet* yang menargetkan sistem operasi Windows. *Botnet* ini menyebar melalui spam *e-mail* ataupun unduhan file yang telah terinfeksi, dan memiliki kemampuan sebagai gerbang untuk mengunduh muatan (*payload*) tambahan dari *server Command and Control* (C2) dan menginstalnya pada perangkat korban. Setelah terinstal pada perangkat korban, *botnet* akan menonaktifkan Windows Defender dan Windows Update sehingga memungkinkan untuk mengambil kendali penuh atas sistem pengguna. Perilaku umum MyloBot adalah melakukan *callback* ke sejumlah domain yang dihasilkan oleh *Domain Generation Algorithm* (DGA). DGA menjadi salah satu metode yang digunakan untuk mempersulit kegiatan deteksi terhadap aktivitas *malware* karena dapat menghasilkan nama domain yang variatif dengan karakteristik dan pola penamaan yang acak dalam jumlah besar. Mylobot juga memiliki teknik anti-VM dan anti-*sandboxing* yang canggih untuk menghindari deteksi dari proses analisis. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk melakukan update sistem dan antivirus yang digunakan secara berkala, melakukan pencadangan data secara berkala, menggunakan password yang kuat, menghindari akses terhadap situs web atau domain yang tidak terpercaya, dan menghindari mengunduh serta membuka *e-mail* dari alamat pengirim yang tidak dikenal.

08 THE REMOTE CONNECTION TOOL ZEROTIER IS ACTIVE

Peringatan ini merujuk pada aktivitas penggunaan *tool remote connection* ZeroTier pada sistem atau jaringan. ZeroTier adalah salah satu solusi VPN berjenis *mesh* yang memungkinkan pengguna untuk membuat jaringan pribadi virtual (VPN) secara instan dan aman melalui internet. Dalam konteks keamanan siber, ZeroTier yang aktif dalam kondisi tidak dikenali oleh *administrator* sistem dapat menjadi indikasi adanya aktivitas mencurigakan atau potensi ancaman, misalnya mungkin telah menginstal ZeroTier pada sistem tanpa sepengetahuan pengguna untuk mendapatkan akses jarak jauh. Sebagai bentuk upaya pencegahan, pengguna disarankan mengimplementasikan pemantauan aktif terhadap aktivitas jaringan terkait ZeroTier, melakukan konfigurasi *firewall* sesuai dengan standar keamanan, mengaktifkan *logging* yang rinci, melakukan segmentasi jaringan, menggunakan ZeroTier dengan menerapkan mekanisme autentikasi yang kuat dan terbatas hanya kepada pengguna yang membutuhkan akses jarak jauh, serta melakukan pembaruan perangkat lunak secara rutin.

09 MINERD MINING VIRUS

Minerd *Mining Virus* adalah jenis *malware* yang dirancang khusus untuk melakukan penambangan mata uang kripto (*cryptocurrency*). Virus ini menggunakan sumber daya komputasi pada sistem yang terinfeksi untuk melakukan operasi penambangan mata uang kripto seperti Bitcoin, Litecoin, atau jenis mata uang digital lainnya. Minerd biasanya disebarkan menggunakan teknik *phishing* atau melalui situs web yang telah dikendalikan oleh . Keberadaan Minerd *Mining Virus* pada suatu sistem dapat menyebabkan penurunan kinerja sistem, peningkatan penggunaan daya listrik yang signifikan, pemanasan berlebih pada perangkat, hingga perusakan perangkat keras. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk melakukan pembaruan antivirus secara teratur, mengkonfigurasi *firewall* untuk membatasi dan memonitor lalu lintas terkait dengan penambangan ilegal, menyelidiki proses-proses mencurigakan yang berjalan di sistem, menghindari penggunaan ekstensi *browser* (*plugin*) yang tidak dikenal, dan memastikan pemutakhiran *firmware* perangkat keras secara teratur.

10 DISCOVER THE COMMUNICATION BEHAVIOR OF THE VPN TOOL WIREGUARD

Wireguard merupakan salah satu *tool* VPN yang digunakan untuk membuat komunikasi secara *private* antara 2 (dua) *endpoint* yang terhubung melalui suatu jaringan secara cepat dan efisien. Namun, terdapat beberapa kerentanan yang ditemukan dalam Wireguard, salah satunya adalah kerentanan CVE-2023-35838 yang merujuk pada kerentanan dimana klien Wireguard 0.5.3 pada Windows mengkonfigurasi sistem operasi dan *firewall* dengan cara yang tidak aman sehingga lalu lintas ke jaringan lokal yang menggunakan alamat IP non-RFC1918 diblokir. Hal ini memungkinkan untuk memanipulasi korban agar memblokir lalu lintas IP ke alamat IP dan layanan tertentu bahkan saat VPN diaktifkan. Kerentanan lain yang ditemukan adalah CVE-2019-14899 yang memungkinkan *threat actor* untuk mengendalikan tautan pada layer 2 (*data link layer*) dan mengirim paket khusus ke perangkat korban untuk secara aktif memeriksa beberapa properti dari koneksi TCP yang berasal dari perangkat korban. Perlu diperhatikan bahwa terdeteksinya penggunaan Wireguard tidak secara otomatis mengindikasikan adanya ancaman, karena banyak organisasi dan individu menggunakan Wireguard untuk tujuan yang sah, seperti akses jarak jauh ke *server* atau jaringan. Oleh karena itu, penting untuk memahami konteks dan konfigurasi spesifik sistem atau jaringan sebelum menentukan apakah aktivitas ini merupakan ancaman. Sebagai bentuk upaya pencegahan, pengguna disarankan melakukan konfigurasi pada *firewall* untuk mengontrol lalu lintas dan menerapkan enkripsi yang kuat pada protokol Wireguard, melakukan pemantauan aktif terhadap lalu lintas jaringan, melakukan audit konfigurasi secara berkala, menerapkan autentikasi ganda untuk lapisan keamanan tambahan, melakukan pembaruan perangkat lunak secara rutin, mengaktifkan *logging* yang rinci, dan menerapkan segmentasi jaringan.

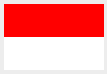
TOP 10

NEGARA SUMBER DAN TUJUAN

Berdasarkan hasil deteksi trafik anomali, didapatkan alamat IP sumber dan tujuan anomali yang 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 *threat actor* berpotensi menggunakan alamat IP tersebut sebagai *proxy* untuk menyembunyikan atau menyamarkan alamat IP asli *threat actor*.

TOP 10 SUMBER ANOMALI


Indonesia
124.644.606

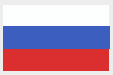

Amerika Serikat
38.737.813


Singapura
16.774.825


Jerman
12.479.179


Belanda
12.177.039


Prancis
8.908.443


Rusia
5.173.928


Tiongkok
5.052.417


Republik Moldova
4.507.275


Republik Ceko
3.352.355

TOP 10 TUJUAN ANOMALI


Indonesia
208.612.734


Amerika Serikat
44.262.119


Jerman
12.617.940


Belanda
9.209.270

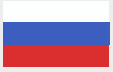

Prancis
9.160.106


Singapura
6.277.960


Kanada
3.314.935


Tiongkok
2.791.992


Australia
2.663.807

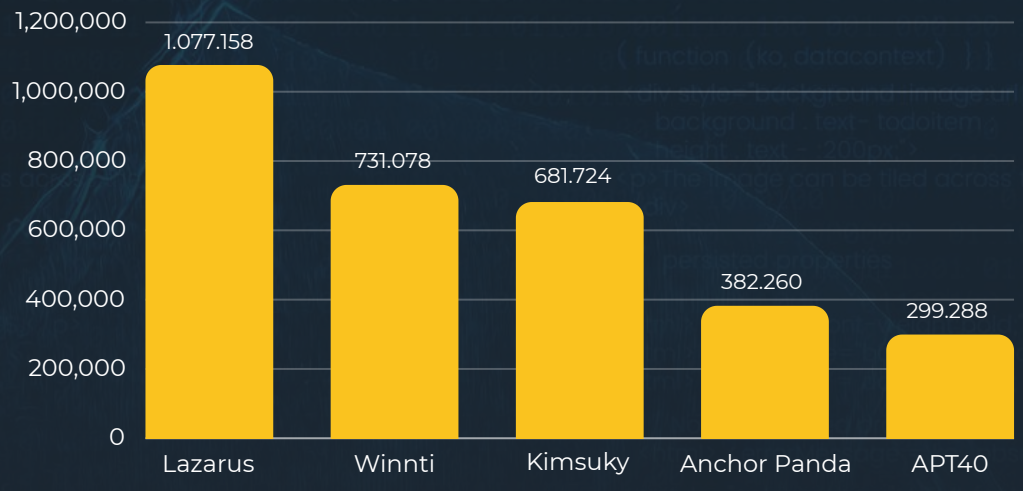

Rusia
2.325.632

AKTIVITAS *ADVANCED PERSISTENT THREAT*

4.001.905

Aktivitas APT di Indonesia Tahun 2023

Advanced Persistent Threat (APT) merupakan *attack campaign* yang dilakukan oleh kelompok serangan siber atau *threat actor* yang memiliki keterkaitan (*state-sponsored*) ataupun tidak berkaitan (*non-state sponsored*) dengan negara tertentu. *Threat actor* ini menggunakan berbagai metode dan teknik canggih yang dirancang untuk melakukan serangan siber secara terus-menerus tanpa terdeteksi perangkat keamanan untuk mendapatkan akses ke sistem dan bertahan dalam sistem tersebut dalam jangka waktu yang lama. Tujuan kelompok serangan siber ini adalah mengakses, memantau, dan mengumpulkan informasi dari sistem atau jaringan target untuk melakukan pencurian data yang bernilai seperti informasi rahasia perusahaan, data keuangan, atau rancangan teknologi tinggi dengan tujuan eksploitasi jangka panjang. Berikut grafik 5 APT yang paling banyak ditemukan pada ruang siber Indonesia:



TOP 5
ADVANCED PERSISTENT THREAT

01

Lazarus

Lazarus juga dikenal sebagai Hidden Cobra atau Labyrinth Chollima, merupakan kelompok serangan siber yang diindikasikan berelasi dengan Korea Utara. Kelompok ini memiliki tujuan untuk melakukan pencurian data dan informasi bernilai tinggi, motif finansial, spionase, sabotase, dan ancaman terhadap stabilitas keamanan dan politik. Keterlibatan pemerintah Korea Utara menambah dimensi geopolitik pada aktivitas Lazarus. Kelompok ini tidak hanya menargetkan sektor keuangan, lembaga pemerintah, dan industri, tetapi juga melakukan operasi serangan besar yang mencakup peretasan bank dan pencurian mata uang kripto.

02

Winnti

Winnti juga dikenal sebagai Blackfly atau Wicked Panda, merupakan kelompok serangan siber yang diindikasikan berelasi dengan Tiongkok. Kelompok ini diketahui aktif sejak tahun 2010 dan memiliki tujuan untuk melakukan pencurian informasi dan spionase. Winnti diketahui terlibat dalam operasi siber yang kompleks dan berfokus pada sektor industri dan lembaga pemerintah, dengan menggunakan metode serangan canggih, termasuk eksploitasi perangkat lunak dan kampanye *spear-phishing*. Kelompok ini terlibat dalam pencurian data rahasia, terutama terkait kekayaan intelektual dan informasi industri, serta terlibat dalam serangan terhadap penyedia perangkat lunak dan pemasaran digital. Selain pencurian data, Winnti juga terlibat dalam serangan yang merusak dan pemalsuan sertifikat digital. Ancaman yang ditimbulkan oleh APT Winnti melibatkan risiko pencurian data bisnis, potensi kerugian finansial, ancaman terhadap keberlanjutan operasional, dan dampak jangka panjang pada keamanan siber global.

03

Kimsuky

Kimsuky juga dikenal sebagai Thallium, Black Banshee, atau Velvet Chollima, merupakan kelompok serangan siber yang diindikasikan berelasi dengan Korea Utara berdasarkan ditemukannya *string* dengan bahasa Korea pada *malware* yang digunakan dalam *campaign* ini. Kelompok ini memiliki tujuan untuk melakukan pencurian informasi maupun spionase, serta terlibat dalam berbagai kampanye serangan dengan target sektor pemerintah, militer, dan lembaga penelitian di berbagai negara. APT Kimsuky dikenal menggunakan metode serangan seperti *spear-phishing*, *malware* yang dikustomisasi, dan eksploitasi kerentanan perangkat lunak untuk mendapatkan akses yang tidak sah. Kimsuky memiliki kecenderungan untuk mengincar informasi rahasia terkait kebijakan dan keamanan nasional. Ancaman dari APT Kimsuky mencakup risiko pencurian data yang signifikan, pelanggaran keamanan nasional, potensi kerugian berat bagi entitas yang ditargetkan, dan potensi dampak serius terhadap kestabilan keamanan global.

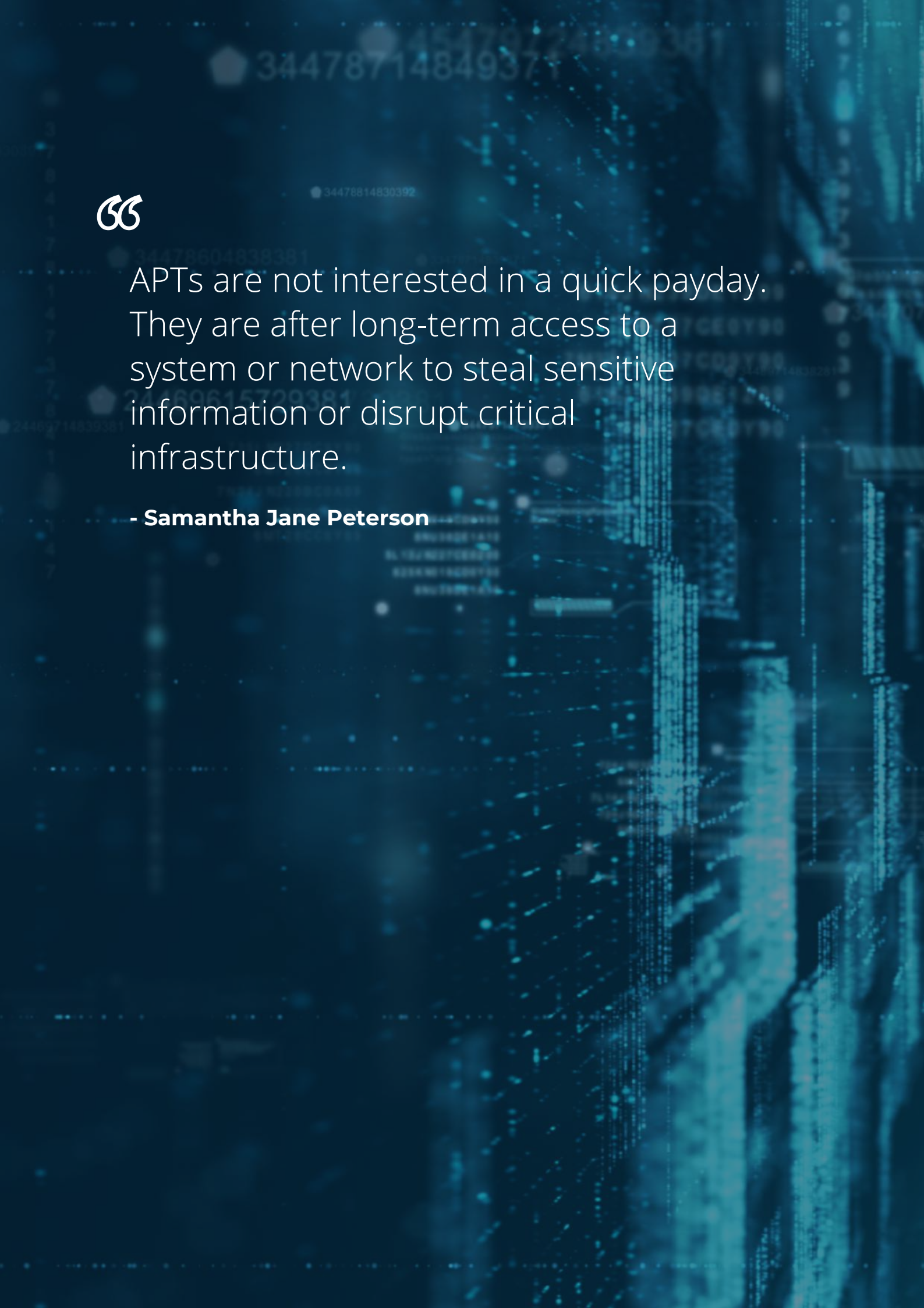
04 Anchor Panda

Anchor Panda juga dikenal sebagai APT 14, merupakan kelompok serangan siber yang diindikasikan berelasi dengan Tiongkok. Kelompok ini diketahui aktif sejak tahun 2012 dan dikenal dengan keterlibatannya dalam aktivitas serangan yang terkoordinasi dan bertarget tinggi. Anchor Panda menargetkan entitas maritim dan kelautan, membawa dampak signifikan pada industri pelayaran, pembangkit listrik, dan teknologi kelautan. Modus operandi kelompok ini melibatkan penggunaan teknik serangan canggih, seperti *spear-phishing*, eksploitasi kerentanan perangkat lunak, dan penggunaan *malware* khusus yang dirancang untuk menyusup dan bertahan dalam jangka waktu yang panjang. *Malware* yang digunakan oleh Anchor Panda antara lain Gh0st RAT, Poison Ivy, dan Torn RAT. Anchor Panda dikenal karena tujuannya yang berkaitan dengan intelijen dan ekonomi. Ancaman dari APT Anchor Panda tidak hanya mencakup risiko pencurian data sensitif, tetapi juga spionase industri yang dapat mengguncang fondasi teknologi dan ekonomi, serta risiko kerahasiaan nasional.

05 APT40

APT 40 juga dikenal sebagai Leviathan, Bronze Mohawk, TA423, atau Red Ladon, merupakan kelompok serangan siber yang diindikasikan berelasi dengan Tiongkok. Kelompok ini diketahui mulai aktif beroperasi sejak tahun 2009 dengan operasi yang terfokus pada pengumpulan intelijen dan spionase di sektor maritim, industri pelayaran, pembangkit listrik, dan teknologi kelautan. Ancaman dari APT40 mencakup risiko pencurian data sensitif, kerahasiaan teknologi, dan potensi dampak terhadap keamanan nasional. Ancaman yang dibawa oleh APT40 tidak hanya merinci ancaman pencurian data dalam sektor pelayaran dan energi, tetapi juga membawa nuansa spionase industri yang dapat merusak stabilitas keamanan nasional. APT40 menggunakan berbagai teknik serangan, termasuk *spear-phishing*, eksploitasi kerentanan perangkat lunak, dan penggunaan *malware* khusus untuk menyusup dan memantau jaringan target.

Pencegahan dampak aktivitas APT memerlukan pendekatan keamanan yang komprehensif, termasuk penguatan keamanan jaringan, pemantauan proaktif terhadap aktivitas jaringan yang mencurigakan, pembaruan perangkat keamanan secara berkala, peningkatan kerjasama internasional untuk menghadapi ancaman siber, penguatan keamanan di berbagai sektor khususnya pada sektor yang ditargetkan, serta peningkatan kesadaran keamanan siber bagi pengguna untuk mendeteksi dan mengidentifikasi teknik serangan dan memitigasi risiko serangan siber yang kompleks dari kelompok ini.



APTs are not interested in a quick payday. They are after long-term access to a system or network to steal sensitive information or disrupt critical infrastructure.

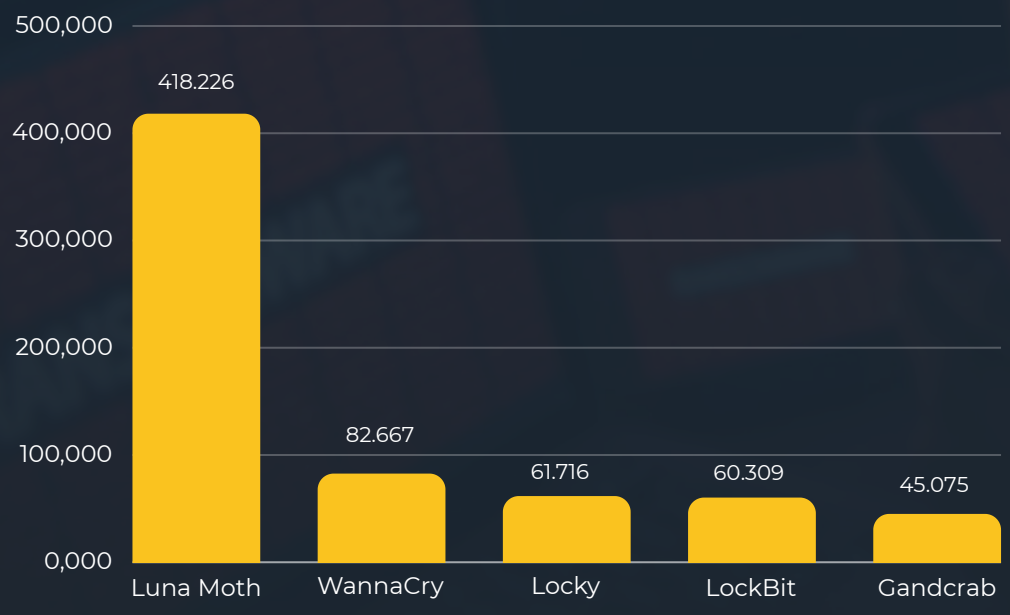
- Samantha Jane Peterson

AKTIVITAS *RANSOMWARE*

1.011.209

Aktivitas *Ransomware*

Ransomware adalah jenis *malware* yang digunakan untuk menyandera aset korban, seperti dokumen, sistem, ataupun perangkat. Setelah aset terenkripsi, korban akan diminta membayar tebusan untuk mendekripsi dan kembali mendapatkan akses pada aset. *Ransomware* menargetkan individu, perusahaan, organisasi, bahkan Pemerintah. Dampak *ransomware* dapat berupa kehilangan akses terhadap data, kerugian finansial, hingga penurunan reputasi. Berikut adalah 5 *Ransomware* yang paling banyak ditemukan pada ruang siber Indonesia berdasarkan hasil monitoring trafik anomali:



TOP 5 RANSOMWARE

01 Luna Moth

Luna Moth juga dikenal sebagai *Silent Ransom Group*. Berbeda dari *ransomware* pada umumnya, Luna Moth tidak menggunakan enkripsi data untuk memeras korban. *Ransomware* ini memiliki fokus pada pencurian data perusahaan melalui kampanye *call-back phishing*, dan menggunakan umpan seperti tagihan palsu layanan langganan untuk menyusup ke perangkat korban. Data sensitif yang dicuri kemudian digunakan untuk memeras dan menuntut tebusan dalam jumlah besar.

