awanpintar.id®
CLOUD SECURITY ENGINE

Green
OPEN

INDONESIA WASPADA

Laporan Ancaman Digital di Indonesia
Semester 1 Tahun 2025

PT PROSPERITA SISTEM INDONESIA
partner@awanpintar.id

Green
OPEN

DAFTAR ISI

Green
OPEN

RINGKASAN EKSEKUTIF

Laporan Ancaman Digital di Indonesia Semester 1 tahun 2025 ditandai dengan penurunan serangan per bulannya. Hal ini merupakan lanjutan trend serangan siber yang mengalami penurunan sangat drastis sejak bulan November (6,5 juta serangan) Desember (4,1 juta) dibandingkan bulan September (1,6 Milyar) dan Oktober (900 juta) di tahun 2024.

Generic Protocol Command Decode yang merupakan anomali data mengalami kenaikan signifikan dibandingkan periode sebelumnya. Temuan menarik terkait anomali data adalah jejak munculnya serangan menggunakan botnet Mirai berbasis Linux yang umumnya digunakan untuk serangan DDoS yang terstruktur dan memiliki komando yang jelas, ini tentunya membuat sebuah catatan tersendiri.

Pelaku kejahatan siber memanfaatkan berbagai teknik, mulai dari brute force hingga rekayasa sosial, untuk mendapatkan akses penuh secara tidak sah ke akun pengguna. Serangan terhadap port komputer juga menunjukkan peningkatan yang mengkhawatirkan. Pelaku kejahatan siber secara aktif memindai dan mengeksploitasi port yang terbuka, membuka pintu bagi penyusupan dan eksfiltrasi data. Selain itu, eksploitasi CVE semakin marak, menunjukkan bahwa pelaku kejahatan siber semakin mahir dalam memanfaatkan kerentanan yang diketahui dalam perangkat lunak dan sistem.

Serangan yang berasal dari dalam negeri menjadi ancaman yang semakin nyata. Pelaku kejahatan siber yang beroperasi di Indonesia menunjukkan peningkatan aktivitas, menargetkan berbagai sektor dengan motif yang beragam. Serangan-serangan ini menggarisbawahi perlunya fokus pada keamanan siber di tingkat nasional, dengan memperkuat pertahanan dan meningkatkan kesadaran di kalangan pengguna dan organisasi. Peningkatan serangan dari dalam negeri ini, juga mengindikasikan perlunya peningkatan kesadaran dan kapasitas keamanan siber di tingkat nasional.

Untuk mengatasi ancaman-ancaman ini, pemerintah, perusahaan, dan pemangku kepentingan keamanan siber harus mengambil langkah-langkah proaktif. Pemerintah perlu memperkuat regulasi keamanan siber, meningkatkan investasi dalam infrastruktur keamanan, dan mendorong kerja sama antara sektor publik dan swasta.

Perusahaan harus memprioritaskan keamanan siber dengan menerapkan praktik terbaik, melakukan penilaian kerentanan secara berkala, dan melatih karyawan tentang kesadaran keamanan. Pemangku kepentingan keamanan siber harus berkolaborasi dalam berbagi informasi ancaman, mengembangkan solusi inovatif, dan meningkatkan kapasitas sumber daya manusia di bidang keamanan siber. Dengan upaya bersama, Indonesia dapat

memperkuat pertahanan sibernya dan melindungi infrastruktur digitalnya dari ancaman yang terus berkembang.

Di tengah dinamika lanskap keamanan siber yang terus berkembang, pemahaman mendalam tentang Common Vulnerabilities and Exposures (CVE) menjadi krusial. Liputan khusus ini hadir untuk mengupas tuntas CVE, mulai dari definisinya yang esensial, bagaimana kerentanan ini diklasifikasikan dan dinilai menggunakan standar industri seperti CVSS, hingga dampaknya yang signifikan terhadap sistem dan data. Kebutuhan akan kepatuhan (Compliance) baik itu NIST 2.0 ataupun ISO 27001-2022 dan regulasi pemerintah RI terkait keamanan siber (UU, Peraturan Presiden, Peraturan BSSN, Peraturan OJK, Peratutan BI) menjadi catatan tersendiri yang perlu dipahami dengan baik bagi yang berkepentingan.

Green
OPEN

TENTANG awanpintar.id®

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

Beberapa solusi turunan dari AwanPintar.id® adalah Cloud Malware Analyzer, Cloud Antimalware File Scanning, Cloud Endpoint Security (CloudID), Cloud Email Security: Vimanamail®, CSIRTradar, Dark Web Monitoring, Vulnerability Alert. AwanPintar.id® terhubung langsung di pusat internet Indonesia (OIX/IIX) – Open Internet Exchange Point / Indonesia Internet Exchange, jantung dari komunikasi internet di Indonesia sehingga mampu menyediakan akses cepat dengan kapasitas koneksi yang tinggi.

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

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

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

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

Green
OPEN

METODOLOGI

Untuk memahami ancaman digital di Indonesia, AwanPintar.id® memasang detektor di jaringan internet Indonesia. Detektor ini menjadi target serangan dari mancanegara dan dalam negeri. Berikut adalah metodologi riset yang digunakan untuk membuat Laporan Ancaman Digital di Indonesia Semester 1:

Pengumpulan Data

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

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

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

Pemilihan Data

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

Analisis Data

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

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

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).

Visualisasi Data

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

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

Green
OPEN

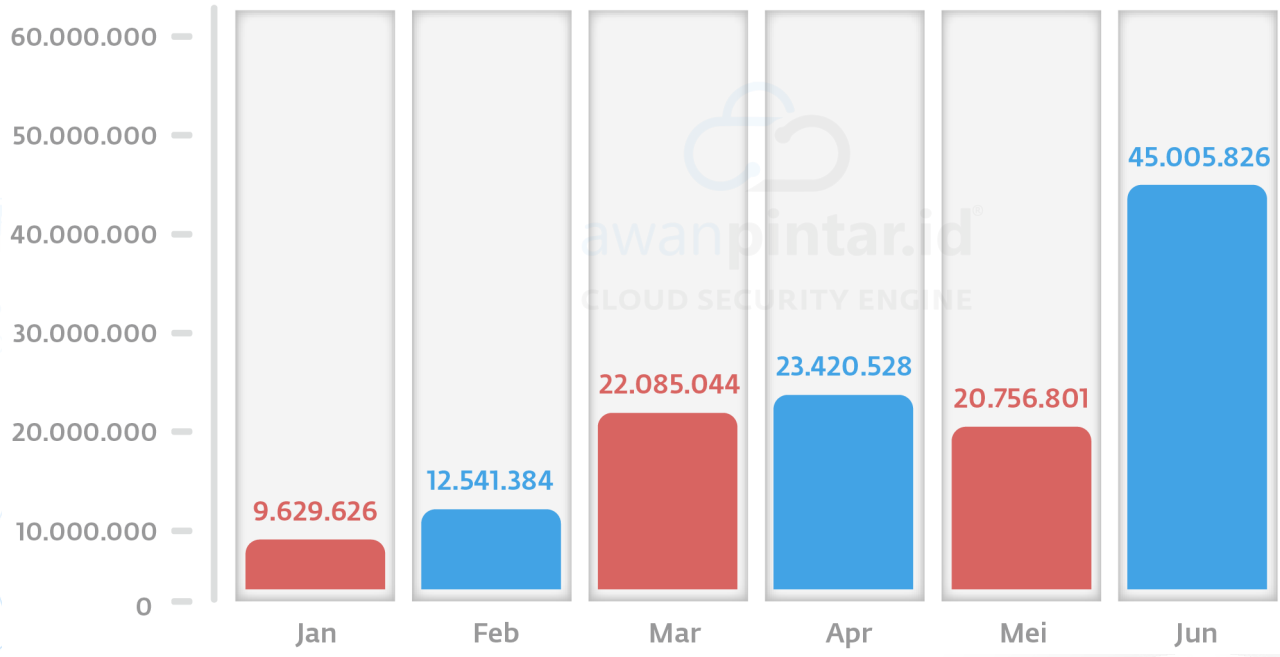
TREN SERANGAN TERKINI

Akumulasi Serangan Siber di Indonesia

Data ini menyajikan analisis komprehensif mengenai akumulasi serangan siber yang terjadi di Indonesia selama semester pertama tahun 2025, yang bertujuan untuk memberikan gambaran yang jelas dan terperinci mengenai situasi keamanan siber di Indonesia.

Data yang disajikan dalam laporan ini merupakan hasil pengumpulan dan analisis mendalam terhadap berbagai insiden keamanan siber yang terjadi, serta pemantauan terhadap tren dan pola serangan yang berkembang.

Data berikut merupakan rata-rata jumlah serangan yang terjadi terhadap satu perangkat bila diletakkan di internet menggunakan IP publik.

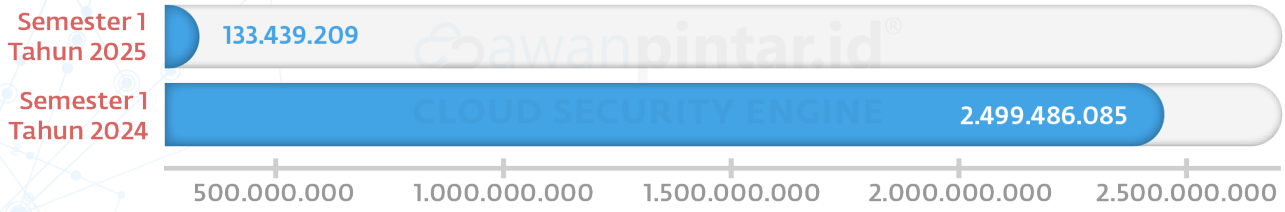


Jumlah total seluruh serangan **133.439.209**

Rata-rata serangan per detik	Rata-rata serangan per menit	Rata-rata serangan per jam	Rata-rata serangan per hari
9	512	30.718	737.233

Green
OPEN

Komparasi total Serangan Semester 1 Tahun 2025 dan Semester 1 Tahun 2024



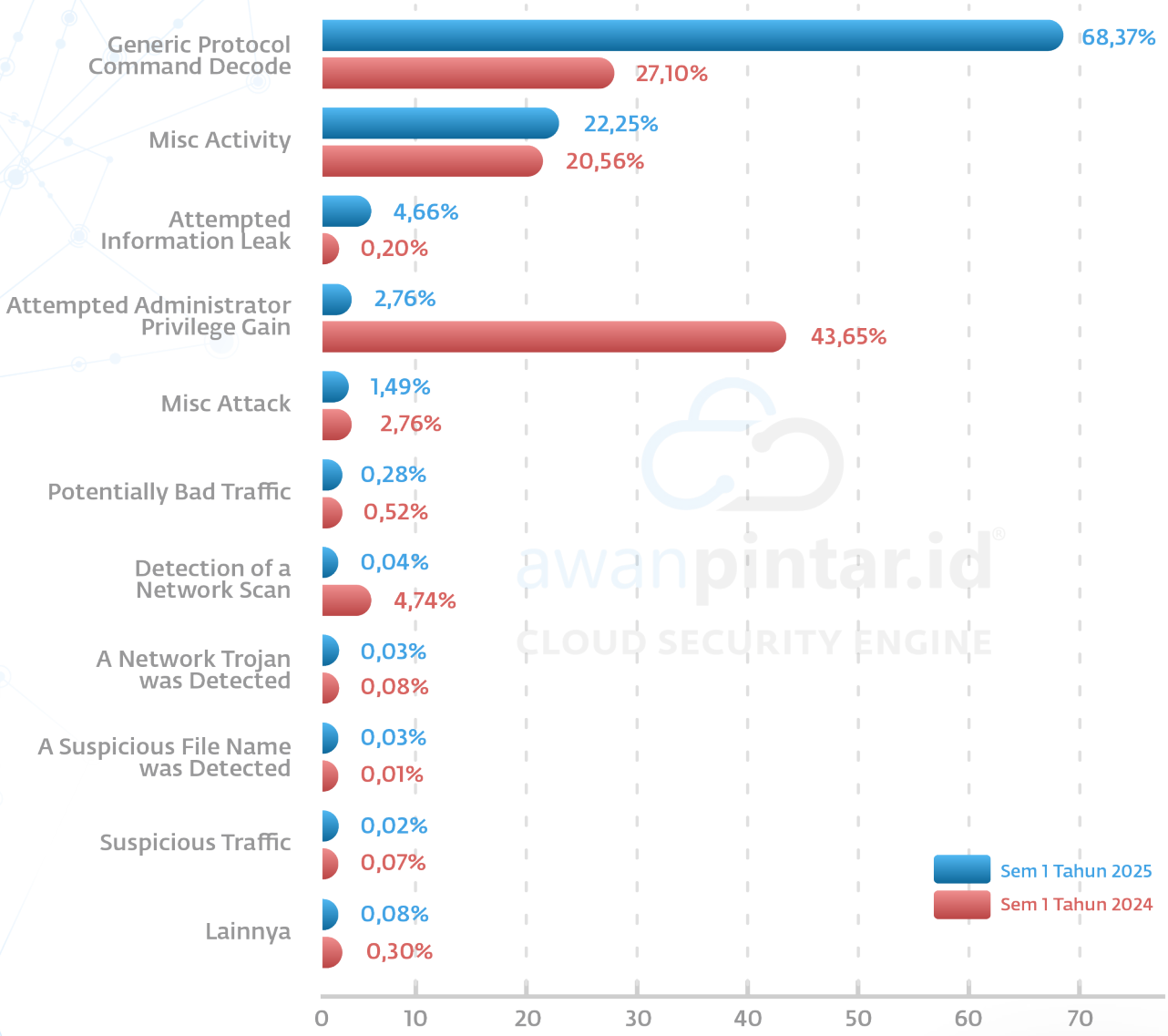
Jumlah Serangan Menurun **-2.366.046.876**
Secara Persentase Menurun **94,66%**

Penurunan serangan yang begitu drastis ini sudah dimulai sejak akhir tahun lalu di bulan November dan Desember dan berlanjut ke tahun ini. Sebagai catatan, di tahun 2024 terdapat peristiwa besar di Indonesia, yaitu pemilihan Presiden dan Wakil Presiden.

Anomali telah berakhir dan pola serangan kembali seperti di tahun 2023, dan penurunan ini tidak berarti bahwa sistem keamanan infrastruktur Indonesia menjadi lebih baik secara signifikan. Terlebih lagi di akhir tahun lalu terjadi upaya pencurian kredensial secara besar-besaran di Indonesia yang dampaknya bisa terlihat dari laporan ancaman digital tahun 2025.

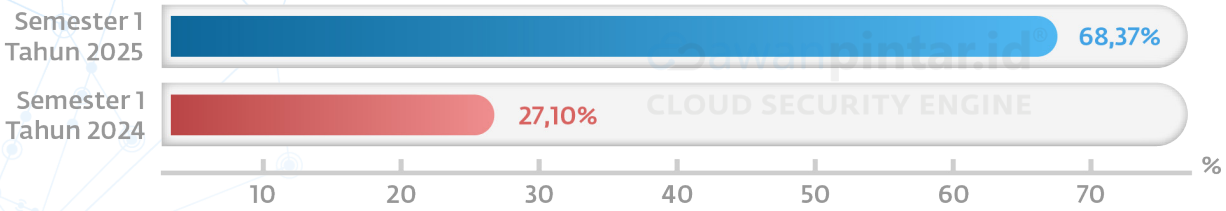
Green
OPEN

10 Jenis Serangan Siber Teratas



Generic Protocol Command Decode

Identifikasi anomali pada paket data protokol jaringan yang tidak diharapkan atau tidak sah. Metode ini dapat digunakan untuk mendeteksi serangan siber yang menggunakan teknik manipulasi atau mencampuradukan protokol jaringan. Salah satu teknik serangan seperti ini adalah DDoS yang memanfaatkan kelemahan untuk melumpuhkan atau mendapatkan hak akses. Kemunculan Mirai botnet menjadi indikator kuat sumbangsih kenaikan anomali paket data. AwanPintar.id® mendeteksi kehadiran botnet Mirai versi sistem operasi Linux yang beredar dan melakukan serangan DDoS.

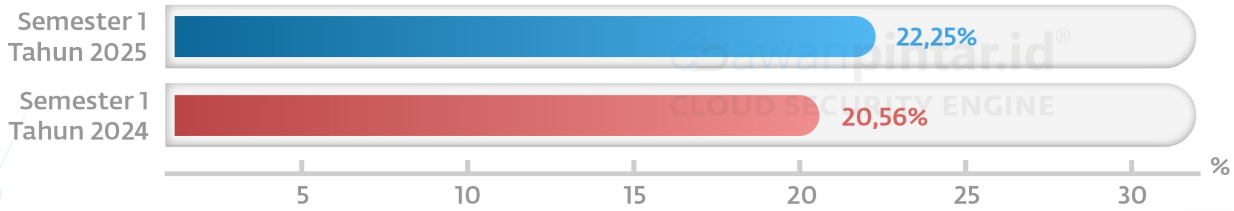


Peningkatan 41,27% dalam setahun, menunjukkan hampir dua pertiga (68,37%) deteksi protokol di Semester 1 2025 dalam serangan jenis ini yang merupakan lonjakan yang sangat tajam. Ini juga menandakan peningkatan signifikan pada serangan DDoS atau upaya manipulasi protokol yang menargetkan ketersediaan layanan dan integritas data.

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.

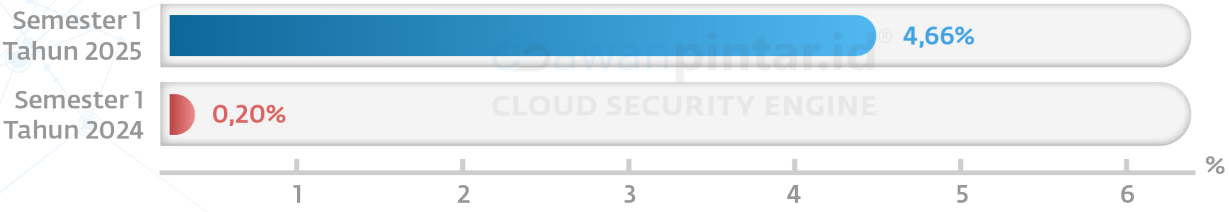


Dari data yang diperoleh dari AwanPintar.id® menunjukkan adanya kenaikan 1,69% dalam deteksi Misc Activity. Meskipun angkanya tidak setinggi kategori lain, peningkatan ini menunjukkan adanya tren aktivitas mencurigakan yang terus-menerus. Kategori ini seringkali merupakan indikator awal dari upaya penyerang untuk memahami dan memetakan target mereka sebelum meluncurkan serangan yang lebih canggih (misalnya, mencari kerentanan atau titik masuk).

Dengan persentase sekitar 20%, Misc Activity merupakan bagian yang cukup stabil dari lanskap ancaman siber, menunjukkan bahwa pengintaian dan pemindaian jaringan adalah aktivitas rutin bagi para penyerang.

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.

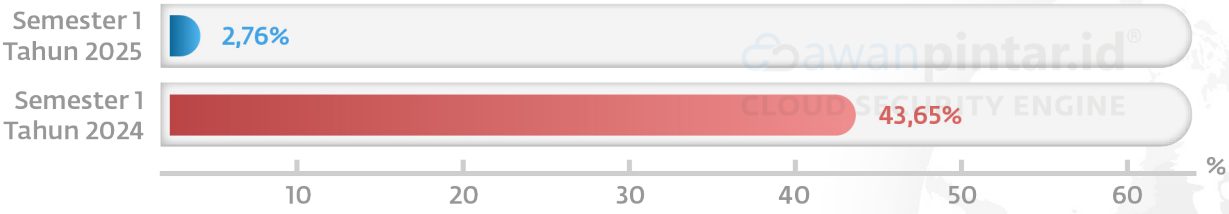


Terjadi lonjakan yang sangat besar, dari 0,20% menjadi 4,66%, yang berarti peningkatan lebih dari 23 kali lipat dalam upaya kebocoran informasi dalam kurun waktu satu tahun. Ini adalah peningkatan persentase yang paling mencolok dibanding kategori serangan lain yang telah dianalisis.

Tingginya persentase ini secara eksplisit mengindikasikan bahwa para penyerang semakin berfokus pada pencurian data berharga, bukan hanya mengganggu layanan. Upaya kebocoran informasi seringkali didorong oleh motif finansial (penjualan data di pasar gelap) atau spionase. Lonjakan sebesar 4,46% adalah sinyal bahaya serius bagi keamanan data. Ini menunjukkan bahwa meskipun pertahanan awal mungkin telah membaik dalam beberapa aspek, penyerang semakin canggih dalam menembus dan mengekstraksi data. Organisasi harus segera memperkuat strategi pencegahan kebocoran data (Data Leak Prevention), secara berkala melakukan pengecekan di Dark Web, meningkatkan pemantauan lalu lintas keluar, dan mengevaluasi ulang efektivitas kontrol akses serta klasifikasi data mereka. Investasi dalam deteksi anomali perilaku dan intelijen ancaman yang lebih baik sangat krusial untuk mengidentifikasi dan merespons upaya ekfiltrasi ini sebelum data sensitif jatuh ke tangan yang salah.

Attempted Administrator Privilege Gain

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



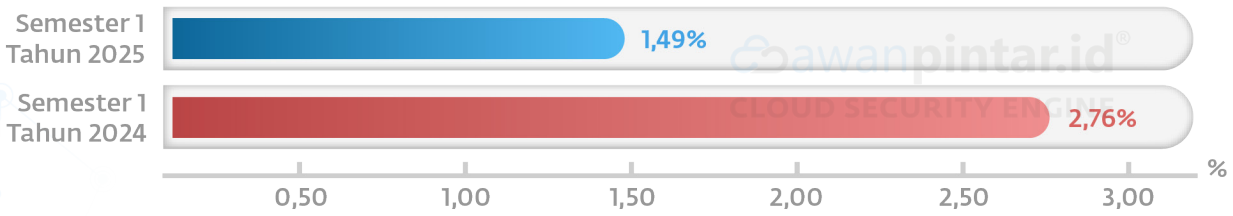
Terjadi penurunan drastis sebesar -40,89%, dari 43,65% menjadi hanya 2,76%. Ini adalah perubahan persentase yang paling besar dan berlawanan arah dibandingkan kategori serangan lain yang telah dianalisis sebelumnya.

Penurunan ini bisa mengindikasikan bahwa para penyerang telah mengubah taktik mereka. Jika sebelumnya mereka banyak berfokus pada upaya mendapatkan hak akses administrator secara langsung, kini mereka mungkin beralih ke metode lain, seperti langsung mencari kebocoran informasi (Attempted Information Leak) yang justru meningkat tajam (dari 0,20% menjadi 4,66%). Selain itu, pelaku telah beradaptasi dan meningkatkan kecanggihan serangan mereka. Mereka kini mungkin lebih fokus pada metode stealthy seperti Living Off The Land, eksploitasi zero-day, atau social engineering yang menargetkan pengguna secara lebih cerdik.

Ini juga bisa menjadi cerminan keberhasilan upaya pertahanan siber di Indonesia dalam mencegah atau mendeteksi upaya peningkatan hak akses. Mungkin ada peningkatan implementasi sistem pencegahan intrusi, manajemen patch yang lebih baik, atau konfigurasi keamanan yang lebih ketat yang membuat upaya ini kurang berhasil.

