awanpintar.id®
CLOUD SECURITY ENGINE

Green
OPEN

INDONESIA WASPADA

Laporan Ancaman Digital di Indonesia
Semester 2 dan Analisis Serangan 2024

PT PROSPERITA SISTEM INDONESIA

DAFTAR ISI

Green
OPEN

RINGKASAN EKSEKUTIF

Sejak awal tahun 2024, pemerintah, dunia usaha maupun masyarakat terus bergulat dengan isu keamanan siber. Kemajuan teknologi telah berdampak pada meningkatnya transformasi digital, sehingga berimplikasi pada bertambahnya risiko keamanan siber. Hal ini menjadi fokus perhatian AwanPintar.id® sepanjang tahun yang kemudian dituangkan dalam Laporan Ancaman Digital di Indonesia Semester 2 dan Analisis Serangan Tahun 2024.

Laporan ini menyoroti isu terkini di ranah siber yang tidak hanya terkait teknologi canggih, namun juga keamanan siber dan tata kelola siber. Sementara tren lain yang sedang berkembang dalam lanskap keamanan siber adalah automasi kejahatan siber. Perkembangan teknologi AI merupakan cakrawala baru yang memberi kemudahan di berbagai aktivitas manusia, namun di sisi lain menjadi senjata atau amunisi baru bagi dunia kejahatan maya.

Di saat jenis kejahatan siber terus bermunculan karena penyalahgunaan teknologi kekinian, kerentanan baru juga terus terungkap setiap tahunnya. AwanPintar.id® mendeteksi secara rinci Common Vulnerability & Exposures yang tercatat di tahun 2024 sebagai informasi yang wajib diketahui oleh setiap pengguna internet di Indonesia.

Laporan ini juga merangkum serangan siber selama satu tahun penuh, termasuk laporan khusus serangan dalam negeri yang akan mengupas segala ancaman yang masuk ke Indonesia yang berasal dari dalam negeri, yang secara konsisten akan terus menjadi bagian dalam laporan setiap semesternya.

Laporan Ancaman Digital di Indonesia Semester 2 dan Analisis Serangan Tahun 2024 oleh AwanPintar.id® merupakan ujung tombak dalam lanskap keamanan siber nasional, dengan berupaya untuk menjadi pusat data terdepan dalam menjaring setiap ancaman siber yang masuk ke Indonesia baik dari dalam maupun dari luar, sehingga data-data valid tersebut dapat digunakan untuk kemaslahatan pengguna internet di tanah air.

Green
OPEN

TENTANG awanpintar.id®

AwanPintar.id® adalah karya PT Prosperita Sistem Indonesia yang menjadi bagian dari Prosperita Group, kelompok perusahaan yang memiliki kepedulian pada keamanan digital di Indonesia, berdiri sejak 2008. Misinya ikut menjaga kedaulatan digital negara Indonesia. Penelitian dan pengembangan di Indonesia terus dilakukan oleh PT Prosperita Sistem Indonesia sebagai penghasil solusi keamanan siber nasional dan PT Prosperita Mitra Indonesia memfokuskan bisnisnya pada distribusi software keamanan data, sistem dan jaringan.

Beberapa solusi turunan dari AwanPintar.id® adalah Cloud Malware Analyzer, Cloud Antimalware File Scanning, Cloud Endpoint Security (CloudID), Cloud Email Security: Vimanamail® www.vimanamail.id.

AwanPintar.id® terhubung langsung di pusat internet Indonesia (OIX/IIX) – *Open Internet Exchange Point / Indonesia Internet Exchange*, jantung dari komunikasi internet di Indonesia sehingga mampu menyediakan akses cepat dengan kapasitas koneksi yang tinggi.

AwanPintar.id® memiliki detektor yang tersebar di jaringan internet nasional Indonesia untuk mengumpulkan data secara realtime. Jutaan data yang masuk tiap harinya diolah dan menjadi umpan balik bagi *Machine Learning* (ML) yang digunakan.

AwanPintar.id® dapat digunakan oleh siapa saja yang membutuhkan, khususnya para IT profesional yang bersinggungan dengan keamanan data. Disediakan konsol yang dapat diakses melalui web. Untuk penggunaan korporasi yang ingin mendapatkan data secara komprehensif, disediakan HTTPS RESTful API yang dapat terhubung langsung. Selain itu, DNSBL sesuai dengan RFC5782 dapat digunakan untuk pengecekan IP secara realtime.

AwanPintar.id® menyediakan detektor yang dapat digunakan di jaringan korporasi yang memerlukan agar data ancaman dapat dianalisa dan ditampilkan untuk keperluan SOC atau CSIRT korporasi. Selain itu, disediakan pula aplikasi berbasis WEB dan RESTful API yang dapat digunakan untuk memperkuat pertahanan digital seperti file scanning, file analytic, IP Intelligence, IP Hunting, CVE Hunting serta fasilitas lain yang berkaitan.

AwanPintar.id® juga membuka kerjasama dengan para pihak terkait yang membutuhkan informasi atau menggunakan fasilitas yang sudah dibangun. AwanPintar.id® dapat diakses di www.awanpintar.id

Green
OPEN

METODOLOGI

Untuk memahami ancaman digital di Indonesia, AwanPintar.id® memasang detektor di jaringan internet Indonesia. Detektor ini menjadi target serangan dari mancanegara dan dalam negeri. Berikut adalah metodologi riset yang digunakan untuk membuat Laporan Ancaman Digital di Indonesia Semester 2 dan Analisa Serangan Tahun 2024:

1 Pengumpulan Data

AwanPintar.id® menggunakan sejumlah detektor yang tersebar di jaringan internet Indonesia dan mengumpulkan seluruh data dari tiap detektor untuk diolah menjadi *Big Data*. Tiap detektor memiliki alamat IP publik dan fungsi spesifik yang bertujuan agar menjadi target serangan sehingga setiap pola serangan dapat dikumpulkan dan dianalisa agar menjadi data terpercaya yang dapat diaplikasikan oleh seluruh pengguna AwanPintar.id® pada sistem yang dimiliki.

Detektor AwanPintar.id® bersifat pasif dan mandiri, yang berarti sebagai detektor hanya menerima masukan yang berupa serangan dari seluruh dunia yang diarahkan ke tiap detektor secara spesifik. Detektor AwanPintar.id® tidak memerlukan teknologi yang sifatnya monitoring seperti SPAN/Port Mirroring, NetFlow, IPFIX, sFlow atau jFlow sehingga terhindar dari kemungkinan pengumpanan data secara sengaja.

Sebaran detektor di jaringan internet Indonesia dilakukan untuk melakukan sampling dari banyak IP dari beragam *AS Number* agar mendapatkan distribusi data yang komprehensif.

2 Pemilihan Data

AwanPintar.id®memiliki kemampuan secara otomatis untuk memilih data yang masuk sesuai dengan pola serangan, asal serangan serta informasi lain yang ada selama serangan dilakukan. Data yang tidak dikategorikan sebagai serangan, tidak dimasukkan ke dalam Big Data.

Green
OPEN

3 Analisis Data

Analisis dilakukan untuk mengidentifikasi pola dan tren, serta untuk menentukan sifat dan sumber serangan siber. Analisis data meliputi metadata jaringan, arus lalu lintas dan informasi serangan. Teknologi *Artificial Intelligence* (AI) dengan *Machine Learning* (ML) digunakan secara efektif untuk analisa data secara otomatis.

Metode analisis deskriptif dan korelatif digunakan untuk mendapatkan pemahaman yang lebih detail dari setiap data yang disajikan. Sangat dimungkinkan tiap topik menggunakan metode yang berbeda mengikuti kebutuhannya. Penamaan nama kota dan negara didapat berdasarkan alamat IP yang terdeteksi mengikuti standar ISO 3166-1 Alpha-2.

4 Evaluasi Risiko

Risiko keamanan siber harus dinilai sesuai dengan kriteria dan kelas risiko yang ditentukan sebelumnya. Evaluasi risiko melibatkan analisis risiko terhadap data dan informasi yang telah dikumpulkan, serta penilaian terhadap kemungkinan dampak serangan terhadap sistem keamanan siber.

Data *Common Vulnerability Exposures* (CVE), evaluasi resiko dibuat berdasarkan acuan informasi yang didapat dari *MITRE Adversarial Tactics, Techniques, and Common Knowledge* (MITRE ATT&CK), *National Institute of Standards and Technology* (NIST) serta *Forum of Incident Response and Security Teams* (FIRST).

5 Visualisasi Data

Untuk mempermudah membaca data yang ada, data keamanan siber diekstraksi dan disajikan dalam bentuk visualisasi data. Ini berguna untuk memperjelas informasi keamanan siber dan memudahkan pemahaman tentang sifat dan sumber serangan. Visualisasi data biasanya berupa grafik, diagram, atau peta.

Skala dalam visualisasi mungkin saja disesuaikan untuk memberikan gambaran yang menarik saat melihat data yang disajikan tanpa mengurangi informasi yang diberikan.

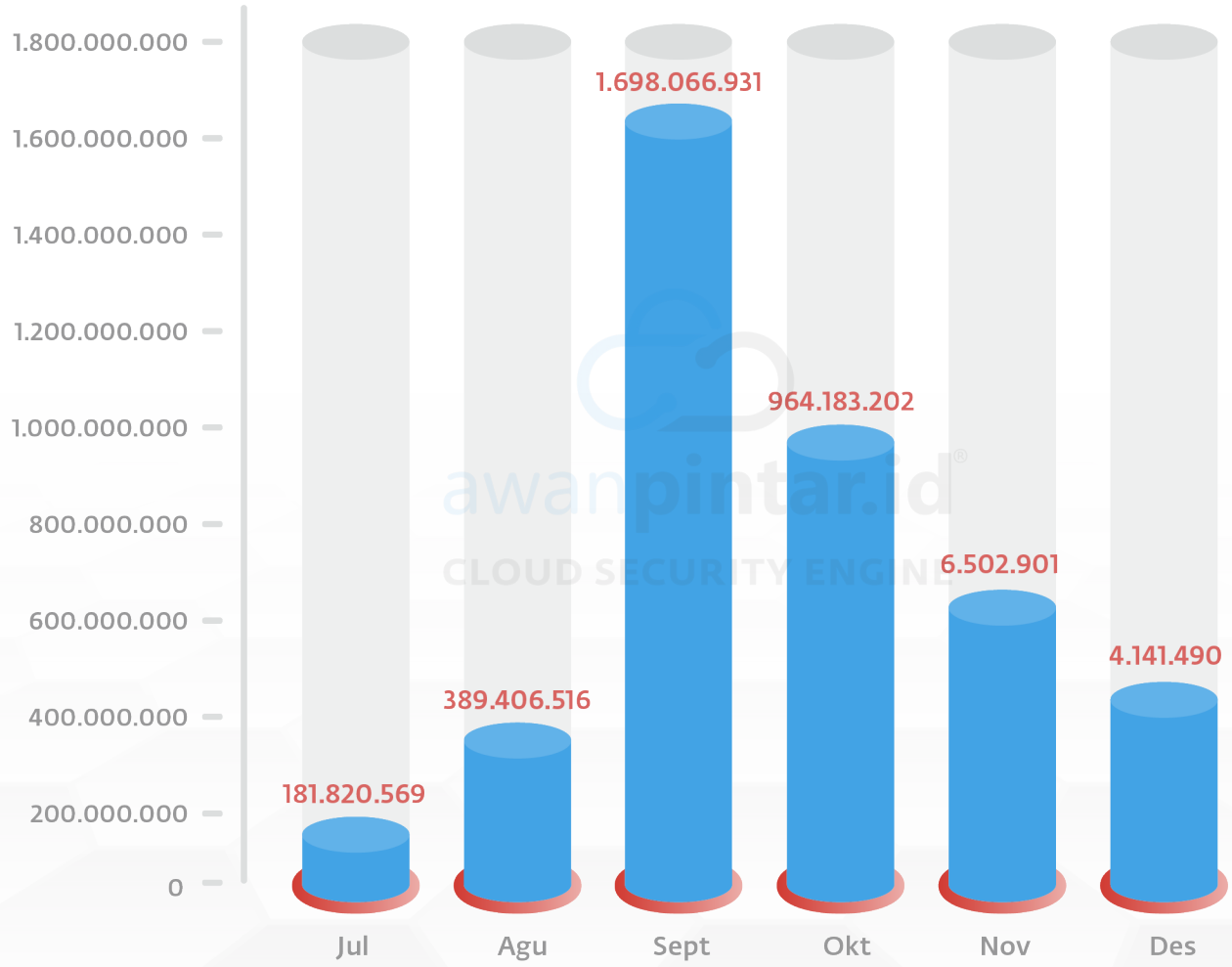
Green
OPEN

TREN SERANGAN TERKINI

Akumulasi Serangan Siber di Indonesia

Berikut ini merupakan data yang diambil secara rata-rata pada sebuah detektor pada Semester 2 dan rata-rata di tahun 2024. Secara umum dapat diartikan, saat sebuah perangkat komputer yang memiliki sebuah IP publik mulai terhubung ke jaringan internet, maka tidak lama kemudian akan dikenali dan dipelajari untuk dicari titik lemah untuk mulai dilakukan infiltrasi.

Rata-rata serangan per detik	Rata-rata serangan per menit	Rata-rata serangan per jam	Rata-rata serangan per hari
204	12.243	734.628	17.631.095



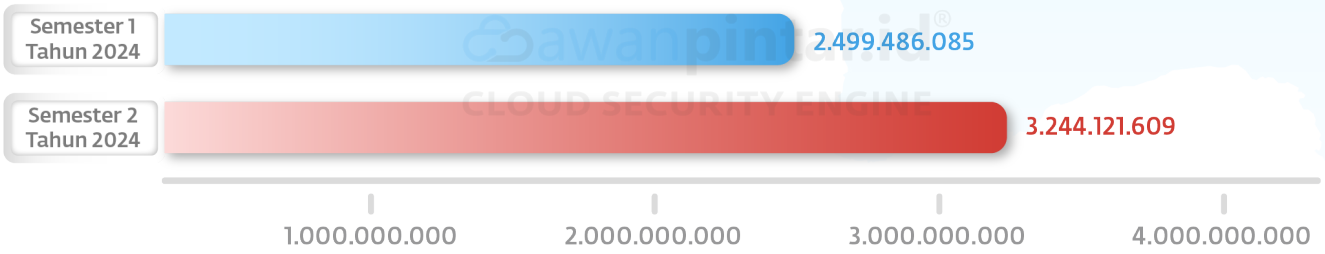
Jumlah total seluruh serangan 3.244.121.609

Green
OPEN

Komparasi total Serangan Semester 2 Tahun 2023 dan Semester 2 Tahun 2024

Jumlah Serangan Meningkat **2.558.349.108** atau **373,06%**

Komparasi total Serangan Semester 1 Tahun 2024 dan Semester 2 Tahun 2024



Jumlah Serangan Meningkat **794.635.524** atau **32,44%**

Memasuki semester 2 tahun 2024 serangan siber di Indonesia melemah dibandingkan akhir semester sebelumnya. Jika ditilik dari bulan ke bulan serangan siber yang terjadi sangat fluktuatif. Meski demikian, dengan total serangan sebesar 3.244.121.609 keamanan digital di Indonesia masih berada di kondisi yang bahkan lebih buruk semester sebelumnya.

Catatan khusus ada di bulan September dan Oktober yang meningkat tajam seiring dengan meningkatnya diskusi mengenai pelarangan judi online dan mulai efektifnya satgas yang dibentuk. Pada bulan September, terjadi serangan siber di tanah air terhadap institusi pemerintah. Untuk bulan Oktober, catatan penting politik di tanah air adalah adanya pergantian Presiden Republik Indonesia.

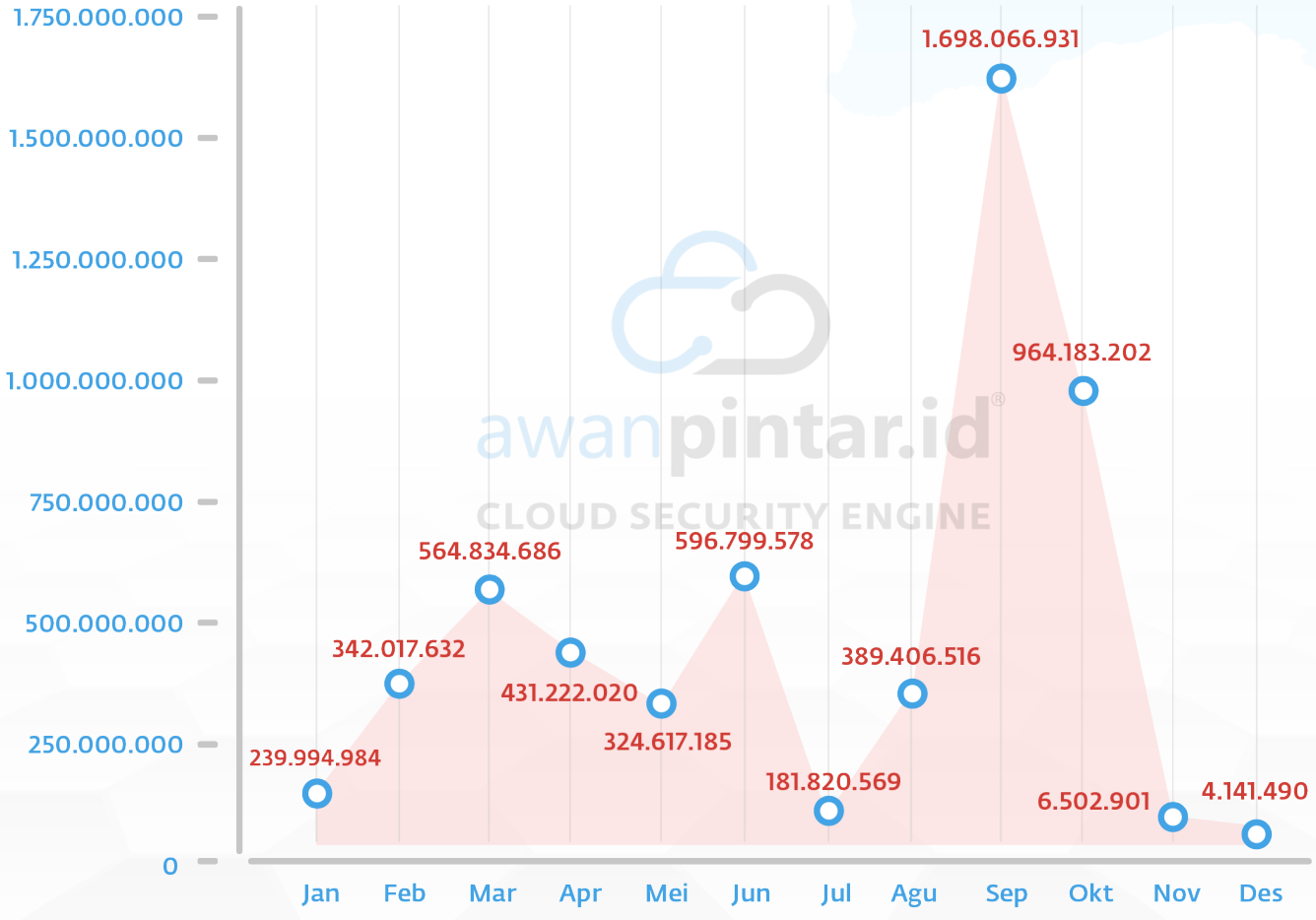
Walaupun di akhir tahun mengalami depresiasi yang sangat luar biasa, menurunnya serangan bisa berarti bahwa penyerang lebih fokus dalam menentukan target serangan. Ini seperti ketenangan sebelum badai, dimana serangan berikutnya biasanya akan meningkat dengan dampak yang lebih buruk.

Green
OPEN

Rata-rata Serangan per Detektor Selama Tahun 2024

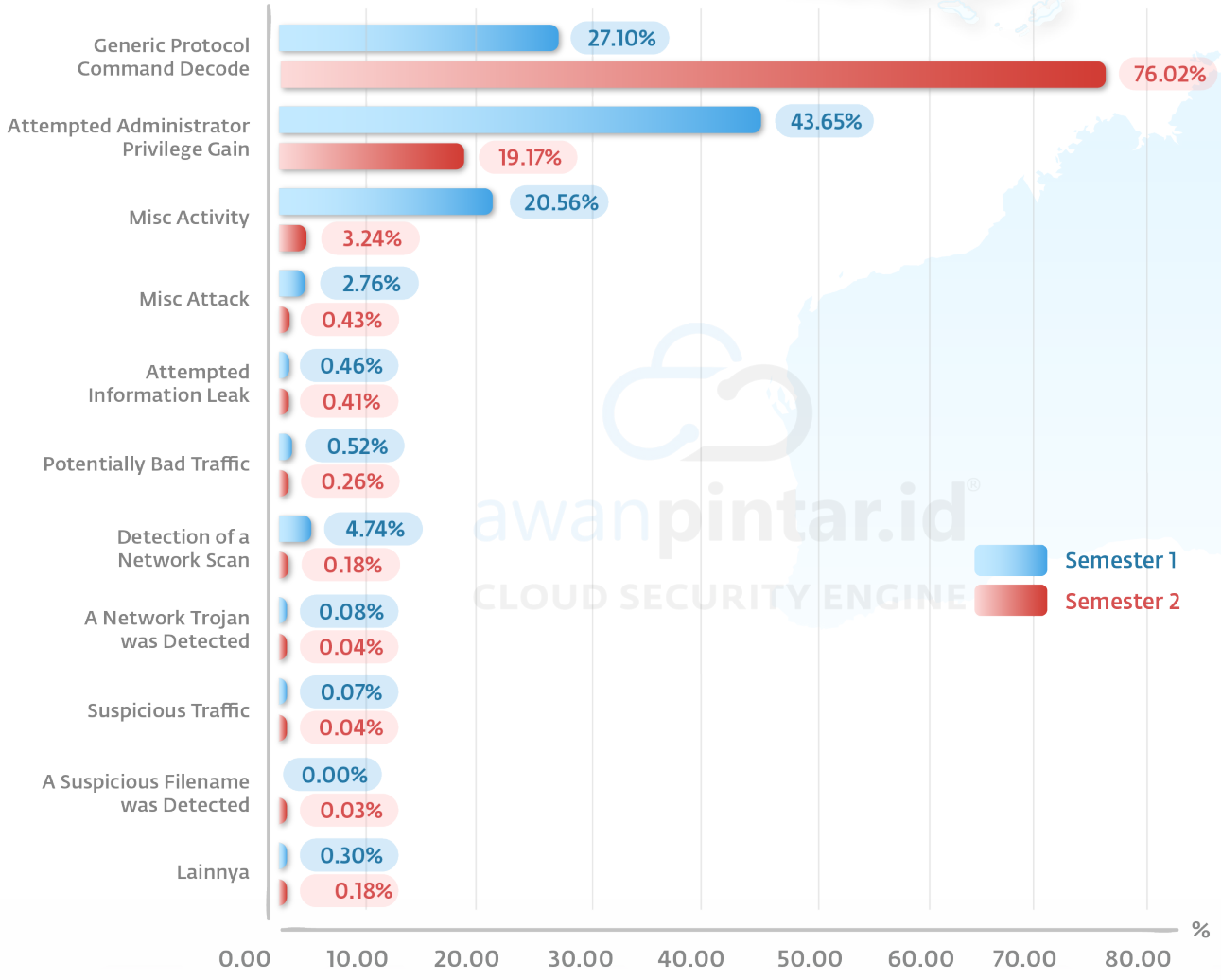
	Semester 1	Semester 2	Rata-rata 2024
Serangan per detik	159	204	182
Serangan per menit	9.537	12.244	10.890
Serangan per jam	572.227	734.629	653.428
Serangan per hari	13.733.440	17.631.096	15.682.268

Serangan Siber Selama Tahun 2024



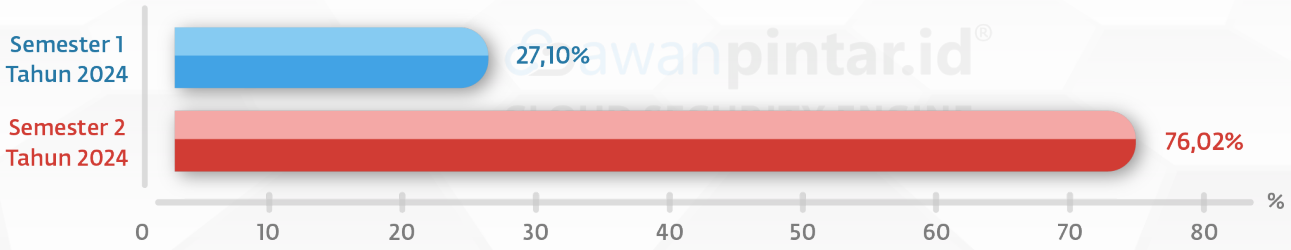
Green
OPEN

10 Jenis Serangan Siber Teratas



Generic Protocol Command Decode

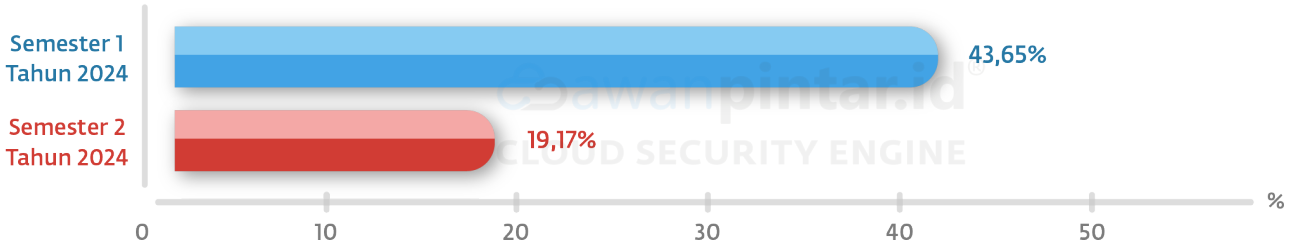
Identifikasi anomali pada paket data protokol jaringan yang tidak diharapkan atau tidak sah. Metode ini dapat digunakan untuk mendeteksi serangan siber yang menggunakan teknik manipulasi atau mencampuradukan protokol jaringan. Salah satu teknik serangan seperti ini adalah DDoS yang memanfaatkan kelemahan untuk melumpuhkan atau mendapatkan hak akses.