02 WannaCry

WannaCry adalah *ransomware* yang pertama kali terdeteksi pada Mei 2017. *Ransomware* ini beroperasi dengan melakukan enkripsi data pada perangkat yang menggunakan sistem operasi Windows, kemudian meminta tebusan dalam bentuk Bitcoin. WannaCry memanfaatkan kerentanan keamanan EternalBlue untuk menyebar dengan cepat di jaringan.

03 Locky

Locky adalah *ransomware* yang disebarkan melalui email *phishing* dengan tujuan untuk melakukan infeksi terhadap komputer, melakukan enkripsi file, dan meminta tebusan dalam bentuk Bitcoin. Setelah melakukan enkripsi, korban akan diarahkan ke situs web untuk pembayaran tebusan.

04 LockBit

LockBit adalah jenis *malware* berbahaya yang melakukan enkripsi data korban dan meminta tebusan Bitcoin. LockBit disebarkan melalui email *phishing*, tautan berbahaya, atau penggunaan perangkat lunak yang rentan. Jika tebusan tidak dibayarkan, maka data korban akan dipublikasikan atau dihapus.

05 GandCrab

GandCrab pertama kali muncul pada Januari 2018 dan sempat menjadi salah satu *ransomware* paling aktif di dunia. *Ransomware* ini menargetkan pengguna Windows dengan metode penyebaran melalui email *phishing*, tautan berbahaya, atau penggunaan perangkat lunak yang rentan. *Ransomware* ini melakukan enkripsi file dengan algoritma RSA dan AES. Jika tebusan tidak dibayarkan dalam waktu tertentu, data korban akan dihapus.

> The rise of ransomware-as-a-service (RaaS) makes it easier for even less technical criminals to launch attacks.
>
> **- Europol**

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

REKAPITULASI NOTIFIKASI DAN DUGAAN INSIDEN SIBER 2023

2

PENGIRIMAN NOTIFIKASI TAHUN 2023

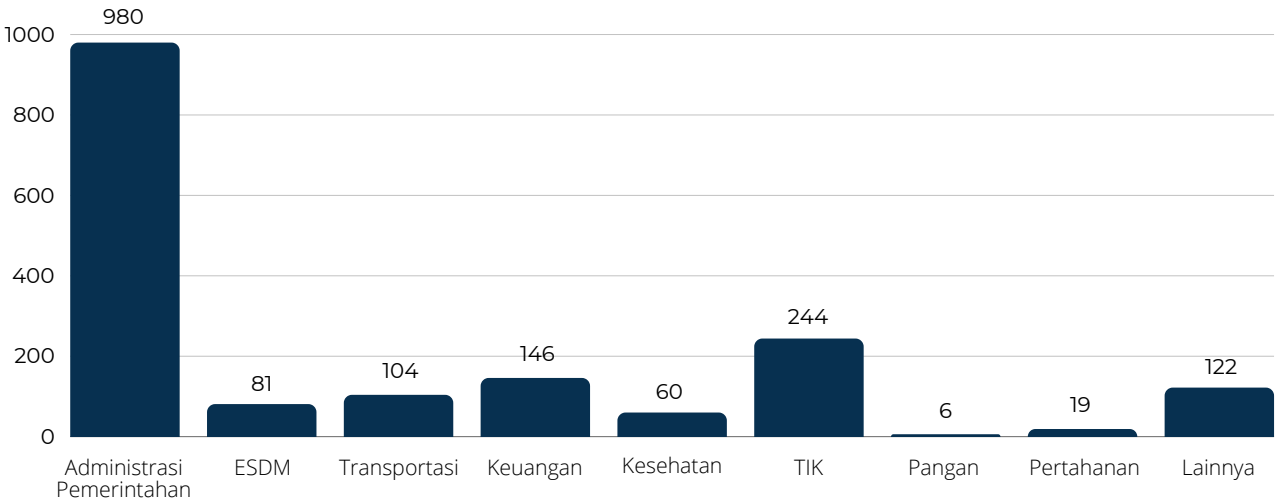
1.762
NOTIFIKASI TERKIRIM

Tim Pusat Kontak Siber BSSN mengirimkan sebanyak **1.762 notifikasi** indikasi insiden siber ke berbagai sektor.

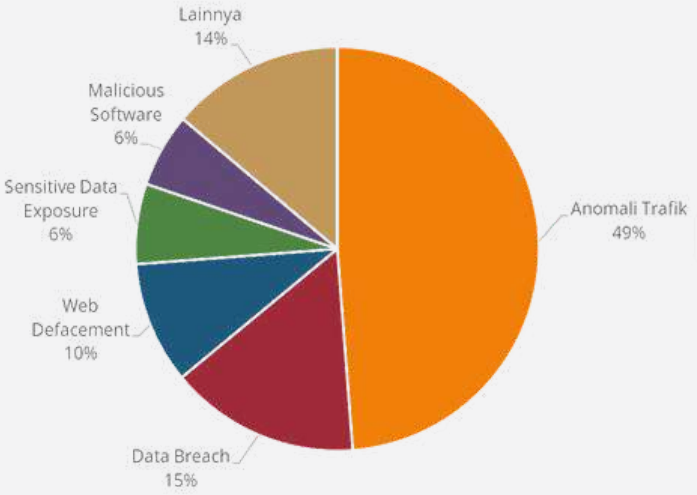
43% | **755 Notifikasi** Direspon

57% | **1007 Notifikasi** Tidak direspon

REKAPITULASI NOTIFIKASI BERDASARKAN SEKTOR



REKAPITULASI NOTIFIKASI BERDASARKAN KLASIFIKASI INDIKASI INSIDEN



Dari 1.762 Notifikasi terkirim, didapatkan hasil Top 5 Klasifikasi Indikasi Insiden yang dinotifikasi oleh BSSN yaitu Anomali Trafik sebanyak 858, *Data Breach* sebanyak 268, *Web Defacement* sebanyak 172, *Senisitive Data Exposure* sebanyak 113, dan *Malicious Software* sebanyak 104.

CYBER THREAT INTELLIGENCE

Hasil pemantauan *Cyber Threat Intelligence* (CTI) ditemukan sebanyak 347 dugaan insiden siber di antaranya yaitu kebocoran data, *ransomware*, *web defacement*, indikasi potensi serangan DDoS, dan pemantauan proaktif dugaan insiden siber. Penelusuran insiden siber merupakan upaya pendalaman terhadap temuan indikasi dugaan insiden siber yang telah terpublikasi melalui forum dan media pada *surface web*, *deepweb*, dan *darkweb*, seperti publikasi dugaan kebocoran data dan publikasi *ransomware*. Pemantauan proaktif dugaan insiden siber merupakan pemantauan secara proaktif terhadap dugaan insiden siber pada *darkweb* seperti data *exposure* yang disebabkan oleh *malware stealer*, informasi potensi serangan siber pada forum *hacking discussion*, serta informasi IoC dan TTP dari *state sponsored threat actor*.

347

Dugaan Insiden Siber

Sebaran Jenis Insiden

Penelusuran Dugaan Insiden
199 laporan

Pemantauan Proaktif Dugaan Insiden
228 laporan

Sektor Terdampak	Jumlah
Adm. Pemerintahan	186
Lainnya	60
Keuangan	38
Transportasi	24
ESDM	18
TIK	5
Kesehatan	5
Pangan	5
Pertahanan	2

DARKNET EXPOSURE

1.674.185

temuan *data exposure*

Darknet exposure merupakan kondisi ketika terdapat data/informasi kredensial akun pada suatu instansi/organisasi tertentu yang terekspos di *darknet*, baik itu pada forum jual beli data, forum diskusi *hacker*, maupun pada *instant messaging*, sehingga berpotensi dapat disalahgunakan oleh pihak yang tidak berkepentingan. *Darknet exposure* dapat disebabkan adanya infeksi *malware stealer* pada perangkat pengguna, ataupun disebabkan adanya pencurian/*dump database* suatu organisasi.

BSSN mengidentifikasi sebanyak 1.674.185 *data exposure* yang mempengaruhi 429 instansi. Analisis lebih lanjut mengungkapkan bahwa sektor pemerintahan memiliki persentase tertinggi dari total *data exposure*, yaitu sebesar 39,78%, diikuti oleh sektor Keuangan dengan 9,86%, sektor Teknologi Informasi dan Komunikasi (TIK) dengan 9,63%, sektor Transportasi dengan 3,40%, Energi dan Sumber Daya Mineral (ESDM) dengan 1,75%, Kesehatan dengan 0,23%, Pangan dengan 0,2%, Pertahanan dengan 0,12%, dan sektor Lainnya sebesar 35,04%.

REKAPITULASI DARKNET EXPOSURE 2023

Sektor	Jumlah Data Exposure	Jumlah Instansi
Adm. Pemerintahan	665.916	134
Lainnya	586.597	56
Keuangan	165.085	58
TIK	161.282	29
Transportasi	56.925	63
ESDM	29.350	19
Kesehatan	3.785	45
Pangan	3.287	17
Pertahanan	1.958	8

Rekomendasi yang dapat diterapkan terkait dengan ancaman pencurian kredensial pengguna antara lain yaitu dengan menerapkan antivirus/EDR, mengimplementasikan *two factor authentication*, menerapkan manajemen akun pengguna, *Restrict File and Directory Permissions*, kebijakan *password* terkait kombinasi karakter dan *update* secara berkala, tidak menggunakan akun/kredensial dinas untuk kepentingan selain kedinasan, dan segmentasi jaringan.

REKAPITULASI INDIKASI KEBOCORAN DATA

103
DUGAAN INSIDEN

BSSN berhasil melakukan deteksi terhadap **103 dugaan** insiden kebocoran data. Dugaan insiden kebocoran data terbanyak terjadi pada bulan Maret 2023 sebanyak 20 kasus dan pada bulan Desember 2023 sebanyak 15 kasus.

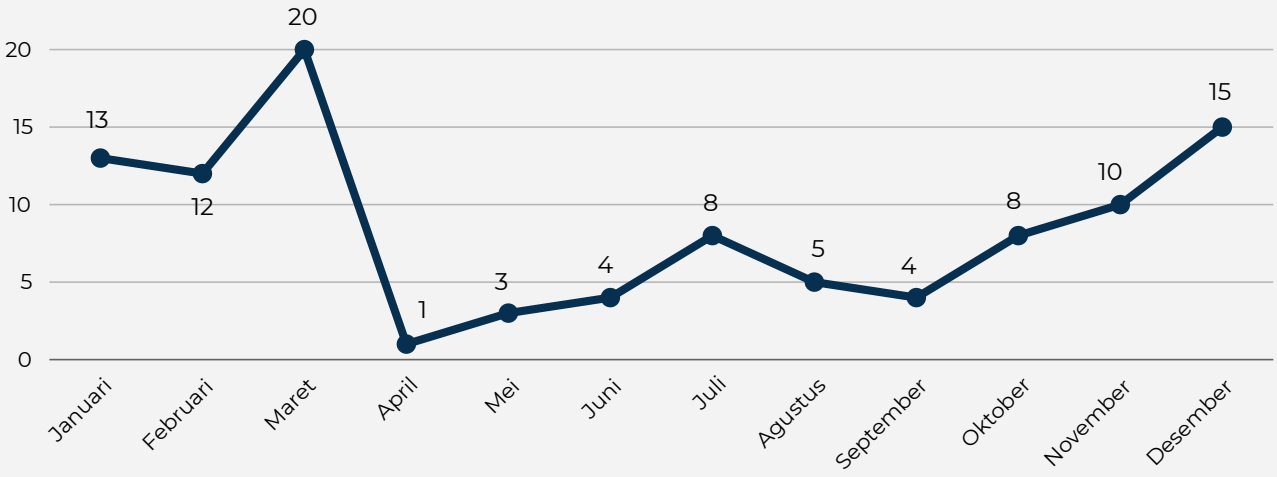
RESPONS

Terdapat **60** ***stakeholder*** yang telah merespons notifikasi.

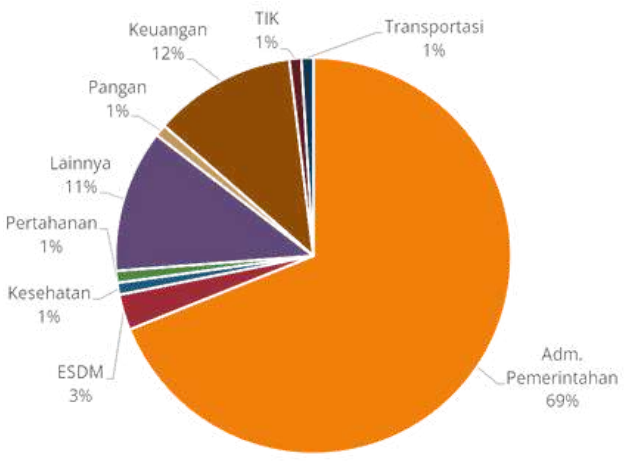
ASISTENSI TINDAK LANJUT

Terdapat **3** ***stakeholder*** yang telah melakukan tindak lanjut dan asisten bersama dengan BSSN.

REKAPITULASI LAPORAN NOTIFIKASI KEBOCORAN DATA 2023



SEKTOR TERDAMPAK



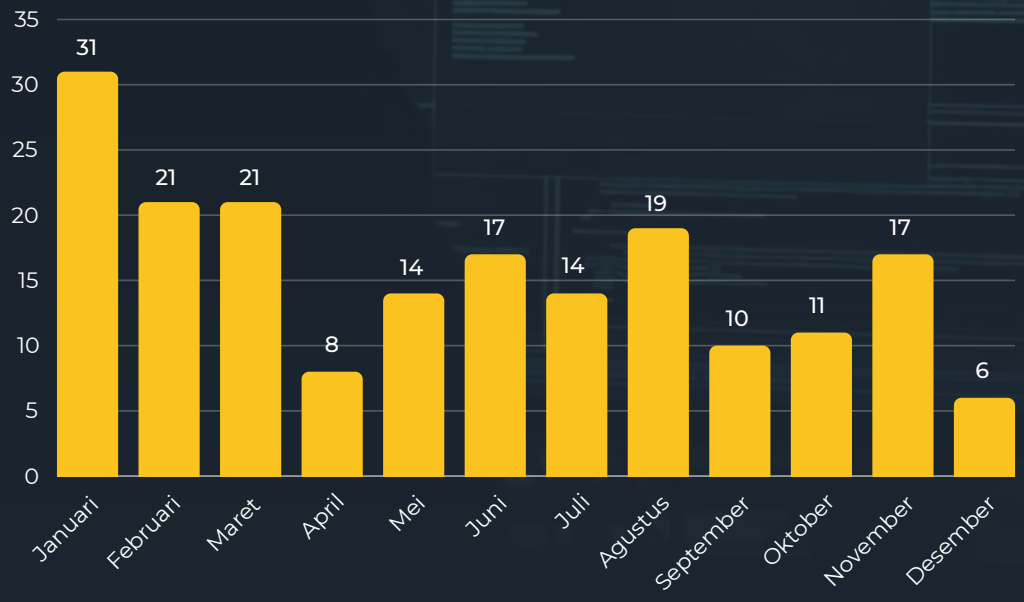
Sektor Administrasi Pemerintahan tercatat memiliki jumlah insiden terbanyak dengan total 71 kasus. Kemudian sektor Keuangan dan Lainnya, masing-masing dengan 12 insiden. Sektor Energi dan Sumber Daya Mineral tercatat memiliki 3 insiden. Sementara itu, sektor Kesehatan, Pangan, Pertahanan, Teknologi Informasi dan Komunikasi, serta Transportasi, masing-masing hanya mengalami 1 insiden. Data ini menunjukkan bahwa sektor Administrasi Pemerintahan merupakan area yang paling banyak terdampak, yang memerlukan perhatian khusus dalam manajemen risiko dan peningkatan keamanan siber.

WEB DEFACEMENT

189

Kasus Web Defacement

Serangan *web defacement* merupakan serangan yang dilakukan untuk mengeksploitasi situs *web* atau *server web* yang rentan dengan memanfaatkan kerentanan dari sistem sehingga *threat actor* dapat merusak, memodifikasi, atau menghapus konten halaman web yang telah diretas. Pelaku serangan *web defacement* disebut sebagai *defacer*. Terdapat 189 kasus *web defacement* yang dinotifikasi kepada pemilik sistem di situs-situs Indonesia dengan kasus terbanyak terjadi pada bulan Januari dengan jumlah kasus sebanyak 31 kasus *web defacement*.



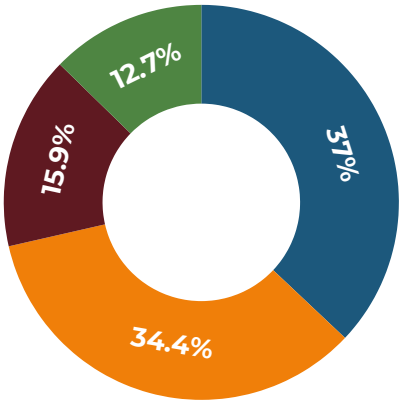
SEKTOR TERDAMPAK WEB DEFACEMENT

Selama tahun 2023, sektor yang paling banyak terkena serangan *web defacement* adalah sektor **Administrasi Pemerintahan** dengan jumlah kasus sebanyak **167 kasus**.

167	Adm. Pemerintahan	**7**	Kesehatan
12	Lainnya	**3**	Pertahanan

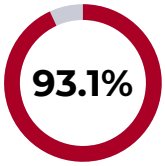
Pengelompokan kasus *web defacement* berdasarkan sebaran waktu bertujuan untuk mengetahui waktu terbanyak terjadinya *web defacement*. Berdasarkan hasil pengelompokan tersebut diketahui bahwa kasus *web defacement* paling banyak terjadi pada ***Weekdays*** **(Senin-Jumat) pada pukul 06.00 – 18.00 WIB** dengan jumlah kasus sebanyak **70 kasus**.

SEBARAN WAKTU TERJADINYA WEB DEFACEMENT

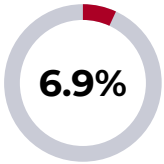


70 kasus	**Weekdays (Senin - Jumat)** 06.00 - 18.00
65 kasus	**Weekdays (Senin - Jumat)** 18.00 - 06.00
30 kasus	**Weekend (Sabtu - Minggu)** 06.00 - 18.00
24 kasus	**Weekend (Sabtu - Minggu)** 18.00 - 06.00

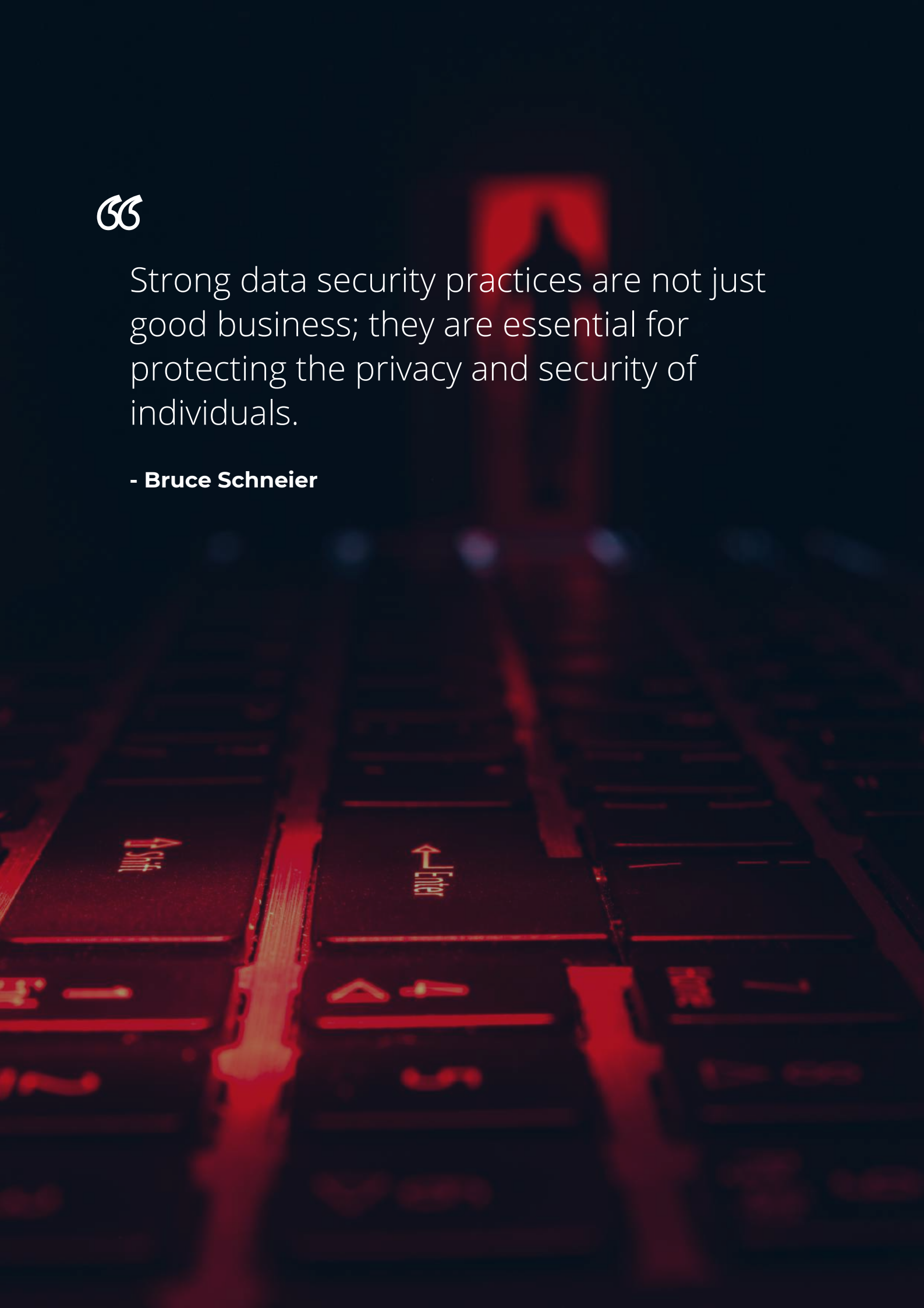
Pada tahun 2023, kasus *web defacement* terjadi pada halaman utama (*homepage*) dan halaman tersembunyi (*hidden*). Terdapat **176 kasus** *defacement* tersembunyi dan **13 kasus** pada halaman utama. *Web Defacement* pada halaman utama mengakibatkan perubahan pada tampilan utama situs, sementara *web defacement* tersembunyi terjadi di lokasi lain dalam situs yang mungkin tidak terdeteksi secara langsung oleh pengguna.



