awanpintar.id®
CLOUD SECURITY ENGINE

Green
OPEN

INDONESIA WASPADA

Laporan Ancaman Digital di Indonesia

Semester 1 Tahun 2024

Green
OPEN

DAFTAR ISI

awanpintar.id®
CLOUD SECURITY ENGINE

Green
OPEN

awanpintar.id
CLOUD SECURITY ENGINE

Green
OPEN

PENTINGNYA REFERENSI TERPERCAYA PETA ANCAMAN DIGITAL DI INDONESIA

oleh Muhammad Arif
Ketua Umum Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)

Assalamu alaikum wr wb, Salam sejahtera, Om swastiastu, Nammo budhaya, Salam kebajikan.

Merupakan sebuah kehormatan bagi saya untuk memberikan kata pengantar pada Laporan Ancaman Digital di Indonesia Semester 1 Tahun 2024, INDONESIA WASPADA, yang dikeluarkan oleh AwanPintar.id®.

Seperti kita ketahui bersama, beberapa tahun belakangan ini negara kita banyak menerima serangan siber yang sangat meresahkan karena berdampak pada berhentinya layanan operasional yang menyebabkan kerugian finansial yang sangat besar. Serangan ransomware ke Bank Syariah Indonesia pada tahun 2023 dan serangan serupa ke Pusat Data Nasional Sementara (PDNS) pada tahun 2024 adalah dua kejadian yang masih hangat dan menjadi pembelajaran berharga bagi para profesional IT, khususnya di sektor pemerintahan dan BUMN.

Menurut Laporan AwanPintar.id® Semester 2 Tahun 2023, serangan siber dari mancanegara ke Indonesia mengalami kenaikan 97,53% dibandingkan Semester 1 pada tahun yang sama. Pada tengah tahun pertama 2024, dilaporkan adanya peningkatan serangan yang luar biasa, yang semakin menarik perhatian sekaligus meningkatkan kewaspadaan kita.

Mengacu kepada Peraturan Presiden Republik Indonesia Nomor 47 tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) berupaya untuk ikut ambil bagian dalam menjaga kedaulatan siber nasional. Salah satu strategi yang dilakukan adalah menjalin kemitraan dengan AwanPintar.id® sejak tahun 2024.

Saat ini, perangkat dan sistem detektor AwanPintar.id® telah tersebar di lima belas lokasi Kepengurusan APJII, satu lokasi di pusat dan 14 lokasi di tingkat wilayah, yaitu: DKI Jakarta (Pusat), Banten, Jawa Barat, DI Yogyakarta, Jawa Tengah, Jawa Timur, Bali-Nusra, Lampung, Jambi, Sumatera Utara, Kepulauan Riau, Sulampua (Sulawesi, Maluku, dan Papua), Kalimantan, dan Riau-Sumatera Barat. Direncanakan jumlah ini masih akan bertambah agar APJII dapat memberikan layanan yang lebih baik kepada para pelaku bisnis Internet Service Provider (ISP) selaku anggota APJII. Melalui kerja sama dengan AwanPintar.id®, APJII dapat memantau serangan yang masuk ke jaringan internet APJII (IX) secara real time dan membaca hasil riset dalam bentuk laporan pada dashboard yang ada.

Green
OPEN

Berdasarkan data internal APJII yang diambil dari https://awanpintar.apjii.or.id/ dari 1 Mei hingga 1 Juli 2024, diketahui telah terjadi sebanyak 460.369.076 serangan yang berasal dari alamat IP anggota APJII yang terhubung di IX. Ini menunjukkan adanya celah kerentanan di jaringan anggota APJII dan menjadi kewajiban APJII untuk mengkomunikasikan cara menghindari atau meminimalisir risiko demi memperkuat pertahanan siber nasional.

Laporan AwanPintar.id® berfungsi sebagai seruan untuk bertindak, mendesak para pemangku kepentingan untuk memprioritaskan keamanan siber dalam agenda strategis mereka. Melalui laporan ini, kita dapat membuka jalan bagi semua pengguna internet di tanah air untuk memetakan kerentanan yang mereka miliki dan melakukan tindakan pencegahan sedari dini, sehingga ke depan dapat memperkuat fondasi dunia maya kita yang saling terhubung.

Dengan data yang dapat diandalkan dari AwanPintar.id®, kita berharap dapat membuat keputusan yang lebih tepat dan strategis dalam mengatasi ancaman siber, meningkatkan kesiapan dan respons terhadap insiden siber, serta membangun sistem keamanan yang lebih kuat dan proaktif. Data ini juga memungkinkan kita untuk melakukan evaluasi dan perbaikan berkelanjutan, memastikan bahwa langkah-langkah keamanan yang diterapkan benar-benar efektif dalam menghadapi ancaman yang terus berkembang. Tantangan keamanan siber akan semakin kompleks dan sulit di masa depan. Hanya dengan kerjasama yang solid antara seluruh pemangku kepentingan keamanan siber nasional, kita dapat mengatasi tantangan ini. APJII dan AwanPintar.id® telah memulai langkah pertama dalam upaya ini, menjadi pelopor untuk menciptakan Indonesia yang lebih aman dan tangguh di dunia digital.

Jakarta, 1 Agustus 2024

Green
OPEN

RINGKASAN EKSEKUTIF

Di era internet, individu, organisasi, perusahaan dan institusi pemerintah sangat bergantung pada infrastruktur TI untuk menjaga mereka tetap aman dari serangan siber. Seiring dengan semakin banyaknya perusahaan yang mengadopsi transformasi digital, risiko kejahatan dunia maya meningkat dengan pesat, begitu pula pentingnya keamanan siber.

Suhu panas yang bergejolak belakangan ini pada lanskap keamanan siber nasional menjadi alarm peringatan yang harus menyadarkan kita semua betapa banyak lubang di sistem keamanan nasional. Lubang-lubang tersebut bisa berupa minimnya teknologi, penerapan teknologi yang tidak tepat guna sampai pada kesalahan manusia karena minim edukasi akan pengetahuan keamanan siber yang baik.

Keamanan siber telah menjadi tameng pertahanan utama bagi insan dunia maya. Keamanan siber yang kuat adalah kolaborasi antara kebijakan dan infrastruktur keamanan siber bersinergi untuk mengamankan sistem dan jaringan komputer dari serangan atau akses yang tidak sah. Oleh karena itu, dunia usaha, individu, dan pemerintah perlu melakukan investasi yang signifikan untuk mendapatkan manfaat keamanan siber dengan teknologi yang tepat guna, guna melindungi aset dan data mereka dari peretas.

Mendukung upaya tersebut di atas, AwanPintar.id® yang merupakan teknologi keamanan siber karya anak bangsa memiliki kepedulian menjaga keamanan siber nasional dan memposisikan dirinya untuk menjadi salah satu pilar penyangga keamanan siber Indonesia dengan terus mengawasi, memonitor, mendata dan menjaring setiap aktivitas siber yang masuk ke jaringan internet Indonesia.

Salah satu bentuk kepedulian direalisasikan dengan secara berkala tiap semester mempublikasikan Laporan Ancaman Digital dari AwanPintar.id®. Ini merupakan bentuk tanggung jawab terhadap publik siber nasional. Laporan sarat memuat informasi dan data semua ancaman siber yang masuk dalam jaringan internet nasional. Laporan ini juga dapat menjadi acuan bagi berbagai kalangan untuk melakukan tindakan preventif ke depan dan membangun sistem keamanan yang komprehensif yang mencakup manusia dan teknologi.

Pada semester satu tahun 2024 AwanPintar.id® melebarkan jangkauan analisa dengan bekerja sama dengan APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) yang secara khusus memantau pola serangan dari dalam Indonesia sendiri. Oleh karena itu, khusus pada laporan kali ini akan ditutup dengan analisa serangan yang berasal dari dalam negeri.

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. Dua perusahaan Prosperita Group yang memfokuskan bisnisnya di bidang teknologi, khususnya teknologi keamanan dunia digital adalah PT Prosperita Sistem Indonesia, telah melahirkan AwanPintar.id® dan beberapa solusi keamanan siber di bawahnya; 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 dan SpamCleaner.

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. 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 http://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 Semester Pertama 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 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 ASN (*Autonomous System 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*.

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 daerah dan negara didapat berdasarkan alamat IP yang terdeteksi.

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.

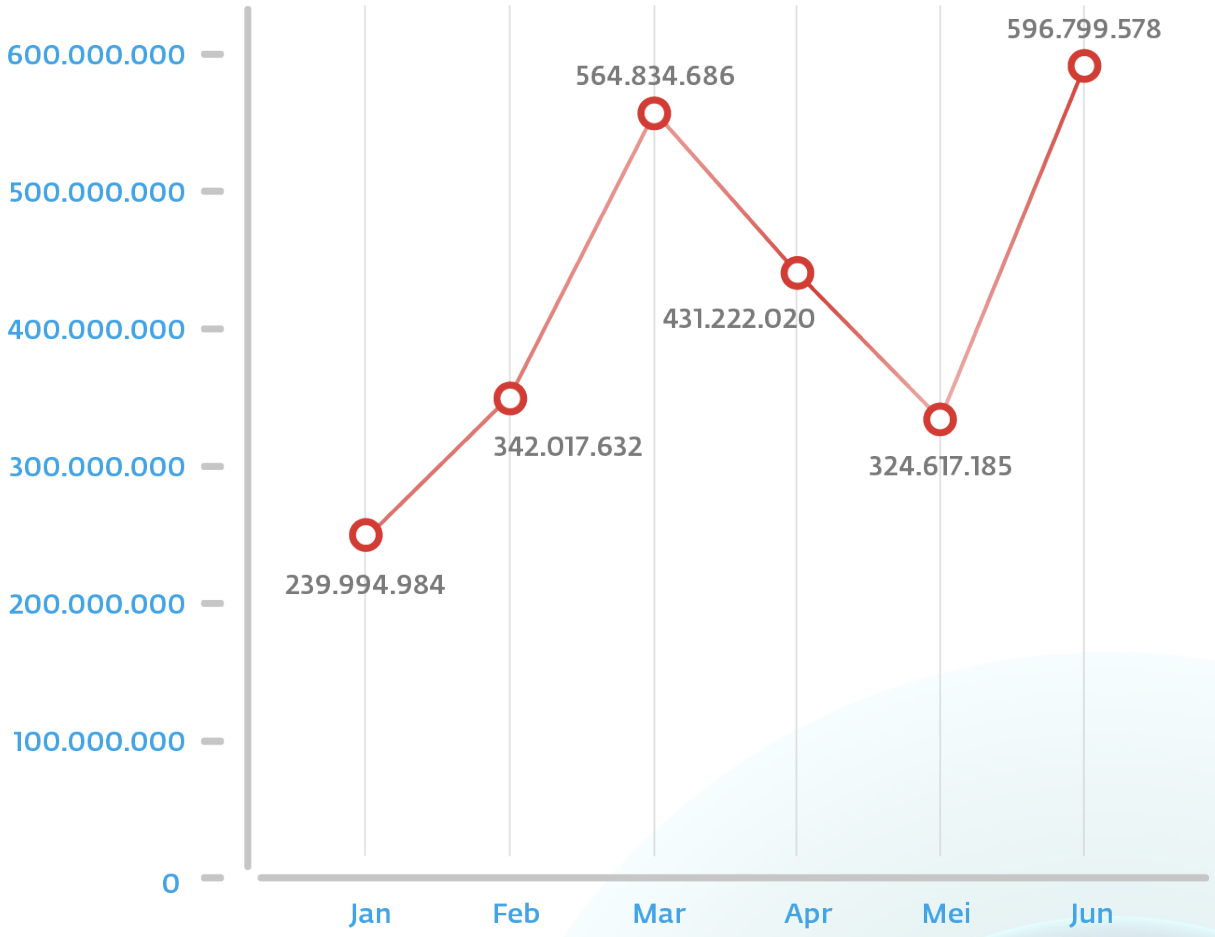
Untuk beberapa data, nilai persentase diambil berdasarkan urutan data dengan persentase total merupakan jumlah dari urutan yang diambil. Nilai di luar urutan tersebut dikesampingkan dengan asumsi kontribusi nilai dianggap tidak diperlukan.

TREN SERANGAN TERKINI

Akumulasi Serangan Siber di Indonesia

Data yang tersaji di bawah merupakan hasil akumulasi dari seluruh data dari detektor AwanPintar.id® yang diambil secara rata-rata pada setiap detektor pada Semester 1 tahun 2024.

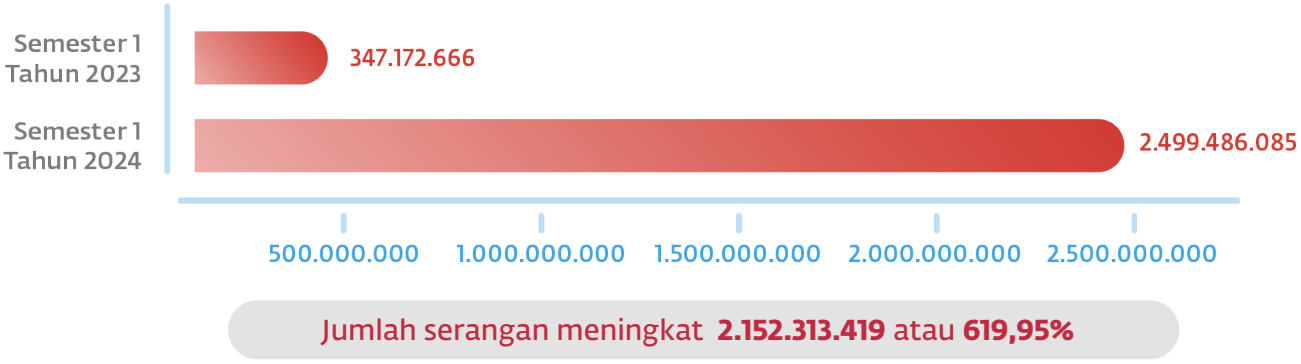
Rata-rata serangan per detik	Rata-rata serangan per menit	Rata-rata serangan per jam	Rata-rata serangan per hari
158	9.537	572.226	13.733.440



Jumlah total seluruh serangan **2.499.486.085**

Serangan pada tahun 2024 diprediksi akan mengalami kenaikan yang mencolok dibandingkan dengan tahun sebelumnya. Data pada paruh waktu pertama di tahun 2024 di atas memperlihatkan lonjakan serangan yang masuk ke infrastruktur AwanPintar.id® di jaringan nasional Indonesia. Dengan data mencatat sebesar 2.499.486.085 serangan atau lebih dari 6 kali lipat dari semester yang sama di tahun sebelumnya. Ini menjadi peringatan besar bagi seluruh pengguna internet di tanah air baik individu, organisasi, instansi maupun perusahaan bahwa Indonesia sedang dilanda gelombang serangan siber.

Sepanjang paruh pertama tahun 2024, tercatat beberapa agenda nasional seperti Pemilu Presiden pada bulan Februari serta insiden siber bulan Maret dan Juni perlu untuk kita lihat secara lebih mendalam, melihat besarnya serangan melebihi dari bulan-bulan sebelumnya. Besarnya serangan bulan Maret dikaitkan dengan bobolnya beberapa grup finance di saat itu, sementara PDNS merupakan isu utama di bulan Juni menjadi gambaran nyata dari serangan siber yang terjadi.

