awanpintar.id®
CLOUD SECURITY ENGINE

INDONESIA WASPADA

Laporan Ancaman Digital di Indonesia

Semester 2 dan Analisis Serangan Sepanjang 2023

Green
OPEN

Daftar Isi

Ringkasan Eksekutif

Peraturan Presiden No. 47 Tahun 2023 yang dikeluarkan pada bulan Juli 2023 mengenai Strategi Keamanan Siber dan Manajemen Krisis Siber menjadi landasan membentuk ketahanan siber nasional. AwanPintar.id® merespon *urgency* ini dengan mengeluarkan Laporan Semester 2 tahun 2023 yang merupakan kelanjutan dari Laporan Semester 1 tahun 2023 yang sudah dirilis sebelumnya. Laporan ini akan mengeksplorasi tren, statistik, dan peristiwa penting yang terjadi pada periode Juli sampai Desember 2023 serta laporan terkait temuan kerentanan data di tahun 2023. Data pada laporan diharapkan dapat menjadi pertimbangan Profesional IT Security untuk mengantisipasi dan meminimalisir dampak kerugian pada organisasinya.

Beberapa catatan penting pada Semester 2 ini adalah munculnya CVE-2023 yang secara khusus akan dibahas di laporan ini. CVE-2023 merupakan kerentanan sistem yang secara resmi diidentifikasi dan diberi nomor pada tahun 2023. Selain itu kemunculan Indonesia dalam 10 besar negara asal serangan menjadi catatan tersendiri dalam tata kelola keamanan digital.

Laporan ini juga menyoroti pentingnya meningkatkan kesadaran akan ancaman siber dan peran teknologi dalam perlindungan terhadap serangan digital. Kesadaran siber yang lebih tinggi di kalangan individu dan organisasi dapat membantu mencegah keberhasilan serangan siber. Sementara itu, teknologi seperti kecerdasan buatan (AI), analitik terpercaya, dan teknologi keamanan canggih memainkan peran penting dalam mendeteksi dan mengatasi ancaman digital yang terus berkembang.

Paruh kedua tahun 2023 menegaskan perlunya koordinasi yang lebih baik antara pemerintah, sektor swasta, dan lembaga keamanan nasional untuk membentuk jaringan keamanan yang kokoh. Kolaborasi antara berbagai pihak ini penting dalam menghadapi serangan siber yang semakin kompleks dan terorganisir, serta dalam memastikan respons yang cepat dan efektif terhadap ancaman digital.

Perlindungan terhadap infrastruktur digital nasional harus menjadi fokus utama dalam menghadapi ancaman siber. Perlindungan siber tidak hanya mencakup upaya teknis, tetapi juga regulasi yang memadai, investasi dalam teknologi keamanan, dan pembangunan kapasitas sumber daya manusia yang mumpuni dalam bidang keamanan digital.

Dalam keseluruhan, laporan ini menunjukkan bahwa ancaman digital pada paruh kedua tahun 2023 terus mengalami peningkatan dalam kompleksitas dan dampak potensialnya. Meningkatkan kesadaran siber, memperkuat jaringan keamanan nasional, dan upaya perlindungan siber yang holistik menjadi kunci dalam menghadapi tren serangan siber yang semakin canggih dan meresahkan.

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. PT Prosperita Sistem Indonesia bergerak sebagai penghasil solusi keamanan siber 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 dan SpamCleaner® www.spamcleaner.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 *detector* 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 profesional TI. 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 *detector* 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. Informasi lanjut mengenai AwanPintar.id® dapat diakses di www.awanpintar.id atau menghubungi partner@awanpintar.id.

Metodologi

Untuk memahami ancaman digital di Indonesia, AwanPintar.id® memasang sejumlah *detector* di jaringan internet Indonesia. *Detector* ini menjadi target serangan dari mancanegara dan dalam negeri. Berikut adalah metodologi riset yang digunakan untuk membuat Laporan Ancaman Digital Semester Kedua 2023:

1. Pengumpulan Data

AwanPintar.id® menggunakan sejumlah *detector* yang tersebar di jaringan internet Indonesia dan mengumpulkan seluruh data dari tiap *detector*nya untuk diolah menjadi BigData. Tiap *detector* 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.

Detector AwanPintar.id® bersifat pasif dan mandiri, yang berarti sebagai *detector* hanya menerima masukan yang berupa serangan dari seluruh dunia yang diarahkan ke tiap *detector* secara spesifik. *Detector* 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 *detector* 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 memilah 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 BigData.

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 analisa 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.

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.

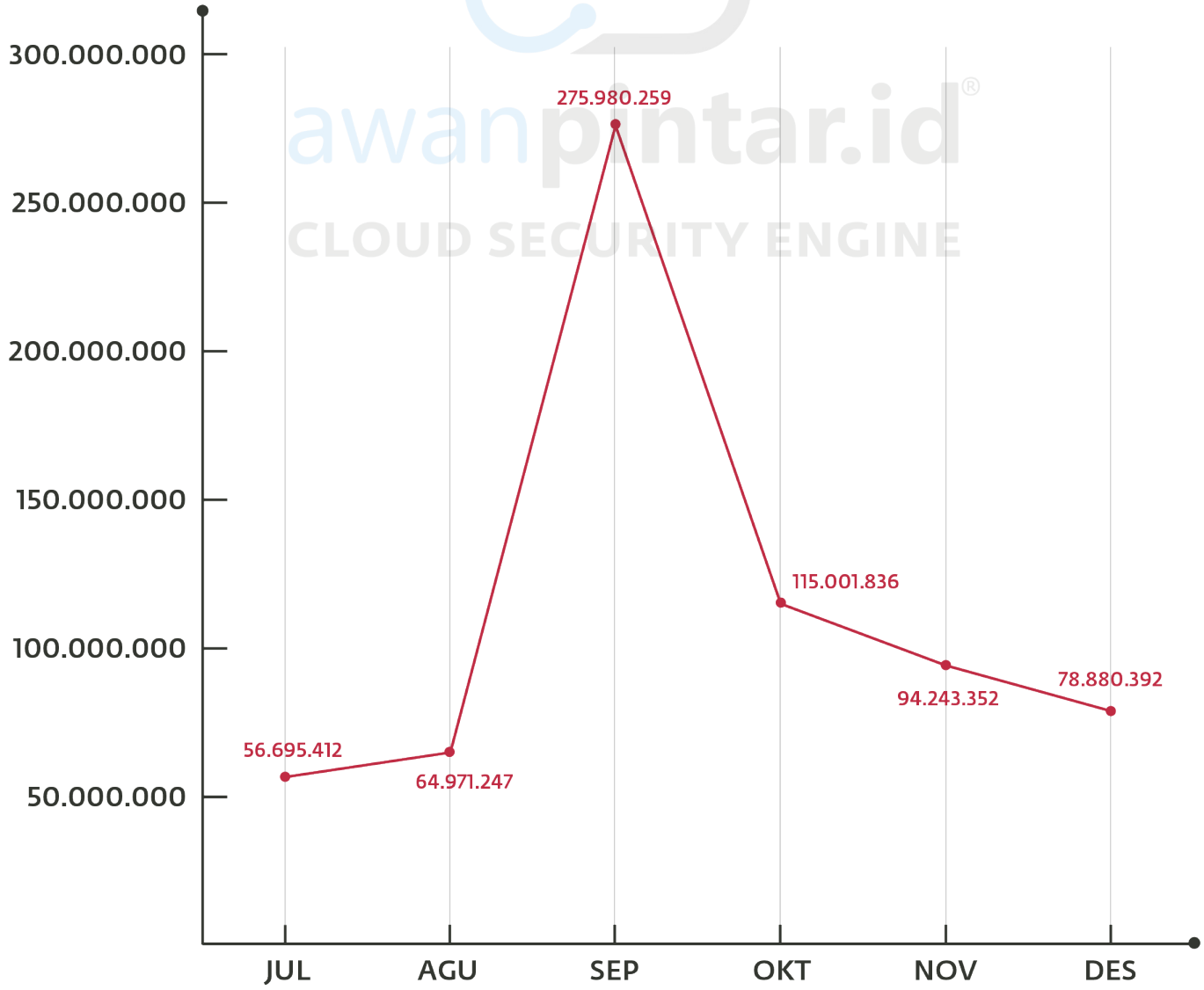
Skala dalam visualisasi mungkin saja disesuaikan untuk memberikan gambaran yang menarik saat melihat data yang disajikan tanpa mengurangi informasi yang diberikan.

Tren Serangan Terkini

AKUMULASI SERANGAN SIBER DI INDONESIA

Berikut ini merupakan data yang diambil secara rata-rata pada sebuah *detector* pada Semester 2 tahun 2023.

Rata-rata serangan per detik	Rata-rata serangan per menit	Rata-rata serangan per jam	Rata-rata serangan per hari
43	2.588	155.292	3.727.024

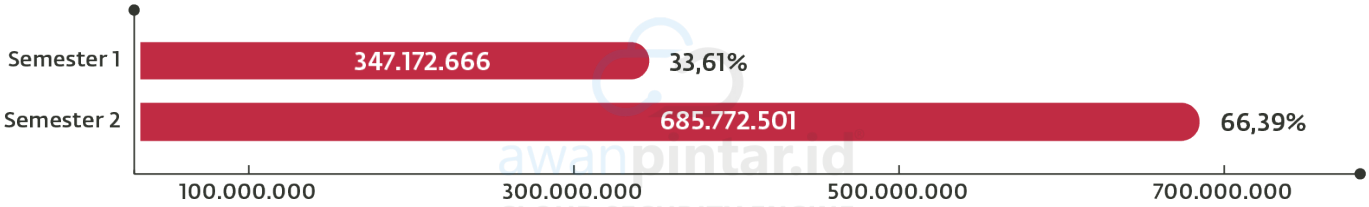


Jumlah total seluruh serangan : 685.772.501

Menginjak Semester 2 tahun 2023 paparan ancaman digital di Indonesia memasuki babak baru yang lebih intens. Dengan total serangan mencapai 685.772.501 serangan per *detector* atau hampir dua kali lipat dari semester sebelumnya yang menunjukkan Indonesia sebagai sasaran favorit penjahat dunia maya.

Yang patut disoroti pada paruh kedua adalah eskalasi serangan siber yang mencapai puncaknya di bulan September dengan total ancaman sebesar 275.980.259 atau 40,24%, hampir separuh dari seluruh serangan di paruh kedua tahun ini.

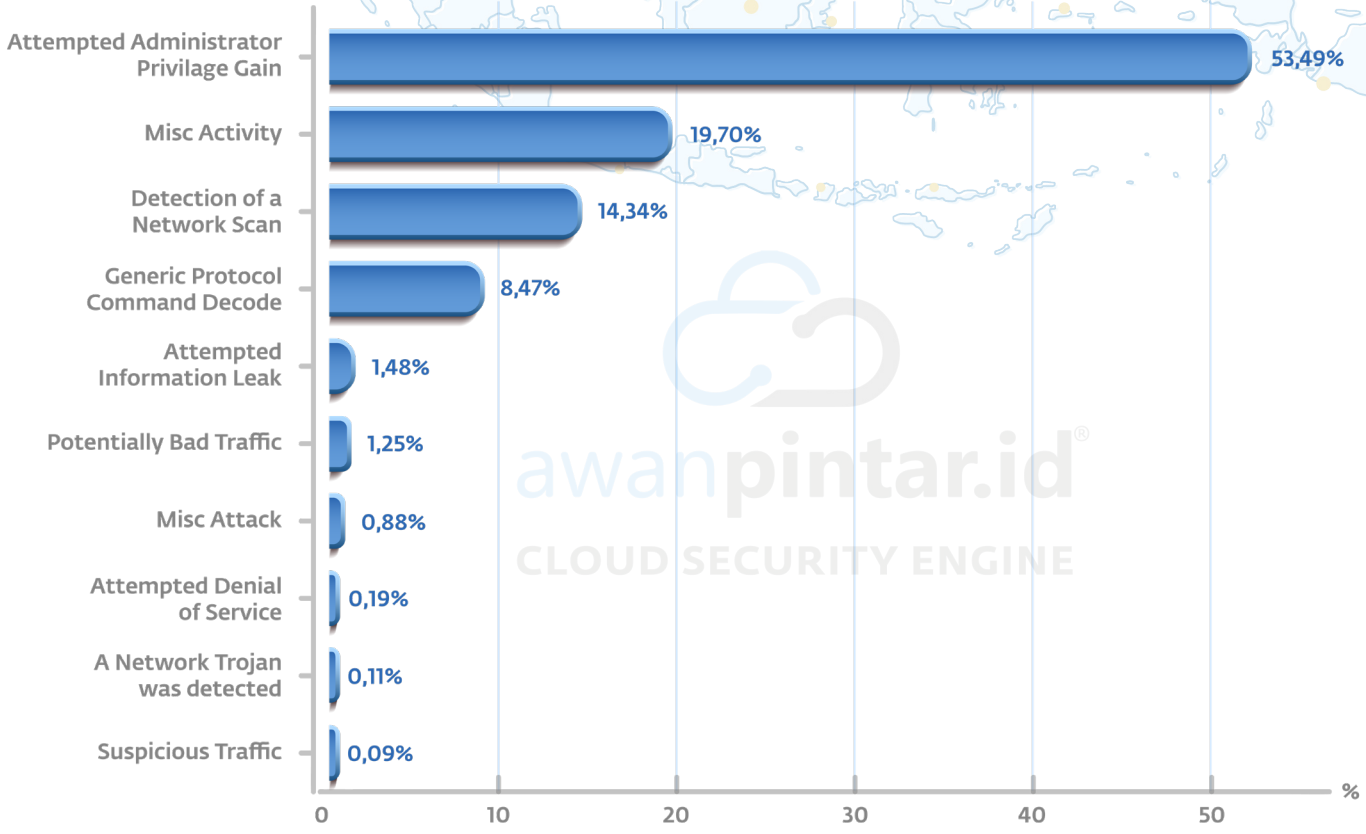
Komparasi Akumulasi Serangan Semester 1 dan 2



Jumlah serangan meningkat: **338.599.835** atau **97,53%**

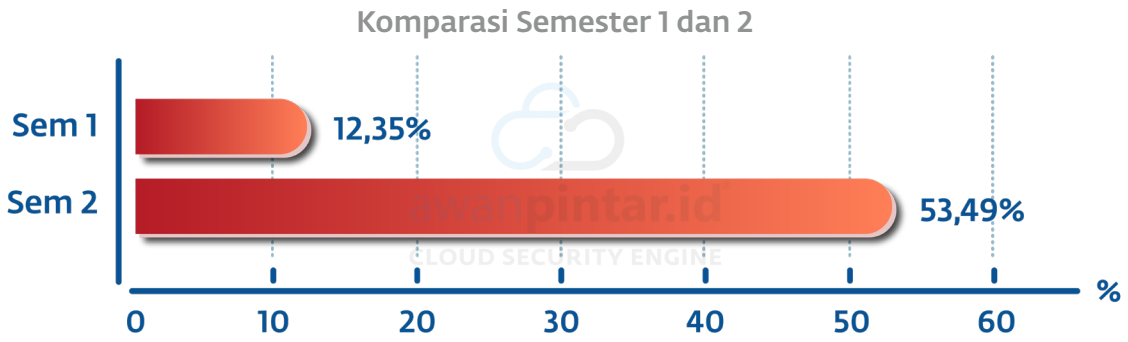
Persentase kenaikan serangan siber dari semester 1 ke semester 2 di tahun 2023 meningkat **97,53%.**

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.