Hasil olah data oleh AwanPintar.id® terdapat perbedaan yang signifikan dalam jumlah serangan jaringan di semester 2 tahun ini dibanding semester 1 di tahun yang sama, dengan terjadi **peningkatan sebesar 48,92%.**

Attempted Administrator Privilege Gain

Upaya untuk mengakses atau mengungkap informasi yang seharusnya tidak dapat diakses orang yang tidak berhak. Hal ini dapat terjadi ketika pelaku mencoba mengambil informasi sensitif seperti akun, data klien, informasi kartu kredit atau informasi penting lainnya.

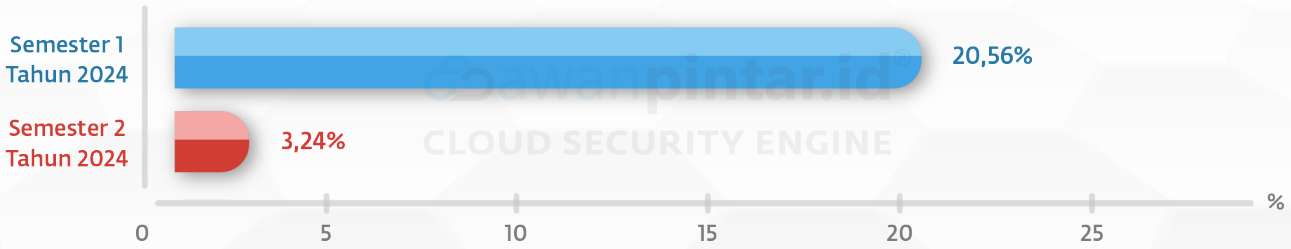


Pencurian informasi merupakan favorit bagi pelaku kejahatan siber, yang menarik adalah besarnya **penurunan hingga -24,48%.** Depresiasi mungkin disebabkan serangan yang dilakukan saat ini lebih berupa serangan acak yang ditujukan secara sembarang dengan tujuan melumpuhkan sebuah sistem.

Misc Activity

Miscellaneous activity mengacu pada aktivitas apa pun yang tidak mudah dikategorikan ke dalam kategori ancaman tertentu. Istilah ini sering digunakan untuk menggambarkan perilaku anomali atau mencurigakan pada jaringan atau sistem yang tidak dapat langsung diidentifikasi sebagai jenis serangan tertentu.

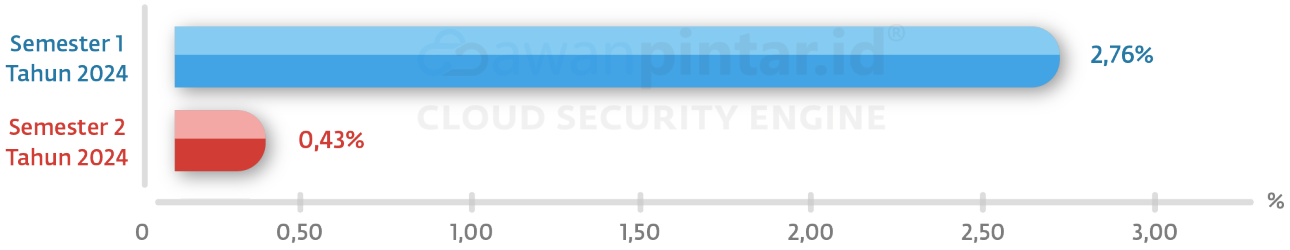
Aktivitas lain-lain dapat mencakup pemindaian port, pengintaian jaringan, atau jenis aktivitas lain yang berpotensi digunakan sebagai pendahulu serangan yang lebih serius. Meskipun aktivitas lain-lain mungkin tidak langsung mengancam, penting bagi profesional keamanan siber untuk memantau dan menyelidiki jenis peristiwa ini untuk mencegah potensi ancaman berkembang menjadi serangan yang lebih serius.



Semester 2 tahun 2024 mungkin paling mencolok dalam tren perubahan serangan siber, dimana berbagai aktivitas mencurigakan yang merupakan bagian dari tahapan serangan siber mengalami **retrogresi drastis hingga -17,32%.** Hal ini terjadi karena pelaku melakukan serangan yang sangat terkoordinasi dan terarah dalam menentukan target.

Misc Attack

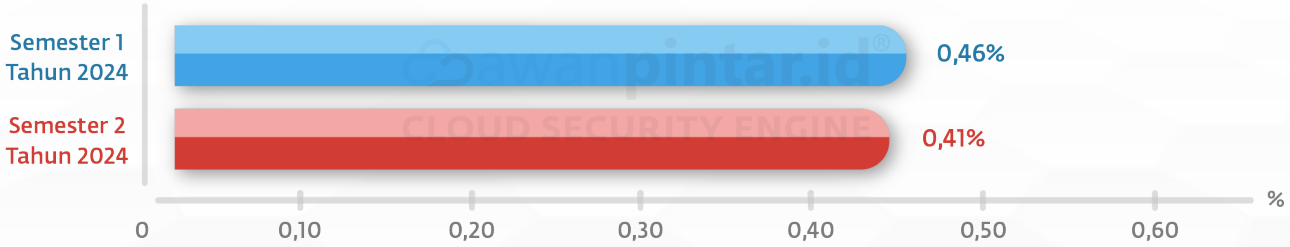
Jenis serangan ini mengeksploitasi server web yang rentan dengan memaksa server cache atau browser web untuk mengungkapkan informasi kredensial, kata sandi, dan informasi yang disimpan. Atau serangan dengan sifat membajak komunikasi yang sedang dilakukan dan serangan pada protokol HTTP.



Dalam deteksi serangan ini terjadi **penurunan -2,33%** dalam upaya pembajakan komunikasi dan eksploitasi server web. Ini merupakan dampak peralihan jenis serangan pencurian kredensial dan serangan yang semakin tertarget.

Attempted Information Leak

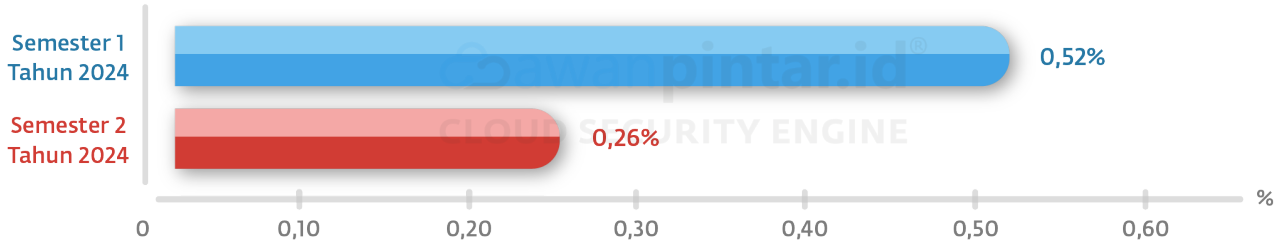
Upaya untuk mengakses atau mengungkap informasi yang seharusnya tidak dapat diakses orang yang tidak berhak. Hal ini dapat terjadi ketika pelaku mencoba mengambil informasi sensitif seperti akun, data klien, informasi kartu kredit atau informasi penting lainnya.



Pencurian informasi sensitif menurun terus sepanjang tahun 2024 walaupun tidak sebesar semester sebelumnya, dengan **penurunan -0,05%** menunjukkan adanya peningkatan dalam kesadaran keamanan pengguna dalam melindungi identitas pribadi dan finansial mereka di internet.

Potentially Bad Traffic

Mencakup lalu lintas yang benar-benar di luar kebiasaan, dan berpotensi menunjukkan adanya sistem yang disusupi. Sistem yang dikuasai dapat berakibat fatal bagi perusahaan, pelaku dapat melakukan manipulasi dan eksploitasi tanpa batas.

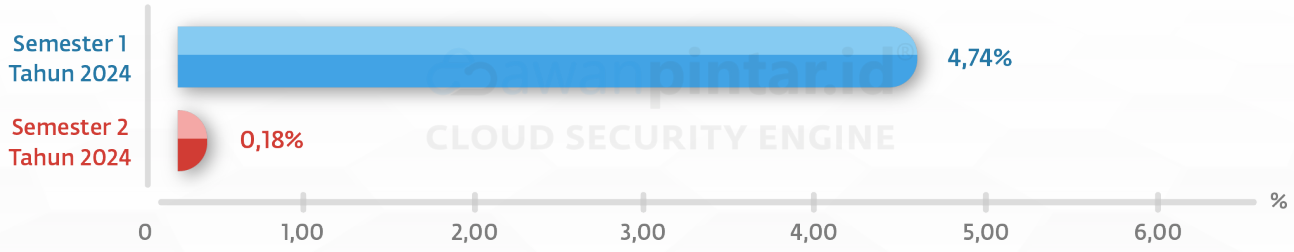


Tindakan penyusupan yang dapat berakibat manipulasi dan eksploitasi tanpa batas juga mengalami **penurunan** yakni sebesar **-0,26%.** Ini merupakan kabar positif bagi dunia usaha, menunjukkan banyak perusahaan memiliki kesadaran kolektif dalam membangun sistem pertahanan yang kuat didukung dengan edukasi karyawan yang baik.

Detection of a Network Scan

Adanya aktivitas ilegal yang melibatkan pendeteksian semua host aktif di jaringan dan memetakan ke alamat IP mereka. Penyerang sering menggunakannya untuk melakukan pengintaian sebelum mencoba menembus jaringan.

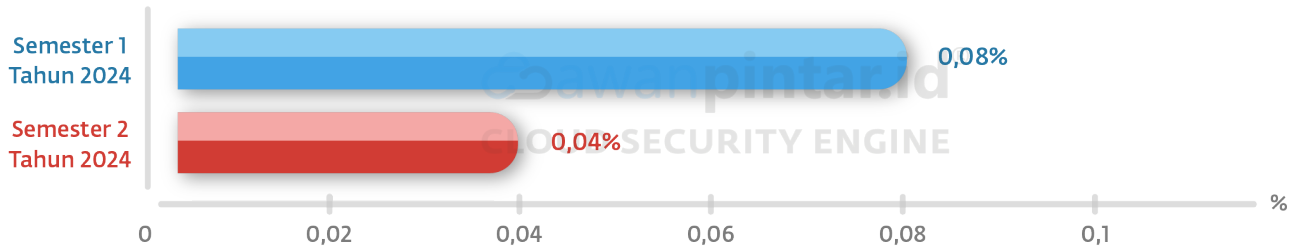
Serangan seperti SUNBURST dapat menggunakan pemindaian jaringan untuk mendapatkan posisi awal serangan. SUNBURST adalah serangan rantai pasokan yang memanfaatkan backdoor yang ditanamkan pada pemasok untuk menargetkan dan mengkompromikan organisasi secara tidak langsung di seluruh dunia.



Reduksi ancaman pada kategori ini semakin menegaskan bahwa penjahat siber terus berbenah dengan menggunakan cara yang paling efektif dalam pergerakkan mereka, **penurunan -4,56%** telah menunjukkan semua.

A Network Trojan was Detected

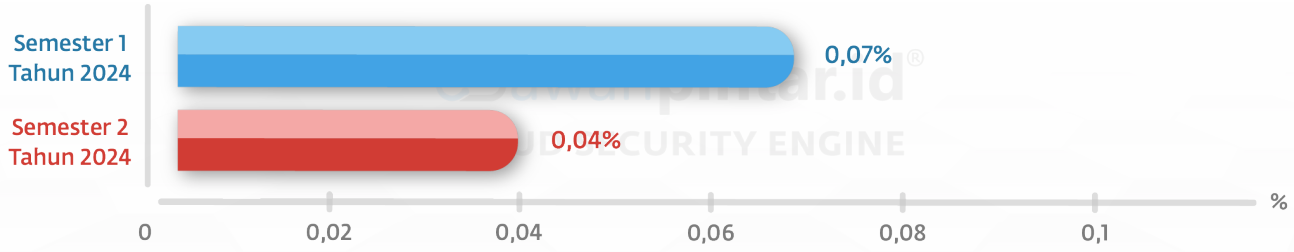
Jenis perangkat lunak berbahaya, yang disebut Trojan, telah terdeteksi di komputer atau jaringan yang dirancang untuk memungkinkan akses tidak sah ke komputer atau jaringan tersebut. Trojan dapat digunakan oleh penjahat dunia maya untuk mengontrol komputer dari jarak jauh, mencuri data sensitif, atau menyebarkan malware lebih lanjut. Beberapa sumber umum Trojan diantaranya email phishing, drive by download, dan unduhan perangkat lunak dari sumber yang tidak terpercaya.



Serangan siber menggunakan trojan horse pada semester 2 tahun 2024 yang didapat dari data AwanPintar.id® mengalami **penurunan 0,04%**, yang artinya upaya trojanisasi tidak berkembang dengan baik seperti semester tahun sebelumnya.

Suspicious Traffic

Klasifikasi deteksi Suspicious Traffic dapat menyesatkan. Aturan yang dikategorikan sebagai mencurigakan dapat bersifat berbahaya dan mengindikasikan adanya gangguan. Sifat lalu lintas yang didefinisikan sebagai mencurigakan bergantung pada situasi di mana lalu lintas tersebut ditemukan.

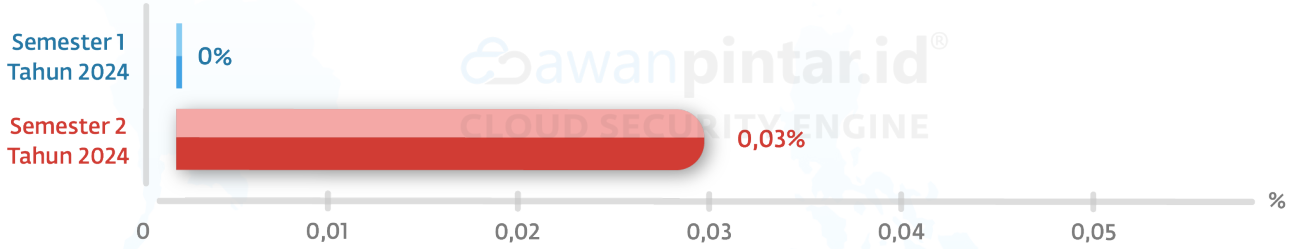


Pergeseran angka yang tidak istimewa yakni **-0,03%** pada ancaman ini, merupakan sinyal positif karena potensi ancaman melalui lalu lintas jaringan **menurun** lebih dari setengah.

A Suspicious Filename was Detected

Salah satu mekanisme penting yang digunakan untuk menjaga keamanan sistem dan data penting yang terintegrasi adalah Deteksi Berkas Mencurigakan. Deteksi ini adalah proses dalam menangani berkas mencurigakan. Berkas-berkas ini berisi kode, skrip, lampiran, atau tautan unduhan yang berpotensi menyebabkan kerusakan atau membahayakan keamanan sistem secara keseluruhan.

Deteksi berkas mencurigakan berfungsi sebagai garis depan pertahanan di bidang keamanan siber. Ini memberikan pendekatan proaktif dan preventif, yang mampu mengidentifikasi potensi ancaman bahkan sebelum menimbulkan kerusakan atau membahayakan sistem. Menjaga integritas sistem, melindungi kumpulan data yang berharga, memastikan kelancaran operasi, dan menjaga kepercayaan pengguna akhir adalah tujuan utama yang mendorong deteksi berkas mencurigakan. Umumnya berkas ini merupakan vektor sebuah malware.



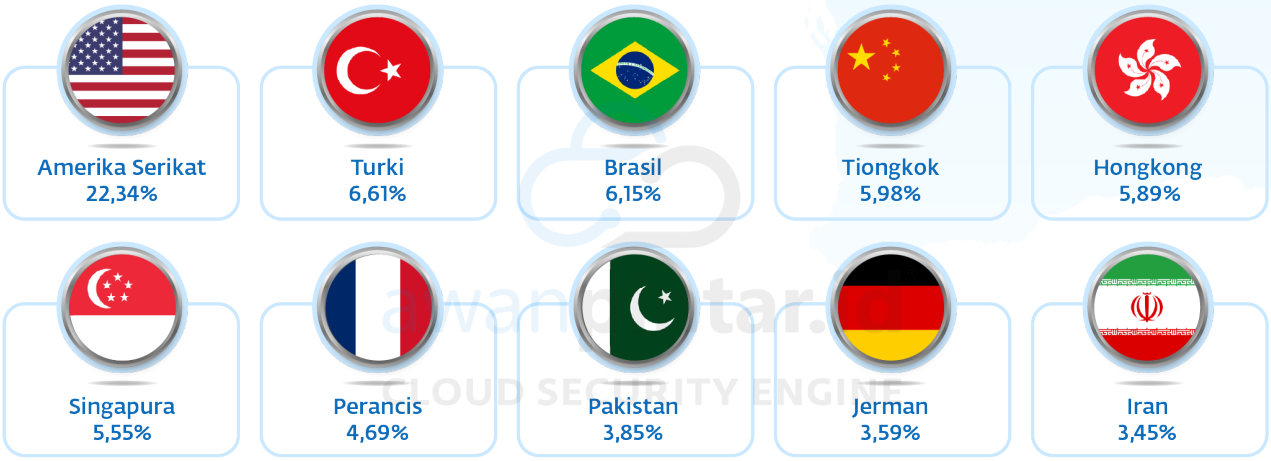
Dari data terbaru AwanPintar.id® dari **kategori ancaman baru** yang ditemukan berkaitan dengan dokumen/berkas, skrip, lampiran atau tautan unduhan yang berbahaya, didapati **0,03%** serangan dalam jaringan internet nasional.

10 Negara Kontributor Serangan Siber

Mengikuti perkembangan jaman dengan mengaplikasikan berbagai teknologi maju dan terhubung secara digital tidak datang tanpa risiko dan konsekuensi. Karakteristik seperti ini, dapat menimbulkan bahaya karena dapat membuka celah yang lebih besar untuk dieksploitasi.

Seperti Indonesia misalnya, yang sering menjadi sasaran serangan siber dari negara lain karena memiliki kerentanan yang dideteksi oleh para pelaku yang berasal dari negara lain. Berikut adalah data negara-negara yang selama periode kedua tahun 2024 paling sering melakukan serangan siber ke Indonesia.

Semester 1 Tahun 2024

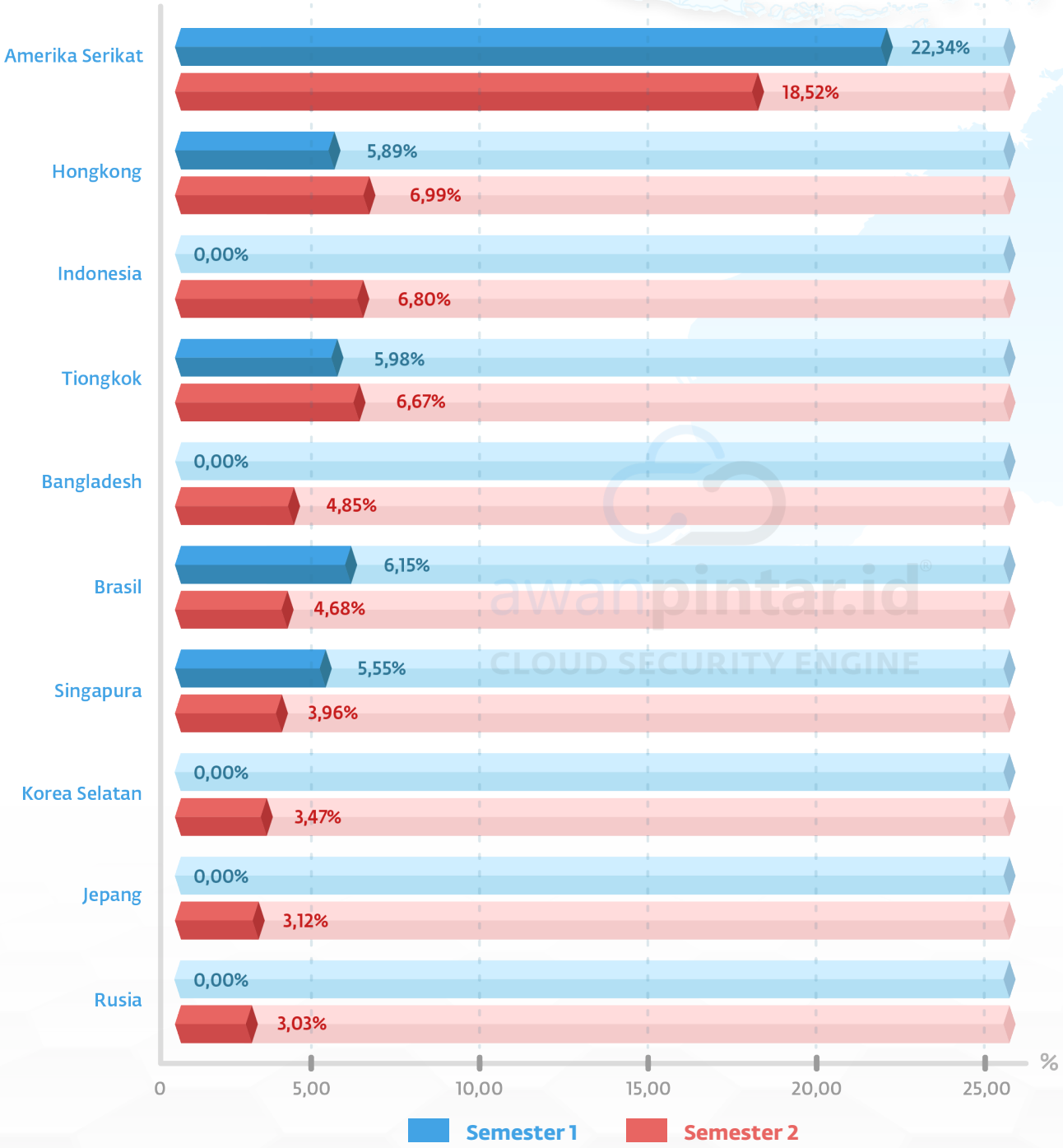


Lainnya **31,90%**

Semester 2 Tahun 2024

Lainnya **37,91%**

10 Negara Kontributor Serangan Siber 2024



Amerika Serikat (Menurun -3,82%)
Hongkong (Meningkat 1,10%)
Indonesia (Negara Ancaman Baru)
Tiongkok (Meningkat 0,69%)
Bangladesh (Negara Ancaman Baru)
Brasil (Menurun -1,47%)
Singapura (Menurun -1,59%)
Korea Selatan (Negara Ancaman Baru)
Jepang (Negara Ancaman Baru)
Rusia (Negara Ancaman Baru)

Bila kita melihat hasil serapan data dari AwanPintar.id® kita melihat banyak penurunan serangan dan munculnya negara-negara baru yang masuk sebagai ancaman baru.