Tersembunyi (Hidden)
176 kasus



Homepage
13 kasus



Strong data security practices are not just good business; they are essential for protecting the privacy and security of individuals.

- Bruce Schneier

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

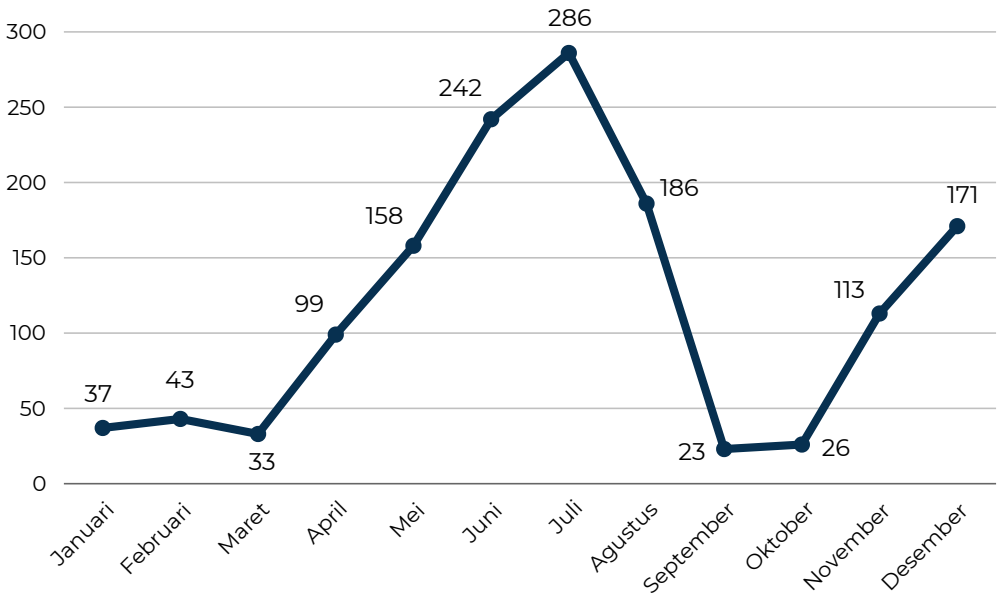
ADUAN SIBER 2023

3

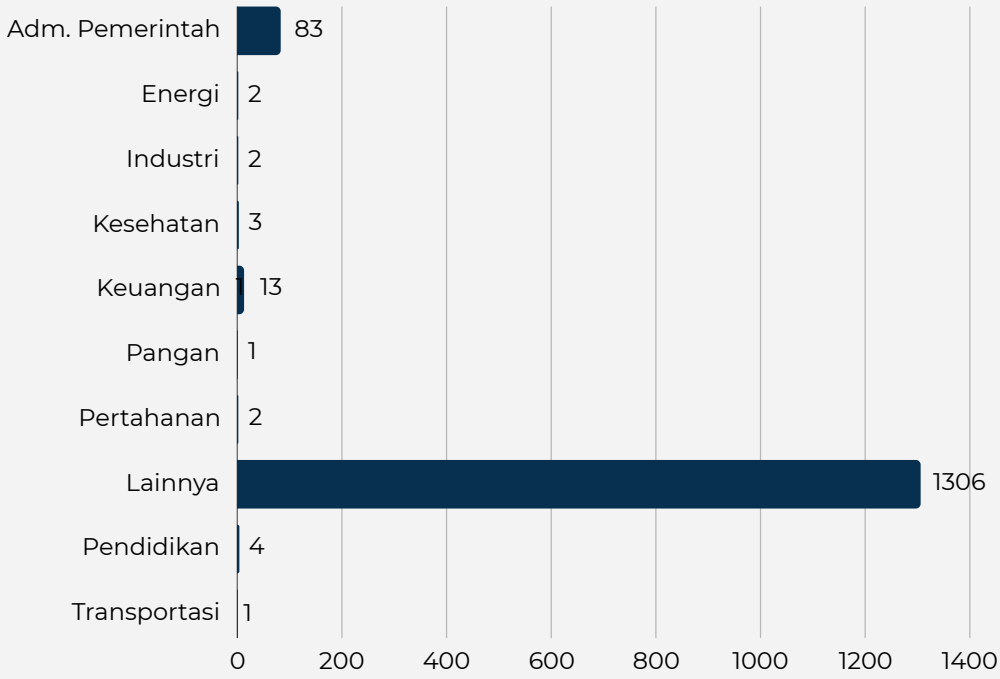
ADUAN SIBER

1.417
Aduan

Selama Tahun 2023, Tim Pusat Kontak Siber BSSN menerima sebanyak **1.417 aduan** siber yang berasal dari berbagai sektor. Adapun aduan terbanyak terdapat pada bulan Juli dengan jumlah **286 aduan**.

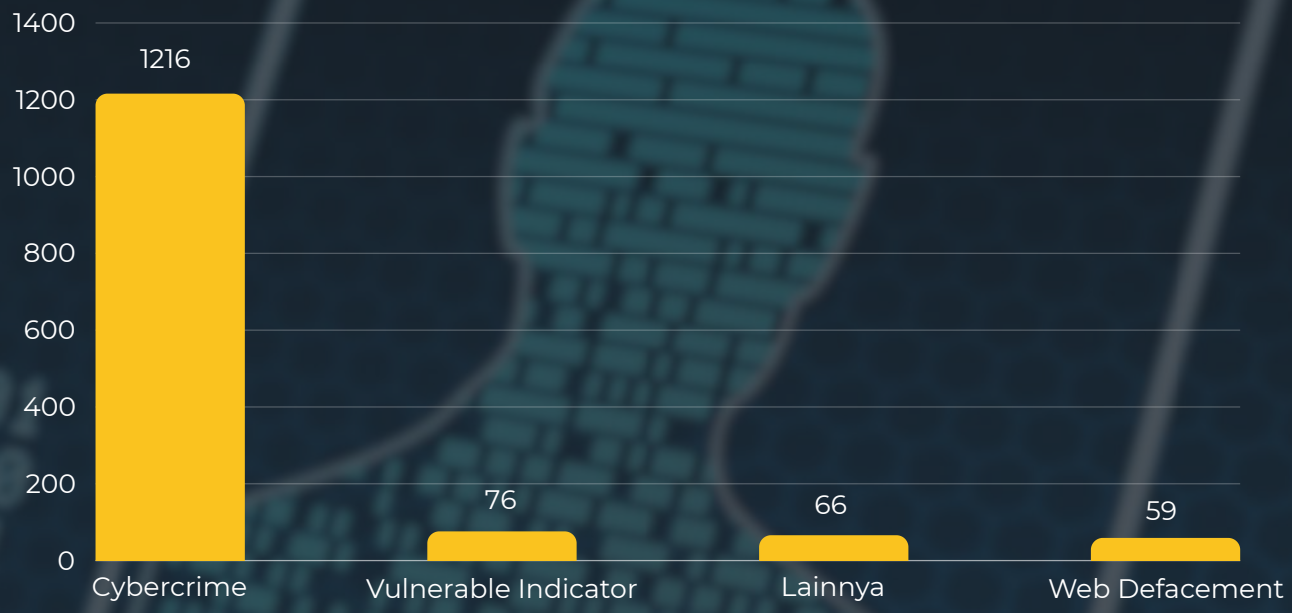


REKAPITULASI ADUAN SIBER BERDASARKAN SEKTOR



KATEGORI ADUAN SIBER

Aduan siber yang diterima oleh BSSN terdiri dari 15 kategori aduan dengan 3 kategori tertinggi yaitu sebagai berikut:



86%

Cybercrime

Tercatat sebanyak **1.216 aduan**. *Cybercrime* adalah tindakan kriminal yang memanfaatkan teknologi, mulai dari perangkat hingga jaringan internet.

5%

Lainnya

Tercatat sebanyak **66 aduan**. Kategori aduan lainnya terdiri dari beberapa kategori yaitu *Ransomware*, *Illegall Access*, *Phishing*, dll.

4%

Web Defacement

Tercatat sebanyak **59 aduan**. *Web defacement* adalah serangan yang dilakukan oleh pihak yang tidak sah untuk mengeksploitasi situs web dengan cara merusak, melakukan modifikasi, atau menghapus isi pada web.

5%

Vulnerable Indicator

Tercatat sebanyak **76 aduan**. *Vulnerability Indicator* merujuk pada kelemahan atau celah dalam suatu sistem yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.

> Cybercrime is not always driven by greed; some attackers are motivated by a desire to cause disruption or make a political statement.

- Europol

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

TOP 5 CVE 2023

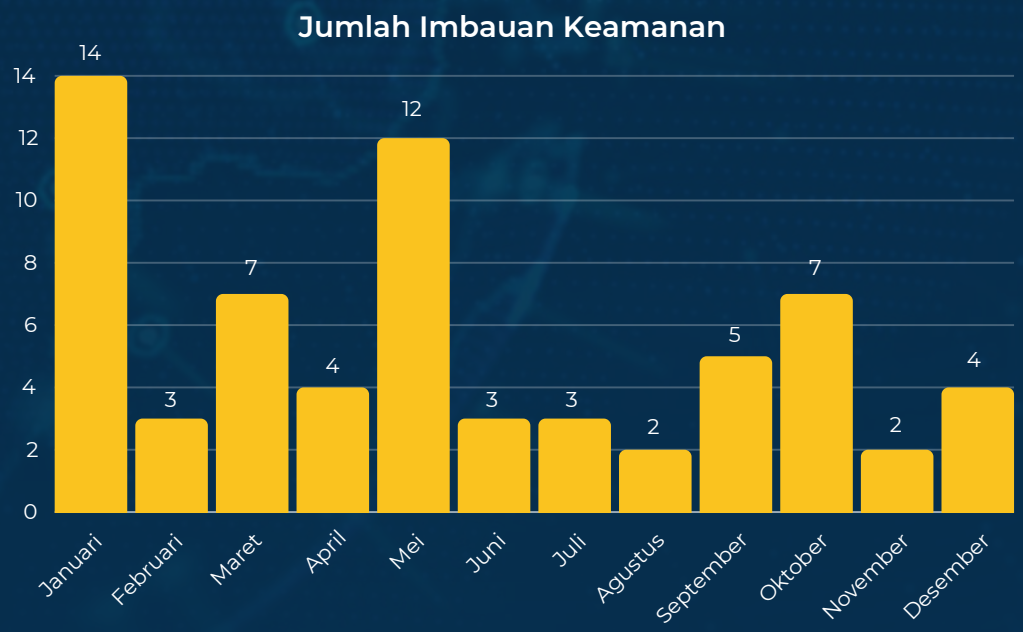
4

TOP 5
CVE GLOBAL

66

Imbauan Keamanan

Common Vulnerabities and Exposures (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 dipublikasikan pada tahun 2023. Adapun kerentanan ini menjadi perhatian karena memiliki skor *Common Vulnerability Scoring System* (CVSS) yang memiliki tingkat dampak *Critical*. Berikut adalah jumlah imbauan keamanan terkait CVE maupun potensi insiden lainnya yang dipublikasikan oleh BSSN:



CVE-2023-20198

CVE-2023-20198 memiliki nilai CVSS **10.00** dengan tingkat dampak ***CRITICAL***. Kerentanan CVE-2023-20198 adalah kerentanan yang ditemukan pada Cisco IOS XE. Kerentanan ini memungkinkan *threat actor* dapat masuk dengan akses user dengan melakukan eksploitasi CVE untuk mendapatkan akses awal dengan menjalankan perintah untuk dapat membuat kombinasi *user* dan *password local*. Hal ini memungkinkan pengguna untuk masuk dengan akses pengguna normal. *Threat actor* kemudian mengeksploitasi komponen lain dari fitur antarmuka pengguna web, memanfaatkan pengguna lokal baru untuk meningkatkan hak akses menjadi *root* dan menulis *implant* ke sistem file.

DAMPAK

Jika berhasil dieksploitasi, kerentanan ini memungkinkan *threat actor* yang tidak sah untuk membuat akun baru dengan hak *administrator* penuh melalui *privilege escalation*. Akun *administrator* yang tidak sah ini bersifat persisten, sehingga *threat actor* tetap ada dalam sistem bahkan jika perangkat di-*restart*.

PANDUAN MITIGASI

Melakukan *upgrade* sistem ke *software* terbaru yang telah di-*update*.

CVE-2023-4596

CVE-2023-4596 memiliki nilai CVSS **9.8** dengan tingkat dampak ***CRITICAL***. Plugin Forminator untuk WordPress ditemukan memiliki kerentanan terkait *arbitrary file upload*. Kerentanan ini berasal dari validasi jenis berkas yang terjadi setelah berkas telah diunggah ke server dalam fungsi upload_post_image(). Masalah keamanan ini memengaruhi versi hingga dan termasuk 1.24.6 dari plugin ini. Sebagai akibatnya, *threat actor* yang tidak sah dapat berpotensi mengeksploitasi kelemahan ini untuk mengunggah berkas acak ke server situs yang terpengaruh, sehingga menciptakan risiko aktivasi kode jarak jauh.

DAMPAK

Threat actor dapat melakukan penambahan, pengubahan bahkan pencurian data sensitif yang disimpan pada *database*. Selain itu, dengan mengetahui data sensitif tersebut memberikan potensi kepada *threat actor* untuk melakukan eskalasi serangan seperti upaya pengaksesan jarak jauh.

PANDUAN MITIGASI

Langkah mitigasi yang dapat dilakukan adalah dengan melakukan pembaruan sistem ke versi terbaru secara berkala.

CVE-2023-23415

CVE-2023-23415 memiliki nilai CVSS **9,8** dengan tingkat dampak ***CRITICAL***. Kerentanan ini terkait sistem operasi Windows yang memengaruhi beragam versi Windows, termasuk personal dan *server*. Penyebabnya adalah kurangnya validasi *input* pada *Internet Control Message Protocol* (ICMP), yang digunakan untuk mengatasi masalah konektivitas di perangkat jaringan.

DAMPAK

Memungkinkan *threat actor* memberikan input berupa kode berbahaya yang disisipkan melalui *backdoor* kemudian mengeksekusinya secara *remote* untuk mengambil alih kendali akses pada target tanpa diketahui korban.

PANDUAN MITIGASI

Melakukan *update patch* keamanan dengan versi terbaru pada Windows.

CVE-2023-41993

CVE-2023-41993 memiliki nilai CVSS **9,8** dengan tingkat dampak ***CRITICAL***. Kerentanan ini ditemukan pada mesin *browser* WebKit dan dieksploitasi untuk meretas iPhone. *Threat actor* bisa mengakses sistem korban dengan memproses konten web yang dirancang khusus. Apple telah memperbaiki masalah ini pada iOS 16.7, 17.0.1, dan produk lainnya seperti MacOS <13.2, iPadOS <17.0.1, WatchOS 9.6.3, dan MacOS Ventura 13.6.

DAMPAK

Threat actor dapat mengeksekusi kode berbahaya yang telah dibuat dan disisipkan pada konten web yang akan diakses oleh korban.

PANDUAN MITIGASI

Melakukan pembaruan sistem dari versi produk yang terdampak. Selain itu, pengguna perlu menghindari pemasangan aplikasi dari sumber yang tidak sah.

CVE-2023-22515

CVE-2023-22515 memiliki nilai CVSS **9,8** dengan tingkat dampak ***CRITICAL***. Kerentanan ini merupakan *Broken Access Control* yang mempengaruhi Atlassian *Confluence Data Center* dan *Server* versi di atas 8.0.0 serta situs Atlassian *Cloud*. Penyebabnya adalah ketidakvalidan input pada *endpoint* /server-info.action yang tidak terotentikasi. CISA, FBI, dan MS-ISAC merilis Panduan Keamanan Siber untuk merespons eksploitasi aktif kerentanan ini.

DAMPAK

Threat actor tanpa otentikasi dapat mengeksploitasi kerentanan untuk membuat akun *administrator Confluence* yang tidak sah dan mengakses instansi *Confluence*.

PANDUAN MITIGASI

Pengguna perlu memperbarui perangkat lunak Atlassian *Confluence Data Center* dan *Server*, membatasi akses ke jaringan tidak terpercaya, dan menerapkan *cybersecurity best practice*.

TOP 5
CVE NASIONAL

Top 5 CVE Nasional adalah daftar 5 (lima) jenis kerentanan yang memiliki jumlah *hit* terbanyak di Indonesia pada tahun 2023. Kerentanan-kerentanan ini memiliki tingkat dampak dari *High* hingga *Critical*. Dalam bab ini, akan disajikan rincian penjelasan mengenai setiap CVE, dampaknya terhadap sistem dan aplikasi, panduan mitigasi untuk mengurangi risiko, serta kategori sektor yang mungkin terpengaruh oleh masing-masing kerentanan dalam Top 5 CVE Nasional.

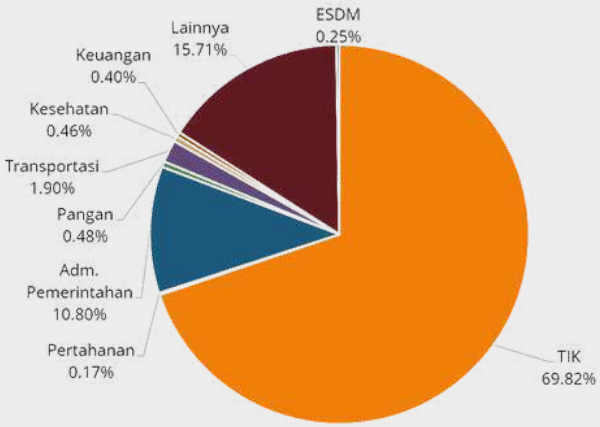
CVE-2022-22721

CVE 2022-22721 memiliki nilai CVSS **9,1** dengan tingkat dampak ***CRITICAL***. Penyebab dari kerentanan ini adalah adanya *integer overflow* yang dipicu oleh adanya izin pemrosesan *request bodies* pada LimitXMLRequestBody dengan ukuran lebih besar dari 350 MB di dalam sistem 32 bit. Adapun ukuran *default* yang diberikan Apache HTTP *Server* untuk LimitXMLRequestBody adalah 1 MB. Hal ini dapat menyebabkan adanya *out of bounds writes*.

DAMPAK

Dampak yang disebabkan berupa *buffer overflow* dengan ukuran *request body* yang sangat besar atau tak terbatas melalui LimitXMLRequestBody.

SEKTOR TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 69.82%, Sektor Lainnya sebesar 15.71%, dan Sektor Administrasi Pemerintahan sebesar 10.80%.

PANDUAN MITIGASI

- Pengguna Apache HTTP Server versi 2.4.52 dan sebelumnya disarankan untuk mengatur opsi LimitXMLRequestBody dengan nilai yang lebih kecil dari 350MB. Mengatur opsi LimitXMLRequestBody menjadi 0 sangat tidak disarankan karena dapat menyebabkan *system out-of-memory* secara keseluruhan. Adapun konfigurasi secara default (LimitXMLRequestBody bernilai 1 MB) tidak terpengaruh pada kerentanan ini.
- Pengguna Apache HTTP Server versi 2.4.52 dan sebelumnya sangat disarankan untuk melakukan pembaruan versi ke versi terbaru saat ini yaitu versi 2.4.55.