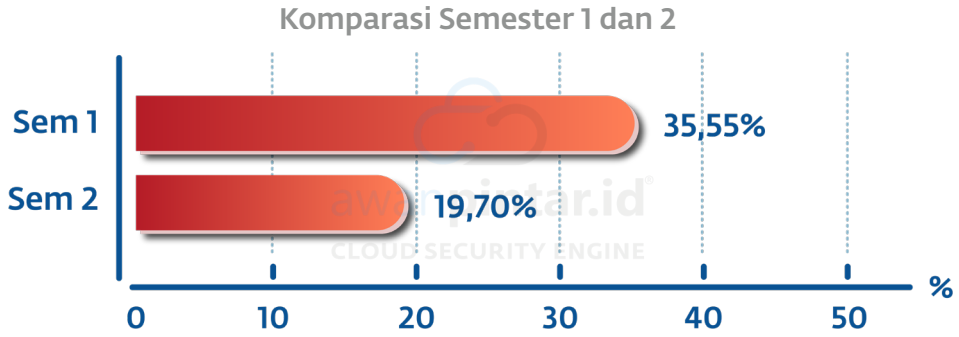


Peningkatan serangan dari attempted administrator privilege gain dari Semester 1 ke Semester 2 mencapai 41.14% dalam serangan untuk mengeksploitasi untuk mengakses hak akses administrator. Kenaikan yang cukup mencolok pada tahap serangan ini menunjukkan serangan sudah mencapai tahap akhir yaitu menargetkan dan menyasar pada tujuan tertentu.

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.

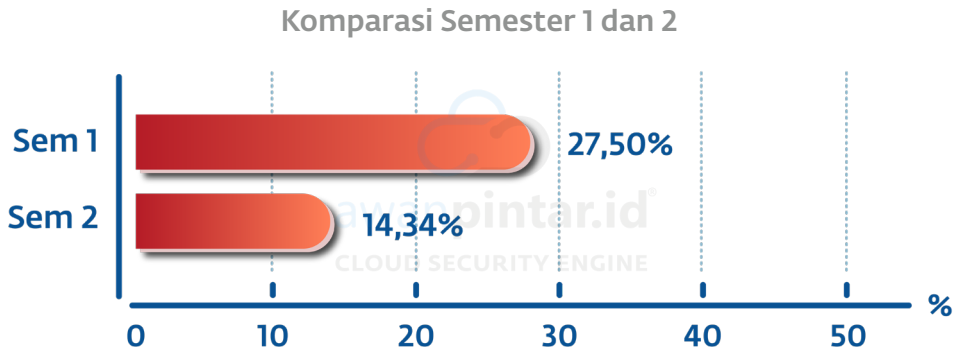
Aktivitas lain-lain dapat mencakup pemindaian port, pengintaian jaringan, atau jenis aktivitas lain yang berpotensi digunakan sebagai pendahulu serangan yang lebih serius. Meskipun aktivitas lain-lain mungkin tidak langsung mengancam, penting bagi profesional keamanan siber untuk memantau dan menyelidiki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



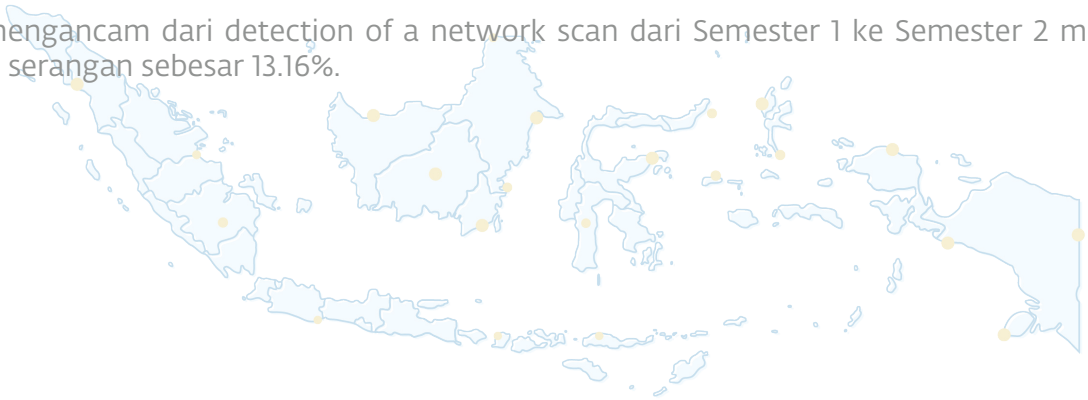
Penurunan pada aktivitas ini 15,85% besar kemungkinan terkait dengan kenaikan tahapan penyerangan yang lebih tinggi.

Detection of a Network Scan

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

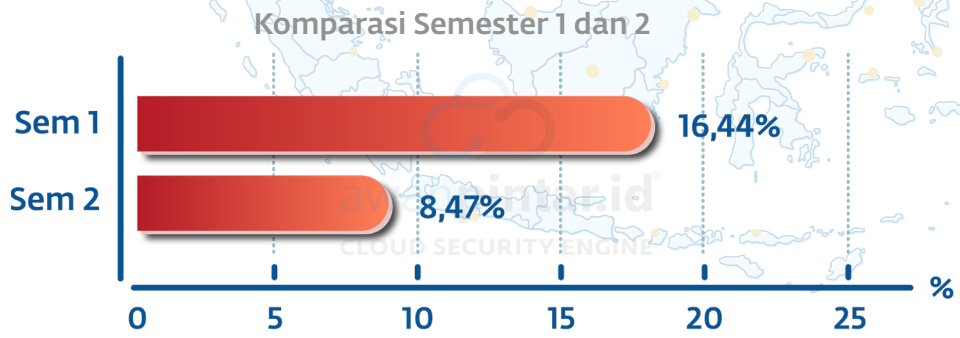


Aktivitas mengancam dari detection of a network scan dari Semester 1 ke Semester 2 mengalami penurunan serangan sebesar 13.16%.



Generic Protocol Command Decode

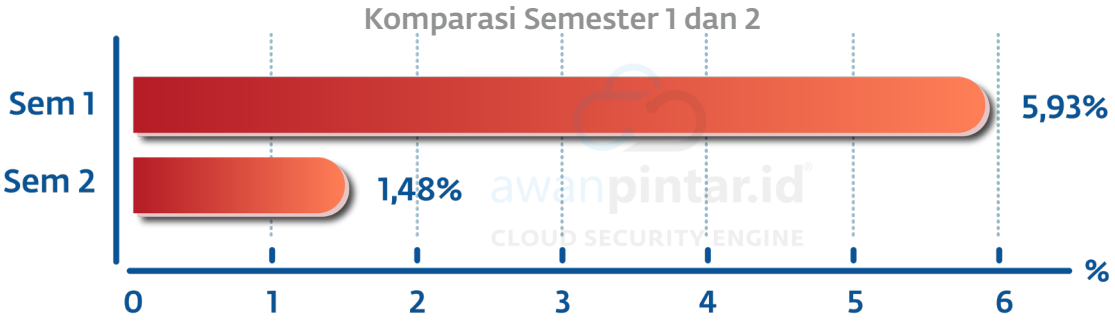
Identifikasi anomali pada paket data protokol jaringan yang tidak diharapkan atau tidak sah. Metode ini dapat digunakan untuk mendeteksi serangan siber yang menggunakan teknik manipulasi atau mencampuradukan protokol jaringan.



Pada deteksi generic protocol command decode terjadi penurunan anomali dari Semester 2 dibanding Semester 1 sebesar 7,97%.

Attempted Information Leak

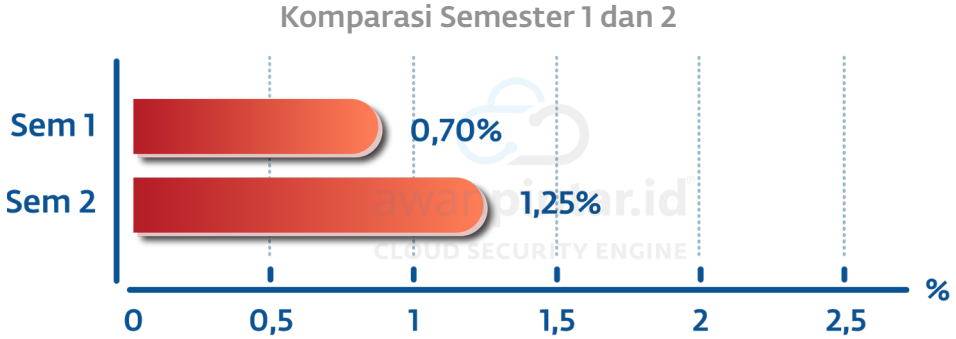
Upaya untuk mengakses atau mengungkap informasi yang seharusnya tidak dapat diakses orang yang tidak berhak. Hal ini dapat terjadi ketika pelaku mencoba mengambil informasi sensitif seperti akun, data klien, informasi kartu kredit atau informasi penting lainnya.



Upaya pencurian informasi pada Semester 2 juga mengalami menurun dibanding Semester 1 yakni sebesar 4,45% pada pencurian informasi sensitif.

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.

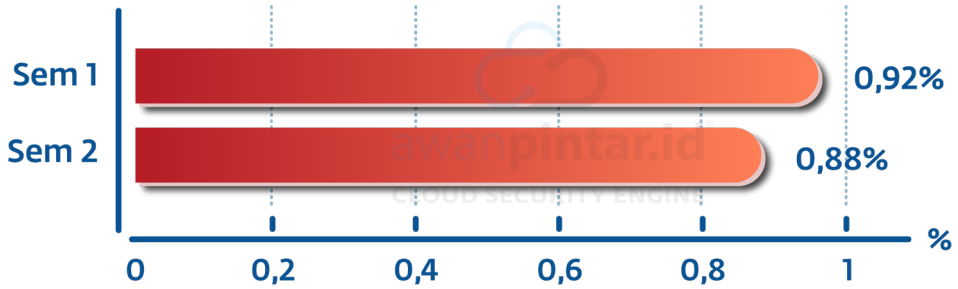


Aktivitas mengancam dari potentially bad traffic dari Semester 1 ke Semester 2 mencapai 0,55% serangan, peningkatan ini terbilang cukup besar jika dibandingkan dengan besar serangan sebelumnya.

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.

Komparasi Semester 1 dan 2

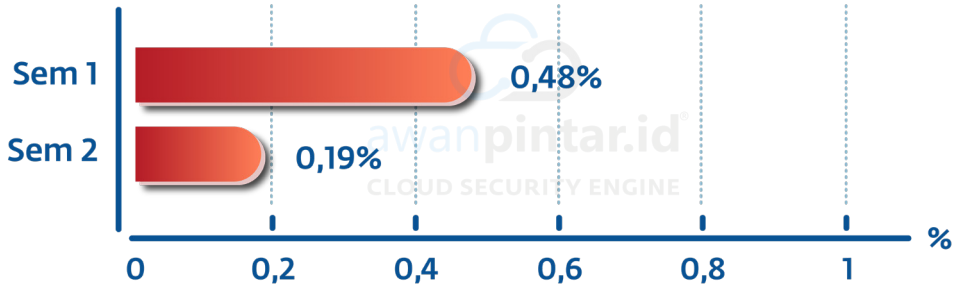


Eksploitasi server web di misc attack ada depresiasi minim sebesar 0,04% dimana bobot serangan lebih dominan dari jumlah serangan secara umum.

Attempted 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).

Komparasi Semester 1 dan 2

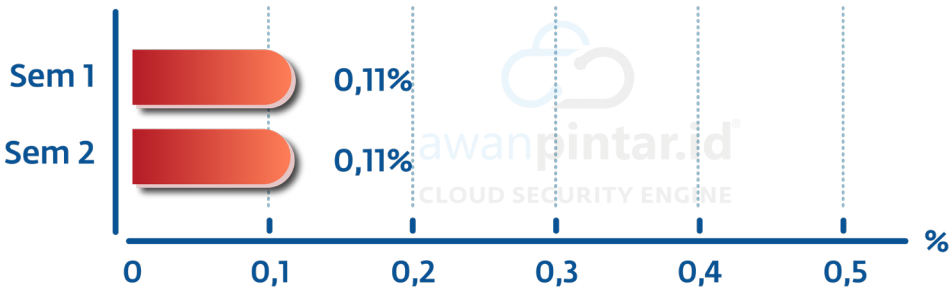


Kategori serangan dalam attempt denial of service di Semester 2 tahun 2023 mengalami penurunan jumlah ancaman sebesar 0,29%, jumlah ini sebenarnya tidak cukup berarti untuk serangan yang bertujuan membanjiri lalu lintas sistem yang diserang.

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.

Komparasi Semester 1 dan 2

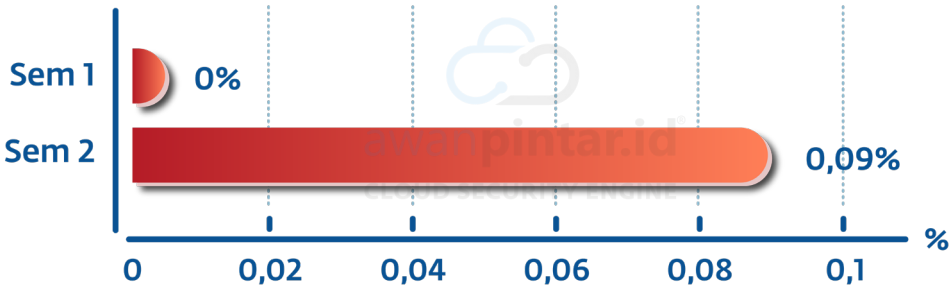


Kategori deteksi a network trojan was detected yaitu ancaman trojan di tanah air menurut kompilasi data AwanPintar.id® persentase serangannya tidak mengalami penurunan atau peningkatan.

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.

Komparasi Semester 1 dan 2



Potensi ancaman pada suspicious traffic merupakan kategori ancaman baru yang masuk dalam daftar 10 besar serangan siber di Indonesia.

10 Negara Kontributor Serangan Siber

Ancaman digital dari negara lain terus berdatangan silih berganti setiap detiknya, meski demikian posisi 10 negara penyumbang serangan terbesar di Indonesia tidak banyak berubah. Negara-negara yang secara konsisten menyerang Indonesia di semester sebelumnya masih mendominasi serangan siber di tanah air saat ini.