Negara-negara yang selama ini konsisten melakukan serangan siber secara terus-menerus seperti Amerika Serikat, Brasil, dan Singapura mengalami penurunan yang bervariasi. Sementara Hongkong dan Tiongkok mengalami peningkatan serangan.

Yang patut disoroti yakni kehadiran beberapa negara baru yang jumlahnya lebih besar dari semester sebelumnya. Indonesia, Bangladesh, Korea Selatan, Jepang dan Rusia menggeser posisi Turki, Perancis, Pakistan, Jerman dan Iran. Namun jika dijumlahkan secara keseluruhan jumlah serangan negara ancaman baru lebih sedikit dari negara yang mereka geser.

Di sisi lain kita melihat ada peningkatan cukup signifikan dari serangan yang berasal dari Indonesia, serangan dari dalam negeri yang sebelumnya berada di luar 10 besar kini langsung naik ke posisi 3. Berkembang pesatnya serangan yang berasal dari negara sendiri tidak menjadi gambaran seutuhnya. Banyak proxy di dalam negeri yang menjadi batu loncatan penyerang dari luar juga bisa menjadi penyebabnya.

10 IP Penyerang Teratas

AwanPintar.id® yang selalu mengawasi setiap lalu lintas yang keluar masuk infrastruktur jaringan Indonesia mencatat berbagai ancaman yang dilakukan melalui serangan alamat IP.

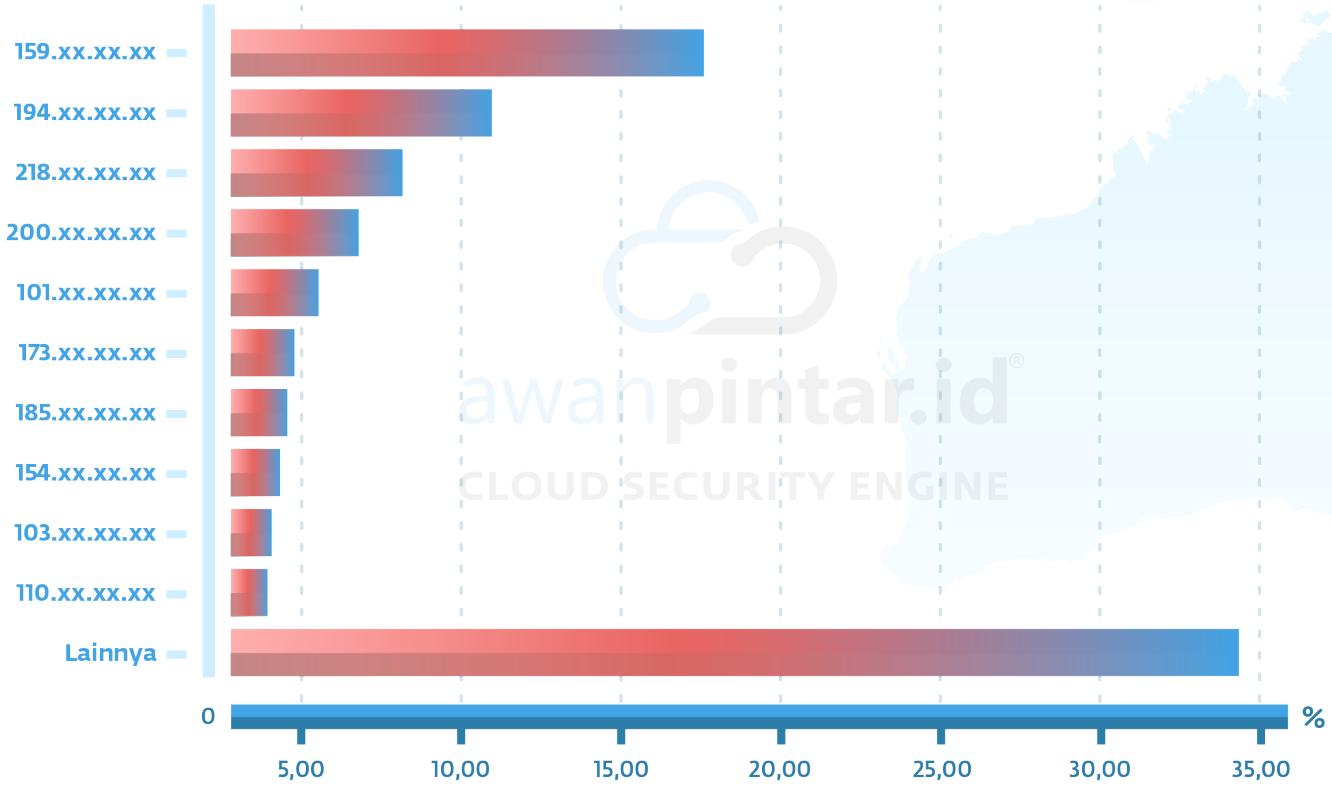
Pelaku kejahatan siber sering menyamarkan komunikasi dari sumber yang tidak dikenal sebagai dari sumber yang dikenal dan terpercaya. Mereka dapat menggunakan IP spoofing untuk mendapatkan akses ke informasi pribadi, menyebarkan malware, atau mendistribusikan ulang lalu lintas. Berikut IP dan negara asal penyerang pada semester 2 tahun 2024.

159.xx.xx.xx Amerika Serikat	17,71%	173.xx.xx.xx Amerika Serikat	4,91%
194.xx.xx.xx Rusia	11,38%	185.xx.xx.xx Indonesia	4,56%
218.xx.xx.xx Korea Selatan	8,15%	154.xx.xx.xx Jepang	4,34%
200.xx.xx.xx Venezuela	7,03%	103.xx.xx.xx Hongkong	4,16%
101.xx.xx.xx Malaysia	5,39%	110.xx.xx.xx Thailand	3,68%

Lainnya 34,69%

Green
OPEN

10 IP Penyerang Teratas Semester 2 Tahun 2024



Belanda yang mendominasi di semester 1 tahun 2024 dan semester 2 tahun 2023 hilang dari peredaran dalam serangan IP. Sedangkan Amerika tetap konsisten dari tahun ke tahun meskipun dari total serangan mereka mengalami penurunan.

Ancaman serangan IP dari Indonesia dalam pantauan AwanPintar.id® juga mengalami peningkatan dibanding semester sebelumnya. Ini juga dapat dimaknai bahwa serangan tersebut bisa juga merupakan serangan kamuflase yang berasal dari luar Indonesia yang memanfaatkan alamat IP yang berhasil mereka kuasai.

Dari negeri jiran, serangan IP kini arahnya anginnya berubah dari Singapura berganti dengan Malaysia. Thailand membuat catatan baru sebagai negara yang baru kali ini masuk dalam 10 besar IP penyerang teratas.

Ancaman Pencurian Kredensial

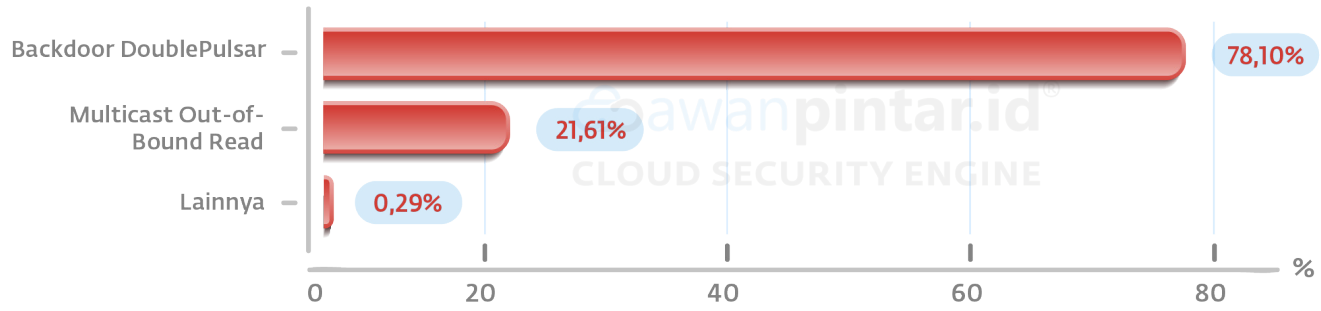
Administrator Privilege

Serangan yang memanfaatkan backdoor DoublePulsar sebagai jalan masuk untuk melakukan pencurian kredensial menurun sangat jauh, meski jumlahnya masih bisa dibilang cukup besar. Penyerang mengalihkan serangan masif mereka pada eksploitasi kerentanan yang mampu mencuri informasi sensitif langsung dari memori yang lebih menjanjikan dalam memperoleh data-data penting.

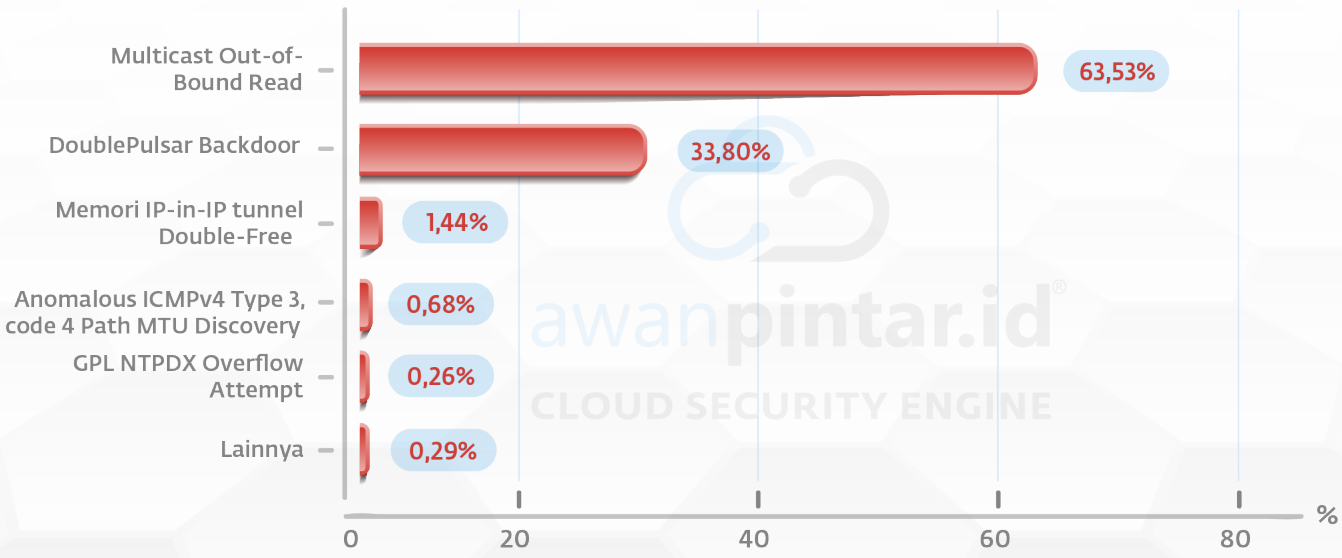
AwanPintar.id® juga mencatat ancaman-ancaman baru yang memanfaatkan celah-celah baru dalam sistem dalam upaya pencurian kredensial. Jumlah serangan yang minim tidak boleh disepelekan, ke depan ancaman ini bisa saja dieksploitasi secara besar-besaran jika lubang baru tersebut tidak diamankan dari sekarang.

Komparasi Administrator Privilege Gain Semester 1 dan Semester 2

Semester 1 Tahun 2024

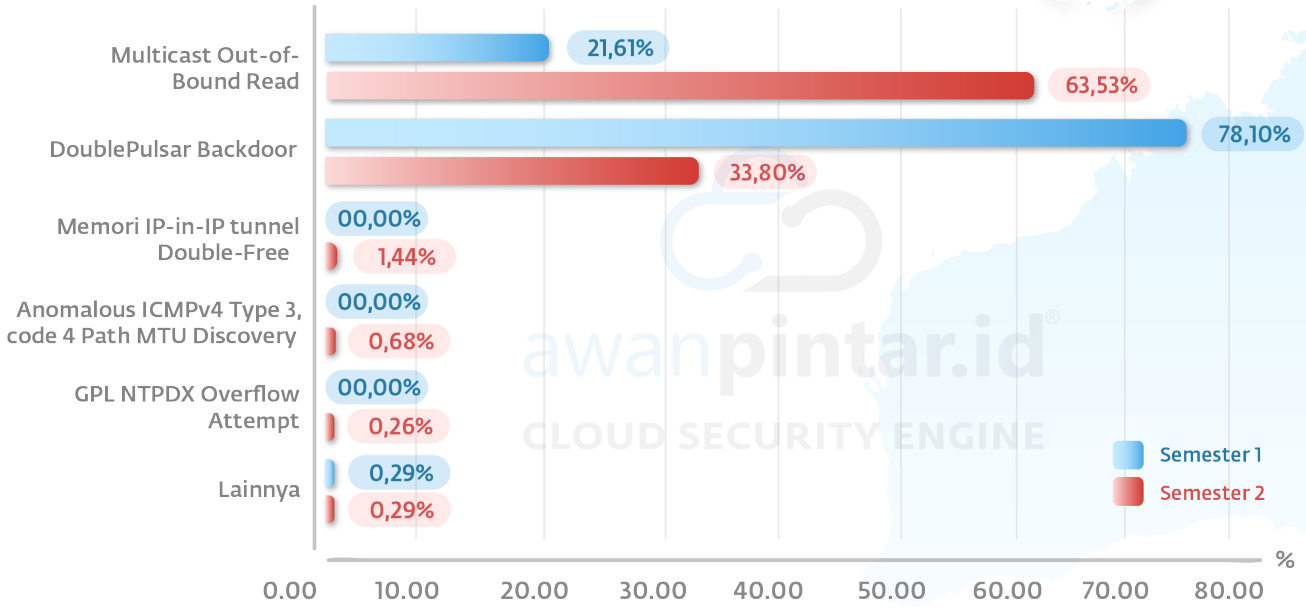


Semester 2 Tahun 2024



Green
OPEN

Attempted Administration Privilege Gain Tahun 2024



Multicast Out-of-Bound Read
Meningkat **41,92%**

IP-in-IP tunnel Double-Free
Ancaman Baru

DoublePulsar Backdoor Installation Communication
Menurun **-44,30%**

Anomalous ICMPv4 Type 3 , Code 4 Path MTU Discovery
Ancaman Baru

GPL NTPDX Overflow Attempt
Ancaman Baru

Multicast Out-of-Bound Read

Validasi input yang tidak benar dalam komponen IPv6 saat menangani paket yang dikirim oleh penyerang jaringan. Kerentanan ini memungkinkan Out-of-bound Read dan kemungkinan Denial of Service Produk membaca data setelah akhir atau sebelum awal dari buffer yang dimaksud. Biasanya, ini memungkinkan penyerang membaca informasi sensitif dari lokasi memori lain atau menyebabkan kerusakan.

DoublePulsar Backdoor Installation Communication

DoublePulsar adalah backdoor implan yang memungkinkan injeksi DLL, eksekusi kode arbitrer. Hal ini memberikan peluang bagi penyerang untuk melanjutkan serangan dengan memasukkan kode berbahaya apa pun yang mereka pilih, sehingga menghasilkan kompromi total.

Serangan ini sangat tersembunyi dan operator sistem tidak akan menyadari adanya gangguan kecuali ada kesalahan yang dilakukan oleh penyerang. Oleh karena itu, banyak sistem yang disusupi kemungkinan besar akan tetap terinfeksi selama beberapa waktu sebelum intrusi ditemukan.

Backdoor DoublePulsar juga digunakan oleh EternalBlue yang merupakan eksploit SMBv1 (Server Message Block 1.0) yang dapat memicu RCE dan menyerang layanan berbagi file SMB. Untuk memahami Backdoor DoublePulsar kita harus tahu bahwa semua berpusat pada protokol SMB dan itu bergantung pada port 445 untuk mengaktifkan jaringan dan di sini letak kelemahannya. Dapat dikatakan, Backdoor DoublePulsar merupakan jalan masuk bagi malware lainnya.

IP-in-IP Tunnel Double-Free

Masalah Double Free dalam komponen tunneling IPv4 saat menangani paket tertentu, yakni saat menangani paket yang dikirim oleh penyerang jaringan. Kerentanan ini dapat mengakibatkan Use-After-Free (UAF).

Use-After-Free (UAF) adalah skenario kerentanan yang diakibatkan oleh manajemen memori yang tidak efisien saat mengembangkan aplikasi perangkat lunak. Secara sederhana, hal ini terjadi saat bahasa pemrograman modern memungkinkan programmer untuk mengalokasikan memori secara dinamis saat dijalankan.

Penyerang dapat mengeksploitasi kerentanan UAF untuk membahayakan sistem dan mengeksekusi kode berbahaya. Hal ini dapat mencakup kebocoran data, peningkatan hak istimewa, aplikasi crash, atau menyebabkan kerusakan lainnya.

Anomalous ICMPv4 Type 3, Code 4 Path MTU Discovery

Proses PMTUD menetapkan tanda "Don't Fragment" (DF) di header IP paket keluar. Jika antarmuka keluar router memiliki Maximum Transmission Unit (MTU) yang lebih kecil daripada paket, maka router akan membuang paket dan mengirimkan kembali pesan ICMP tipe 3, kode 4. Pesan ini memberitahu host sumber bahwa tujuan tidak dapat dijangkau, fragmentasi diperlukan, dan tanda "Don't Fragment" telah ditetapkan.

Tujuannya agar host sumber kemudian mengurangi jalurnya MTU dan mengulangi proses tersebut hingga MTU cukup kecil untuk melewati seluruh jalur tanpa fragmentasi. Hal ini mencegah fragmentasi dan memastikan bahwa paket tidak dibuang.

Firewall yang salah dikonfigurasi sehingga menjatuhkan paket ICMP adalah masalah umum pada PMTUD. Untuk melindungi CPU router dari serangan DoS, ia mungkin membatasi jumlah pesan ICMP yang tidak dapat dijangkau yang dikirimkannya menjadi dua pesan per detik.

GPL EXPLOIT NTPDX Overflow Attempt

Penyerang mengeksploitasi masalah buffer overflow dengan menimpa memori aplikasi. Ini mengubah jalur eksekusi program, memicu respons yang merusak file atau mengungkap informasi pribadi. Misalnya, seorang penyerang dapat memasukkan kode tambahan, mengirimkan instruksi baru ke aplikasi untuk mendapatkan akses ke sistem TI.

Jika penyerang mengetahui tata letak memori suatu program, mereka dapat dengan sengaja memasukkan input yang tidak dapat disimpan oleh buffer, dan menimpa area yang menyimpan kode yang dapat dieksekusi, menggantinya dengan kode mereka sendiri. Sebagai contoh, penyerang dapat menimpa pointer (objek yang menunjuk ke area lain di memori) dan mengarahkannya ke payload exploit, untuk mendapatkan kendali atas program.

Attempted Information Leak

Setiap memasuki semester baru jenis kejahatan siber terus bertambah atau saling mengisi silih berganti, beragamnya variasi serangan menunjukkan bahwa penjahat dunia digital senantiasa mencoba segala cara, atau menguji semua kemungkinan untuk mendapatkan titik serang baru.

Sementara pada ancaman kambuhan yang berulang kali melakukan serangan pada titik yang sama angka serangannya terjun bebas pada satu kategori tapi mengalami eskalasi serangan pada kategori lain dengan jumlah serangan yang cukup besar.

Sehingga dapat diterjemahkan bahwa upaya untuk mengambil informasi sensitif seperti akun, data klien, informasi kartu kredit atau informasi penting lainnya dari data AwanPintar.id® mengalami peningkatan yang progresif.

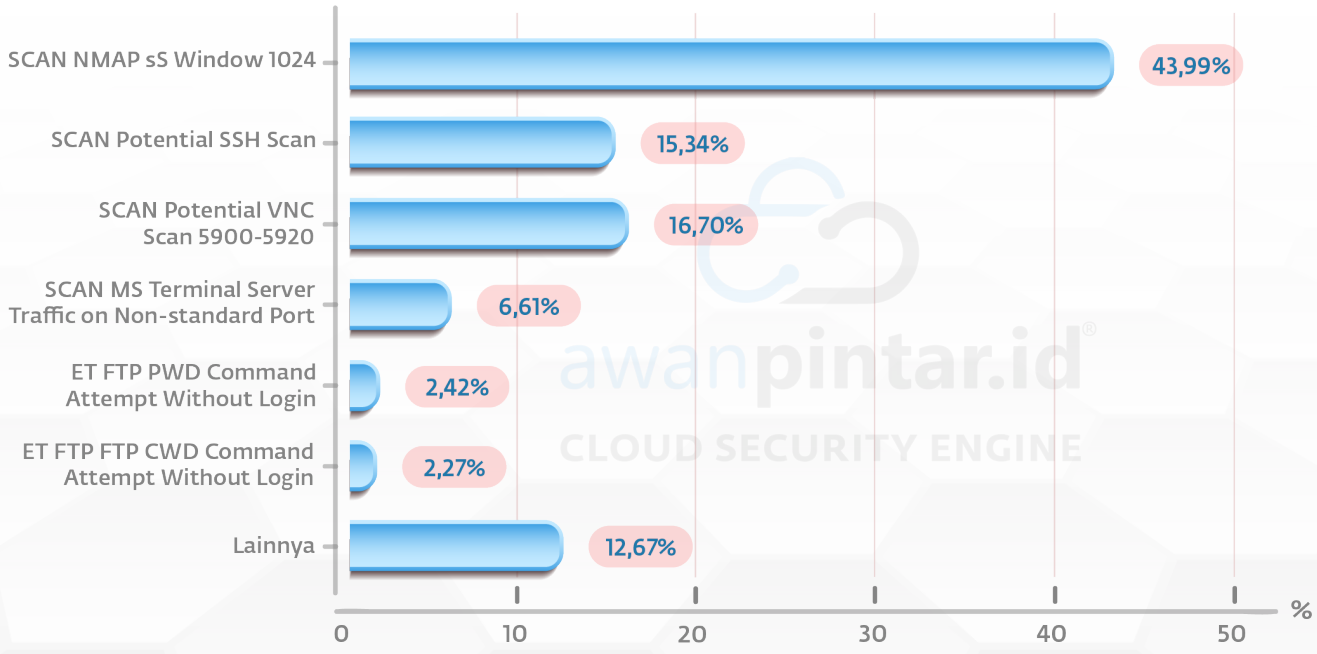
Serangan Brute Force RDP adalah serangan yang berupaya mengambil paksa hak akses ke jaringan, peningkatan ini didorong karena penyerang sudah mendapat pijakan di dalam sistem, mereka selangkah lagi untuk menguasai hak akses utama sehingga melakukan serangan secara besar-besaran.