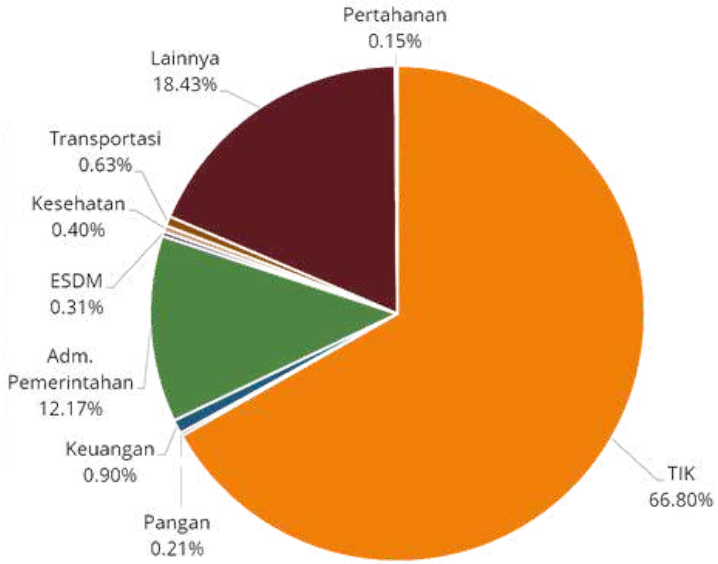
CVE-2022-26377

CVE-2022-26377 memiliki nilai CVSS **7,5** dengan tingkat dampak ***HIGH***. Penyebab utama kerentanan ini yaitu adanya interpretasi yang tidak konsisten pada HTTP *request* (kerentanan HTTP *request Smuggling*) dalam mod_proxy_ajp. Kerentanan ini dapat dimanfaatkan *threat actor* untuk menyisipkan *request* ke *server* AJP tempat *request* diteruskan.

DAMPAK

Dampak dari adanya kerentanan ini adalah *threat actor* dapat mengancam sistem target dan melakukan perubahan data sehingga mempengaruhi aspek integritas.

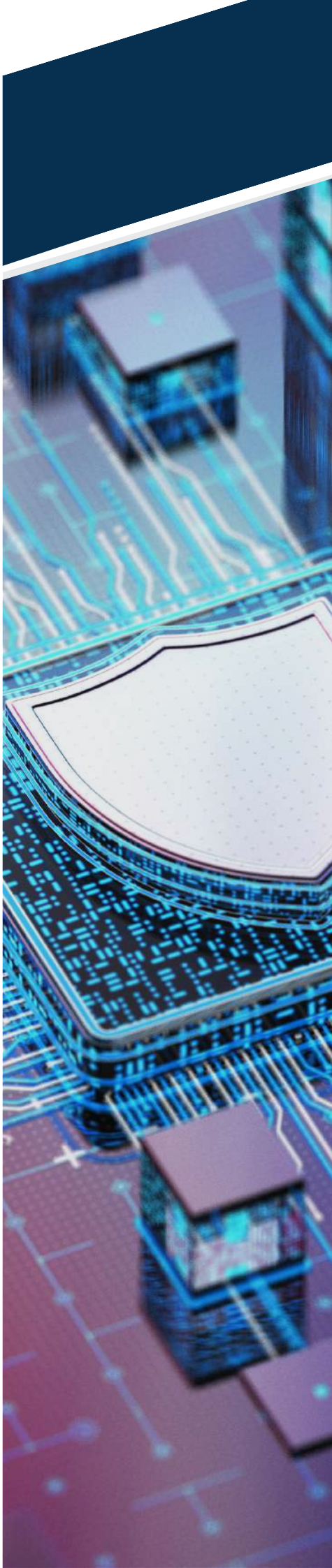
SEKTOR TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 66.80%, Sektor Lainnya sebesar 18.43%, dan Sektor Administrasi Pemerintahan sebesar 12.17%.

PANDUAN MITIGASI

- Pengguna Apache HTTP Server versi 2.4.53 dan sebelumnya sangat disarankan untuk melakukan pembaruan versi ke versi terbaru saat ini yaitu versi 2.4.56.
- Menonaktifkan fungsi mod_proxy_ajp dan melakukan *restart* terhadap layanan httpd.
- Menerapkan protokol komunikasi SSL.



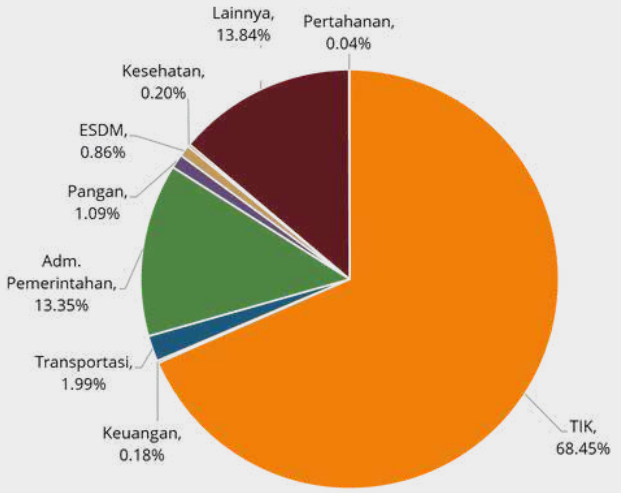
CVE-2023-0662

CVE-2023-0662 memiliki nilai CVSS **7,5** dengan tingkat dampak ***HIGH***. Kerentanan ini terdapat pada PHP 8.0 (sebelum versi 8.0.28), PHP 8.1 (sebelum versi 8.1.16), dan PHP 8.2 (sebelum versi 8.2.3). Penyebab utama dari kerentanan CVE-2023-0662 berkaitan dengan salah satu konfigurasi *default* PHP, yaitu proses *parsing multipart request body* yang mengizinkan *threat actor* tanpa autentikasi untuk mengakses CPU time dalam jumlah besar dan memicu *excessive logging* (pencatatan yang berlebihan).

DAMPAK

Threat actor dapat memblokir semua worker process yang tersedia dan secara signifikan memperlambat pemrosesan permintaan pengguna yang sah. Hal tersebut sangat berpengaruh terhadap akses ketersediaan dari sistem yang tereksploitasi.

SEKTOR TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 68,45%, Sektor Lainnya sebesar 13,84%, dan sektor Administrasi Pemerintahan sebesar 13,35%.

PANDUAN MITIGASI

- Melakukan *patching* versi PHP menjadi versi terbaru atau minimal pada versi yang tidak terdampak kerentanan (V8.0.28 keatas untuk versi 8.0, V8.1.16 keatas untuk versi 8.1, dan versi 8.2.3 untuk versi 8.2).
- Mengurangi post_max_size hingga mendekati nol. Hal Ini akan membuat sebagian besar situs web tidak dapat berinteraksi dan mengganggu unggahan file.
- Melakukan pemantauan lalu lintas jaringan secara secara teratur untuk mendeteksi serangan DoS dengan menggunakan alat pemantauan jaringan yang dapat memberikan pemberitahuan atau peringatan saat lalu lintas jaringan yang tidak normal telah terdeteksi.
- Melakukan implementasi sistem dan infrastruktur yang redundan untuk mengurangi dampak serangan DoS. Misalnya, menggunakan *multiple server* atau menggunakan layanan *cloud* yang menawarkan replikasi dan penyebaran lalu lintas jaringan.
- Melakukan pengujian keamanan secara berkala untuk mengidentifikasi kerentanan dalam sistem dan aplikasi. Upaya yang dapat dilakukan adalah audit keamanan dan pengujian penetrasi dapat membantu mengidentifikasi dan memperbaiki kerentanan yang berpotensi dapat dimanfaatkan oleh serangan DoS.

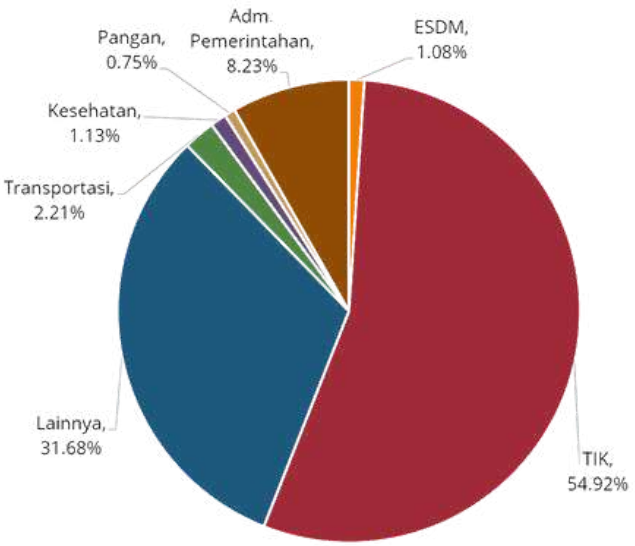
CVE-2023-30799

CVE-2023-30799 memiliki nilai CVSS **7,2** dengan tingkat dampak ***HIGH***. Kerentanan ini berdampak pada versi MikroTik RouterOS *stable* sebelum 6.49.7 dan *long term* hingga 6.48.6 rentan terhadap serangan *Privilege Escalation*. *Threat actor* secara jarak jauh dan terotentikasi dapat meningkatkan *privilege* dari *admin* ke *super admin* melalui Winbox atau HTTP.

DAMPAK

Threat actor dapat menyalahgunakan kerentanan ini untuk mengeksekusi kode arbitrer pada sistem yang berdampak pada *confidentiality*, *integrity*, dan *availability* serta menjadikan *botnet Distributed Denial-of-Service* (DDoS) dan menggunakan sebagai *proxy command-and-control*.

SEKTOR TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 54,92%, Sektor Lainnya sebesar 31,68%, dan sektor Administrasi Pemerintahan sebesar 8,23%.

PANDUAN MITIGASI

- Melakukan verifikasi dan validasi pada aset yang berpotensi rentan, terutama jika dimiliki oleh ISP atau penyedia layanan *hosting*, serta memberikan notifikasi kepada *stakeholder*/pelanggan terkait.
- Melakukan remediasi segera dengan memperbarui perangkat ke versi terbaru (6.49.8 atau 7.x) untuk menutup celah kerentanan.
- Melakukan mitigasi dengan menutup akses *Router* Mikrotik dari internet, membatasi alamat IP *administrator*, menonaktifkan Winbox dan antarmuka web, serta mengonfigurasi SSH menggunakan *Public/Private Key* dan menonaktifkan akses menggunakan *password*.
- Melakukan *compromised assessment* pada aset yang berpotensi terdampak untuk mengidentifikasi eksploitasi kerentanan.
- Menggunakan IDS, IPS, dan perangkat deteksi anomali untuk mendeteksi dan mencegah eksploitasi kerentanan.

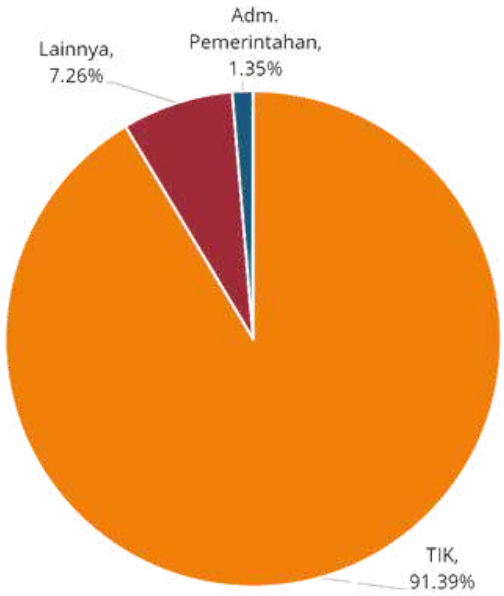
CVE-2022-3602

CVE-2022-3602 memiliki nilai CVSS **7,5** dengan tingkat dampak ***HIGH***. Kerentanan ini disebabkan oleh *buffer overrun* saat memverifikasi sertifikat X.509, terutama dalam pemeriksaan *name constraint*. Kerentanan ini memengaruhi fungsi ossl_punycode_decode di OpenSSL, yang digunakan untuk mengonversi domain Punycode ke Unicode selama validasi sertifikat X.509. Hal ini terjadi setelah verifikasi tanda tangan *certificate chain* dan membutuhkan tindakan CA untuk menandatangani sertifikat yang berpotensi berbahaya atau memungkinkan aplikasi melanjutkan verifikasi sertifikat meskipun gagal membangun jalur ke *trusted issuer*.

DAMPAK

Threat actor dapat membuat alamat *email* berbahaya untuk melakukan *overflow four attacker-controlled bytes* yang berisi `.' karakter (*decimal* 46) pada *stack*. Hal ini akan berdampak pada kerahasiaan, integritas, dan ketersediaan data. *Buffer overflow* yang ditimbulkan dapat menyebabkan *crash* yang mengarah ke penolakan layanan. Kerentanan ini juga memungkinkan *threat actor* jarak jauh untuk mengeksekusi kode arbitrer dan mengeksploitasi korban yang menjalankan versi OpenSSL rentan hanya dengan mengarahkan klien ke *server* TLS jahat yang menggunakan sertifikat yang dibuat khusus.

SEKTOR TERDAMPAK



Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 91,39%, Sektor Lainnya sebesar 7,26%, dan Sektor Administrasi Pemerintahan sebesar 1,35%.

PANDUAN MITIGASI

Pengguna OpenSSL versi 3.0.0 – 3.0.6 disarankan segera memperbarui ke versi 3.0.7. Jika menggunakan salinan OpenSSL dari vendor sistem operasi atau pihak ketiga, sebaiknya mencari versi terbaru. Jika tidak dapat memperbarui, menonaktifkan autentikasi klien TLS yang sedang digunakan merupakan alternatif sementara.

Ignoring cyber vulnerabilities is akin to leaving your door unlocked. We must actively identify, prioritize, and address them.

- General Ban Ki-moon

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

HIGHLIGHT IT SECURITY ASSESSMENT 2023

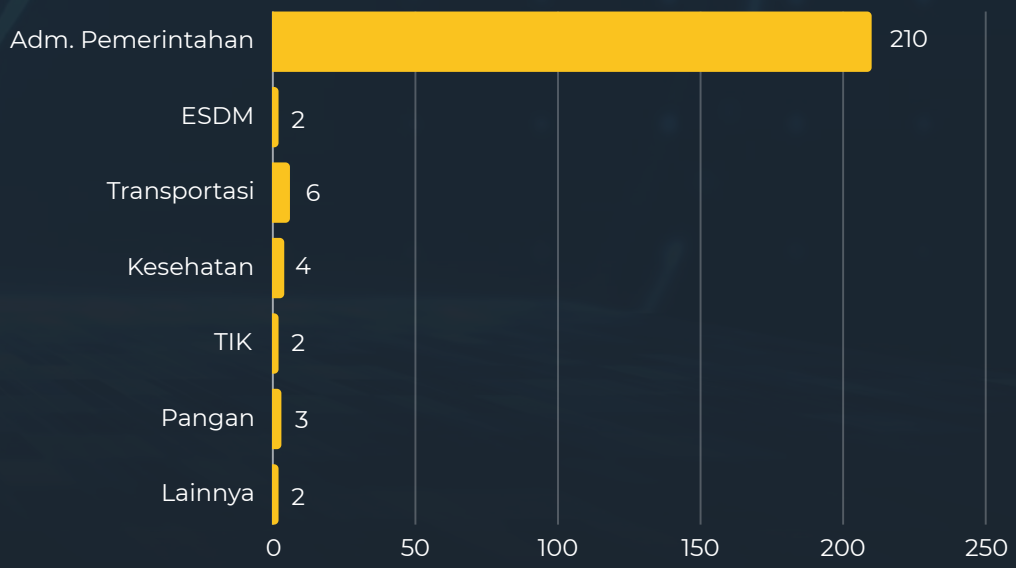
5

ITSA PADA SISTEM ELEKTRONIK

586

Sistem Elektronik yang Diuji

Salah satu layanan BSSN yaitu *Information Technology Security Assessment* (ITSA) untuk melakukan pengujian terhadap keamanan sistem elektronik serta memastikan sistem elektronik tersebut dapat digunakan dengan baik dan optimal. Tujuan dari ITSA adalah untuk mengidentifikasi dan mengevaluasi potensi risiko keamanan informasi, serta memberikan rekomendasi untuk memperbaiki kelemahan yang ditemukan. Proses ini membantu organisasi untuk meningkatkan pertahanan keamanan mereka, mengurangi risiko kehilangan data atau serangan siber, dan mematuhi standar keamanan yang berlaku.



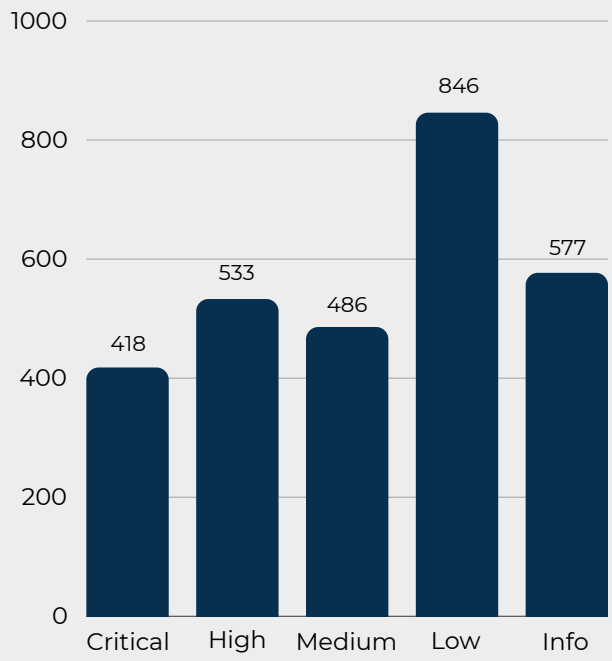
HASIL ITSA TAHUN 2023

2.860
celah keamanan ditemukan

BSSN telah melaksanakan kegiatan ITSA pada 138 instansi dengan jumlah 586 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).

GRAFIK TINGKAT RISIKO

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



- Tingkat risiko *CRITICAL*, harus segera diperbaiki karena sangat rentan atau berpeluang menerima serangan dari luar, juga menimbulkan kerugian yang sangat besar bagi organisasi
- Tingkat risiko *HIGH*, harus segera diperbaiki karena sangat rentan atau berpeluang menerima serangan dari luar, juga mengganggu performa dari sebuah web aplikasi yang rentan
- Tingkat risiko *MEDIUM*, dampak kerentanan dapat mengakibatkan permasalahan pada internal web seperti kerusakan pada data.
- Tingkat risiko *LOW*, mengindikasikan perlu diambilnya sebuah tindakan sederhana seperti peningkatan versi *software* atau penambahan rules pada aplikasi web.
- Tingkat risiko *INFO*, mengindikasikan adanya informasi temuan sederhana pada web yang tidak membutuhkan sebuah tindakan perbaikan signifikan.

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

TOP 5 KERENTANAN

Berdasarkan hasil ITSA pada tahun 2023, ditemukan sebanyak 2.860 celah keamanan yang memiliki tingkat risiko yang beragam. Dari seluruh kerentanan yang terdeteksi, berikut merupakan 5 (lima) kerentanan dengan tingkat risiko *Critical* pada tahun 2023.

01 Insecure Direct Object Reference (IDOR)

Kerentanan *Insecure Direct Object Reference* (IDOR) adalah kerentanan umum yang sering terjadi pada aplikasi web. Dalam IDOR, *threat actor* dapat dengan mudah mengakses atau memodifikasi data tanpa memerlukan validasi atau otorisasi yang memadai. Hal ini dapat mengakibatkan akses yang tidak sah ke informasi dan sumber daya yang harusnya terlindungi. Untuk mengatasi kerentanan IDOR, aplikasi web perlu menerapkan kontrol akses yang ketat, memastikan adanya otorisasi yang kuat, serta menggunakan teknik enkripsi data yang sesuai. Dengan langkah-langkah ini, aplikasi dapat menjaga keamanan dan integritas data yang disimpannya.

02 Broken Access Control (BAC)

Broken Access Control (BAC) adalah kerentanan keamanan yang terjadi ketika sistem atau aplikasi tidak memberikan kontrol akses yang memadai. Dalam situasi ini, *threat actor* dapat memanfaatkannya untuk mendapatkan akses yang tidak sah. Contoh kerentanan BAC melibatkan kegagalan dalam memeriksa otorisasi pengguna, parameter URL yang dapat diubah, validasi akses hanya di sisi klien, kurangnya proteksi terhadap sesi, dan kesalahan konfigurasi. Upaya perbaikan BAC harus memfokuskan pada validasi yang ketat, perlindungan terhadap parameter URL, pemrosesan akses di sisi *server*, manajemen sesi yang efektif, dan konfigurasi yang benar pada tingkat *server* atau aplikasi.

03 SQL Injection

SQL Injection (SQLi) adalah jenis serangan keamanan pada aplikasi web yang mengeksploitasi celah dalam pemrosesan *input* oleh sistem manajemen basis data (*Database Management System* - DBMS). Dalam serangan ini, *threat actor* menyisipkan kode SQL berbahaya dalam input aplikasi untuk menjalankan perintah SQL yang tidak sah. Untuk melindungi aplikasi dari *SQL Injection*, perlu dilakukan penyaringan dan validasi *input* yang tepat, serta menggunakan *parameterized queries* atau *prepared statements*. Selain itu, penting untuk melakukan pengujian keamanan secara berkala dan menjaga perangkat lunak serta sistem basis data tetap diperbarui untuk mengurangi risiko serangan *SQL Injection*.

04 File Upload Vulnerability

File Upload Vulnerability adalah jenis kerentanan keamanan pada aplikasi web yang mengizinkan *threat actor* untuk mengunggah *file* berbahaya ke *server*, yang kemudian dapat digunakan atau diakses oleh *threat actor*. Kerentanan ini terjadi ketika aplikasi tidak melakukan validasi atau pemeriksaan yang memadai terhadap *file* yang diunggah oleh pengguna. *Threat actor* dapat memanfaatkan kerentanan ini untuk mengunggah *file* berbahaya seperti *script* eksekusi atau *malware*, yang berpotensi merusak integritas dan keamanan sistem. Untuk mengatasi *File Upload Vulnerability*, penting untuk melakukan validasi yang ketat terhadap jenis dan ekstensi file yang diunggah, serta memeriksa keabsahan *file* sebelum memungkinkan akses atau eksekusi. Selain itu, pemantauan dan pembaruan rutin terhadap aplikasi web juga merupakan praktik penting dalam menjaga keamanan terhadap kerentanan ini.