Amerika Serikat
25,43%

Tiongkok
12,47%

Hongkong
9,84%

Belanda
4,27%

Singapura
3,85%

Brasil
19,72%

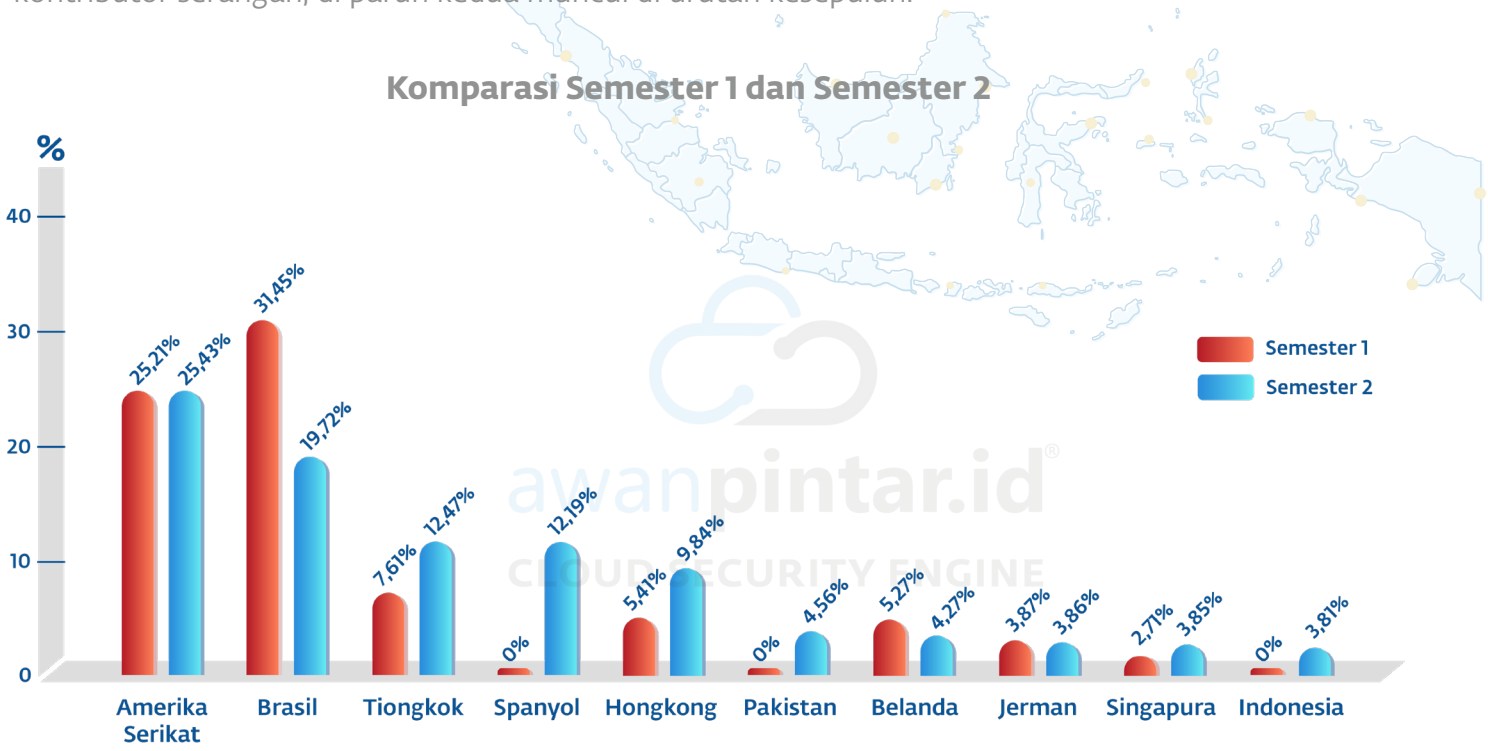
Spanyol
12,19%

Pakistan
4,56%

Jerman
3,86%

Indonesia
3,81%

Dari hasil akumulasi data AwanPintar.id® selama 6 bulan terakhir, terjadi perubahan pada negara penyerang. Perubahan ini terkait dengan perubahan lanskap ancaman siber di Indonesia secara umum, terutama dari dalam negeri, Indonesia yang sebelumnya tidak masuk dalam 10 besar negara kontributor serangan, di paruh kedua muncul di urutan kesepuluh.



Amerika Serikat
Jumlah ancaman meningkat 0,22%

Brasil
Jumlah ancaman menurun 11,73%

Tiongkok
Jumlah ancaman meningkat 4,86%

Belanda
Jumlah ancaman menurun 1,00%

Singapura
Jumlah ancaman meningkat 1,14%

Spanyol
Negara kontributor terbaru

Hongkong
Jumlah ancaman meningkat 4,43%

Pakistan
Negara kontributor terbaru

Jerman
Jumlah ancaman menurun 0,01%

Indonesia
Negara kontributor terbaru

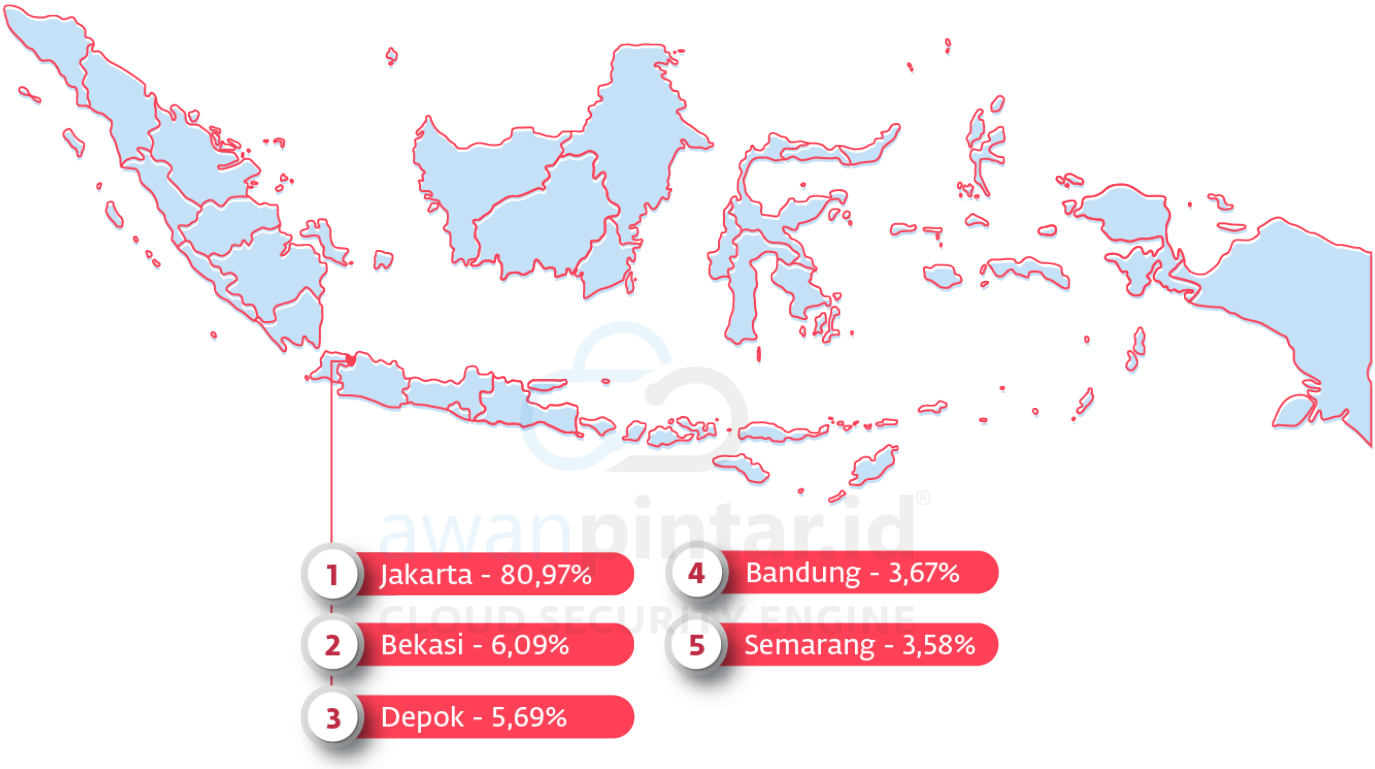
Ada beberapa hal yang perlu menjadi catatan dalam negara kontributor serangan ke Indonesia, mencuatnya tiga negara baru dalam daftar 10 besar, yakni Spanyol, Pakistan dan Indonesia. Hal ini menunjukkan aktivitas ilegal mereka terus meningkat meninggalkan negara-negara yang sebelumnya dominan di semester pertama, terutama Iran yang sebelumnya menduduki posisi 3 besar harus tergusur keluar bersama Korea Selatan dan Perancis. Meningkatnya serangan secara umum menjadi gambaran bahwa eskalasi ancaman digital yang telah dan tengah berlangsung merupakan fakta bahwa infrastruktur internet di Indonesia semakin menjadi sasaran favorit penjahat dunia maya.

Munculnya Indonesia di urutan 10 tidak mengherankan karena pada semester sebelumnya, Indonesia menempati posisi ke 11. Ini menandakan bahwa di dalam infrastruktur Indonesia terjadi serangan dalam negeri yang cukup intens. Menjadi catatan tersendiri bagi Indonesia untuk membenahi beragam sektor untuk menutup kemungkinan celah keamanan atau sumber serangan di infrastruktur dalam negeri.

5 Daerah Penyerang Teratas di Indonesia

Dari 514 kota dan kabupaten yang ada di Indonesia, ada daerah-daerah yang dideteksi oleh AwanPintar.id® sebagai wilayah yang terdepan melakukan serangan siber dalam konteks ancaman dalam negeri.

Berikut 5 daerah penyerang teratas di Indonesia:



AwanPintar.id® terus menambah jumlah *detector* yang disebar di jaringan internet di Indonesia, tujuannya adalah untuk menajamkan validitas angka serangan yang masuk ke tanah air.

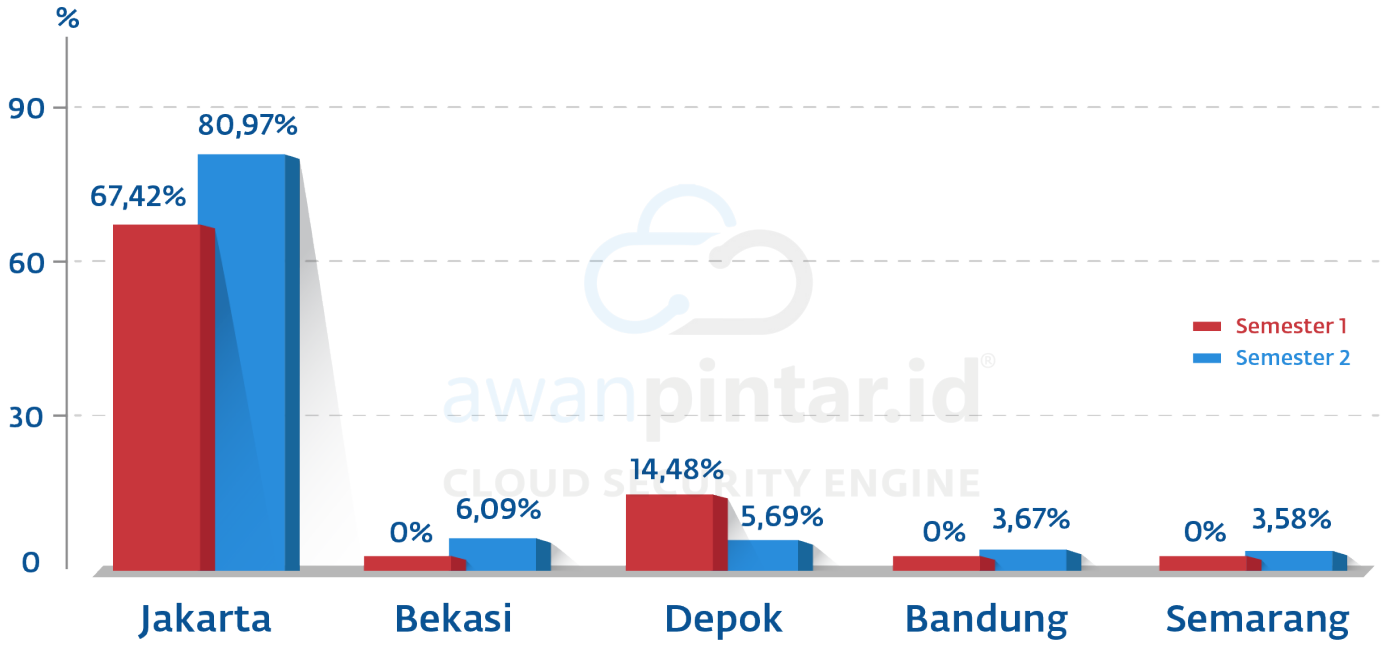
Hasil penjaringan data melalui *detector-detector* tersebut diketahui bahwa ancaman terbesar dari dalam negeri masih datang dari Jakarta dengan jumlah serangan mencapai 80,97% yang mendominasi ancaman daerah di seluruh Indonesia.

Di Indonesia tidak bisa dipungkiri jika pulau Jawa memiliki infrastruktur internet terbaik dibanding dengan pulau lain di Indonesia, sehingga tidak mengejutkan jika 5 ancaman terbesar dari dalam negeri semua berasal dari kota-kota yang ada di pulau Jawa dan didominasi oleh kota-kota yang berada dalam kisaran Jabodetabek.

Ini bisa dilihat dengan Jakarta, Bekasi dan Depok yang berada di urutan 1 sampai dengan 3, lalu disusul Bandung dan Semarang di keempat dan kelima. Seperti kita ketahui bahwa kelima daerah tersebut memiliki infrastruktur dan akses internet yang baik sehingga memudahkan dalam melancarkan ancaman di dalam negeri.

Yang perlu diingat meskipun ancaman tersebut datang dari dalam negeri sendiri, bukan berarti operator serangan tersebut melakukan aksinya dari dalam Indonesia. Pelaku bisa saja berasal dari negara lain yang memanfaatkan perangkat digital yang berhasil mereka kuasai di Indonesia.

Komparasi Semester 1 dan Semester 2



Jakarta
Serangan siber meningkat 13,55%

Bekasi
Daerah penyerang teratas baru

Depok
Serangan siber menurun 8,79%

Bandung
Daerah penyerang teratas baru

Semarang
Daerah penyerang teratas baru

Bekasi sebagai nama daerah baru yang masuk daftar penyerang teratas semakin mengukuhkan bahwa daerah Jabodetabek sebagai penyumbang serangan siber nasional.

Masuknya Bandung dan Semarang sebagai daerah penyerang yang masuk dalam 5 besar teratas sebenarnya berita buruk bagi keamanan siber di Indonesia, mengingat sebelumnya hanya Jabodetabek daerah yang menjadi sumber serangan di dalam negeri.