Menurunnya upaya pencarian kerentanan melalui Nmap AwanPintar.id® melihat ini disebabkan karena penyerang sudah jauh hari memiliki pijakan di dalam sehingga fokus mereka bukan mencari kerentanan namun mendapatkan jalan untuk menguasai sistem.

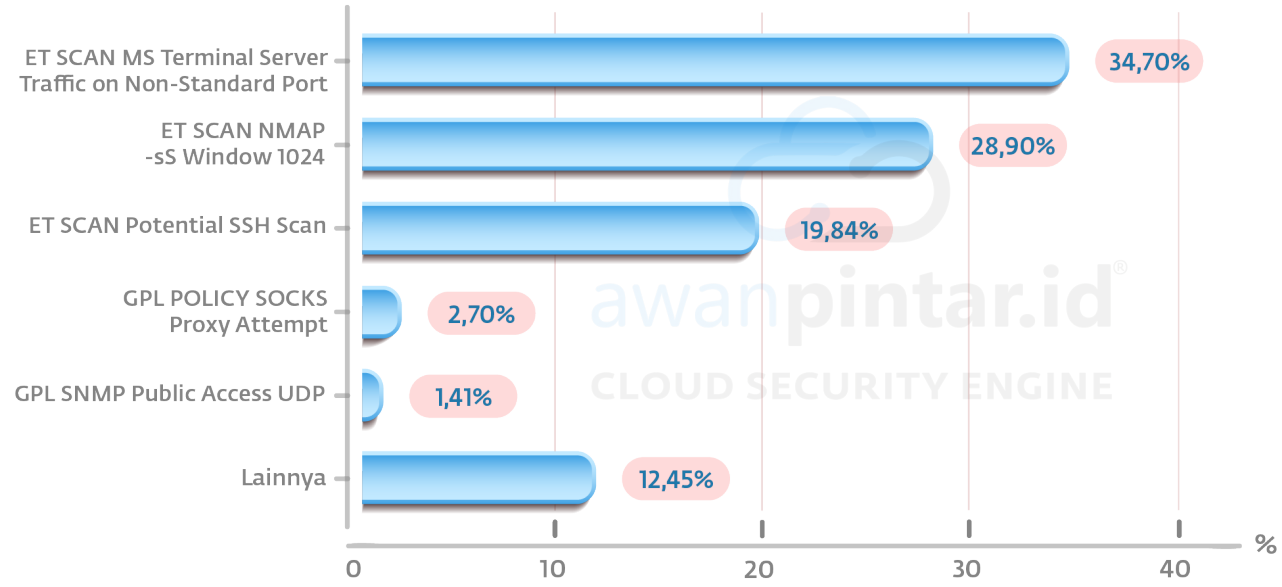
Selain dimonopoli oleh serangan lawas yang berulang pada jaringan internet Indonesia, ditemukan juga dua ancaman baru walaupun tidak signifikan, serangan ini tidak boleh dianggap remeh, setiap ruang yang berhasil dieksploitasi sudah dapat dinilai sebagai kerugian itu sendiri.

Komparasi Attempted Information Leak Semester 1 dan Semester 2

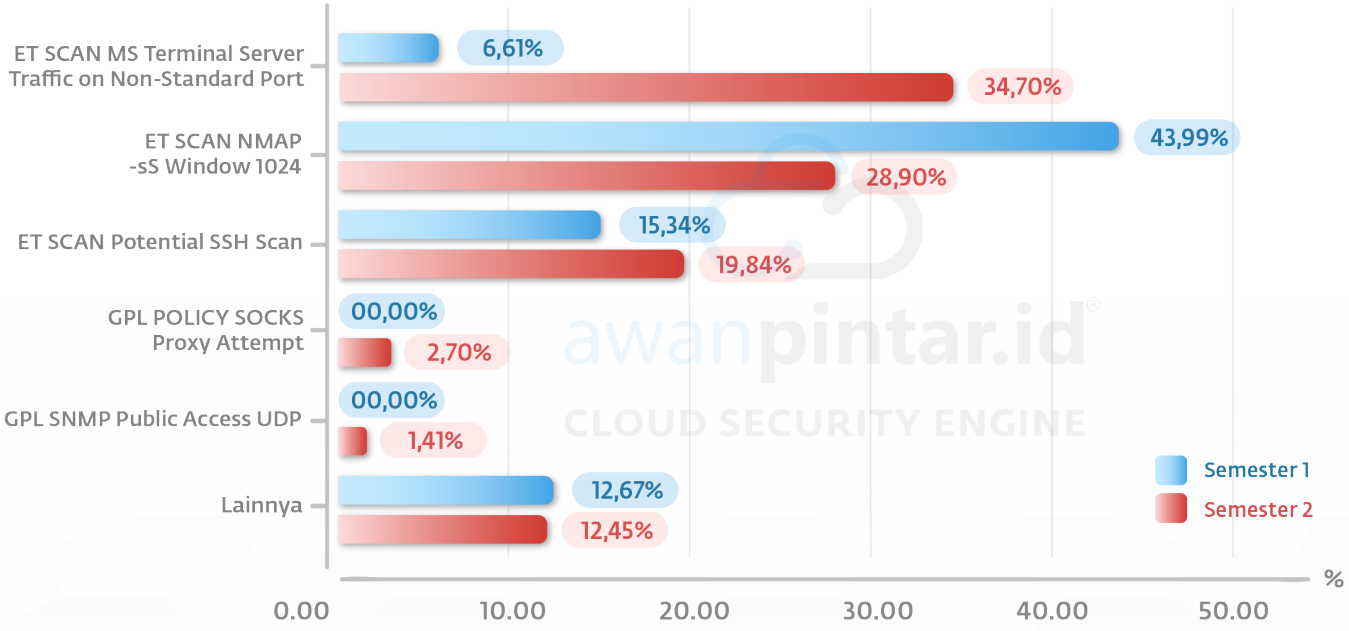
Semester 1 Tahun 2024



Semester 2 Tahun 2024



Attempted Information Leak Tahun 2024



ET SCAN MS Terminal Server Traffic on Non-Standard Port
Meningkat **28,09%**

IET SCAN NMAP -sS Window 1024
Menurun **-15,09%**

ET SCAN Potential SSH Scan
Meningkat **4,50%**

GPL POLICY SOCKS Proxy Attempt
Ancaman Baru

GPL SNMP PublicAccess UDP
Ancaman Baru

ET SCAN MS Terminal Server Traffic on Non-Standard Port

Brute Force RDP mengacu pada jenis serangan siber di mana penyerang secara sistematis berupaya mendapatkan akses tidak sah ke jaringan dengan berulangkali menebak atau "memaksa" kata sandi akun RDP.

Serangan Brute Force RDP dapat dilakukan oleh pelaku dengan berbagai motivasi, termasuk mencuri data sensitif, mendapatkan kendali sistem untuk eksploitasi lebih lanjut, atau menyebabkan gangguan pada jaringan atau sistem yang ditargetkan. Serangan ini bisa sangat efektif jika kata sandi yang digunakan lemah atau mudah ditebak.

ET SCAN Nmap -sS Window 1024

Nmap dapat digunakan oleh peretas untuk mengetahui akses ke port yang tidak terkontrol pada suatu sistem. Semua yang perlu dilakukan peretas untuk berhasil masuk ke sistem yang ditargetkan adalah menjalankan Nmap yang ditargetkan ke arah sistem itu, mencari kerentanan, dan mencari cara untuk mengeksploitasinya. Peretas bukan satu-satunya orang yang menggunakan platform perangkat lunak ini.

Perintah ini akan menjalankan pemindaian TCP SYNC dengan window size 1024 byte. Umumnya ini dilakukan untuk melakukan pengecekan maksimum windows size pada target sebelum dilakukan pengiriman paket data susulan.

ET SCAN Potential SSH Scan

Serangan Brute Force SSH adalah teknik peretasan yang melibatkan percobaan berulang kali kombinasi nama pengguna dan kata sandi yang berbeda hingga penyerang mendapatkan akses ke server jarak jauh. Penyerang menggunakan alat otomatis yang dapat mencoba ribuan kombinasi nama pengguna dan kata sandi dalam hitungan detik, menjadikannya cara yang cepat dan efektif untuk menyusupi server.

Serangan Brute Force SSH mengeksploitasi kata sandi lemah atau default yang biasa digunakan di server. Kata sandi ini dapat dengan mudah ditebak oleh penyerang menggunakan daftar kata sandi umum dan alat otomatis. Setelah penyerang mendapatkan akses, mereka kemudian dapat menggunakan server untuk tujuan jahat, seperti mencuri data atau melancarkan serangan lebih lanjut.

GPL POLICY SOCKS Proxy Attempt

Memastikan privasi dan keamanan memainkan peran penting dalam seluruh tujuan penggunaan proxy. Proksi SOCKS bertindak sebagai mediator antara klien dan server untuk mengamankan aktivitas daring Anda dan membuatnya lebih sulit dilacak.

Proksi HTTP banyak digunakan untuk proyek perlindungan email dan keamanan siber karena kemampuannya memahami paket data dan memfilternya sesuai kebutuhan tertentu. Ini juga dapat berguna untuk aktivitas web scraping dan penambangan data.

Proksi SOCKS (Socket Secure) dapat rentan terhadap sejumlah serangan, seperti buffer overflow, serangan DoS, serangan Man-in-the-Middle, dan cryptomine atau penambangan uang kripto. Selain itu Server proxy juga rentan terhadap pelanggaran data jika menyimpan alamat IP pengguna dan data permintaan web tanpa enkripsi. Beberapa proksi bahkan dapat menjual data ini ke pihak ketiga.

GPL SNMP Public Access UDP

GPL adalah singkatan dari General Public License, yang merupakan lisensi perangkat lunak sumber terbuka yang luas dan populer. SNMP adalah singkatan dari Simple Network Management Protocol.

Yang digunakan untuk mengumpulkan informasi dan mengelola perangkat jaringan seperti router, switch, server, printer, dan lainnya. UDP merujuk pada Protokol Datagram Pengguna, yang merupakan protokol komunikasi yang digunakan oleh SNMP untuk mengirimkan data. Istilah 'publik' dalam konteks ini mungkin merujuk pada string komunitas default yang digunakan dalam SNMP versi 1 dan 2c.

Yang merupakan jenis kata sandi atau kontrol akses. Namun, menggunakan 'publik' sebagai string komunitas di SNMP merupakan risiko keamanan, karena sudah dikenal dan memberikan akses baca-saja ke informasi perangkat jaringan.

SPAM & MALWARE

Pengguna internet secara terus-menerus dihadapkan pada berbagai ancaman online yang membahayakan privasi dan keamanannya. Dua bahaya umum yang sering mengganggu dan merusak pengalaman online pengguna adalah spam dan malware. Meskipun keduanya merugikan pengguna, keduanya berbeda secara signifikan dalam metode, tujuan, dan potensi konsekuensinya.

Secara historis efektivitas email dalam penyebaran informasi tidak terbantahkan dalam skala dan luasnya. Dengan metode yang sama, pelaku spam melancarkan serangan melalui miliaran email spam yang dihasilkan setiap hari.

Pada laporan kali ini, klasifikasi 5 negara terbanyak pengirim spam akan dibedakan dengan pengirim malware untuk mendapatkan data lebih detail.

Spam

Spam email terutama memiliki dua tujuan

1. Untuk iklan, misalnya mempromosikan produk, layanan, atau konten.
2. Untuk penipuan, misalnya berusaha melakukan scam atau phishing.

Email spam untuk iklan pada dasarnya bersifat promosi, seringkali tidak berbahaya dalam mempamerkan produk atau layanan kepada khalayak luas. Biasanya dikirim secara massal, gangguan utama spam terletak pada volumenya yang sangat banyak, dan skenario terburuknya mungkin melibatkan infeksi malware atau kerugian finansial kecil.

Di sisi lain email phishing dibuat untuk mengelabui penerima agar mengungkapkan informasi sensitif. Email tersebut mungkin dirancang khusus untuk meniru entitas terpercaya, memanfaatkan ajakan bertindak yang mendesak untuk memikat orang yang tidak menaruh curiga. Meskipun email spam pada dasarnya merupakan gangguan, konsekuensi dari penipuan phishing lebih parah, mulai dari pencurian identitas hingga dampak finansial yang signifikan atau bahkan pelanggaran data berskala besar. Dewasa ini kita mengenal istilah BEC (*Business Email Compromised*) yaitu phishing dengan target terkait penipuan usaha. Umumnya pelaku BEC mengirimkan email yang bertujuan mengalihkan transaksi keuangan.

Spam umumnya didistribusikan melalui kampanye email masal, namun juga dapat ditemukan di bagian komentar situs web, platform pesan instan, media sosial, dan forum. Seringkali, pelaku spam menggunakan bot otomatis untuk mengirim pesan dalam jumlah besar, menargetkan khalayak luas dengan harapan sebagian akan mengambil umpan tersebut.

Malware

Malware merupakan sebutan umum untuk software berbahaya yang memiliki beragam bentuk tergantung tujuan penggunaannya, seperti spyware untuk memata-matai, ransomware yang berfungsi menyandera data untuk mendapatkan tebusan dan masih banyak lagi.

Malware dapat menyusup ke sistem dengan berbagai cara, sering kali mengeksploitasi kelemahan perangkat lunak, kesalahan manusia, atau kombinasi keduanya. Setelah malware menginfeksi sistem, malware dapat melakukan berbagai aktivitas berbahaya, mulai dari mencuri informasi pribadi hingga membajak sumber daya komputer untuk serangan yang lebih besar, seperti serangan Distributed Denial-of-Service (DDoS).
Di era digital, malware merupakan ancaman yang konstan dan berubah, tetapi risiko infeksi dapat dikurangi secara signifikan dengan pengetahuan dan tindakan pencegahan. Dengan memahami cara kerja malware dan mematuhi praktik terbaik untuk keamanan siber, individu dan organisasi dapat melindungi data mereka dan menjaga integritas sistem mereka. Dalam perang melawan malware, kewaspadaan adalah garis pertahanan pertama.

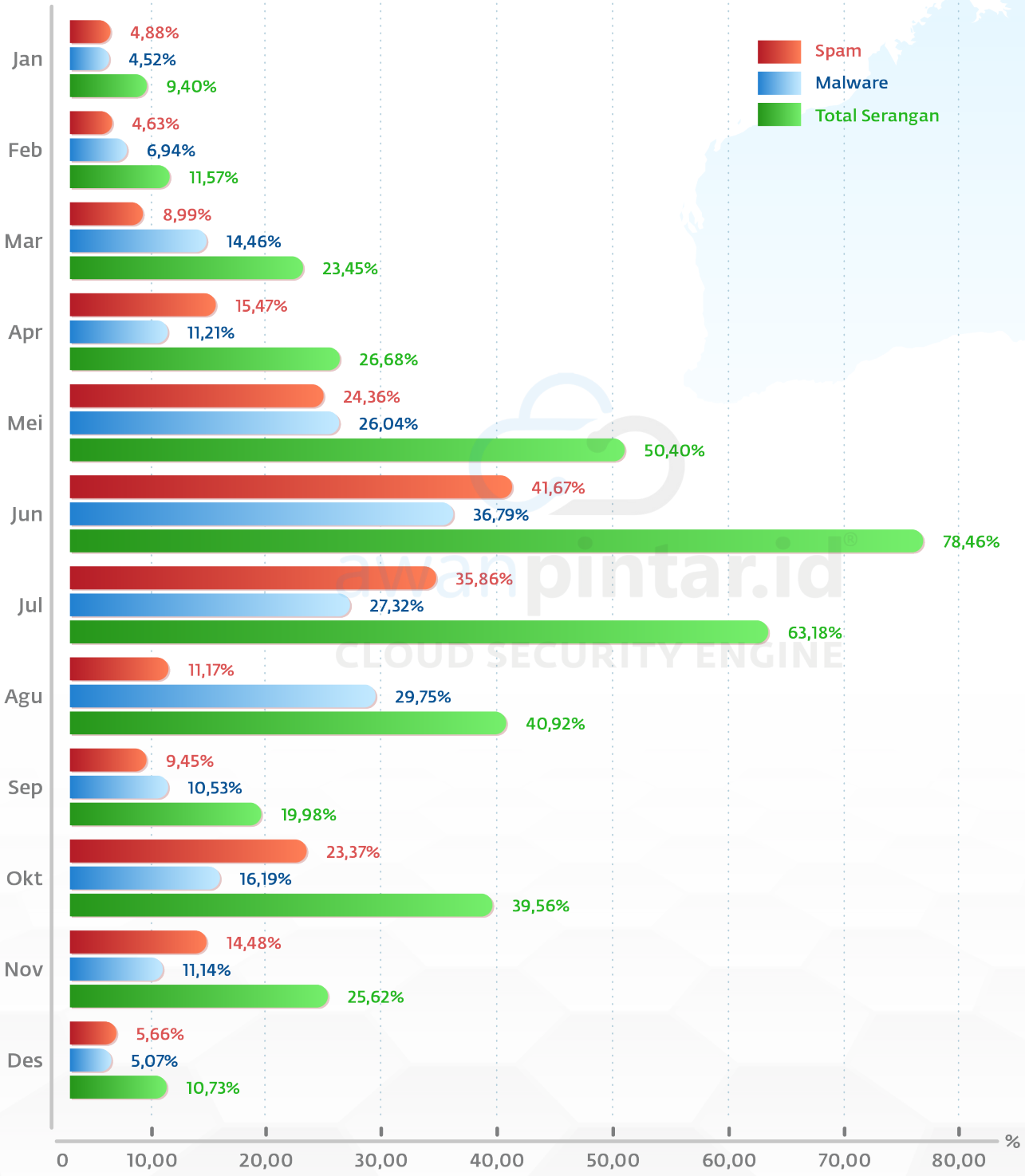
Melibatkan AI

AI berkembang dengan cepat, merevolusi banyak bidang termasuk spam. Di luar seperti chatbots, Siri atau Alexa, sistem AI dapat digunakan di luar ruang lingkup aslinya, untuk memicu operasi spam dari berbagai jenis.

Fenomena ini selanjutnya dikenal sebagai spamming dengan AI, mengisyaratkan fakta bahwa AI digunakan sebagai alat untuk membuat bentuk spam baru. Konsep baru spam AI, menunjukkan bahwa AI dapat dimanipulasi dan bahkan dikompromikan oleh spammer atau peretas dalam arti yang lebih luas. Kemajuan dalam visi komputer, virtual dan augmented reality memproyeksikan kita di era dimana batas antara kenyataan dan fiksi semakin kabur.

Kombinasi keduanya menjadi momok bagi dunia digital, kemampuan email yang mampu menyebar melewati protokol keamanan menjadi kelebihannya yang paling utama, sehingga menempatkannya sebagai ancaman utama. Untuk mengetahui lebih lanjut sepak terjang spam dan malware di tanah air, berikut data yang dikumpulkan oleh AwanPintar.id®

Persentase Jumlah Spam & Malware Terhadap Total Email Masuk



Data yang dipaparkan di atas ini merupakan jumlah persentase dari total spam dan malware terhadap jumlah email yang masuk dan didata oleh AwanPintar.id® selama tahun 2024.

Deskripsi Serangan Spam

Secara umum persentase serangan spam selama satu tahun begitu fluktuatif, yang paling terlihat jelas adalah jumlah serangan paling rendah sepanjang tahun berada di awal dan akhir tahun. Sementara di pertengahan tahun menjadi puncak dari seluruh serangan spam di tanah air.

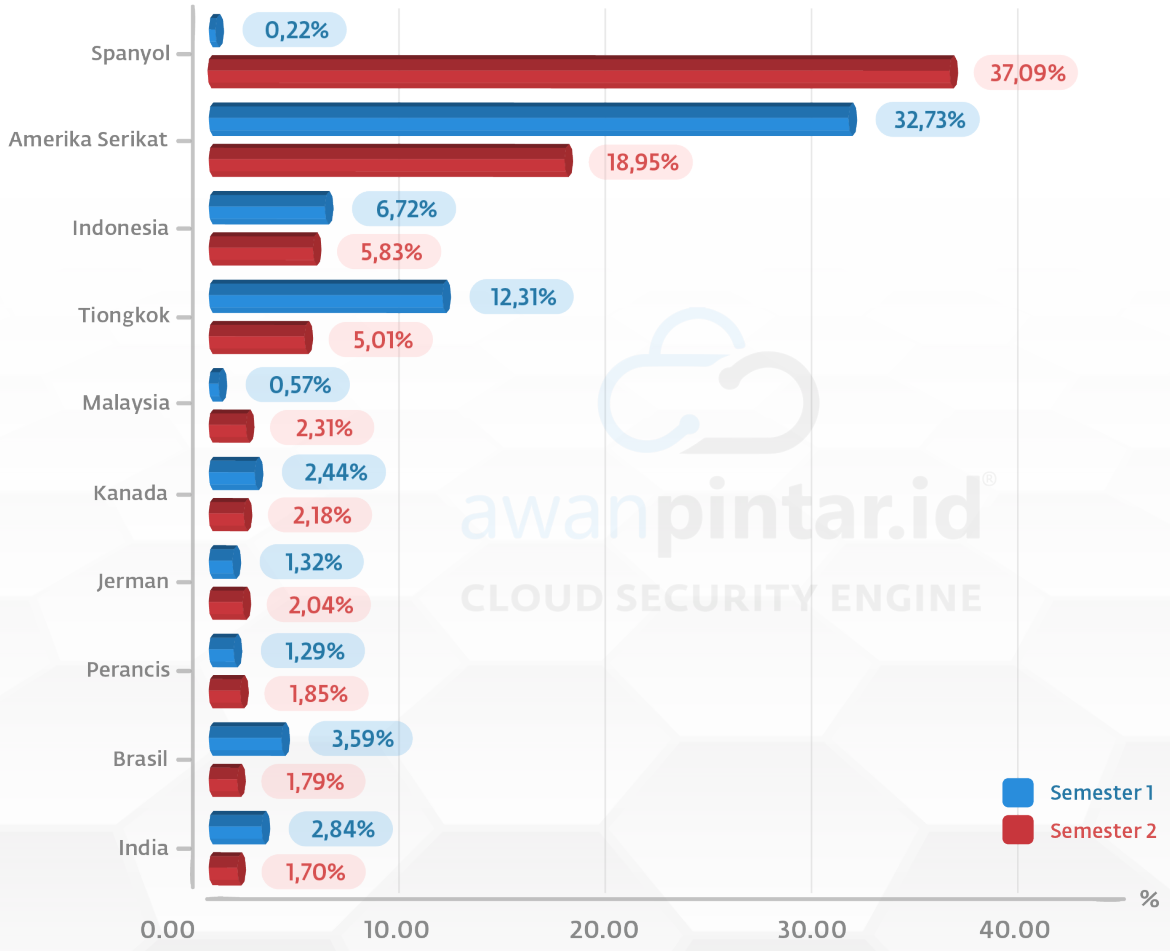
Yang menjadi anomali adalah bulan September, jika di tahun lalu bulan September begitu mendominasi dengan mencapai jumlah serangan tertinggi. Di tahun 2024 September sangat kontradiktif.