05 Privilege Escalation

Privilege Escalation adalah ketika *threat actor* berhasil meningkatkan tingkat akses atau hak istimewa yang melebihi wewenang yang seharusnya dimiliki pada sistem atau aplikasi. Kerentanan *privilege escalation* adalah kelemahan yang memungkinkan *threat actor* untuk memperoleh kontrol lebih besar atas sistem atau data. Untuk mencegah serangan *Privilege Escalation,* tindakan berikut dapat diambil:

1. Melakukan pembaruan perangkat lunak dan sistem operasi secara berkala untuk mengatasi kerentanan yang telah ditemukan dan diperbaiki.
2. Memastikan manajemen kredensial yang aman, termasuk penggunaan password yang kuat dan autentikasi ganda.
3. Menetapkan dan memantau kontrol akses dengan ketat untuk menghindari *threat actor* mendapatkan akses yang tidak sah.
4. Melakukan pemantauan aktifitas pengguna secara rutin untuk mendeteksi tindakan mencurigakan atau tanda-tanda *privilege escalation*.

Cyber threats are constantly evolving, so we must constantly adapt our defenses. The fight against cyberattacks is a never-ending battle.

- Robert Gates

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

TOP 10 CYBERSECURITY INSIGHT

6

TOP 10 CYBERSECURITY INSIGHT

01

Bareskrim Menyelidiki Modus Kejahatan Kriminal Bermodus Penipuan Undangan Nikah Melalui Whatsapp

Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri menyelidiki modus baru penipuan dengan menggunakan tautan undangan pernikahan yang ramai terjadi di masyarakat. Pelaku penipuan mengirimkan file melalui WhatsApp dengan format APK dengan nama surat undangan pernikahan. Kemudian pelaku mengirimkan pesan instan "Kami harap kehadirannya" kemudian mengirimkan tautan seolah itu adalah undangan dan peta ke lokasi acara di bawahnya.

02

Serangan QakNote Terbaru Menggunakan Dokumen Microsoft OneNote Untuk Menyisipkan QBot Malware

QBot *Malware* terbaru yang dijuluki QakNote menggunakan Microsoft OneNote *malicious attachment* yang menginfeksi sistem dengan *Banking Torjan*. OneNote *attachment* pada *email phising* merupakan *attack vector* terbaru yang menggantikan *malicious macros* pada dokumen Micrososft Office yang telah dihilangkan.

03

Kelompok Ransomware LockBit 3.0 Bertanggung Jawab atas Serangan Siber yang Menargetkan Salah Satu Perusahaan di Sektor Keuangan

Serangan siber terhadap perusahaan di sektor keuangan telah diungkap, di mana kelompok peretas *ransomware* LockBit 3.0 mengaku bertanggung jawab atas serangan tersebut. Serangan *ransomware* LockBit 3.0 terhadap perusahaan tersebut mengganggu layanan secara menyeluruh dan mencuri data pribadi jutaan pelanggan.

04

APT Sharp Panda Menargetkan Entitas Pemerintahan di Asia Tenggara

Kampanye yang dikaitkan dengan kelompok APT Sharp Panda yang menargetkan entitas pemerintah yang berprofil tinggi di Asia Tenggara. Aktivitas kelompok ini diidentifikasi pertama kali pada awal 2021, saat kelompok tersebut menargetkan entitas pemerintah di Asia Tenggara dengan serangan *spear-phishing* yang berisi dokumen RTF berbahaya. Kelompok ini diindikasikan menargetkan entitas di negara-negara Asia Tenggara, seperti Vietnam, Indonesia, dan Thailand.

05

Malware Luna Grabber Menargetkan Pengembang Roblox untuk Mencuri Data Melalui Package NPM

Terdapat indikasi penargetan serangan siber yang canggih pada pengembang *platform* game Roblox. *Threat actor* telah mendistribusikan *malicious package* npm. *Malicious package* tersebut diidentifikasi sebagai *malware* Luna Grabber yang menyamar sebagai perangkat lunak sah. Luna Grabber dapat mencuri data sensitif dari *browser*, aplikasi Discord, dan konfigurasi sistem.

06 Dugaan Kebocoran Data Salah Satu Perusahaan di Sektor Pariwisata Mencapai 1,2 Juta Data Pengguna

Kebocoran data diduga telah membahayakan keamanan salah satu perusahaan di sektor pariwisata dan berpotensi mengungkap 1,2 juta data pribadi pengguna. Seorang pelaku ancaman, yang dikenal dengan nama 'Sheriff' di *darkweb*, telah melapor dan mengklaim kebocoran data tersebut, yang mencakup detail sensitif seperti nama, alamat email, negara tempat tinggal, kota, dan lainnya. Disarankan untuk pengguna segera mengambil langkah untuk mengamankan akun, seperti mengatur ulang password dan mengaktifkan fitur 2FA. Pengguna juga harus waspada terhadap *email* atau pesan dari nomor yang tidak dikenal.

07 GitLab Mendesak Pengguna untuk Menginstal Pembaruan Keamanan terkait Kerentanan Pipeline yang Critical

GitLab telah merilis pembaruan keamanan untuk mengatasi kerentanan kritis (CVE-2023-5009) yang memungkinkan *threat actor* menjalankan *pipeline* sebagai pengguna lain melalui kebijakan pemindaian keamanan terjadwal. Kerentanan ini berdampak pada GitLab *Community Edition* (CE) dan *Enterprise Edition* (EE) versi 13.12 hingga 16.2.7 dan versi 16.3 hingga 16.3.4. GitLab menyarankan pengguna untuk segera menerapkan pembaruan keamanan yang tersedia untuk memitigasi masalah ini.

08 Kerentanan Zero-Day pada WIndows Telah Dieksploitasi Oleh Kelompok Ransomware

Sebuah celah keamanan *zero-day* pada sistem operasi Windows telah dieksploitasi oleh para *threat actor* dalam serangan *ransomware*. Celah keamanan CVE-2023-28252 berdampak pada semua server dan *client* Windows yang dapat diserang dengan tingkat kesulitan yang rendah. Kelompok ini menggunakan setidaknya 5 *Common Log File System* (CLFS) sejak Juni 2022 yang diketahui membagi kodenya dengan kelompok *ransomware* lain seperti JSWorm, Karman, dan Nemty *ransomware*.

09 Security Update Untuk Mengatasi Kerentanan Critical Pada Network Attached Storage

Perusahaan teknologi jaringan Zyxel telah merilis pembaruan keamanan pada *Network Attached Storage* (NAS). Kerentanan pada NAS dicatat sebagai CVE-2023-27992 dengan kemungkinan dampak critical (CVSS 9.8). Kerentanan tersebut memungkinkan *threat actor* untuk melakukan *command injection* tanpa melakukan otentikasi. Beberapa versi NAS yang terdampak kerentanan ini antara lain NAS326 V5.21(AAZF.13)C0, NAS540 V.21(AATB.10)C0, dan NAS542 V5.21(ABAG.10)C0.

10 Jutaan Motherboard PC Dijual dengan Backdoor Firmware

Terdapat 2 (dua) kerentanan Linux pada *firmware motherboard Gigabyte* yang digunakan pada PC *gaming* dan komputer yang memiliki *high performance*. Kerentanan ini diketahui sebagai CVE-2023-32629 dan CVE-2023-2640, kerentanan tersebut memungkinkan pengguna lokal yang tidak memiliki hak istimewa yang lebih tinggi dan berpotensi mengeksekusi kode yang sewenang-wenang. Para peneliti dari Eclypsium menemukan bahwa mekanisme tersembunyi di dalam *firmware*, dengan tujuan pembaruan, diimplementasikan secara tidak aman, sehingga rentan dieksploitasi untuk instalasi *malware.*

Referensi: https://idsirtii.or.id/pustaka.html

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

ASISTENSI TANGGAP INSIDEN SIBER

7

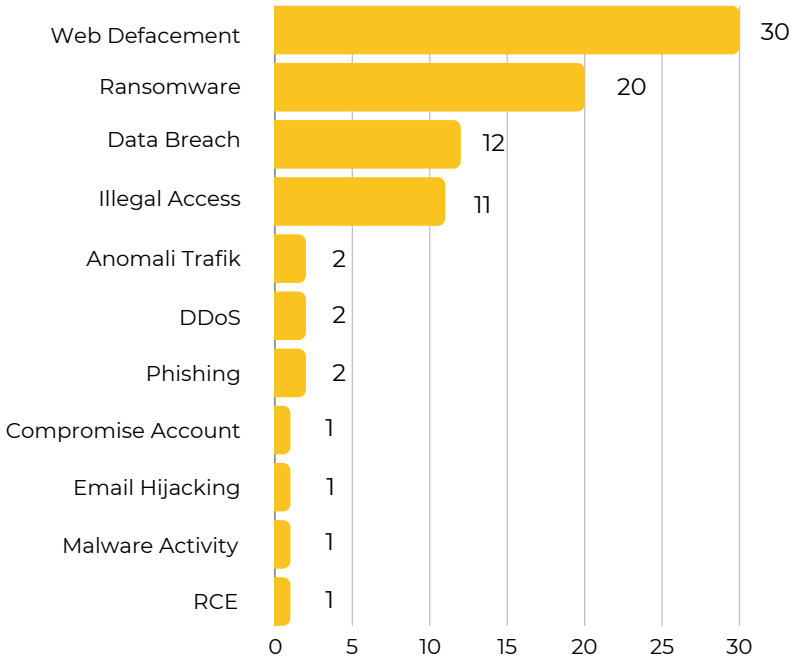
ASISTENSI TANGGAP INSIDEN SIBER

83
asistensi tanggap insiden siber

BSSN telah melaksanakan 83 kegiatan asistensi tanggap insiden siber di 74 *stakeholder*. Adapun terdapat 3 (tiga) kategori pelaksanaannya sebagai berikut:

HANDLE BSSN	KOLABORASI	HANDLE PSE/CSIRT ORGANISASI
29 Insiden	23 Insiden	31 Insiden
Proses asistensi penanganan insiden siber dilakukan secara penuh oleh BSSN.	Proses asistensi penanganan insiden siber dilakukan oleh PSE/CSIRT yang bekerja sama dengan BSSN	Proses asistensi penanganan insiden siber yang dilakukan secara penuh oleh PSE/CSIRT.

Berikut merupakan klasifikasi insiden dan sektor yang dilakukan Layanan Asistensi Tanggap Insiden Siber:



Sektor	Jumlah
Adm. Pemerintahan	59
ESDM	6
Kesehatan	5
Keuangan	5
Lainnya	4
Transportasi	3
TIK	1

Adapun dari 83 insiden yang diasistensi ditemukan adanya 3 (tiga) insiden dengan kasus terbanyak di tahun 2023 yaitu *Web Defacement*, *Ransomware*, dan *Data Breach*.

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

LESSON LEARNED TOP 3 INSIDEN SIBER

8

INSIDEN
WEB DEFACEMENT

Serangan *web defacement* adalah tindakan yang dilakukan oleh pihak yang tidak sah untuk mengeksploitasi situs web dengan cara merusak, melakukan modifikasi, atau menghapus isi pada web. Pada tahun 2023, kasus *web defacement* paling banyak terjadi di bulan Januari dengan sektor terbanyak yaitu Administrasi Pemerintah. Dalam kaitannya pada insiden judi *online* situs web pemerintah dijadikan target dengan memanfaatkan kerentanan yang memungkinkan *threat actor* menyisipkan *script* yang dapat menampilkan tampilan judi *online* sehingga dapat mempengaruhi reputasi instansi dan kepercayaan masyarakat terhadap pelayanan yang diberikan oleh pemerintah. Selain itu pada dampak yang lebih parah, instansi korban dapat mengalami pencurian data dan pengambilalihan hak akses secara penuh.

TOP 3 ATTACK VECTOR

Active Scanning (T1595)

Pihak yang mengancam melakukan pemindaian untuk mengumpulkan informasi yang dapat dieksploitasi dari sistem yang menjadi target.

Compromised Account (T1586)

Pihak yang mengancam menggunakan akun-akun yang sudah diretas oleh perangkat lunak pencuri *malware* untuk mengakses sistem.

Exploit Public-Facing Application (T1190)

Pihak yang mengancam menggunakan kerentanan yang ada di situs web untuk melakukan berbagai percobaan serangan seperti Injeksi SQL, Unggah Berkas, XSS, dan sejenisnya.

LESSON LEARNED
WEB DEFACEMENT

01

Melakukan *Security Hardening* Pada OS Server

Tindakan ini bertujuan untuk mengurangi potensi serangan terhadap sistem operasi (OS) server, baik pada *server* yang sedang aktif digunakan, sehingga membuatnya lebih sulit bagi para peretas untuk melakukan serangan terhadap *server* tersebut. Langkah ini juga termasuk dalam penerapan perlindungan tambahan seperti *antivirus* atau *End-Point Detection and Response* (EDR) pada *server*.

02

Meningkatkan Keamanan dan Manajemen Autentikasi Pengguna yang Mengakses *Server* Secara *Remote*

Pengguna disarankan untuk membatasi akses pada autentikasi akun SSH dengan mengonfigurasi daftar putih/hitam pengguna SSH, menyesuaikan *port* SSH (sebaiknya tidak menggunakan *port* umum), menerapkan sertifikat untuk autentikasi SSH, membatasi pengguna yang memiliki hak akses *root*, serta melakukan peninjauan akses pengguna secara teratur.

03

Pemantauan Aktivitas Situs

Mekanisme pemantauan aktivitas situs penting dimiliki oleh organisasi untuk mendeteksi perubahan tak terduga pada situs web. Hal ini dapat dilakukan dengan memperhatikan tanda-tanda aktivitas yang mencurigakan, organisasi dapat bertindak lebih cepat untuk mengatasi serangan *web defacement*.

04

Pengelolaan Akses

Sistem diharapkan memiliki mekanisme pengelolaan akses yang bertujuan untuk membatasi izin hak akses pengguna sesuai dengan peran dan tugas pengguna tersebut.

05 **Kesadaran Pengguna**

Pengguna diharapkan memiliki kesadaran akan bahaya ancaman keamanan siber sehingga waspada untuk tidak mengklik tautan atau lampiran mencurigakan yang berpotensi dapat menyebabkan serangan *web defacement*.

06 **Menangani Kelemahan yang Ada dan Mengaktifkan Kembali Layanan Web**

Setelah analisis dilakukan dan ditemukan celah keamanan serta *file* berbahaya, langkah-langkah penanggulangan perlu dilakukan seperti penghapusan *file* berbahaya, penggantian index.php dengan yang baru, serta penerapan *patch* terbaru pada aplikasi agar layanan situs web dapat kembali berjalan normal. Langkah selanjutnya, perlu dilakukan pemulihan layanan situs web guna mencegah gangguan terhadap proses bisnis yang sedang berlangsung.

07 **Melakukan Penguatan Keamanan pada CMS yang Sedang Digunakan**

Menerapkan *best practice* terhadap keamanan CMS dan secara teratur melakukan pembaruan pada CMS. Tujuannya adalah untuk mengurangi peluang serangan melalui celah keamanan pada CMS yang dapat dimanfaatkan oleh *threat actor*.

INSIDEN RANSOMWARE

Kejadian *ransomware* merupakan insiden siber yang dipicu oleh *malware* yang menyerang perangkat, melakukan enkripsi pada data yang ada di dalamnya, dan juga mencuri data dengan tujuan untuk mengintimidasi korban agar membayar sejumlah tebusan guna mendapatkan kembali akses ke data tersebut. Saat ini, taktik *ransomware* telah berkembang menjadi ekstorsi ganda (*double extortion*), yaitu selain melakukan penyanderaan data melalui enkripsi, pelaku juga mengancam untuk mengungkapkan data sensitif jika tebusan tidak diserahkan oleh pemilik sistem. Berikut adalah Top 3 *ransomware* yang ditemukan pada asistensi tanggap insiden siber:

TOP 3 RANSOMWARE

01 **LockBit 3.0**

LockBit 3.0 yang juga dikenal sebagai "LockBit Black" merupakan hasil pengembangan dari *ransomware* LockBit yang memiliki kemiripan dengan *Ransomware* Blackmatter dan Blackcat. LockBit 3.0 berfungsi sebagai model *Ransomware-as-a-Service* (RaaS) dan varian *ransomware* berbasis afiliasi. Menurut laporan Cyberint, sepanjang tahun 2023 terdapat lebih dari 743 serangan *Ransomware* LockBit 3.0 di seluruh dunia. Di Indonesia, kelompok ini telah melakukan serangan pada beberapa perusahaan dan perbankan.

---

02 **Mallox**

Mallox adalah varian *ransomware* yang mengincar sistem Microsoft (MS) Windows. Varian ini aktif sejak Juni 2021 dan mengalami peningkatan aktivitas hampir 174% pada tahun 2023. *Ransomware* ini cukup dikenal karena memanfaatkan server MS-SQL yang tidak aman sebagai vektor penetrasi untuk meretas jaringan korban.

---

03 **BianLian**

Ransomware BianLian pertama kali muncul pada Juni 2022 dan terus berkembang hingga tahun 2023. *Ransomware* tersebut menyusup ke dalam sistem korban dengan menggunakan kredensial *Remote Desktop Protocol* (RDP) yang sah. Setelah mendapatkan akses, kelompok ini menggunakan utilitas sumber terbuka dan *script* baris perintah untuk mengekstrak data korban sebagai data yang disandera melalui *File Transfer Protocol* (FTP), Rclone, atau Mega.

TOP 5 ATTACK VECTOR

Exploiting Remote Desktop Protocol (T1021.001)

Konfigurasi yang salah (*misconfiguration*) pada *Remote Desktop Protocol* (RDP) menjadi kerentanan yang sering kali dimanfaatkan oleh kelompok *ransomware* untuk mendapatkan akses tanpa izin ke dalam sistem. Setelah berhasil masuk, *threat actor* dapat melakukan *lateral movement* ke seluruh jaringan, meningkatkan hak akses, dan menyebarkan muatan *ransomware* dengan lebih efektif. Dalam rangka mengurangi risiko serangan, pengelola sistem dapat menerapkan password yang kuat, otentikasi multi-faktor, dan pengaturan batasan akses.

Phishing Campaigns (T1566)

Kelompok *ransomware* masih menggunakan kampanye *phishing* sebagai metode utama untuk memperoleh akses awal ke jaringan target. Metode yang dilakukan melalui pengiriman email atau pesan yang mengelabui, pengguna yang kurang waspada berhasil dikelabui oleh *threat actor*. Tingkat kewaspadaan dan kesadaran pengguna memegang peran kunci dalam mengurangi risiko terkait dengan upaya *phishing* ini.

Software Vulnerabilities (T1203)

Threat actor memanfaatkan kerentanan perangkat lunak sebagai salah satu untuk menyebarkan *ransomware* dengan cara menargetkan perangkat lunak yang belum diperbaiki atau usang untuk mendapatkan akses di lingkungan target. Pembaruan perangkat lunak secara secara berkala dan penilaian kerentanan secara teratur perlu dilakukan untuk meminimalkan risiko serangan *ransomware* yang berhasil.

Supply Chain Attacks (T1195)

TTP dalam serangan ransomware memiliki tren untuk menargetkan *supply chain*, mengompromi vendor atau pihak ketiga yang terpercaya untuk mendapatkan akses ke jaringan klien. Peningkatan keamanan pada *supply chain* dan evaluasi terhadap *best practice* keamanan siber yang diterapkan oleh vendor menjadi hal yang krusial untuk mengurangi risiko ini.

Living-off-the-Land Techniques (T1218)

Teknik *Living-off-the-Land* memanfaatkan alat dan proses yang sah pada jaringan korban untuk melakukan kegiatan berbahaya. Teknik ini berpotensi membuat *threat actor* tidak terdeteksi oleh sistem keamanan dalam waktu yang lama sehingga dapat melakukan proses eksfiltrasi data dari perangkat korban.

LESSON LEARNED
RANSOMWARE

01

Pembaruan Sistem dan Perangkat Lunak

Pembaruan sistem operasi dan perangkat lunak secara rutin perlu dilakukan untuk memitigasi risiko *ransomware*. Pembaruan tersebut tidak hanya menyediakan fitur baru, tetapi juga memperbaiki kerentanan keamanan yang dapat dimanfaatkan oleh *threat actor*.

02

Pelatihan Security Awareness Kepada Pengguna

Pelatihan *security awareness* kepada pengguna adalah langkah penting yang perlu dilakukan terhadap berbagai komponen masyarakat dari level individu hingga organisasi untuk mengenali modus penyebaran serangan *ransomware*.

03

Penggunaan Perangkat Keamanan dan Deteksi Ancaman Siber

Firewall, *antivirus*, *anti-malware,* sistem monitoring pada jaringan dan *endpoint* sebagai solusi keamanan sehingga dapat membantu mendeteksi dan mencegah ransomware sebelum dapat merusak sistem. Solusi ini juga sering kali dilengkapi dengan teknologi heuristik dan pembaruan secara otomatis untuk mengatasi ancaman yang terus berkembang.

04

Pengelolaan Hak Akses dengan Bijak

Prinsip manajemen izin hak akses perlu diterapkan terhadap sistem sesuai dengan peran dan tugas pengguna, sehingga dapat membantu mencegah penyebaran *ransomware* melalui eksploitasi akun pengguna yang terkompromi.