Misc Attack

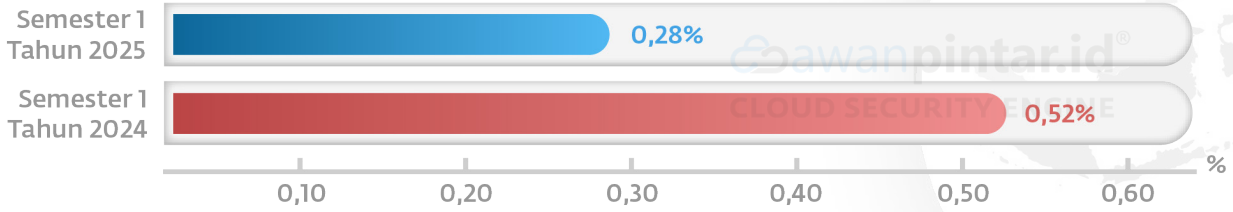
Jenis serangan ini mengeksploitasi server web yang rentan dengan memaksa server cache atau browser web untuk mengungkapkan informasi kredensial, kata sandi, dan informasi yang disimpan. Atau serangan dengan sifat membajak komunikasi yang sedang dilakukan dan serangan pada protokol HTTP.



Eksploitasi server web rentan untuk mencuri kredensial atau membajak komunikasi HTTP, mengalami penurunan besar -1,27%. Pergeseran taktik penyerang yang kini mungkin beralih ke metode serangan yang lebih canggih atau dari kredensial yang mereka miliki, penyerang melakukan eskalasi hak admin untuk mendapatkan objek serangan lebih luas. Meskipun demikian potensi ancaman dari jenis serangan ini tidak bisa dianggap remeh.

Potentially Bad Traffic

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

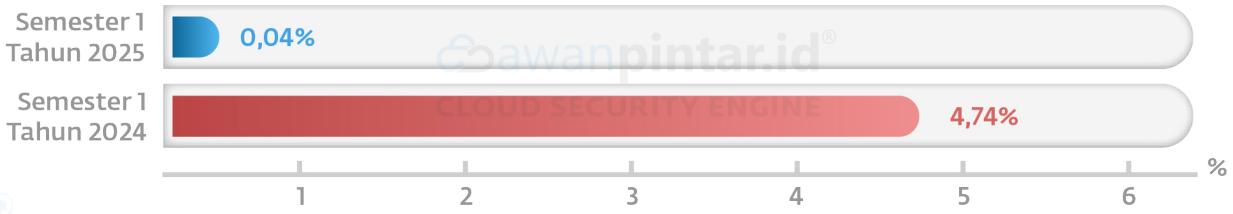


Terjadi penurunan sebesar 0,24% dalam deteksi Potentially Bad Traffic dari 0,52% di Semester 1 2024 menjadi 0,28% di Semester 1 2025. Meskipun ada penurunan, persentase total Potentially Bad Traffic yang terdeteksi tetap sangat rendah (di bawah 1%) di kedua periode.

Walau persentasenya kecil, Potentially Bad Traffic menandakan ancaman yang sangat serius. Jika sistem sudah disusupi, kontrol penuh oleh penyerang dapat menyebabkan kerugian besar. Oleh karena itu, bahkan persentase kecil ini memerlukan perhatian serius.

Detection of a Network Scan

Adanya aktivitas ilegal yang melibatkan pendeteksian semua host aktif di jaringan dan melakukan pemetaan ke alamat IP mereka. Penyerang sering menggunakannya untuk melakukan pengintaian sebelum mencoba menembus jaringan. Serangan seperti SUNBURST dapat menggunakan pemindaian jaringan untuk mendapatkan posisi awal serangan. SUNBURST adalah serangan rantai pasokan yang memanfaatkan backdoor yang ditanamkan pada pemasok untuk menargetkan dan mengkompromikan organisasi secara tidak langsung di seluruh dunia.



Dari data yang diperoleh dari AwanPintar.id® diketahui terjadi penurunan yang luar biasa besar, yaitu -4,70%, dari 4,74% di Semester 1 2024 menjadi hanya 0,04% di Semester 1 2025. Ini adalah penurunan persentase terbesar dan paling signifikan di antara semua kategori serangan yang telah dianalisis.

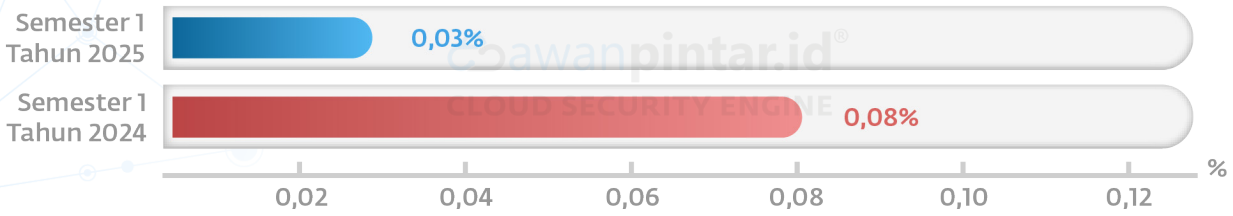
Penurunan ini bisa menunjukkan bahwa penyerang tidak lagi terlalu mengandalkan pemindaian jaringan tradisional yang mudah dideteksi. Mereka mungkin beralih ke metode pengintaian yang lebih canggih, tersembunyi, atau low-and-slow yang tidak menghasilkan traffic pemindaian yang jelas, atau menggunakan informasi yang sudah mereka peroleh dari sumber lain (misalnya, melalui kebocoran data atau reconnaissance terbuka).

Organisasi harus meningkatkan kemampuan deteksi reconnaissance mereka di luar pemindaian tradisional. Ini bisa melibatkan analisis log yang lebih mendalam, threat intelligence yang lebih baik, dan pemantauan anomali perilaku jaringan yang lebih canggih.

Green
OPEN

A Network Trojan was Detected

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



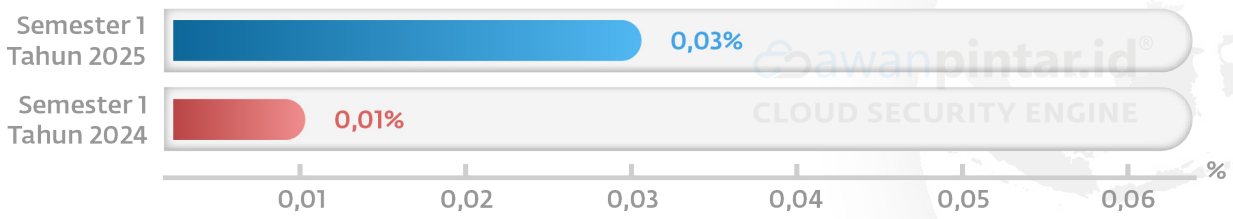
Hasil olah data dari AwanPintar.id® telah terjadi penurunan sebesar 0,05% dalam deteksi Trojan jaringan, dari 0,08% di Semester 1 2024 menjadi 0,03% di Semester 1 2025. Persentase total deteksi Trojan jaringan di kedua periode sangatlah rendah, di bawah 0,1%.

Meskipun persentasenya rendah dan menurun, Trojan tetap merupakan ancaman serius karena kemampuannya untuk memberikan akses jarak jauh dan mencuri data. Angka yang kecil bukan berarti tidak ada risiko, melainkan bahwa deteksinya mungkin lebih sulit atau serangan ini lebih tersembunyi.

A Suspicious Filename was Detected

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

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

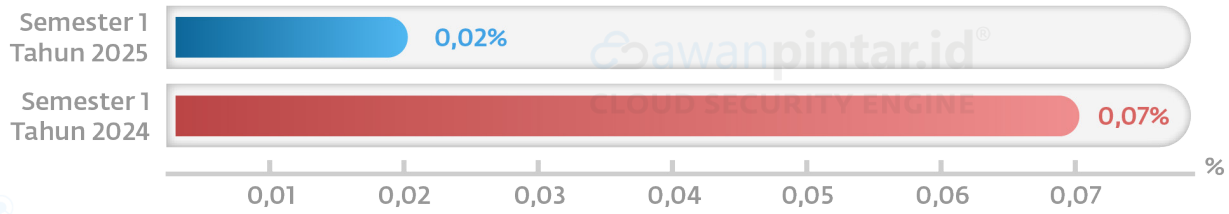


Peningkatan sebesar 0,02% ini menunjukkan bahwa deteksi berkas mencurigakan meningkat hingga tiga kali lipat. Ini mengindikasikan adanya peningkatan upaya penyerang dalam menggunakan berkas sebagai vektor infeksi. Peningkatan ini secara langsung berhubungan dengan upaya penyebaran malware, karena berkas mencurigakan seringkali adalah malware itu sendiri atau pembawa malware.

Peran Sebagai Garis Depan: Data ini menekankan peran vital deteksi berkas mencurigakan sebagai "garis depan pertahanan" untuk menangkap ancaman sejak dini, sebelum mereka dapat menginfeksi sistem secara lebih dalam.

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.



Data dari AwanPintar.id® menunjukkan adanya penurunan pada deteksi Suspicious Traffic di Indonesia yakni -0,05. Meskipun persentasenya kecil dan menurun, Suspicious Traffic tetap merupakan indikator potensi masalah. Tim keamanan harus tetap waspada dan menyelidiki setiap deteksi ini secara mendalam untuk memastikan tidak ada ancaman tersembunyi yang terlewat.

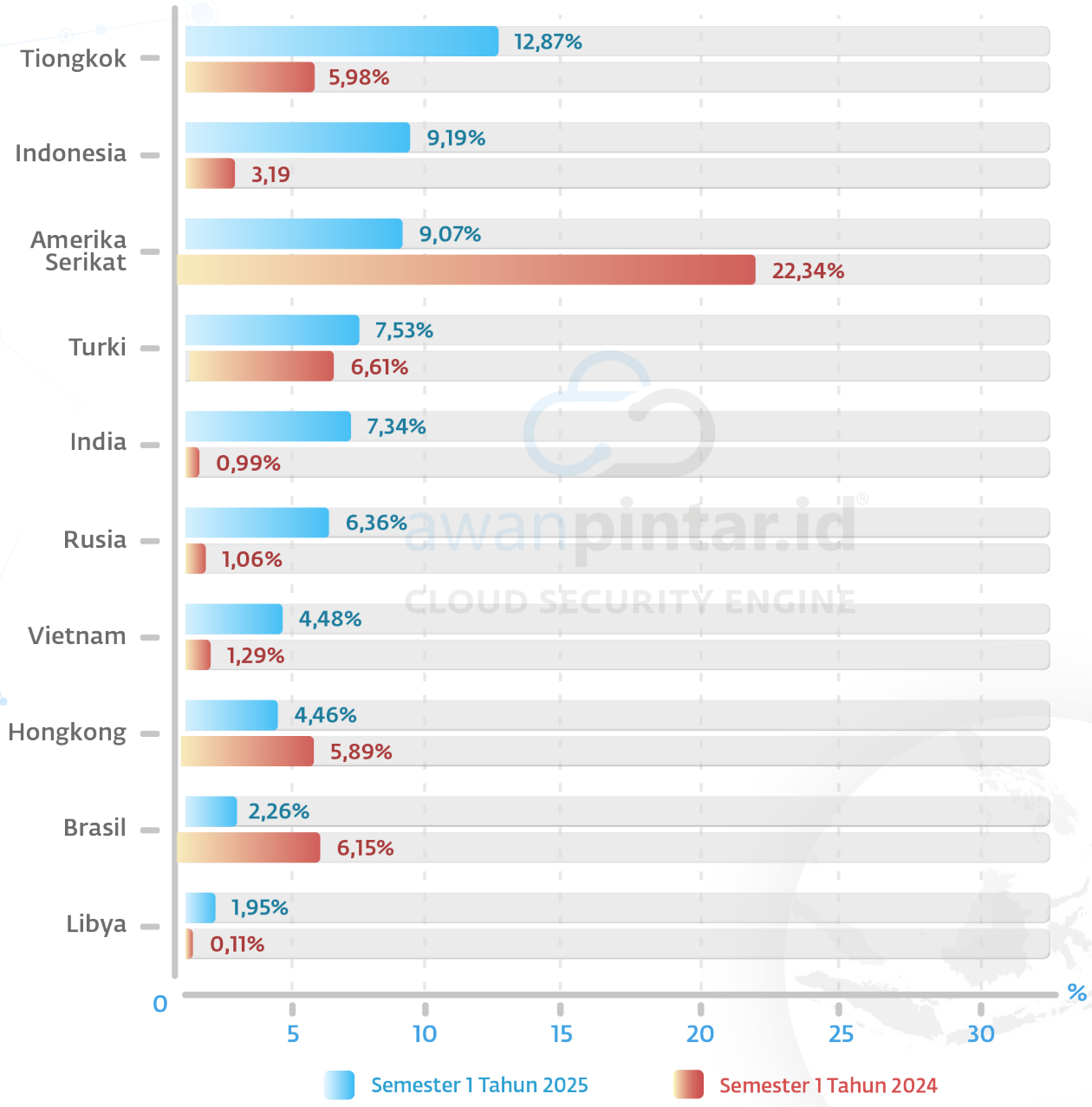
Penyerang mungkin telah mengadopsi teknik yang lebih canggih dan stealthy (tersembunyi), sehingga lalu lintas berbahaya yang mereka hasilkan tidak lagi jatuh dalam kategori "sangat mencurigakan" melainkan meniru lalu lintas normal atau memanfaatkan celah spesifik yang terdeteksi di kategori lain.

Green
OPEN

10 Negara Kontributor Serangan Siber

Dalam laporan ancaman digital semester pertama tahun 2025, AwanPintar.id® menganalisis mengenai sepuluh negara yang teridentifikasi sebagai kontributor utama serangan siber ke Indonesia di tingkat global. Data yang dikumpulkan selama periode pelaporan menyoroti negara-negara yang secara konsisten menjadi sumber aktivitas siber berbahaya.

Ini bertujuan untuk memberikan pemahaman yang lebih baik tentang lanskap ancaman siber internasional, serta mengidentifikasi faktor-faktor yang berkontribusi terhadap aktivitas siber yang berasal dari negara-negara tersebut.



Tiongkok
Peningkatan 6,89%

Indonesia
Pendatang baru dengan kenaikan 6,00%

Amerika Serikat
Penurunan -13,27%

Turki
Peningkatan 0,92%

India
Pendatang baru dengan kenaikan 6,35%

Rusia
Pendatang baru dengan kenaikan 5,30%

Vietnam
Pendatang baru dengan kenaikan 3,19%

Hongkong
Penurunan -1,43%

Brasil
Penurunan -3,89%

Libya
Pendatang baru dengan kenaikan 1,84%

Serapan data yang dihimpun oleh AwanPintar.id® hasil komparasinya menunjukkan adanya pergeseran signifikan dalam lanskap negara kontributor serangan siber ke Indonesia. Tren ini mengindikasikan dinamika baru dalam aktivitas siber global yang perlu diwaspadai.

Peningkatan Dominasi dan Kemunculan Baru

Tiongkok menunjukkan peningkatan yang paling mencolok, melonjak dari 5,98% menjadi 12,87%, atau mengalami peningkatan 6,89%. Ini menempatkan Tiongkok sebagai kontributor terbesar serangan siber ke Indonesia. Negara ini secara konsisten menjadi negara yang rutin menyerang Indonesia dari tahun ke tahun dengan serangan yang terus meningkat.

Turki juga meningkat, dari 6,61% menjadi 7,53%, meskipun jauh lebih kecil yaitu 0,92%. Turki juga merupakan negara yang rutin menunjukkan peningkatan aktivitas siber terhadap Indonesia.

Yang paling menarik adalah kemunculan lima negara baru dalam daftar 10 kontributor teratas pada Semester 1 Tahun 2025:

- Indonesia sendiri, dengan peningkatan 6,00% (dari 3,19% menjadi 9,19%). Kehadiran Indonesia yang masuk sebagai 3 besar dalam daftar ini, mengindikasikan potensi berkembangnya para penyerang lokal atau adanya botnet atau infrastruktur yang terkompromi di dalam negeri yang digunakan untuk menyebarkan ancaman.
- India, melonjak 6,35% (dari 0,99% menjadi 7,34%).
- Rusia, dengan kenaikan 5,30% (dari 1,06% menjadi 6,36%).
- Vietnam, yang naik 3,19% (dari 1,29% menjadi 4,48%). Keberadaan Vietnam sebagai pendatang baru cukup mengejutkan mengingat mereka selalu di bawah radar.
- Libya, dengan kenaikan signifikan 1,84% (dari 0,11% menjadi 1,95%). Yang paling menarik di sini adalah Libya, negara yang sedang dalam krisis berkelanjutan tersebut dengan infrastruktur terbatas mampu secara masif melakukan invasi secara digital.

Penurunan Kontribusi dari Sumber Lama

Amerika Serikat mengalami penurunan paling drastis, dari 22,34% menjadi 9,07%, yaitu -13,27%. Ini menunjukkan bahwa meskipun masih menjadi kontributor, perannya sebagai sumber utama telah berkurang secara signifikan.

Dari belahan dunia yang lain, Brasil juga menunjukkan penurunan yang substansial, dari 6,15% menjadi 2,26%, yaitu -3,89%.

Sementara Hong Kong hanya mengalami penurunan kecil, dari 5,89% menjadi 4,46%, yaitu -1,43%.

Meski demikian, negara-negara tersebut (Amerika Serikat, Brasil, Hong Kong) menunjukkan konsistensi dalam mengganggu keamanan dalam jaringan internet nasional, meskipun dengan kontribusi yang menurun pada periode ini.

Implikasi

Pergeseran ini menggarisbawahi bahwa sumber ancaman siber bersifat dinamis dan terus berubah. Peningkatan kontribusi dari Tiongkok dan kemunculan negara-negara baru, termasuk Indonesia sendiri, menuntut adaptasi strategi keamanan siber yang lebih gesit.

Organisasi dan individu di Indonesia perlu meningkatkan kewaspadaan terhadap lalu lintas yang berasal dari sumber-sumber yang sedang meningkat ini, seperti Tiongkok, India, Rusia, Vietnam, dan Libya. Selain itu, sangat krusial untuk secara rutin memantau dan mengamankan infrastruktur internal guna mendeteksi dan membersihkan potensi kompromi yang dapat menjadikan mereka bagian dari sumber spam dan malware (seperti yang terlihat dari masuknya Indonesia dalam daftar kontributor teratas). Strategi keamanan nasional harus berfokus pada intelijen ancaman global yang lebih adaptif untuk mengantisipasi pola serangan baru dan memperkuat pertahanan di titik-titik rentan.

Analisis ini menunjukkan bahwa lanskap ancaman siber ke Indonesia semakin kompleks, dengan munculnya pemain baru dan perubahan dinamika dari kontributor lama.

Green
OPEN

10 IP Penyerang Teratas

Analisis lalu lintas serangan siber di Indonesia selama periode ini oleh AwanPintar.id® mengungkap keberadaan sepuluh alamat IP yang paling aktif dalam melancarkan serangan. Data ini memberikan gambaran penting mengenai sumber-sumber utama aktivitas siber berbahaya yang menargetkan infrastruktur digital nasional.

Keberadaan IP-IP ini, yang terdeteksi melalui pemantauan intensif terhadap jaringan internet Indonesia, mengindikasikan adanya upaya kontinyu untuk mengeksploitasi kerentanan dan mengganggu stabilitas sistem.

Identifikasi sepuluh IP penyerang teratas ini bukan hanya sekadar pendataan belaka, tetapi juga merupakan representasi dari pola serangan yang kompleks dan beragam. Di bawah ini adalah daftar alamat IP beserta darimana IP tersebut berasal.

Tiongkok	192. xxx.xxx.xxx 36,710,382 21.45%	84. xxx.xxx.xxx 13,538,791 7.91%	Swiss
Tiongkok	125. xxx.xxx.xxx 7,208,772 4.21%	212. xxx.xxx.xxx 5,915,252 3.46%	Turki
Belanda	193. xxx.xxx.xxx 4,953,036 2.89%	154. xxx.xxx.xxx 4,949,369 2.89%	Amerika Serikat
Kanada	142. xxx.xxx.xxx 4,780,863 2.79%	103. xxx.xxx.xxx 4,741,160 2.77%	Indonesia
Indonesia	103. xxx.xxx.xxx 4,101,015 2.40%	103. xxx.xxx.xxx 3,861,921 2.26%	Indonesia

Lainnya 46.97%

Green
OPEN

Kompilasi data AwanPintar.id® untuk Semester 1 Tahun 2025 mengungkapkan gambaran ancaman serangan siber yang mengkhawatirkan di Indonesia. Data ini menampilkan 10 IP teratas yang terdeteksi sebagai penyerang, beserta negara asal dan persentase kontribusinya terhadap total serangan.

Temuan Kunci:

Tiongkok Mendominasi: Tiongkok adalah sumber serangan terbesar, dengan dua IP menyumbang total 25.66% (21.45% + 4.21%). IP 192.xxx.xxx.xxx saja bertanggung jawab atas lebih dari seperlima (21.45%) dari serangan teratas.

Keragaman Global: Selain Tiongkok, serangan juga berasal dari berbagai negara lain seperti Swiss (7.91%), Turki (3.46%), Belanda (2.89%), Amerika Serikat (2.89%), dan Kanada (2.79%). Ini menunjukkan sifat global dari ancaman siber yang menargetkan Indonesia.

Kontribusi dari Dalam Negeri: Tiga IP teratas dari Indonesia (103.xxx.xxx.xxx, 103.xxx.xxx.xxx, 103.xxx.xxx.xxx) juga masuk dalam 10 besar, menyumbang total 7.43% dari serangan teratas. Ini mengindikasikan bahwa sebagian serangan yang menargetkan Indonesia juga berasal dari dalam negeri, kemungkinan dari sistem yang terkompromi atau botnet.

Implikasi:

Data ini menggarisbawahi bahwa Indonesia menghadapi ancaman siber dari berbagai penjuru dunia, dengan Tiongkok sebagai sumber dominan. Kehadiran IP Indonesia dalam daftar ini juga menunjukkan adanya sistem yang disalahgunakan di dalam negeri. Mitigasi harus mencakup pemblokiran IP dari luar negeri yang mencurigakan serta penanganan sistem yang terinfeksi di dalam negeri.

Green
OPEN

Ancaman Pencurian Kredensial

Pencurian kredensial merupakan salah satu ancaman siber yang paling mengkhawatirkan di era digital saat ini. Pelaku kejahatan siber terus mengembangkan teknik-teknik baru untuk mendapatkan akses tidak sah ke akun pengguna dengan memanfaatkan kelemahan sistem keamanan. Dampak dari pencurian kredensial dapat sangat merugikan, mulai dari kerugian finansial hingga pencurian identitas dan pelanggaran privasi.