Serangan spam pada awal semester 2 tahun 2024 terlihat masif dan meluas, mendominasi bahkan selama sepanjang tahun. Kemudian bulan Oktober juga memberi gebrakan yang hampir sama walau tak sebesar bulan Juli.

Penurunan aktivitas serangan spam yang terjadi pada akhir tahun tidak seperti yang terjadi di awal tahun, bisa disimpulkan selama paruh kedua tahun 2024 ancaman spam secara umum lebih besar dari semester 1 tahun ini.

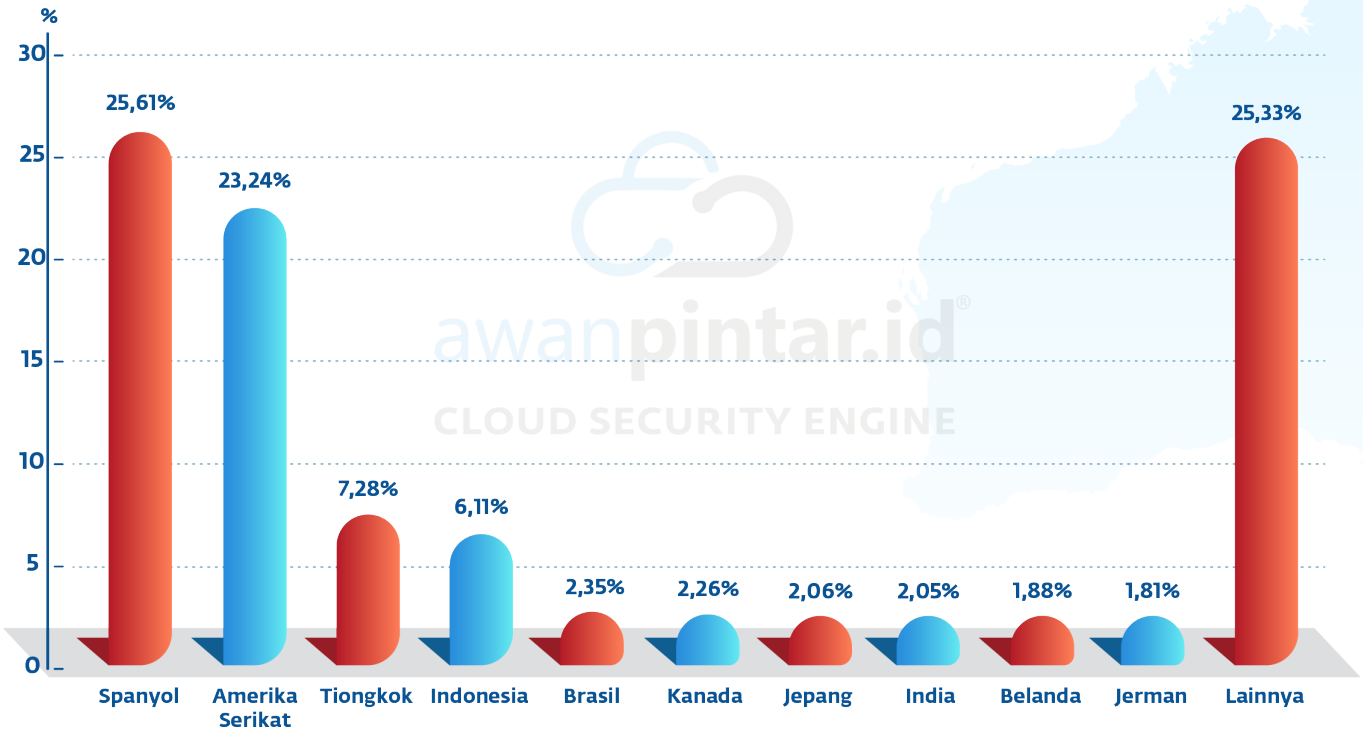
Selama semester kedua tahun 2024 terjadi penurunan serangan malware di empat bulan terakhir tahun 2024 jika dibandingkan dengan periode yang sama pada tahun 2023. Di sisi lain, dengan peningkatan serangan hanya terjadi di awal bulan, ini dikarenakan penyerang melakukan serangan secara terukur dan terbatas namun dengan efektivitas serangan lebih tinggi.

Komparasi 10 Negara Pengirim Spam Semester 1 dan 2 Tahun 2024



10 Negara Pengirim Spam Tahun 2024

Total 198 Negara



Spam email merupakan produk serangan siber paling sederhana sekaligus paling berbahaya dengan biaya yang sangat minim, oleh karena itu serangan semacam ini selalu menjadi favorit bagi para penjahat siber di belahan dunia manapun tanpa terkecuali.

Spam email phishing selalu menjadi senjata mematikan yang terlihat tidak mencurigakan sama sekali, di sinilah letak bahayanya, karena situasi seperti ini sering membuat orang menurunkan kewaspadaannya dan tanpa sadar menempatkan dirinya dalam situasi berisiko.

Dalam data yang dihimpun oleh AwanPintar.id® pada semester 2 tahun 2024 ada sebuah kejutan buruk, Spanyol yang selama ini tidak pernah masuk dalam ancaman signifikan terhadap Indonesia, menduduki posisi pertama sebagai negara pengirim spam terbanyak.

Dan yang tak pernah luput dari perhatian, Amerika Serikat, Tiongkok dan Brasil menjadi negara yang konsisten dan tidak pernah absen dalam mengirim email berbahaya ke Indonesia, walau jumlah serangan mereka menurun drastis hingga dua digit. Ini merupakan pergeseran arus serangan yang cukup besar dalam lanskap serangan di infrastruktur jaringan nasional.

Yang mengkhawatirkan malah datang dari negeri sendiri, Indonesia yang pada tahun 2023 berada di posisi buncit, saat ini melonjak pesat ke posisi empat dalam daftar negara pengirim spam terbanyak. Peningkatan ini didorong oleh potensi serangan spam yang memanfaatkan domain-domain lokal yang

dimanfaatkan dan kemudian disalahgunakan untuk menipu pengguna internet di tanah air.

Data selama satu tahun 2024 sedikit berbeda dengan data semester 2 pada tahun yang sama. Jepang yang hanya masuk dalam 10 besar pada semester 1 dan terlempar pada semester 2, secara total selama tahun 2024 masuk dalam 10 besar pengirim spam. Jumlah negara dalam setahun juga lebih tinggi daripada jumlah tiap semester. Ini menunjukkan adanya negara pengirim spam yang terdaftar pada semester 1 namun pada semester 2 tidak mengirimkan spam sama sekali, demikian pula sebaliknya.

Di luar data 10 besar negara pengirim spam, memiliki persentase 25.33% merupakan sisa negara lainnya mendekati Spanyol sebagai pemegang rekor terbanyak 25.61%.

Deskripsi Serangan Malware

Seperti data yang dipaparkan oleh AwanPintar.id® dari hasil komparasi dan total keseluruhan serangan malware diketahui bahwa persentase serangan malware tidak mengalami perubahan dari tahun sebelumnya.

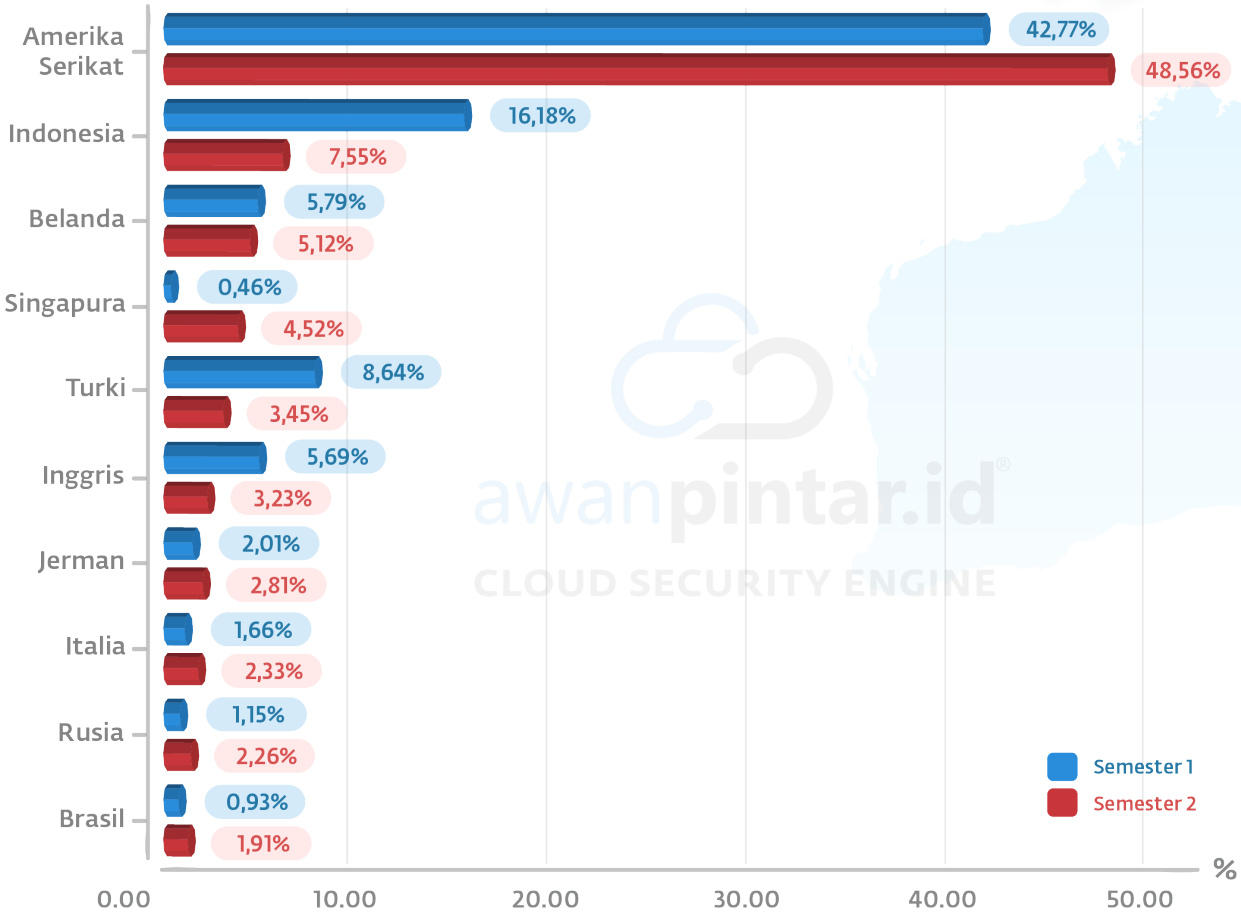
Dari bentuk Intensitas ancaman malware tersebut memberi gambaran bahwa serangan malware dikonsentrasikan pada sasaran terbatas.

Terlihat bahwa serangan malware seiring dan sejalan dengan serangan spam yang terjadi tahun ini. Memang ada korelasi jika ditarik benang merah, karena seringkali serangan malware diawali dengan spam yang masif.

Sehingga peningkatan serangan spam di pertengahan tahun 2024 berimbas pada jumlah serangan malware di tempat yang sama. Hal serupa terjadi ketika ada penurunan serangan menunjukkan adanya simbiosis di antara keduanya.

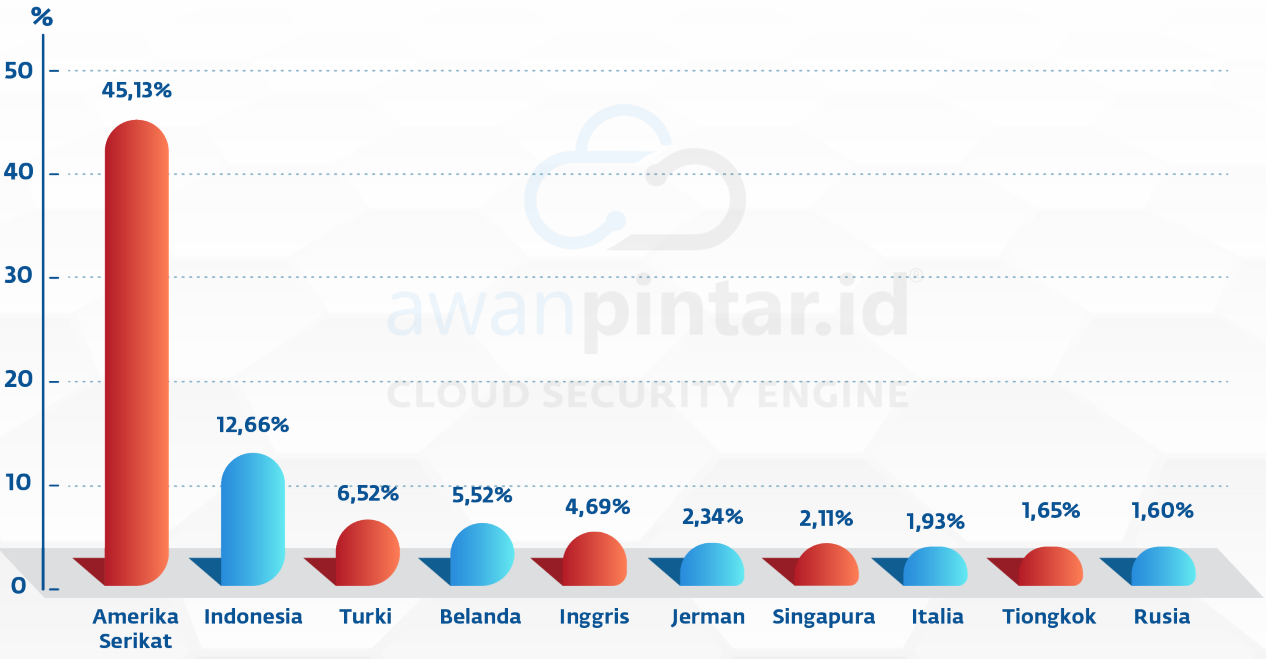
Jika dilihat dari polanya, awal tahun ancaman tidak seberapa besar namun perlahan meningkat seiring berjalannya waktu hingga pertengahan tahun, kemudian secara perlahan menurun meski sempat ada fluktuasi tapi di akhir tahun ancaman menurun sangat drastis.

Komparasi 10 Negara Pengirim Malware Semester 1 dan 2 Tahun 2024



10 Negara Pengirim Malware Tahun 2024

Total 86 Negara



Malware sering menjadi penumpang gelap yang diselundupkan melalui email spam, trik ini sangat umum digunakan di dunia bawah tanah kejahatan siber. Dari data AwanPintar.id® kita dapat menemukan korelasi yang kuat antara peningkatan serangan spam mendongkrak jumlah serangan malware yang masuk ke Indonesia.

Dalam Laporan Ancaman Digital di Indonesia Semester 2 Tahun 2024 oleh AwanPintar.id® ditemukan beberapa informasi menarik bahwa serangan malware secara umum mengalami peningkatan pesat dan masuk-masuknya negara baru yang mengubah lanskap ancaman serangan malware.

Amerika Serikat tetap menunjukkan dominasinya di posisi puncak dengan kenaikan persentase pengiriman malware pada semester 2 tahun 2024. Brasil dan Singapura masuk sebagai pendatang baru di semester 2 ini, serangan malware dari Brasil dan Singapura dinilai cukup memberi dampak jika dilihat dari besaran serangannya.

Pada rentang data tahun 2024, Turki yang langsung menempati posisi ketiga dalam daftar. Sementara Amerika dan Indonesia terus menjaga hegemoni mereka dengan eskalasi serangan yang lebih dari sebelumnya.

Vietnam dan Armenia yang pada semester 1 menempati posisi 9 dan 10 tidak masuk dalam daftar pada semester 2 dan kumulasi tahun 2024. Besar kemungkinan IP address negara tersebut hanya menjadi bot/proxy dan sudah banyak dilakukan perbaikan untuk mengurangi kebocoran sistem.

Green
OPEN

PORT FAVORIT PERETAS

10 Port Paling Rentan di Indonesia

Port merupakan bagian integral dari komunikasi berbasis TCP/IP. Semua layanan yang menggunakan peramban web, halaman web, dan layanan transfer file untuk menjalankan aktivitasnya bergantung pada port untuk mengirimkan informasi. Satu port didedikasikan untuk satu layanan dan tidak dapat digunakan untuk proyek lain.

Risiko Keamanan Port Terbuka

Port terbuka tidak menimbulkan risiko keamanan. Namun, hal itu bergantung pada konfigurasi dan perlindungan port. Jika port tidak dikonfigurasi dengan benar, peretas berpotensi mengakses komputer atau jaringan, mengeksploitasi kerentanan perangkat lunak, dan menguasai sistem.

Port yang tidak dilindungi mengungkapkan aktivitas jaringan kepada penyerang, yang memungkinkan mereka untuk menyadap layanan yang sedang berjalan, menemukan kelemahan, dan merencanakan serangan yang ditargetkan secara strategis. Serangan semacam itu dapat menyebabkan pelanggaran data yang menyebabkan pencurian kekayaan intelektual, serta kerusakan finansial dan reputasi.

Lantas port apa saja di Indonesia yang paling sering menjadi incaran penjahat siber, berikut data port yang paling rentan yang dihimpun oleh AwanPintar.id®

Green
OPEN

Persentase Port Paling Rentan Semester 1 dan 2 Tahun 2024

PORT	Semester 1	Semester 2	Keterangan
UDP 53	96.26%	94.27%	Jumlah Penurunan -1,99%
TCP 445	1.54%	0.38%	Jumlah penurunan -1,16%
TCP 135	0.01%	0.18%	Jumlah peningkatan 0,17%
UDP 500	0.00%	0.14%	Baru masuk 10 besar
TCP 5900	0.36%	0.08%	Jumlah penurunan -0,28%
TCP 22	0.09%	0.08%	Jumlah penurunan -0,01%
TCP 3389	0.00%	0.02%	Baru masuk 10 besar
UDP 161	0.00%	0.02%	Baru masuk 10 besar
TCP 8443	0.00%	0.02%	Baru masuk 10 besar
UDP 1900	0.17%	0.01%	Jumlah penurunan -0,16%
Lainnya	0.43%	4.86%	

Sebenarnya tidak banyak perubahan dalam serangan terhadap port terentan di Indonesia dalam Laporan Ancaman Digital di Indonesia semester 2 tahun 2024 oleh AwanPintar.id®. Port 53 seperti tahun sebelum terus mengalami serangan dalam jumlah yang sangat besar bahkan fokus serangan terhadap port hampir semua berpusat kepada port tersebut, mengingat port ini selalu terbuka pada sistem.

Perubahan terjadi dengan pergeseran beberapa port, yakni port 135, 500, 161 dan 8443 mengambil alih posisi port 80, 110, 123, dan 5060. Dari komposisi pergeseran ini port 135 dan 500 langsung menyodok ke posisi ketiga dan keempat sebagai port paling rentan.

Dinamika pada perubahan sejumlah port yang diserang, menunjukkan peretas berupaya melakukan ekspansi serangan dengan mencari celah-celah lain yang bisa mereka eksploitasi. Semoga petunjuk ini menjadi perhatian masyarakat digital nasional adanya ancaman-ancaman baru dalam sistem jaringan lokal.

Definisi Port

Port UDP 53

DNS menggunakan Port 53 yang hampir selalu terbuka pada sistem, firewall, dan klien untuk mengirimkan permintaan DNS. Dibandingkan dengan Transmission Control Protocol (TCP) yang lebih familiar, kueri ini menggunakan User Datagram Protocol (UDP) karena latensinya yang rendah, bandwidth, dan penggunaan sumber daya dibandingkan kueri yang setara dengan TCP. UDP tidak memiliki kemampuan kontrol kesalahan atau aliran, juga tidak memiliki pemeriksaan integritas untuk memastikan data tiba secara utuh.

DNS adalah protokol internet yang penting dan mendasar, sering digambarkan sebagai "buku telepon internet" yang memetakan nama domain ke alamat IP, dan banyak lagi, seperti yang dijelaskan dalam RFC inti untuk protokol tersebut. Keberadaan DNS di mana-mana (dan kurangnya pengawasan) dapat memungkinkan metode yang sangat elegan dan halus untuk berkomunikasi, dan berbagi data, di luar maksud awal protokol.

Terdapat sejumlah alat yang dapat memungkinkan penyerang membuat saluran rahasia melalui DNS untuk tujuan menyembunyikan komunikasi atau melewati kebijakan yang ditetapkan oleh administrator jaringan. Kasus penggunaan yang populer adalah melewati registrasi koneksi Wi-Fi hotel, kafe, dll dengan menggunakan DNS yang sering dibuka dan tersedia. Terutama alat-alat ini tersedia secara online secara gratis di tempat-tempat seperti GitHub dan mudah digunakan.

Port TCP 445

Port 445 adalah port jaringan Microsoft yang juga terhubung ke layanan NetBIOS yang ada di Sistem Operasi Microsoft versi sebelumnya. Ini menjalankan Server Message Block (SMB), yang memungkinkan sistem di jaringan yang sama untuk berbagi file dan printer melalui TCP/IP.

Port ini tidak boleh dibuka untuk jaringan eksternal. Semua perangkat Microsoft sebagian besar memiliki port 445 terbuka karena port tersebut digunakan untuk komunikasi LAN.

Penyerang dapat melakukan pemindaian port menggunakan alat open source seperti Nmap, Metasploit, dan NetScan Tools Pro. Alat pemindaian ini mengidentifikasi layanan yang memanfaatkan port 445 dan mengumpulkan informasi penting tentang perangkat. Setelah mengetahui detail perangkat, penyerang melancarkan serangan malware dan ransomware dengan memanfaatkan port ini.

Port TCP 135

Port 135 didedikasikan untuk Layanan Pemetaan Remote Procedure Call (RPC) Windows. Banyak layanan penting, seperti Microsoft Active Directory (AD), mengandalkan port ini untuk komunikasi klien-server jarak jauh.

Tujuan dari port 135 adalah untuk memfasilitasi komunikasi jarak jauh antara klien dan server di lingkungan Windows. Tanpa akses ke port.

135 pada perangkat, perangkat lain tidak akan dapat menentukan layanan apa yang tersedia pada perangkat tersebut, dan juga tidak dapat mengetahui port mana yang menjalankan layanan tersebut.

Port UDP 500

Port 500 adalah salah satu port yang memainkan peran penting dalam mengamankan komunikasi jaringan, khususnya dalam jaringan privat virtual (VPN).

Port 500 secara resmi ditetapkan untuk digunakan oleh protokol Internet Key Exchange (IKE). IKE adalah komponen penting dari rangkaian IPsec (Internet Protocol Security), yang digunakan untuk membuat koneksi yang aman dan terenkripsi melalui internet.

Protokol IKE membantu dalam menyiapkan asosiasi keamanan (SA) dengan menegosiasikan dan menetapkan kunci dan algoritma kriptografi yang akan digunakan untuk komunikasi IPsec. Dalam istilah yang lebih sederhana, Port 500 adalah gerbang tempat perangkat memulai dan mengelola pertukaran data yang aman dalam VPN.