Ini berarti potensi ancaman domestik meluas ke daerah-daerah lain, menjadi indikasi potensi banyak aset di daerah kemungkinan dikuasai oleh pelaku dari negara lain.

10 IP Penyerang Teratas

Serangan yang masuk ke dalam jaringan internet Indonesia meninggalkan jejak yang dapat ditelusuri dari paket data yang tersimpan, seperti salah satunya adalah IP address penyerang. AwanPintar.id® mencatat 10 besar alamat IP yang aktif melakukan serangan ke dalam sistem jaringan di Indonesia.

IP yang terdeteksi merupakan IP yang disalahgunakan sebagai media menyerang. Sangat dimungkinkan aktor di belakang layar menggunakan IP lain untuk mengkontrol perangkat remote (bot/zombie). Umum dilakukan para penyerang untuk memanfaatkan server atau komputer lain dalam melakukan serangan agar mampu mengelabui dan lokasi mereka tidak terdeteksi pihak yang berwajib.

Yang menarik, beberapa alamat IP tersebut berasal dari Indonesia. Ini dapat diartikan bahwa kerentanan pada perangkat tersebut sudah dieksploitasi orang lain atau memang perangkat tersebut secara aktif melakukan serangan yang disadari ataupun tidak.

Berikut adalah data IP address yang berhasil dijaring oleh AwanPintar.id® saat melakukan serangan:

86.xx.xx.xx Amerika Serikat 32,24%			152.xx.xx.xx Swiss 24,81%
178.xx.xx.xx Belanda 23,04%			2.xx.xx.xx Belanda 10,24%
98.xx.xx.xx Indonesia 7,81%			103.xx.xx.xx Indonesia 7,81%
162.xx.xx.xx Amerika Serikat 7,70%			2.xx.xx.xx Belanda 7,51%
63.xx.xx.xx Indonesia 5,59%			212.xx.xx.xx Bulgaria 5,48%

Ancaman Pencurian Kredensial

Di seluruh dunia, data individu yang paling pribadi dan rahasia telah menjadi target penjahat dunia maya. Serangan dan pelanggaran data di seluruh dunia terus meningkat, hal yang sama berlaku juga di Indonesia.

Bahkan ketika organisasi berupaya melawan dan membentengi diri dengan segala daya dan upaya, penjahat dunia maya terus-menerus menemukan cara baru untuk mengakses dan mengeksploitasi data yang tersimpan.

Dari studi laporan keamanan siber semester kedua diketahui bahwa ancaman-ancaman ini telah mencapai tingkat yang tinggi dibandingkan semester sebelumnya. Dan kini, dengan data lengkap dari tahun 2023, banyak indikator yang menunjukkan bahwa ancaman tersebut semakin memburuk.

1. Administrator Privilege Gain

- Backdoor DoublePulsar 95.86%
- Bypass Autentikasi RDP 3.85%
- FortiOS SSL VPN 0.21%
- Eksploitasi Kerentanan 0.06%
- Serangan Buffer Overflow 0.02%

Backdoor DoublePulsar

(Backdoor DoublePulsar Installing 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 sinilah letak kelemahannya. Dapat dikatakan, Backdoor DoublePulsar merupakan jalan masuk bagi malware lainnya.

Bypass Autentikasi RDP

(HUNTING RDP Authentication Bypass Attempt)

Remote Desktop Protocol (RDP) adalah salah satu protokol komunikasi paling populer untuk sistem pengendalian jarak jauh. RDP hadir dengan semua sistem operasi Windows saat ini, dan antarmuka pengguna grafisnya menjadikannya alat akses jarak jauh yang mudah digunakan. Selain itu, Microsoft memposisikannya sebagai metode default untuk mengelola mesin virtual Azure yang menjalankan Windows.

Bahayanya port RDP terbuka, penjahat dunia maya dapat masuk dan melakukan eksploitasi berbahaya. Mereka dapat memanfaatkan Network Level Authentication (NLA) sebagai pengamanan dengan memicu pemutusan RDP sementara dan pemulihannya yang menyebabkan keadaan tidak terkunci.

Dengan penyerang memicu kerentanan, mereka akan dapat mengakses sesi yang terpengaruh setelah tersambung kembali. Kerentanan ini juga muncul untuk mem-bypass sistem autentikasi multi-faktor yang terintegrasi dengan layar login Windows.

FortiOS SSL VPN

(EXPLOIT FortiOS SSL VPN-Information Disclosure (CVE-2018-13379)

Kerentanan ini adalah cacat pra-autentikasi, yang berarti penyerang tidak perlu diautentikasi ke perangkat yang rentan untuk mengeksploitasinya. Eksploitasi yang berhasil akan memungkinkan penyerang membaca konten file sesi "sslvpn_websesion" yang berisi nama pengguna dan kata sandi dalam plaintext.

Kerentanan konfigurasi default di FortiGate SSL VPN. Di bawah konfigurasi default, ketika server Lightweight Directory Access Protocol (LDAP) mengirim permintaan koneksi ke perangkat FortiGate, sertifikat tidak diverifikasi. Untuk mengeksploitasi kerentanan, penyerang dapat terhubung ke perangkat FortiGate yang rentan dengan menyamar sebagai server LDAP. Eksploitasi yang berhasil akan memungkinkan penyerang mengambil informasi sensitif yang ditujukan untuk server LDAP yang sah.

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.

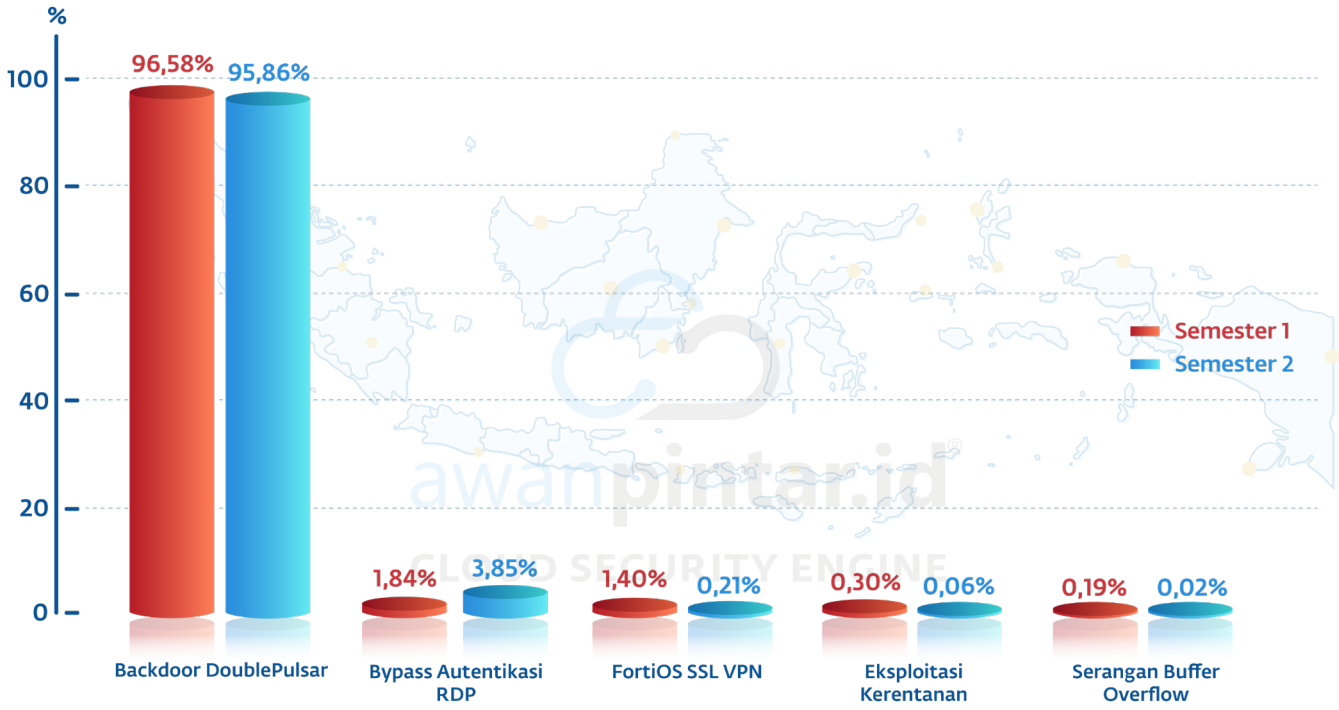
Serangan Buffer Overflow

(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.

Komparasi Administrator Privilege Gain Semester 1 dan Semester 2



Backdoor DoublePulsar
Jumlah serangan menurun 0,72%

Bypass Autentikasi RDP
Jumlah serangan meningkat 2,01%

FortiOS SSL VPN
Jumlah serangan menurun 1,19%

Eksploitasi Kerentanan
Jumlah serangan menurun 0,24%

Serangan Buffer Overflow
Jumlah serangan menurun 0,17%

Perbandingan serangan dalam upaya pencurian kredensial mengalami kenaikan. Meski demikian, jenis serangan yang dilakukan berkurang dari sebelumnya, seperti upaya eksploitasi Mikrotik Winbox, Brute Force Admin, Eksploitasi Realtek. Ini menunjukan respons positif terhadap laporan ancaman digital sebelumnya.

2. Information Leak

- SCAN MS Terminal Server Traffic on Non-standard Port 66,04%
- SCAN NMAP sS window 1024 18,84%
- POLICY CURL User Agent 10,22%
- INFO User-Agent (python-requests) 2,61%
- SCAN Potential VNC Scan 5900-5920 2,29%
- SCAN Potential SSH Scan 0,56%

Serangan-serangan ini semakin berdampak karena masyarakat kini lebih banyak menjalani kehidupan mereka secara online, yang berarti bahwa perusahaan, pemerintah, dan organisasi lainnya mengumpulkan lebih banyak data pribadi, terkadang dengan sedikit pilihan dari individu.

Dan karena sebagian besar data pribadi seseorang dapat dieksploitasi dan dijual untuk mendapatkan keuntungan yang besar, data ini menjadi target yang semakin meningkat bagi para penjahat dunia maya.

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.

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 User Agent
(POLICY CURL User Agent)

User agent berisi informasi tentang aplikasi dan perangkat tempat situs web diakses, ditambah informasi lain yang diperlukan untuk menampilkan halaman yang diminta dengan benar. Jika agen pengguna berisi data yang berlebihan, data ini dapat digunakan dalam serangan selanjutnya pada perangkat pengguna.

Eksploitasi Server Web
(INFO User-Agent (python-requests))

Bocornya informasi dapat terjadi dengan mudah di dunia maya. Deteksi ini berguna untuk menemukan banyak eksploitasi server web.

String User-Agent default untuk proyek Python menggunakan pustaka python-requests secara harfiah adalah "permintaan-python [versionNumber]" kecuali jika diubah. Musuh yang menggunakan kode Python sering lupa mengubah nilai ini untuk menyamar sebagai UA lainnya.

Dengan sendirinya, Anda akan melihat User Agent permintaan python ribuan kali untuk server web mana pun di internet.

Eksploitasi VNC
(SCAN Potential VNC Scan 5900-5920)

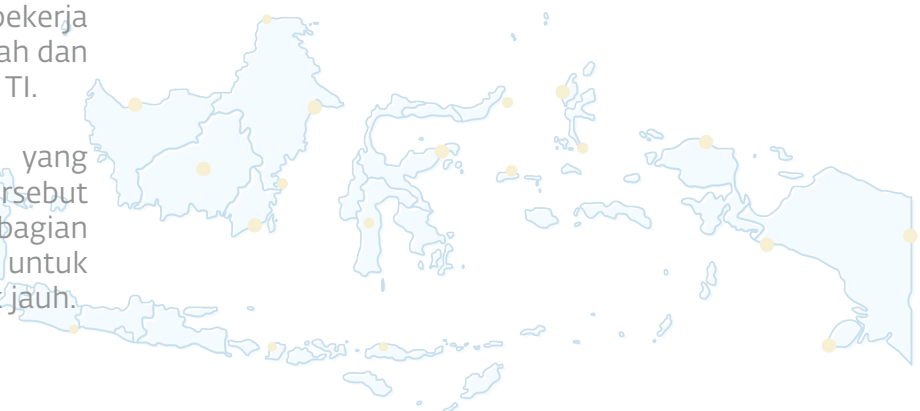
Virtual Network Computing (VNC) adalah sistem kendali desktop jarak jauh yang tidak bergantung pada platform. Ada banyak implementasi VNC (LibVNC, TightVNC, UltraVNC, dll.) yang berjalan di Windows, Linux, macOS, iOS, Android, dan sistem operasi lainnya. VNC menggunakan port 5900 atau 5800. VNC digunakan 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.

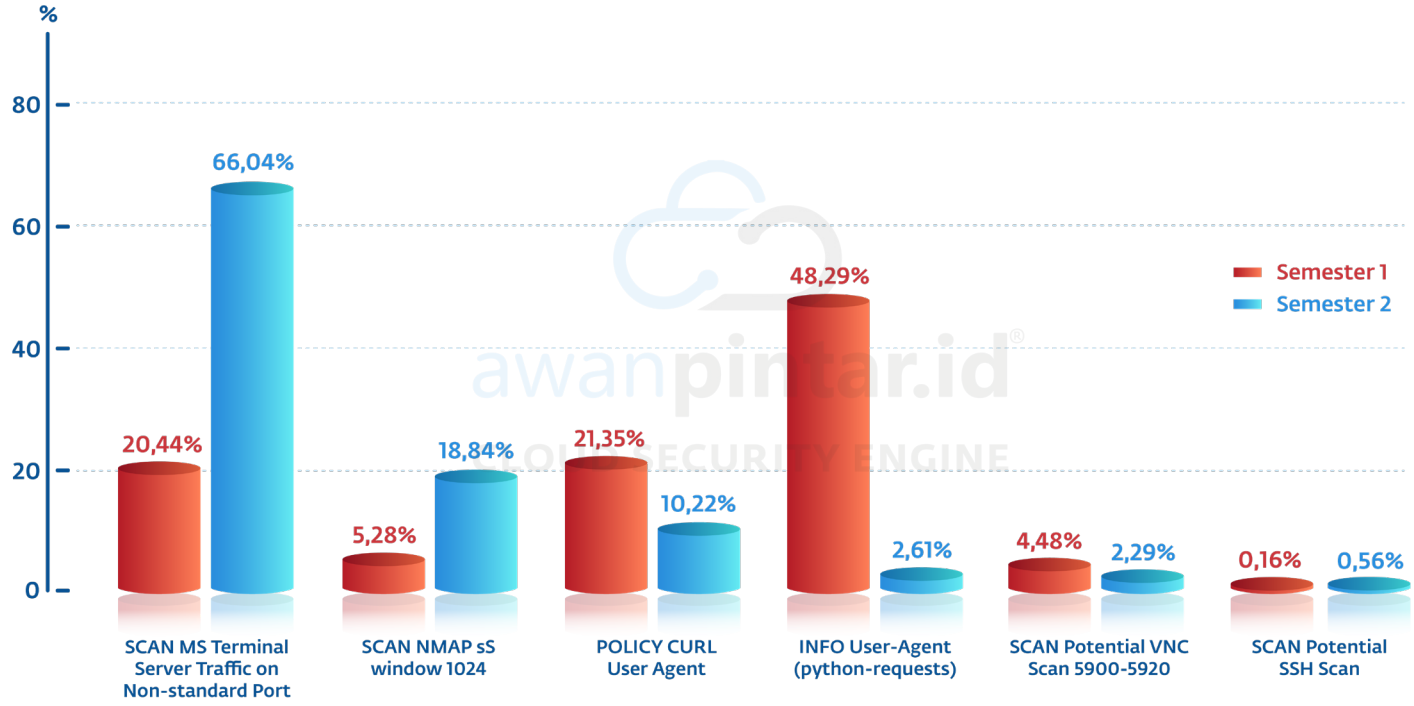
Brute Force SSH
(SCAN Potential SSH Scan)

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.