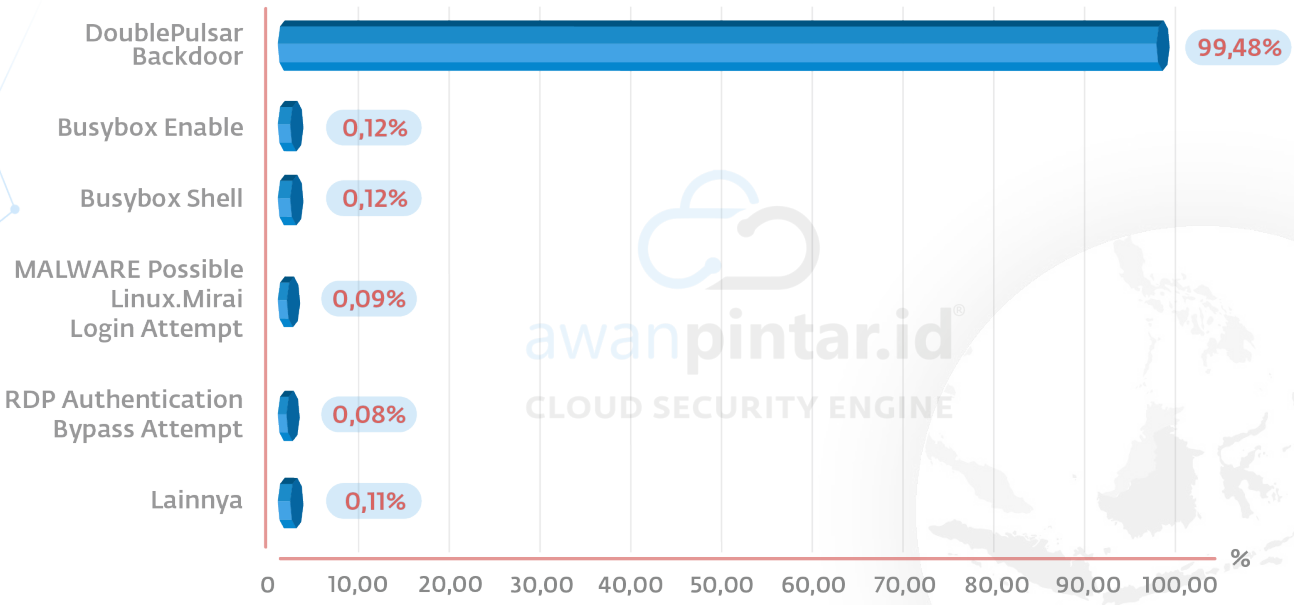
Fenomena pencurian kredensial tidak hanya mengancam individu, tetapi juga organisasi dan perusahaan dari berbagai sektor. Data dan informasi sensitif yang tersimpan dalam akun pengguna menjadi target utama para pelaku kejahatan siber. Berikut data-data yang dihimpun oleh AwanPintar.id®

Administrator Privilege

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

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

Semester 1 Tahun 2025



DoublePulsar Backdoor Communication Installation

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

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

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

Busybox Enable

Merupakan indikator yang menandakan aktivitas mencurigakan terkait penggunaan perintah busybox enable. Ini bukan serangan langsung yang pasti, melainkan indikator anomali atau potensi aktivitas pasca-eksploitasi (misalnya, penyerang mencoba mengaktifkan fitur atau layanan di sistem yang disusupi, terutama pada perangkat IoT atau embedded). Peringatan ini berfungsi sebagai sinyal untuk investigasi lebih lanjut oleh tim keamanan untuk menentukan apakah aktivitas tersebut sah atau merupakan bagian dari serangan.

Penyerang juga seringkali mengunggah atau menggunakan BusyBox untuk menjalankan perintah dasar seperti mengaktifkan atau memfungsikan, komponen Busybox dalam konteks yang tidak biasa atau mencurigakan. Menggunakan busybox enable bisa menjadi bagian dari upaya mereka untuk menyiapkan lingkungan untuk aktivitas berbahaya.

Busybox Shell

BusyBox adalah perangkat lunak yang menyediakan banyak utilitas Unix standar (seperti ls, cp, mv, sh, dll.) dalam satu executable kecil. Ia sering digunakan dalam sistem embedded, perangkat IoT (Internet of Things), firmware router, atau lingkungan Linux minimal karena ukurannya yang kecil dan efisien.

Meskipun BusyBox itu sendiri adalah alat yang sah, keberadaan atau penggunaannya dalam konteks yang tidak biasa di jaringan dapat menjadi indikator kuat adanya aktivitas jahat. Deteksi ini kemungkinan besar dipicu ketika mendeteksi pola komunikasi atau eksekusi perintah yang menunjukkan bahwa penyerang telah mendapatkan akses ke sistem dan menggunakan BusyBox shell untuk melakukan tindakan.

MALWARE Possible Linux.Mirai Login Attempt

Peringatan ini mengindikasikan adanya aktivitas mencurigakan yang terdeteksi pada sistem Linux, menunjukkan kemungkinan upaya masuk (login) yang terkait dengan malware Mirai. Mirai adalah jenis botnet yang terkenal karena kemampuannya dalam menginfeksi perangkat Internet of Things (IoT) yang tidak aman, seperti kamera IP, DVR, dan router, untuk kemudian melancarkan serangan Distributed Denial of Service (DDoS) berskala besar. Upaya login yang terdeteksi ini bisa jadi merupakan indikasi bahwa penyerang mencoba untuk

mendapatkan akses ke sistem Linux Anda menggunakan kredensial yang lemah atau melalui celah keamanan, dengan tujuan untuk menambahkan perangkat Anda ke dalam jaringan botnet Mirai atau melakukan aktivitas jahat lainnya. Sangat penting untuk segera menginvestigasi peringatan ini, memeriksa log sistem, memperbarui semua perangkat lunak, dan memperkuat kebijakan kata sandi untuk mencegah kompromi lebih lanjut.

Besar kemungkinan aktivitas Mirai ini terkait dengan Busybox Shell yang menjadi peringkat ke dua dan ke tiga. Umumnya ketiga ativitas ini merupakan sebuah kesatuan pada saat sebuah serangan dilancarkan terhadap sebuah perangkat.

Bypass Autentikasi RDP

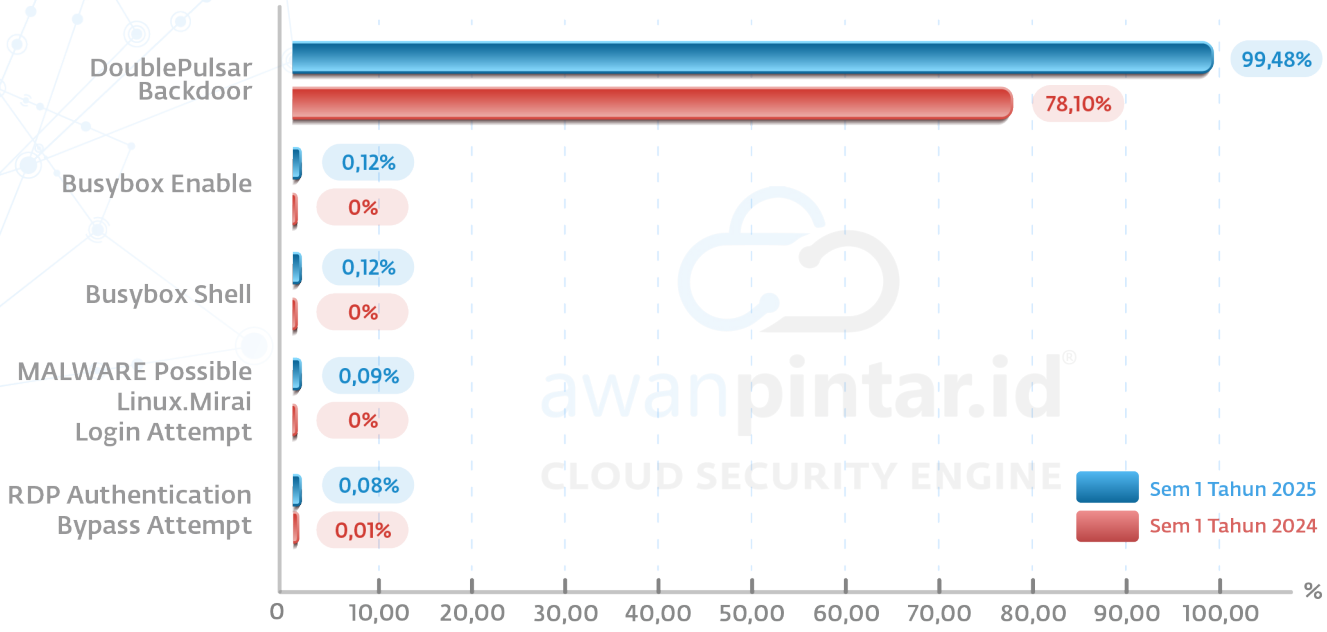
Remote Desktop Protocol (RDP) adalah salah satu protokol komunikasi paling populer untuk sistem pengendalian jarak jauh. RDP hadir dengan semua sistem operasi Windows saat ini, dan antarmuka pengguna grafisnya menjadikannya alat akses jarak jauh yang mudah digunakan. Selain itu, Microsoft memposisikannya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

Green
OPEN

Komparasi Administrator Privilege Semester 1 Tahun 2025 & Semester 1 Tahun 2024



DoublePulsar Backdoor
Mengalami Peningkatan 21,38%

BusyBox Enable
Ancaman Baru

BusyBox Shell
Ancaman Baru

MALWARE Possible Linux.Mirai Login Attempt
Ancaman Baru

Authentication Bypass RDP
Ancaman Baru 0,07%

Data menunjukkan pergeseran lanskap ancaman yang signifikan terkait upaya perolehan hak istimewa (administrator) antara Semester 1 (S1) 2024 dan S1 2025.

Temuan Kunci:

Dominasi Mutlak DoublePulsar Backdoor: Ancaman ini melonjak tajam, dari 78,10% menjadi 92,62%. Ini menunjukkan bahwa DoublePulsar kini menjadi vektor serangan utama untuk mendapatkan hak istimewa, hampir sepenuhnya menggantikan metode lain.

Kemunculan Ancaman Baru Berbasis Linux/IoT: Tiga ancaman baru BusyBox Enable, BusyBox Shell, dan Linux.Mirai muncul dengan kontribusi total 6,34%. Kemunculan mereka secara tiba-tiba mengindikasikan adanya pergeseran fokus penyerang ke sistem berbasis Linux dan perangkat IoT (Internet of Things) yang seringkali menggunakan BusyBox dan menjadi target botnet seperti Mirai.

Ketika melihat peringatan peringatan terkait Mirai dan Busybox, sangat mungkin bahwa upaya login Mirai telah berhasil, dan sekarang malware tersebut sedang menjalankan perintah atau mencoba menginfeksi lebih lanjut melalui shell BusyBox. Deteksi kedua ini mengonfirmasi bahwa ada eksekusi kode yang tidak sah di sistem, yang merupakan indikasi kuat dari kompromi. Langkah-langkah mitigasi darurat harus segera diambil, seperti mengisolasi perangkat, mengganti semua kredensial, memeriksa log secara mendalam, dan memindai malware.

Hilangnya Ancaman Lama: Ancaman Multicast out-of-Bound Read yang sebelumnya signifikan (21,61%) kini hampir menghilang, hanya menyisakan 0,45%. Hal ini menunjukkan bahwa penyerang telah meninggalkan metode lama yang mungkin tidak lagi efektif atau lebih mudah dideteksi.

Implikasi:

Data menunjukkan pergeseran signifikan di mana DoublePulsar Backdoor kini mendominasi (92,62%) sebagai vektor perolehan hak istimewa, menuntut prioritas mitigasi melalui patching dan EDR agresif.

Secara bersamaan, kemunculan ancaman baru berbasis Linux dan IoT (BusyBox, Mirai) mengindikasikan perlunya peningkatan keamanan pada perangkat tersebut (sandi kuat, segmentasi jaringan). Pergeseran dari ancaman lama juga menekankan pentingnya adaptasi deteksi yang terus-menerus, tidak hanya mengandalkan signature tetapi juga analisis perilaku untuk mengidentifikasi taktik penyerang yang terus berevolusi.

Attempted Information Leak

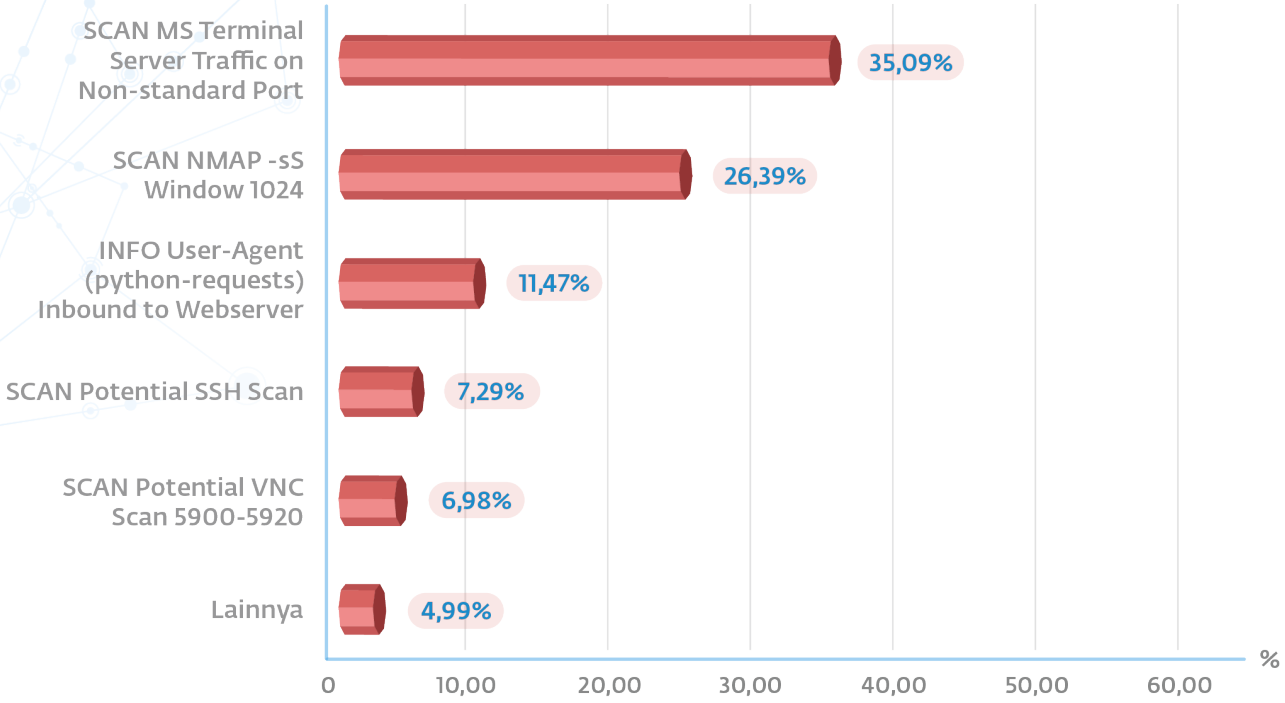
Setiap memasuki semester baru jenis kejahatan siber terus bertambah atau saling mengisi silih berganti, beragamnya variasi serangan menunjukkan bahwa penjahat dunia digital senantiasa mencoba segala cara, atau menguji semua kemungkinan untuk mendapatkan titik serang baru. Serangan Brute Force RDP adalah serangan yang berupaya mengambil paksa hak akses ke jaringan, peningkatan ini didorong karena penyerang sudah mendapat pijakan di dalam sistem, mereka selangkah lagi untuk menguasai hak akses utama sehingga melakukan serangan secara besar-besaran.

Sementara pada ancaman kambuhan yang berulang kali melakukan serangan pada titik yang sama angka serangannya terjun bebas pada satu kategori tapi mengalami eskalasi serangan pada kategori lain dengan jumlah serangan yang cukup besar.Menurunnya upaya pencarian kerentanan melalui Nmap, AwanPintar.id® melihat ini disebabkan karena penyerang sudah jauh hari memiliki pijakan di dalam sehingga fokus mereka bukan mencari kerentanan namun mendapatkan jalan untuk menguasai sistem.

Sehingga dapat diterjemahkan bahwa upaya untuk mengambil informasi sensitif seperti akun, data klien, informasi kartu kredit atau informasi penting lainnya dari data AwanPintar.id® mengalami peningkatan yang progresif. Selain dimonopoli oleh serangan lawas yang berulang pada jaringan internet Indonesia, ditemukan juga dua ancaman baru walaupun tidak signifikan, serangan ini tidak boleh dianggap remeh, setiap ruang yang berhasil dieksploitasi sudah dapat dinilai sebagai kerugian itu sendiri.

Green
OPEN

Semester 1 Tahun 2025



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 -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.

User-Agent (python-requests) Inbound to Webserver

Deteksi Suricata dengan signature "User-Agent (python-requests) Inbound to Webserver" mengindikasikan adanya lalu lintas masuk (inbound) ke webserver Anda yang berasal dari klien dengan User-Agent yang teridentifikasi sebagai "python-requests".

Meskipun penggunaan python-requests itu sendiri tidak selalu berbahaya (banyak aplikasi sah juga menggunakannya), deteksi ini penting karena bisa menjadi indikator aktivitas yang mencurigakan atau berbahaya, seperti pemindaian otomatis, serangan brute force, pengumpulan data, aktivitas bot dan eksploitasi celah kerentanan.

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.

SCAN Potential VNC Scan 5900-5920

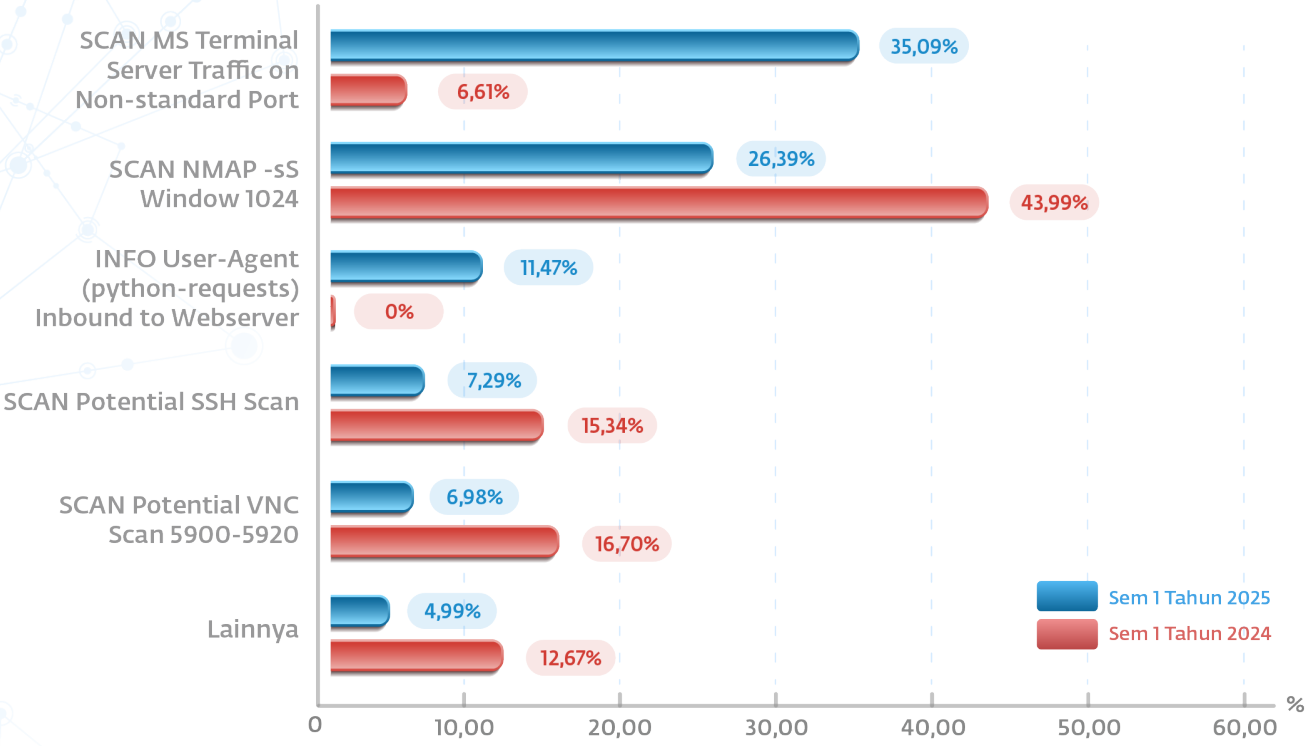
Virtual Network Computing (VNC) adalah sistem kendali desktop jarak jauh yang tidak bergantung pada platform. Ada banyak implementasi VNC (LibVNC, TightVNC, UltraVNC, dll.) yang berjalan di Windows, Linux, macOS, iOS, Android, dan sistem operasi lainnya.

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.

Penting bagi setiap individu dan organisasi untuk memahami risiko yang terkait dengan pencurian kredensial dan mengambil langkah-langkah proaktif untuk melindungi diri mereka sendiri. Kesadaran akan praktik keamanan siber yang baik, seperti penggunaan katasandi yang kuat dan unik, serta penerapan otentikasi dua faktor, menjadi kunci dalam mencegah terjadinya pencurian kredensial.

Green
OPEN

Komparasi Attempted Information Leak Semester 1 Tahun 2025 & Semester 1 Tahun 2024



SCAN MS Terminal Server Traffic on Non-standard Port
Mengalami Peningkatan 28,48%

SCAN NMAP -sS window 1024
Mengalami Penurunan -17,60%

User-Agent (python-requests) Inbound to Webserver
Ancaman Baru

SCAN Potential SSH Scan
Mengalami Penurunan -8,05%

ET SCAN Potential VNC Scan
Mengalami Penurunan -9,72%

Data menunjukkan telah terjadi perubahan yang cukup mencolok dalam taktik ancaman Attempted Information Leak (upaya pencurian atau pengungkapan informasi) antara Semester 1 2024 dan Semester 1 2025.

Temuan Kunci

- Lonjakan Drastis Trafik Terminal Server Non-Standar: Deteksi "SCAN MS Terminal Server Traffic on Non-standard Port" melonjak sangat tajam dari 6,61% menjadi 35,09%, mengalami peningkatan signifikan sebesar 28,48%. Ini menempatkan serangan ini sebagai vektor utama dalam upaya kebocoran informasi.
- Penurunan Signifikan Pemindaian Konvensional: Taktik pemindaian yang lebih umum, seperti "SCAN NMAP -sS window 1024" mengalami penurunan dari 43,99% menjadi 26,39% (-17,60%). Demikian pula, "SCAN Potential VNC Scan" turun dari 16,70% menjadi 6,98% (-9,72%), dan "SCAN Potential SSH Scan" turun dari 15,34% menjadi 7,45% (-8.05%). Ini menunjukkan taktik pemindaian yang lebih "berisik" ini kurang dominan dibandingkan sebelumnya.
- Munculnya Ancaman Baru Python-Requests: Deteksi "User-Agent (python-requests) Inbound to Webserver" muncul sebagai ancaman baru pada Semester 1 2025 dengan persentase 11,47%. Ini mengindikasikan adanya penggunaan scripting berbasis Python yang baru atau lebih terdeteksi dalam upaya kebocoran informasi.