Port 500 merupakan komponen penting dalam pembentukan koneksi jaringan yang aman, khususnya dalam konteks VPN yang menggunakan protokol IPsec. Port ini memfasilitasi proses negosiasi IKE, memastikan bahwa data dienkripsi dan dikirimkan dengan aman melalui internet. Namun, seperti layanan jaringan lainnya, Port 500 bukannya tanpa kerentanan.

Dengan memahami potensi risiko yang terkait dengan port ini, seperti serangan MitM, serangan DoS, dan kelemahan dalam protokol IKE, administrator jaringan dapat mengambil langkah-langkah untuk mengamankan sistem mereka. Ini termasuk menggunakan protokol yang diperbarui seperti IKEv2, menerapkan algoritma enkripsi yang kuat, dan memastikan konfigurasi yang tepat untuk melindungi dari akses yang tidak sah dan potensi eksploitasi.

Port TCP 5900

Port 5900 biasanya digunakan untuk koneksi desktop jarak jauh menggunakan protokol Remote Frame Buffer (RFB). Hal ini terkait dengan sistem Virtual Network Computing (VNC), yang memungkinkan pengguna untuk mengontrol komputer melalui jaringan dan transfer file dari jarak jauh.

Port ini digunakan untuk menjalankan aplikasi desktop bersama dan platform remote control mandiri. VNC sangat populer dan juga digunakan untuk dukungan jarak jauh di banyak organisasi besar. Cara kerjanya tidak jauh berbeda dengan pcAnywhere.
Penyerang dapat menyalahgunakan VNC untuk melakukan tindakan jahat sebagai pengguna yang masuk seperti membuka dokumen, mengunduh file, dan menjalankan perintah tak terbatas.

Port TCP 22

SSH adalah singkatan dari Secure Shell. Ini adalah port TCP yang digunakan untuk memastikan akses jarak jauh yang aman ke server. Peretas dapat mengeksploitasi port 22 dengan menggunakan kunci SSH yang bocor atau kredensial paksa.

Peretas yang menguasai port ini dapat mengeksploitasi port SSH dengan brute force kredensial SSH atau menggunakan kunci privat untuk mendapatkan akses ke sistem target.

Atau penyerang yang tidak diautentikasi dengan akses jaringan ke port 22 dapat mengalirkan lalu lintas acak TCP ke host lain di jaringan melalui perangkat Ruckus. Penyerang dapat mengeksploitasi kerentanan ini untuk membatasi keamanan dan mendapatkan akses tidak sah ke aplikasi yang rentan.

Port TCP 3389

Port 3389 digunakan untuk Windows Remote Desktop Protocol (RDP) dan terkadang juga digunakan oleh Windows Terminal Server. Terutama digunakan untuk membantu pengguna menyelesaikan masalah dengan komputer mereka.

Protokol Desktop Jarak Jauh secara historis sangat rentan terhadap berbagai bentuk serangan yang memungkinkan peretas untuk berkompromi dan melanggar lingkungan. Apakah protokol itu sendiri aman? Tidak seperti HTTP dan FTP yang tidak terenkripsi, Remote Desktop Protocol (RDP) ditransmisikan melalui saluran terenkripsi. Ini mencegah penyerang dapat menyadap lalu lintas jaringan dan membahayakan data sensitif. Namun, ada celah RDP yang perlu diperhatikan, yakni kerentanan keamanan, salah konfigurasi dan brute force.

Peretas menggunakan RDP untuk mendapatkan akses ke komputer atau jaringan host dan kemudian menginstal ransomware pada sistem. Setelah diinstal, pengguna biasa kehilangan akses ke perangkat, data, dan jaringan yang lebih besar hingga pembayaran dilakukan.

Port UDP 161

Port 161 dikaitkan dengan Simple Network Management Protocol (SNMP). SNMP adalah protokol yang digunakan secara luas yang memungkinkan administrator jaringan untuk mengelola dan memantau perangkat pada jaringan, seperti router, switch, server, dan printer.

Dengan menggunakan SNMP, administrator dapat mengumpulkan data, memantau kinerja, dan mengendalikan perangkat jaringan dari lokasi terpusat, sehingga manajemen jaringan menjadi lebih efisien dan efektif.

Port 161 merupakan komponen dasar manajemen jaringan, yang memungkinkan administrator untuk memantau, mengkonfigurasi, dan mengendalikan perangkat jaringan melalui protokol SNMP. Namun, karena perannya yang penting, port ini juga berpotensi menjadi target berbagai ancaman keamanan.

Untuk melindungi jaringan yang menggunakan Port 161, penting untuk menerapkan langkah-langkah keamanan yang kuat, seperti menggunakan versi SNMP yang dienkripsi (seperti SNMPv3), mengubah string komunitas default, dan memastikan bahwa hanya pengguna yang berwenang yang memiliki akses.

Dengan memahami penggunaan dan kerentanan Port 161, administrator jaringan dapat mengamankan infrastruktur mereka dengan lebih baik dan mempertahankan operasi jaringan yang kuat.

Port TCP 8443

Port 8443 adalah nomor port alternatif yang mewakili HTTPS atau Hypertext Transfer Protocol melalui koneksi aman sebagaimana diberikan oleh SSL/TLS. Dengan kata lain, ini adalah nomor port alternatif untuk nomor port HTTPS default yang banyak digunakan, yaitu 443, yang digunakan untuk mengakses sumber daya web dengan aman.

Port HTTPS 8443 terutama digunakan untuk komunikasi web yang aman. Situs web, aplikasi web, dan layanan menggunakan port ini agar data yang mengalir antara pengguna dan server tetap terenkripsi dan aman dari kemungkinan penyadapan.

Port 8443 dapat rentan terhadap serangan eksekusi kode jarak jauh (RCE). Misalnya, kerentanan CVE-2023-38035 di Ivanti Sentry memungkinkan penyerang yang tidak diautentikasi untuk membaca dan menulis

file ke server Ivanti Sentry. Penyerang juga dapat menjalankan perintah OS sebagai administrator sistem (root).

Port UDP 1900

SSDP adalah tulang punggung arsitektur UPnP. Ini memungkinkan Anda untuk dengan mudah menghubungkan perangkat rumah yang bekerja dalam jaringan kecil yang sama atau terhubung ke titik WiFi yang sama.

Perangkat tersebut dapat mencakup, misalnya, smartphone, printer dan MFP, smart TV, konsol media, speaker, camcorder, dll. Agar SSDP berfungsi, perangkat ini harus mendukung UPnP.

Dari sudut pandang keamanan informasi, perlu diingat bahwa, pertama, protokol SSDP itu sendiri tidak menyediakan enkripsi dan kedua, di banyak perangkat yang dimaksud untuk digunakan di rumah atau di lingkungan kantor kecil, dukungan SSDP diaktifkan secara default, menimbulkan risiko akses tidak sah. Selain itu, fitur SSDP digunakan dalam implementasi serangan DDoS seperti "SSDP amplification".

Green
OPEN

COMMON VULNERABILITY & EXPOSURES

Setiap sistem komputer dengan kerentanan dapat terkena serangan siber, jika sistem tersebut terhubung ke internet atau jaringan eksternal apa pun dan saat ini, hampir semua komputer mengalaminya.

Sehingga setiap strategi keamanan yang kuat dimulai dengan pengetahuan yang mengetahui di mana kelemahan dalam sistem dan aplikasi. Di situlah CVE dapat membantu, CVE daftar kerentanan atau kelemahan keamanan informasi dalam perangkat lunak atau perangkat keras yang telah diungkapkan kepada publik.

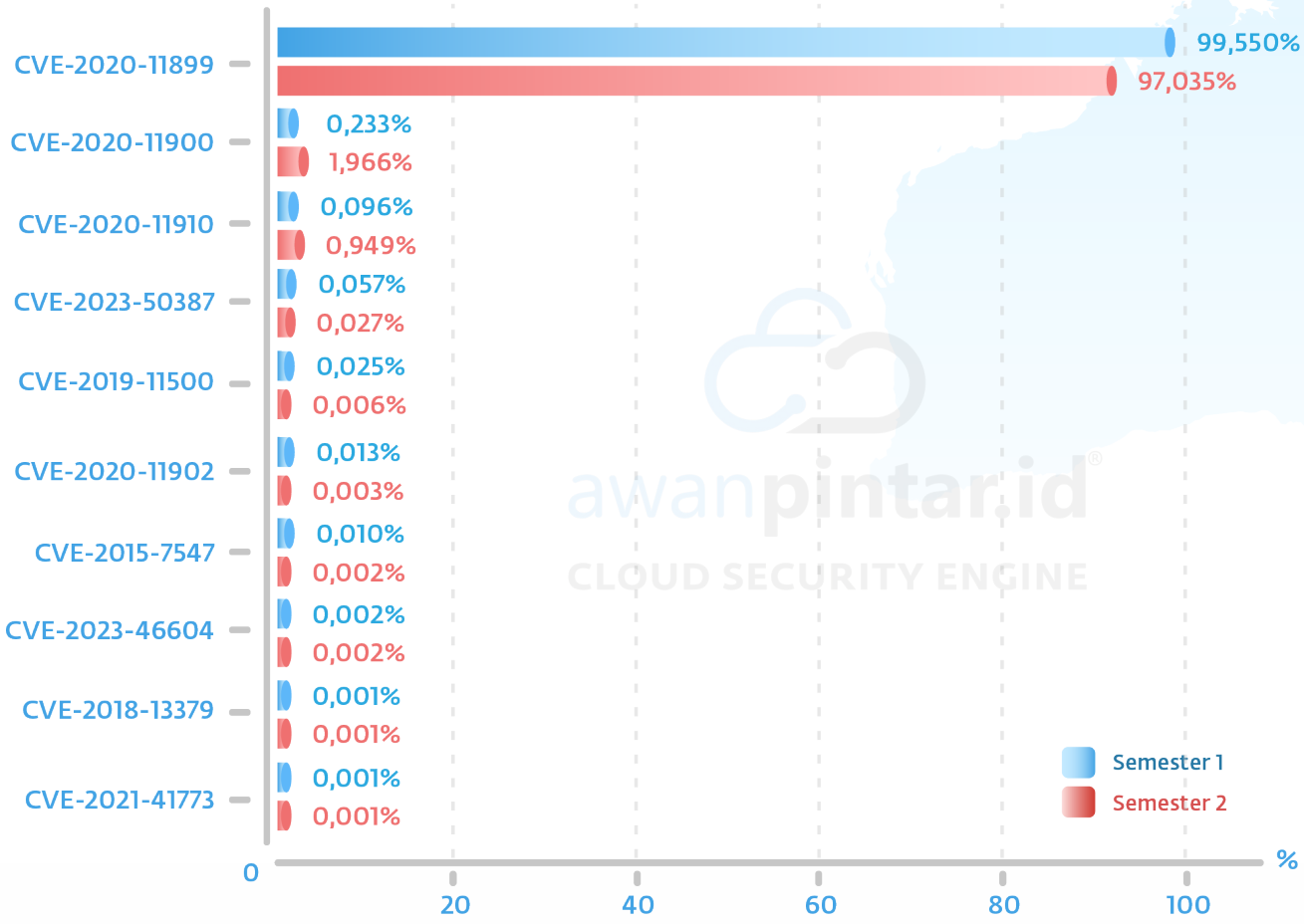
CVE dimaksudkan untuk standardisasi identifikasi kerentanan, memberikan bahasa umum kepada para profesional TI. Program CVE saat ini dijalankan oleh MITRE Corporation dengan pendanaan dari Cybersecurity and Infrastructure Security Agency (CISA).

Common Vulnerabilities and Exposures (CVE) adalah sumber pengetahuan yang kaya. Mengetahui potensi kelemahan sistem berarti dapat mengevaluasi langkah-langkah keamanan lebih efektif terhadapnya untuk memenuhi tujuan penting, yakni membangun mekanisme pertahanan yang lebih kuat.

Di Indonesia kerentanan umum seperti ini banyak ditemui dapat dideteksi dengan mudah. Untuk meningkatkan kewaspadaan dan kesadaran keamanan siber, berikut data Common Vulnerability & Exposures (CVE) yang diperoleh dari AwanPintar.id® dari berbagai kolektor yang tersebar di seluruh Indonesia.

Green
OPEN

Komparasi Common Vulnerability & Exposures Semester 1 Tahun 2024 dan Semester 2 Tahun 2024



CVE-2020–11899
Mengalami penurunan **-2,515%**

CVE-2020-11900
Mengalami peningkatan **1,733%**

CVE-2020-11910
Mengalami peningkatan **0,853%**

CVE-2023-50387
Mengalami penurunan **-0,030%**

CVE-2019-11500
Mengalami penurunan **-0.019%**

CVE-2020-11902
Mengalami penurunan **-0,010%**

CVE-2015-7547
Mengalami penurunan **-0,008%**

CVE-2023-46604
Mengalami Stagnasi

CVE-2018-13379
Mengalami Stagnasi

CVE-2021-41773
Mengalami Stagnasi

CVE-2020-11899
CVSS Score: 5.4 Medium

CVE-2020-11899,kerentananpadatumpukan Treck TCP/IP sebelum versi 6.0.1.66 memiliki Bacaan Di Luar Batas IPv6. Hal ini disebabkan oleh validasi input yang tidak tepat pada komponen IPv6 saat menangani paket yang dikirim oleh penyerang jaringan yang tidak sah. Kerentanan ini dapat menyebabkan adanya potensi Denial-of-Service.

Dampak
Masalah ini mempengaruhi kode yang tidak diketahui dari komponen IPv6 Handler. Manipulasi dengan masukan yang tidak diketahui menyebabkan kerentanan di luar batas.

Produk Terdampak
TCP/IP versions before (<) 6.0.1.66

Mitigasi Kerentanan
Treck merekomendasikan pengguna untuk menerapkan versi terbaru dari produk yang terpengaruh (Treck TCP/IP 6.0.1.67 atau versi yang lebih baru) CISA merekomendasikan pengguna mengambil tindakan defensif untuk meminimalkan risiko eksploitasi kerentanan ini. Secara khusus, pengguna harus:

- Meminimalkan paparan jaringan untuk semua perangkat dan/atau sistem kontrol, dan pastikan perangkat dan/atau sistem tersebut tidak dapat diakses dari internet.
- Temukan jaringan sistem kontrol dan perangkat jarak jauh di belakang firewall dan isolasi dari jaringan bisnis.
- Jika akses jarak jauh diperlukan, gunakan metode aman, seperti Virtual Private Network (VPN), mengetahui VPN mungkin memiliki kerentanan maka harus diperbarui ke versi terbaru yang tersedia. Ketahuilah juga bahwa VPN hanya seaman perangkatnya yang terhubung.

CVE-2020-11900
CVSS Score: 8.2 High

Kerentanan ini dikenal sebagai CVE-2020-11900 sejak 19/04/2020. Dimungkinkan untuk melancarkan serangan dari jarak jauh. Eksploitasi tidak memerlukan autentikasi dalam bentuk apa pun. Tidak ada rincian teknis atau eksploitasi yang tersedia untuk umum.

Dampak
Kerentanan ditemukan di Treck TCP-IP Stack. Ini telah diklasifikasikan sebagai kritis. Yang terpengaruh adalah blok kode yang tidak diketahui dari komponen Tunneling IPv4. Manipulasi dengan masukan yang tidak diketahui menyebabkan kerentanan bebas ganda.

CWE mengklasifikasikan masalah ini sebagai CWE-415. Produk calls free dua kali pada alamat memori yang sama, yang berpotensi menyebabkan modifikasi lokasi memori yang tidak terduga. Hal ini akan berdampak pada kerahasiaan, integritas, dan ketersediaan.

Produk Software yang Terdampak:
TCP/IP, vendor Treck

Mitigasi Kerentanan
Jika pembaruan firmware tidak memungkinkan, mitigasinya akan mencakup segmentasi jaringan, atau pembatasan jaringan pada perangkat. Mungkin juga firewall paket pemeriksaan mendalam dapat mengatasi hal ini, karena semua eksploitasi dianggap sebagai paket jaringan ilegal.

Paket-paket tersebut mungkin dilewatkan oleh router/switch dan bahkan firewall, namun firewall inspeksi paket mendalam yang melakukan perakitan ulang dan memeriksa ketidakteraturan paket lainnya harus mampu menghentikan serangan ini.

US-Cert membuat daftar aturan pola jaringan potensial untuk mendeteksi dan berpotensi melindungi terhadap serangan ini. Pada akhirnya pelanggan harus memvalidasi bahwa semua langkah ini akan menjadi mitigasi kerentanan.

Beberapa langkah yang disarankan:
- Nonaktifkan atau blokir tunneling IP baik
- IPV6 dan IPv4 atau IP-in-IP.
- Blokir perutean sumber.
- Terapkan pemeriksaan TCP dan tolak paket TCP yang salah format.
- Blokir pesan kontrol ICMP yang tidak digunakan seperti pembaruan MTU dan pembaruan masker alamat.
- Normalisasikan atau blokir fragmen IP jika tidak didukung di lingkungan Anda.

Memutakhirkan ke versi 6.0.1.41 menghilangkan kerentanan ini.

CVE-2020-11910
CVSS Score: 5.3 Medium

Laboratorium penelitian JSOF telah menemukan serangkaian kerentanan zero-day dalam pustaka perangkat lunak TCP/IP tingkat rendah yang digunakan secara luas yang dikembangkan oleh Treck, Inc. 19 kerentanan, diberi nama Ripple20 dan CVE-2020-11910 salah satunya.

Kerentanan ini ada karena validasi yang tidak memadai dari input yang disediakan pengguna dalam komponen ICMPv4. Penyerang jarak jauh dapat mengirim paket yang dibuat khusus, memicu pembacaan di luar batas dan membaca isi memori pada sistem.

Dampak
Kerentanan memungkinkan penyerang jarak jauh untuk mendapatkan akses ke informasi sensitif atau mengambil kendali atas perangkat di dalam jaringan. Jika telah berhasil menyusup ke jaringan dapat menggunakan kerentanan library untuk menargetkan perangkat tertentu di dalamnya.

Pelaku dapat melakukan serangan yang mampu mengambil alih semua perangkat yang terkena dampak di jaringan secara bersamaan. Atau menggunakan perangkat yang terpengaruh sebagai cara untuk tetap tersembunyi di dalam jaringan selama bertahun-tahun.

Produk Terdampak
Ripple20 menjangkau perangkat IoT kritis dari berbagai bidang, yang melibatkan berbagai kelompok vendor. Vendor yang terkena dampak berkisar dari toko butik satu orang hingga perusahaan multinasional Fortune 500, termasuk HP, Schneider Electric, Intel, Rockwell Automation, Caterpillar, Baxter, serta banyak vendor internasional besar lainnya yang diduga rentan dalam kontrol medis, transportasi, industri, perusahaan, energi (migas), telekomunikasi, ritel dan perdagangan, dan industri lainnya.

Mitigasi Kerentanan
Vendor perangkat akan memiliki pendekatan yang berbeda dari operator jaringan. Secara umum, kami merekomendasikan langkah-langkah berikut:
- Semua organisasi harus melakukan penilaian risiko yang komprehensif sebelum menerapkan tindakan defensif.
- Pertama-tama terapkan tindakan defensif dalam mode “Alert” pasif.

Mitigasi untuk vendor perangkat:
- Tentukan apakah Anda menggunakan tumpukan Treck yang rentan.
- Hubungi Treck untuk memahami risiko.
- Perbarui ke versi tumpukan Treck terbaru (6.0.1.67 atau lebih tinggi).
- Jika pembaruan tidak memungkinkan, pertimbangkan untuk menonaktifkan fitur yang rentan, jika memungkinkan.

Mitigasi bagi operator dan jaringan:
(berdasarkan penasehat CERT/CC dan CISA ICS-CERT)
Mitigasi pertama dan terbaik adalah memperbarui ke versi yang ditambal dari semua perangkat.
Jika perangkat tidak dapat diperbarui, langkah-langkah berikut disarankan:

- Minimalkan eksposur jaringan untuk perangkat tertanam dan kritis, pertahankan eksposur seminimal mungkin, dan pastikan bahwa perangkat tidak dapat diakses dari internet kecuali benar-benar penting.
- Pisahkan jaringan dan perangkat OT di belakang firewall dan isolasi dari jaringan bisnis.
- Aktifkan hanya metode akses jarak jauh yang aman.
- Blokir lalu lintas IP anomali.
- Blokir serangan jaringan melalui inspeksi paket mendalam, untuk mengurangi risiko pada perangkat Anda yang mendukung TCP/IP tersemat Treck.

CVE-2023-50387
CVSS Score: 7.5 High

Aspek DNSSEC tertentu dari protokol DNS (dalam RFC 4033, 4034, 4035, 6840, dan RFC terkait) memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (konsumsi CPU) melalui satu atau beberapa respons DNSSEC, alias masalah "KeyTrap".

Salah satu kekhawatirannya adalah ketika ada zona dengan banyak rekaman DNSKEY dan RRSIG, spesifikasi protokol menyiratkan bahwa suatu algoritma harus mengevaluasi semua kombinasi rekaman DNSKEY dan RRSIG.

Dampak
Memproses respons yang dibuat khusus yang berasal dari zona bertanda DNSSEC dapat menyebabkan penggunaan CPU yang tidak terkendali, yang mengarah ke Penolakan Layanan di sisi resolver yang memvalidasi DNSSEC. Kerentanan ini hanya berlaku untuk sistem tempat validasi DNSSEC diaktifkan.

Produk yang Terdampak
Versi yang terpengaruh:
BIND

- 9.0.0 → 9.16.46
- 9.18.0 → 9.18.22
- 9.19.0 → 9.19.20

(Versi sebelum 9.11.37 tidak dinilai.)

Mitigasi
Tingkatkan ke rilis yang ditambal yang paling erat kaitannya dengan versi BIND 9 Anda saat ini:

- 9.16.48
- 9.18.24
- 9.19.21

CVE-2019-11500
CVSS Score: 9.8 Critical

CVE-2019-11500 dipublikasikan pada 28 Agustus 2019. Cacat ditemukan di Dovecot. Pengurai protokol IMAP dan ManageSieve tidak menangani byte NULL dengan benar.

Kerentanan memungkinkan penyerang jarak jauh untuk mengkompromikan sistem yang rentan. Kerentanan terjadi karena kesalahan batas dalam penerapan protokol IMAP dan ManageSieve saat memindai data dalam string yang dikutip. Penyerang jarak jauh dapat mengirim permintaan yang dibuat khusus ke server yang terpengaruh, memicu penulisan di luar batas, dan mengeksekusi kode arbitrer pada sistem target.

Dampak
Ancaman tertinggi dari kerentanan ini adalah terhadap kerahasiaan dan integritas data serta ketersediaan sistem. Ini menjadi tanda peringatan bagi pengguna Linux di Indonesia agar lebih waspada.

Produk yang Terdampak
Di Dovecot sebelum 2.2.36.4 dan 2.3.x sebelum 2.3.7.2 (dan Pigeonhole sebelum 0.5.7.2), pemrosesan protokol dapat gagal untuk string yang dikutip. Ini terjadi karena karakter '\0' salah penanganan, dan dapat menyebabkan penulisan di luar batas dan eksekusi kode jarak jauh.

Mitigasi Kerentanan
Melakukan patching atau update pada sistem operasi Linux yang digunakan dan melakukan pemindaian untuk mengidentifikasi adanya penyusupan.

CVE-2020-11902
CVSS Score: 7.3 High

Kerentanan dalam tumpukan TCP/IP Treck sebelum versi 6.0.1.66 memungkinkan untuk Out-of-Bounds Read selama tunneling IPv6 over IPv4. Masalah ini muncul akibat penanganan IPv6 over IPv4 tunneling yang tidak tepat, yang menyebabkan Pembacaan di Luar Batas.