05

Backup dan Pemulihan Data yang Teratur

Pencadangan data secara teratur dan menyimpannya di lokasi yang aman merupakan langkah penting untuk mengurangi dampak serangan *ransomware*. Melalui pemulihan data yang teratur, organisasi dapat mengembalikan sistem dan informasi yang terpengaruh ke keadaan normal tanpa harus membayar tebusan kepada *threat actor*.

06

Menguatkan Keamanan *Supply Chain*

Peningkatan keamanan dalam *supply chain* melibatkan evaluasi dan peningkatan keamanan vendor maupun pihak ketiga yang berinteraksi dengan organisasi. Oleh karena itu, vendor/pihak ketiga juga perlu dipastikan untuk melakukan implementasi *best practice* keamanan siber dalam rangka mencegah serangan *ransomware*.

07

Mengamankan *Remote Desktop Protocol* (RDP)

Keamanan RDP dapat dilakukan dengan menerapkan penggunaan password yang kuat, otentikasi multi-faktor, dan pembatasan akses ke koneksi RDP dapat membantu melindungi jaringan dari serangan *ransomware* yang dapat memanfaatkan lemahnya protokol jarak jauh ini.

INSIDEN
DATA BREACH

Kejadian kebocoran data (*data breach*) merupakan situasi dalam ruang siber di mana informasi atau data rahasia yang dimiliki oleh suatu organisasi diakses dan diungkap kepada publik oleh pihak yang mengancam, tanpa sepengetahuan pemilik sistem. Data yang diambil oleh *threat actor* biasanya termasuk informasi yang bersifat sangat pribadi, seperti *Personal Identifiable Information* (PII), data yang sangat rahasia bagi individu maupun organisasi, dan informasi lainnya yang semestinya hanya diketahui oleh pihak yang berwenang.

SKEMA TERJADINYA INSIDEN

Information Gathering

Threat actor akan menentukan sasaran, melakukan pemindaian untuk mencari informasi dalam sistem yang dapat dieksploitasi. Selain itu, *threat actor* juga akan berupaya mendapatkan data pengguna yang dapat digunakan sebagai sasaran dalam serangan *phishing*.

Attack

Threat actor menggunakan informasi sistem yang telah diperoleh untuk mengeksploitasi sistem dan berusaha untuk tetap ada serta bahkan melakukan *lateral movement* ke *administrator*, atau dengan mengirimkan serangan *phishing* kepada pengguna yang sudah dikenali sebelumnya untuk menyebarkan *malware*.

Exfiltration Data

Setelah berhasil masuk ke sistem, *threat actor* akan mengakses dan mengekspor basis data atau dokumen penting lainnya. Informasi tersebut juga diperjual belikan di *darkweb*.

TOP 5 ATTACK VECTOR

System Time Discovery (T1124)

Threat actor dapat menemukan waktu sistem dan/atau zona waktu untuk menjadwalkan tugas untuk menjalankan program secara terjadwal, untuk melakukan eksekusi jarak jauh, untuk memperoleh hak istimewa sistem, atau untuk menjalankan proses di bawah konteks akun tertentu.

Exploit Public-Facing Application (T1190)

Pihak yang mengancam menggunakan kerentanan yang ada di situs web untuk melakukan berbagai percobaan serangan seperti Injeksi SQL, Unggah Berkas, XSS, dan sejenisnya.

Password Policy Discovery (T1201)

Threat actor mencoba menemukan kebijakan yang diterapkan dalam organisasi untuk membuat daftar password yang akan dicoba untuk serangan *brute force* atau jenis serangan lainnya.

External Remote Services (T1133)

Threat actor menggunakan layanan *remote* seperti VPN untuk terhubung ke sumber daya jaringan perusahaan internal dari lokasi eksternal.

Exfiltration Over Command and Control Channel (T1041)

Threat actor menggunakan *backdoor* untuk melakukan kendali jarak jauh supaya dapat melakukan transfer file ke sistem lokal *threat actor*.

LESSON LEARNED
DATA BREACH

01

Menetapkan Kebijakan Penggunaan password yang Kuat

Pemilik sistem diharapkan dapat menerapkan kebijakan penggunaan password yang kuat dan secara berkala mengganti password. Tujuannya adalah untuk mengurangi risiko akun yang diretas serta menghambat serangan *brute force*.

02

Melakukan Edukasi Terhadap Pengguna Sistem

Pengguna menjadi sasaran terlemah dalam keamanan jaringan yang bisa dieksploitasi oleh *threat actor* sebagai *entry point* ancaman keamanan siber. *Threat actor* dapat menggunakan rekayasa sosial atau *phishing* untuk menipu korban. Oleh karena itu, pengguna sistem disarankan untuk tidak membuka tautan, *file*, *email*, atau URL dari sumber yang tidak dikenal, serta menghindari mengakses situs ilegal.

03

Melakukan Audit Akun Sistem dan Aplikasi

Akun pengguna menjadi faktor penting dalam situasi kebocoran data karena pelaku ancaman menggunakan akun yang telah diretas untuk mendapatkan akses yang sah ke sistem dan melakukan *lateral movement* ke sistem lainnya. Oleh karena itu, perlu untuk secara rutin meninjau daftar akun pengguna.

04

Menonaktifkan Port Layanan yang Tidak Digunakan

Threat actor sering memanfaatkan layanan sistem atau *port* sebagai *entry point* ke sistem. Layanan sistem seperti SMB, SSH, FTP, dan RDP sering kali dimanfaatkan oleh mereka sebagai akses awal dan bahkan untuk melakukan *lateral movement*. Oleh karena itu, penting untuk menonaktifkan layanan yang tidak digunakan.

05

Memvalidasi Data Terkait Insiden yang Terjadi

Dalam beberapa insiden yang terjadi, diketahui bahwa data yang bocor oleh *threat actor* merupakan hasil penggabungan dengan data lain dengan penambahan beberapa bidang basis data. Oleh karena itu, pemilik sistem perlu melakukan verifikasi terhadap data yang bocor oleh *threat actor* untuk memastikan keakuratannya.

06

Melakukan Penguatan Keamanan atau Pembaruan Pada Sistem yang Terdampak

Kerentanan yang berhasil dieksploitasi oleh *threat actor* sebagai *entry point* sering terjadi pada berbagai insiden. Hal tersebut dikarenakan masih terdapat sistem atau aplikasi yang *outdated* serta belum adanya perimeter keamanan yang mumpuni. Penambahan sistem deteksi pada sisi jaringan dan endpoint akan memperkuat keamanan dari sistem terdampak.

Organizations have a responsibility to protect the data they collect from their customers and employees.

- European Union General Data Protection Regulation (GDPR)

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

PENGAMANAN SIBER PADA EVENT NASIONAL DAN INTERNASIONAL

9

EVENT DI 2023

BSSN berperan aktif di **6 *event* internasional** seperti F1H2O, MOTOGP, KTT ASEAN, KTT AIS, Piala Dunia U-17 dan **7 *event* nasional seperti** Pemilu, Pengamanan HUT RI, Seleksi Penerimaan POLRI, Kongres Ikatan Notaris, Pengamanan Sidang Tahunan MPR-DPR, Satuan Tugas Pelindungan Data, dan Panitia Seleksi ASN dalam menjaga keamanan siber melalui pengujian sistem, pemasangan alat deteksi dan monitoring, tanggap insiden dan *digital forensic incident response*. Proses ini mencakup dari fase pra pelaksanaan hingga *recovery pasca-event*, termasuk perbaikan celah keamanan yang terdeteksi.

01 F1H2O

Operasi pengamanan siber F1H20 di Danau Toba berlangsung dari 18 hingga 26 Februari 2023, mencakup pemasangan perangkat monitoring, ITSA, pemantauan kebocoran data di *darkweb*, penerapan *honeypot*, forensik digital, dan *compromise assessment*. Operasi ini bertujuan untuk menanggulangi potensi insiden siber dan mengatasi ancaman yang teridentifikasi selama kegiatan F1H20.

02 MOTOGP

Operasi pengamanan MOTOGP Mandalika berlangsung dari 6 hingga 15 Oktober 2023. Tim Satgas telah melaksanakan rangkaian kegiatan pengamanan di antaranya yaitu pemasangan NIDS, pemantauan anomali trafik, identifikasi aset TIK/sistem elektronik, ITSA dan *hardening* pada aset TIK yang telah teridentifikasi dan melakukan pemetaan kerentanan aset sebagai upaya untuk penanganan potensi insiden siber yang mungkin terjadi, serta melakukan mitigasi terhadap indikasi ancaman siber ditemukan selama pelaksanaan rangkaian kegiatan MOTOGP.

03 KTT ASEAN 42

Kegiatan Pengamanan Rangkaian KTT ASEAN Ke-42 di Labuan Bajo dilaksanakan pada tanggal 3 s.d 14 Mei 2023. BSSN melakukan Pengamanan Siber dan Sandi pada 3 Rangkaian event puncak KTT ASEAN Ke-42 di Labuan Bajo yaitu, *Committee of Permanent Representatives* (CPR) dan ASEAN *Senior Officials' Meeting* (SOM), ASEAN *Foreign Ministers' Meeting* (AMM) dan *Main event* KTT ASEAN 42. Tim satgas melakukan beberapa kegiatan seperti pemasangan NIDS, melakukan ITSA terkait KTT ASEAN Ke-42. Kegiatan pengamanan tersebut dilaksanakan sebagai upaya untuk penanganan potensi insiden siber yang mungkin terjadi, serta melakukan mitigasi terhadap indikasi ancaman siber ditemukan selama pelaksanaan rangkaian kegiatan KTT ASEAN Ke-42.

04 KTT ASEAN 43

Kegiatan Pengamanan Rangkaian KTT ASEAN Ke-43 di Jakarta dilaksanakan pada tanggal 3 s.d 8 September 2023. Tim Satgas melakukan beberapa kegiatan seperti pengujian celah kerentanan sistem, melakukan penelusuran indikasi kerentanan sistem, melakukan pemantauan anomali trafik jaringan dan mengirimkan dokumen notifikasi indikasi insiden keamanan siber. Kegiatan pengamanan tersebut dilaksanakan sebagai upaya untuk penanganan potensi insiden siber yang mungkin terjadi, serta melakukan mitigasi terhadap indikasi ancaman siber ditemukan selama pelaksanaan rangkaian kegiatan KTT ASEAN Ke-43.

05 Konferensi Tingkat Tinggi Archipelagic and Island States Forum (KTT AIS)

Kegiatan Pengamanan Event Nasional Konferensi Tingkat Tinggi *Archipelagic and Island States Forum* (KTT AIS) dilaksanakan pada tanggal 29 September s.d 14 Oktober 2023 di Bali. Tim Satgas telah melaksanakan rangkaian kegiatan pengamanan di antaranya yaitu pembentukan mini SOC, identifikasi aset TIK/sistem elektronik, ITSA dan *hardening* pada aset TIK yang telah teridentifikasi, monitoring trafik jaringan, menyediakan platform pertukaran informasi dini ancaman siber kepada *stakeholder* terkait, dan penempatan personil pada *venue* kegiatan sebagai upaya untuk penanganan potensi insiden siber yang mungkin terjadi, serta melakukan mitigasi terhadap indikasi ancaman siber ditemukan selama pelaksanaan rangkaian kegiatan KTT AIS Forum 2023.

06 Piala Dunia U-17

Kegiatan Pengamanan Piala Dunia U-17 dilakukan dalam rangka perwujudan peran serta BSSN dalam rangka menjaga keamanan dan kedaulatan siber, serta mendukung kesuksesan Penyelenggaraan FIFA U-17 World Cup 2023 di Surakarta, maka BSSN membentuk Tim Operasi Pengamanan Siber dan Sandi yang menjalankan fungsi identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pengendalian informasi, dan operasi sandi.

07 PEMILU

Operasi Pengamanan Pemilu Instansi Pusat, yang berlangsung dari Februari hingga Desember 2023, mencakup sejumlah langkah seperti ITSA, Asistensi Proteksi, *Monitoring* Anomali Trafik, dan pemasangan Sensor EDR. Selain itu, operasi serupa juga dilaksanakan di KPU Daerah pada Oktober-Desember 2023, PPLN pada November 2023, serta kegiatan konsolidasi dan uji coba *cyberdrill* pada November-Desember 2023, semua bertujuan untuk mengatasi potensi insiden dan mengurangi ancaman siber selama proses Pemilu.

08 Pengamanan HUT RI Tahun 2023

Badan Siber dan Sandi Negara (BSSN) terlibat dalam kegiatan Pengamanan Hari Ulang Tahun Republik Indonesia Tahun 2023 yaitu dalam kegiatan Information Technology Security Assessment (ITSA) pada Aplikasi Pandang Istana yang digunakan sebagai media pendaftaran kehadiran pada acara HUT RI di Istana Negara, monitoring keamanan, Cyber Threats Intelligence (CTI), dan forensik digital sebagai upaya pencegahan dan penguatan terhadap ancaman siber selama kegiatan Hari Ulang Tahun Republik Indonesia Tahun 2023.

09 Seleksi Penerimaan Anggota POLRI

Seleksi penerimaan anggota POLRI merupakan rangkaian kegiatan yang diselenggarakan Polri, dalam rangka penerimaan anggota Polri baik dari tingkat pusat maupun tingkat daerah. Polri dalam hal ini berkolaborasi dengan BSSN selaku pengawas eksternal yang melakukan pengamanan aset saat kegiatan berlangsung. Tim BSSN yang bertugas tidak hanya melakukan pengamanan kegiatan ujian penerimaan anggota POLRI, namun juga pengamanan ujian kenaikan jenjang dan pangkat bagi anggota POLRI

10 Kongres Ikatan Notaris Indonesia

Tim BSSN ikut terlibat pada pengamanan kegiatan Kongres Ikatan Notaris Indonesia dengan melakukan *monitoring* menggunakan XDR yang terpasang pada 5 *Server* dan menggunakan AWS *Security*. Hasil *monitoring* menunjukkan bahwa tidak terdapat aktivitas anomali yang terdeteksi. Selain itu, Tim IR bersama kominfo juga melakukan *hashing* untuk memberikan jaminan integritas pada hasil *voting*. Tim melakukan instalasi tambahan EDR pada *server Hash Signing* sehingga total yang dipasangkan EDR menjadi 5 *Server* yang akan tetap terpasang sampai masa tenggang selesai.

11 Pengamanan Sidang Tahunan MPR-DPR Tahun 2023

Pengamanan Sidang Tahunan MPR-DPR berlangsung dari tanggal 7 hingga 16 Agustus 2023. Tim pengamanan Sidang Tahunan MPR-DPR ini terdiri dari Tim Pengendalian dan Pengamanan Informasi, Tim ITSA, Tim Monitoring, Tim Insiden Respon, dan Tim internal DPR RI yang standby sebelum dan pada saat hari H pelaksanaan sidang. Rangkaian kegiatan pengamanan yang dilakukan diantaranya yaitu pemantauan dan pengiriman notifikasi anomali trafik, pelaksanaan ITSA pada aset TIK/sistem elektronik sebelum pelaksanaan sidang, dan monitoring kanal sosial media yang dilakukan untuk *streaming* pelaksanaan Sidang Tahunan MPR-DPR Tahun 2023. Secara keseluruhan acara sidang tahunan MPR-DPR berjalan dengan baik dan tidak terdapat kendala maupun serangan siber yang terjadi selama sidang berlangsung.

12 Satuan Tugas Pelindungan Data

Satuan tugas pelindungan data BSSN adalah bentuk nyata upaya BSSN dalam melaksanakan pelindungan data. Sepanjang tahun 2023, Satgas Perlindungan Data BSSN melakukan melakukan upaya pelindungan data pada sistem elektronik di 23 (dua puluh tiga) instansi pemerintah pusat. Upaya tersebut berhasil berhasil menurunkan 24% tingkat kerentanan pada sistem elektronik pemerintah.

13 Panitia Seleksi ASN

BSSN terlibat dalam kegiatan Pengamanan Seleksi Aparatur Sipil Negara Badan Kepegawaian Negara dilaksanakan (Seleksi ASN BKN) yang diselenggarakan pada Tahun 2023. Operasi ini melibatkan personil dari Direktorat Operasi Keamanan Siber, Direktorat Operasi Sandi, dan Pusat Sertifikasi Teknologi Keamanan Siber dan Sandi. Rangkaian operasi yang telah dilakukan yaitu meliputi ITSA, monitoring keamanan, penerapan modul kripto (KMS dan OTP), uji petik pengamanan titik lokasi, *Cyber Threats Intelligence* (CTI), dan forensik digital sebagai upaya pencegahan dan penguatan terhadap ancaman siber selama kegiatan Pengamanan Seleksi Aparatur Sipil Negara Badan Kepegawaian Negara.

KOLABORASI & KERJA SAMA

10

KOLABORASI NASIONAL

Dalam menjaga keamanan siber, BSSN tidak dapat bekerja sendiri dan memerlukan kolaborasi menyeluruh. Kolaborasi dan partisipasi dari berbagai pihak sangat diperlukan dalam menciptakan keamanan siber nasional. Peningkatan serangan siber dari tahun ke tahun membuat berbagai sektor saling berkolaborasi meningkatkan keamanan siber secara luas. Dalam mewujudkan keamanan siber dengan cakupan yang lebih luas, BSSN melalui layanan yang ada melakukan kolaborasi dengan sektor pemerintah, berbagai instansi dan pemangku kepentingan lainnya, serta aktif mengikuti forum-forum Nasional maupun Internasional untuk meningkatkan keamanan siber sebagai upaya untuk menjaga ruang siber di Indonesia.

01 F5 API Hackathon

Merupakan kompetisi yang diselenggarakan oleh F5 pada tanggal 25 – 26 September 2023, untuk menyelesaikan masalah pada API. Kegiatan ini mengundang beberapa instansi pemerintah. Kegiatan dengan *workshop* kerentanan dan teknologi F5, kemudian dilanjutkan dengan Kompetisi *Hackathon*.

02 Capture the Flag BPK 2023

Merupakan rangkaian kegiatan yang diselenggarakan oleh BPK, dalam rangka HUT BPK RI ke 77. Kegiatan ini diikuti oleh pegawai BPK dari seluruh indonesia yang kemudian diambil 5 tim terbaik untuk melaksanakan final di Jakarta, adapun BSSN dilibatkan dalam pembuatan soal.

03

Forum Komunikasi dan Koordinasi NAT-CSIRT 2023

BSSN bergabung dengan berbagai komunitas keamanan siber berskala internasional, salah satunya yaitu *The Organization of The Islamic Cooperation - Computer Emergency Response Teams* (OIC- CERT).

BSSN telah mengadakan kegiatan *sharing session* sebagai upaya peningkatan kesadaran keamanan siber kepada anggota-anggota OIC-CERT. Forum Komunikasi dan Koordinasi NAT-CSIRT merupakan wujud dari salah satu penyediaan wadah kolaborasi dan koordinasi serta pelaksanaan layanan bimbingan teknis penanganan insiden pada CSIRT Organisasi pada Tahun 2023.

Tujuan kegiatan ini adalah untuk menambah pengetahuan dan wawasan mengenai kegiatan tanggap insiden pada para peserta masing-masing CSIRT sehingga mampu secara mandiri untuk melakukan penanganan insiden dan juga aktif dalam melakukan berbagi informasi keamanan siber.

KOLABORASI INTERNASIONAL

01 Cyber SEA-Games 2023

Cyber SEA Games 2023 merupakan kegiatan lomba *Capture the Flag* (CTF) yang diikuti oleh 10 negara-negara ASEAN. Kegiatan ini diselenggarakan pada tanggal 8 hingga 11 November 2023. Kegiatan Cyber SEA Game 2023 yang merupakan perlombaan CTF diikuti oleh Tim BSSN sebagai perwakilan dari Indonesia. Tim BSSN meraih posisi ke-5 dari 10 negara dengan total poin akhir 4306 serta menyelesaikan seluruh soal yang ada.

02 UNODC Ransomware Investigation Training

UNODC menyelenggarakan pelatihan *Ransomware Training* di Bandung pada tanggal 27-29 Maret 2023. Pelatihan ini bertujuan untuk membangun dan berbagi pengalaman dalam investigasi kejahatan siber serta metode investigasi terbaru yang terkait dengan kejahatan-keajahatan yang melibatkan penipuan online seperti tilang otomatis, penipuan email bisnis, dan serangan siber (serangan *ransomware*). Pelatihan ini diikuti oleh perwakilan dari beberapa instansi yang terlibat dalam investigasi penanganan serangan *ransomware* di Indonesia seperti POLRI, PPATK, Kejaksaan, dan BSSN.

03 UNODC Regional Ransomware Investigation Training Exercise

Pelatihan UNODC Regional *Ransomware Investigation Training* yang telah dilaksanakan pada 25 s.d. 29 Juli 2023 di Holiday Inn & Suites Makati, Manila, Filipina. Pemateri pada Pelatihan UNODC Regional *Ransomware Investigation Training* adalah tim dari UNODC (*United Nations Office on Drugs and Crime*). Kegiatan Pelatihan UNODC Regional *Ransomware Investigation Training* berisi serangkaian kegiatan pengayaan informasi serta atribusi data insiden dan *threat actor* termasuk metode pendanaan yang digunakan oleh *threat actor ransomware* (*follow the money*).