Implikasi

Pergeseran ini mengindikasikan bahwa penyerang telah mengubah taktik mereka secara fundamental dalam upaya pencurian informasi. Mereka kini menjauhi metode pemindaian jaringan yang "berisik" dan mudah dideteksi (seperti NMAP, SSH, VNC scan), dan beralih ke pendekatan yang lebih terfokus dan terselubung.

Lonjakan trafik Terminal Server non-standar menunjukkan penyerang mungkin mencoba memanfaatkan atau menyalahgunakan protokol akses jarak jauh (RDP/Terminal Services) untuk eksfiltrasi data atau komunikasi C2 yang meniru lalu lintas sah. Ini bisa berarti upaya pembobolan yang lebih canggih atau penargetan kelemahan dalam konfigurasi server yang kurang diawasi.

Munculnya User-Agent (python-requests) Inbound to Webserver sebagai ancaman baru menegaskan penggunaan tooling yang fleksibel dan umum oleh penyerang. Pustaka python-requests sering digunakan untuk otomatisasi web, yang berarti penyerang mungkin menggunakan script kustom untuk pengintaian yang lebih spesifik, eksfiltrasi data yang ditargetkan melalui webserver, atau bahkan komunikasi dengan malware di dalam jaringan.

Green
OPEN

SPAM & MALWARE

Spam

Email spam dan phising sama-sama memenuhi kotak masuk kita, tetapi keduanya memiliki tujuan dan risiko yang berbeda secara mendasar. Spam pada dasarnya bersifat promosi, seringkali tidak berbahaya, dalam memamerkan produk atau layanan kepada khalayak luas. Biasanya dikirim secara massal, gangguan utama spam terletak pada volumenya yang sangat banyak, dan skenario terburuknya mungkin melibatkan infeksi malware atau kerugian finansial.

Di sisi lain, email phising adalah email yang lebih licik. Email phising dibuat untuk mengelabui penerima agar mengungkapkan informasi sensitif. Email tersebut mungkin dirancang khusus untuk meniru entitas tepercaya, memanfaatkan ajakan bertindak yang mendesak untuk memikat orang yang tidak menaruh curiga. Meskipun spam pada dasarnya merupakan gangguan, konsekuensi dari penipuan phising lebih parah, mulai dari pencurian identitas hingga dampak finansial yang signifikan atau bahkan pelanggaran data berskala besar.

Meskipun spam dan phising adalah email yang tidak diminta yang dapat menimbulkan ancaman, phising lebih terarah dan seringkali menimbulkan ancaman yang lebih besar, sehingga memerlukan kewaspadaan dan kehati-hatian yang lebih tinggi.

Malware

Malware (singkatan dari malicious software) adalah sebuah kategori luas dari program perangkat lunak yang sengaja dirancang untuk melakukan fungsi-fungsi destruktif, disruptif, atau intrusif terhadap sistem komputer, jaringan, atau data, seringkali tanpa sepengetahuan atau persetujuan pengguna.

Secara teknis, malware beroperasi dengan mengeksploitasi kerentanan (vulnerabilities) pada perangkat lunak, sistem operasi, atau bahkan perilaku pengguna (social engineering) untuk mendapatkan akses yang tidak sah atau melakukan tindakan jahat. Tujuan utamanya bervariasi, mulai dari pencurian informasi sensitif (seperti kredensial, data finansial, atau kekayaan intelektual), sabotase operasional, eskalasi hak akses (privilege escalation), hingga penggunaan sumber daya komputasi korban untuk aktivitas ilegal (misalnya, penambangan cryptocurrency atau serangan DDoS).

Malware menunjukkan polimorfisme tinggi, adaptasi terhadap mekanisme pertahanan, dan seringkali menggunakan teknik obfuscation (penyamaran) untuk menghindari deteksi oleh solusi keamanan tradisional seperti antivirus berbasis tanda tangan. Evolusi malware kini bergerak menuju serangan yang lebih canggih, seperti fileless malware yang beroperasi langsung di memori, zero-day exploits yang memanfaatkan kerentanan yang belum diketahui, serta Advanced Persistent Threats (APTs) yang bertujuan untuk infiltrasi jangka panjang dan spionase.

Persentase Jumlah Spam & Malware Terhadap Total Email Masuk

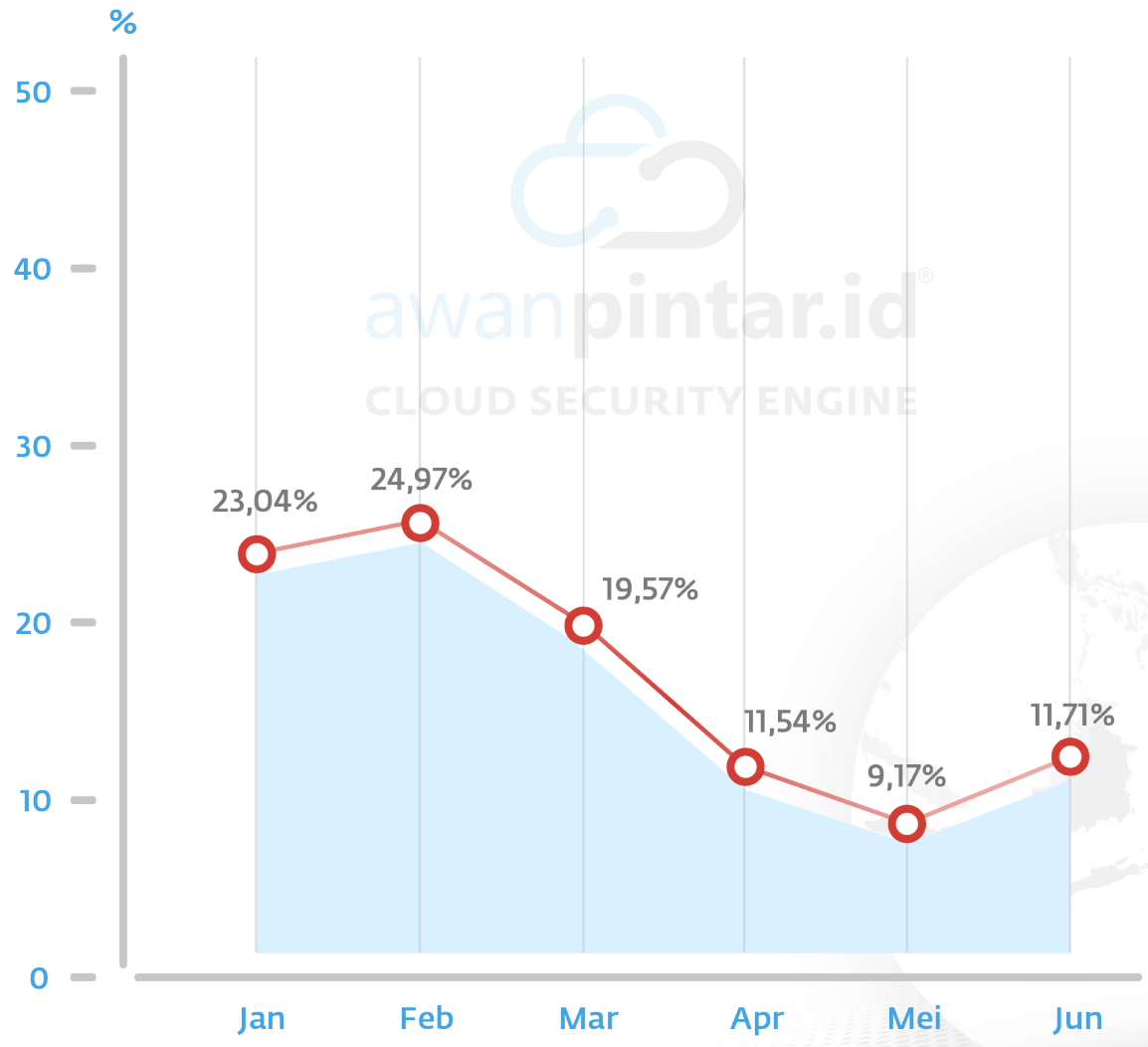
Memantau kesehatan dan keamanan komunikasi digital adalah hal krusial, dan dalam konteks ini, persentase jumlah spam dan malware terhadap total email masuk menjadi indikator vital.

Berdasarkan data yang dihimpun oleh AwanPintar.id®, rasio ini memberikan gambaran jelas mengenai tingkat ancaman yang dihadapi dalam penggunaan email di Indonesia dari lalu lintas email sehari-hari.

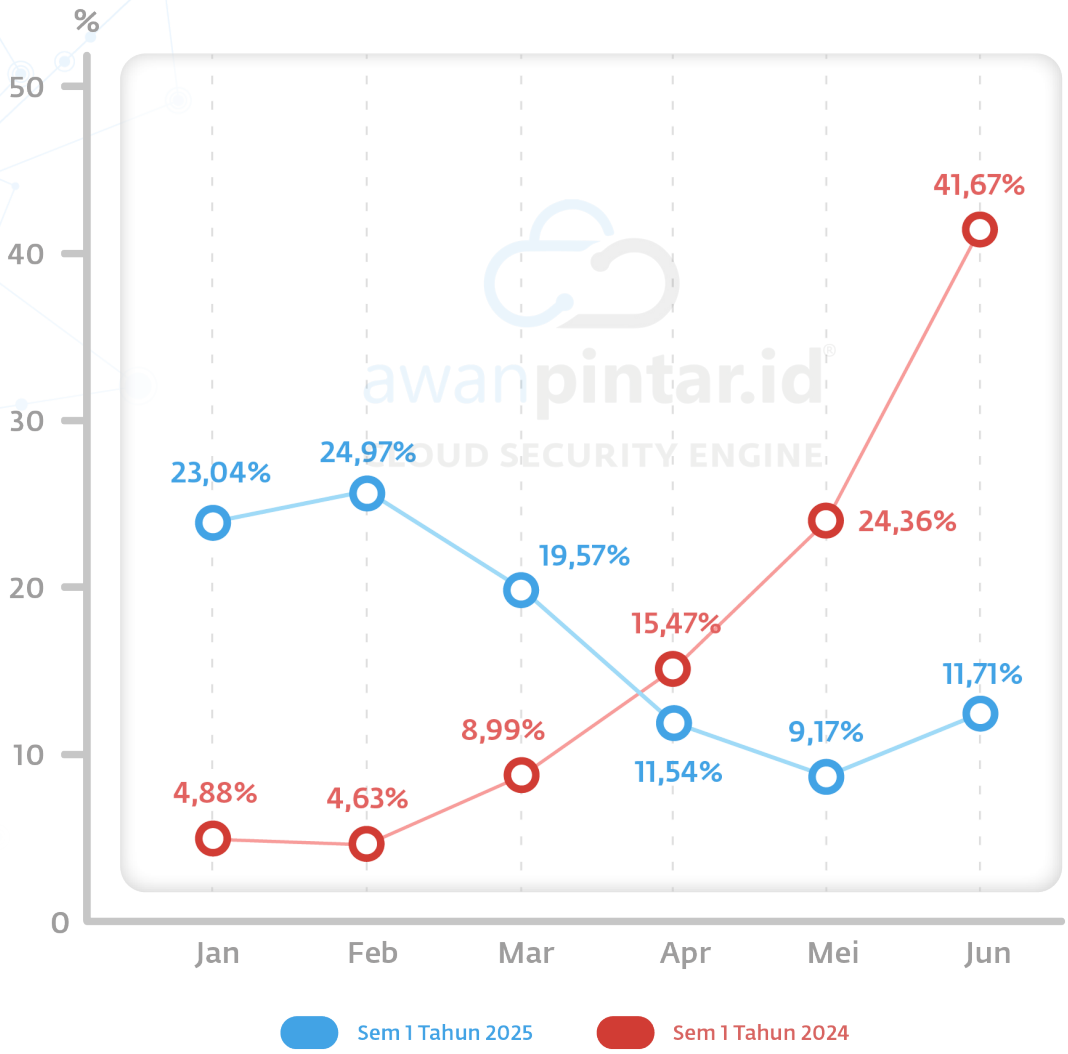
Angka persentase ini tidak hanya mencerminkan seberapa efektif filter keamanan yang diterapkan, tetapi juga menyoroti volume konstan upaya serangan siber dan upaya phising yang beredar, yang berpotensi membahayakan integritas data dan keamanan sistem.

Oleh karena itu, pemahaman mendalam tentang statistik ini sangat penting untuk merumuskan strategi keamanan email yang lebih tangguh dan proaktif.

Jumlah Spam yang Masuk Semester 1 Tahun 2025



Komparasi Jumlah Spam Semester 1 Tahun 2025 & Semester 1 Tahun 2024



Januari
Mengalami Peningkatan 18,16%

Februari
Mengalami Peningkatan 20,34%

Maret
Mengalami Peningkatan 10,58%

April
Mengalami Penurunan -3,93%

Mei
Mengalami Penurunan -15,19%

Juni
Mengalami Penurunan -29,96%

Data komparasi jumlah spam yang terdeteksi selama Semester 1 Tahun 2024 dan Semester 1 Tahun 2025 menunjukkan adanya perubahan pola yang tidak biasa dalam volume spam bulanan. Tren ini memberikan wawasan penting tentang bagaimana aktivitas spamming berevolusi dari waktu ke waktu.

Lonjakan Awal Tahun yang Mencolok di 2025

Pada awal Semester 1 Tahun 2025, terjadi lonjakan spam yang sangat besar dibandingkan dengan tahun sebelumnya:

- Januari 2025 menunjukkan peningkatan drastis sebesar 18,16%, melonjak menjadi 23,04% dari 4,88% di 2024.
- Februari 2025 melanjutkan tren peningkatan, dengan kenaikan tajam sebesar 20,34% menjadi 24,97% dari 4,63% di 2024.
- Maret 2025 juga mengalami peningkatan yang signifikan sebesar 10,58% menjadi 19,57% dari 8,99% di 2024.

Tren ini mengindikasikan adanya intensifikasi aktivitas spamming secara besar-besaran di awal tahun 2025, jauh melebihi volume yang terlihat pada periode yang sama di tahun sebelumnya. Hal ini bisa disebabkan oleh peluncuran kampanye spam skala besar, peningkatan jumlah botnet yang aktif, atau adaptasi penyerang terhadap celah keamanan baru.

Penurunan Drastis di Akhir Semester 1 Tahun 2025

Menariknya, pola tersebut berbalik secara dramatis di pertengahan dan akhir Semester 1 Tahun 2025:

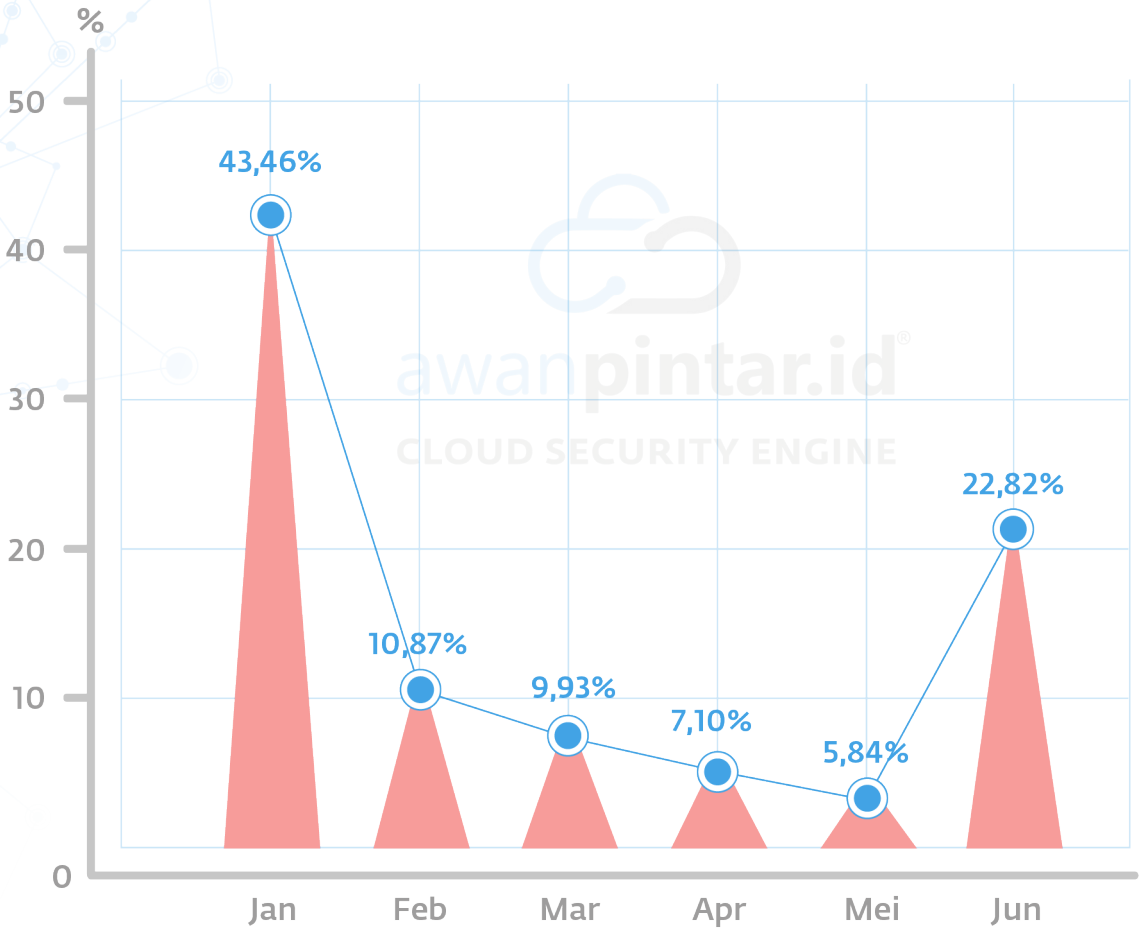
- April 2025 mengalami penurunan sebesar 3,93% dibandingkan April 2024.
- Mei 2025 menunjukkan penurunan yang lebih signifikan sebesar 15,19% (menjadi 9,17% dari 24,36% di 2024).
- Juni 2025 mencatat penurunan paling tajam, yaitu 29,96% (menjadi 11,71% dari 41,67% di 2024).

Penurunan tajam di akhir semester 2025 ini menunjukkan kemungkinan adanya mitigasi yang efektif, atau perubahan strategi dari para spammer yang mungkin beralih ke metode serangan lain, atau bahkan adanya operasi penumpasan botnet yang berhasil.

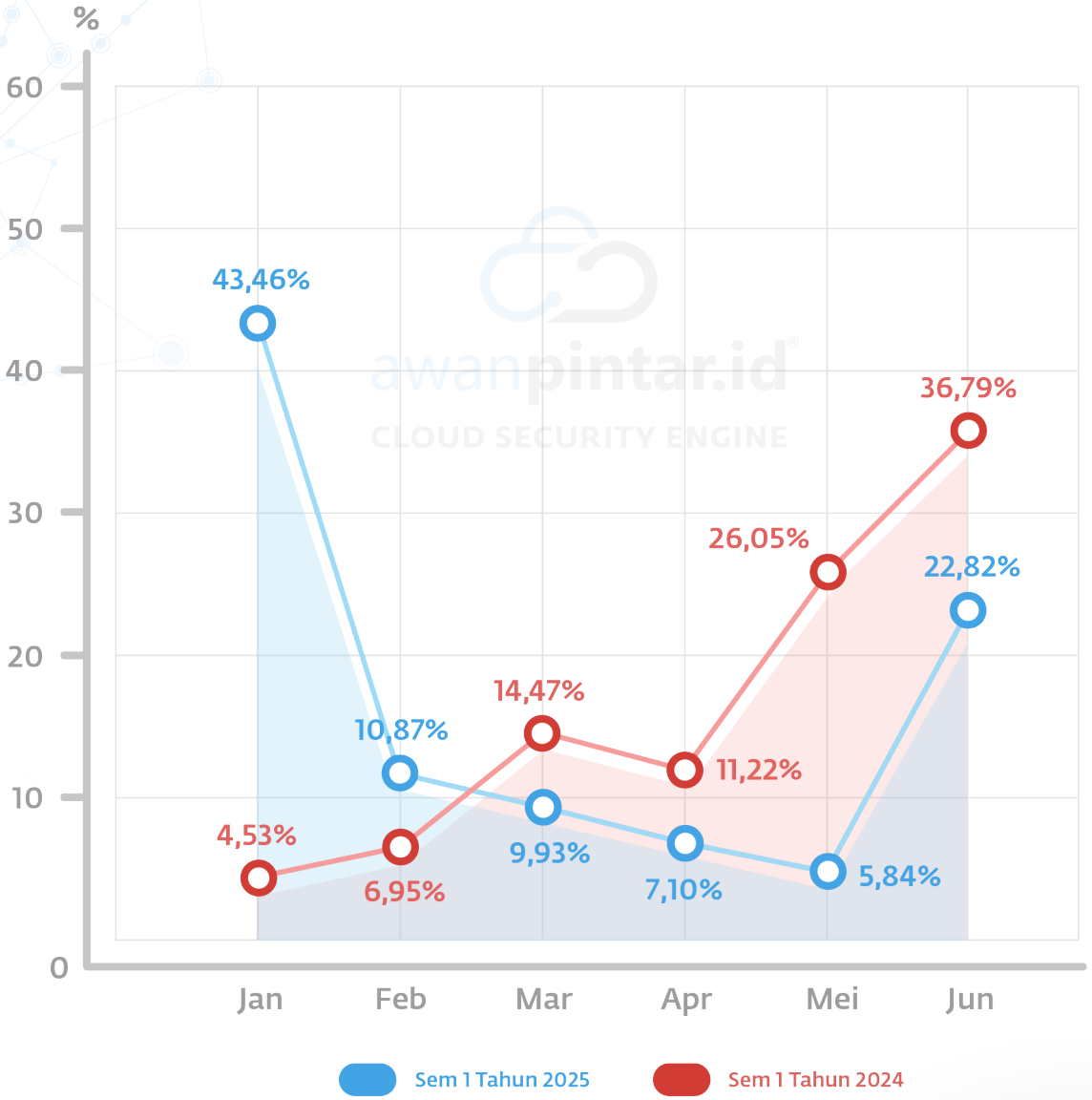
Kesimpulan

Secara keseluruhan, komparasi data ini menggambarkan dinamika yang berlawanan antara awal dan akhir Semester 1 Tahun 2025 dibandingkan dengan tahun 2024. Lonjakan spam yang masif di semester pertama tahun 2025 mengindikasikan serangan yang lebih agresif, sementara penurunan signifikan di kuartal kedua memberikan sinyal positif, meskipun perlu diinvestigasi lebih lanjut untuk memahami penyebab pasti penurunan tersebut. Data ini sangat penting bagi penyedia layanan keamanan dan pengguna untuk terus beradaptasi dengan pola ancaman spam yang terus berubah.

Jumlah Malware yang Masuk Semester 1 Tahun 2025



Komparasi Jumlah Malware Semester 1 Tahun 2025 & Semester 1 Tahun 2024



Januari
Mengalami Peningkatan 38,93%

Februari
Mengalami Peningkatan 3,92%

Maret
Mengalami Penurunan -4,54%

April
Mengalami Penurunan -4,12%

Mei
Mengalami Penurunan -20,21%

Juni
Mengalami Penurunan -13,97%

Analisis Komparasi Jumlah Malware Per Bulan (S1 2024 vs. S1 2025)

Data komparasi jumlah malware yang terdeteksi selama Semester 1 Tahun 2024 dan Semester 1 Tahun 2025 menunjukkan adanya pola aktivitas yang sangat dinamis dan perubahan fokus penyerang dari waktu ke waktu.