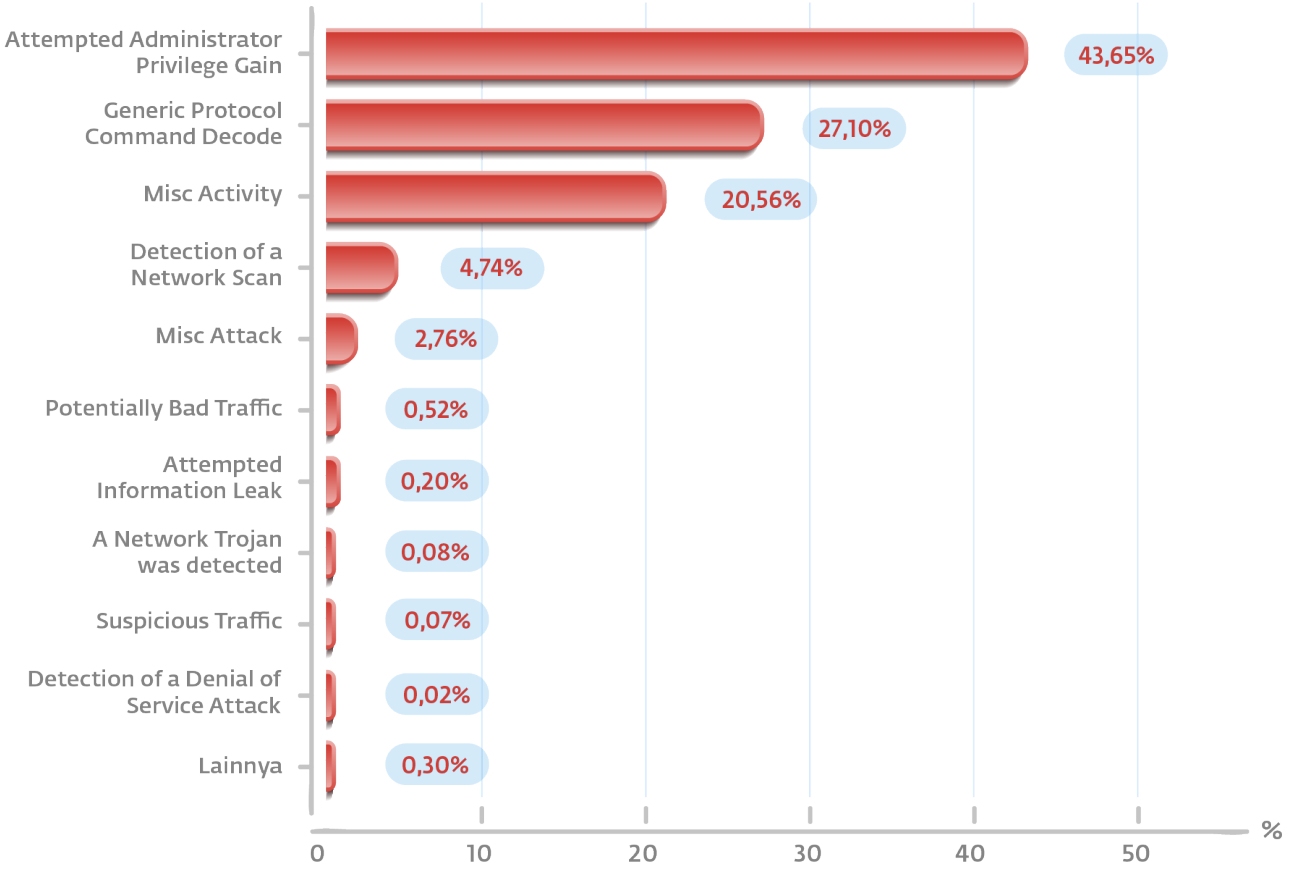


Jumlah serangan meningkat **2.152.313.419** atau **619,95%**

Jumlah serangan di Semester 1 tahun 2024 jauh lebih besar dari semester yang sama di tahun 2023, bahkan masih lebih besar dari total serangan di tahun 2023.

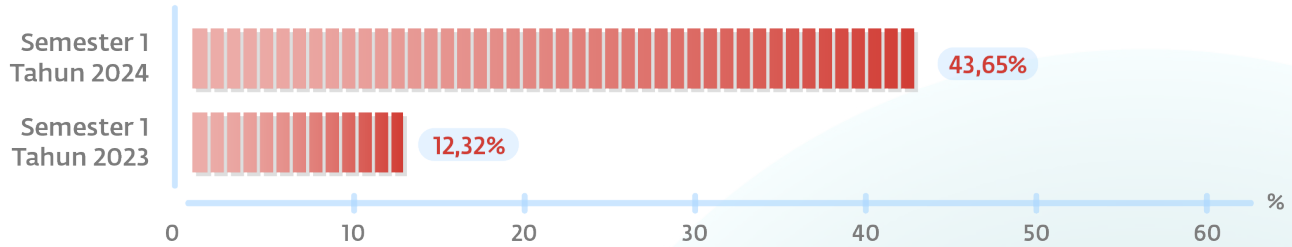
Data faktual di atas adalah bukti nyata bahwa serangan siber nasional sudah membutuhkan perhatian khusus. Meningkatnya ancaman yang sampai berkali lipat adalah sinyal adanya banyak celah keamanan yang terbuka di sistem keamanan nasional dan ini butuh kepedulian nasional terutama semua yang berkecimpung di dunia IT nasional untuk segera melakukan langkah-langkah inovatif, progresif dan preventif untuk melindungi kepentingan bangsa Indonesia demi terciptanya kedaulatan siber negara.

10 Jenis Serangan Siber Teratas



Attempted Administrator Privilege Gain

Deteksi upaya untuk mengakses sumber daya tingkat pengguna super atau hak akses administrator serta eksploitasi yang berupaya membahayakan host dan memberikan akses utama ke pelaku. Upaya akses ke bagian ADMIN$ pada sistem Windows adalah contoh yang baik dari upaya untuk mengakses.

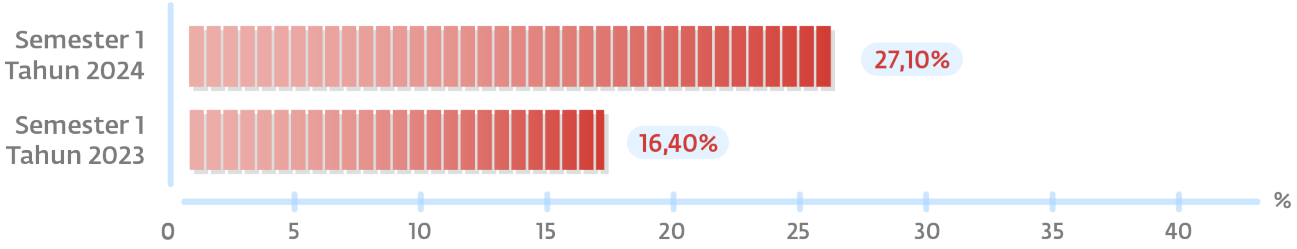


Mengalami peningkatan **31,33%**

Kategori serangan ini adalah upaya pencurian kredensial dengan berusaha mengakses hak akses administrator atau hak admin, mengalami peningkatan yang signifikan dibanding semester 1 di tahun sebelum yakni sebesar 31,33%. Serangan ini juga dapat menjadi cerminan berbagai insiden siber yang terjadi di Indonesia.

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.



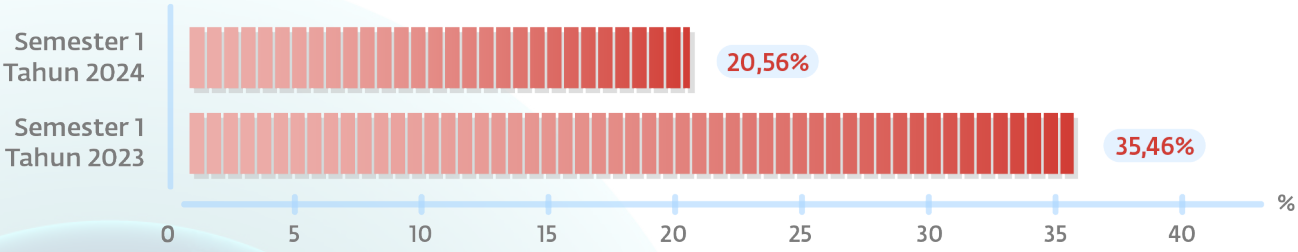
Mengalami peningkatan 10,70%

Peningkatan ancaman dari manipulasi juga pada titik yang meresahkan, jika dibandingkan tahun ini meningkat hingga 10,70% dari tahun lalu di semester yang sama.

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.

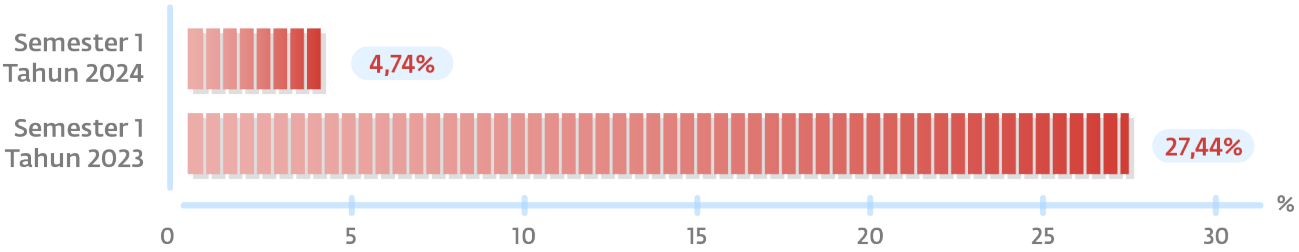


Mengalami penurunan -14,90%

Eskalasi aktivitas-aktivitas mencurigakan yang merupakan bagian dari tahapan-tahapan serangan siber mengalami penurunan sebesar 14,90% Situasi ini dapat dibaca penargetan sasaran lebih terfokus pada target-target tertentu atau *targeted attack*.

Detection of a Network Scan

Adanya aktivitas ilegal yang melibatkan pendeteksian semua host aktif di jaringan dan melakukan pemetaan 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.

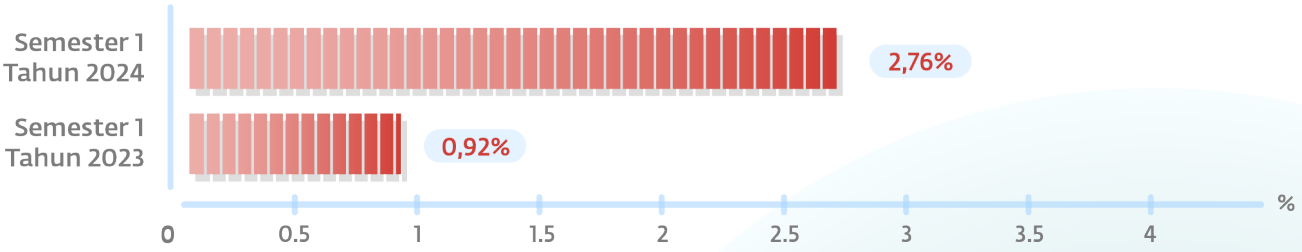


Mengalami penurunan -22,70%

Penurunan serangan pada kategori ini sebesar 22.70% yang merupakan masuk dalam serangan random yang menunjukkan bahwa para penjahat siber fokus pada sasaran tertentu ketimbang melakukan serangan secara acak.

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.

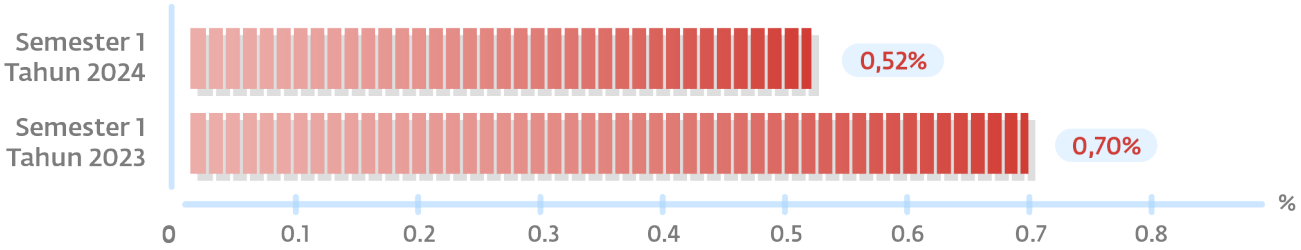


Mengalami peningkatan 1,84%

Upaya eksploitasi server web untuk mencuri kredensial pengguna meningkat sebesar 1,84%. Artinya lebih banyak pengguna internet di Indonesia menjadi korban pencurian kredensial melalui server web dan browser dibanding tahun lalu.

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 organisasi, pelaku dapat melakukan manipulasi dan eksploitasi tanpa batas.

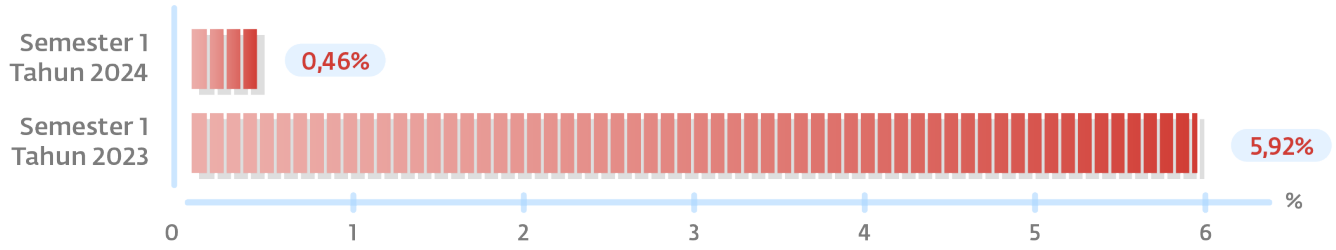


Mengalami penurunan -0,18%

Tidak ada hal yang mengejutkan dari arus lalu lintas mencurigakan, meskipun mengalami penurunan, penurunannya hanya 0,18%.

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.

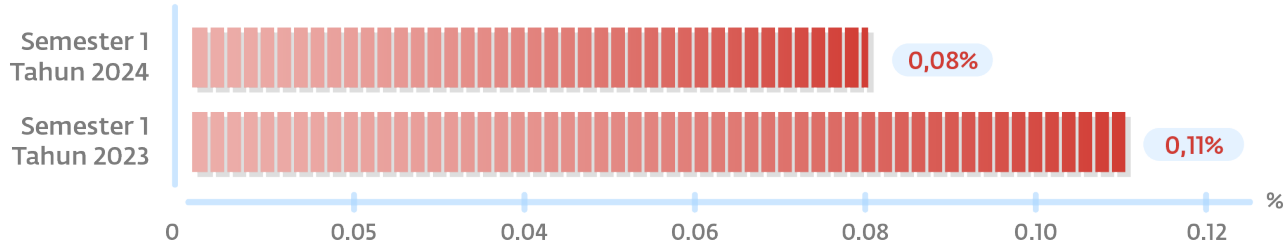


Mengalami penurunan -5,46%

Ini menjadi kabar baik bagi semua kalangan pengguna internet di tanah air karena pencurian informasi sensitif berkurang drastis sebesar 5,46%. Menandakan mulai terbangunnya kesadaran keamanan di kalangan pengguna dalam memproteksi dirinya dengan melakukan langkah-langkah keamanan siber mandiri.

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 phising, drive by download, dan unduhan perangkat lunak dari sumber yang tidak terpercaya.

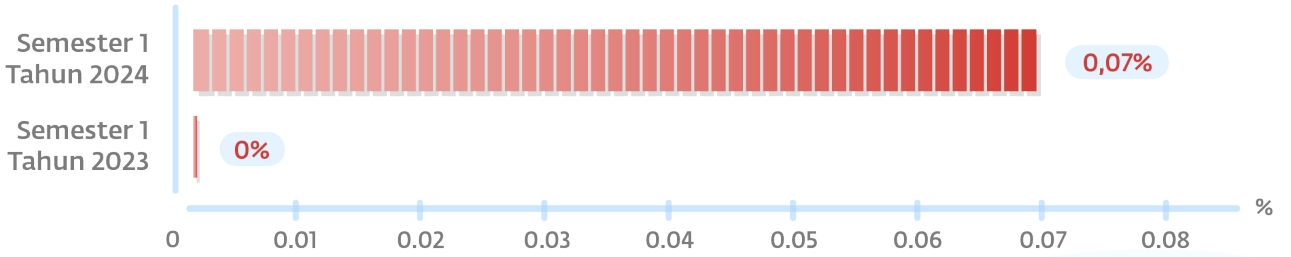


Mengalami penurunan -**0,03%**

Situasi pada serangan trojan menurun sebesar 0,03% dimana ancaman ini tidak terlalu menunjukkan peningkatan ancaman signifikan di dunia maya.

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.