04 CRDF GLOBAL ThreatSpace Workshop: Cyber Capacity Building for Highly Trafficked Ports

Pada 22-25 Agustus 2023, BSSN berpartisipasi dalam *workshop* yang diselenggarakan oleh CRDF Global yang berkolaborasi dengan Mandiant Inc di Manila, Filipina, yang didukung oleh Departemen Luar Negeri AS dengan topik workshop "ThreatSpace Workshop: Cyber Capacity Building for Highly Trafficked Ports". Kegiatan ini diikuti oleh 33 praktisi keamanan siber dari 6 negara Indo-Pasifik yang bertujuan untuk memberdayakan peserta dengan pengetahuan dan keterampilan untuk mengatasi ancaman siber yang dapat mengganggu perdagangan. *Workshop* ini sebagai bagian dari upaya untuk meningkatkan kecerdasan dan keamanan, keterampilan praktis, dan pelatihan berbasis teknologi untuk meningkatkan kemampuan respon ancaman siber.

05 UAE Cybersecurity Council and EXPO2020 Dubai – Cyber Protective Shield Global Cyber Exercise

Liaison Officer sekaligus menjabat sebagai ketua IDSIRTII/CC BSSN menghadiri OIC-CERT *Physical Board Meeting* Ke-1 tahun 2023 yang merupakah salah satu dari rangkaian GISEC 2023, yaitu pameran dan konferensi keamanan siber terbesar di Timur Tengah & Afrika (MENA), yang dijadwalkan berlangsung dari 14 hingga 16 Maret 2023 di Dubai World Trade Centre, Uni Emirat Arab. Kegiatan ini sebagai acara penghubung terbesar untuk Komunitas Keamanan Siber Timur Tengah dan Afrika, kegiatan ini dihadiri oleh lebih dari 30.000 orang dari institusi pemerintah dan perusahaan global setiap tahunnya serta mengumpulkan 300 merek keamanan siber dari lebih dari 100 negara.

06 Elections and Cybersecurity: Protecting Indonesia's Election in 2024 and Beyond

US Embassy menyelenggarakan forum diskusi terkait *Elections and Cybersecurity: Protecting Indonesia's Election in 2024 and Beyond* pada tanggal 7 – 9 November 2023 di Bali.

07 OIC-CERT Annual Meeting and Cyber Drill

Memasuki kuartal ke-4 tahun 2023, IDSIRTII/CC BSSN menghadiri kegiatan OIC-CERT *Board Meeting* yang merupakan bagian dari kegiatan Regional *Cyber Security Week.* Kegiatan ini diinisiasi dan didanai oleh *Cyber Security Council* - Uni Emirat Arab dan dilaksanakan di Abu Dhabi pada 8-12 Oktober 2023. Pada kegiatan ini juga dilaksanakan *cyber drill* secara tatap muka di mana ITU-ARCC yang berbasis di Oman mencetak lima Rekor Dunia Guinness selama 11th *Regional Cybersecurity Week* dari 9 hingga 12 Oktober di Abu Dhabi. Rekor-rekor tersebut termasuk simulasi serangan siber terluas dengan melibatkan lebih dari 50 ahli; kontes simulasi serangan siber terbesar yang diikuti oleh 11 organisasi global; kompetisi keamanan siber dengan perwakilan dari lebih dari 30 negara, termasuk Indonesia, yang mencetak rekor dalam keragaman peserta; simulasi ancaman berbasis kota terbesar dalam keamanan siber; dan jumlah terbanyak warga negara yang berpartisipasi dalam sebuah kuliah untuk menyebarkan kesadaran tentang keamanan siber, dengan lebih dari 500 peserta.

08 OIC-CERT 5G Security Framework, Cloud Security, and the Blockchain Working Group

Pada Desember 2023, BSSN berpartisipasi dalam OIC-CERT *Working Group Workshop* yang diselenggarakan oleh OIC-CERT yang bekerja sama dengan Huawei di Dongguan dan Shenzhen, China. Adapun topik workshop yang diangkat yaitu 5G *Security Framework, Cloud Security Framework, AI Security,* dan *Supply Chain Security*. Kegiatan ini diikuti oleh perwakilan dari 7 negara *board member* OIC-CERT dengan masing-masing mengirimkan 3 personel untuk mengikuti kegiatan tersebut. *Workshop* ini dilakukan untuk diskusi bersama dari hasil *working group* yang telah dibuat pada tahun 2023, perluasan pemahaman terkait tren terbaru di dunia keamanan siber, dan menentukan rencana *working group* pada tahun 2024.

09 Red Hat Ansible and Trellix XDR Introduction by Ingram Micro

BSSN sebagai Lembaga di sektor Keamanan Siber diundang dalam Red Hat and Trellix *Customer Bootcamp* bersama Ingram Micro di Singapura pada tanggal 4 s.d. 6 Oktober 2023. Pertemuan tersebut memperkenalkan produk-produk terbaru dari Red Hat yaitu otomasi manajemen dan Trellix yaitu XDR (*Extended Detection and Response*) serta fitur-fitur yang lebih dalam untuk memberikan gambaran operasional teknis kepada undangan, serta menunjukkan kondisi keamanan siber di Indonesia secara umum dari fitur-fitur XDR yang diperkenalkan.

10 International Law Enforcement Academy (ILEA) DarkWeb Investigation and Cryptocurrency Investigative

Kegiatan pelatihan *Cyber DarkWeb and Virtual Currency Investigate Workshop* diadakan oleh ILEA dan dilaksanakan di Bangkok, Thailand pada Desember 2023. Pelatihan ini diikuti oleh beberapa negara di Asia Tenggara yaitu Indonesia, Malaysia, Singapura, Thailand, Filipina, Kamboja, Vietnam, Korea Selatan, dan Cina. Kegiatan ini bertujuan untuk membangun pengetahuan dan kapasitas investigasi yang melibatkan penggunaan *Darknet* dan keterlibatan mata uang kripto untuk transaksinya.

11 Regulatory Training Course on Cryptocurrencies “Supervisory Best Practises Workshop”

BSSN turut serta dalam program pelatihan bertajuk UNODC *Regulatory Training Course on Cryptocurrencies* "Supervisory Best Practices Workshop" pada 18-19 Juli 2023. Kegiatan ini bertujuan untuk menghimpun perwakilan dari setiap institusi pemerintah dan aparat penegak hukum untuk memperkuat kerja sama antar organisasi dan meningkatkan pemahaman mengenai standar global dan kerangka regulasi terhadap mata uang virtual. Kegiatan ini mengundang Joey Garcia, pakar *blockchain* internasional yang memberikan pemahaman mengenai konsep *blockchain*, dan bagaimana regulasi terhadapnya dilakukan di negara-negara lain.

12 UNODC Cybercrime Rountable Discussion

Kegiatan ini bertujuan untuk mengumpulkan Badan Penegak Hukum nasional, lembaga keadilan pidana, agensi *regulator*, dan sektor swasta dalam upaya berkelanjutan untuk mendorong dan memperkuat kerja sama intra-agensi serta diskusi guna memahami lebih baik ancaman terkait kejahatan siber, pelanggaran, statistik, pencucian uang termasuk pelanggaran terkait *cryptocurrency* dalam kerangka standar/regulasi virtual global yang ada, serta rekomendasi FATF. Diskusi melibatkan para pihak pada acara tersebut lebih lanjut bertujuan untuk menjadi forum bagi UNODC dan Negara-Negara Anggota dengan poin-poin aksi, sekaligus berbagi informasi mengenai ancaman siber saat ini di negara tersebut, kapasitas untuk menanggulangi ancaman tersebut, praktik terbaik, pelajaran yang dipetik, tantangan, dan langkah-langkah ke depan bersama. Platform kolaboratif ini bertujuan untuk memperkuat ketahanan kolektif terhadap ancaman siber yang terus berkembang dengan memfasilitasi pertukaran pengetahuan dan kerjasama strategis.

13 Microsoft Cybersecurity and Personal Data Protection Roundtable

Bersamaan dengan kunjungan Jean-Philippe Courtois, *Executive Vice President and President, National Transformation Partnerships*, Microsoft Corporation ke Jakarta, Microsoft Indonesia mengundang para pemangku kepentingan untuk berpartisipasi dalam kegiatan Microsoft *Cybersecurity & Personal Data Protection Roundtable* bersama Mr. Jean-Philippe Courtois, guna bertukar ide, gagasan, dan pengalaman terkait pemanfaatan teknologi untuk mendukung perkembangan ekonomi yang berkelanjutan dan inklusif. Berkaitan dengan harapan kerja sama di masa yang akan datang, Microsoft Indonesia saat ini menampung saran dan masukan untuk kemudian ditindaklanjuti, terutama dalam hal penanganan insiden siber yang disampaikan oleh BSSN.

14 UNODC Countering Cyber Security Threats to Maritime Law Agencies

UNODC menyelenggarakan Pelatihan *Cyber Security Threats to Maritime Law Agencies* pada tanggal 22 – 23 Mei 2023 di Yogyakarta. Pelatihan dilaksanakan dilatarbelakangi oleh adanya kejahatan dunia maya yang terus berkembang, sehingga dibutuhkan pemahaman terkait keamanan siber.

15 The Asia Pacific Internet Security Conference Security Training Course

The APISC Training Course 2023, diselenggarakan oleh KrCert/CC di Seoul, Korea Selatan pada 23-27 Oktober 2023, adalah acara tahunan yang bertujuan meningkatkan kapabilitas Tim CSIRT. Kegiatan ini dihadiri oleh 20 orang perwakilan CSIRT dari 18 negara Asia Pasifik, acara ini mencakup diskusi tentang lanskap keamanan siber nasional, kebijakan, dan kegiatan yang dilakukan oleh masing-masing negara, serta pembekalan materi teknis dan manajemen CSIRT serta latihan Manajemen Krisis Siber melalui kegiatan *Table-Top Exercise*.

16 ASEAN Japan Cybersecurity Capacity Building Centre (AJCCBC) Cybersecurity Technical Training

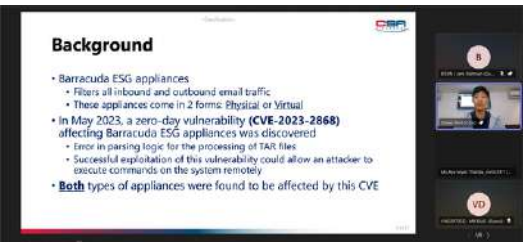
ASEAN Japan *Cybersecurity Capacity Building Centre* (AJCCBC) diselenggarakan pada tanggal 16 s.d 20 Oktober 2023 di Bangkok, Thailand dengan tema yang fokus pada *Cybersecurity Technical Training*-J3. Program pelatihan ini mencakup *Cyber Defense Exercise with Recurrence* (CYDER) and *Network Forensics* yang dihadiri oleh 17 praktisi professional keamanan siber sebagai perwakilan dari sektor pemerintah dan pengelola infrastruktur informasi kritikal dari 8 negara ASEAN.

17 Singapore-Industrial Control Systems Cybersecurity 301 (SG-ICS301) Course

CSA Academy Singapura bekerja sama dengan CISA untuk menyelenggarakan pelatihan terkait Singapore *Industrial Control Systems Cybersecurity* 301 (SG-ICS301) pada tanggal 21 – 25 Agustus 2023 di Singapura. Pelatihan ini bertujuan untuk mengembangkan pemahaman tentang ICS, ancaman siber terhadap ICS dan solusi yang dapat diimplementasikan.

18 Seminar & Hand-on Exercise Korea Internet & Security Agency (KISA) Global Cybersecurity Center for Development (GCCD) - BSSN Cybersecurity Joint Program

Seminar & *Hands-on Exercise Global Cybersecurity Center for Development* (GCCD) diselenggarakan atas kerja sama Korea Internet & Security Agency (KISA) dan BSSN. Pada acara seminar tanggal 21 November 2023, National CSIRT menyampaikan profil keamanan siber di Indonesia tahun 2023, dan membahas mengenai Tren Ancaman Keamanan Siber dan upaya mitigasinya. BSSN menyoroti mengenai perkembangan ancaman *ransomware*, membahas model ancaman, teknik serangan, dan model bisnis *Ransomware-as-a-Service* (RaaS), serta pembelajaran dari insiden ransomware, sementara BSSN juga mengikuti *Hands-on Exercise* tentang forensik digital pada 22-24 November 2023 di Jakarta.



19 Human Resource Development for Cyber Security Professionals (Bhutan GoVTech Agency visits to IDSIRTII)

Universitas Indonesia (UI) dan Japan International Organization Agency (JICA) telah menjalankan proyek Pengembangan Sumber Daya Manusia untuk Profesional Keamanan Siber sejak Mei 2019. Salah satu komponen dari proyek ini adalah untuk mengembangkan sumber daya manusia keamanan siber tidak hanya di Indonesia tetapi juga di negara-negara lain. Berdasarkan program tersebut, UI dan JICA membawa Bhutan Gyalpozhing College of Information Technology (GCIT) & GoVTech Agency dalam kunjungan ke ID-SIRTII/CC BSSN. Tujuan utama dari kunjungan ini adalah untuk membahas tentang kolaborasi/peran di antara akademisi, pemerintah, dan kelompok industri dalam membangun ekosistem keamanan siber di Indonesia dari sudut pandang ID-SIRTII/CC BSSN sebagai pihak pemerintah, sebagai *best practices* yang dapat dipelajari Pemerintah Bhutan.

20 Sing-CERT Sharing Session onBarracuda Zero-day

SingCERT menyelenggarakan *sharing session* dengan National CSIRT negara-negara ASEAN pada tanggal 6 Desember 2023. Dalam sesi ini, SingCERT memberikan informasi terkini terkait eksploitasi kerentanan *Zero-Day* Barracuda (CVE-2023-2868), yang telah dimanfaatkan oleh pelaku ancaman sejak Oktober 2022. Sing-CERT membahas bagaimana serangan ini terjadi, tantangan yang dihadapi dalam merespons, studi kasus, serta langkah mitigasi. Selain itu, perwakilan negara-negara ASEAN memberikan presentasi mengenai lanskap ancaman siber negara masing-masing, termasuk statistik kasus, insiden signifikan, dan kebijakan keamanan siber terbaru. Hal ini bertujuan agar setiap National CSIRT dapat memahami lebih baik ancaman regional, bersiap menghadapi risiko yang muncul, dan menjaga keamanan siber nasional.

21 UNODC Southeast Asia Senior Officials Regional Meeting on Cross-Border Money Laundering through Digital Channels

UNODC menyelenggarakan kegiatan forum terkait pencucian uang melalui *platform digital* yang dilaksanakan di Manila, Filipina pada bulan Desember 2023. Kegiatan tersebut diikuti oleh 4 (empat) negara, yaitu Indonesia, Thailand, Malaysia, dan Filipina. Kegiatan tersebut bermaksud untuk memberikan pandangan dan gambaran terkait kejahatan siber di Indonesia dan potensi pencucian uang menggunakan *platform* digital.

22 UNODC Workshop on Financial Crimes Investigation Involving Cryptoasset

United Nations Office on Drugs and Crime (UNODC) menyelenggarakan kegiatan *Focus Group Discussion* terkait Investigasi dan penuntutan kejahatan keuangan yang melibatkan aset kripto yang dihadiri oleh BSSN, Polri, PPATK, Kejaksaan, Bappebti, dan Asosiasi Pedagang Aset Kripto. FGD ini bertujuan menghasilkan *output* berupa *Handbook Development* sebagai Buku Saku Panduan serta *National Approach* dalam investigasi dan penuntutan kejahatan keuangan yang melibatkan aset kripto. Kegiatan ini dilaksanakan pada bulan Agustus 2023 dan rangkaian kegiatan penyusunan buku saku panduan penanganan tindak pidana dengan menggunakan aset kripto dilaksanakan dari bulan Agustus 2023 hingga Desember 2023.

23 Workshop Cybersecurity dan Infrastructure Security Agency (CISA)-Amerika Serikat

Kedutaan Besar Amerika Serikat di Jakarta bersama dengan CISA Departemen Keamanan Dalam Negeri Amerika Serikat menyelenggarakan lokakarya dalam rangka peningkatan kapasitas keamanan siber melalui kegiatan *Cyber Hygiene Workshop* yang berlangsung di Surabaya, Jawa Timur.

24 Capacity Building for Responding to Cryptocurrency Heist in ASEAN Region

Korea International Cooperation Agency (KISIA) melalui KOICA menyelenggarakan program peningkatan kapabilitas untuk merespon pencurian aset virtual bagi negara-negara di ASEAN pada Oktober 2023. Kegiatan dihadiri oleh 5 (lima) negara di ASEAN, yaitu Laos, Vietnam, Indonesia, Thailand, dan Filipina. Agenda pada program ini, antara lain serangan siber yang menargetkan *exchanger* dan penyedia layanan aset virtual, Solusi untuk memperkuat keamanan siber untuk tanggap insiden, dan peningkatan peraturan di tingkat pemerintah.

25 Key Performance Indicator (KPI) OIC-CERT

BSSN berperan dalam menjalankan salah satu *Key Performance Indicator* (KPI) OIC-CERT pada pilar strategis *Capacity Building* dengan mengangkat beberapa tema seperti *The Role of ISACs in Improving Cybersecurity and Resilience: Introduction and Implementation of Best Practice, Building and Managing ISAC in Government Sector, ISAC Ransomware and Cloud Security Governance dan Data Protection In Cybersecurity –A Critical Imperative.*

26 The 6th UNODC Southeast Asia Cryptocurrencies Working Group Meeting

UNODC menyelenggarakan kegiatan diskusi terkait *cryptocurrency* yang diadakan di Jakarta. Tujuan dari kegiatan ini adalah untuk mendukung upaya kolaboratif dan kerja sama internasional terkait dengan kejahatan siber dan kejahatan yang terkait mata uang kripto yang sedang berlangsung di antara negara-negara di Asia Tenggara. Agenda dalam kegiatan diskusi ini antara lain pertukaran ide dan solusi untuk kerangka kerja regulasi yang efektif dalam merespon kejahatan yang terkait dengan mata uang kripto.

27 International Law Enforcement Academy (ILEA) Investigating Criminal Use of Cryptocurrency Training

ILEA mengadakan pelatihan dengan tajuk *Investigating Criminal Use of Cryptocurrency Training* yang berlangsung di Bangkok, Thailand pada Juni 2023. Pelatihan ini diikuti oleh 10 negara, antara lain Indonesia, Kamboja, Laos, Malaysia, Filipinan, Singapore, Thailand, Vietnam, Korea Selatan, dan Taiwan. Kegiatan ini bertujuan untuk memberikan prosedur dan mekanisme operasional berbagai mata uang kripto dan cara mengidentifikasi keberadaan mata uang kripto dalam penyelidikan.

28 ASEAN Cyber Shield Hacking Contest Jakarta

BSSN berpartisipasi dalam kegiatan ACS 2023 yang diadakan oleh Korean Internet and Security Agency (KISA) pada tanggal 20 - 24 November 2023 Di Jakarta. Tim mengikuti 2 (dua) jenis kategori perlombaan pada kegiatan ACS 2023, yaitu CTF (*Open Division*) dan *Hackthon*. Perlombaan CTF dilaksanakan berformat Jeopardy. Tim bertugas mampu meraih posisi ke 7 dari 20 pada Perlombaan CTF. Tim bertugas juga berhasil mengerjakan 10 soal pada *Hackathon* dan mendapatkan posisi juara 2 pada perlombaan *Hackathon*.

KERJA SAMA LAYANAN HONEYNET

Kerja sama ISIF Project

Kolaborasi *Honeynet* BSSN dengan Swiss German University (SGU) dan komunitas Indonesia *Honeynet Project* (IHP) sudah berlangsung sejak tahun 2018. Kerja sama ini berfokus pada 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 di suatu 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*.

Pemasangan Honeypot

Pada tahun 2023, terdapat penambahan 12 titik pemasangan *honeypot*, sehingga jumlah *Honeypot* BSSN yang terpasang mencapai 105 titik yang tersebar di 27 provinsi di Indonesia. Penambahan titik *Honeypot* ini diharapkan dapat mengumpulkan data serangan siber lebih luas yang menyerang Indonesia berdasarkan sistem *Honeynet* BSSN yang telah terpasang. 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.

105
titik
yang tersebar di 27 provinsi

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

https://bssn.go.id/honeynet

KETERLIBATAN KEGIATAN PAMERAN

Pameran National Cybersecurity Connect

Honeynet BSSN mengikuti kegiatan dan pameran keamanan siber yang diperuntukkan bagi komunitas keamanan siber dan masyarakat umum. Kegiatan yang diikuti oleh Honeynet BSSN yaitu National Cybersecurity Connect 2023 yang dilaksanakan pada tanggal 25 s.d. 26 Oktober 2023 di Birawa Assembly Hall, Bidakara, Jakarta. Kegiatan National Cybersecurity Connect adalah kegiatan keamanan siber terbesar yang dihadirkan untuk menjadi solusi dan wadah bagi seluruh pemangku kepentingan untuk berkumpul, berdiskusi, guna meningkatkan kesadaran dan keahlian masyarakat Indonesial dalam bidang keamanan siber.

INDOSEC Summit 2023

Indosec Summit 2023 merupakan kegiatan yang bertujuan untuk mendukung kerja sama antara sektor publik dan swasta serta mengatasi ancaman siber yang semakin meningkat di Indonesia. Kegiatan tersebut dilaksanakan pada tanggal 29-30 Agustus 2023 di The Ritz-Carlton Jakarta, Pacific Place. Acara ini juga menampilkan IndoSec Awards 2023 untuk memberikan penghargaan kepada sejumlah talenta keamanan siber terbaik di Indonesia dalam berbagai kategori pada 31 Agustus 2023. Layanan Honeynet BSSN turut memberikan dukungan pada acara tersebut untuk memperkenalkan teknologi keamanan siber di bidang pengelolaan informasi dini ancaman siber yang telah dimiliki oleh BSSN. Masyarakat umum dapat menambah informasi terkait teknologi keamanan siber dan mengetahui pentingnya pemanfaatan Honeynet yang dapat dijadikan sebagai sumber data informasi serangan siber.