Komparasi Information Leak Semester 1 dan Semester 2



SCAN MS Terminal Server Traffic on Non-standard Port
Jumlah serangan meningkat 45,60%

SCAN NMAP sS window 1024
Jumlah serangan meningkat 13,56%

POLICY CURL User Agent
Jumlah serangan menurun 11,13%

INFO User-Agent (python-requests)
Jumlah serangan menurun 45,68%

SCAN Potential VNC Scan 5900-5920
Jumlah serangan menurun 2,19%

SCAN Potential SSH Scan
Jumlah serangan Meningkat 0,40%

Information leak atau kebocoran data pada Semester 2 secara umum menunjukkan grafik yang menurun. Penurunan diikuti dengan jenis pilihan serangan yang ikut berkurang. Sentimen positif ini merupakan kabar baik, adanya peningkatan kesadaran keamanan pengguna internet di Indonesia dalam melindungi kredensialnya.

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.

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 berbagai cara seperti dengan phising misalnya.

Malware

Mencakup kategori luas perangkat lunak berbahaya yang dirancang untuk mengeksploitasi, merusak, atau mendapatkan akses tidak sah ke sistem komputer.

Tidak seperti spam, malware dibuat dengan niat jahat dan tidak bergantung pada iklan. 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.

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

Juli	3,77%	Agustus	6,42%
September	15,72%	Oktober	3,56%
November	9,04%	Desember	2,17%

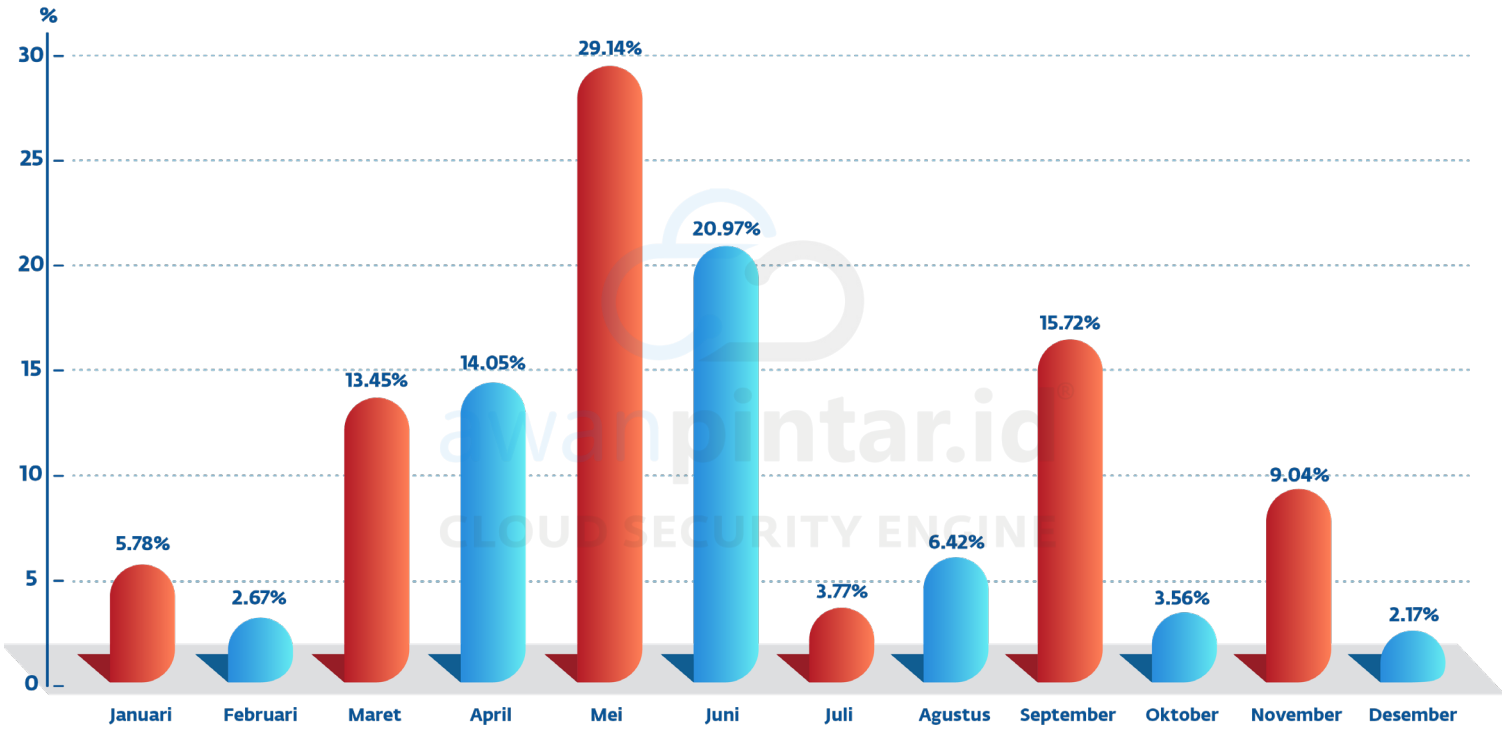
Memasuki paruh kedua tahun 2023 serangan spam malware tidak semasif dan seaktif 6 bulan pertama tahun ini. Anomali terjadi di bulan September, selebihnya intensitas serangan terus menurun.

Bulan September memang menjadi pengecualian karena di belahan dunia lain di bulan yang sama terjadi eskalasi serangan siber yang tinggi. September sepertinya menjadi bulan siber terburuk bagi dunia secara umum tak terkecuali Indonesia.

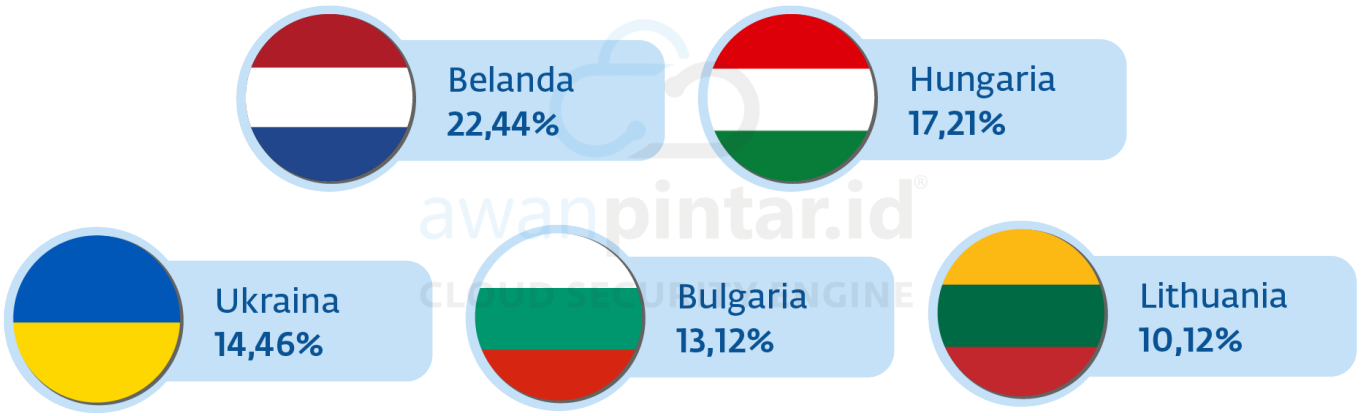
Yang perlu diperhatikan pula adalah turunnya persentase serangan spam dan malware di bulan Desember yang merupakan terendah tidak hanya di semester kedua tahun ini tetapi juga dalam satu tahun belakangan.

Menurunnya jumlah spam dan malware harus diwaspadai karena ini bisa jadi merupakan indikator bahwa pelaku serangan spam & malware melakukan serangan mereka lebih tertarget.

Persentase Serangan Selama 1 Tahun



5 Negara Pengirim Malware

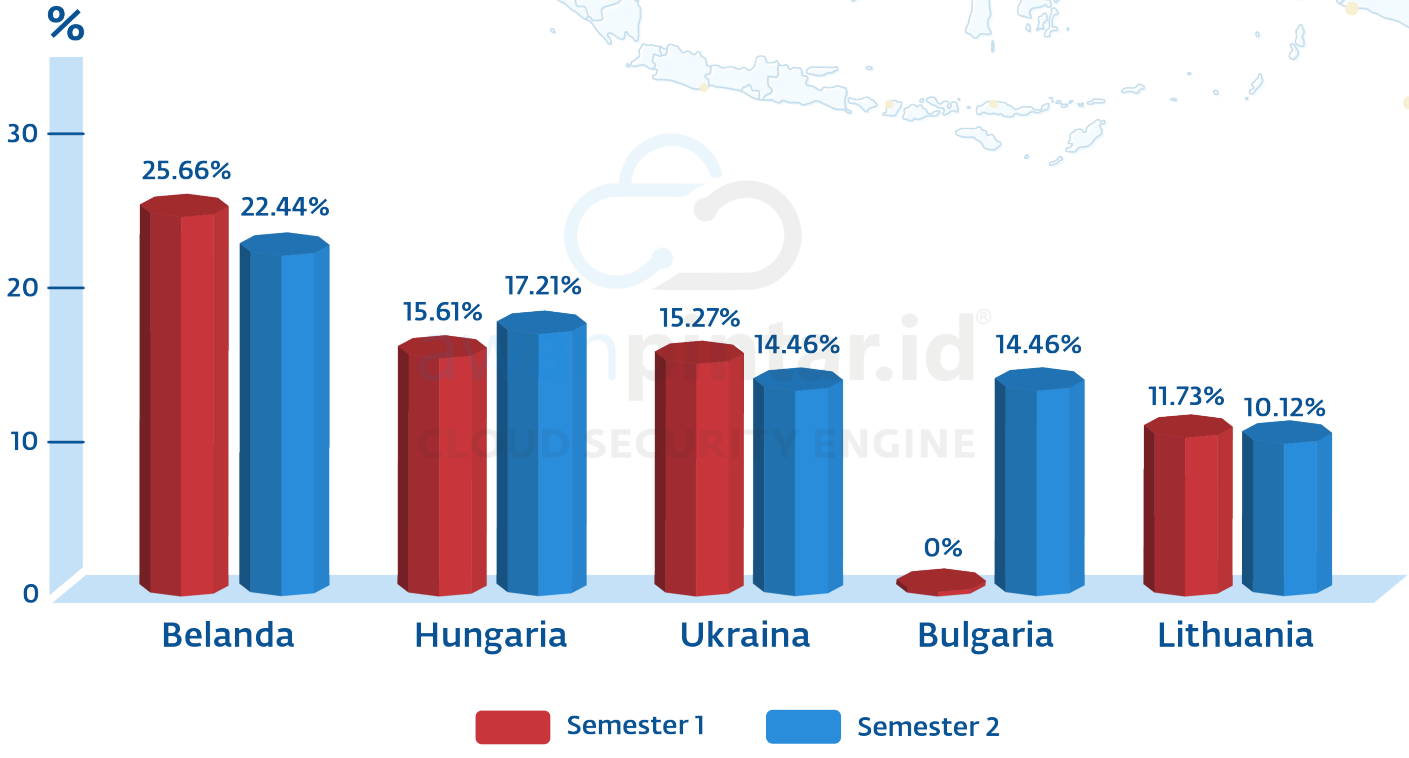


Email akan selalu menjadi sarana favorit bagi penjahat dunia maya untuk menyebar email secara masif maupun tertarget. Selain murah dan mudah, email masih menjadi alat komunikasi utama bagi individu dan perusahaan, selain itu banyak aktivitas online selalu menyertakan email sebagai syarat utama.

Menariknya dari 5 negara pengirim malware terbanyak ke Indonesia yang dideteksi oleh AwanPintar.id®, hanya Belanda yang masuk dalam 10 besar negara yang berkontribusi dalam serangan digital secara umum di Indonesia.

Amerika Serikat yang menduduki posisi kedua sebagai negara terbesar pengirim malware di semester 1 tahun 2023 malah keluar dan berada di posisi 10, digantikan Bulgaria yang semakin mengokohkan dominasi negara Eropa sebagai negara yang menjadikan Indonesia sebagai sasaran.

Komparasi Negara Pengirim Malware Semester 1 dan 2



Belanda
Aktivitas malware menurun 3,22%

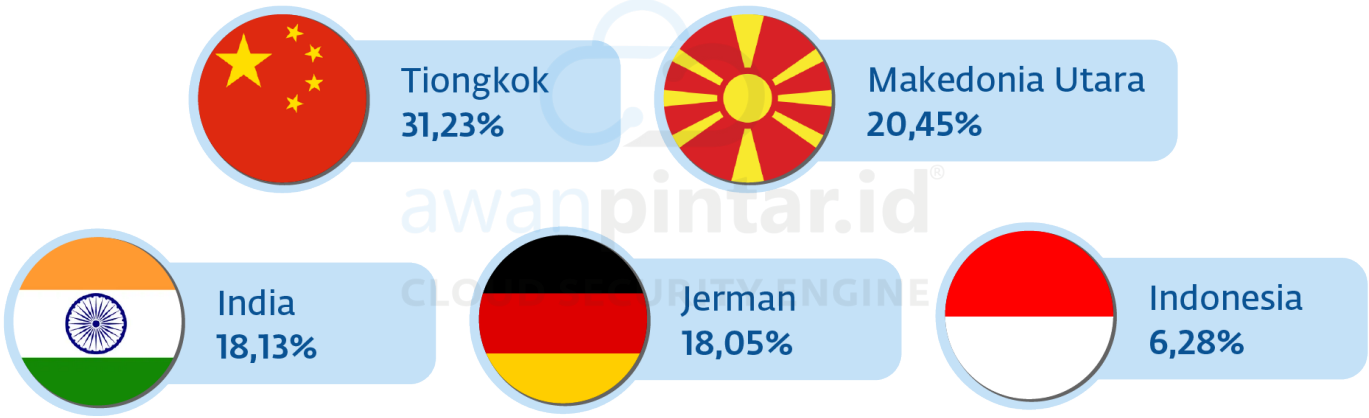
Hungaria
Aktivitas malware meningkat 1,6%

Ukraina
Aktivitas malware menurun 0,81%

Bulgaria
Negara baru pengirim malware

Lithuania
Aktivitas malware menurun 1,61%

5 Negara Pengirim Spam Terbanyak



Ada banyak alasan mengapa penjahat siber lebih memilih serangan spam email dibandingkan metode social engineering lainnya. Ini karena email tersebar luas, masih banyak penggunanya yang tidak memiliki kesadaran keamanan siber sehingga mereka mudah untuk ditargetkan.