Lonjakan Awal Tahun yang Mencolok di 2025

Pada awal Semester 1 Tahun 2025, terjadi lonjakan malware yang sangat besar dibandingkan dengan tahun sebelumnya:

- Januari 2025 menunjukkan peningkatan drastis sebesar 38,93%, melonjak menjadi 43,36% dari 4,53% di 2024. Ini adalah anomali paling menonjol.
- Februari 2025 melanjutkan tren peningkatan, dengan kenaikan sebesar 3,92% menjadi 10,87% dari 6,95% di 2024.

Tren ini mengindikasikan adanya intensifikasi aktivitas malware secara besar-besaran di awal tahun 2025, jauh melebihi volume yang terlihat pada periode yang sama di tahun sebelumnya. Hal ini bisa disebabkan oleh peluncuran kampanye malware skala besar, kemunculan varian baru yang sangat aktif, atau penyerang yang memanfaatkan momen awal tahun.

Penurunan Drastis Menjelang Akhir Semester 1 Tahun 2025

Menariknya, pola yang ekstrem di awal tahun berbalik secara signifikan di pertengahan dan akhir Semester 1 Tahun 2025:

- Maret 2025 mengalami sedikit penurunan sebesar -4,54% dibandingkan Maret 2024.
- April 2025 juga menunjukkan penurunan sebesar -4,12% dibandingkan April 2024.
- Mei 2025 mencatat penurunan yang sangat signifikan sebesar -20,21% (menjadi 5,84% dari 26,05% di 2024).
- Juni 2025 mengalami penurunan berkelanjutan sebesar -13,97% (menjadi 22,82% dari 36,79% di 2024).

Penurunan tajam di akhir semester 2025 ini menunjukkan kemungkinan adanya mitigasi yang efektif terhadap malware yang beredar di awal tahun, atau perubahan strategi dari para pelaku malware yang mungkin beralih ke metode serangan lain yang tidak dikategorikan sebagai malware tradisional, atau bahkan adanya operasi penumpasan infrastruktur malware yang berhasil.

Implikasi

Secara keseluruhan, komparasi data ini menggambarkan dinamika yang sangat kontras antara awal dan akhir Semester 1 Tahun 2025 dibandingkan dengan tahun 2024. Lonjakan malware yang masif di awal tahun 2025 mengindikasikan gelombang serangan yang sangat agresif yang harus diwaspadai di awal setiap tahun.

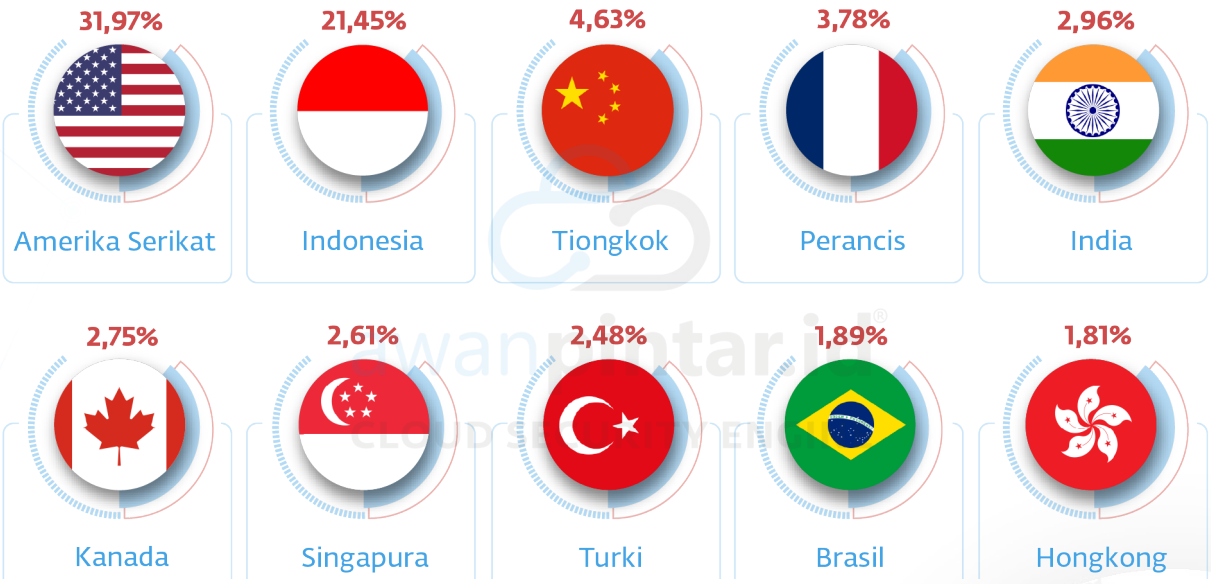
Sementara itu, penurunan signifikan di kuartal kedua memberikan sinyal positif terhadap keberhasilan upaya deteksi dan mitigasi, namun juga menuntut investigasi berkelanjutan untuk memahami apakah penurunan tersebut disebabkan oleh efektivitas pertahanan atau sekadar adaptasi taktik penyerang. Data ini sangat penting bagi penyedia layanan keamanan dan organisasi untuk terus beradaptasi dengan pola ancaman malware yang sangat berubah-ubah.

10 Negara Pengirim Spam Terbanyak

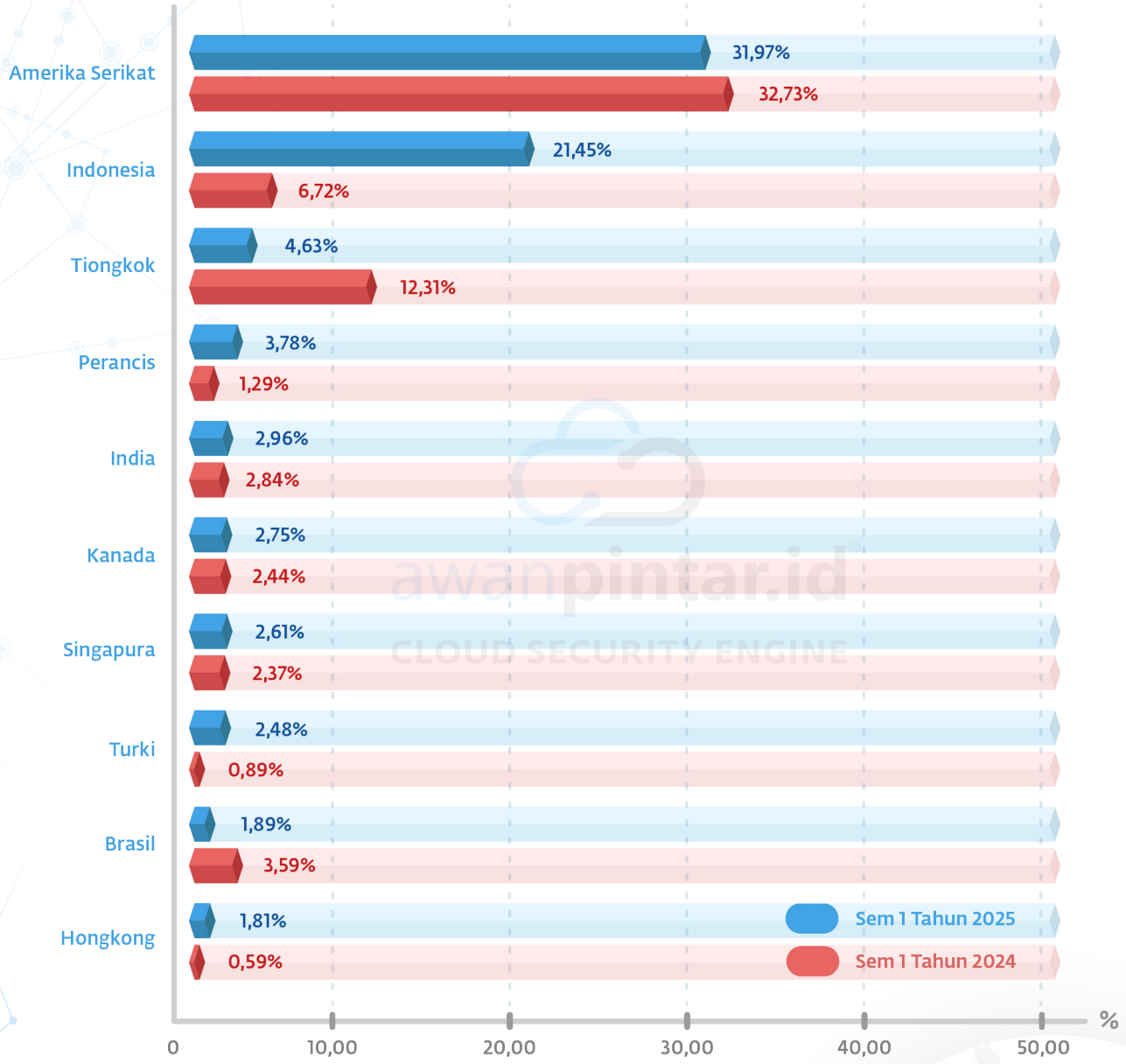
Dalam era konektivitas digital yang tanpa batas, volume email serangan spam yang terus melonjak menjadi tantangan serius bagi keamanan siber di Indonesia. Untuk memberikan perspektif yang lebih mendalam mengenai pola ancaman ini, AwanPintar.id® secara rutin menganalisis lalu lintas data yang masuk.

Data dari AwanPintar.id® ini menunjukkan konsentrasi upaya jahat dari yurisdiksi tertentu, yang mungkin disebabkan oleh keberadaan botnet yang masif, infrastruktur hosting yang disalahgunakan, atau aktivitas siber kriminal yang terorganisir di negara-negara tersebut. Dengan mengetahui asal spam secara spesifik, entitas di Indonesia dapat memperkuat firewall, menyesuaikan filter email, dan meningkatkan kewaspadaan terhadap komunikasi yang berasal dari wilayah berisiko tinggi, sehingga secara proaktif mengurangi eksposur terhadap serangan dan meningkatkan ketahanan siber nasional, sebagai berikut:

Semester 1 Tahun 2025



Komparasi 10 Negara Pengirim Spam Semester 1 Tahun 2025 dan Semester 1 Tahun 2024



Amerika Serikat
Mengalami Penurunan -0,76%

Indonesia
Mengalami Peningkatan 14,73%

Tiongkok
Mengalami Penurunan -7,68%

Perancis
Mengalami Peningkatan 2,49%

India
Mengalami Peningkatan 0,12%

Kanada
Mengalami Peningkatan 0,31%

Singapura
Negara Pengirim Spam Baru 0,24%

Turki
Negara Pengirim Spam Baru 1,59%

Brasil
Mengalami Penurunan -1,70%

Hongkong
Negara Pengirim Spam Baru 1,22%

Data yang dihimpun oleh AwanPintar.id® menunjukkan adanya pergeseran signifikan dalam lanskap negara kontributor pengirim spam yang menargetkan Indonesia. Tren ini mengindikasikan dinamika baru dalam aktivitas siber global yang perlu diwaspadai, terutama peningkatan ancaman dari dalam negeri.

Peningkatan Dominasi dan Ancaman Internal

Amerika Serikat tetap menjadi kontributor utama spam, dengan persentase 31,97% di Semester 1 Tahun 2025. Meskipun mengalami penurunan tipis sebesar -0,76% dari 32,73% di tahun sebelumnya, AS tetap memegang posisi teratas sebagai sumber spam terbesar yang menargetkan Indonesia.

Yang paling mencolok adalah lonjakan ekstrem dari Indonesia sendiri, yang melonjak dramatis dari 6,72% pada Semester 1 Tahun 2024 menjadi 21,45% pada Semester 1 Tahun 2025, menandai kenaikan signifikan sebesar 14,73%. Kemunculan Indonesia di posisi kedua ini merupakan indikator kuat adanya kompromi infrastruktur domestik, seperti botnet atau server yang disalahgunakan di dalam negeri, yang kini turut aktif menyebarkan spam.

Tiongkok, meskipun masih signifikan, menunjukkan penurunan kontribusi sebesar -7,68% (dari 12,31% menjadi 4,63%). Ini menunjukkan pergeseran fokus atau penurunan efektivitas infrastruktur spam mereka terhadap Indonesia.

Perancis mengalami peningkatan substansial sebesar 2,49% (dari 1,29% menjadi 3,78%), menjadikannya pemain yang lebih menonjol.

India dan Kanada juga menunjukkan peningkatan masing-masing sebesar 0,12% (dari 2,84% menjadi 2,96%) dan 0,31% (dari 2,44% menjadi 2,75%), menunjukkan kontribusi yang sedikit meningkat.

Kemunculan Sumber Baru dan Penurunan Kontribusi Lama

Daftar 10 besar pada Semester 1 Tahun 2025 memperkenalkan tiga pemain yang masuk sebagai pendatang baru (dengan peningkatan persentase yang signifikan dari tahun sebelumnya atau baru terdeteksi secara dominan):

- Singapura, dengan peningkatan 0,24% (dari 2,37% menjadi 2,61%).
- Turki, dengan peningkatan 1,59% (dari 0,89% menjadi 2,48%).
- Hong Kong, dengan peningkatan 1,22% (dari 0,59% menjadi 1,81%).
- Kehadiran mereka mengindikasikan diversifikasi sumber spam global.

Sebaliknya, Brasil mengalami penurunan sebesar -1,70% (dari 3,59% menjadi 1,89%).

Implikasi

Ancaman spam yang masuk ke Indonesia bersifat sangat dinamis. Peningkatan drastis dari sumber domestik di Indonesia menjadi peringatan keras bagi entitas lokal untuk lebih intensif dalam mengamankan infrastruktur mereka. Hal ini memerlukan audit keamanan yang lebih sering pada server, jaringan, dan perangkat pengguna di Indonesia untuk mengidentifikasi dan membersihkan botnet atau malware yang mungkin beroperasi dari dalam.

Sementara itu, meskipun Amerika Serikat tetap menjadi sumber utama, kemunculan beragam negara baru dan pergeseran persentase dari sumber lama menunjukkan bahwa strategi pertahanan siber harus adaptif, tidak hanya berfokus pada sumber tradisional tetapi juga mewaspadai ancaman yang muncul dari berbagai belahan dunia, termasuk dari dalam negeri sendiri. Ini menekankan pentingnya threat intelligence yang komprehensif dan kemampuan untuk merespons ancaman dari lokasi geografis yang beragam.

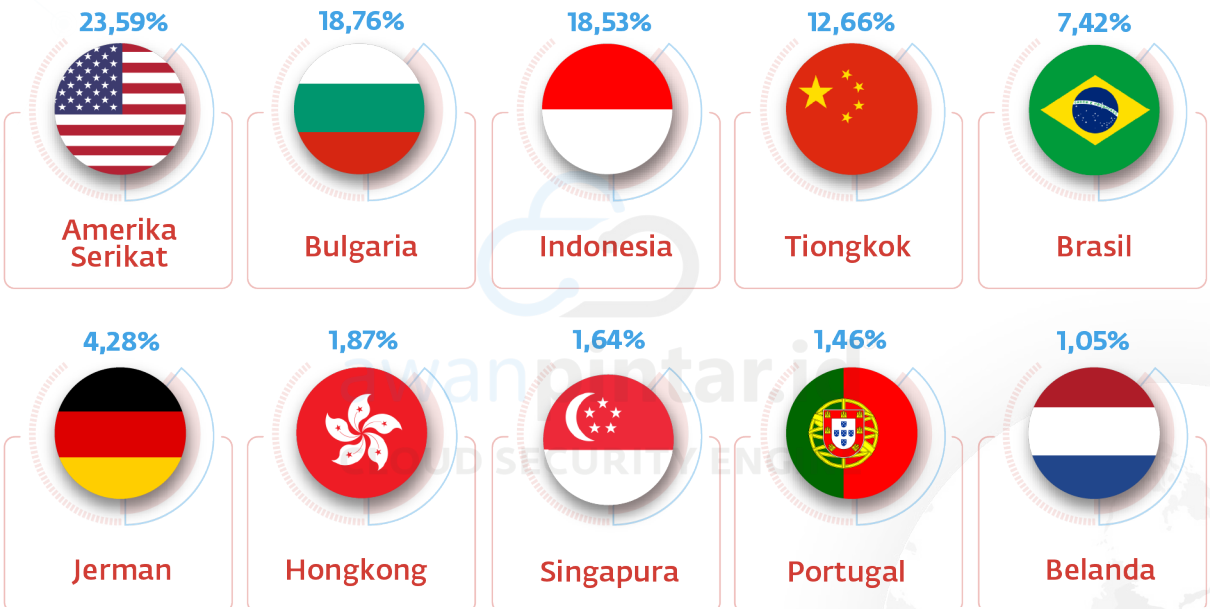
10 Negara Pengirim Malware Terbanyak

Ancaman malware terus menjadi bayangan gelap yang mengintai di dunia digital, mengancam data pribadi hingga infrastruktur penting. Untuk memberikan gambaran yang lebih jelas mengenai asal-muasal serangan ini, AwanPintar.id® telah mengumpulkan dan menganalisis data mengenai 10 negara pengirim malware terbesar selama semester pertama tahun 2025.

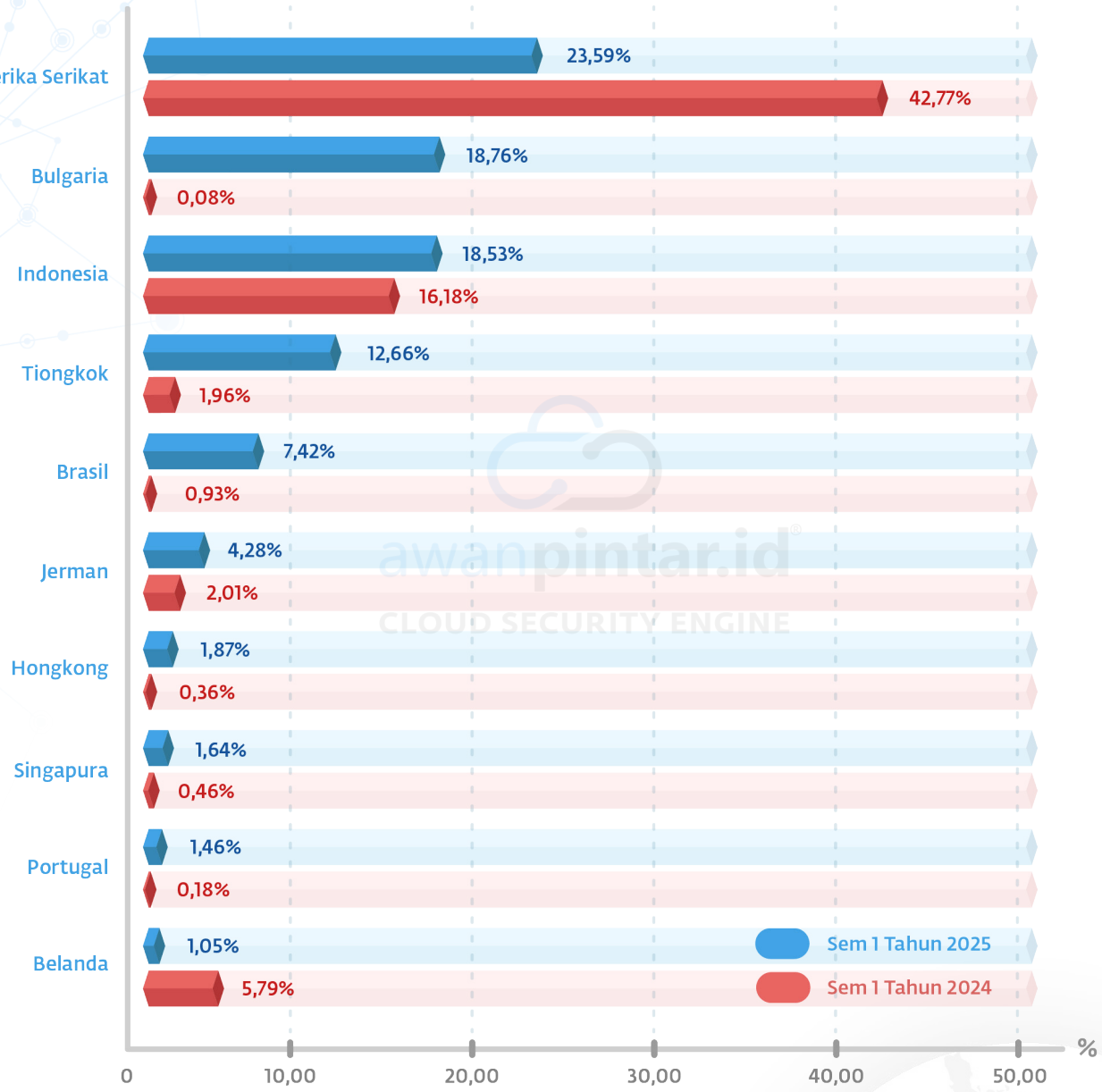
Statistik ini tidak hanya menunjukkan peta persebaran ancaman siber secara global, tetapi juga menyoroti titik-titik panas di mana malware paling banyak berasal. Pemahaman akan data ini sangat penting bagi kita semua untuk meningkatkan kewaspadaan dan memperkuat sistem keamanan digital kita.

Deskripsi Serangan Malware

Semester 1 Tahun 2025



Komparasi 10 Negara Pengirim Malware Semester 1 Tahun 2025 dan Semester 1 Tahun 2024



Amerika Serikat
Mengalami Penurunan -19,18%

Bulgaria
Negara Pengirim Baru 18,68%

Indonesia
Mengalami Peningkatan 2,35%

Tiongkok
Negara Pengirim Baru 10,70%

Brasil
Mengalami Peningkatan 6,49%

Jerman
Mengalami Peningkatan 2,27%

Hongkong
Negara Pengirim Baru 1,51%

Singapura
Mengalami Peningkatan 1,18%

Portugal
Negara Pengirim Baru 1,28%

Belanda
Mengalami Penurunan -4,74%

Data yang dihimpun oleh AwanPintar.id® menunjukkan adanya perubahan yang cukup signifikan dalam lanskap negara kontributor pengirim malware yang menargetkan Indonesia. Pola ini mengindikasikan dinamika baru dalam sumber ancaman malware global, dengan beberapa negara menunjukkan peningkatan drastis.

Pergeseran Dominasi dan Kemunculan Sumber Baru yang Agresif

Amerika Serikat, meskipun masih menjadi kontributor utama, menunjukkan penurunan drastis sebesar -19,18% (dari 42,77% menjadi 23,59%). Ini menandakan penurunan signifikan dalam perannya sebagai sumber malware dominan yang menargetkan Indonesia.

Yang paling mencolok adalah lonjakan ekstrem dari Bulgaria, yang melonjak dari 0,08% menjadi 18,76% pada Semester 1 Tahun 2025. Peningkatan sebesar 18,68% ini menempatkan Bulgaria sebagai pengirim malware kedua terbesar dan menandai kemunculannya sebagai pemain baru yang sangat agresif.