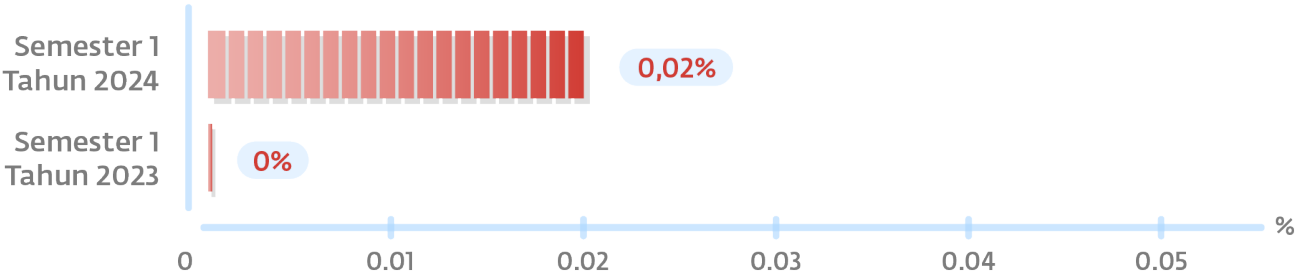


Kategori jenis serangan baru **0,07%**

Anomali pada lalu lintas pada infrastruktur jaringan nasional memiliki potensi berbahaya jika tidak dimonitor dengan baik. Walaupun jumlahnya tidak besar yakni 0,07%, namun dalam dunia siber hal sekecil apa pun tidak boleh diremehkan.

Detection of a Denial of Service

Serangan dunia maya di mana pelaku jahat bertujuan untuk menonaktifkan atau mengganggu aksesibilitas sistem atau jaringan dengan mengirimkan sejumlah besar permintaan atau lalu lintas data yang berlebihan untuk membuat sistem atau jaringan tidak responsif atau crash seperti DOS, SYN Flood atau Ping Flood. Seiring dengan waktu, serangan model ini sudah berkembang menjadi Ransom DDoS (RDDoS).



Kategori jenis serangan baru **0,02%**

Serangan dengan membanjiri sistem atau jaringan dengan lalu lintas data yang berlebihan merupakan kategori ancaman baru di Semester 1 tahun 2024.

10 Negara Kontributor Serangan Siber

Dalam era digitalisasi, dunia terhubung satu sama lain tanpa batas dan tanpa sekat. Segalanya jadi mudah dilakukan tapi ibarat dua sisi mata koin, internet yang membawa manfaat besar bagi umat manusia memiliki sisi gelap yang menyertainya.

Ancaman siber menjadi lebih berbahaya karena mereka bisa dilakukan dari berbagai tempat di dunia, tak ada tempat yang benar-benar aman dari ancaman siber. Banyak kejahatan siber di dunia disponsori oleh negara, perang digitalisasi ini meluas dan tak mengenal batas.

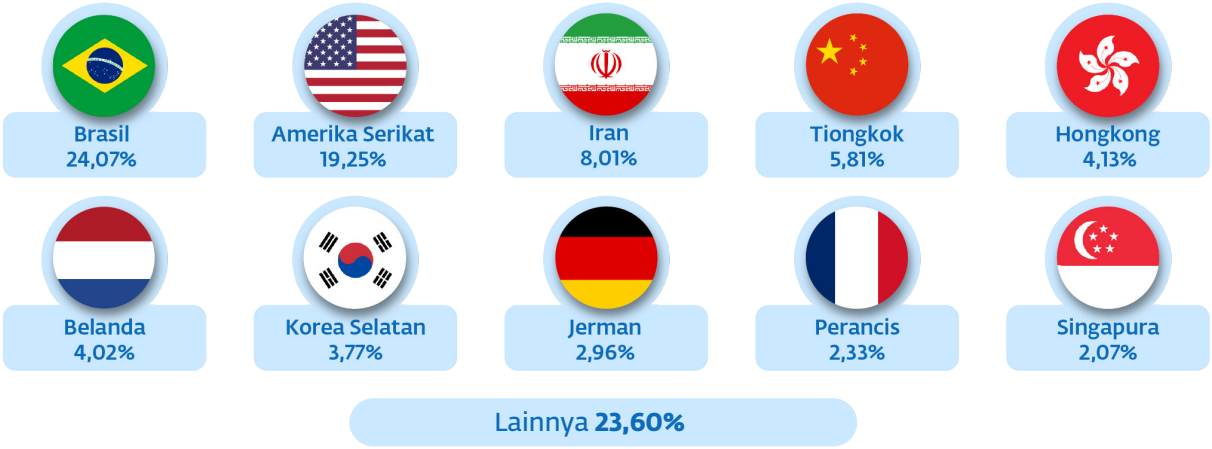
AwanPintar.id® yang memiliki detektor yang menyebar di seluruh infrastruktur jaringan nasional mendeteksi berbagai ancaman siber yang masuk dan menyerang Indonesia, di bawah ini adalah data-data serangan siber dari berbagai negara yang berhasil dijaring.

Semester 1 Tahun 2024

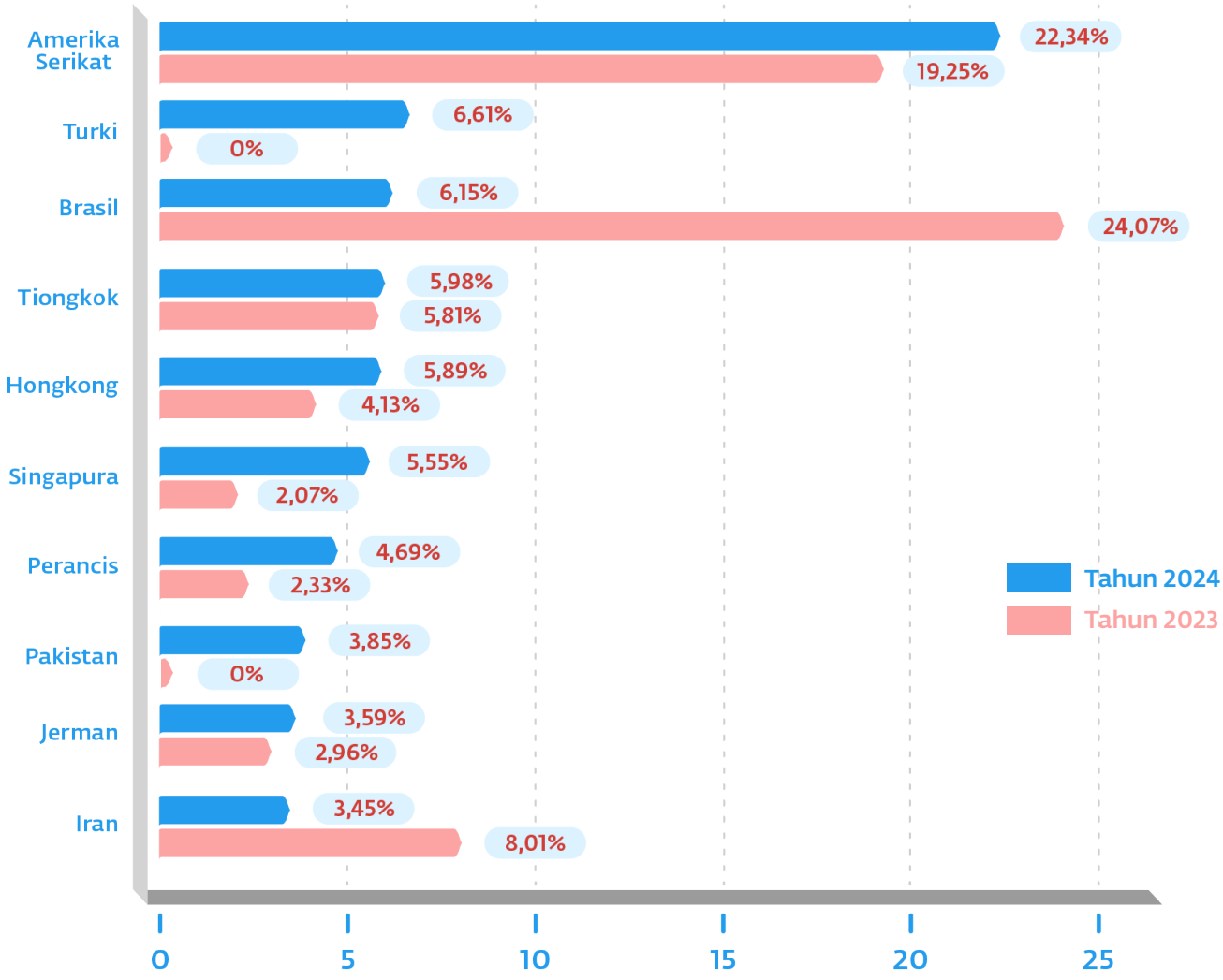
Amerika Serikat 22,34%	Turki 6,61%	Brasil 6,15%	Tiongkok 5,98%	Hongkong 5,89%
Singapura 5,55%	Perancis 4,69%	Pakistan 3,85%	Jerman 3,59%	Iran 3,45%

Lainnya **31,90%**

Semester 1 Tahun 2023



Komparasi Semester 1 Tahun 2023 dan Semester 1 Tahun 2024



Amerika Serikat
Mengalami peningkatan serangan **3,09%**

Belanda diganti Turki
Pendatang baru dalam daftar 10 negara kontributor **(6,61%)**

Brasil
Mengalami penurunan serangan **-17,92%**

Tiongkok
Mengalami peningkatan serangan **0,17%**

Hongkong
Mengalami peningkatan serangan **1,76%**

Singapura
Mengalami peningkatan serangan **3,48%**

Perancis
Mengalami peningkatan serangan **2,36%**

Korea Selatan diganti Pakistan
Pendatang baru dalam daftar 10 negara kontributor **(3,85%)**

Jerman
Mengalami peningkatan serangan **0,63%**

Iran
Mengalami penurunan serangan **-4,56%**

Bila kita lihat data yang diakumulasi oleh AwanPintar.id® bisa kita simpulkan bahwa mayoritas negara kontributor serangan dari semester yang sama di tahun lalu sebagian besar masih sama.

Dan yang mengkhawatirkan adalah secara umum telah terjadi eskalasi serangan dari sebagian besar negara kontributor yang konsisten melakukan serangan siber di Indonesia. Sementara dua negara yakni Brasil dan Iran mengalami penurunan serangan yang cukup drastis.

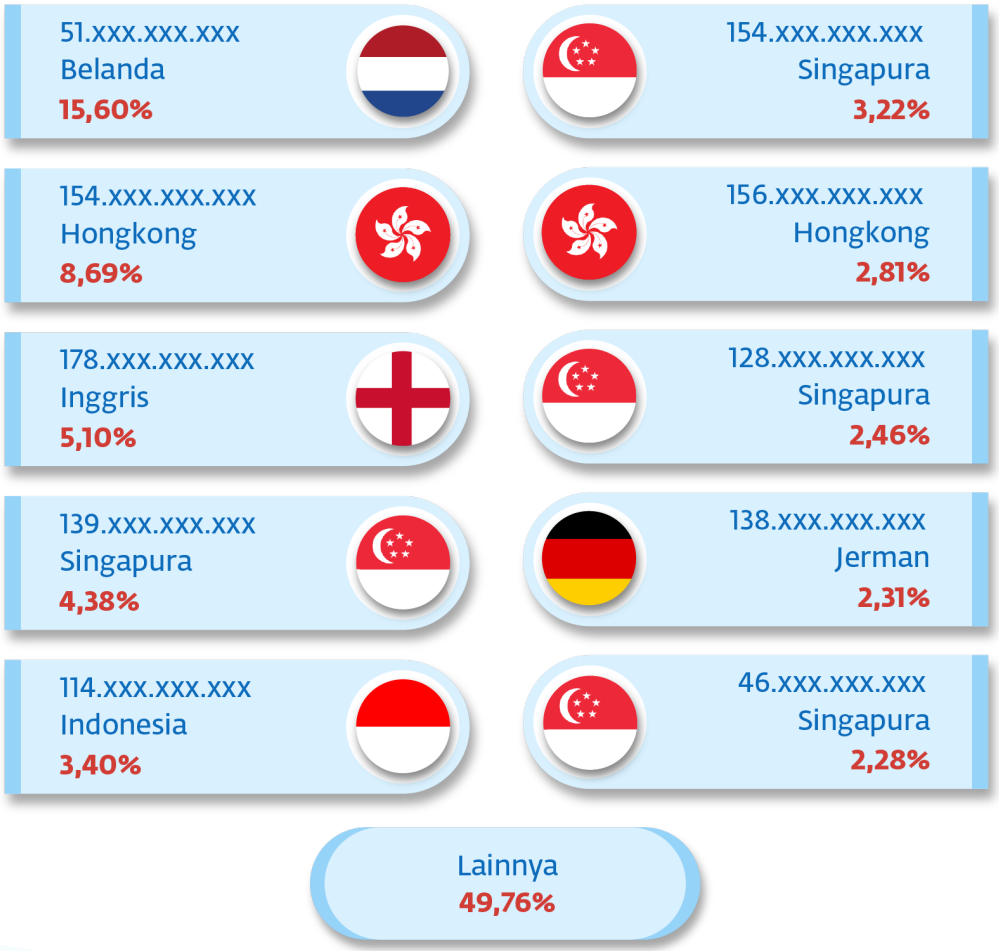
Di sisi lain ada dua negara pendatang baru sebagai kontributor serangan siber yaitu Turki dan Pakistan menggeser Belanda dan Korea Selatan dari 10 besar. Selain itu, Turki maupun Pakistan memberikan kontribusi serangan yang jauh lebih besar dari pendahulunya yang tentu saja dapat memberi imbas buruk pada Indonesia.

Indonesia sendiri menempati posisi 11, posisi yang sama dengan semester 1 pada tahun 2023. Dengan serangan sebesar 3,19% yang mengalami kenaikan 1,13% dibandingkan semester 1 tahun 2023.

10 IP Penyerang Teratas

Penjahat dunia maya menjadi ancaman besar bagi pengguna internet di seluruh dunia. Banyak dari penjahat ini sangat berani karena mereka percaya bahwa mereka dapat bersembunyi di balik anonimitas di Internet.

Namun, aksi mereka bukan tanpa jejak, dalam dunia digital tidak mudah menghapus jejak digital, salah satunya dapat dilacak melalui IP Address yang mereka gunakan. Berikut adalah jejak data yang berhasil dilacak oleh AwanPintar.id® di infrastruktur jaringan di Indonesia.



Yang menjadi sorotan utama dari 10 IP penyerang teratas yakni pengguna IP Singapura mendominasi serangan, meskipun jika ditotal masih di bawah pengguna IP dari Belanda, tapi yang perlu dicermati adalah bahwa Singapura di tahun lalu tidak pernah masuk dalam 10 besar sama sekali.

Sedangkan pengguna IP Address asal Amerika Serikat yang semester pertama tahun lalu begitu dominan di tahun lalu menghilang dari peredaran, di dalam 10 besar pengguna IP Amerika Serikat mengalami penurunan sangat drastis. Meski demikian bisa jadi serangan mereka diubah dengan memanfaatkan IP dari negara lain yang mereka bajak dan difungsikan sebagai BOT.

Ancaman Pencurian Kredensial

Dalam lanskap digital saat ini, keamanan kredensial online telah menjadi perhatian utama karena penjahat dunia maya terus-menerus menemukan cara baru untuk membobol sistem dan mendapatkan akses tidak sah ke data sensitif.

Kredensial curian adalah komoditas utama di DarkWeb yang sering kali menyebabkan serangan ransomware, salah satu bentuk kejahatan dunia maya yang paling luas dan merusak.

Penting bagi individu dan bisnis untuk memprioritaskan keamanan akun dan melindungi kredensial online mereka yang berharga. Berikut ini AwanPintar.id® akan memaparkan upaya pencurian kredensial yang terjadi di seluruh Indonesia.

1. Administrator Privilege Gain

- Backdoor DoublePulsar **78,10%**
- Eksploitasi Kerentanan (CVE-2020-11899) **21,61%**
- Lainnya **0.29%**

Backdoor DoublePulsar

(Backdoor DoublePulsar Installing Communication) DoublePulsar adalah backdoor implan yang memungkinkan iInjeksi 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.