Ini juga adalah metode penargetan yang mudah dan sederhana, karena tidak memerlukan keahlian teknis, penjahat tidak perlu meretas sistem atau membuat kata sandi agar berhasil.

Setelah email terkirim, yang perlu mereka lakukan hanyalah menunggu balasan, klik, pengunduhan lampiran. Tugas utama mereka hanyalah mengirim email itu sendiri lalu mengakses jaringan melalui malware dan pastinya tidak perlu melewati protokol keamanan yang ketat.

Serangan phising dapat melakukan serangan yang ditargetkan (spear phishing) atau serangan jaringan luas yang tidak ditargetkan untuk mendapatkan pijakan sebanyak mungkin.

Teknik serbaguna dengan banyak varian, phising, spear phising, spear phising internal dan ini dapat digunakan untuk mengirimkan berbagai jenis kode berbahaya seperti ransomware.

Di dalam negeri, AwanPintar.id® memiliki kemampuan untuk mendeteksi dan mendata serangan spam email yang masuk ke Indonesia, dari data tersebut diketahui bahwa 5 negara teratas pengirim spam terbanyak masih sama dilakukan oleh negara yang menjadi pengirim spam terbanyak di Semester 1 tahun 2023.

Kelima negara secara konsisten melakukan spam besar-besaran ke Indonesia. Perubahan yang paling terlihat adalah bagaimana Indonesia sebagai salah satu negara pengirim spam terbanyak juga masuk dalam 10 besar negara yang melakukan serangan digital secara umum ke Indonesia, bersama dengan Tiongkok yang menempati posisi ketiga.

Port Favorit
Peretas

10 PORT PALING RENTAN DI INDONESIA

Komputer modern memiliki berbagai port yang dapat Anda gunakan untuk menyambungkan periferal ke komputer Anda. Port dapat menyediakan berbagai fungsi, seperti mengirim dan menerima informasi, menyambung ke layar, atau memasang alat berguna seperti mouse atau tablet.

Selain memiliki banyak fungsi dan manfaat untuk komputer, port juga dapat menjadi jalan masuk bagi penjahat dunia maya untuk melakukan penetrasi ke ekosistem komputer, menyebarkan malware dan berbagai hal lainnya.

Komparasi Port Paling Rentan Semester 1 dan Semester 2

Port	Semester 1	Semester 2	Keterangan
Port UDP 53	84,55%	93,36%	Jumlah peningkatan 8,81%
Port TCP 445	5,59%	4,60%	Jumlah penurunan 0,99%
Port UDP 1900	5,35%	1,06%	Jumlah penurunan 4,29%
Port TCP 5900	2,37%	0,40%	Jumlah penurunan 1,97%
Port TCP 22	0,50%	0,17%	Jumlah penurunan 0,33%
Port TCP 110	0,37%	0,13%	Jumlah penurunan 0,24%
Port UDP 5060	0,83%	0,08%	Jumlah penurunan 0,75%
Port TCP 8080	0%	0,08%	Terbaru dalam daftar 10 port terentan
Port TCP 3389	0,21%	0,08%	Jumlah penurunan 0,14%
Port UDP 161	0%	0,04%	Terbaru dalam daftar 10 port terentan

Serangan terhadap port paling rentan di Indonesia pada paruh kedua tahun 2023 meningkat namun tersegmentasi pada port tertentu yang menerima ancaman paling dominan di antara yang lainnya.

Port 8080 dan port 161 muncul di permukaan masuk dalam 10 port terentan menggusur port 25565 dan port 21 sebagai momok baru.

Persentase merupakan cerminan bahwa masih banyak port yang belum mendapat pengamanan secara memadai. Dikhawatirkan kedepan dampaknya bisa sangat buruk terutama bagi keamanan siber nasional secara umum.

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 dan 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 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 Wi-Fi 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 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 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 110

Port 110 digunakan oleh protokol POP3 untuk akses tidak terenkripsi ke surat elektronik. Port ditujukan bagi pengguna akhir untuk terhubung ke server email untuk mengambil pesan.

Pop3 "Post Office Protocol" digunakan oleh klien email untuk pengambilan email mereka dari server "post office" email yang ditunjuk. Klien email seperti Microsoft Outlook, Netscape, Eudora, dan banyak lainnya, terhubung ke port 110 dari server email jarak jauh, kemudian menggunakan protokol POP3 untuk mengambil email mereka.

Mereka mengawali dengan mengidentifikasi dan mengautentikasi diri mereka sendiri dengan masuk ke server email jarak jauh menggunakan informasi akun email mereka. Setelah melakukannya, mereka diizinkan untuk

melihat dan mengunduh email menunggu mereka.

Peretas berpotensi mendengarkan lalu lintas jaringan atau data dalam email menggunakan POP3 karena agen transportasi dapat disusupi dengan cara apa pun.

Port UDP 5060

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.

Session Initiation Protocol (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 TCP 8080

Port 8080 tidak hanya digunakan bagi HTTP, tapi juga bagi proxy karena masih berjalan pada satu layanan yang sama. Port nomor 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 sering kali melibatkan SQL injections, cross-site scripting, serangan DDoS, dan pemalsuan permintaan.

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 didedikasikan untuk Simple Network Management Protocol (SNMP), yang Anda gunakan untuk mengelola dan memantau perangkat jaringan dari jarak jauh. Manajer SNMP menggunakan port 161 untuk mengirimkan perintah ke agen SNMP di perangkat.

Simple Network Management Protocol (SNMP) adalah seperangkat protokol untuk manajemen

dan pemantauan jaringan. Kebanyakan orang menggunakan SNMP untuk memantau perangkat di jaringan seperti firewall, router, switch, server, printer, bridge, drive NAS, UPS, dan banyak lagi.

Dengan kata lain, SNMP adalah protokol yang digunakan secara luas dan juga merupakan bagian penting dari strategi manajemen jaringan apa pun. Hasilnya, administrator TI menggunakan pemantauan SNMP untuk mendeteksi dan mengelola perangkat, mendapatkan wawasan tentang kinerja dan ketersediaan, serta memastikan kesehatan jaringan mereka.

Kerentanan dan Masalah Keamanan Port 161

Ada masalah kerentanan serius terkait penggunaan SNMP melalui port 161, yang dapat Anda mitigasi dengan menggunakan protokol versi terbaru dan memblokir port di firewall saat Anda tidak memerlukannya untuk dibuka.

SNMP versi satu dan dua sangat rentan terhadap serangan, karena pesan SNMP dalam versi protokol ini dikirim tidak terenkripsi. Hal ini memungkinkan peretas membaca data sensitif, seperti kredensial, dengan menggunakan packet sniffer.

Protokol versi tiga yang dikenal sebagai SNMPv3 memberikan keamanan yang jauh lebih baik dengan menambahkan fitur seperti enkripsi, autentikasi, dan kontrol akses. Namun, penting untuk dicatat bahwa hal ini tidak membuatnya kebal terhadap serangan. Satu-satunya cara pasti untuk melakukan ini adalah dengan memblokir port 161 di firewall Anda.

Common Vulnerability Exposures (CVE)

10 KERENTANAN TERTINGGI

Dalam kurun waktu enam bulan terakhir banyak hal telah terjadi pada Common Vulnerability & Exposures, serangan pada kerentanan yang fluktuatif sampai ancaman kerentanan baru yang muncul. Berikut data terbaru Semester 2 tahun 2023 dari AwanPintar.id® dan komparasinya.

CVE-2020-11899	97,59%	CVE-2020-2551	0,05%
CVE-2018-13379	1,62%	CVE-2022-27255	0,05%
CVE-2020-11910	0,43%	CVE-2023-46604	0,01%
CVE-2021-44228	0,15%	CVE-2020-11900	0,01%
CVE-2019-11500	0,06%	CVE-2021-35394	0,01%

CVE-2020-11899

CVSS 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 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:

- Minimalkan 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 Jaringan Pribadi Virtual (VPN), mengetahui VPN mungkin memiliki kerentanan maka harus diperbarui ke versi terbaru yang tersedia. Ketahuilah juga bahwa VPN hanya seaman perangkatnya yang terhubung.

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.

Sistem 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.

- 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.
- Nonaktifkan 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.

CVE-2020-11910

CVSS: 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-2021-44228

CVSS: 10 Critical

CVE-2021-44228 adalah kerentanan eksekusi kode jarak jauh yang memengaruhi banyak versi library Apache Log4j. Kerentanan ini sangat kritis karena CVE-2021-44228 memungkinkan pelaku ancaman untuk mengambil kendali penuh atas server tanpa memerlukan autentikasi apa pun. Dalam hal tingkat keparahan diberi peringkat 10 dari 10 tingkat kerentanan.

CVE-2021-45046 adalah kerentanan yang baru ditemukan sehubungan dengan CVE-2021-44228 yang muncul karena perbaikan sebelumnya tidak berfungsi dalam konfigurasi non-default tertentu.

Karena kerentanan ini, penyerang hanya perlu memicu kejadian log yang berisi string berbahaya (khususnya Penamaan Java dan URL Antarmuka Direktori) yang kemudian secara otomatis dicatat dan dibuka oleh Log4j.

Dampak
Beberapa pengguna mungkin khawatir bahwa Log4j versi 1.x dipengaruhi oleh kerentanan. Untungnya tidak demikian karena penyebaran Log4j ini tidak menawarkan mekanisme pencarian JNDI di tingkat pesan.

Karena library logging Java banyak digunakan oleh perusahaan seperti Minecraft, Uber, Airbnb, dan Pinterest serta lebih dari 9937 perusahaan lain (menurut Stackshare), akan ada banyak aplikasi yang saat ini rentan terhadap CVE-2021-44228.

Produk Terdampak
Versi 2.0 dan 2.14.1 dari Log4j keduanya terpengaruh sementara Java Development Kit (JDK) versi 6u211, 7u201, 8u191 dan 11.0.1 tidak terpengaruh.

Mitigasi Kerentanan
Intinya dengan mengikuti saran mitigasi yang diberikan oleh Apache:
- Identifikasi aplikasi yang menggunakan dependensi Log4j di bawah 2.15.0 (seperti di atas).
- Tingkatkan dependensi Log4j ke setidaknya versi 2.17.0 (2.15.0 dan 2.16.0 telah mengetahui kerentanan Denial of Service [DoS], dikutip dalam CVE-2021-45046 dan CVE-2021-45105, jadi rekomendasi dari Apache adalah menggunakan 2.17.0 dan yang lebih baru).

CVE-2019-11500
CVSS 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 mengompromikan 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-2020-2551
CVSS: 9.8 Critical

Eksekusi kode jarak jauh WebLogic (CVE-2020-2551) dapat melewati patch keamanan yang dirilis oleh Oracle pada Oktober 2019. IIOP mengakses objek jarak jauh melalui antarmuka Java yang diaktifkan secara default.

WebLogic dari Oracle, adalah server aplikasi Java untuk mengembangkan, mengintegrasikan, menyebarkan, dan mengelola aplikasi web terdistribusi skala besar, aplikasi jaringan, dan aplikasi database. WebLogic dimulai adalah server aplikasi Java (J2EE) pertama yang sukses secara komersial dan masih menjadi salah satu pemimpin di pasar.

Dampak
Pelaku dapat mengakses antarmuka ini dari jarak jauh tanpa autentikasi di Server WebLogic melalui IIOP, mengirim data yang dibuat dengan

hati-hati, dan mengeksekusi kode arbitrer di server target. Skor CVSS adalah 9,8.

Produk Dampak
Versi yang terkena dampak:
- Web Logic Server 10.3.6.0.0
- Web Logic Server 12.1.3.0.0
- Web Logic Server 12.2.1.3.0
- Web Logic Server 12.2.1.4.0

Mitigasi Kerentanan
1. Oracle telah merilis patch resmi untuk memperbaiki kerentanan ini. Silakan merujuk ke https://www.oracle.com/security-alerts/cpujan2020.html
2. Eksploitasi kerentanan untuk sementara dapat dimitigasi dengan menutup IIOP. Untuk menutup IIOP lakukan hal berikut:
   - Di konsol WebLogic, pilih "Layanan" > "AdminServer" > "Protokol" dan hapus centang "Aktifkan IIOP".
   - Mulai ulang proyek WebLogic untuk menerapkan konfigurasi.

CVE-2022-27255
CVSS: 9.8 Critical

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

CVE Numbering Authority (CNA): 8.5 (High)

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 terpengaruh 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-2023-46604
CVSS: 9.8 High

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 dipatch. 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-2021-24563
CVSS: 6.1 Medium

Netralisasi input yang tidak tepat selama pembuatan halaman web (Cross-site Scripting).

Plugin WordPress Pengunggah Frontend hingga 1.3.2 tidak mencegah pengunggahan file HTML melalui formulirnya, memungkinkan pengguna yang tidak diautentikasi untuk mengunggah file HTML berbahaya yang berisi JavaScript misalnya, yang akan dipicu ketika seseorang mengakses file secara langsung.

Produk tidak menetralisir atau salah menetralkan masukan yang dapat dikontrol pengguna sebelum ditempatkan dalam keluaran yang digunakan sebagai halaman web yang disajikan kepada pengguna lain.

Dampak
Setelah skrip berbahaya disuntikkan, penyerang dapat melakukan berbagai aktivitas jahat. Penyerang dapat mentransfer informasi pribadi, seperti cookie yang mungkin berisi informasi sesi, dari mesin korban ke penyerang.

Penyerang dapat mengirimkan permintaan jahat ke situs web atas nama korban, yang bisa sangat berbahaya bagi situs tersebut jika korban memiliki hak administrator untuk mengelola situs tersebut.

Serangan phishing dapat digunakan untuk meniru situs web tepercaya dan mengelabui korban agar memasukkan kata sandi, sehingga penyerang dapat menyusup ke akun korban di situs web tersebut.

Terakhir, skrip tersebut dapat mengeksploitasi kerentanan di browser web itu sendiri yang mungkin mengambil alih mesin korban, terkadang disebut sebagai “drive by download” Dalam banyak kasus, serangan dapat dilancarkan tanpa korban menyadarinya.