Indonesia sendiri menunjukkan peningkatan sebesar 2,35% (dari 16,18% menjadi 18,53%). Ini menempatkan Indonesia di posisi ketiga, semakin menegaskan adanya infrastruktur domestik yang terkompromi, seperti botnet atau server yang disalahgunakan di dalam negeri, yang kini juga menjadi sumber penting penyebaran malware.

Tiongkok juga muncul sebagai pengirim baru yang signifikan, melonjak 10,70% (dari 1,96% menjadi 12,66%). Ini menempatkan Tiongkok di posisi keempat dan menunjukkan peningkatan fokus dari negara ini dalam penyebaran malware.

Beberapa negara lain juga menunjukkan peningkatan:
- Brasil melonjak 6,49% (dari 0,93% menjadi 7,42%).
- Jerman meningkat 2,27% (dari 2,01% menjadi 4,28%).
- Hong Kong naik 1,51% (dari 0,36% menjadi 1,87%).
- Singapura meningkat 1,18% (dari 0,46% menjadi 1,64%).
- Portugal muncul sebagai pengirim baru dengan peningkatan 1,28% (dari 0,18% menjadi 1,46%).

Penurunan Kontribusi dari Sumber Lama

Belanda mengalami penurunan substansial sebesar -4,74% (dari 5,79% menjadi 1,05%), menunjukkan penurunan perannya sebagai sumber malware yang signifikan ke Indonesia.

Implikasi

Lanskap ancaman malware yang masuk ke Indonesia menunjukkan dinamika pergeseran kekuatan yang jelas. Penurunan dominasi Amerika Serikat, bersamaan dengan lonjakan ekstrem dari Bulgaria dan Tiongkok, mengindikasikan adanya pergeseran geografis dalam sumber malware global. Hal ini mungkin terkait dengan pengembangan infrastruktur malware baru atau pergeseran fokus kelompok penjahat siber.

Peningkatan kontribusi dari Indonesia sendiri merupakan peringatan serius. Ini menunjukkan bahwa infrastruktur di dalam negeri semakin sering dikompromikan dan digunakan sebagai bagian dari jaringan distribusi malware. Organisasi dan individu di Indonesia perlu memperketat keamanan siber internal, melakukan audit rutin, dan membersihkan sistem yang terinfeksi untuk mencegah mereka menjadi bagian dari botnet atau malware global.

Strategi pertahanan siber harus beradaptasi dengan cepat untuk menargetkan sumber-sumber yang sedang meningkat ini. Ini mencakup peningkatan threat intelligence yang spesifik untuk regional, pemblokiran lalu lintas dari IP range yang diketahui terlibat dalam aktivitas malware dari negara-negara yang melonjak, dan peningkatan deteksi perilaku anomali untuk mengidentifikasi ancaman yang berasal dari dalam negeri.

Green
OPEN

PORT FAVORIT PERETAS

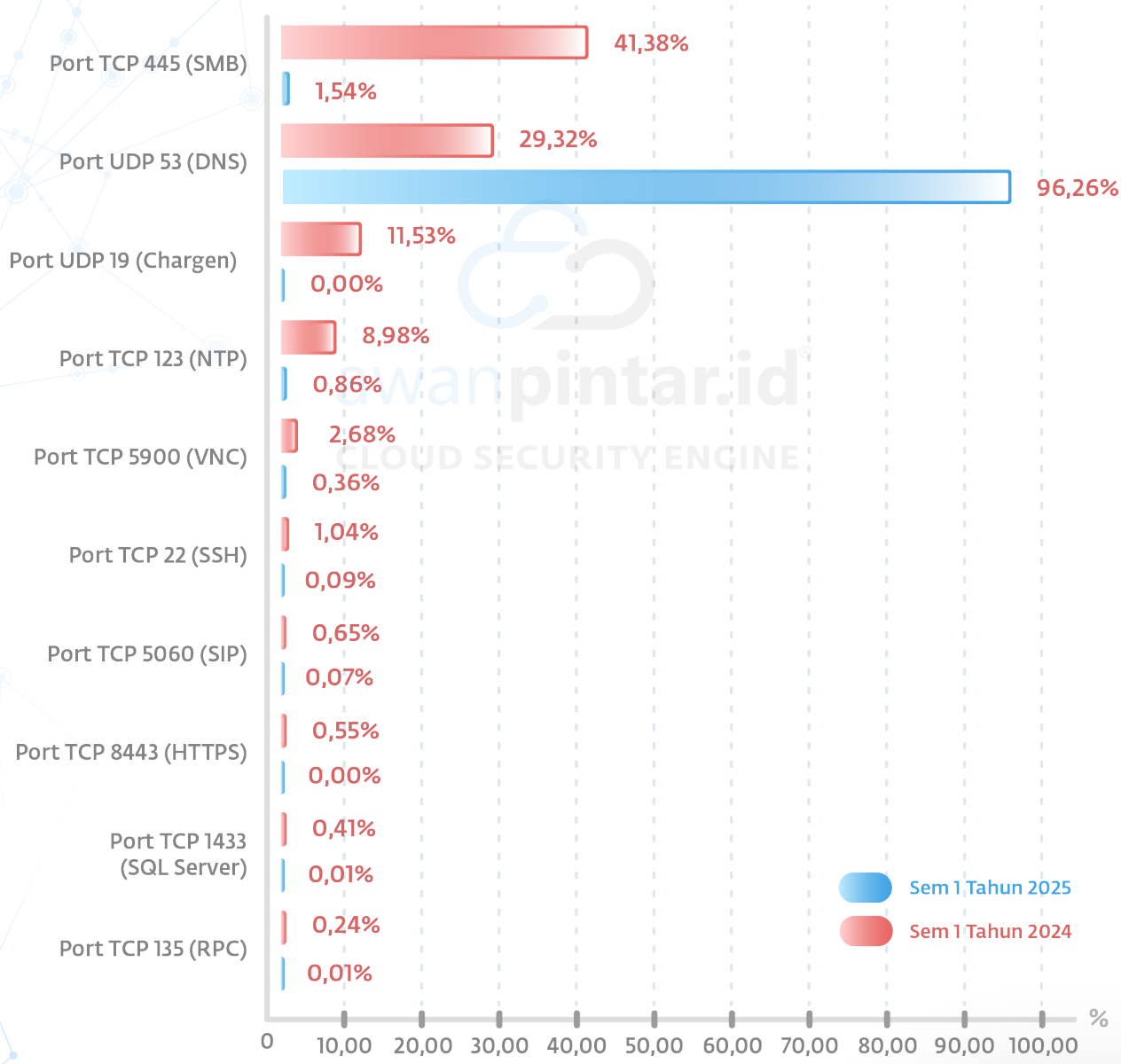
Berdasarkan analisis komprehensif dari AwanPintar.id®, terungkap bahwa sejumlah port standar terus-menerus menunjukkan tingkat keterbukaan dan kerentanan yang tinggi di berbagai infrastruktur. Persentase ini bukan sekadar angka, ia mencerminkan seberapa luas celah keamanan yang belum tertutup dan bagaimana port-port tersebut menjadi target utama bagi aktor jahat siber yang selalu mencari titik masuk termudah untuk eksploitasi.

Data persentase kerentanan port dari AwanPintar.id® ini menjadi tolok ukur penting bagi organisasi dan individu dalam memetakan risiko siber mereka. Tingginya persentase port-port tertentu yang terbuka atau tidak terproteksi secara memadai mengindikasikan adanya praktik konfigurasi yang lemah, kurangnya pembaruan keamanan, atau abainya pengawasan terhadap layanan yang berjalan di belakang port-port tersebut.

Pemahaman akan statistik ini sangat vital untuk memprioritaskan upaya mitigasi, mulai dari menutup port yang tidak perlu, memperketat aturan firewall, hingga mengimplementasikan sistem deteksi intrusi, demi membangun pertahanan siber yang lebih kokoh dan proaktif di seluruh ekosistem digital Indonesia. Dari data yang berhasil dikumpulkan, di bawah ini adalah data port paling rentan, sebagai berikut:

Port	Persentase
Port TCP 445 (SMB)	41,38%
Port UDP 53 (DNS)	29,32%
Port UDP19 (Chargen)	11,53%
Port UDP 123 (NTP)	8,98%
Port TCP 5900 (VNC)	2,68%
Port TCP 22 (SSH)	1,04%
Port TCP 5060 (SIP)	0,65%
Port TCP 8443 (HTTPS)	0,55%
Port TCP 1433 (SQL Server)	0,41%
Port TCP 135 (RPC)	0,24%

Komparasi Port Paling Rentan Semester 1 Tahun 2025 & Tahun 2024



Port TCP 445 (SMB)
Mengalami Peningkatan 39,84%

Port UDP 53 (DNS)
Mengalami Penurunan -66,94%

Port UDP 19 (CHARGEN)
Port Paling Rentan Baru 11,53%

Port TCP 123 (NTP)
Mengalami Peningkatan 8,12%

Port TCP 5900 (VNC)
Mengalami Peningkatan 2,32%

Port TCP 22 (SSH)
Mengalami Peningkatan 0,95%

Port TCP 5060 (SIP)
Mengalami Peningkatan 0,58%

Port TCP 8443 (HTTPS)
Port Paling Rentan Baru 0,55%

Port TCP 1433 (SQL Server)
Port Paling Rentan Baru 0,40%

Port TCP 135 (RPC)
Mengalami Peningkatan 0,23%

Data ini menunjukkan pergeseran signifikan dalam port jaringan yang paling sering ditargetkan atau disalahgunakan oleh penyerang antara S1 2024 dan S1 2025.

Temuan Kunci:

1. Dominasi Baru Port TCP 445 (SMB): melonjak drastis dari 1,54% menjadi 41,38% (+39,84%). Ini menjadi port paling rentan pada S1 2025, mengindikasikan peningkatan serangan terkait SMB (misalnya ransomware, pergerakan lateral).
2. Penurunan Tajam Port UDP 53 (DNS): mengalami penurunan masif dari 96,26% menjadi 29,32% (-66,94%). Ini menunjukkan penyerang beralih dari serangan berbasis DNS yang sebelumnya dominan.
3. Kemunculan Port Amplifikasi DDoS Baru: Port UDP 19 (Chargen) dan TCP 8443 (HTTPS) muncul sebagai port rentan baru, dengan CHARGEN mencapai 11,53%. Selain itu, Port TCP 123 (NTP) juga mengalami peningkatan signifikan dari 0,86% menjadi 8,98%. Ini semua adalah protokol yang dapat disalahgunakan untuk serangan DDoS amplification.
4. Peningkatan Serangan Akses/Layanan: Port seperti TCP 5900 (VNC) (+2,32%), TCP 22 (SSH) (+0,95%), TCP 5060 (SIP) (+0,58%), TCP 1433 (SQL Server) (ancaman baru 0,40%), dan TCP 135 (RPC) (+0,23%) semuanya menunjukkan peningkatan. Ini mengindikasikan upaya penyerang untuk mendapatkan akses ke sistem atau mengeksploitasi layanan spesifik.

Implikasi:

Lanskap kerentanan port telah berubah drastis. Penyerang kini secara agresif menargetkan kelemahan SMB (Port TCP 445) yang sangat terkait dengan ransomware dan pergerakan di dalam jaringan. Mereka juga beralih dari serangan DDoS berbasis DNS ke metode amplification yang berbeda menggunakan protokol seperti Chargen dan NTP.

Peningkatan serangan pada port akses/layanan lain menunjukkan penyerang terus mencari celah di berbagai layanan yang terekspos. Organisasi harus segera memperketat keamanan SMB, memitigasi risiko DDoS amplification, dan mengamankan layanan yang terekspos di port-port yang menunjukkan peningkatan aktivitas ini.

DEFINISI PORT

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 53 DNS

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

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

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

Port UDP 19 CHARGEN

Character Generator Protocol (CHARGEN) adalah layanan jaringan sederhana yang dirancang terutama untuk pengujian, debugging, dan pengukuran kinerja jaringan. Saat terhubung, server yang menjalankan protokol CHARGEN terus-menerus menghasilkan aliran karakter acak hingga klien menutup koneksi. Awalnya dikembangkan untuk tujuan diagnostik, protokol ini jarang digunakan dalam sistem modern tetapi masih ada di banyak perangkat dan instalasi lama.

CHARGEN menimbulkan risiko keamanan yang signifikan karena kemampuan aliran datanya yang tidak diautentikasi dan berkelanjutan. Ini terkenal digunakan dalam serangan amplifikasi untuk Distributed Denial of Service (DDoS). Penyerang mengirim

paket UDP palsu ke server CHARGEN, yang merespons dengan paket yang jauh lebih besar ke korban palsu, sehingga membuat jaringan mereka kewalahan.

Tidak adanya autentikasi atau pembatasan kecepatan membuatnya rentan terhadap eksploitasi oleh pelaku jahat yang bertujuan menghasilkan lalu lintas berlebih. Secara historis, perangkat yang salah konfigurasi yang menjalankan CHARGEN telah disalahgunakan sebagai reflektor atau penguat dalam kampanye serangan.

Port TCP 123 NTP

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

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

Port TCP 5900 VNC

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

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

Port TCP 22 SSH

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 5060 SIP

Port 5060 didedikasikan untuk Session Initiation Protocol (SIP), yang memungkinkan perangkat memulai, memelihara, dan mengakhiri sesi komunikasi dalam voice over IP (VoIP) dan aplikasi multimedia lainnya. SIP diangkut melalui UDP dan TCP. Ini adalah protokol kontrol Lapisan Aplikasi yang membuat, memodifikasi, dan mengakhiri sesi dengan satu atau lebih peserta. SIP adalah protokol peer-to-peer.

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

biasanya digunakan untuk lalu lintas yang dienkripsi dengan Transport Layer Security (TLS).

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

Port TCP 8443 HTTPS

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

Port HTTPS 8443 terutama digunakan sebagai alternatif untuk komunikasi web yang aman. Umumnya digunakan untuk aplikasi berbasis web agar data yang mengalir antara pengguna dan server tetap terenkripsi dan aman dari kemungkinan penyadapan.

Port 8443 dapat rentan terhadap serangan eksekusi kode jarak jauh (RCE). Misalnya, kerentanan CVE-2023-38035 di Ivanti Sentry memungkinkan penyerang yang tidak diautentikasi untuk membaca dan menulis file ke server Ivanti Sentry. Penyerang juga dapat menjalankan perintah OS sebagai administrator sistem (root).

Port TCP 1433 SQL Server

Port 1433 adalah port jaringan yang umum digunakan yang terkait dengan sistem manajemen basis data Microsoft SQL Server. Port ini adalah port default yang digunakan oleh SQL Server untuk berkomunikasi dengan aplikasi klien dan server basis data lainnya.

Saat instans SQL Server diinstal, biasanya dikonfigurasikan untuk mendengarkan koneksi masuk pada port 1433. Port ini penting untuk aplikasi yang perlu berinteraksi dengan database SQL Server, karena menyediakan cara standar bagi klien dan server untuk bertukar data dan perintah.

Meskipun penting untuk fungsionalitas, port ini juga menjadi target utama serangan karena kerentanannya. Jika tidak diamankan dengan baik, port ini dapat dieksploitasi untuk berbagai ancaman keamanan, termasuk akses tidak sah, pencurian data, penyebaran malware, dan serangan DDoS.

Port TCP 135 RPC

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

Tujuan dari port 135 adalah untuk memfasilitasi komunikasi jarak jauh antara klien dan server di lingkungan Windows. Tanpa akses ke port 135 pada perangkat, perangkat lain tidak akan dapat menentukan layanan apa yang tersedia pada perangkat tersebut, dan juga tidak dapat mengetahui port mana yang menjalankan layanan tersebut.

Green
OPEN

COMMON VULNERABILITY & EXPOSURES

Common Vulnerabilities and Exposures (CVE) adalah sistem penomoran standar untuk kerentanan keamanan informasi yang diketahui publik. Setiap kerentanan yang terdaftar di CVE diberikan pengenal unik yang memungkinkan para profesional keamanan untuk merujuk dan melacak kerentanan tersebut secara konsisten. CVE dikelola oleh MITRE Corporation dan didanai oleh Badan Keamanan Siber dan Infrastruktur (CISA) Departemen Keamanan Dalam Negeri AS.

Tujuan utama CVE adalah untuk menyediakan cara standar untuk mengidentifikasi dan mendiskusikan kerentanan keamanan. Dengan adanya CVE, para peneliti keamanan, vendor perangkat lunak, dan pengguna akhir dapat berkomunikasi secara efektif tentang kerentanan yang sama, terlepas dari perbedaan terminologi atau alat yang digunakan. Hal ini mempermudah proses penanganan kerentanan, mulai dari identifikasi hingga perbaikan.

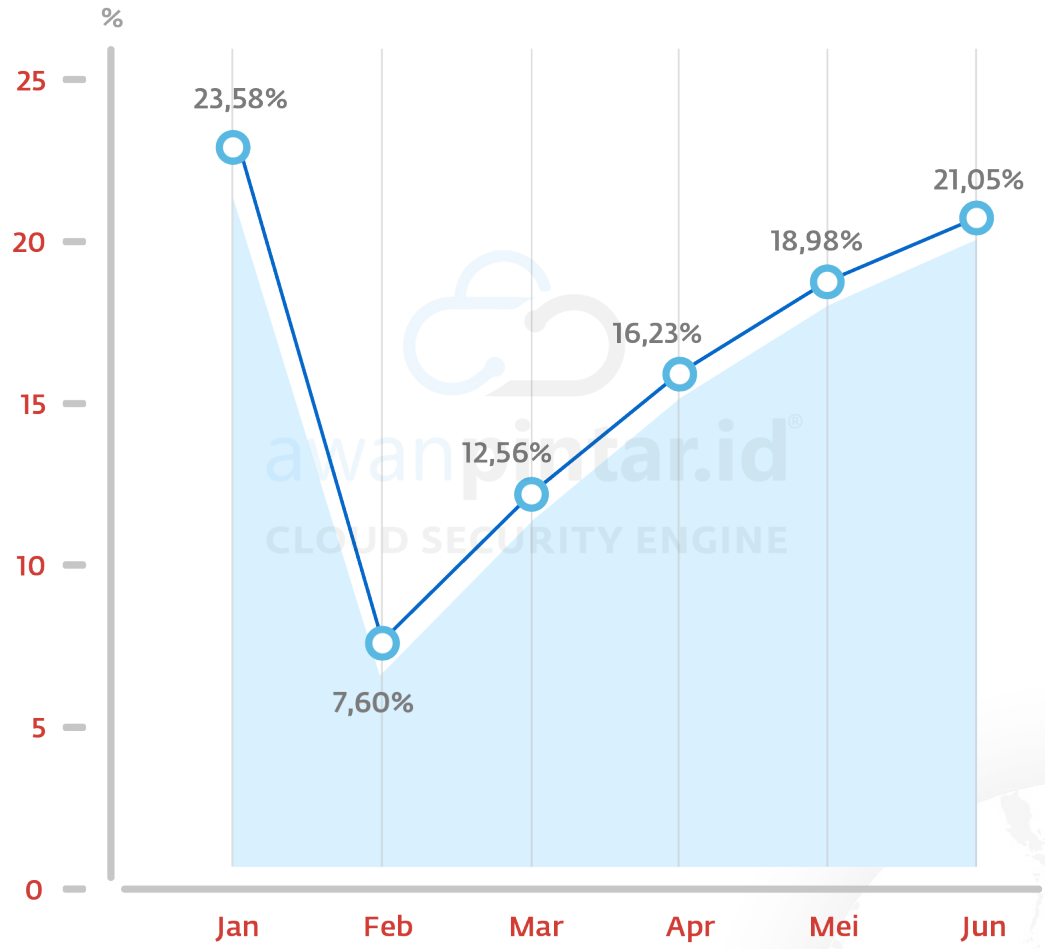
Setiap entri CVE mencakup deskripsi singkat tentang kerentanan, perangkat lunak atau perangkat keras yang terpengaruh, dan referensi ke informasi lebih lanjut. Informasi ini sangat berharga bagi organisasi dalam menilai risiko keamanan mereka dan memprioritaskan upaya perbaikan. CVE juga terintegrasi dengan alat dan database keamanan lainnya, sehingga memudahkan para profesional keamanan untuk mengotomatiskan proses manajemen kerentanan.

Meskipun CVE sangat berguna, penting untuk diingat bahwa CVE hanyalah sebuah daftar kerentanan yang diketahui. Kerentanan baru terus ditemukan, dan tidak semua kerentanan akan terdaftar di CVE. Oleh karena itu, perusahaan tidak boleh hanya mengandalkan CVE untuk melindungi diri mereka dari ancaman keamanan. Mereka juga perlu menerapkan praktik keamanan yang baik, seperti pembaruan perangkat lunak secara teratur, pemantauan jaringan, dan pelatihan kesadaran keamanan bagi karyawan.

EKSPLOITASI CVE SEMESTER 1 TAHUN 2025

Setiap hari, kita makin bergantung pada teknologi, mulai dari smartphone di genggaman hingga sistem besar yang menggerakkan berbagai layanan penting. Namun, di balik kemudahan itu, ada ancaman tersembunyi yang disebut CVE (Common Vulnerabilities and Exposures), atau celah keamanan.

Sepanjang semester pertama tahun 2025 ini, celah-celah tersebut terus dieksploitasi, menciptakan lubang besar bagi para penjahat siber untuk menyerang data dan privasi kita. Mari kita telaah lebih jauh bagaimana eksploitasi CVE ini berkembang dan apa artinya bagi keamanan digital kita.



Green
OPEN

EKSPLOITASI CVE BERDASAR TAHUN RILIS

Keamanan siber bukan lagi sekadar urusan perusahaan besar, tetapi telah menjadi perhatian kita semua. Dengan menganalisis total serangan CVE (Common Vulnerabilities and Exposures) berdasar tahunnya, kita bisa melihat dengan jelas bagaimana ancaman siber berevolusi.