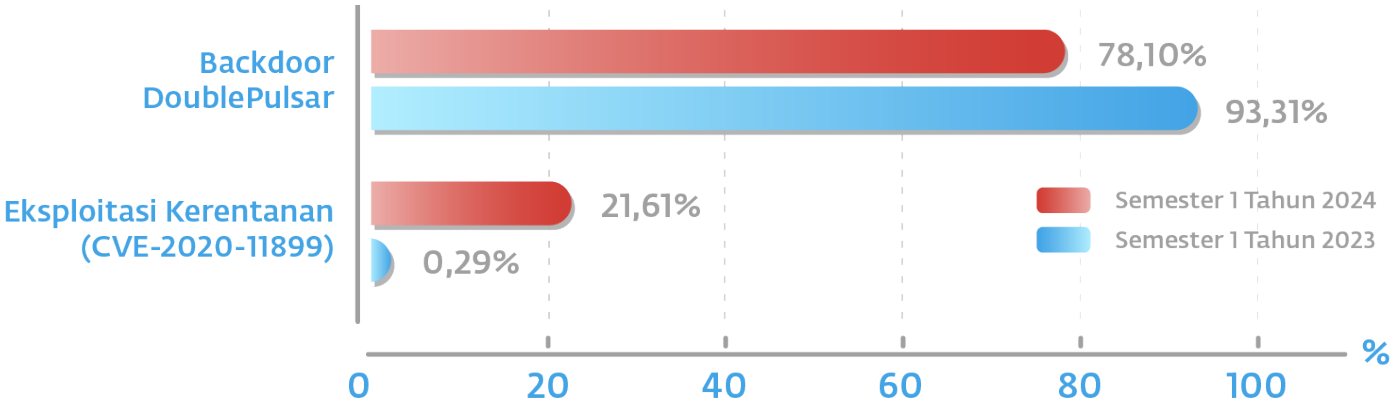
Untuk memahami Backdoor DoublePulsar kita harus tahu bahwa semua berpusat pada protokol SMB dan itu bergantung pada port 445 untuk mengaktifkan jaringan dan di sini letak kelemahannya. Dapat dikatakan, Backdoor DoublePulsar merupakan jalan masuk bagi malware lainnya.

Eksploitasi Kerentanan (EXPLOIT Possible CVE-2020-11899 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.

Komparasi Administration Privilege Gain Semester 1 Tahun 2023 & Semester 1 Tahun 2024



Backdoor DoublePulsar
Mengalami penurunan **-15,21%**

Eksploitasi Kerentanan (CVE-2020-11899)
Mengalami peningkatan **21,32%**

Serangan pencurian kredensial kali ini terlihat lebih terkonsentrasi, dilihat dari besarnya serangan difokuskan pada dua celah yang menjadi masalah umum di dalam sistem keamanan dalam jaringan internet lokal.

Ada penurunan yang relatif tidak terlalu besar, tapi di sisi lain terjadi lonjakan eksploitasi kerentanan yang sangat signifikan dan masif pada pencurian data atau kredensial penting.

2. Information Leak

- ET SCAN NMAP -sS window 1024 **43,99%**
- ET SCAN Potential VNC Scan5900-5920 **16,70%**
- ET SCAN Potential SSH Scan **15,34%**
- ET SCAN MS Terminal Server Traffic on Non-standard Port **6,61%**
- ET FTP FTP PWD command attempt without login **2,42%**
- ET FTP FTP CWD command attempt without login **2,27%**
- Lainnya **12,67%**

SCAN NMAP (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.

Eksploitasi VNC (SCAN Potential VNC Scan 5900-5920)

Virtual Network Computing (VNC) adalah sistem kendali desktop jarak jauh yang tidak bergantung pada platform. Ada banyak implementasi VNC (LibVNC, TightVNC, UltraVNC, dll.) yang berjalan di Windows, Linux, macOS, iOS, Android, dan sistem operasi lainnya. VNC menggunakan port 5900 atau 5800. VNC digunakan untuk skenario bekerja dari rumah dan untuk pemecahan masalah dan pemeliharaan jarak jauh oleh profesional TI.

VNC memiliki beberapa kerentanan yang terekspos, dimana kerentanan tersebut mempengaruhi empat produk VNC. Sebagian besar dari ini memungkinkan penyerang untuk mengeksekusi kode pada komputer jarak jauh.

Brute Force SSH (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.

RDP Brute Force (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.

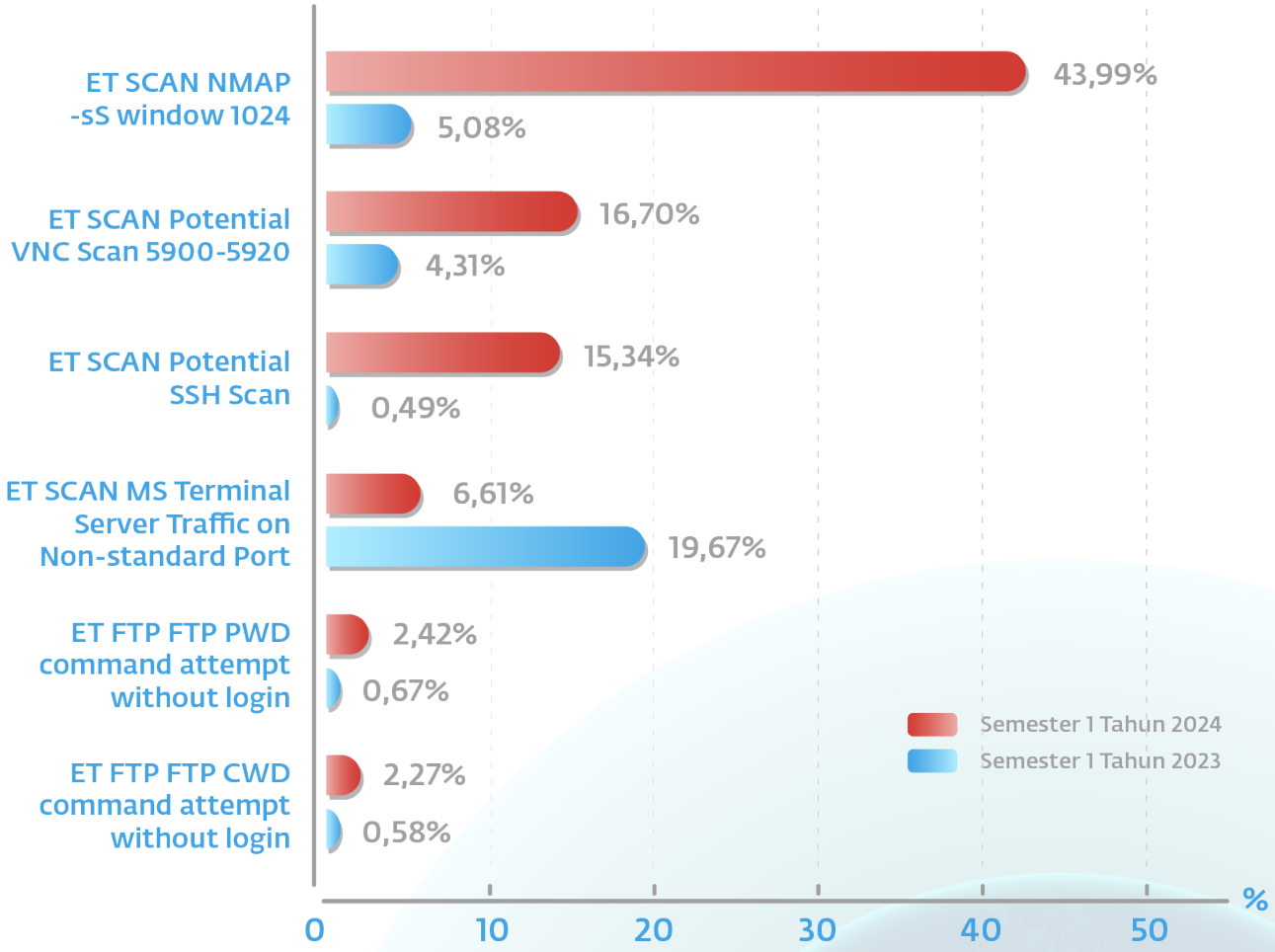
ET FTP FTP PWD command attempt without login

Perintah ini menampilkan direktori kerja saat ini di server untuk pengguna yang login. FTP tidak dibangun untuk keamanan. Ini umumnya dianggap sebagai protokol yang tidak aman karena bergantung pada nama pengguna dan kata sandi teks-jelas untuk otentikasi dan tidak menggunakan enkripsi.

ET FTP FTP CWD command attempt without login

Perintah CWD dikeluarkan untuk mengubah direktori kerja klien saat ini ke jalur yang ditentukan dengan perintah tersebut. FTP Voyager dan klien FTP berbasis GUI lainnya akan secara otomatis mengeluarkan perintah ini saat pengguna menelusuri sistem file jarak jauh dari dalam program. Data yang dikirim melalui FTP rentan terhadap serangan sniffing, spoofing, dan brute force, di antara metode serangan dasar lainnya.

Komparasi Information Leak Semester 1 Tahun 2023 & Semester 1 Tahun 2024



Green
OPEN

ET SCAN NMAP -sS window 1024
Mengalami peningkatan **38,91%**

ET SCAN Potential VNC Scan 5900-5920
Mengalami peningkatan **12,39%**

ET SCAN Potential SSH Scan
Mengalami peningkatan **14,85%**

ET SCAN MS Terminal Server Traffic on Non-standard Port
Mengalami penurunan **-13,06%**

ET FTP FTP PWD command attempt without login
Mengalami peningkatan **1,75%**

ET FTP FTP CWD command attempt without login
Mengalami peningkatan **1,69%**

SPAM & MALWARE

Sebagai pengguna internet, kita terus-menerus dihadapkan pada berbagai ancaman online yang membahayakan privasi dan keamanan kita. Dua bahaya umum yang sering merusak pengalaman online kita adalah spam dan malware.

Spam

Spam mengacu pada pesan yang tidak diminta dan tidak relevan yang dikirim ke sejumlah besar penerima melalui email, pesan instan, atau saluran komunikasi lainnya. Tujuan utama spam adalah untuk mengiklankan produk, layanan, atau konten, dan sering kali spam berasal dari entitas komersial yang mencoba mempromosikan penawaran mereka. Meskipun spam dapat mengganggu tujuan utamanya adalah menghasilkan pendapatan melalui cara yang sah atau terkadang meragukan, seperti penipuan phishing.

Spam umumnya didistribusikan melalui kampanye email massal, 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 perangkat lunak berbahaya yang dirancang untuk mengeksploitasi, merusak, atau mendapatkan akses tidak sah ke sistem komputer. Bentuknya bisa bermacam-macam, termasuk virus, worm, trojan, ransomware, dan spyware. Tujuan utama malware adalah untuk membahayakan keamanan sistem atau mencuri informasi sensitif, yang sering kali mengakibatkan kerugian finansial, pelanggaran data, atau akses tidak sah ke data pribadi atau perusahaan.

Malware dapat didistribusikan melalui berbagai vektor, termasuk lampiran email, tautan berbahaya, situs web yang terinfeksi, unduhan perangkat lunak, media yang dapat dipindahkan, dan jaringan yang disusupi. Penjahat dunia maya sering kali menggunakan teknik rekayasa sosial untuk memancing pengguna agar mengunduh atau mengeksekusi malware tanpa disadari.

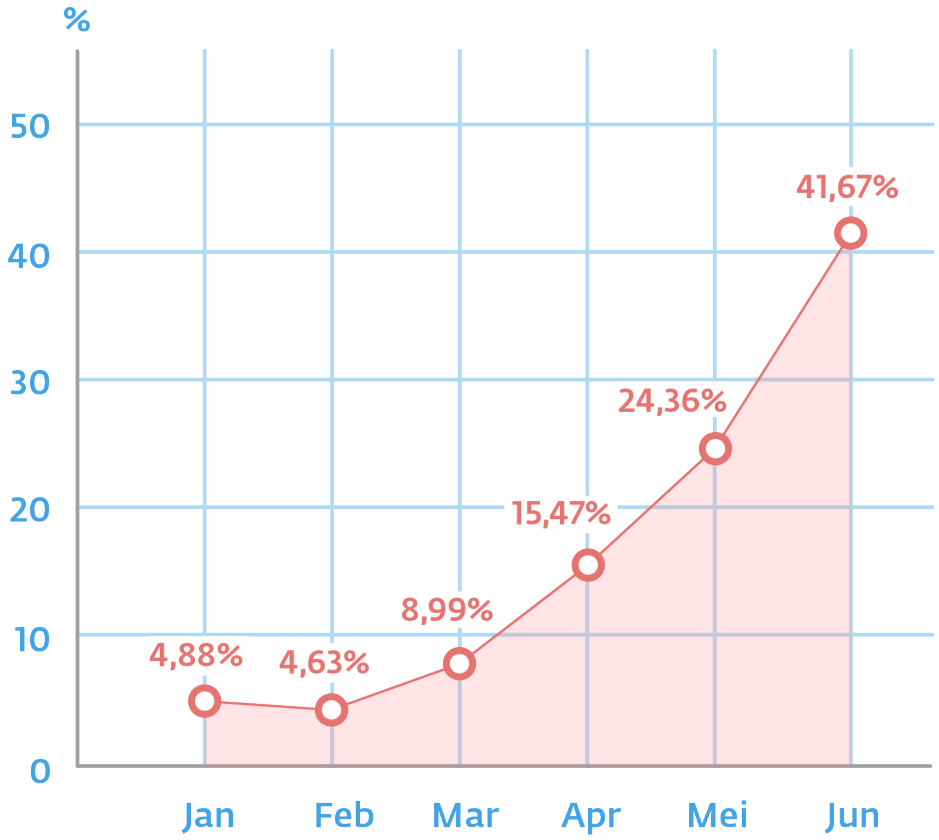
Dalam konteks dunia siber spam dan malware merupakan dua entitas yang dapat bersinergi satu sama lain menjadi ancaman yang sangat berbahaya yang mampu mencakup sasaran dalam jumlah besar dan luas.

Bicara cakupan ancaman dari spam dan malware berikut adalah data yang diperoleh dari AwanPintar.id® di Semester 1 Tahun 2024 mengenai sebaran ancaman spam dan malware yang masuk ke Indonesia:

Persentase Jumlah Spam & Malware Terhadap Total Email Masuk

Data berikut adalah persentase dari jumlah spam dan malware yang masuk terhadap total email masuk, data berikut diakumulasi oleh AwanPintar.id®.

Jumlah Spam yang Masuk Semester 1 Tahun 2024



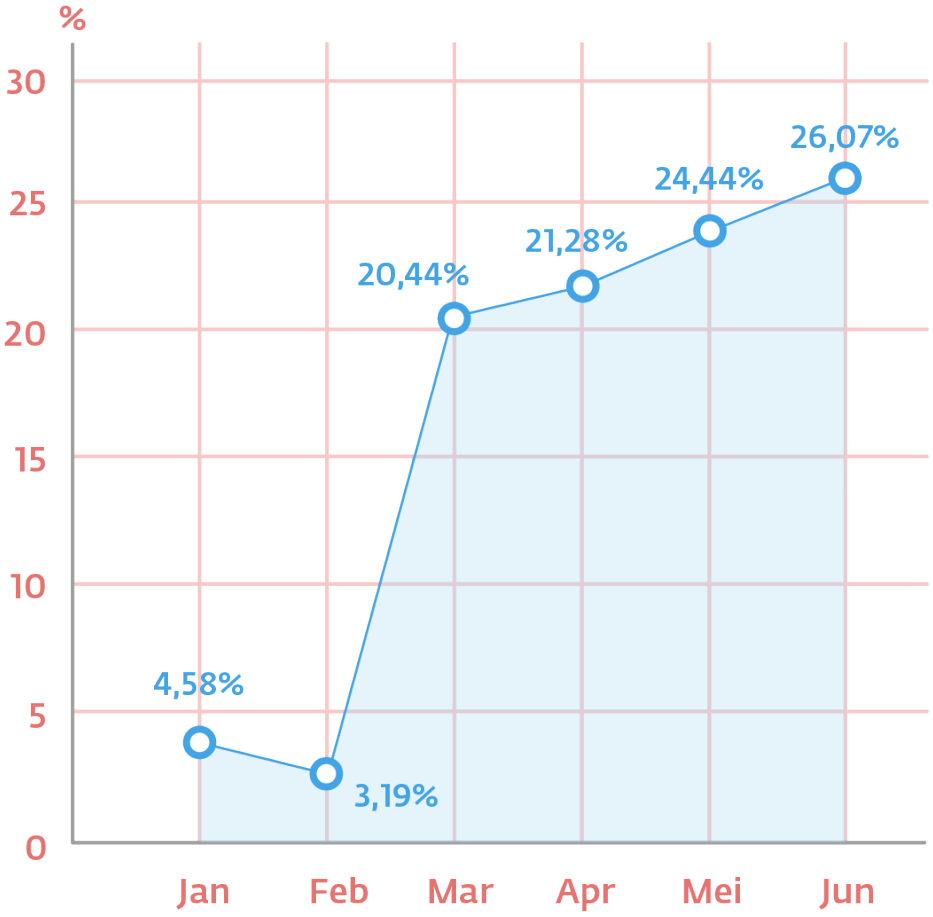
Sepertinya sudah membentuk sebagai sebuah tren jika serangan spam email di bulan-bulan awal tahun selalu rendah. Namun, seiring perjalanan waktu serangan tersebut mengalami peningkatan berkali lipat hingga pertengahan tahun.