Bahkan dengan pengguna yang berhati-hati, penyerang sering kali menggunakan berbagai metode untuk menyandikan bagian serangan yang berbahaya, seperti pengkodean URL atau Unicode, sehingga permintaan tersebut terlihat tidak terlalu mencurigakan.

Produk Terdampak
Perangkat lunak yang terpengaruh Frontend_uploader-Frontend_uploader_project * 1.3.2

Mitigasi Kerentanan
Berikut beberapa langkah mitigasi yang dapat dilakukan untuk mencegah eksploitasi kerentanan adalah sebagai berikut:

- Gunakan library atau framework yang terverifikasi yang tidak memungkinkan terjadinya kelemahan ini atau menyediakan konstruksi yang membuat kelemahan ini lebih mudah dihindari.
- Contoh library dan framework yang memudahkan menghasilkan keluaran yang dikodekan dengan benar mencakup library Anti-XSS Microsoft, modul Pengkodean OWASP ESAPI, dan Apache Wicket.
- Untuk setiap data yang akan dikeluarkan ke halaman web lain, terutama data apa pun yang diterima dari masukan eksternal, gunakan pengkodean yang sesuai pada semua karakter non-alfanumerik.
- Gunakan dan tentukan pengkodean output yang dapat ditangani oleh komponen hilir yang membaca output. Pengkodean umum mencakup ISO-8859-1, UTF-7, dan UTF-8. Jika pengkodean tidak ditentukan, komponen hilir dapat memilih pengkodean yang berbeda, baik dengan mengasumsikan pengkodean default atau secara otomatis menyimpulkan pengkodean mana yang sedang digunakan, yang bisa jadi salah. Ketika pengkodean tidak konsisten, komponen hilir mungkin memperlakukan beberapa urutan karakter atau byte sebagai sesuatu yang istimewa, meskipun mereka tidak istimewa dalam pengkodean aslinya. Penyerang mungkin dapat mengeksploitasi perbedaan ini dan melakukan serangan injeksi; mereka bahkan mungkin dapat melewati mekanisme perlindungan yang menganggap pengkodean asli juga digunakan oleh komponen hilir.

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 memitigasi 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-2019-9621
CVSS: 7.5 High

Diidentifikasi pada 30 April 2019 pada Zimbra Collaboration Autodiscover Servlet XXE dan ProxyServlet SSRF. Modul ini mengeksploitasi kerentanan entitas eksternal XML dan pemalsuan permintaan sisi server untuk mendapatkan eksekusi kode yang tidak diautentikasi pada Zimbra Collaboration Suite.

Dampak
Kredensial zimbra digunakan untuk mendapatkan cookie autentikasi pengguna dengan cookie message.admin AuthRequest. Setelah mendapatkan cookie admin, servlet unggahan klien digunakan untuk mengunggah webshell JSP yang dapat dipicu dari server web untuk mendapatkan eksekusi perintah di host.

Produk Terdampak
Masalah tersebut dilaporkan memengaruhi Zimbra Collaboration Suite v8.5 hingga v8.7.11. Modul ini diuji dengan Zimbra Rilis 8.7.1.GA.1670 dengan sistem operasi LINUX UBUNTU 16.64, LINUX UBUNTU16_64 edisi FOSS.

Mitigasi Kerentanan
Untuk mengamankan versi Zimbra yang didukung (8.7 dan 8.8)
- Pengguna Zimbra yang menjalankan versi 8.8 harus meningkatkan ke 8.8.10 Patch 7 atau 8.8.11 Patch 3.
- Pengguna Zimbra yang menjalankan versi dukungan jangka panjang (LTS) 8.7.11 harus meningkatkan ke 8.7.11 Patch 10.

Untuk mengamankan versi Zimbra yang tidak didukung (8.6 dan sebelumnya)
- Pengguna yang menjalankan 8.6 harus meningkatkan ke Patch 13.
- Zimbra versi lama rentan hingga ditingkatkan ke versi yang didukung.

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 UDPServer. 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.

Komparasi Common Vulnerability & Exposures Semester 1 dan 2

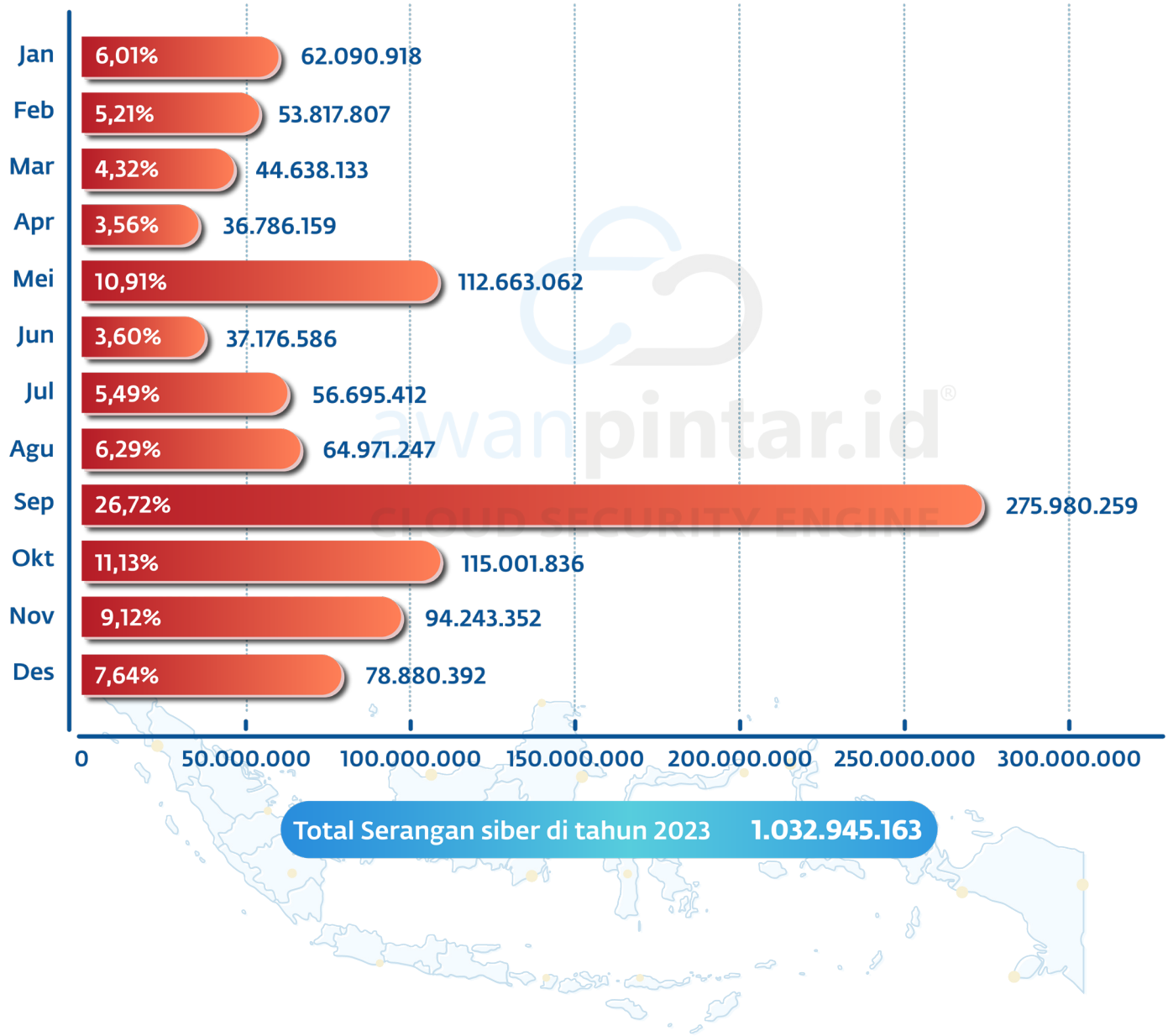
CVE	Semester 1	Semester 2	Keterangan
CVE-2020-11899	11,65%	97,59%	Meningkat 85,94%
CVE-2018-13379	54,09%	1,62%	Menurun 52,47%
CVE-2020-11910	0,39%	0,43%	Meningkat 0,04%
CVE-2021-44228	1,81%	0,15%	Menurun 1,66%
CVE-2019-11500	0,39%	0,06%	Menurun 0,22%
CVE-2020-2551	0,16%	0,05%	Menurun 0,11%
CVE-2022-27255	6,69%	0,05%	Menurun 0,64%
CVE-2023-46604	0%	0,01%	Ancaman CVE terbaru
CVE-2020-11900	0%	0,01%	Ancaman CVE terbaru
CVE-2021-35394	0%	0,01%	Ancaman CVE terbaru

Kesimpulan Laporan 2023

TREN SERANGAN SELAMA TAHUN 2023

Seiring kemajuan teknologi, ancaman keamanan siber yang ditimbulkan oleh peretas jahat, pembuat malware, dan penjahat siber lainnya juga meningkat. Bahaya digital semakin sering terjadi dan semakin parah, dan tidak ada bisnis atau organisasi yang mampu mengabaikannya.

Seperti halnya yang terjadi di tanah air, bahaya digital terus terjadi tanpa henti setiap detiknya. Untuk memberi gambaran lebih jelas tentang tren serangan yang ada di Indonesia tahun ini, berikut kompilasi statistik serangan siber selama tahun 2023. Data berikut merupakan nilai rata-rata serangan pada sebuah perangkat yang mengunakan alamat IP Public dan terhubung ke internet.



Fluktuasi serangan pada suatu negara adalah hal yang umum terjadi, kejanggalan seperti anomali lalu lintas serangan yang tiba-tiba melonjak signifikan seperti yang terjadi di bulan Mei, September dan Oktober yang perlu mendapat perhatian lebih khusus karena masuk dalam tiga serangan tertinggi selama tahun 2023.

Laju serangan di ketiga bulan tersebut berubah abnormal bukan tanpa sebab, jika dicermati lebih teliti, pada bulan Mei di Indonesia terjadi insiden ransomware LockBit yang menginvasi beberapa institusi. Keberhasilan serangan ini disinyalir kemudian menjadi katalis bagi penjahat siber lain untuk semakin intens meningkatkan serangannya di Indonesia.

Hal yang sama berlaku pada bulan September dan Oktober di mana serangan siber serupa gelombang kedua kembali terjadi membuat Indonesia kembali dibanjiri oleh ancaman digital yang lebih besar. Sebagai catatan, pada bulan yang sama, di Indonesia juga terjadi insiden serangan Ransomware di salah satu lembaga keuangan.

Sepanjang tahun 2023 penjahat dunia maya terus-menerus menemukan cara baru untuk menembus pertahanan keamanan, mencuri data berharga, dan mengganggu operasi. Secara umum selama 2023 banyak insiden terjadi di Indonesia, seperti pencurian kredensial, phising, social engineering, DDoS, ransomware yang terus tumbuh dan semakin marak dengan berbagai trik dan strateginya.

Angka-angka di atas merupakan cerminan derasnya serangan yang masuk, yang berusaha mengeksploitasi semua lini infrastruktur tanah air yang berimbas pada keamanan jaringan internet nasional.

COMMON VULNERABILITY & EXPOSURES 2023

Sepanjang tahun 2023 AwanPintar.id® mendeteksi kehadiran kerentanan baru atau CVE-2023 yang masuk ke Indonesia. Hal ini dapat diartikan sebagai berikut:

1. Pelaku ancaman digital dengan cepat memanfaatkan kerentanan setelah informasi kerentanan dirilis secara resmi.
2. Ancaman digital terkini sudah masuk ke Indonesia dengan cepat.
3. AwanPintar.id® mampu mendeteksi sedini mungkin *(early warning system)* untuk ancaman terbaru.
4. AwanPintar.id® akurat dalam mendeteksi dan mengklasifikasikan serangan berdasarkan CVE.

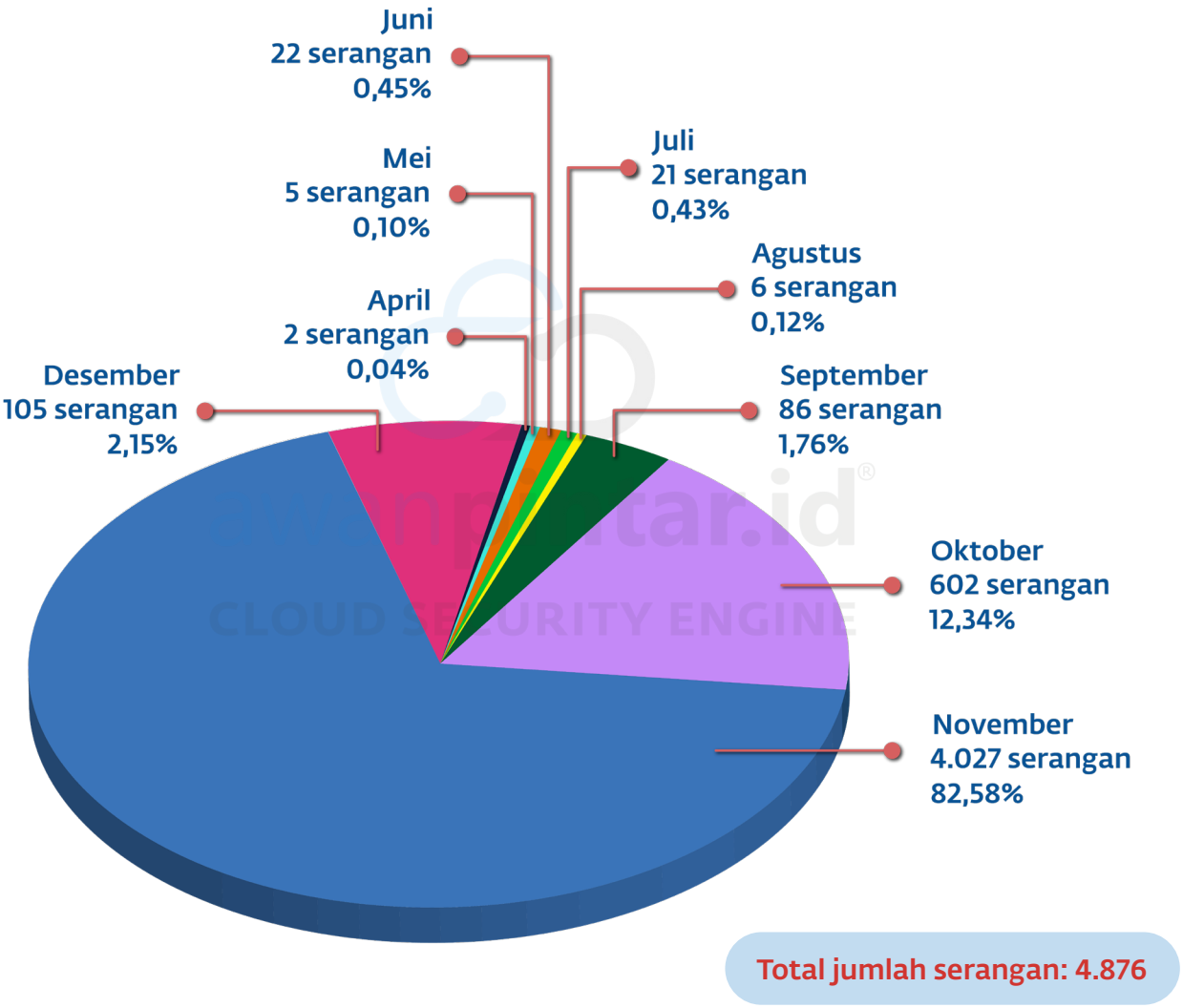
Sebagai kerentanan baru, informasi seputar CVE-2023 masih terbatas, sehingga pastinya masih banyak yang masih awam dengan ancaman tersebut. Identifikasi CVE menjadi penting bagi sebuah organisasi bebasis IT sebagai peringatan dini *(early warning)* untuk menselaraskan dengan sistem yang ada di dalam organsisasi tersebut.