KERJA SAMA LABORATORIUM FORENSIK DIGITAL

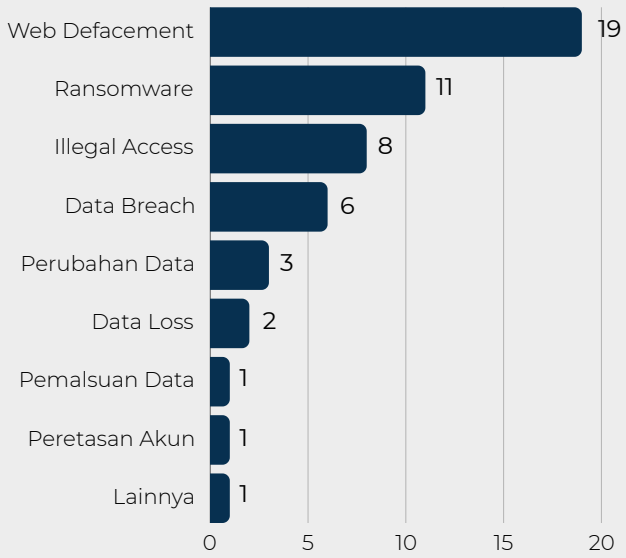
55
layanan LFD

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

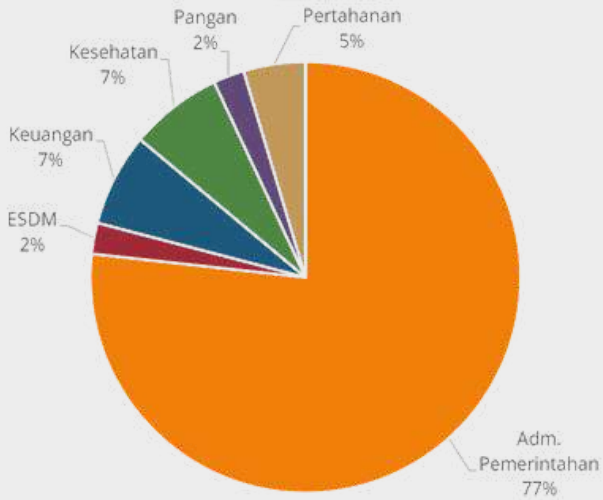
JENIS LAYANAN LABORATORIUM FORENSIK DIGITAL

52	Pemeriksaan Forensik Digital
2	Perbantuan Keterangan Ahli
1	Dukungan Penyidikan

JENIS INSIDEN YANG DITANGANI



SEBARAN SEKTOR TERDAMPAK



AKREDITASI LABORATORIUM FORENSIK DIGITAL BSSN

Manajemen Sistem Mutu Laboratorium Forensik Digital BSSN Berdasarkan Standar ISO/IEC 17025:2017

Laboratorium forensik digital BSSN melakukan manajemen sistem mutu berdasarkan standar ISO/IEC 17025:2017 dengan kegiatan sebagai berikut:

Laboratorium Forensik Digital BSSN Raih Sertifikat Akreditasi ISO/IEC 17025:2017

Laboratorium Forensik Digital BSSN telah melewati seluruh tahapan akreditasi sehingga berhasil mendapatkan sertifikat akreditasi SNI ISO/IEC 17025:2017 per tanggal 23 Agustus 2023 dan berlaku sampai tanggal 22 Agustus 2028. Sertifikat akreditasi ini menunjukkan bahwa Laboratorium Forensik Digital BSSN kompeten sebagai laboratorium penguji berdasarkan SNI ISO/IEC 17025:2017.

Uji Banding Antar Laboratorium Laboratorium Forensik Digital Berdasarkan ISO 17025:2017

Berdasarkan persyaratan rangkaian akreditasi ISO 17025:2017 suatu Laboratorium yang telah terakreditasi perlu melakukan uji banding minimal kepada 2 (dua) laboratorium dalam 1 (satu) tahun yang mulai dilaksanakan paling cepat 6 (enam) bulan setelah Laboratorium Forensik Digital BSSN terakreditasi untuk memastikan bahwa kompetensi laboratorium sesuai dengan persyaratan yang ditetapkan pada standar. Pada tahun 2023, uji banding laboratorium dilakukan bersama POLDA Jawa Timur.


We need to build a culture of cybersecurity where security is everyone's responsibility.
- William A. Owens

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2023

PREDIKSI POTENSI ANCAMAN SIBER TAHUN 2024

11

PREDIKSI POTENSI ANCAMAN SIBER

Berdasarkan pengumpulan data dari sumber terbuka, hasil deteksi keamanan siber dari trafik internet Indonesia, penelusuran *cyber threat intelligence*, analisis celah kerentanan pada aplikasi berbasis internet yang telah dilakukan pengujian keamanan oleh BSSN, dan lesson learn dari penanganan insiden, telah diprediksi potensi ancaman siber yang dapat menjadi serangan pada tahun 2024. Ancaman tersebut meliputi *Web Defacement*, *Malware stealer* dan *Ransomware*, *Cyber Threat Based Artificial Intelligence* (AI), *Internet of Things* (IoT) *Attack*, *Advanced Persistent Threat* (APT), *Phishing,* dan *Distributed Denial of Service* (DDoS). Penetapan potensi ancaman ini didasarkan pada peningkatan jumlah yang signifikan dalam beberapa tahun terakhir, menunjukkan kecenderungan meningkat yang diperkirakan akan berlanjut pada tahun 2024. Untuk mengantisipasi potensi ancaman ini, langkah-langkah yang disarankan antara lain melakukan backup data secara berkala, menerapkan pembatasan hak akses, dan melakukan pembaruan sistem operasi secara teratur.

> The best cure for security vulnerabilities is not to have them, but the next best cure is to find and fix them as fast as possible.
>
> **- Phil Zimmermann**

WEB DEFACEMENT

Ancaman *web defacement* merupakan bentuk serangan siber yang mengubah tampilan suatu situs web dengan tujuan menyampaikan pesan atau merusak reputasi pemiliknya. Pada sebuah serangan *defacement*, *threat actor* seringkali memilih target yang memiliki nilai simbolis, seperti situs web pemerintah, perusahaan besar, atau lembaga penting. Pesan yang disampaikan bervariasi, mulai dari pesan teks, gambar, hingga pesan politis atau ideologis. *Threat actor* seringkali memanfaatkan celah keamanan pada situs web atau menggunakan teknik *hacking* untuk mendapatkan akses tak sah, sehingga dapat dengan mudah mengganti halaman utama situs tersebut dengan pesan atau konten yang dimaksudkan. Ancaman *web defacement* tidak hanya merupakan pelanggaran terhadap privasi dan integritas suatu situs web, tetapi juga dapat memiliki dampak serius terhadap reputasi dan kepercayaan pengguna yang mengakses situs tersebut. Mengingat pada tahun 2024 merupakan tahun poliitik dan akan diadakan event besar Pemilihan umum maka intensi terhadap ancaman *web defacement* diindikasikan akan banyak terjadi.

Ransomware and digital extortion like many other crimes that are fueled by cryptocurrency, only work if the bad guys get paid, which means we have to bust their business model

- Lisa O. Monaco

MALWARE STEALER & RANSOMWARE

Berdasarkan hasil deteksi terhadap *darknet exposure* tahun 2023, banyak ditemukan data kredensial di *darknet* yang bocor akibat adanya *malware stealer*. Ancaman *malware stealer* diprediksi akan menjadi tren potensi ancaman pada tahun 2024. *Malware stealer* dapat disebarkan akibat penggunaan aplikasi bajakan, *advertising*/iklan, maupun melalui *phishing*. Selain *malware stealer*, salah satu kategori malware lainnya yang diprediksi menjadi tren potensi ancaman yaitu *ransomware*. Ancaman *ransomware* telah menjadi salah satu tantangan serius dalam keamanan siber.

Berdasarkan data *monitoring* anomali lalu lintas jaringan nasional BSSN tahun 2023, *ransomware* termasuk dalam 10 besar anomali terbanyak dan berdasarkan data penanganan insiden BSSN, *ransomware* masuk ke dalam 5 besar insiden yang terjadi tahun 2023. *Threat actor* menggunakan metode *phishing* untuk menyebarkan *malware* tersebut, dengan mengirimkan email palsu yang tampak sah dan mengklaim urgensi dari email tersebut. *Social engineering* juga digunakan sebagai alat untuk mengeksploitasi kelemahan manusia, dengan *threat actor* memanipulasi emosi atau menyamar sebagai entitas yang dipercayai untuk memancing tindakan berbahaya dari korban. Selain itu, threat actor juga memanfaatkan *zero-day vulnerabilities*, celah keamanan yang belum ditemukan oleh para pengembang, untuk merancang serangan yang tidak terdeteksi. Melalui penggabungan ketiga metode ini, *ransomware* dapat dengan cepat menyebar, mengenkripsi data berharga, dan mengancam untuk merusak integritas sistem.

CYBER THREAT BASED **ARTIFICIAL INTELLIGENCE (AI)**

Success in creating effective AI could be the biggest event in the history of our civilization. Or the worst. We just don't know. So we cannot know if we will be infinitely helped by AI, or ignored by it and side-lined, or conceivably destroyed by it.

- Stephen Hawking

Pemanfaatan AI untuk mempermudah aktivitas manusia juga dimanfaatkan *threat actor* untuk mempermudah melakukan serangan. Ancaman siber yang memanfaatkan AI telah menjadi isu yang semakin mengkhawatirkan dalam ekosistem digital. Berdasarkan data Security Report yang dikeluarkan oleh Check Point Research (CPR) pada pertengahan 2023 mengungkapkan bahwa terdapat indikasi *threat actor* menggunakan teknologi seperti AI untuk melancarkan serangannya. Penggunaan AI dalam serangan siber dapat meningkatkan tingkat kompleksitas dan efektivitas serangan. Para *threat actor* dapat menggunakan teknologi AI untuk mengidentifikasi dan mengeksploitasi celah keamanan dengan lebih cepat, serta mengelabui sistem keamanan dengan serangan yang dapat beradaptasi secara otomatis. Kemampuan AI untuk mengenali pola, belajar mandiri, dan beradaptasi, sehingga dapat meningkatkan serangan siber menjadi lebih canggih dan sulit dideteksi.

Pada *phishing*, AI dapat digunakan untuk menciptakan pesan dan situs web buatan yang lebih meyakinkan dan sulit terdeteksi oleh filter keamanan, bahkan dapat mempersonalisasi pesan berdasarkan profil korban dengan menggunakan analisis data dari berbagai sumber. Pada serangan *malware*, AI dapat digunakan untuk mengidentifikasi kelemahan sistem target dan mengadaptasi malware secara otomatis guna menghindari deteksi perangkat keamanan. AI juga dapat digunakan dalam serangan bertarget, seperti serangan *ransomware* yang dapat memilih secara otomatis target yang dinilai paling rentan. Serangan DDoS juga dapat dilakukan lebih efektif dengan bantuan AI, melalui pola serangan yang disesuaikan dengan kapasitas sistem yang dimiliki oleh target. Selain itu, pengggunaan AI pada serangan DDoS dapat mempersulit dilakukannya penelusuran terhadap sumber serangan yang dapat mengelabui sistem deteksi ancaman melalui modifikasi otomatis dalam pola perilaku. Serangan siber yang memanfaatkan AI juga mencakup serangan berbasis bot yang otomatis dan adaptif.

IoT will play a crucial role in transforming every aspect of our lives - from home automation to transportation, from smart cities to precision agriculture. But IoT devices also present new security and privacy challenges that must be addressed.

- Satya Nadella

INTERNET OF THINGS (IOT) ATTACK

IoT secara perlahan-lahan mendapatkan popularitas dan mengubah objek-objek sehari-hari menjadi perangkat pintar yang saling terhubung. IoT bertujuan untuk memudahkan keseharian dengan menghubungkan perangkat ke jaringan yang terintegrasi. Integrasi jaringan ini membawa risiko karena setiap perangkat IoT dalam suatu ekosistem berpotensi menjadi titik masuk bagi pihak *threat actor*. Kelemahan dalam satu perangkat yang terhubung satu sama lain dapat memiliki efek domino dan mengompromikan keamanan seluruh jaringan.

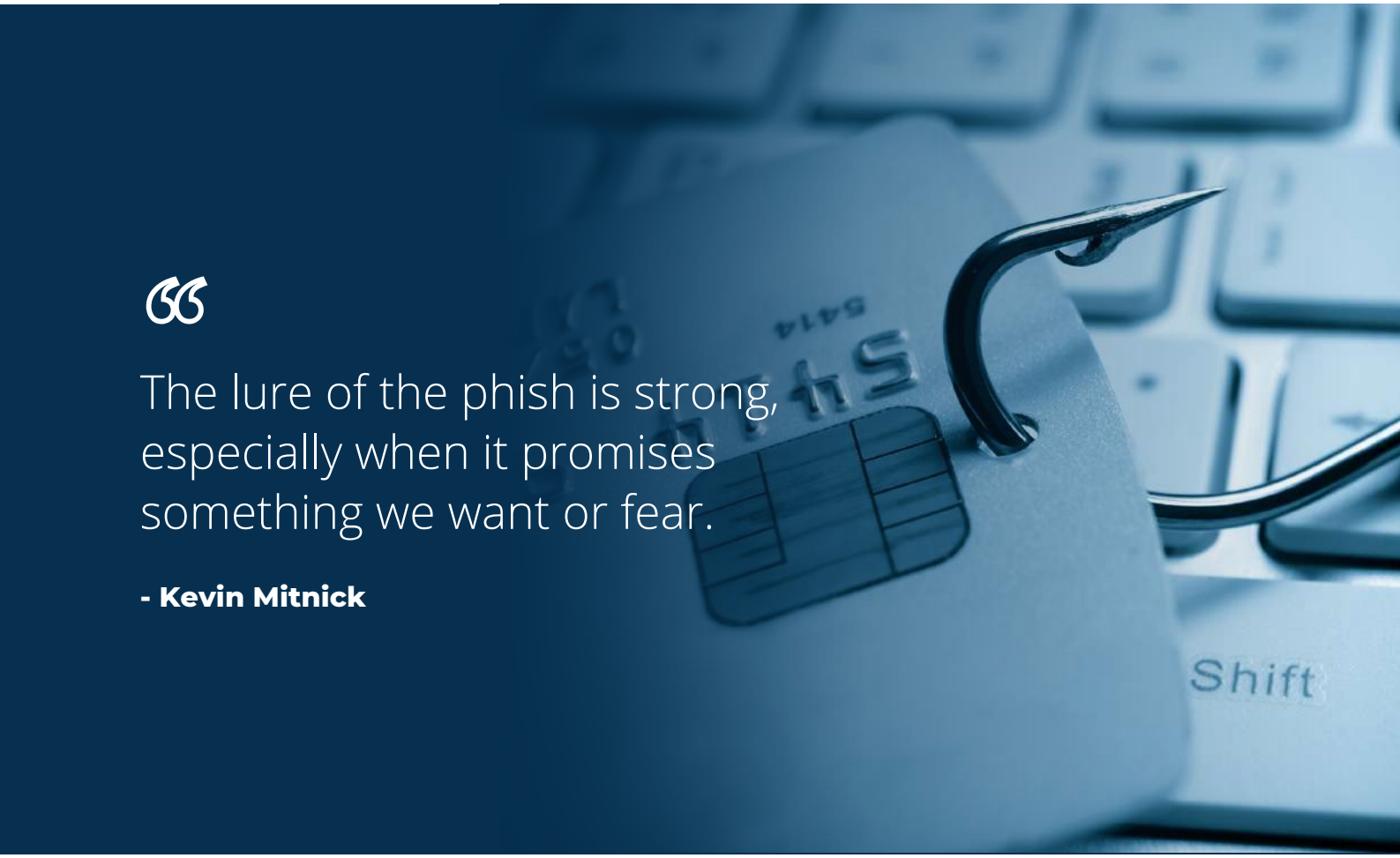
Salah satu serangan yang menargetkan IoT adalah Mirai. Mirai merupakan malware yang mampu mengubah IoT menjadi botnet sebagai senjata dalam melancarkan serangan DDoS dan serangan lainnya. Berdasarkan data *monitoring* anomali lalu lintas jaringan nasional BSSN pada tahun 2023, anomali berupa Mirai mencapai 80.319 anomali. Selain itu, terdapat juga malware-malware lain yang menargetkan perangkat IoT yang secara tren terus berkembang, sehingga diperkirakan pada tahun 2024 berpotensi akan tetap muncul dan terus meningkat.

ADVANCED PERSISTENT THREAT

An APT is like a burglar who has moved into your house and is slowly learning your routines, looking for valuables, and planning the best time to strike.

- John McAfee

APT (*Advanced Persistent Threat*) adalah ancaman siber tingkat lanjut yang berlangsung lama dan melibatkan upaya terus-menerus dan terstruktur dari *threat actor* untuk mempertahankan akses tidak sah ke sistem atau jaringan. Dengan karakteristik utama berupa keberlanjutan, kecanggihan melalui penggunaan malware khusus dan teknik eksploitasi, serta tujuan spesifik seperti pencurian informasi rahasia atau gangguan operasi bisnis, serangan APT umumnya dilakukan oleh kelompok dengan sumber daya dan motivasi signifikan, seperti kelompok peretas negara atau organisasi kejahatan siber. Pencegahan dan deteksi APT memerlukan langkah-langkah keamanan siber menyeluruh, pemantauan aktif, dan respons cepat terhadap indikasi serangan. Berdasarkan data monitoring anomali lalu lintas jaringan nasional BSSN, serangan APT masuk dalam 10 besar anomali terbanyak. Pada tahun 2024, serangan APT akan lebih berfokus pada sektor-sektor kritis, pemerintahan, dan bisnis-bisnis besar dengan tujuan spionase atau pengintaian dan pencurian data sensitif. Ancaman ini menjadi semakin parah mengingat banyaknya negara yang mulai bermain dalam operasi siber demi keuntungan geopolitik masing-masing. Hal ini terlihat dari banyaknya intelijen ataupun serangan siber berbasis APT atau *ransomware* yang menargetkan pemerintah dan mata uang kripto. Beberapa negara lainnya juga bahkan sudah mulai mendanai aksi untuk operasi spionase.



> The lure of the phish is strong, especially when it promises something we want or fear.
>
> **- Kevin Mitnick**

PHISHING

Phishing adalah upaya untuk memperoleh informasi pribadi seperti password dan rincian keuangan dengan menyamar sebagai entitas terpercaya melalui komunikasi elektronik, sering kali melalui *email* atau situs *web* palsu. Serangan *phishing* termasuk dalam jenis serangan yang perlu menjadi fokus berdasarkan banyaknya masyarakat yang menjadi korban. *Phishing* juga termasuk ke dalam 10 besar insiden yang terjadi tahun 2023 berdasarkan data penanganan insiden BSSN. Pada tahun 2024, diperkirakan akan banyak terjadi serangan *phishing* tingkat lanjut. Di sini, bukan hanya serangan *phishing* melalui *email* yang dimaksud, tetapi juga serangan SEO *(Search Engine Optimization*) *poisoning* yang merupakan ancaman *phishing* yang semakin meningkat. SEO *poisoning attacks* merupakan serangan *phishing* yang dirancang untuk menarik korban ke situs *web* yang menyerupai aslinya dengan memanfaatkan algoritma mesin pencari (*search engine*). Serangan ini mencoba memanipulasi hasil pencarian mesin pencari sehingga korbannya diarahkan ke situs web palsu yang tampak seperti situs resmi. Contohnya, seorang karyawan yang mencari layanan *cloud online* mungkin akan menemukan situs palsu dan tanpa sadar memberikan kredensialnya langsung kepada pelaku kejahatan siber. Hal ini dapat menyebabkan mesin korban terinfeksi *malware*.

DISTRIBUTED DENIAL OF SERVICE

DDoS attacks are cyber weapons wielded by those who seek to silence dissent, disrupt commerce, and sow chaos. They represent the dark side of technology.

- Bruce Schneier

Serangan *Denial of Service* (DoS) merupakan jenis serangan terhadap sistem dalam jaringan internet dengan cara menghabiskan *resource* yang dimiliki oleh suatu sistem sehingga tidak dapat menjalankan fungsinya dengan benar dan secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan sistem yang diserang tersebut. Serangan DoS memanfaatkan kelemahan sistem pada keterbatasan sumber daya, baik *bandwidth*, kemampuan menyimpan memori, *server* dan kelemahan lainnya. Kebanyakan DoS menyerang bisnis kecil hingga menengah yang tidak memiliki sumber daya yang besar. Pada dasarnya tujuan *threat actor* hanya untuk membuat sistem lumpuh, tapi tak jarang juga ada yang kemudian meminta biaya tebusan untuk menghentikan serangan.

Dalam serangan DoS *threat actor* menggunakan satu komputer dan satu koneksi internet saja ketika meluncurkan serangan. Untuk melancarkan serangan yang berskala lebih besar, *threat actor* bisa menggunakan banyak komputer dan banyak koneksi internet yang dikontrol secara bersamaan dengan menggunakan botnet. Botnet merupakan sejumlah komputer yang terinfeksi *malware* tanpa disadari oleh penggunanya. Serangan DoS secara bersama-sama tersebut disebut *Distributed Denial of Service* (DDoS). Selama tahun 2023 melalui *monitoring* yang dilakukan oleh BSSN telah ditemukan banyak upaya serangan DDoS yang menargetkan Indonesia dan hingga 2024 diprediksi potensi serangan ini akan terus meningkat.

LANSKAP

KEAMANAN SIBER INDONESIA

2023

BADAN SIBER DAN SANDI NEGARA

TLP: CLEAR