Bulan Maret merupakan awal eskalasi serangan yang mencapai dua kali lipat dari bulan-bulan sebelumnya. Di bulan yang sama terjadi peretasan terhadap beberapa grup finance.

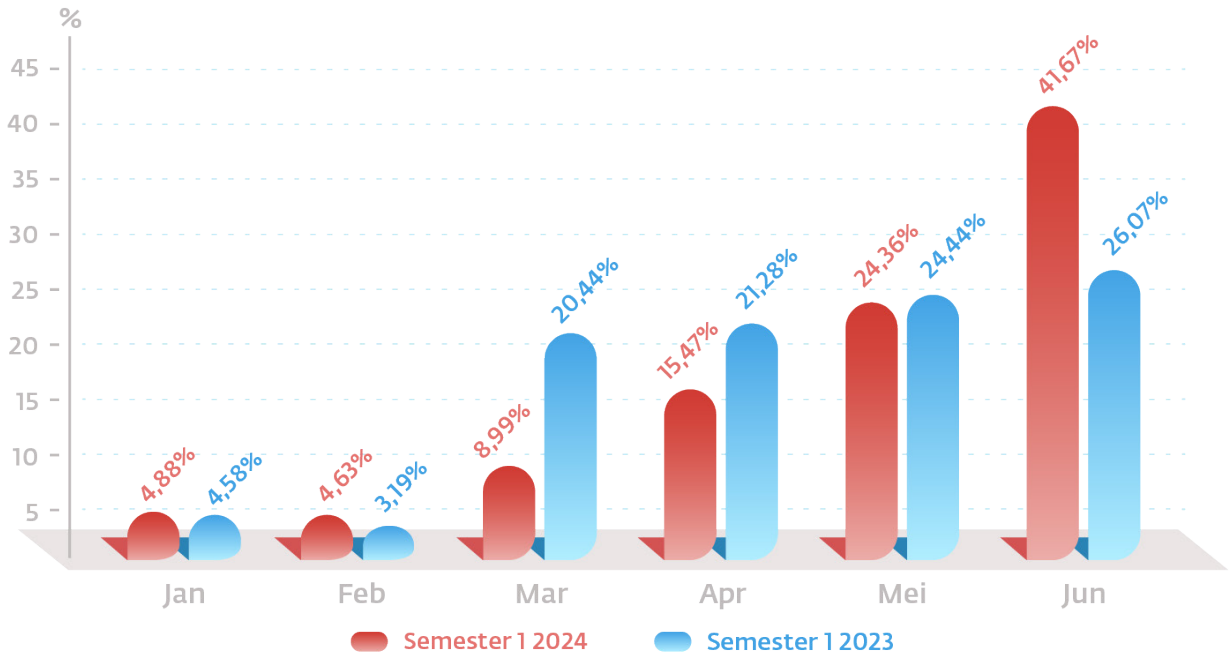
Dan serangan-serangan tersebut terus menjadi masif dan meluas di dua bulan terakhir di semester pertama tahun 2024. Mei dan Juni menjadi bulan dengan serangan spam dan malware terparah. Sementara di saat yang sama institusi-institusi pemerintah menghadapi masalah siber berat.

Semester 1 tahun 2024 berisi kabar buruk tentang berbagai peretasan di dalam negeri, baik swasta maupun pemerintah menghadapi kesulitan serupa dalam mengatasi serangan siber yang datang bergelombang.

Jumlah Spam yang Masuk Semester 1 Tahun 2023



Komparasi Jumlah Spam Semester 1 Tahun 2023 & Semester 1 Tahun 2024



Januari
Jumlah spam meningkat **0,30%**

Februari
Jumlah spam meningkat **1,44%**

Maret
Jumlah spam menurun **-11,45%**

April
Jumlah spam menurun **-5,81%**

Mei
Jumlah spam menurun **-0,08%**

Juni
Jumlah spam meningkat **15,60%**

Aliran jumlah serangan spam yang masuk pada dasarnya mengalami peningkatan di Semester 1 tahun 2024 jika dibandingkan dengan semester yang sama di tahun sebelumnya. Secara umum jumlah serangan terus meningkat setiap bulannya, walaupun di akhir semester ada sedikit penurunan namun tidak signifikan.

Dari data AwanPintar.id® tersebut kita bisa melihat bahwa serangan spam setiap tahunnya cenderung meningkat dan selalu konsisten dalam jumlah serangan setiap bulannya seperti tahun sebelumnya.

5 Negara Pengirim Spam & Malware Terbanyak pada Semester 1 2024

Amerika Serikat **23,87%**
Spanyol **20,20%**
Tiongkok **11,29%**
Indonesia **7,30%**
Brasil **2,83%**

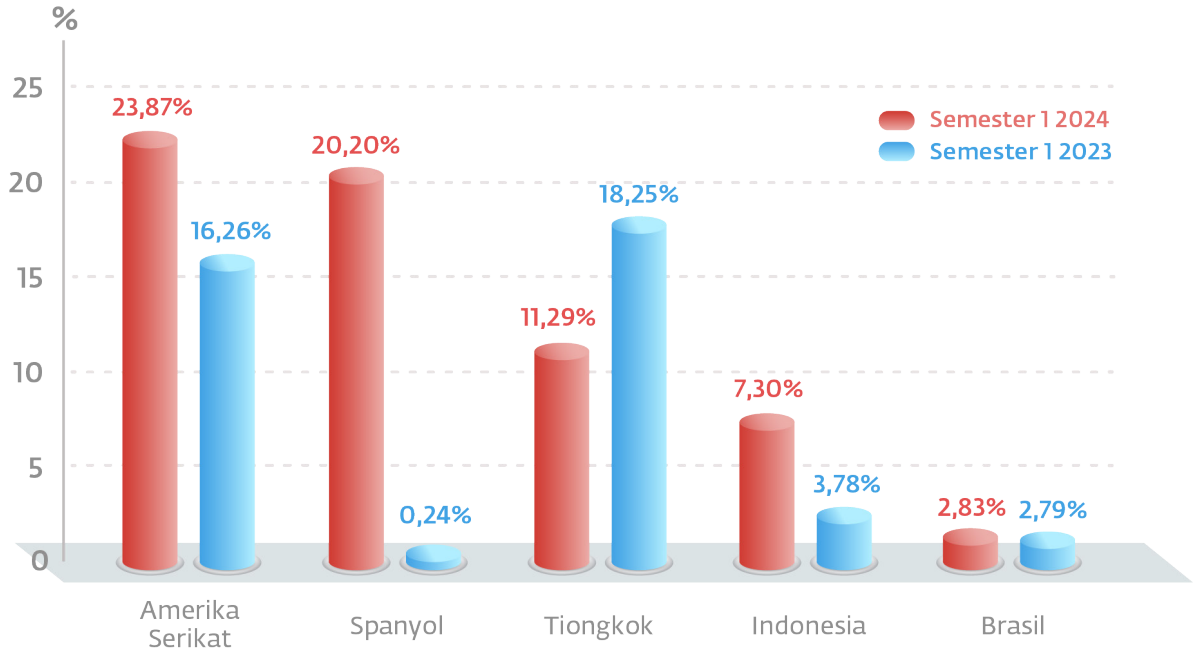
Lainnya **34,50%**

5 Negara Pengirim Spam & Malware Terbanyak 2023

Tiongkok **18,25%**
Amerika Serikat **16,26%**
Jerman **7,66%**
India **6,84%**
Makedonia Utara **6,77%**

Lainnya **44,21%**

Komparasi Semester 1 Tahun 2023 & Semester 1 Tahun 2024



Amerika Serikat
Mengalami peningkatan serangan **7,61%**

Spanyol
Negara baru di 5 besar

Tiongkok
Mengalami penurunan serangan **-6,96%**

Indonesia
Negara baru di 5 besar

Brasil
Negara baru di 5 besar

Amerika Serikat selalu konsisten dari tahun ke tahun masuk dalam 5 besar negara yang paling sering dan banyak mengirimkan serangan spam dan malware ke Indonesia.

Sementara Tiongkok yang tahun sebelumnya berada di posisi pertama bergeser menjadi posisi ketiga. Kemudian Makedonia Utara, India dan Jerman bergeser dari posisinya masing-masing digantikan oleh negara-negara baru pengirim spam terbanyak.

Dari semua negara pengirim malware, sebagian besar merupakan negara pengirim malware baru. Negara-negara yang mengirim malware ini terlihat lebih dinamis dengan banyaknya negara baru yang mendominasi.

Yang cukup mengejutkan, Indonesia berada di posisi ke empat dengan persentase yang mengalami kenaikan hampir 100% dibandingkan semester yang sama pada tahun sebelumnya yang hanya menempati posisi 8 dengan nilai 3.78%.

PORT FAVORIT PERETAS

10 Port Paling Rentan di Indonesia

Port adalah suatu titik pada komputer tempat berlangsungnya pertukaran informasi antara beberapa program dan internet ke perangkat atau komputer lain. Untuk memastikan konsistensi dan menyederhanakan proses pemrograman, port diberi nomor port. Ini, bersama dengan alamat IP, membentuk informasi penting yang digunakan setiap penyedia layanan internet (ISP) untuk memenuhi permintaan.

Nomor port berkisar dari 0 hingga 65.535 dan diberi peringkat berdasarkan popularitas. Port bernomor 0 hingga 1.023 disebut port "terkenal", yang biasanya disediakan untuk penggunaan internet tetapi juga dapat memiliki tujuan khusus. Port ini, yang ditetapkan oleh Internet Assigned Numbers Authority (IANA), dipegang oleh bisnis terkemuka dan Layanan Bahasa Kueri Terstruktur (SQL).

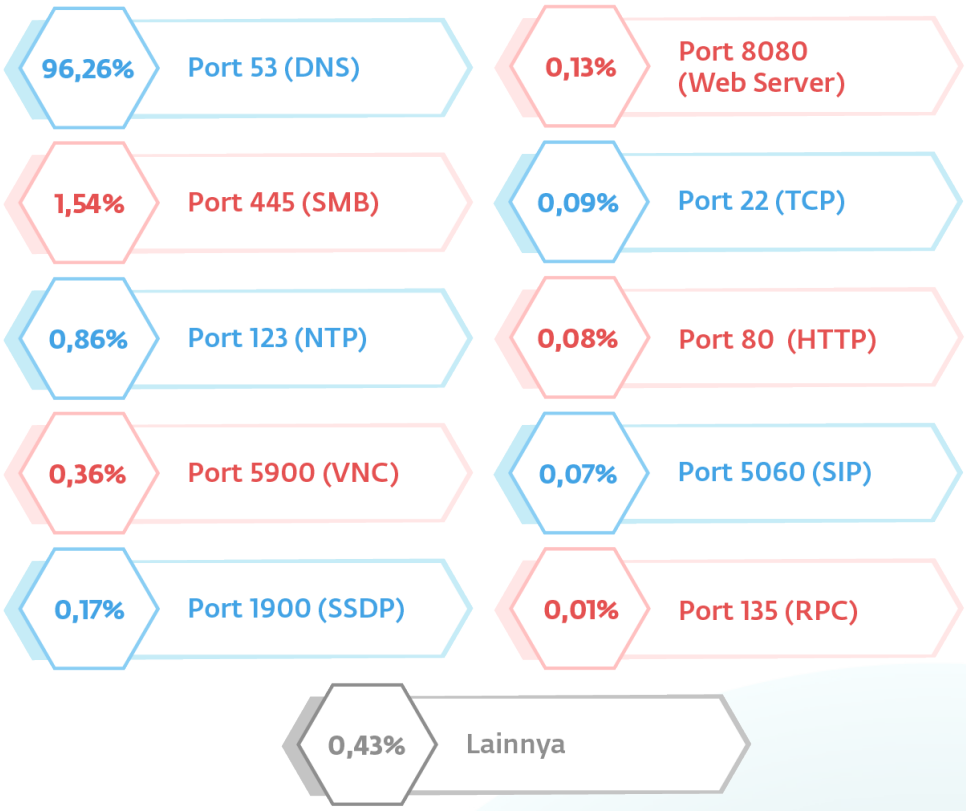
Port dengan nomor 1.024 hingga 49.151 dianggap sebagai "port terdaftar" dan didaftarkan oleh perusahaan perangkat lunak. Port bernomor 49.152 hingga 65.535 dianggap port dinamis dan pribadi, yang dapat digunakan oleh hampir semua orang di internet.

Persentase Port Paling Rentan

Port terbuka pada komputer berisiko karena dapat diserang oleh peretas untuk mengeksploitasi data. Sebagian besar port terbuka membantu untuk terhubung dengan Internet. Data mungkin bocor dan disalahgunakan melalui port terbuka. Melakukan pemeriksaan keamanan itu penting.

Para peretas memiliki akses ke port FTP dan UDP. Mereka mungkin menginstal file dan program berbahaya ke dalam komputer yang dapat menyebabkan perkembangan virus ataupun malware. Yang juga dapat menyebabkan data menjadi rusak dan disalahgunakan

Ancaman melalui port komputer sering terjadi di Indonesia bahkan dibandingkan dengan tahun sebelumnya di semester yang sama. Dari data yang berhasil dihimpun oleh AwanPintar.id® diketahui fakta-fakta berikut:



Komparasi Port Paling Rentan Semester 1 Tahun 2023 & Tahun 2024

Nama Port	S1 Tahun 2024	S1 Tahun 2023	Keterangan
Port 53 (DNS)	96,26%	81,08%	Mengalami peningkatan 15,18%
Port 445 (SMB)	1,54%	5,36%	Mengalami penurunan -3,82 %
Port 123 (NTP)	0,86%	0%	Port paling rentan terbaru
Port 5900 (VNC)	0,36%	2,27%	Mengalami penurunan -1,91%
Port 1900 (SSDP)	0,17%	5,13%	Mengalami penurunan -4,96%
Port 8080 (Web Server)	0,13%	0%	Port paling rentan terbaru
Port 22 (TCP)	0,09%	0,48%	Mengalami penurunan -0,39%
Port 80 (HTTP)	0,08%	0%	Port paling rentan terbaru
Port 5060 (SIP)	0,07%	0,80%	Mengalami penurunan -0,73%
Port 135 (RPC)	0,01%	0%	Port paling rentan terbaru

Dari hasil komparasi pada semester yang sama di tahun 2023 dan tahun 2024 kita bisa melihat terjadi banyak penurunan serangan pada beberapa port, meski demikian penurunan tersebut masih dibilang rendah. Port yang mengalami penurunan dalam skala serangan juga tidak besar.

Sementara yang patut dijadikan perhatian adalah serangan pada port 53 yang sangat mendominasi dari seluruh serangan terhadap port malah mengalami peningkatan besar hingga 15,18%, port ini dari tahun sebelumnya memang menjadi favorit pelaku kejahatan siber.