Penyerang dapat mengeksploitasi kerentanan ini untuk mendapatkan akses tidak sah atau mengganggu sistem.

Dampak
Kerentanan tersebut berpotensi menyebabkan akses tidak sah, kebocoran data, atau kerusakan sistem.

Sistem yang Terdampak
Versi tumpukan TCP/IP Treck sebelum 6.0.1.66 terpengaruh.

Mitigasi Kerentanan
Langkah-langkah untuk mengatasi dan mencegah CVE.

Langkah segera yang harus diambil:
- Perbarui tumpukan TCP/IP Treck ke versi 6.0.1.66 atau yang lebih baru.
- Pantau lalu lintas jaringan untuk aktivitas yang mencurigakan.
- Perbarui perangkat lunak dan firmware secara berkala untuk menambal kerentanan.
- Terapkan segmentasi jaringan untuk membatasi dampak potensi pelanggaran.
- Lakukan audit keamanan dan pengujian penetrasi secara berkala.

CVE-2015-7547
CVSS Score: 8.1 High

Beberapa buffer overflow berbasis tumpukan dalam fungsi (1) send_dg dan (2) send_vc dalam pustaka libresolv di GNU C Library (alias glibc atau libc6) sebelum 2.23 memungkinkan penyerang jarak jauh untuk menyebabkan penolakan layanan (crash) atau mungkin mengeksekusi kode arbitrer melalui respons DNS yang dibuat yang memicu panggilan ke fungsi getaddrinfo dengan alamat AF_UNSPEC atau AF_INET6, yang terkait dengan pelaksanaan "kueri DNS A/AAAA ganda" dan modul NSS libnss_dns. so.2.

Dampak
Kerentanan dalam resolver DNS GNU libc (glibc) memungkinkan eksekusi kode jarak jauh (CVE-2015-7547). Namun, masalah ini hanya dapat dieksploitasi dari server DNS yang berada di bawah kendali penyerang.

Produk yang Terdampak
Masalah ini memengaruhi PAN-OS 5.0.19 dan versi sebelumnya; PAN-OS 5.1.12 dan versi sebelumnya; PAN-OS 6.0.14 dan versi sebelumnya; PAN-OS 6.1.12 dan versi sebelumnya; PAN-OS 7.0.7 dan versi sebelumnya; PAN-OS 7.1.3 dan versi sebelumnya.

Mitigasi
Kerentanan ini dapat memengaruhi perangkat lunak PAN-OS hanya jika perangkat dikonfigurasi dengan server DNS yang berada di bawah kendali penyerang. Palo Alto Networks tidak menganjurkan konfigurasi perangkat dengan server DNS yang tidak terpercaya.

CVE-2023-46604
CVSS Score: 9.8 Critica

Kerentanan marshaller protokol Java OpenWire terhadap eksekusi kode jarak jauh. Kerentanan dengan tingkat keparahan kritis yang dapat dieksploitasi di Apache ActiveMQ.

Hal ini memungkinkan penyerang jarak jauh dengan akses jaringan ke broker OpenWire berbasis Java (seperti ActiveMQ) atau klien untuk menjalankan perintah shell dengan memanipulasi tipe kelas serial dalam protokol OpenWire untuk menyebabkan klien atau broker (masing-masing) membuat instance kelas mana pun di jalur kelas.

Dampak
CVE 2023-46604 memengaruhi perangkat lunak apa pun yang menggunakan protokol OpenWire berbasis Java. Khususnya, ActiveMQ Classic dan ActiveMQ Artemis, serta klien OpenWire berbasis Java, seperti ketergantungan Maven pada ActiveMQ-Client.

Produk Terdampak
Hal ini akan berdampak pada versi ActiveMQ Classic di bawah 5.18.3, 5.17.6, 5.16.7, dan 5.15.16, serta Artemis 2.31.2. Dengan kata lain, sudah diperbaiki di ActiveMQ 5.18.3, namun rentan di 5.18.2, 5.18.1, dan 5.18.0, dan seterusnya.

Kerentanan ini telah dieksploitasi, sehingga sistem harus segera ditambal. Eksploitasi CVE-2023-46604 yang berhasil dapat mengakibatkan berbagai tindakan, seperti:
- Mencuri data sensitif
- Menginstal malware
- Mengganggu operasional server
- Meluncurkan serangan lebih lanjut terhadap sistem lain yang terhubung dengan broker

Mitigasi Kerentanan
Mitigasi yang paling pasti adalah meningkatkan ke versi ActiveMQ yang di-patch. Versi berikut mengatasi kerentanan:
- 15.5.16
- 5.16.7
- 5.17.6
- 5.18.3

Versi lama dalam setiap cabang (5.15, 5.16, 5.17, dan 5.18) masih rentan.

Pilihan lainnya adalah menonaktifkan OpenWire. Ini akan membatasi serangan, namun juga membatasi fungsionalitas. Akses jaringan dapat dibatasi hanya untuk klien yang berwenang. Ini akan membantu mengurangi permukaan serangan. Kemudian langkah-langkah keamanan tambahan dapat diterapkan, seperti firewall, kontrol akses, dan sistem deteksi intrusi.

CVE-2018-13379
CVSS: 9.1 Critical

Ini menunjukkan upaya serangan untuk mengeksploitasi kerentanan pengungkapan informasi di FortiOS pada perangkat Fortinet. Kerentanan ini disebabkan oleh kesalahan dalam aplikasi yang rentan saat menangani permintaan yang disalahgunakan.

Terdeteksi sejak tahun 2018, pelaku yang tidak diotentikasi dapat mengeksploitasi ini untuk mengakses informasi sensitif di mesin yang terpengaruh melalui permintaan yang dibuat.

Produk yang Terdampak:
- FortiOS versi 5.4.12 hingga 5.6.0
- FortiOS versi 5.6.3 hingga 5.6.7
- FortiOS versi 6.0.0 hingga 6.0.4
- FortiProxy versi 1.0.0 hingga 1.0.7
- FortiProxy versi 1.1.0 hingga 1.1.6
- FortiProxy versi 1.2.0 hingga 1.2.8
- FortiProxy versi 2.0.0 yang menggunakan SSL-VPN

Mitigasi Kerentanan
Untuk mencegah serangan yang menargetkan sistem FortiOS adalah dengan mengupgrade versi FortiOS atau menonaktifkan Layanan SSL-VPN baik dalam mode kanal dan web.

CVE-2021-41773
CVSS Score: 7.5 High

Cacat ditemukan dalam perubahan yang dilakukan pada normalisasi jalur di Apache HTTP Server 2.4.49. Seorang penyerang dapat menggunakan serangan traversal jalur untuk memetakan URL ke berkas di luar direktori yang dikonfigurasi oleh direktif mirip Alias. Jika berkas di luar direktori ini tidak dilindungi oleh konfigurasi default yang biasa "require all denied", permintaan ini dapat berhasil.

Dampak
Jika skrip CGI juga diaktifkan untuk jalur alias ini, ini dapat memungkinkan eksekusi kode jarak jauh. Masalah ini diketahui dieksploitasi secara luas. Masalah ini hanya memengaruhi Apache 2.4.49 dan bukan versi sebelumnya. Perbaikan di Apache HTTP Server 2.4.50 ditemukan tidak lengkap, lihat CVE-2021-42013.

Produk yang Terkena Dampak
- Oracle Instantis Enterprisetrack
- Sistem Operasi Fedora
- Apache Software Foundation Apache HTTP Server

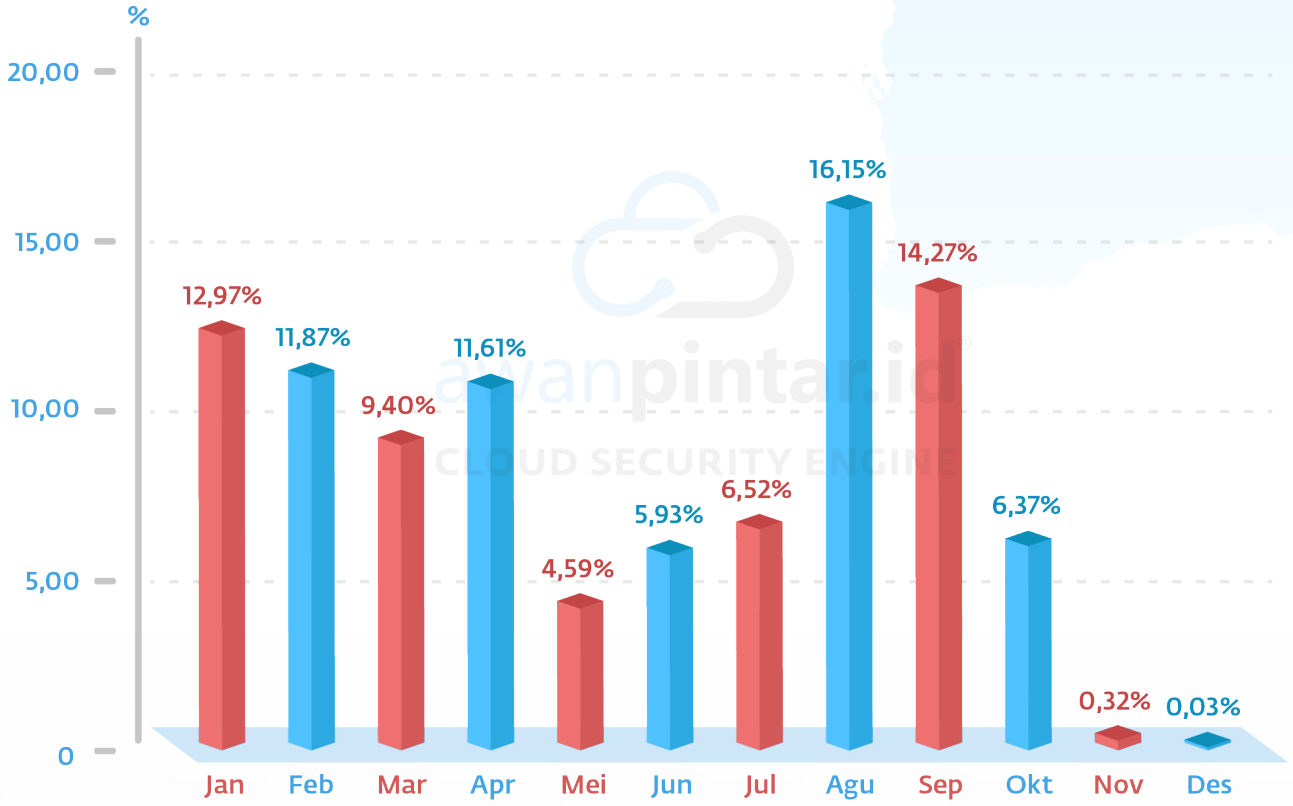
Mitigasi Kerentanan
Untuk memperbaiki kerentanan ini, disarankan memutakhirkan Apache ke versi terbaru 2.4.50. Periksa perbaikan Vulcan Cyber Remedy Cloud untuk CVE-2021-41773 untuk tindakan perbaikan lebih lanjut.

Fakta bahwa kerentanan tersebut diperkenalkan pada versi 2.4.49 dan diperbaiki pada versi 2.4.50 berarti mungkin sebagian besar pelanggan bahkan tidak mendapat kesempatan untuk memutakhirkan ke versi yang rentan ini.

Eksploitasi CVE Sepanjang Tahun 2024

Pada tahun 2024 ada beberapa kejutan dalam data yang dikeluarkan oleh AwanPintar.id®. Dari serangan yang mengeksploitasi Common Vulnerability & Exposures diketahui bahwa tidak ada kerentanan yang dieksploitasi secara dominan, berbeda dengan tahun sebelumnya.

Bahkan ancaman yang datang dari CVE menurun dengan sangat drastis di bulan-bulan akhir tahun 2024. Bahkan bulan Desember tidak ada ancaman yang masuk dari memanfaatkan Common Vulnerability & Exposures.



Bila ditarik kesimpulan, ancaman dari kerentanan umum secara garis besar cukup signifikan di awal bulannya. Peningkatan dan penurunan persentase di setiap bulannya menunjukkan adanya fluktuasi yang cukup besar, di tahun 2024 setiap enam bulan terjadi penurunan serangan yang drastis.

Tren penurunan serangan seperti ini terjadi di setiap lini ancaman, dimana di beberapa bulan terakhir tahun 2024 semua ancaman menyusut jauh. Penyerang membatasi serangan pada kerentanan umum dan mengalihkan perhatian mereka kepada sasaran lain yang lebih memiliki prospek lebih tinggi.

Penurunan ancaman pada CVE ini patut disyukuri sekaligus wajib diwaspadai, ini seperti ketenangan sebelum badai. Tahun 2025 akan banyak tantangan siber yang akan dihadapi, sedia payung sebelum hujan adalah tindakan preventif yang seharusnya.

Green
OPEN

CVE-2024 Berdasarkan Jumlah Serangan

Secara khusus AwanPintar.id® memberikan catatan khusus terhadap CVE-2024 yaitu CVE yang dirilis pada tahun 2024 dan pada tahun yang sama dimanfaatkan oleh para penyerang untuk segera dieksploitasi. Serangan setelah jeda Zero-Day umumnya dilakukan terhadap perangkat atau sistem yang terlambat melakukan patching dan merupakan bentuk serangan termudah karena dibiarkan terbuka.

Kode	Alert Signature	Persentase
CVE-2024-327	ET WEB_SPECIFIC_APPS D-Link NAS devices Backdoor Account Access and Command Injection Attempt	80.84%
CVE-2024-24919	ET WEB_SPECIFIC_APPS Checkpoint Quantum Security Gateway Arbitrary File Read Attempt	7,19%
CVE-2024-1709	ET WEB_SPECIFIC_APPS ConnectWise ScreenConnect - Attempted SetupWizard Auth Bypass	5,15%
CVE-2024-24919	ET WEB_SPECIFIC_APPS Checkpoint Quantum Security Gateway Arbitrary File Read Attempt	1,44%
CVE-2024-36104	ET WEB_SPECIFIC_APPS Apache OFBiz Directory Traversal Remote Code Execution Attempt	0,84%
CVE-2024-0204	ET WEB_SPECIFIC_APPS GoAnywhere MFT Authentication Bypass Attempt - GET Request M1	0,60%
CVE-2024-45519	ET EXPLOIT Zimbra postjournal RCE Attempt Inbound	0,48%
CVE-2024-21893	ET EXPLOIT Ivanti Connect Secure (9.x,22.x) / Ivanti Policy Secure (9.x,22.x) / Ivanti Neurons for ZTA SSRF Pattern	0,36%
CVE-2024-1709	ET WEB_SPECIFIC_APPS ConnectWise ScreenConnect - Attempted SetupWizard Auth Bypass CWE-288	0,36%
CVE-2024-0204	ET WEB_SPECIFIC_APPS GoAnywhere MFT Authentication Bypass Attempt - GET Request M1	0,36%
CVE-2024-22024	ET WEB_SPECIFIC_APPS Ivanti Connect Secure XXE Attempt	0,36%

Green
OPEN

Jenis CVE-2024 Setiap Bulan

Bulan	Kode CVE	Bulan Rilis CVE	Alert Signature
2024-02	CVE-2024-0204	2024-01	ET WEB_SPECIFIC_APPS GoAnywhere MFT Authentication Bypass Attempt - GET Request M1
2024-03	CVE-2024-1709	2024-02	ET WEB_SPECIFIC_APPS ConnectWise ScreenConnect - Attempted SetupWizard Auth Bypass CWE-288
	CVE-2024-27198	2024-03	ET WEB_SPECIFIC_APPS JetBrains TeamCity Authentication Bypass Attempt - Vulnerability Check
2024-04	CVE-2024-21893	2024-01	ET EXPLOIT Ivanti Connect Secure (9.x,22.x) / Ivanti Policy Secure (9.x,22.x) / Ivanti Neurons for ZTA SSRF Pattern
	CVE-2024-23897	2024-01	ET EXPLOIT Jenkins Unauthenticated RCE Attempt Observed
	CVE-2024-1709	2024-02	ET WEB_SPECIFIC_APPS ConnectWise ScreenConnect - Attempted SetupWizard Auth Bypass CWE-288
	CVE-2024-3273	2024-04	ET WEB_SPECIFIC_APPS D-Link NAS devices Backdoor Account Access and Command Injection Attempt
	CVE-2024-0204	2024-01	ET WEB_SPECIFIC_APPS GoAnywhere MFT Authentication Bypass Attempt - GET Request M1
	CVE-2024-22024	2024-02	ET WEB_SPECIFIC_APPS Ivanti Connect Secure XXE Attempt
	CVE-2024-27198	2024-03	ET WEB_SPECIFIC_APPS JetBrains TeamCity Authentication Bypass Attempt - Vulnerability Check
2024-05	CVE-2024-3273	2024-04	ET WEB_SPECIFIC_APPS D-Link NAS devices Backdoor Account Access and Command Injection Attempt
	CVE-2024-3400	2024-04	ET WEB_SPECIFIC_APPS Palo Alto GlobalProtect Session Cookie Command Injection Attempt
2024-06	CVE-2024-24919	2024-05	ET WEB_SPECIFIC_APPS Checkpoint Quantum Security Gateway Arbitrary File Read Attempt
	CVE-2024-3273	2024-04	ET WEB_SPECIFIC_APPS D-Link NAS devices Backdoor Account Access and Command Injection Attempt
2024-07	CVE-2024-36104	2024-06	ET WEB_SPECIFIC_APPS Apache OFBiz Directory Traversal Remote Code Execution Attempt
	CVE-2024-24919	2024-05	ET WEB_SPECIFIC_APPS Checkpoint Quantum Security Gateway Arbitrary File Read Attempt
2024-08	CVE-2024-7029	2024-08	ET WEB_SPECIFIC_APPS AVTECH IP Camera LED Brightness Parameter Command Injection Attempt
2024-09	CVE-2024-7029	2024-08	ET WEB_SPECIFIC_APPS AVTECH IP Camera LED Brightness Parameter Command Injection Attempt
	CVE-2024-36401	2024-07	ET WEB_SPECIFIC_APPS Geoserver Unsafe jxpath Evaluation RCE Attempt M2
	CVE-2024-36401	2024-07	ET WEB_SPECIFIC_APPS Geoserver Unsafe jxpath Evaluation RCE Attempt M5
2024-10	CVE-2024-23334	2024-01	ET EXPLOIT aiohttp Directory Traversal in Static Routing
	CVE-2024-7029	2024-08	ET WEB_SPECIFIC_APPS AVTECH IP Camera LED Brightness Parameter Command Injection Attempt
2024-11	CVE-2024-45519	2024-09	ET EXPLOIT Zimbra postjournal RCE Attempt Inbound

Dalam tabel, ada kategori signature yang ditandai dengan warna merah, ini menunjukkan bahwa nomor CVE-2024 tersebut begitu dirilis langsung dieksploitasi oleh pelaku kejahatan siber pada bulan yang sama. Berikut CVE-2024 yang dimaksud:
CVE-2024-27198

Di tabel yang sama juga dapat ditemui kategori signature yang diberi warna jingga, warna tersebut menandai bahwa kategori tersebut merupakan CVE-2024 yang dieksploitasi oleh pelaku kejahatan siber satu bulan setelah kerentanan tersebut dirilis. Berikut daftar CVE-2024 yang dimaksud:

- CVE-2024-0204
- CVE-2024-1709
- CVE-2024-27198
- CVE-2024-3273
- CVE-2024-3273
- CVE-2024-3400
- CVE-2024-24919
- CVE-2024-36104
- CVE-2024-7029
- CVE-2024-45519

Dari penjabaran di atas jika menilik dari kerentanan tahun lalu yang langsung dieksploitasi begitu dirilis, pada tahun ini pemanfaatan tersebut mengalami penurunan. Sementara eksploitasi yang dilakukan sebulan kemudian masih sama jumlah eksploitasinya.

Catatan khusus diberikan pada CVE-2024-45519 yang dirilis pada bulan Oktober 2024 dengan CVSS Score 9.8 Critical. Banyaknya pengguna mail server Zimbra Collaboration Suite (ZCS) di Indonesia bisa menjadi catatan khusus untuk mendapatkan perhatian. Dampak yang ditimbulkan tergolong berbahaya karena siapapun dapat menjalankan perintah di server Zimbra. Sangat disarankan untuk segera dilakukan patching. Terkait Zimbra, ditemukan juga CVE-2019-9621 dan CVE-2019-9670 yang dirilis tahun 2019. Ini menunjukkan serangan dengan target sistem tertentu menyerang Indonesia. Upaya serangan terhadap Zimbra cukup konsisten dengan mencoba CVE rilis di tahun yang lama dan baru.
Zimbra Patch:

- Zimbra 8.8.15 Patch minimal 46
- Zimbra 9.0.0 Patch minimal 41
- Zimbra 10.0.x gunakan patch terakhir
- Zimbra 10.1.x gunakan patch terakhir

SERANGAN DALAM NEGERI

Akumulasi Serangan dalam Negeri

Seperti dalam edisi sebelumnya dalam laporan ancaman digital edisi kali ini disertakan juga reportase khusus tentang serangan dalam negeri. Serangan dalam negeri merupakan ancaman yang berasal dari dalam negeri yang berasal dari suatu daerah ke daerah lain dalam lingkup nusantara.

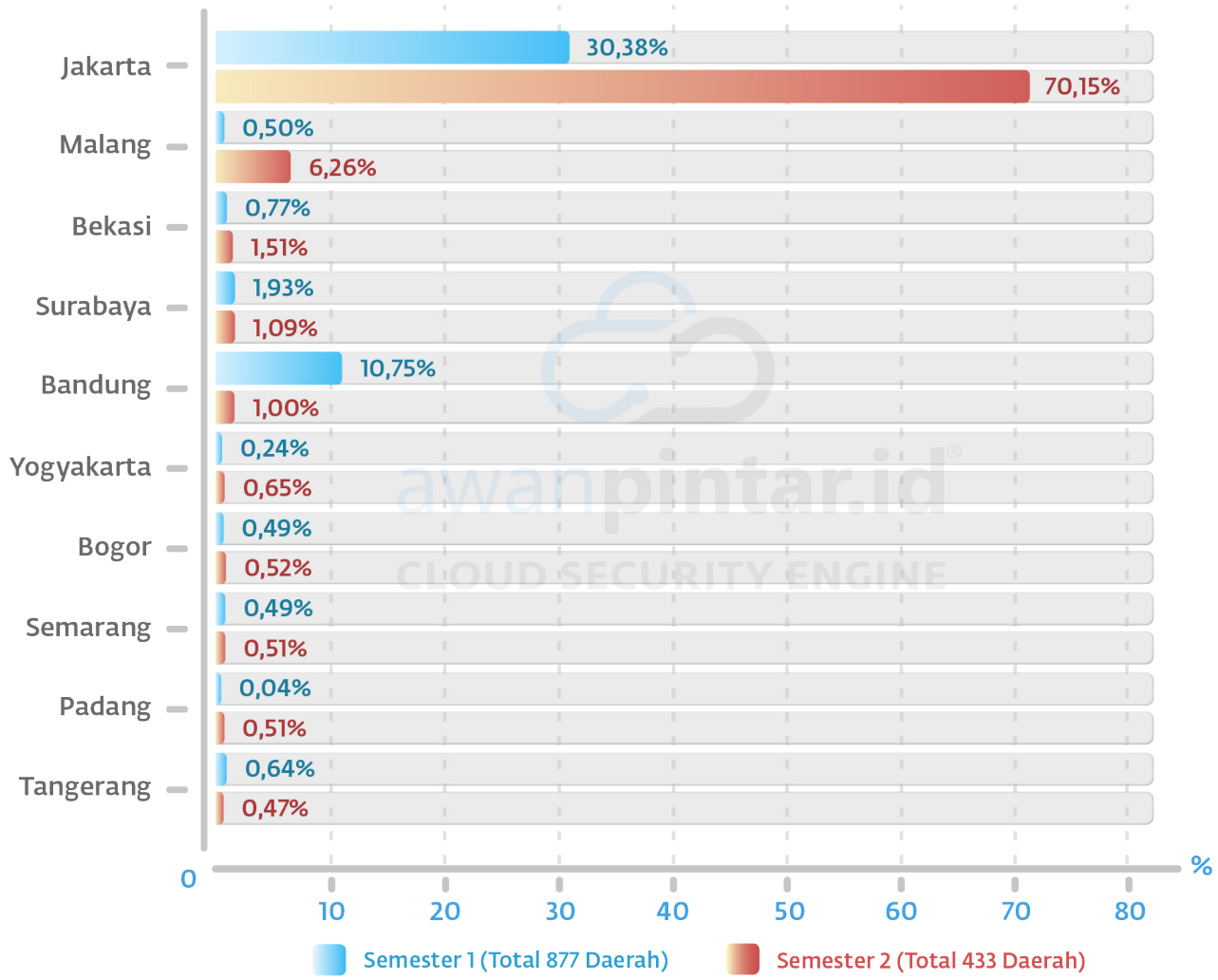
Namun serangan semacam ini bisa juga menjadi serangan kamuflase, yakni serangan datang dari luar Indonesia yang memanfaatkan IP lokal untuk melakukan serangan ke daerah lain yang ada di Indonesia.