Umumnya terdapat jeda waktu saat CVE dirilis dengan kecepatan vendor mengeluarkan perbaikan (patch) untuk menambal lubang kerentanan. Jangka waktu ini disebut sebagai Zero-Day, dan pada selang waktu ini, para penjahat siber mulai melakukan serangan (Zero-Day Attack) memanfaatkan informasi yang didapat terkait kerentanan sistem.

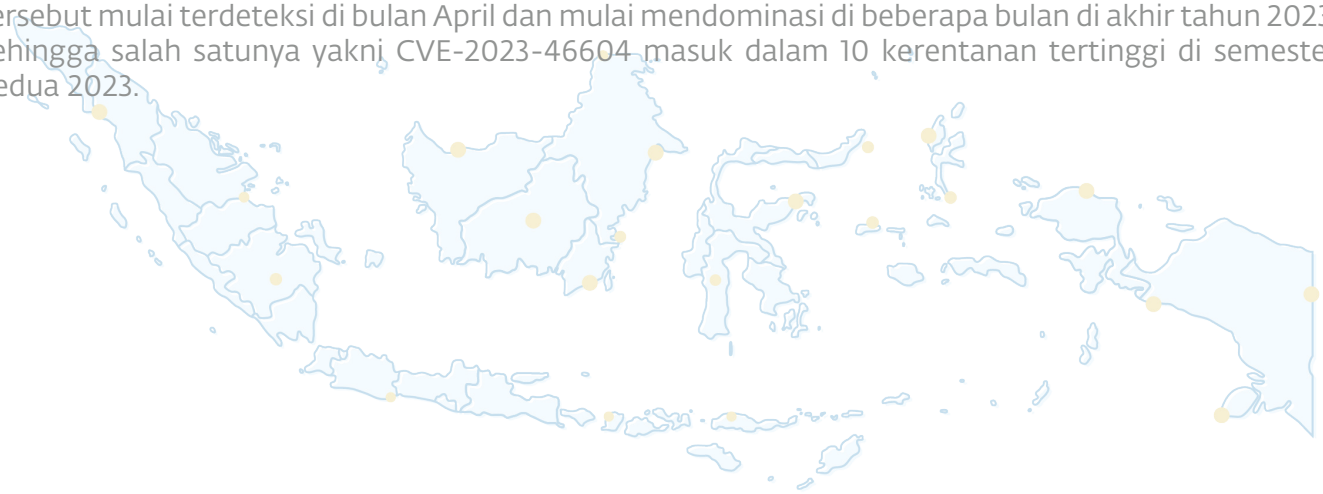
Akumulasi Serangan CVE Selama Tahun 2023

Serangan yang memanfaatkan Common Vulnerability & Exposures selama tahun 2023 memunculkan anomali yang sangat signifikan di bulan Mei, September dan Oktober dengan bulan September menjadi puncak ancaman di sepanjang tahun ini.

Ancaman siber per bulan selama setahun, berikut persentase fluktuasi ancamannya:



Ancaman pada tabel di atas khusus untuk Common Vulnerability Exposures (CVE) 2023. Ancaman tersebut mulai terdeteksi di bulan April dan mulai mendominasi di beberapa bulan di akhir tahun 2023, sehingga salah satunya yakni CVE-2023-46604 masuk dalam 10 kerentanan tertinggi di semester kedua 2023.



Jumlah Serangan Berdasar Jenis CVE-2023

Kode	ALERT SIGNATURE	Bulan Rilis	% Serangan
CVE-2023-46604	ET EXPLOIT Apache ActiveMQ Remote Code Execution Attempt (CVE-2023-46604)	Oktober	66.40%
CVE-2023-26801	ET EXPLOIT LB-Link Command Injection Attempt (CVE-2023-26801)	Maret	20.65%
CVE-2023-1389	ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound (CVE-2023-1389)	Maret	5.95%
CVE-2023-22515	ET CURRENT_EVENTS Possible Atlassian ConfluenceCVE-2023-22515 Scan Activity	Oktober	2.46%
CVE-2023-24488	ET WEB_SPECIFIC_APPS Possible Citrix Gateway CVE-2023-24488 Exploit Attempt M1	Juli	2.42%
CVE-2023-27350	ET EXPLOIT PaperCut MF/NG SetupCompleted Authentication Bypass (CVE-2023-27350)	April	0.64%
CVE-2023-41093	ET EXPLOIT ownCloud Information Disclosure Attempt (CVE-2023-41093)	Desember	0.59%
CVE-2023-0669	ET EXPLOIT Fortra MFT Deserialization Remote Code Execution Attempt (CVE-2023-0669) M3	Februari	0.35%
CVE-2023-20198	ET EXPLOIT Cisco IOS XE Web Server Auth Bypass (CVE-2023-20198) (Inbound) M2	Oktober	0.18%
CVE-2023-42793	ET EXPLOIT JetBrains TeamCity Auth Bypass Attempt (CVE-2023-42793)	September	0.15%
CVE-2023-47246	ET EXPLOIT Possible SysAid Traversal Attack (CVE-2023-47246)	November	0.07%
CVE-2023-26360	ET EXPLOIT Adobe ColdFusion Deserialization of Untrusted Data (CVE-2023-26360) M3	Maret	0.05%
CVE-2023-26359	ET WEB_SPECIFIC_APPS Adobe Coldfusion Local File Inclusion Attempt (CVE-2023-26360, CVE-2023-26359) M2	Maret	0.05%
CVE-2023-36846	ET EXPLOIT Junos OS - Unauthenticated Arbitrary File Upload Attempt (CVE-2023-36847)	Agustus	0.03%
CVE-2023-36847	ET EXPLOIT Junos OS - Unauthenticated Arbitrary File Upload Attempt (CVE-2023-36847)	Agustus	0.03%
CVE-2023-20887	ET EXPLOIT VMware Aria Operations for Networks RCE Attempt (CVE-2023-20887)	Juni	0.02%

Walaupun 80 persen serangan didominasi oleh dua kerentanan umum, dalam ancaman Common Vulnerability & Exposures satu serangan saja sudah terlalu banyak. Satu exploit yang berhasil dibuat, dalam jangka waktu yang tidak lama bisa menyebar dengan cepat dan berkembang berkali-kali lipat.

Jenis CVE-2023 Setiap Bulan

Bulan	Kode CVE	Bulan Rilis CVE	ALERT SIGNATURE
2023-04	CVE-2023-27350	2023-04	ET EXPLOIT PaperCut MF/NG SetupCompleted Authentication Bypass
2023-05	CVE-2023-27350	2023-04	ET EXPLOIT PaperCut MF/NG SetupCompleted Authentication Bypass
2023-05	CVE-2023-1389	2023-03	ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound
2023-06	CVE-2023-1389	2023-03	ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound
2023-07	CVE-2023-27350	2023-04	ET EXPLOIT PaperCut MF/NG SetupCompleted Authentication Bypass
2023-07	CVE-2023-1389	2023-03	ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound
2023-07	CVE-2023-24488	2023-07	ET WEB_SPECIFIC_APPS Possible Citrix Gateway Exploit Attempt M1
2023-07	CVE-2023-24488	2023-07	ET WEB_SPECIFIC_APPS Possible Citrix Gateway Exploit Attempt M2
2023-08	CVE-2023-1389	2023-03	ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound
2023-08	CVE-2023-20887	2023-06	ET EXPLOIT VMware Aria Operations for Networks RCE Attempt
2023-09	CVE-2023-1389	2023-03	ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound
2023-10	CVE-2023-22515	2023-10	ET CURRENT_EVENTS Possible Atlassian Confluence Scan Activity
2023-10	CVE-2023-42793	2023-09	ET EXPLOIT JetBrains TeamCity Auth Bypass Attempt
2023-10	CVE-2023-26801	2023-03	ET EXPLOIT LB-Link Command Injection Attempt
2023-10	CVE-2023-27350	2023-04	ET EXPLOIT PaperCut MF/NG SetupCompleted Authentication Bypass
2023-10	CVE-2023-1389	2023-03	ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound
2023-10	CVE-2023-22515	2023-10	ET WEB_SPECIFIC_APPS Atlassian ConfluenceStep 1/2 Attempt
2023-10	CVE-2023-22515	2023-10	ET CURRENT_EVENTS Possible Atlassian Confluence Scan Activity
2023-11	CVE-2023-22515	2023-10	ET CURRENT_EVENTS Possible Atlassian Confluence Scan Activity
2023-11	CVE-2023-46604	2023-10	ET EXPLOIT Apache ActiveMQ Remote Code Execution Attempt
2023-11	CVE-2023-20198	2023-10	ET EXPLOIT Cisco IOS XE Web Server Auth Bypass (Inbound) M2

Bulan	Kode CVE	Bulan Rilis CVE	ALERT SIGNATURE
2023-11	CVE-2023-36846	2023-08	ET EXPLOIT Junos OS - Unauthenticated Arbitrary File Upload Attempt
2023-11	CVE-2023-36847	2023-08	ET EXPLOIT Junos OS - Unauthenticated Arbitrary File Upload Attempt
2023-11	CVE-2023-26801	2023-03	ET EXPLOIT LB-Link Command Injection Attempt
2023-11	CVE-2023-47246	2023-11	ET EXPLOIT Possible SysAid Traversal Attack
2023-11	CVE-2023-1389	2023-03	ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound
2023-11	CVE-2023-22515	2023-10	ET WEB_SPECIFIC_APPS Atlassian Confluence Step 1/2 Attempt
2023-11	CVE-2023-24488	2023-07	ET WEB_SPECIFIC_APPS Possible Citrix Gateway Exploit Attempt M1
2023-11	CVE-2023-24488	2023-07	ET WEB_SPECIFIC_APPS Possible Citrix Gateway Exploit Attempt M2
2023-12	CVE-2023-26360	2023-03	ET EXPLOIT Adobe ColdFusion Deserialization of Untrusted Data M3
2023-12	CVE-2023-46604	2023-10	ET EXPLOIT Apache ActiveMQ Remote Code Execution Attempt
2023-12	CVE-2023-20198	2023-10	ET EXPLOIT Cisco IOS XE Web Server Auth Bypass (Inbound) M2
2023-12	CVE-2023-0669	2023-02	ET EXPLOIT Fortra MFT Deserialization Remote Code Execution Attempt M3
2023-12	CVE-2023-26801	2023-03	ET EXPLOIT LB-Link Command Injection Attempt
2023-12	CVE-2023-1389	2023-03	ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound
2023-12	CVE-2023-41093	2023-12	ET EXPLOIT ownCloud Information Disclosure Attempt
2023-12	CVE-2023-26359	2023-03	ET WEB_SPECIFIC_APPS Adobe Coldfusion Local File Inclusion Attempt M2
2023-12	CVE-2023-26360	2023-03	ET WEB_SPECIFIC_APPS Adobe Coldfusion Local File Inclusion Attempt M2
2023-12	CVE-2023-24488	2023-17	ET WEB_SPECIFIC_APPS Possible Citrix Gateway Exploit Attempt M1
2023-12	CVE-2023-24488	2023-17	ET WEB_SPECIFIC_APPS Possible Citrix Gateway Exploit Attempt M2

Pada tabel berwarna merah memberikan gambaran pada beberapa nomor CVE-2023 langsung dimanfaatkan oleh para pelaku ancaman digital pada bulan yang sama informasi dirilis. CVE-2023 yang masuk dalam kategori ini adalah:
CVE-2023-27350
CVE-2023-22515
CVE-2023-47246
CVE-2023-41093

Kemudian, pada tabel berwarna hijau memberikan gambaran pada beberapa nomor CVE-2023 langsung dimanfaatkan oleh para pelaku ancaman digital tepat satu bulan setelah informasi dirilis. CVE-2023 yang masuk dalam kategori ini adalah:
CVE-2023-27350
CVE-2023-42793
CVE-2023-22515
CVE-2023-46604
CVE-2023-20198

Yang menarik, kerentanan pada ApacheMQ (CVE-2023-46604) yang dipublikasikan pada tanggal 27 Oktober 2023 menduduki tipe serangan kerentanan tertinggi pada bulan berikutnya (November 2023). Besar kemungkinan dikarenakan jumlah dan beragamnya pengguna ApacheMQ hingga mencapai pengguna Enterprise menjadi daya tarik tersendiri bagi penyerang.

Penutup

Dalam menghadapi ancaman siber yang semakin meningkat, laporan ini telah menyoroti beberapa kendala utama yang dihadapi dalam menjaga keamanan siber di tahun 2023. Ancaman seperti malware, pencurian kredensial, dan serangan siber lainnya telah menjadi fokus utama dalam upaya melindungi infrastruktur digital.

Meskipun tantangan yang dihadapi sangat nyata, terdapat pula cahaya di ujung terowongan. Kesadaran akan bahaya siber telah meningkat di kalangan pengguna internet, yang tercermin dalam penurunan beberapa bentuk ancaman secara luas. Namun demikian, peningkatan drastis dalam frekuensi serangan yang berhasil dilakukan menyoroti perlunya perusahaan dan individu untuk tetap waspada, walaupun terdapat penurunan jumlah serangan.

Keamanan siber bukan hanya tanggung jawab satu entitas, melainkan merupakan upaya kolektif dari berbagai pihak. Stakeholder bisnis dan individu sebagai pengguna internet perlu terlibat aktif dalam menjaga keamanan siber. Di samping itu, kebijakan pemerintah pun memiliki peran penting dalam menciptakan lingkungan digital yang aman dan terpercaya bagi seluruh pemangku kepentingan.

Dengan demikian, laporan ini menyimpulkan pentingnya kesadaran akan ancaman siber, perlunya kewaspadaan terus-menerus, serta tanggung jawab bersama dalam menjaga keamanan siber. Hanya dengan kolaborasi dan kesadaran bersama, kita dapat menciptakan lingkungan digital yang aman dan terlindungi dari ancaman siber di masa mendatang.