Definisi Port

Port 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 445 SMB

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 123 NTP

Port 123 digunakan untuk sinkronisasi dengan server menggunakan NTP (Network Time Protocol) dimana tingkat akurasi tinggi sangat diperlukan. Kerentanan ini disebabkan penggunaan port 123 yang tidak tepat oleh perangkat lunak yang terpengaruh.

Peretas dapat mengeksploitasi kerentanan ini dengan mengirimkan paket berbahaya ke sistem yang ditargetkan. Eksploitasi yang berhasil dapat memungkinkan pelaku untuk mengendalikan sistem sepenuhnya.

Port 5900 VNC

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 1900 SSDP

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".

Port 8080 Web Server

Port 8080 tidak hanya digunakan bagi HTTP, tapi juga bagi proxy karena masih berjalan pada satu layanan yang sama. Port nomer 8080 biasanya digunakan untuk web server. Ketika nomor port ditambahkan ke akhir nama domain, itu mengarahkan lalu lintas ke server web. Namun, pengguna tidak dapat memesan port 8080 untuk server web sekunder.

Nomor 8080 sering digunakan sebagai port default untuk server web, seperti Apache Tomcat dan Jetty, dan server aplikasi, seperti GlassFish. Awalnya dipilih sebagai default karena lebih tinggi dari nomor port terkenal (0-1023), yang dicadangkan untuk layanan tertentu dalam daftar Internet Assigned Numbers Authority (IANA), dan lebih rendah dari nomor port istimewa (1024 -49151), yang dicadangkan untuk proses sistem.

Sebagai protokol internet paling populer, HTTP cenderung menjadi sasaran pelaku jahat. Tindakan mereka seringkali melibatkan SQL injections, cross-site scripting, serangan DDoS, dan pemalsuan permintaan.

Port 22 TCP

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 80 HTTP

Digunakan untuk koneksi HTTP secara default. Ini adalah port yang populer dan banyak digunakan di seluruh dunia. Ini menghubungkan Anda ke web di seluruh dunia (WWW).

Port 80 memungkinkan penyerang mendapatkan akses admin ke situs web, atau bahkan server web itu sendiri. Tetapi yang sebenarnya dilakukan oleh penyerang adalah menggunakan lalu lintas keluar pada port 80 untuk komunikasi C2 (command and control) dan eksfiltrasi data setelah mereka berhasil menyusup ke jaringan misalnya dengan email phising atau drive-by-download.

Dan yang juga dilakukan oleh penyerang adalah membuat pengguna di dalam jaringan perusahaan mengunjungi situs yang mengirimkan malware. Ini misalnya dilakukan dengan menginfeksi situs yang biasa dikunjungi pengguna (watering hole attack) atau menggunakan iklan bertarget (malvertising). Pelaku juga mungkin membuat korban memberikan kredensial login dengan memikat korban (biasanya menggunakan email phishing) ke situs yang meniru layanan umum yang digunakan korban seperti Paypal, email web, Netflix dan sebagainya.

Port 5060 SIP

Port 5060 didedikasikan untuk Session Initiation Protocol (SIP), yang memungkinkan perangkat memulai, memelihara, dan mengakhiri sesi komunikasi dalam voice over IP (VoIP) dan aplikasi multimedia lainnya.

SIP diangkut melalui UDP dan TCP. Ini adalah protokol kontrol Lapisan Aplikasi yang membuat, memodifikasi, dan mengakhiri sesi dengan satu atau lebih peserta. SIP adalah protokol peer-to-peer.

SIP menggunakan elemen desain yang mirip dengan model transaksi HTTP request/response. Klien SIP biasanya menggunakan TCP atau UDP pada nomor port 5060 atau 5061 untuk terhubung ke server SIP dan titik akhir SIP lainnya. Port 5060 umumnya digunakan untuk lalu lintas pensinyalan yang tidak dienkripsi, sedangkan port 5061 biasanya digunakan untuk lalu lintas yang dienkripsi dengan Transport Layer Security (TLS).

Port 5060 ini yang digunakan untuk signaling pada trafik yang tidak terenkripsi (non-encrypted traffic) sering dimanfaatkan oleh penyerang. Melalui lalu lintas yang tidak terenkripsi pelaku dapat mengakses data, melakukan pencurian atau pengubahan data secara besar-besaran di seluruh jaringan.

Port 135 RPC

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 135 rentan terhadap beberapa eksploitasi serius. Jika port 135 dibiarkan terbuka di Internet publik, hal ini dapat membuat perangkat rentan terhadap serangan berbahaya seperti Remote Service Execution (RCE), paparan data sensitif, dan serangan penolakan layanan terdistribusi (DDoS).

Oleh karena itu, pengguna harus mengamankan port 135 dengan benar pada perangkat klien dan server Anda yang menggunakan port tersebut.

COMMON VULNERABILITY & EXPOSURES

Common vulnerability & exposure (CVE) adalah daftar yang menampilkan keamanan informasi apa saja pada suatu software atau firmware yang cukup rentan hingga berpotensi mendapat serangan siber.

CVE adalah simbol dari celah kerentanan yang juga merupakan bahaya laten yang sering diabaikan orang atau masih banyak orang yang tidak mengetahui dan menyadari bahaya ini. Penyerang atau *hacker* biasanya akan memanfaatkan celah tersebut untuk mengganggu fungsi website yang dijadikan sebagai target.

Celah kerentanan tersebut juga menjadi sasaran penjahat siber dalam melakukan aksi-aksinya, dan di antaranya telah diklasifikasikan oleh AwanPintar.id®, kerentanan yang paling masif dimanfaatkan dan dieksploitasi di tanah air.

CVE	Jumlah	Persentase
CVE-2020-11899	151.314.072	99,55%
CVE-2023-50387	353.849	0,23%
CVE-2020-11910	146.054	0,10%
CVE-2022-27255	86.859	0,06%
CVE-2020-11900	37.419	0,02%
CVE-2019-11500	19.796	0,01 %
CVE-2015-7547	14.620	0,01 %
CVE-2021-43798	2,537	0,0%
CVE-2021-35394	2.113	0,0%
CVE-2018-13379	1.552	0,0%
Lainnya	-	0,02%

CVE-2020-11899
CVSS Score: 5.4 Medium

CVE-2020–11899, kerentanan pada tumpukan 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.

Serangan dapat dimulai dari jarak jauh. Tidak diperlukan bentuk autentikasi agar eksploitasi berhasil. Detail teknisnya tidak diketahui dan eksploitasinya tidak tersedia untuk umum.

Produk Terdampak
TCP/IP Versions sebelum (<) 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:
- Meminimalisir paparan jaringan untuk semua perangkat dan/atau sistem-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 Jaringan Pribadi Virtual (VPN), karena VPN yang mengenali mungkin memiliki kerentanan dan harus diperbarui ke versi terbaru yang tersedia. Ketahuilah juga bahwa VPN hanya seaman perangkatnya yang terhubung.

CVE-2023-50387
CVSS Score: 7.5

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

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

Dampak
Dengan membanjiri pemecah masalah target dengan pertanyaan yang mengeksploitasi kelemahan ini, penyerang dapat secara signifikan mengganggu kinerja penyelesai, secara efektif menolak akses klien yang sah ke layanan penyelesaian DNS.

Atau dengan kata lain eksploitasi kerentanan ini yang berhasil dapat menyebabkan Denial of Service (DoS).

Produk Terdampak
- Active IQ Unified Manager for VMware vSphere
- NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S
- NetApp HCI Baseboard Management Controller (BMC) - H410C

Mitigasi Kerentanan

Meskipun hal ini tidak disarankan, menonaktifkan validasi DNSSEC sepenuhnya akan menghilangkan kerentanan. Kami sangat menyarankan untuk menginstal salah satu versi BIND yang tercantum di bawah ini, yang mana validasi DNSSEC yang sangat rumit tidak akan lagi menghambat beban kerja server lain.

Tingkatkan ke rilis yang di-patch yang paling terkait dengan versi BIND 9 Anda saat ini:
16.09.48
18.09.24
19.09.21

Edisi Pratinjau yang Didukung BIND adalah cabang pratinjau fitur khusus dari BIND yang disediakan untuk pelanggan dukungan ISC yang memenuhi syarat.
9.16.48-S1
9.18.24-S1

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, energi, 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 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.

*https://www.jsof-tech.com/disclosures/ripple20/

CVE-2022-27255
CVSS Score: 8.5 (High)

Kerentanan ini dikenal sebagai CVE-2022-27255 sejak 20 Maret 2022. Kerentanan ini ditemui pada Realtek eCos RSDK 1.5.7p1 dan MSDK 4.9.4p1, fungsi SIP ALG yang menulis ulang data SDP memiliki buffer overflow berbasis stack. Hal ini memungkinkan penyerang mengeksekusi kode dari jarak jauh tanpa autentikasi melalui paket SIP buatan yang berisi data SDP berbahaya.

CVE-2022-27255 adalah kerentanan tanpa klik, yang berarti bahwa eksploitasi diam dan tidak memerlukan interaksi dari pengguna. Pelaku hanya membutuhkan alamat IP eksternal dari perangkat yang rentan. Jika eksploitasi berubah menjadi worm, ia bisa menyebar ke internet dalam hitungan menit.

Dampak
Menurut Realtek, perangkat yang menggunakan firmware OS eCos SDK Realtek sebelum Maret 2022 rentan terhadap CVE-2022-27255. Akar penyebab kerentanan adalah "validasi yang tidak memadai pada buffer yang diterima, dan panggilan yang tidak aman ke strcpy. Modul 'SIP ALG' memanggil strcpy untuk menyalin beberapa konten paket SIP (protokol inisiasi sesi) ke buffer tetap yang telah ditentukan dan tidak memeriksa panjang konten yang disalin.

Pelaku ancaman dapat "mengeksploitasi kerentanan melalui antarmuka WAN dengan membuat argumen dalam data SDP (Session Desciption Protocol) atau header SIP untuk membuat paket SIP tertentu, dan eksploitasi yang berhasil akan menyebabkan crash atau mencapai eksekusi kode jarak jauh."

Produk yang terdampak
Kerentanan mempengaruhi produk apa pun yang menggunakan seri Realtek eCos SDK OS rtl819x-eCos-v0.x atau rtl819x-eCos-v1.x. Menurut para peneliti, kerentanan tersebut mempengaruhi 31 perangkat dari setidaknya 19 vendor.

Mitigasi Kerentanan
Perusahaan disarankan untuk mulai menilai keterpaparan mereka terhadap kerentanan ini sekarang dengan memastikan daftar aset selalu diperbarui, terutama untuk perangkat jaringan bervolume rendah seperti router bisnis kecil hingga menengah dan perangkat internet of things.

Secara khusus, perusahaan harus:
- Melakukan aktivitas penemuan dan mendokumentasikan perangkat yang berpotensi mempengaruhi dalam daftar aset mereka.
- Beri tahu pemilik aset informasi di mana perangkat yang rentan diidentifikasi.
- Pastikan proses lokal tersedia untuk mengidentifikasi dan mengeluarkan pembaruan firmware darurat untuk perangkat yang terpengaruh.
- Perbarui perangkat yang terpengaruh saat tambalan tersedia dari vendor.

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 Terdampak

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-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 pada sistem operasi Linux Red Hat.

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 Red Hat yang digunakan dan melakukan pemindaian untuk mengidentifikasi adanya penyusupan.

Green
OPEN

CVE-2015-7547
CVSS: 8.1 Critical

Kerentanan pada penyelesai 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.

Masalah glibc ini hanya dapat dieksploitasi oleh penyerang yang mengendalikan server DNS yang dikonfigurasi untuk perangkat tersebut. Selain itu, penyerang harus mengatasi mitigasi anti-eksploitasi tambahan, seperti ASLR, agar serangan berhasil.

Produk Terdampak
Masalah ini mempengaruhi:
PAN-OS 5.0.19 dan versi lebih lama.
PAN-OS 5.1.12 dan versi lebih lama.
PAN-OS 6.0.14 dan versi lebih lama.
PAN-OS 6.1.12 dan versi lebih lama.
PAN-OS 7.0.7 dan versi lebih lama.
PAN-OS 7.1.3 dan versi lebih lama.

Mitigasi Kerentanan
Kerentanan ini dapat mempengaruhi perangkat lunak PAN-OS hanya ketika perangkat dikonfigurasi dengan server DNS yang berada di bawah kendali penyerang. Tidak disarankan konfigurasi perangkat dengan server DNS yang tidak terpercaya.

Lakukan update terbaru:
PAN-OS 5.0.20 dan lebih baru.
PAN-OS 5.1.13 dan lebih baru.
PAN-OS 6.0.15 dan lebih baru.
PAN-OS 6.1.13 dan lebih baru.
PAN-OS 7.0.8 dan lebih baru.
PAN-OS 7.1.4 dan yang lebih baru.

CVE-2021-43798
CVSS: 7.5 HIGH

Grafana adalah platform sumber terbuka untuk pemantauan dan observasi. Grafana versi 8.0.0-beta1 hingga 8.3.0 (kecuali untuk versi yang di-patch) rentan terhadap traversal direktori, sehingga memungkinkan akses ke file lokal. Jalur URL yang rentan adalah:

`<grafana_host_url>/public/plugins//`, yang merupakan ID plugin untuk setiap plugin yang diinstal. Grafana Cloud tidak pernah rentan.

Produk Terdampak
Produk yang terdampak adalah versi di bawah ini:
- 8.0, 8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.0.5, 8.0.6
- 8.1, 8.1.0, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6, 8.1.7
- 8.2, 8.2.0, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.2.6
- 8.3

Mitigasi Kerentanan
Untuk mengatasi masalah pada kerentanan ini berikut solusinya:
- Meningkatkan ke versi 8.0.7, 8.1.8, 8.2.7 atau 8.3.1 menghilangkan kerentanan ini. Menerapkan patch c798c0e958d15d9cc7f27c72113d572fa58545ce mampu menghilangkan masalah ini.
- Perbaikan bug siap diunduh di github. com. Mitigasi terbaik disarankan untuk meningkatkan ke versi terbaru.

CVE-2021-35394
CVSS: 9.8 Critical

Realtek Jungle SDK versi v2.x hingga v3.4.14B menyediakan alat diagnostik bernama MP Daemon yang biasanya dikompilasi sebagai biner UDP Server. Biner dipengaruhi oleh beberapa kerentanan kerusakan memori dan kerentanan injeksi arbitrary command yang dapat dieksploitasi oleh penyerang jarak jauh yang tidak diautentikasi.

Dampak
Eksploitasi kerentanan ini memungkinkan penyerang jarak jauh mengeksekusi kode arbitrer pada perangkat yang rentan, sehingga menyebabkan kompromi sistem.

Malware seperti RedGoBot, GooberBot, Mirai, Gafgyt dan Mozi dilaporkan terkait dengan CVE-2021-35394.

Produk Terdampak
Realtek_jungle_sdk, vendor Realtek, start version 2.0, end version 3.4.14b

Mitigasi Kerentanan
Melakukan patching atau update software terbaru untuk mencegah eksploitasi terhadap produk yang diketahui terdampak dan rentan ancaman siber.

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 diautentikasi dapat mengeksploitasi ini untuk mengakses informasi sensitif di mesin yang terpengaruh melalui permintaan yang dibuat.

Produk 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.

- Pertimbangkan untuk menerapkan browser sandbox untuk melindungi sistem dari malware yang berasal dari penjelajahan web. Browser dengan sandbox mengisolasi mesin host dari kode berbahaya.
- Mewajibkan semua akun dengan login kata sandi (misalnya akun layanan, akun admin, dan akun admin domain) untuk mematuhi standar NIST untuk mengembangkan dan mengelola kebijakan kata sandi.
- Selalu perbarui semua sistem operasi, perangkat lunak, dan firmware.
- Ikuti praktik terbaik dengan hak istimewa paling rendah.
- Terapkan filter di gateway email untuk memfilter email dengan indikator berbahaya yang diketahui, seperti baris subjek berbahaya yang diketahui, dan memblokir alamat IP yang mencurigakan di firewall.
- Instal firewall aplikasi web dan konfigurasikan dengan aturan yang sesuai untuk melindungi aset perusahaan.
- Kembangkan dan perbarui secara berkala diagram jaringan komprehensif yang menggambarkan sistem dan aliran data dalam jaringan organisasi Anda.
- Aktifkan pengelogan PowerShell yang ditingkatkan.