10 Daerah Penyerang Teratas di Indonesia Semester 1 dan 2 Tahun 2024

Penyebaran teknologi dan internet di Indonesia begitu pesatnya sehingga masuk ke berbagai pelosok di tanah air. Dengan terus meningkatnya penetrasi internet di berbagai daerah setiap tahunnya, banyak manfaat yang diperoleh oleh masyarakat kebanyakan.

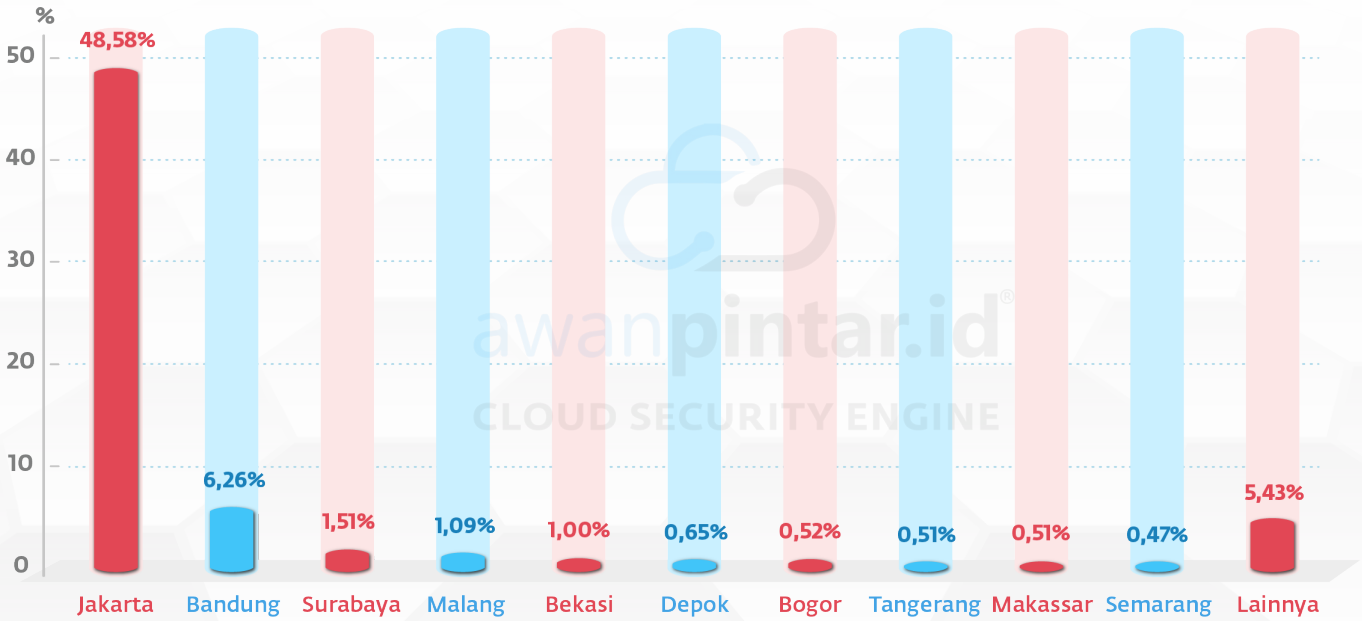
Namun, di sisi lain ada risiko besar yang mengancam keamanan siber para penggunanya, pencurian data personal, data perbankan, finansial dan berbagai data berharga lainnya dengan sendiri akan juga meningkat, sementara kesadaran praktik keamanan siber yang baik belum sepenuhnya dipahami oleh masyarakat pada umumnya.

Berikut adalah data yang berhasil diakumulasi oleh AwanPintar.id® dari lalu lintas jaringan internet di Indonesia dalam enam bulan terakhir.



10 Daerah Penyerang Tahun 2024

Total 921 Daerah



Ketahanan siber nasional akan semakin diuji dengan semakin meratanya penyebaran infrastruktur di Indonesia. DKI Jakarta sebagai ibukota negara dan daerah yang paling maju dan terdepan dalam penerapan teknologi sekaligus menjadi pusat pengembangan keamanan siber.

Situasi dan kondisi yang ideal tersebut merupakan tempat yang nyaman juga bagi pelaku kejahatan siber untuk melakukan aksi-aksi ilegal digital mereka. Tidak heran apabila kemudian Jakarta selalu menjadi di posisi pertama termasuk sebagai daerah yang paling sering melakukan serangan siber ke daerah lain.

Pada semester 2 tahun 2024, di luar dugaan adalah eskalasi serangan dari DKI Jakarta yang meningkat harus menjadi perhatian. Kemudian Malang dan Bekasi yang langsung mengisi posisi kedua dan ketiga walau pada semester sebelumnya tidak masuk dalam peringkat 5 besar.

Bekasi bukan pertama kali berada di 5 besar daerah penyerang teratas, tahun sebelumnya kota satelit ini mampu berdiri di bawah DKI Jakarta. Sedangkan Malang yang memiliki pertumbuhan internet yang sangat baik dengan banyaknya provider internet dan menyebarnya infrastruktur digital membuat daerah tersebut subur dalam perkembangan teknologi.

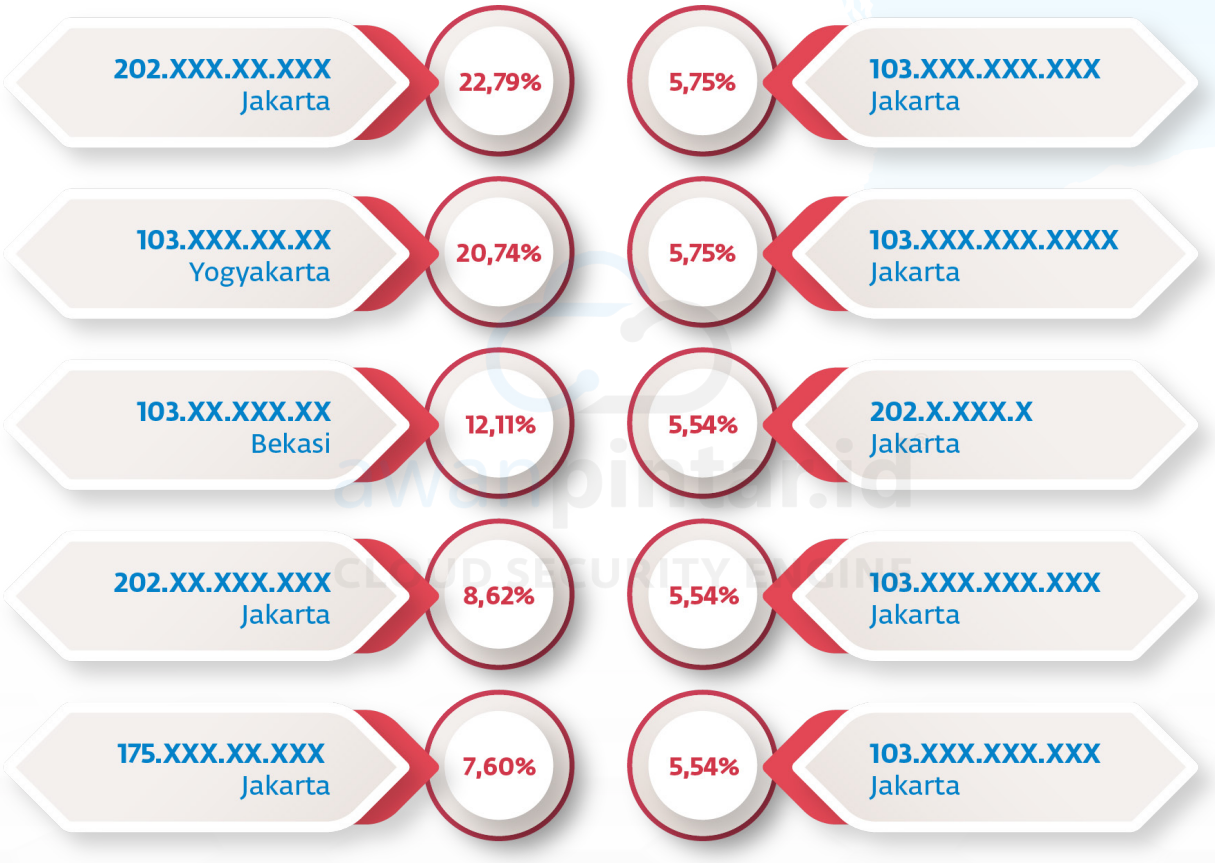
Jika melihat data selama tahun 2024, Jakarta, Bandung dan Surabaya tetap berada di puncak daerah penyerang. Malang, daerah yang pada tahun sebelumnya tidak masuk ke dalam 5 besar, pada tahun ini berada pada posisi nomor 4 menggeser Bekasi dan Depok yang berada di bawahnya. Depok yang pada tahun sebelumnya berada pada posisi 5 besar, pada tahun ini tergusur ke posisi 6.

IP Spam dan Malware di Indonesia

Alamat IP seperti nomor identifikasi yang terhubung dengan perangkat yang memberitahukan darimana trafik internet berasal. Alamat IP dengan kata lain merupakan jejak digital yang bisa ditelusuri.

Serangan spam dan malware dapat ditelusuri dari IP yang digunakannya, berikut adalah data IP spam dan malware yang digunakan untuk melakukan serangan siber di tanah air.

IP Spam di Indonesia



Jakarta sebagai daerah dengan infrastruktur terbaik di Indonesia merupakan alasan utama yang menempatkan mereka di puncak daftar. Pelaku kejahatan siber membutuhkan koneksi yang baik untuk menjalankan aktivitas ilegal mereka.

Terlepas dari semua kelebihan Jakarta, yang cukup menjadi perhatian adalah Yogyakarta yang memiliki aktivitas serangan melalui IP yang tidak jauh persentasenya jika berdasar satuan serangan.

Begitu pula Bekasi sebagai kota satelit juga memiliki sarana teknologi informasi yang tak begitu berbeda dengan ibukota. Modal ini punya peranan besar dalam jumlah persentase serangan IP di Indonesia.

IP Malware di Indonesia

Selaras dengan asal alamat IP untuk serangan spam, dalam serangan malware di Indonesia, alamat IP yang dideteksi sebagian besar berasal dari Jakarta. Malware sendiri sering dibawa melalui serangan spam, sehingga hasil data yang diperoleh AwanPintar.id® tidak menunjukkan banyak perbedaan.

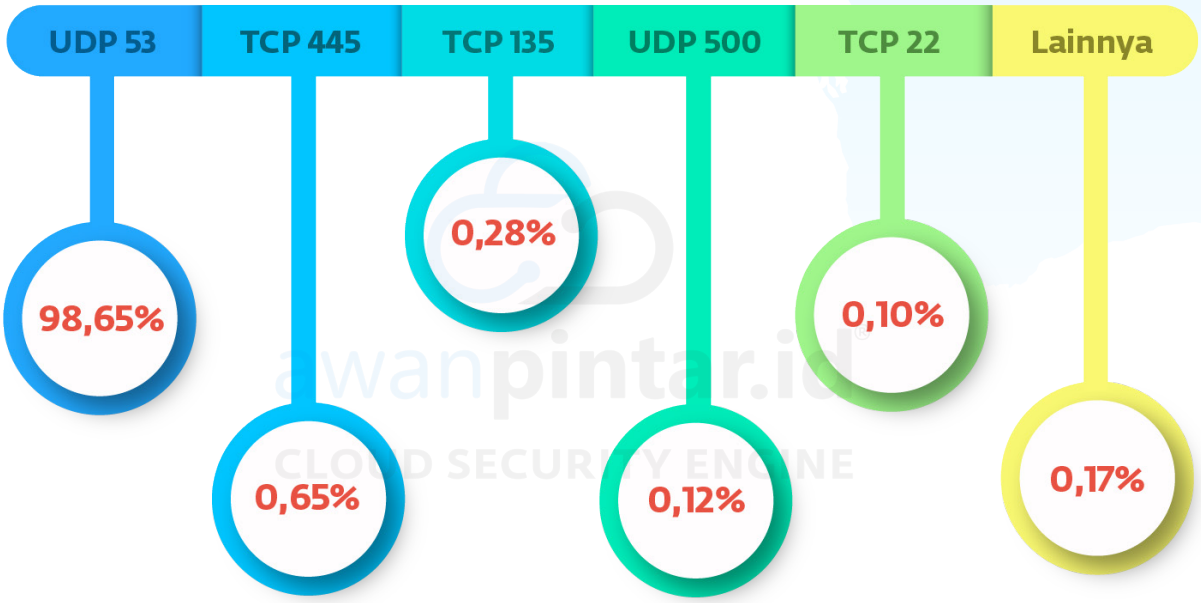
Yang menarik dari data yang disajikan, hadirnya NTB dan Mergoyoso, Jawa Timur dalam peta serangan IP malware di Indonesia. Terlebih lagi NTB berada di puncak daftar benar-benar sebuah anomali.

Namun, penggunaan IP yang berasal dari NTB bisa juga merupakan proxy atau kamuflase yang digunakan oleh pelaku dari daerah lain untuk menyamarkan aktivitasnya agar sulit untuk dilacak.

Serangan Port Dalam Negeri

Port sarana favorit peretas mencari jalan masuk ke dalam sistem. Seringkali port tidak dikonfigurasi dengan baik dan kurang mendapat perhatian dalam keamanannya merupakan masalah klasik yang berulang.

AwanPintar.id® dalam reportase kali ini juga mengolah data-data port yang sering diincar oleh pelaku kejahatan siber di dalam negeri.



Serangan pada port dalam serangan dalam negeri dimana ancaman siber melalui port berasal dari serangan yang datang dari Indonesia secara garis besar hasilnya tidak terlalu berbeda dengan laporan port favorit peretas.

Pada ancaman port di serangan port dalam negeri, sumber utama hampir semua serangan berasal dari port 53. Fungsi port ini digunakan untuk mengirim dan menerima data dalam protokol DNS (Domain Name System). DNS adalah sistem yang digunakan untuk mengubah nama domain menjadi alamat IP. Dengan menguasai port 53 ini sama dengan membuka jalan ke setiap sistem yang lalu lalang dalam jaringan.

Pengguna internet dan para tim IT perusahaan harus mampu mengkonfigurasi port dengan tepat dan melindungi keamanannya dengan baik, bisa membantu meminimalisir atau mengurangi sebagian besar ancaman. Ini juga berlaku untuk port yang lain juga.

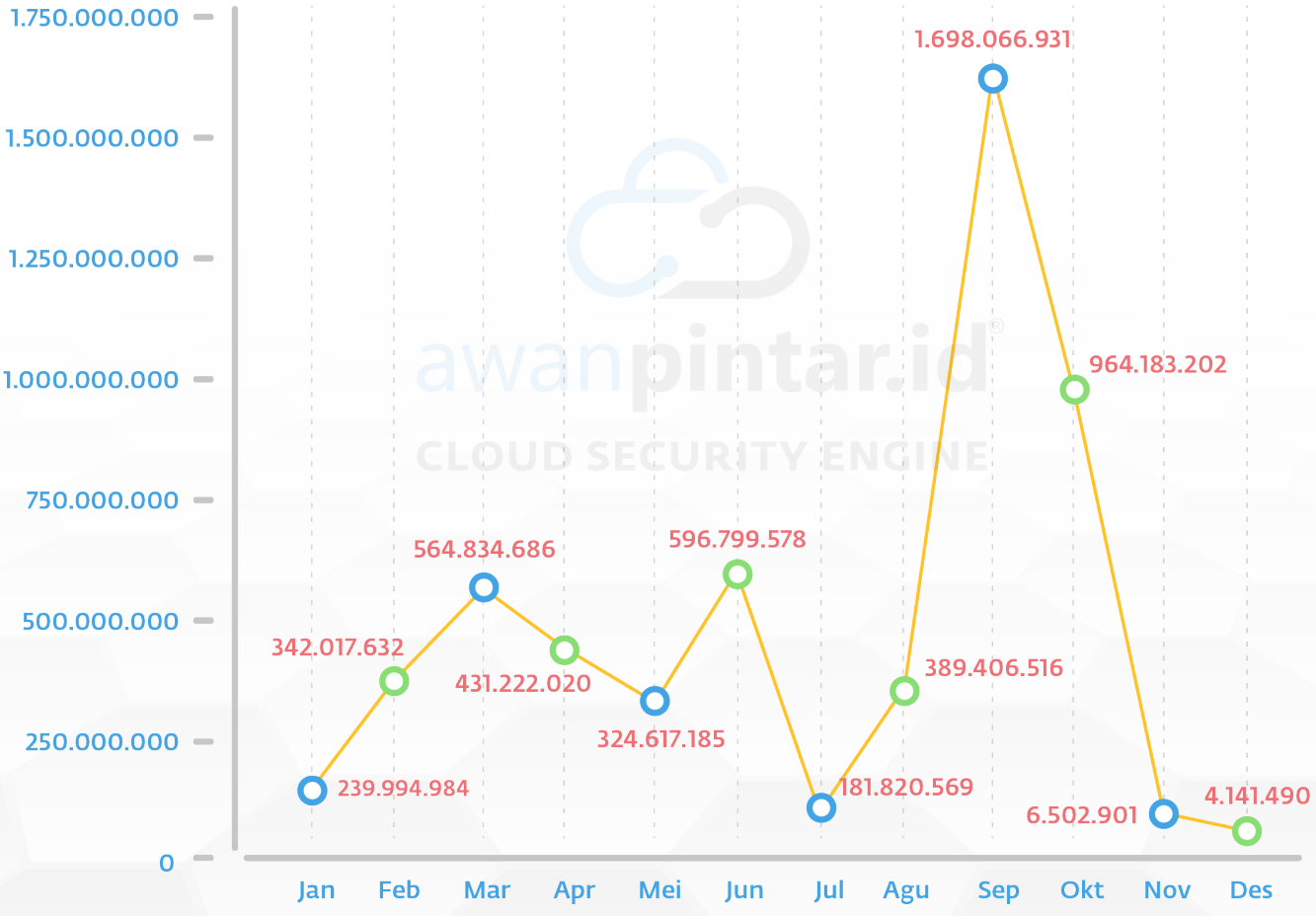
Green
OPEN

KESIMPULAN LAPORAN 2024

Tren serangan siber di tahun 2024 terangkum secara utuh dalam kesimpulan laporan 2024, yang memberikan wawasan secara eksplisit serangan siber yang melanda Indonesia.

Merambahnya teknologi yang menjangkau ke berbagai penjuru nusantara yang semakin memarakkan penggunaan internet membawa manfaat dan bencana di saat yang bersamaan. Keinginan untuk terus mengikuti arus perkembangan jaman, pada tempatnya harus juga siap menghadapi risiko yang dibawanya.

Untuk mengetahui risiko-risiko tersebut, AwanPintar.id® sebagai teknologi siber yang dikembang oleh anak bangsa telah merangkum data-data ancaman yang masuk tahun ini.



Bisa dikatakan hampir sepanjang tahun atau selama delapan bulan lamanya, fluktuasi serangan siber di Indonesia tidak mengalami perubahan yang mencolok. Serangan siber baru melonjak secara eksponensial. Pertumbuhan terjadi begitu cepat dalam hal jumlah dan varian serangan dalam infrastruktur jaringan internet nasional.

Yang cukup mengejutkan adalah begitu serangan melonjak dengan drastis dalam dua bulan kemudian dalam dua bulan kemudian serangan menurun dengan sangat cepat dan signifikan. Pada dua bulan terakhir tahun 2024 para penjahat dunia maya hanya fokus melakukan upaya pencurian kredensial.

Serangan ini sangat tertarget melihat dari sasaran yang dituju adalah hak akses pengguna super atau hak akses administrator, dimana penyerang yang berhasil menguasai akses tersebut dapat melakukan apapun pada sistem yang dikuasai. Serangan tertarget adalah serangan yang dilakukan bertahap dan dipersiapkan dengan sangat matang, korban-korban sudah diincar dan ditentukan jauh hari sebelumnya dan dipelajari sebaik-baiknya sebelum dieksekusi.

Beberapa catatan terkait pemanfaatan kelemahan sistem yaitu CVE-2024-45519 terkait Zimbra Email Server serta CVE pada tahun sebelumnya terkait Apache, Fortinet Cisco dan Mikrotik. Sistem tersebut banyak digunakan di Indonesia dan layak mendapatkan peringatan dan perhatian khusus.

Berdasarkan data dari AwanPintar.id® ini maka kalangan dunia usaha dan institusi pemerintah ada baiknya melakukan audit ulang untuk semua akses admin mereka untuk menjamin kerahasiaan data yang disimpan secara digital.

PENUTUP

Dalam Laporan Ancaman Digital di Indonesia Semester 2 dan Analisa Serangan Tahun 2024 mendapatkan data ancaman yang datang silih berganti dengan berbagai bentuk dan teknik serangannya. Menunjukkan banyaknya ruang yang terbuka untuk dieksploitasi, baik itu kerentanan lama maupun kerentanan baru.

Pemerintah dan dunia siber nasional perlu meningkatkan ketahanan infrastruktur siber untuk menghadapi serangan siber yang semakin kompleks. Salah satu caranya adalah dengan melakukan pengelolaan keamanan digital bersama agar lebih efektif dalam mengidentifikasi dan mitigasi potensi ancaman siber.

Langkah tersebut sudah AwanPintar.id® lakukan melalui kerjasama dengan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) di semester 1 tahun 2024, untuk memperluas cakupan dan mengintensifkan pengamanan jaringan nasional secara berkelanjutan demi memastikan keamanan, kedaulatan dan konektivitas digital di Indonesia.

Selain itu, AwanPintar.id® juga berupaya terus meningkatkan kualitas pengelolaan jaring pengamanan nasional dalam mendeteksi dan mengidentifikasi setiap ancaman yang masuk dan keluar di Indonesia, berbagi kajian data ancaman sebagai informasi dan edukasi kepada masyarakat.