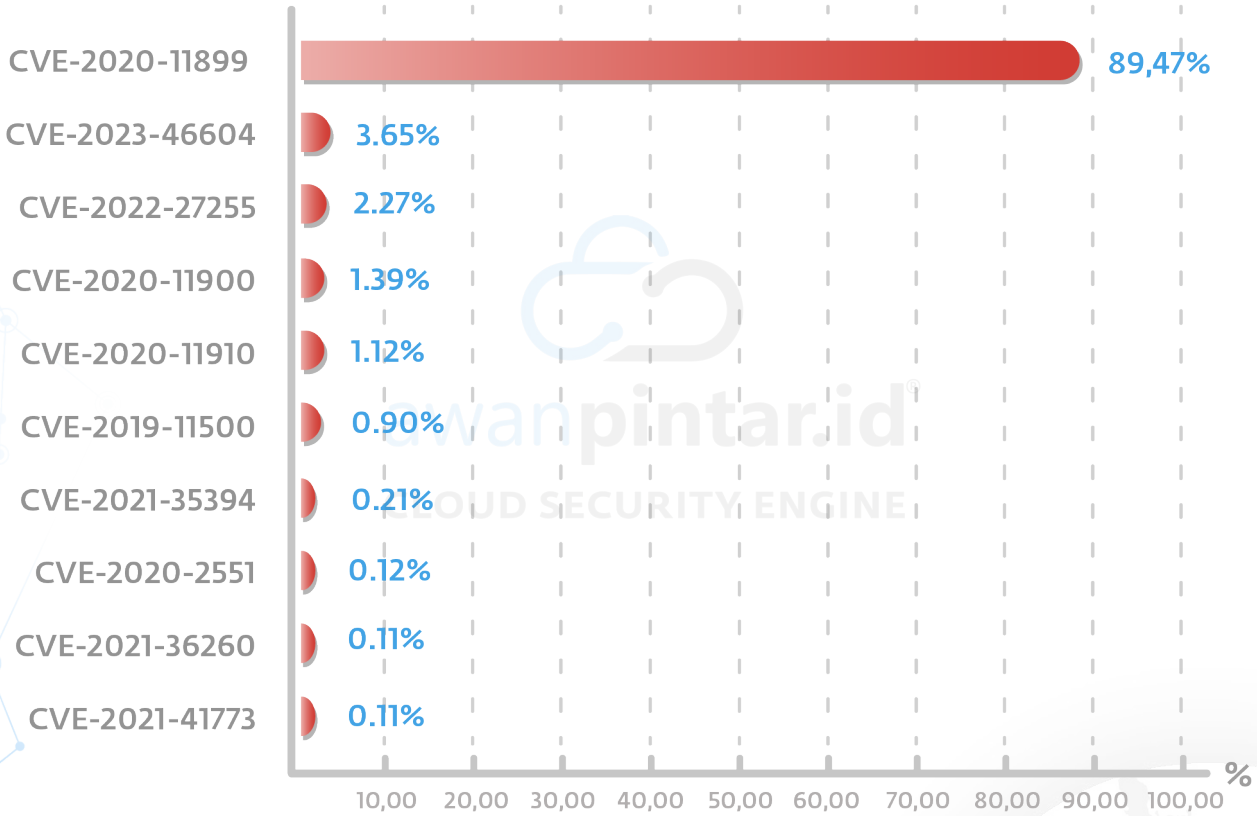
Angka-angka ini bukan sekadar statistik, mereka memaparkan riwayat tentang semakin banyaknya titik lemah yang ditemukan dan dimanfaatkan, serta tantangan yang harus kita hadapi untuk melindungi data dan sistem kita di masa depan. Berikut data-data yang dihimpun dari AwanPintar.id®.

Tahun Rilis	Bulan					
	Jan	Feb	Mar	Apr	Mei	Jun
CVE-2012	-	-	8	-	-	-
CVE-2013	31	3	79	5	87	20
CVE-2014	8	3	144	6	-	2
CVE-2015	-	-	-	-	2	-
CVE-2016	-	3	1	6	-	-
CVE-2017	121	-	24	8	29	30
CVE-2018	1	1	68	18	26	89
CVE-2019	1.058	800	1.186	1.480	944	799
CVE-2020	97.207	30.462	45.682	65.427	77.854	81.370
CVE-2021	390	544	5.359	1.082	450	596
CVE-2022	106	58	158	81	42	2.043
CVE-2023	3	2	1	1	205	3.369

10 KERENTANAN TERTINGGI

Di paruh pertama tahun 2025, AwanPintar.id® lanskap keamanan siber terus diuji oleh gelombang eksploitasi kerentanan yang dikenal sebagai Common Vulnerabilities and Exposures (CVE). CVE adalah daftar publik berisi celah keamanan yang teridentifikasi dalam software dan hardware, dan menjadi target utama para penyerang siber untuk mendapatkan akses tidak sah, menyebarkan malware, atau melancarkan serangan yang lebih merusak.

Memahami tren eksploitasi CVE selama semester ini dapat memberikan wawasan lebih mendalam tentang kerentanan umum yang sering dieksploitasi di Indonesia, dan mendapat gambaran jelas tentang metode yang paling sering digunakan penjahat siber dan area mana saja yang paling rentan terhadap serangan di berbagai sektor digital.



CVE-2020-11899

CVSS Score: 5.4 Medium

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

Dampak

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

Produk Terdampak

TCP/IP versions before (<) 6.0.1.66

Mitigasi Kerentanan

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

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

CVE-2023-46604

CVSS Score: 9.8 Critica

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

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

Dampak

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

Produk Terdampak

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

Kerentanan ini telah dieksploitasi, sehingga sistem harus segera ditambal. Eksploitasi CVE-2023-46604 yang berhasil dapat mengakibatkan berbagai tindakan, seperti:

- Mencuri data sensitif
- Menginstal malware
- Mengganggu operasional server
- Meluncurkan serangan lebih lanjut terhadap sistem lain yang terhubung dengan broker

Mitigasi Kerentanan

Mitigasi yang paling pasti adalah meningkatkan ke versi ActiveMQ yang di-patch. Versi berikut mengatasi kerentanan:

- 15.5.16
- 5.16.7
- 5.17.6
- 5.18.3

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

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

CVE-2022-27255

CVSS Score: 8.5 (High)

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

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

Dampak

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

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

Produk yang Terdampak

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

Mitigasi Kerentanan

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

Secara khusus, perusahaan harus:

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

CVE-2020-11900

CVSS Score: 8.2 High

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

Dampak

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

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

Produk Software yang Terdampak:

TCP/IP, vendor Treck

Mitigasi Kerentanan

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

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

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

Beberapa langkah yang disarankan:

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

Memutakhirkan ke versi 6.0.1.41 menghilangkan kerentanan ini.

CVE-2020-11910

CVSS Score: 5.3 Medium

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

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

Dampak

Kerentanan memungkinkan penyerang jarak jauh untuk mendapatkan akses ke informasi sensitif atau mengambil kendali atas perangkat di dalam jaringan.

Jika telah berhasil menyusup ke jaringan dapat menggunakan kerentanan library untuk menargetkan perangkat tertentu di dalamnya.

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

Produk Terdampak

Ripple20 menjangkau perangkat IoT kritis dari berbagai bidang, yang melibatkan berbagai kelompok vendor. Vendor yang terkena dampak berkisar dari toko butik satu orang hingga perusahaan multinasional Fortune 500, termasuk HP, Schneider Electric, Intel, Rockwell Automation, Caterpillar, Baxter, serta banyak vendor internasional besar

lainnya yang diduga rentan dalam kontrol medis, transportasi, industri, perusahaan, energi (migas), telekomunikasi, ritel dan perdagangan, dan industri lainnya.

Mitigasi Kerentanan
Semua organisasi harus melakukan penilaian risiko yang komprehensif sebelum menerapkan tindakan defensif.

Sebagai langlah awal dapat melakukan 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-2019-11500

CVSS Score: 9.8 Critical

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

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

Dampak

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

Produk yang Terdampak

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

Mitigasi Kerentanan

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

Green
OPEN

CVE-2021-35394

CVSS: 9.8 Critical

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

Dampak

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

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

Produk Terdampak

Realtek_jungle_sdk, vendor Realtek, start version 2.0, end version 3.4.14b.

Mitigasi Kerentanan

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

CVE-2020-2551

CVSS Score 9.8 (Critical)

CVE-2020-2551 Kerentanan dalam produk Oracle WebLogic Server dari Oracle Fusion Middleware (komponen: Komponen Inti WLS). Yang merupakan kerentanan eksekusi kode jarak jauh kritis (RCE) yang mempengaruhi Server Windows yang dikonfigurasi untuk menjalankan peran server DNS

Serangan yang berhasil dari kerentanan ini dapat mengakibatkan pengambilalihan Oracle WebLogic Server.

Dampak

Kerentanan yang mudah dieksploitasi memungkinkan penyerang yang tidak diautentikasi dengan akses jaringan melalui IIOP untuk mengkompromikan Oracle WebLogic Server.

Serangan ini sangat tertarget karena hanya tertuju pada server Windows. Berhasilnya serangan ini menguasai sistem pada perusahaan yang menjadi incaran.

Produk Terdampak

Versi didukung yang terpengaruh adalah:
10.3.6.0.0,
12.1.3.0.0,
12.2.1.3.0
12.2.1.4.0.

Mitigasi Kerentanan

- Oracle telah merilis tambalan resmi untuk memperbaiki kerentanan ini. Silakan merujuk ke https://www.Oracle.com/security-alerts/cpujan 2020.html
- Eksploitasi kerentanan dapat dikurangi untuk sementara dengan menutup IIOP. Untuk menutup IIOP, lakukan hal berikut:
  1. Di konsol WebLogic, pilih“ Layanan“ > “AdminServer” > “Protokol“ dan hapus centang “ Aktifkan IIOP”.
  2. Restart proyek WebLogic untuk menerapkan konfigurasi.

CVE-2021-36260

CVSS Score: 9.8 (Critical)

CVE-2021-36260 adalah kerentanan command injection pada sistem manajemen kamera Hikvision (Hikvision IP Camera/ NVR/DVR). Kerentanan ini memungkinkan penyerang yang tidak diautentikasi (tanpa perlu login) untuk mengirim command injection ke perangkat melalui web server yang terekspos.

Serangan yang berhasil dari kerentanan ini dapat mengakibatkan eksekusi kode arbitrer jarak jauh (RCE) pada perangkat yang

rentan. Artinya, penyerang bisa mengambil alih kendali penuh atas perangkat kamera atau NVR/DVR Hikvision tersebut.

Dampak

Kerentanan ini sangat mudah dieksploitasi dan tidak memerlukan autentikasi. Penyerang dengan akses jaringan ke perangkat Hikvision yang rentan dapat menyuntikkan perintah (commands) ke sistem operasi dasar perangkat.

Jika berhasil, serangan ini dapat menyebabkan:

- Pengambilalihan penuh perangkat: Penyerang dapat mengontrol kamera, melihat rekaman, memanipulasi pengaturan, atau bahkan menghapus data.
- Akses ke jaringan internal: Perangkat yang terkompromi bisa menjadi pivot point bagi penyerang untuk masuk lebih dalam ke jaringan internal perusahaan atau rumah.
- Penyebaran malware: Penyerang dapat menginstal malware atau backdoor pada perangkat untuk tujuan jangka panjang.
- DDoS botnet participation: Perangkat yang terinfeksi dapat dijadikan bagian dari botnet untuk meluncurkan serangan DDoS skala besar.

Produk Terdampak

Kerentanan ini memengaruhi berbagai produk kamera IP dan Network Video Recorder (NVR) dari Hikvision. Versi firmware yang terdampak luas meliputi:

- Produk Kamera IP: Seri DS-2CD (misalnya DS-2CD2T86G2-4I/SL, DS-2CD2347G2-LU), Seri DS-2CD (khususnya yang terpengaruh), dan seri lainnya.
- Produk NVR/DVR: Seri DS-76xxNI-I2/P, DS-77xxNI-I4/P, DS-96xxNI-I8, dan seri lainnya.

Secara umum, perangkat dengan firmware versi sebelum 2021-09-08 dan versi firmware V5.5.0 hingga V6.7.1 yang tidak spesifik memiliki potensi kerentanan ini. Untuk daftar lengkap model dan firmware yang terpengaruh, disarankan untuk merujuk langsung ke advisory resmi Hikvision.

Mitigasi Kerentanan

Hikvision telah merilis patch firmware resmi untuk memperbaiki kerentanan ini. Langkah-langkah mitigasi yang direkomendasikan adalah:

- Segera Perbarui Firmware: Perbarui firmware perangkat Hikvision Anda ke versi terbaru yang disediakan oleh Hikvision. Pastikan Anda mengunduh firmware hanya dari situs web resmi Hikvision.
- Isolasi Jaringan: Jika pembaruan segera tidak memungkinkan, isolasi perangkat Hikvision Anda ke segmen jaringan terpisah dan batasi akses hanya untuk pengguna yang berwenang dan IP address yang terpercaya.
- Blokir Akses Eksternal: Jika tidak ada kebutuhan akses remote ke antarmuka web perangkat, blokir akses ke port HTTP/HTTPS perangkat (biasanya port 80/443 atau port manajemen lainnya) dari internet publik menggunakan firewall.
- Ubah Kredensial Default: Meskipun kerentanan ini tidak memerlukan autentikasi, selalu merupakan praktik terbaik untuk mengubah kata sandi default dan menggunakan kata sandi yang kuat untuk semua perangkat.
- Audit Log: Pantau log perangkat untuk aktivitas mencurigakan atau upaya akses yang tidak sah.

Untuk informasi lebih lanjut dan daftar patch spesifik, silakan merujuk ke security advisory resmi dari Hikvision atau database CVE terpercaya.

Green
OPEN

CVE-2021-41773

CVSS Score: 7.5 High

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

Dampak

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

Produk yang Terkena Dampak

- Oracle Instantis Enterprisetrack
- Sistem Operasi Fedora
- Apache Software Foundation Apache HTTP Server

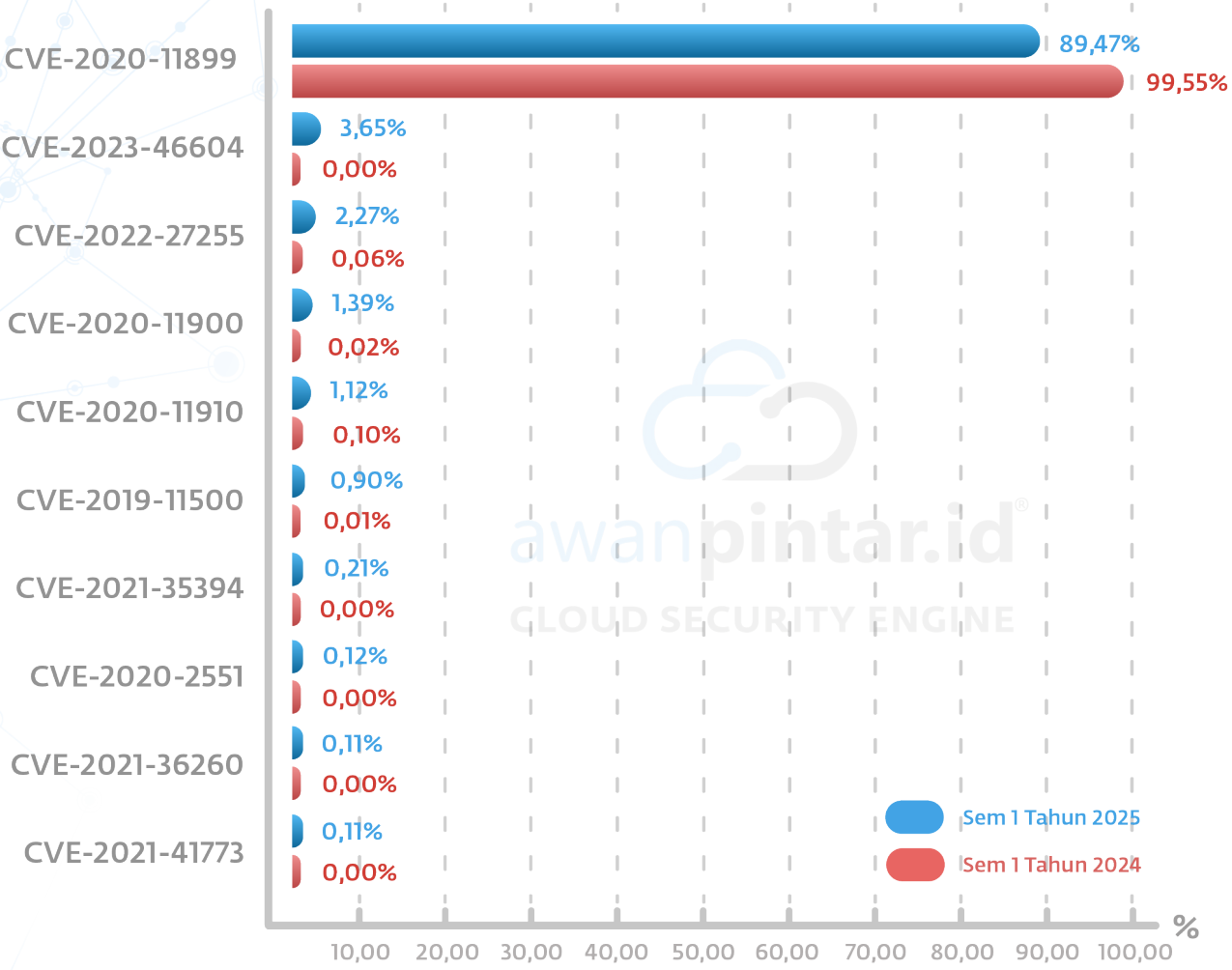
Mitigasi Kerentanan

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

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

Green
OPEN

Komparasi Eksploitasi CVE Semester 1 Tahun 2025 & Semester 1 Tahun 2024



CVE-2020-11899
Mengalami Penurunan -10,08%

CVE-2023-46604
Eksploitasi Baru 3,65%

CVE-2022-27255
Mengalami Peningkatan 2,21%

CVE-2020-11900
Mengalami Peningkatan 1,37%

CVE-2020-11910
Mengalami Peningkatan 1,02%

CVE-2019-11500
Mengalami Peningkatan 0,89%

CVE-2021-35394
Mengalami Peningkatan 0,21%

CVE-2020-2551
Eksploitasi Baru 0,12%

CVE-2021-36260
Eksploitasi Baru 0,11%

CVE-2021-41773
Eksploitasi Baru 0,11%

Green
OPEN

Data ini menyajikan gambaran tentang kerentanan Common Vulnerabilities and Exposures (CVE) yang paling sering dieksploitasi dalam Semester 1 (S1) 2024 dan S1 2025, berdasarkan deteksi AwanPintar.id®. Analisis ini mengungkapkan pergeseran signifikan dalam fokus dan preferensi penyerang terhadap jenis-jenis kerentanan.

1. Dominasi Bergeser namun Tetap Kuat: CVE-2020-11899

- S1 2025: 88,47%
- S1 2024: 99,55%
- Perubahan: Penurunan -10,08%

Meskipun mengalami penurunan, CVE-2020-11899 tetap menjadi kerentanan yang paling dominan dieksploitasi, menyumbang hampir 90% dari seluruh deteksi. Ini adalah kerentanan Remote Code Execution (RCE) pada produk Micro Focus Operation Bridge Reporter (OBR).

Implikasi

Penurunan persentase ini mungkin menunjukkan beberapa hal:

- Peningkatan Patching: Organisasi mungkin telah lebih aktif dalam menambal kerentanan ini.
- Diversifikasi Serangan: Penyerang mulai mencari dan mengeksploitasi kerentanan lain, meskipun CVE-2020-11899 masih sangat efektif.
- Target yang Semakin Sedikit: Jumlah sistem yang rentan terhadap CVE ini mungkin semakin berkurang seiring waktu.

2. Peningkatan Signifikan pada Beberapa CVE

Beberapa CVE menunjukkan peningkatan persentase yang sangat substansial, meskipun dari basis yang relatif rendah di tahun 2024:

CVE-2022-27255:

- S1 2025: 2,27%
- S1 2024: 0,06%
- Perubahan: Peningkatan 2,21% (Catatan: CVE-2022-27255 adalah kerentanan RCE pada SoftEther VPN)

CVE-2020-11900:

- S1 2025: 1,39%
- S1 2024: 0,02%
- Perubahan: Peningkatan 1,37% (Catatan: CVE-2020-11900 juga terkait dengan Micro Focus OBR, menunjukkan bahwa penyerang mungkin mendiversifikasi serangan mereka di antara kerentanan dalam produk yang sama atau menggunakan exploit chain yang melibatkan CVE ini)

CVE-2020-11910:

- S1 2025: 1,12%
- S1 2024: 0,10%
- Perubahan: Peningkatan 1,02%

CVE-2019-11500:

- S1 2025: 0,90%
- S1 2024: 0,01%
- Perubahan: Peningkatan 0,89% (Catatan: CVE-2019-11500 adalah kerentanan Pre-Auth Arbitrary File Read pada Pulse Secure VPN. Peningkatan eksploitasinya mengindikasikan bahwa penyerang masih secara aktif menargetkan perangkat VPN yang belum ditambal untuk mendapatkan akses awal ke jaringan)

CVE-2021-35394:

- S1 2025: 0,21%
- S1 2024: 0,00%
- Perubahan: Peningkatan 0,21%

Implikasi:
Peningkatan ini, terutama untuk

kerentanan pada VPN (CVE-2022-27255, CVE-2019-11500) dan produk bisnis (Micro Focus OBR), menegaskan bahwa penyerang terus mencari dan memanfaatkan celah untuk mendapatkan akses awal atau eksekusi kode pada perangkat yang terekspos ke internet.

3. Kemunculan Eksploitasi Baru (Tanda Ancaman Aktif)

Beberapa CVE baru muncul dalam daftar teratas di S1 2025, yang tidak terdeteksi pada S1 2024, mengindikasikan adopsi cepat exploit oleh penyerang:

CVE-2023-46604:

- S1 2025: 3,65%
- S1 2024: -
- Eksploitasi Baru (Catatan: CVE-2023-46604 adalah kerentanan RCE pada Apache ActiveMQ.)

CVE-2020-2551:

- S1 2025: 0,12%
- S1 2024: 0,00%
- Eksploitasi Baru (Catatan: CVE-2020-2551 adalah kerentanan RCE kritis pada Oracle WebLogic Server.)

CVE-2021-36260:

- S1 2025: 0,11%
- S1 2024: -
- Eksploitasi Baru (Catatan: CVE-2021-36260 adalah kerentanan command injection pada kamera Hikvision IP/NVR/DVR.)

CVE-2021-41773:

- S1 2025: 0,11%
- S1 2024: -
- Eksploitasi Baru (Catatan: CVE-2021-41773 adalah kerentanan path traversal pada Apache HTTP Server.)

Implikasi: Kemunculan CVE-CVE ini sangat penting:

- Adopsi Cepat Exploit: Ini menunjukkan bahwa penyerang dengan cepat mengadopsi CVE-CVE terbaru begitu mereka dipublikasikan atau diumumkan proof-of-concept-nya, seperti CVE-2023-46604 yang baru dirilis akhir 2023.
- Fokus pada Sistem Kritis: CVE-2020-2551 pada Oracle WebLogic Server dan CVE-2021-41773 pada Apache HTTP Server menunjukkan fokus penyerang pada eksploitasi web server dan middleware yang umum digunakan dan vital.
- Ancaman IoT/Perangkat Jaringan: Kemunculan CVE-2021-36260 pada Hikvision menyoroti kerentanan pada perangkat IoT/kamera keamanan yang sering terekspos ke internet.

Implikasi dari Tren Eksploitasi CVE

Prioritas Patching Bergeser dan Berkelanjutan: Meskipun dominasi CVE-2020-11899 sedikit menurun, kemunculan kerentanan yang lebih baru dan berbahaya seperti CVE-2023-46604 dan eksploitasi berkelanjutan dari CVE-2019-11500 (VPN) menunjukkan bahwa siklus penambalan harus cepat dan komprehensif. Kerentanan lama yang belum ditambal tetap menjadi pintu masuk, sementara yang baru segera dieksploitasi.