- Konfigurasikan Registri Windows agar memerlukan persetujuan UAC untuk operasi PsExec apa pun.
- Terapkan kebijakan keamanan lokal untuk mengontrol eksekusi aplikasi (misalnya Kebijakan Pembatasan Perangkat Lunak (SRP), AppLocker, Kontrol Aplikasi Windows Defender (WDAC)) dengan daftar yang diizinkan secara ketat.
- Batasi penggunaan NTLM dengan kebijakan keamanan dan firewall.
- Menonaktifkan port yang tidak digunakan.
- Tinjau layanan yang terhubung ke internet dan nonaktifkan layanan apa pun yang tidak lagi menjadi persyaratan bisnis untuk diekspos atau batasi akses hanya untuk pengguna yang memiliki persyaratan eksplisit untuk mengakses layanan, seperti SSL, VPN, atau RDP. Jika layanan yang terhubung ke internet harus digunakan, kontrol akses dengan hanya mengizinkan akses dari rentang IP admin [CPG 2.X].
- Tinjau pengontrol domain, server, stasiun kerja, dan direktori aktif untuk akun baru dan/atau tidak dikenal.
- Verifikasi tingkat keamanan domain direktori aktif secara rutin dengan memeriksa kesalahan konfigurasi.

Validasi Kontrol Keamanan

Selain menerapkan mitigasi, disarankan untuk melakukan, menguji, dan memvalidasi program keamanan organisasi terhadap perilaku ancaman yang dipetakan ke kerangka kerja MITRE ATT&CK untuk perusahaan. Dan inventaris kontrol keamanan untuk menilai kinerjanya terhadap teknik ATT&CK.

Green
OPEN

SERANGAN DALAM NEGERI

Akumulasi Serangan dalam Negeri

AwanPintar.id® secara khusus pada laporan kali ini juga melakukan pemantauan terhadap serangan yang berasal dari dalam negeri. Hal ini menjadi penting mengingat perlunya melakukan monitoring dan perbaikan pada sistem yang ada secara Nasional agar semakin meningkatkan kewaspadaan siber Nasional.

Secara teknis, ada beberapa kemungkinan alasan masuknya IP Indonesia sebagai kategori penyerang. IP tersebut bisa saja memang dengan sengaja dimanfaatkan oleh penggunanya untuk menyerang atau dimanfaatkan oleh orang lain sebagai BOT untuk melakukan penyerangan ke dalam negeri sendiri. Hal ini menjadi penting untuk diwaspadai untuk mengurangi kemungkinan semakin banyaknya IP Indonesia yang masuk *blocklist* pada beragam sistem yang ada.

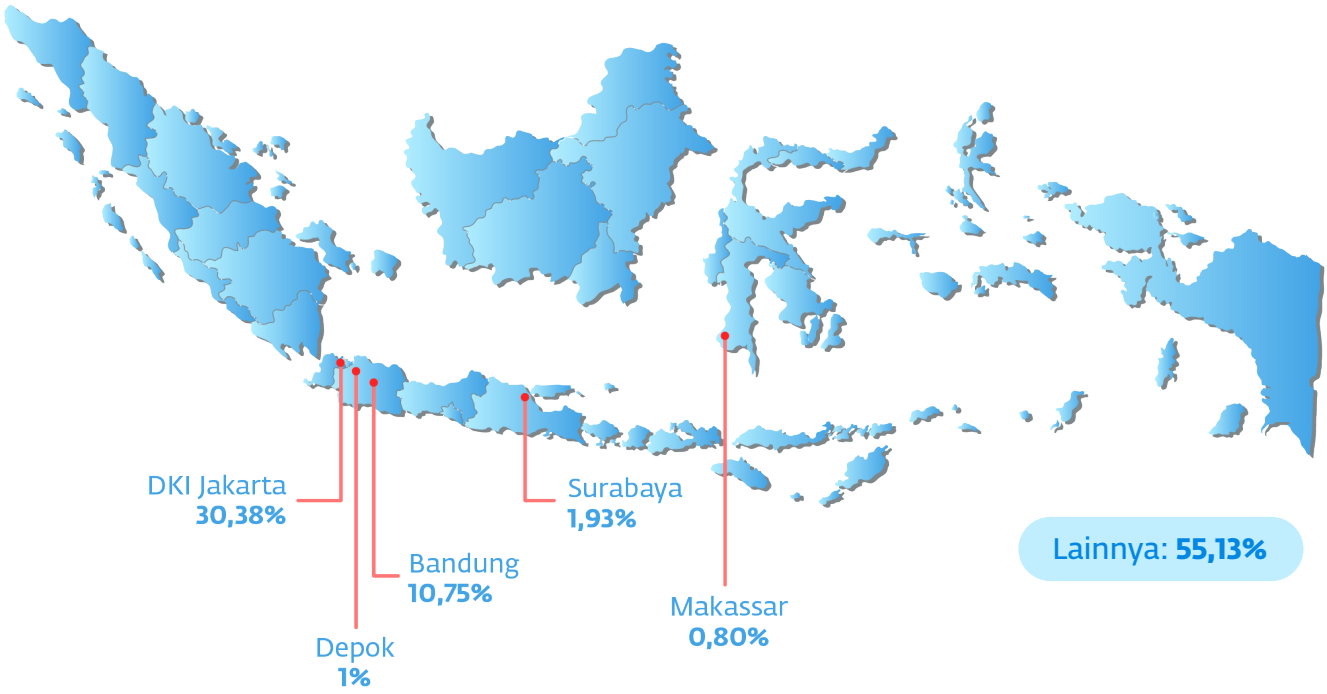
Dan dari data tersebut diketahui ada daerah atau kabupaten wilayah yang menjadi sentra serangan siber di dalam negeri yang dihimpun secara rinci dalam database AwanPintar.id®. Berikut data-datanya.

5 Daerah Penyerang Teratas di Indonesia

Dengan luas 1.916.906 kilometer persegi, Indonesia memiliki 17.001 pulau yang terbagi menjadi 38 provinsi dan 514 kota/kabupaten, Indonesia merupakan negara yang besar dan sangat luas.

Dari serapan data yang diperoleh dari detektor AwanPintar.id® diketahui 5 daerah teratas yang melakukan serangan secara besar-besaran ke ekosistem digital nasional, sebagai berikut:

Semester 1 Tahun 2024



Dari laporan terbaru ini kita bisa melihat DKI Jakarta dan Depok secara konsisten dari tahun ke tahun menjadi daerah yang selalu masuk dalam daftar melakukan serangan ke dalam negeri. Jumlah serangan keduanya juga paling mendominasi di antara yang lainnya.

Sementara ketiga daerah pendatang baru merupakan daerah utama di Indonesia, dua berasal dari pulau Jawa sedangkan satunya dari pulau Sulawesi. Masuknya Makassar sebagai salah satu daerah penyerang teratas cukup mengejutkan, mengingat wilayah ini sebelumnya tidak terlalu aktif sebagai agresor.

Komparasi Semester 1 Tahun 2023 & Semester 1 Tahun 2024

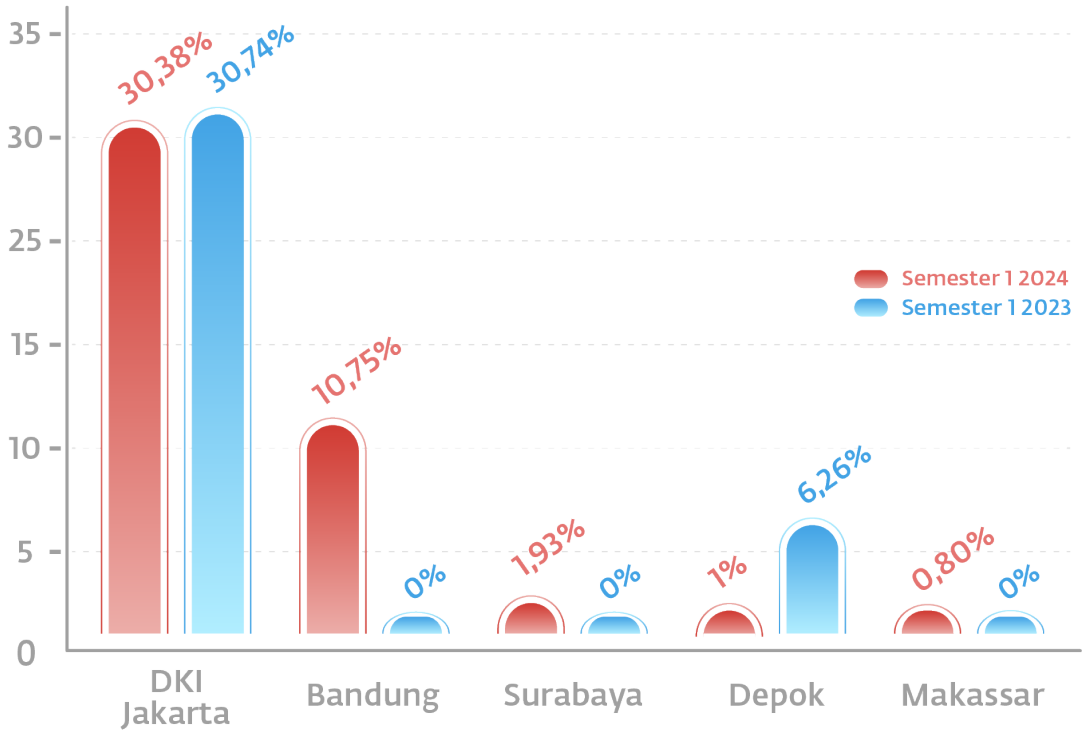
Untuk melihat sejauh apa perkembangan ancaman di dalam negeri berikut perbandingan antara Semester 1 tahun 2023 dan Semester 1 tahun 2024.

Semester 1 Tahun 2024

1	DKI Jakarta	30,38%	4	Depok	1,00%
2	Bandung	10,75%	5	Makassar	0,80%
3	Surabaya	1,93%	6	Lainnya	55,13%

Semester 1 Tahun 2023

1	DKI Jakarta	30,74%	4	Bogor	2,35%
2	Depok	6,26%	5	Jatikramat	2,18%
3	Tangerang	3,29%	6	Lainnya	55,17%



DKI Jakarta
Mengalami penurunan **-0,36%**

Depok
Mengalami penurunan **-5,26%**

Bandung
Daerah penyerang teratas terbaru

Makassar
Daerah penyerang teratas terbaru

Surabaya
Daerah penyerang teratas terbaru

Jakarta dan Depok adalah dua daerah yang selalu konsisten menjadi sentra serangan di dalam negeri.

DKI Jakarta adalah daerah yang menjadi pilar teknologi, yang merupakan pusat bisnis, industri dan tempat kompilasi big data dari seluruh Indonesia. DKI Jakarta juga pusat pembangunan infrastruktur digital terbesar, yang tentu saja memposisikan ibukota Indonesia ini sebagai sasaran utama bagi para penjahat dunia maya.

Sementara Depok yang merupakan daerah satelit, sebagai daerah penyangga DKI Jakarta, tentu memiliki infrastruktur digital yang cukup baik, karena dekat dengan Jakarta juga merupakan keuntungan sendiri, sehingga tidak heran banyak tindak kejahatan siber ikut marak dari daerah ini.

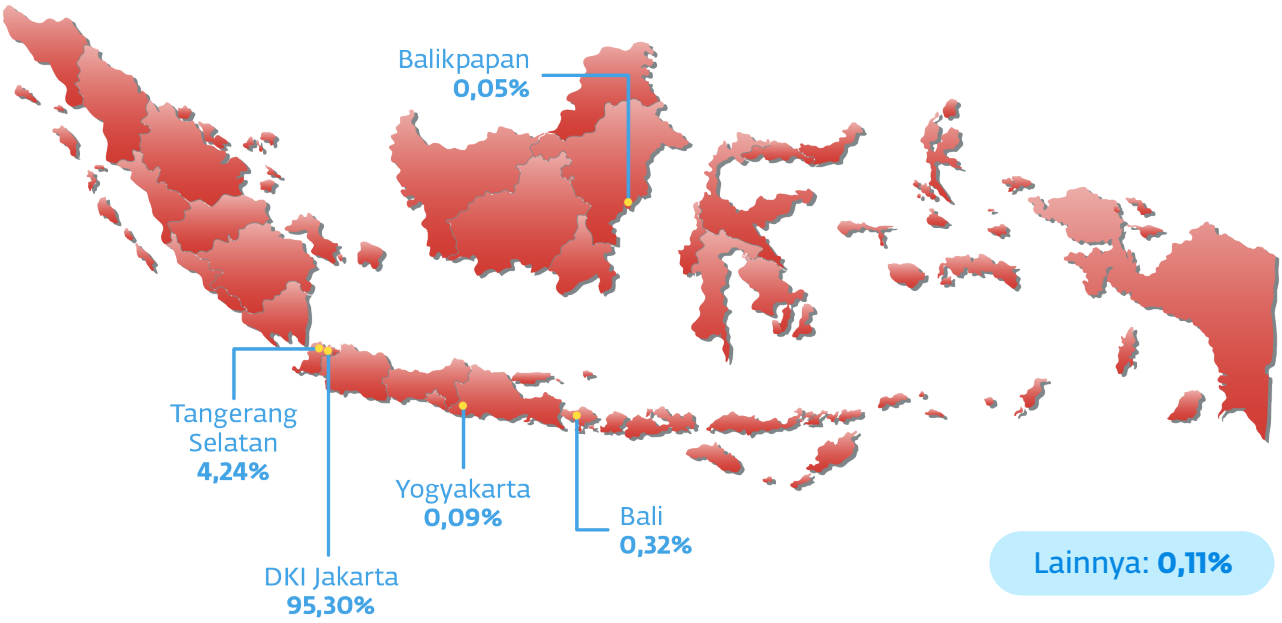
Selain 5 besar daerah di atas, yang patut dilihat adalah nilai persentase pada daerah lain mencapai nilai 55.13%. Bisa diartikan bahwa asal serangan sudah semakin menyebar sampai ke dengan jumlah penduduk jauh lebih kecil dibandingkan 5 daerah teratas.

Berikut ini adalah 10 daerah sumber serangan terkecil:

1. Majenang
2. Patuk
3. Kacapiring
4. Blega
5. Pahlawan
6. Dompu
7. Panembahan
8. Pakemitan
9. Bumiayu
10. Nagasari

5 Daerah Paling Sering Diserang

Indonesia saat ini memasuki tahap awal perang teknologi antara pemerintah daerah dan infrastruktur perkotaan melawan kejahatan siber. Daerah di tanah air ke depannya akan terus menjadi objek serangan siber dari tahun ke tahun. Di bawah ini adalah daerah di Indonesia yang paling sering menjadi target serangan siber.



Dari hasil olah data AwanPintar.id® daerah yang paling sering menjadi korban serangan dari dalam negeri merupakan daerah yang menjadi pusat perputaran uang, bisnis atau pariwisata.

DKI Jakarta adalah pusat perputaran uang, bisnis dan sentral data penting di Indonesia, ini yang kemudian menjadikan DKI Jakarta sebagai pusat serangan siber. Berbagai insiden yang menimpa berbagai sektor dan institusi menjadi ilustrasi dari dominasi serangan tersebut.

Keberadaan Tangerang Selatan di posisi kedua ini disebabkan karena posisi daerah ini berdekatan dengan DKI Jakarta juga dalam penggunaan infrastruktur jaringan nasional dan sistem perkotaan, sehingga daerah ini bisa menjadi pijakan awal bagi kelompok siber tertentu yang ingin menyerang DKI Jakarta.

Sementara Bali dan Yogyakarta dikenal sebagai daerah pariwisata yang ramai dikunjungi oleh turis dalam negeri maupun mancanegara. Maraknya transaksi bisnis, putaran perekonomian daerah melalui transaksi-transaksi digital dapat mengundang kejahatan siber.

IKN yang sedang dalam pembangunan harus bersiap dengan membangun infrastruktur keamanan siber yang kuat sedari dini. Masuknya Balikpapan sebagai salah satu daerah besar penyangga IKN yang menjadi daerah paling sering dihinggapi serangan siber merupakan sinyal kuat, ada upaya-

upaya dari kelompok-kelompok siber yang ingin menjadi Balikpapan sebagai pijakan awal mereka untuk ancaman di masa depan.

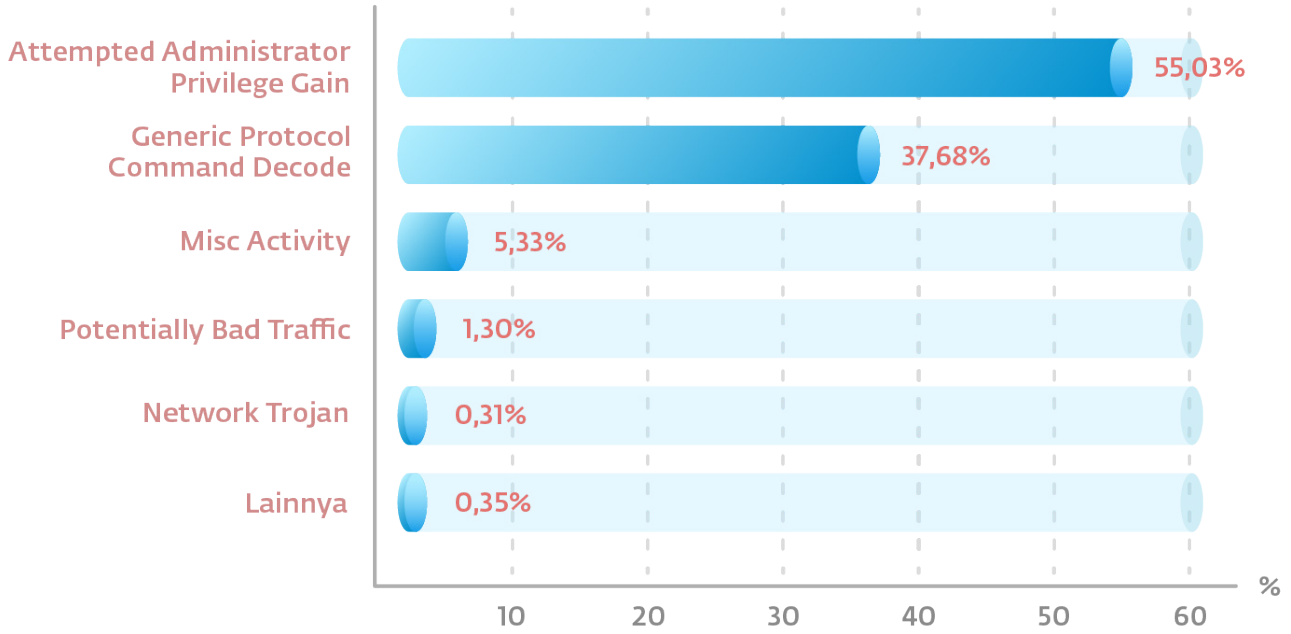
Pemberantasan kejahatan siber akan terus memerlukan perhatian para pemimpin dan lembaga penegak hukum, pertumbuhan ancaman siber tidak dapat lagi diabaikan. Para pemimpin pusat maupun daerah harus mengadopsi pola pikir keamanan digital.

Hal ini berarti menyiapkan rencana darurat dan bencana sebelum keadaan darurat siber berikutnya terjadi. Kedua, para eksekutif daerah harus mengambil peran kepemimpinan dalam memastikan keselamatan dan keamanan digital konstituennya. Dengan kebijakan yang pro aktif terhadap kejahatan siber yang terus berkembang, karena keamanan digital tidak hanya tentang perangkat keras dan perangkat lunak.

Keamanan harus dipahami sebagai prioritas penting, sesuatu yang dirancang dalam setiap elemen infrastruktur daerah, bukan sekadar hal yang muncul kemudian. Hal ini memerlukan pengembangan peraturan, regulasi, prosedur, dan anggaran bagi pemerintah daerah, dunia usaha, dan masyarakat untuk bersiap dan merespons ancaman digital ketika dan setelah.

Jenis Serangan Paling Dominan

Dari seluruh serangan yang berasal dari serangan dalam negeri, serangan tersebut terbagi menjadi beberapa kategori sebagai serangan yang paling sering dilancarkan ke dalam negeri.



Upaya pengambilalihan hak akses admin menunjukkan penyerang sudah ada di dalam sistem korban, tujuan akhir mereka adalah menguasai akses admin yang artinya menguasai seluruh sistem. Jika ini terjadi maka ini akan menjadi bencana bagi korbannya. Sementara, Eksploitasi jaringan merupakan umum yang paling sering terjadi berikutnya di Indonesia. Dan ini adalah langkah paling berbahaya yang menjadi faktor yang berujung pada pelanggaran data.
Angka yang cukup besar yang diperoleh dari AwanPintar.id®yakni pemindaian dan pengintaian jaringan yang merupakan upaya memetakan kelemahan dan kerentanan dalam jaringan internet di Indonesia, dari besarnya angka yang masuk, upaya ini cukup mengkhawatirkan.

Penyusupan sistem dan serangan Trojan menunjukkan potensi adanya sistem disusupi agresor. Yang membedakan, serangan Trojan ini merupakan ancaman yang terdeteksi di komputer atau jaringan. Kedua ancaman ini mengindikasikan bahwa penyerang dalam tahap lanjut dalam penguasaan jaringan.

Upaya Pengambilalihan Hak Akses Administrator (Attempted Administrator Privilege Gain)

Deteksi upaya untuk mengakses sumber daya tingkat pengguna super atau hak akses administrator serta eksploitasi yang berupaya membahayakan host dan memberikan akses utama ke pelaku. Upaya akses ke bagian ADMIN$ pada sistem Windows adalah contoh yang baik dari upaya untuk mengakses.

Eksploitasi Jaringan (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.

Pemindaian dan Pengintaian Jaringan (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.

Upaya Penyusupan Sistem (Potentially Bad Traffic)

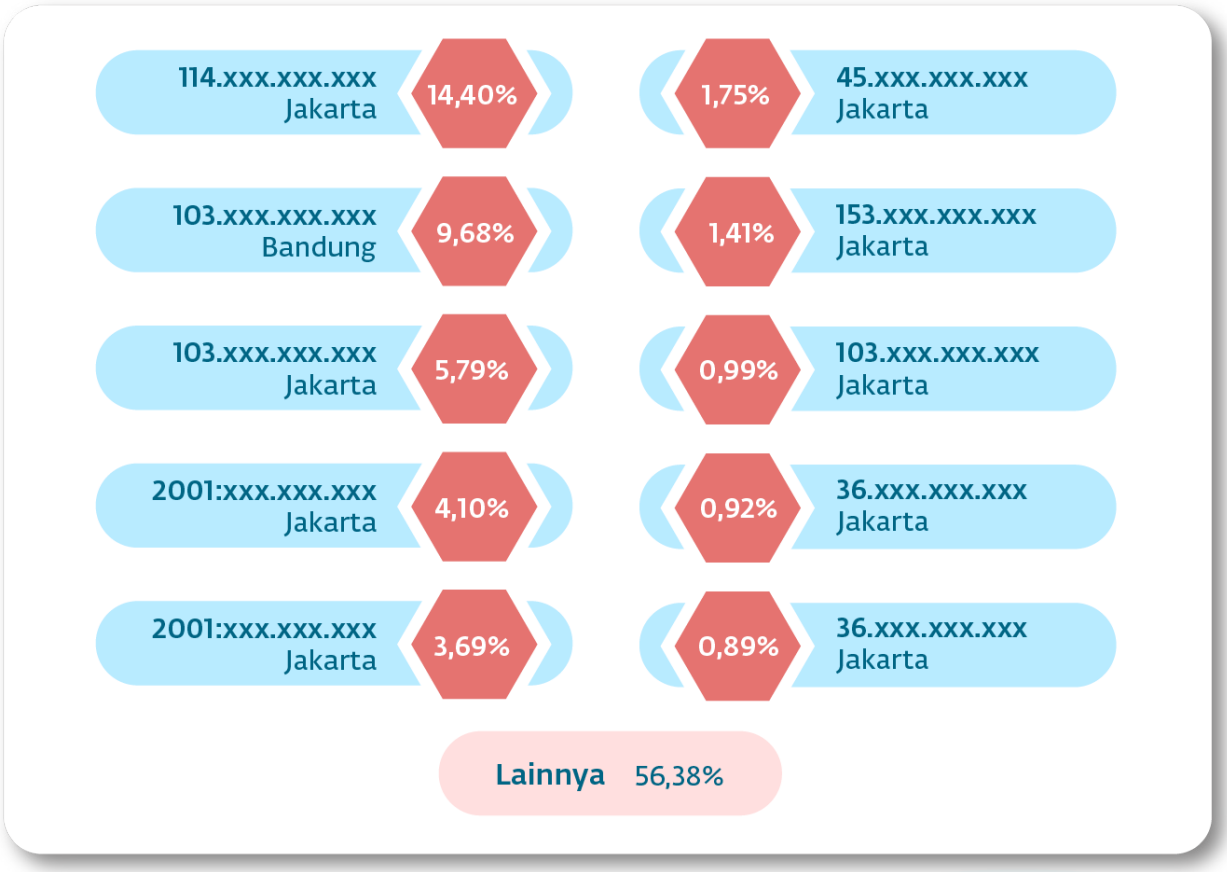
Mencakup lalu lintas yang benar-benar di luar kebiasaan, dan berpotensi menunjukkan adanya sistem yang disusupi. Sistem yang dikuasai dapat berakibat fatal bagi organisasi, pelaku dapat melakukan manipulasi dan eksploitasi tanpa batas.

Serangan Trojan (Network Trojan)

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 phising, drive by download, dan unduhan perangkat lunak dari sumber yang tidak terpercaya.

IP Penyerang dari Dalam Negeri

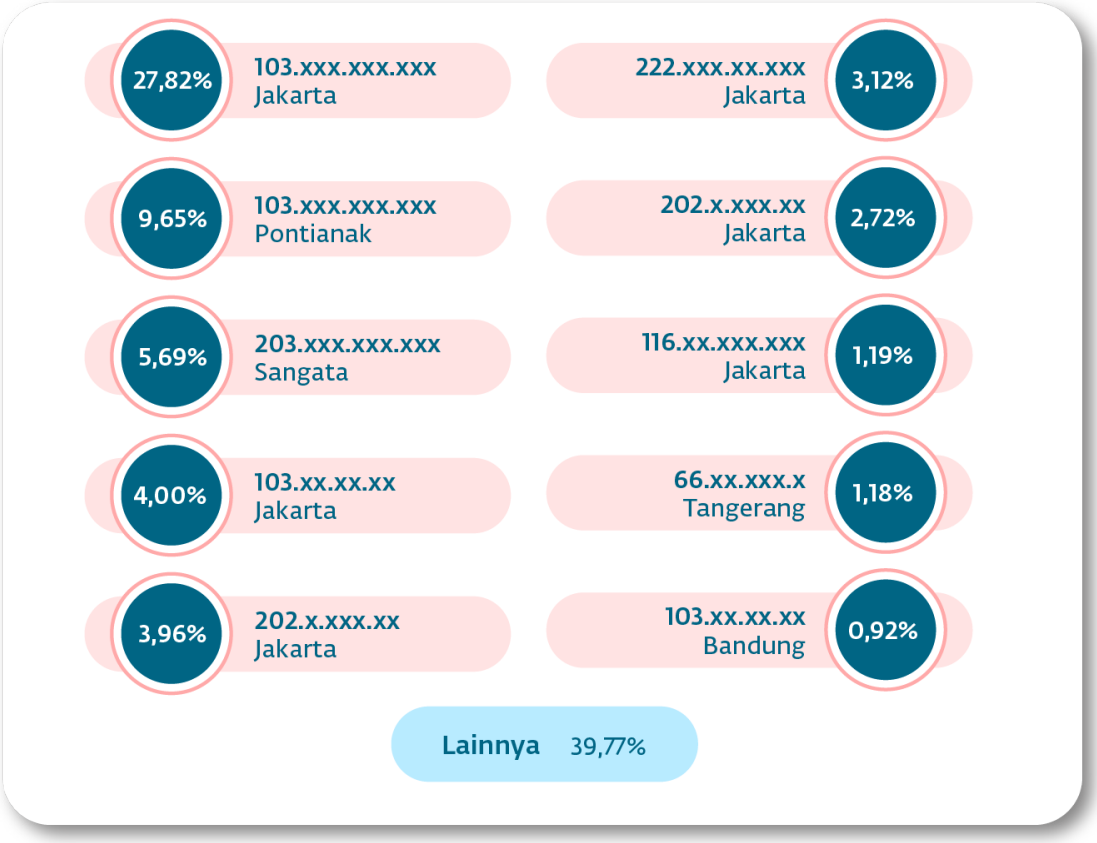
Serangan dalam negeri bisa dilacak dari jejak digital yang salah satunya bisa dideteksi melalui IP Address penyerangnya. Daftar ini adalah IP penyerang dari dalam negeri yang didata oleh AwanPintar.id®



Serangan dari dalam negeri didominasi oleh IP address dari DKI Jakarta dan daerah yang paling banyak diserang juga DKI Jakarta. Di dalam daftar IP penyerang teratas yang menyerang Indonesia IP address dari Indonesia berada di peringkat 5 besar.

IP Spam dan Malware di Indonesia

Serangan spam dan malware di Indonesia dapat ditelusuri dari IP address yang digunakan oleh pelakunya, jejak data dari alamat IP tersebut berhasil dihimpun oleh AwanPintar.id® sebagai berikut:



Paparan data yang disuguhkan menunjukkan bahwa serangan spam dan malware di Indonesia banyak berasal dari IP address yang berasal dari Jakarta. Walau jumlah serangannya tidak besar, namun akumulasi seluruh serangan menjadi serangan terbesar.

Yang menarik dari jejak alamat IP yang tercatat, Kalimantan Barat dan Kalimantan Timur masuk dalam tiga besar IP asal spam dan malware. Perluasan infrastruktur internet di daerah-daerah menjadi jalan munculnya serangan siber dari berbagai daerah, terlebih lagi daerah Tangerang dan Bandung yang sudah dari jauh hari memiliki infrastruktur internet yang lebih baik.

Green
OPEN

PENUTUP

Dunia maya menawarkan manfaat dan peluang yang sangat besar serta ancaman dan bahaya yang besar. Hal ini secara rutin dieksploitasi oleh berbagai agresor seperti negara-negara tertentu, bisnis yang melakukan spionase komersial dan pencurian atau individu dan organisasi kriminal yang melakukan berbagai macam penipuan dan eksploitasi.

Ini terjadi karena kejahatan dunia maya pada dasarnya tidak mengenal batas negara dan berkembang dengan cepat, terkadang lebih cepat daripada reaksi yang dapat dilakukan oleh otoritas nasional. Yang menambah kompleksitas adalah sifat horizontal kejahatan dunia maya, hampir semua jenis kejahatan saat ini dapat terjadi melalui internet.

Oleh karena itu, respons nasional yang efektif terhadap kejahatan dunia maya seringkali memerlukan kolaborasi multilevel. Penguatan kerja sama antara berbagai pihak baik nasional maupun internasional adalah salah satu kuncinya, karena dunia maya bersifat internasional dan bersifat lintas batas.

Keamanan siber juga harus memperhatikan tatanan yaitu keselamatan, keamanan, dan tata kelola ekosistem digital nasional yang terbentuk dengan cepat dan bermanfaat, di setiap tingkat dan di setiap bidang aktivitas manusia. Menggabungkan kedua perspektif, perlindungan dan kemajuan, untuk mendukung hal tersebut Laporan Keamanan Siber AwanPintar.id® ini dibuat.

Laporan ini juga bertujuan untuk memberikan gambaran jelas mengenai kejahatan dunia maya secara umum. Laporan keamanan siber AwanPintar.id® dapat juga menjadi sumber informasi yang berguna dan wawasan mengenai tantangan umum yang dihadapi oleh para praktisi, sehingga dapat menjadi bahan diskusi mengenai cara terbaik untuk mengatasi fenomena kejahatan dunia maya.