Fokus pada Akses Awal dan RCE: Mayoritas CVE yang dieksploitasi adalah Remote Code Execution (RCE) atau kerentanan yang memungkinkan akses awal ke sistem (seperti VPN dan web server). Ini menunjukkan tujuan utama penyerang adalah mendapatkan pijakan awal dan kendali penuh atas sistem target.

Ancaman Terus Berevolusi (dan Berulang): Penyerang dengan cepat mengadopsi exploit untuk CVE terbaru, namun pada saat yang sama, mereka juga terus memanfaatkan kerentanan lama yang belum ditambal secara luas. Ini menciptakan tantangan ganda bagi tim keamanan.

Pentingnya Manajemen Kerentanan Proaktif: Data ini menggarisbawahi kebutuhan kritis akan program manajemen kerentanan yang kuat, termasuk:

- Pemindaian kerentanan reguler.
- Prioritas patching berdasarkan tingkat keparahan CVE dan eksposur sistem.
- Pemantauan deteksi eksploitasi oleh IDS/IPS secara real-time.
- Fokus pada vendor dan software yang sering menjadi target (misalnya Micro Focus, Apache, solusi VPN, kamera IoT/ CCTV).

Secara keseluruhan, lanskap eksploitasi CVE menunjukkan bahwa penyerang sangat adaptif, terus mencari dan memanfaatkan setiap celah yang ada, baik yang lama maupun yang baru, untuk mendapatkan akses dan kontrol atas sistem. Organisasi harus tetap waspada dan proaktif dalam strategi manajemen kerentanan mereka.

Green
OPEN

SERANGAN DALAM NEGERI

Akumulasi Serangan dalam Negeri

Secara kontinyu AwanPintar.id® terus melanjutkan memberikan reportase khusus mengenai serangan siber yang terjadi dari dalam negeri. Data yang terkumpul mengungkap bahwa pelaku kejahatan siber domestik semakin aktif dan terorganisir, melancarkan serangan dengan berbagai modus operandi.

Mereka juga semakin mahir dalam menggunakan alat dan teknik yang canggih untuk melancarkan serangan yang lebih efektif. Peningkatan kapasitas dan kapabilitas pelaku kejahatan siber domestik ini menjadi tantangan serius bagi upaya penegakan hukum dan keamanan siber di Indonesia.

Tren ini mengindikasikan adanya pergeseran signifikan dalam dinamika ancaman siber, di mana aktor-aktor lokal memainkan peran yang semakin dominan. Serangan-serangan ini tidak hanya menargetkan infrastruktur kritikal dan sektor bisnis, tetapi juga individu-individu yang rentan, menimbulkan dampak yang luas dan merugikan.

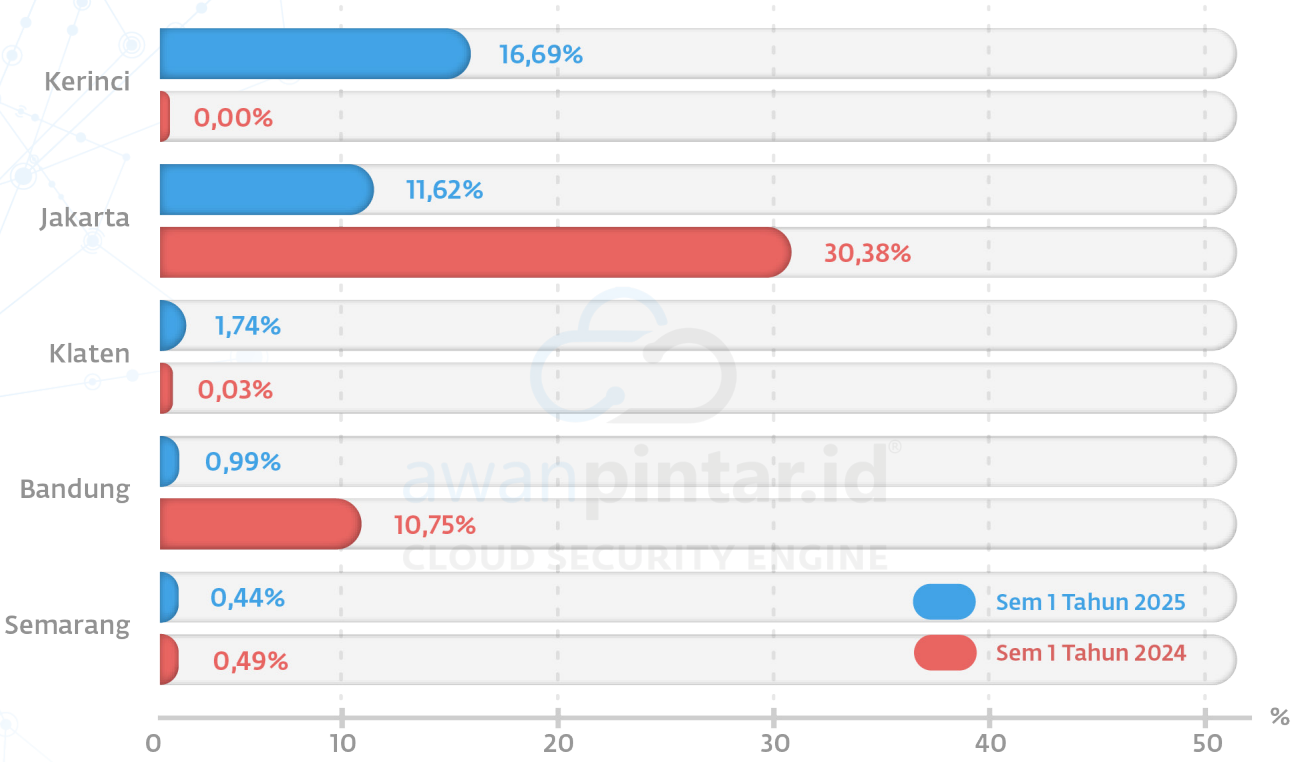
5 Daerah Penyerang Teratas di Indonesia

Data ini mengungkapkan tentang 5 daerah di Indonesia yang menjadi pusat serangan siber ke dalam negeri yang merupakan hasil akumulasi dari AwanPintar.id® pada semester 1 tahun 2025.

Dengan melokalisir daerah-daerah yang secara spartan menyerang secara domestik, dapat memberi gambaran peta ancaman siber dalam negeri seperti apa, berikut 5 daerah yang menjadi penyerang teratas di Indonesia.

Semester 1 Tahun 2025

Komparasi 5 Daerah Penyerang di Indonesia Semester 1 Tahun 2025 & Semester 1 Tahun 2024



Kerinci
Daerah Penyerang Teratas Baru 16,69%

Jakarta
Mengalami Penurunan Serangan -18,76%

Klaten
Daerah Penyerang Teratas Baru -1,71%

Bandung
Mengalami Peningkatan Serangan -9,76%

Semarang
Daerah Penyerang Teratas Baru -0,05%

Data ini menampilkan distribusi geografis sumber serangan siber teratas di Indonesia antara Semester 1 (S1) 2024 dan S1 2025, berdasarkan deteksi AwanPintar.id®.

Perubahan Pola Serangan Domestik

Kemunculan Sumber Utama Baru: Kerinci muncul sebagai daerah penyerang teratas baru di S1 2025 dengan 16,69%. Ini adalah perubahan drastis, mengindikasikan adanya kluster baru atas infrastruktur yang disalahgunakan secara signifikan di wilayah tersebut yang sebelumnya tidak terdeteksi atau aktif.

Perubahan Status: Dengan lonjakan ini, Klaten yang sebelumnya memiliki kontribusi minimal, kini menjadi salah satu daerah yang perlu diwaspadai sebagai sumber serangan siber domestik. Sementara itu, Semarang juga tercatat sebagai "Daerah Penyerang Teratas Baru" meskipun mengalami penurunan kecil -0,05% (dari 0,49% menjadi 0,44%). Hal ini menandakan kontribusi mereka yang relatif kecil namun tetap ada dalam lanskap ancaman domestik.

Penurunan Dominasi Jakarta dan Bandung: Jakarta mengalami penurunan besar -18,76% (dari 30,38% menjadi 11,62%). Demikian pula, Bandung turun dari 10,75% menjadi 0,99% (-9,76%). Meskipun masih menjadi kontributor, porsi serangan dari kedua kota besar ini menurun drastis, menunjukkan kemungkinan peningkatan pertahanan atau penyerang beralih target.

Implikasi

Pola ini menunjukkan diversifikasi sumber serangan siber dari dalam negeri. Ancaman tidak lagi terkonsentrasi di pusat-pusat metropolitan seperti Jakarta dan Bandung. Kemunculan Kerinci sebagai hotspot serangan utama sangat mengkhawatirkan dan menuntut investigasi segera terhadap infrastruktur di wilayah tersebut untuk mengidentifikasi penyebab lonjakan aktivitas ini, yang mungkin berasal dari botnet atau sistem yang terkompromi.

Penurunan persentase dari Jakarta dan Bandung, meskipun positif dari satu sisi, harus dilihat dengan hati-hati. Ini bisa berarti penyerang telah mengubah taktik atau beralih ke lokasi lain untuk melancarkan serangan, seperti yang terlihat dengan munculnya Kerinci.

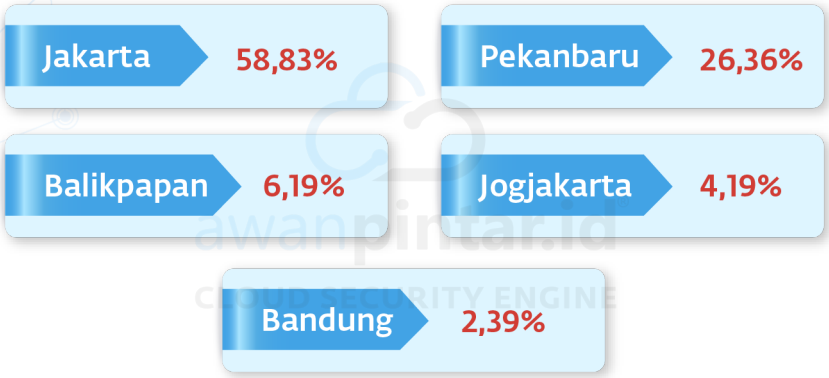
Secara keseluruhan, kapasitas untuk melancarkan serangan siber menyebar ke berbagai daerah di Indonesia, kemungkinan melalui botnet atau sistem yang terkompromi. Organisasi dan ISP perlu memperluas jangkauan pemantauan dan mitigasi mereka ke wilayah-wilayah yang baru teridentifikasi ini untuk mengatasi ancaman domestik secara lebih efektif. Hal ini juga menekankan pentingnya keamanan siber merata di seluruh wilayah, tidak hanya terpusat pada kota-kota besar.

5 Daerah Paling Sering Diserang

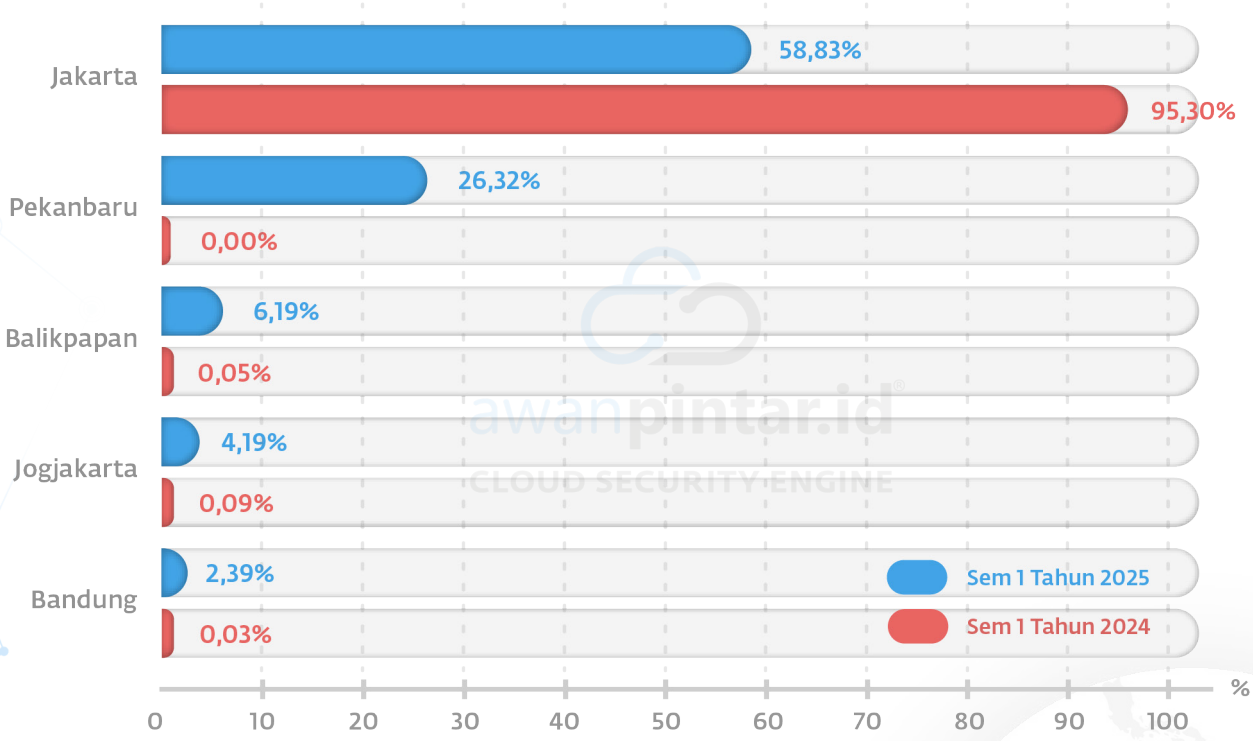
Perang siber antar kota tidak dapat dihindari di Indonesia, progresifnya kemajuan teknologi, penetrasi internet yang tinggi ke berbagai daerah mendorong peningkatan penggunaan teknologi digital di berbagai sektor termasuk di kota-kota di Indonesia. Yang di satu sisi juga membuka kerentanan siber di berbagai wilayah karena tidak meratanya kesadaran keamanan dan pengetahuan siber.

Daerah-daerah yang lemah dalam infrastruktur keamanan digital kemudian menjadi sasaran dalam serangan siber yang berkelanjutan. Berikut data dari AwanPintar.id® yakni daftar 5 daerah yang paling sering mendapat serangan siber dari dalam negeri.

Semester 1 Tahun 2025



Komparasi Daerah Paling Sering Diserang Semester 1 Tahun 2024 & Semester 1 Tahun 2025



Jakarta
Mengalami Penurunan -36,47%

Pekanbaru
Daerah Paling Diserang Baru 26,32%

Balikpapan
Mengalami Peningkatan 6,14%

Jogjakarta
Mengalami Peningkatan 4,10%

Bandung
Daerah Paling Diserang Baru 2,36%

Persentase ini merepresentasikan proporsi dari total serangan yang terdeteksi AwanPintar.id® di seluruh Indonesia yang terjadi di masing-masing kota.

Jakarta: Penurunan Signifikan dalam Persentase Serangan

S1 2025: 58,83%
S1 2024: 95,30%
Perubahan: Mengalami penurunan -36,47%

Meskipun Jakarta masih menjadi target utama serangan siber di Indonesia (dengan persentase tertinggi pada S1 2025), penurunannya sangat drastis. Ini bisa mengindikasikan beberapa hal:

Peningkatan Pertahanan di Jakarta: Organisasi di Jakarta mungkin telah meningkatkan infrastruktur keamanan siber mereka, membuat kota ini menjadi target yang lebih sulit dan kurang "menguntungkan" bagi penyerang.

Pergeseran Fokus Penyerang: Para pelaku ancaman mungkin telah mendiversifikasi target mereka, menyebarkan serangan ke wilayah lain yang mungkin memiliki pertahanan yang lebih lemah atau kurang siap.

Perbaikan Pelaporan/Deteksi di Wilayah Lain: Bisa jadi kemampuan deteksi dan pelaporan AwanPintar.id® di wilayah lain juga telah meningkat, sehingga persentase serangan yang sebelumnya didominasi Jakarta kini lebih tersebar.

Pekanbaru & Bandung: Kemunculan sebagai Target Baru

Pekanbaru:
S1 2025: 26,32%
S1 2024: 0,00%
(Daerah Paling Diserang Baru)

Bandung:
S1 2025: 2,39%
S1 2024: 0,03%
(Daerah Paling Diserang Baru dengan peningkatan +2,36%)

Kemunculan Pekanbaru dan Bandung sebagai target yang signifikan pada S1 2025, padahal tidak tercatat dominan pada S1 2024 (atau persentasenya sangat kecil), merupakan indikator yang sangat penting:

Ekspansi Target Serangan: Pelaku ancaman jelas sedang memperluas jangkauan operasional mereka ke kota-kota lapis kedua atau kota-kota dengan perkembangan ekonomi dan digital yang pesat.

Kerentanan Baru Ditemukan: Penyerang mungkin telah mengidentifikasi kerentanan spesifik di infrastruktur atau organisasi yang berbasis di kota-kota ini.

Kurangnya Kesiapan Keamanan: Kota-kota yang baru menjadi target seringkali memiliki tingkat kesiapan keamanan siber yang lebih rendah dibandingkan pusat ekonomi besar seperti Jakarta, menjadikannya target yang lebih mudah. Pekanbaru khususnya menonjol dengan persentase yang sangat tinggi (26,32%), menjadikannya target kedua terbesar setelah Jakarta.

Balikpapan & Jogjakarta: Peningkatan Serangan yang Perlu Diwaspadai

Balikpapan:
S1 2025: 6,19%
S1 2024: 0,05%
Perubahan: Peningkatan +6,14%

Jogjakarta:
S1 2025: 4,19%
S1 2024: 0,09%
Perubahan: Peningkatan +4,10%

Peningkatan yang signifikan di Balikpapan dan Jogjakarta, meskipun dari basis yang sangat rendah, mengonfirmasi tren diversifikasi target:

Kota Ekonomi Berkembang: Kedua kota ini memiliki pertumbuhan ekonomi dan digital yang pesat, dengan industri kunci (pertambangan/energi di Balikpapan, pariwisata/pendidikan/ekonomi kreatif di Jogjakarta) yang mungkin menjadi target menarik bagi penyerang.

Potensi Kelemahan yang Dieksploitasi: Peningkatan ini menunjukkan bahwa penyerang menemukan lebih banyak peluang atau kerentanan di jaringan yang beroperasi di kedua kota ini.

Secara Umum

Data ini secara jelas menggambarkan pergeseran geografis dalam lanskap ancaman siber di Indonesia antara tahun 2024 dan 2025:

Dominasi Jakarta Menurun, Tetapi Tetap Paling Tinggi: Meskipun Jakarta tetap menjadi target utama, proporsi serangannya menurun drastis, menunjukkan kemungkinan peningkatan pertahanan atau diversifikasi penyerang.

Ekspansi Agresif ke Wilayah Baru: Pekanbaru dan Bandung muncul sebagai target baru yang signifikan, dengan Pekanbaru menunjukkan persentase yang sangat tinggi, menandakan penyerang mencari target yang lebih rentan.

Peningkatan Ancaman di Kota Berkembang: Balikpapan dan Jogjakarta juga mengalami lonjakan, menegaskan bahwa kota-kota dengan pertumbuhan ekonomi juga menjadi magnet bagi pelaku kejahatan siber.

Implikasinya adalah bahwa kesiapan keamanan siber di Indonesia tidak bisa lagi hanya terfokus pada kota-kota besar yang tradisional menjadi target. Organisasi dan pemerintah di kota-kota berkembang dan yang sebelumnya kurang diserang harus meningkatkan kewaspadaan dan investasi dalam keamanan siber untuk menghadapi ancaman yang semakin menyebar dan berkembang ini.

Green
OPEN

Jenis Serangan Paling Dominan

Di ranah digital Indonesia, ancaman siber terus berevolusi dan beradaptasi, menargetkan berbagai sektor dan individu. Untuk memberikan gambaran yang jelas mengenai lanskap ancaman di dalam negeri, AwanPintar.id® telah menganalisis data serangan siber yang terjadi pada semester pertama tahun 2025.

Data tersebut menunjukkan jenis serangan paling dominan yang beredar di Indonesia, memberikan wawasan krusial bagi kita semua. Dengan memahami modus operandi yang paling sering digunakan, kita dapat lebih efektif dalam membangun benteng pertahanan dan melindungi aset digital penting dari berbagai ancaman di dunia maya. Berikut data-datanya:

Upaya Pengambilalihan Hak Akses Administrator (Attempted Administrator Privilege Gain)

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

Semester 1 Tahun 2025: 78,14%
Semester 1 Tahun 2024: 55,03%

Angka-angka menunjukkan peningkatan yang sangat signifikan dalam upaya serangan ini. Peningkatan sebesar 23,11% ini mengindikasikan bahwa para pelaku kejahatan siber semakin memfokuskan serangan mereka untuk mendapatkan kendali penuh atas sistem. Dominasi jenis serangan ini menegaskan bahwa pencurian kredensial dan eskalasi privilese menjadi prioritas utama penyerang di Indonesia, yang berpotensi fatal bagi keamanan perusahaan karena akses administrator memungkinkan manipulasi dan eksploitasi tanpa batas.

Eksploitasi Jaringan (Generic Protocol Command Decode)

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

Semester 1 Tahun 2025: 17,67%
Semester 1 Tahun 2024: 37,68%

Data dari AwanPintar.id® menunjukkan penurunan drastis dalam jenis serangan Eksploitasi Jaringan. Penurunan sebesar -20,01% ini merupakan indikasi positif bahwa upaya pengamanan dan deteksi terhadap manipulasi protokol jaringan mungkin telah meningkat secara efektif, atau penyerang telah mengurangi penggunaan teknik ini, beralih ke metode lain yang mungkin lebih sulit dideteksi. Ini mencerminkan evolusi berkelanjutan dalam pertarungan keamanan siber.

Pemindaian dan Pengintaian Jaringan (Misc Activity)

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

Aktivitas lain-lain dapat mencakup pemindaian port, pengintaian jaringan, atau jenis aktivitas lain yang berpotensi digunakan

sebagai pendahulu serangan yang lebih serius. Meskipun aktivitas lain-lain mungkin tidak langsung mengancam, penting bagi profesional keamanan siber untuk memantau dan menyelidiki jenis peristiwa ini untuk mencegah potensi ancaman berkembang menjadi serangan yang lebih serius.

Semester 1 Tahun 2025: 3,20%
Semester 1 Tahun 2024: 5,33%

Data menunjukkan penurunan signifikan pada "Misc Activity" dari 5,33% pada Semester 1 Tahun 2024 menjadi 3,20% pada Semester 1 Tahun 2025. Ini merupakan penurunan sebesar -2,13% poin persentase.

Meskipun terlihat positif, penurunan ini tidak berarti ancaman berkurang. Sebaliknya, hal ini bisa menjadi indikator bahwa penyerang menjadi lebih stealthy (tersembunyi) atau mengubah attack chain mereka, sehingga aktivitas pengintaian yang mereka lakukan tidak lagi masuk dalam kategori "Misc Activity" yang terdeteksi.

Upaya Penyusupan Sistem (Potentially Bad Traffic)

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

Semester 1 Tahun 2025: 0,23%
Semester 1 Tahun 2024: 1,30%

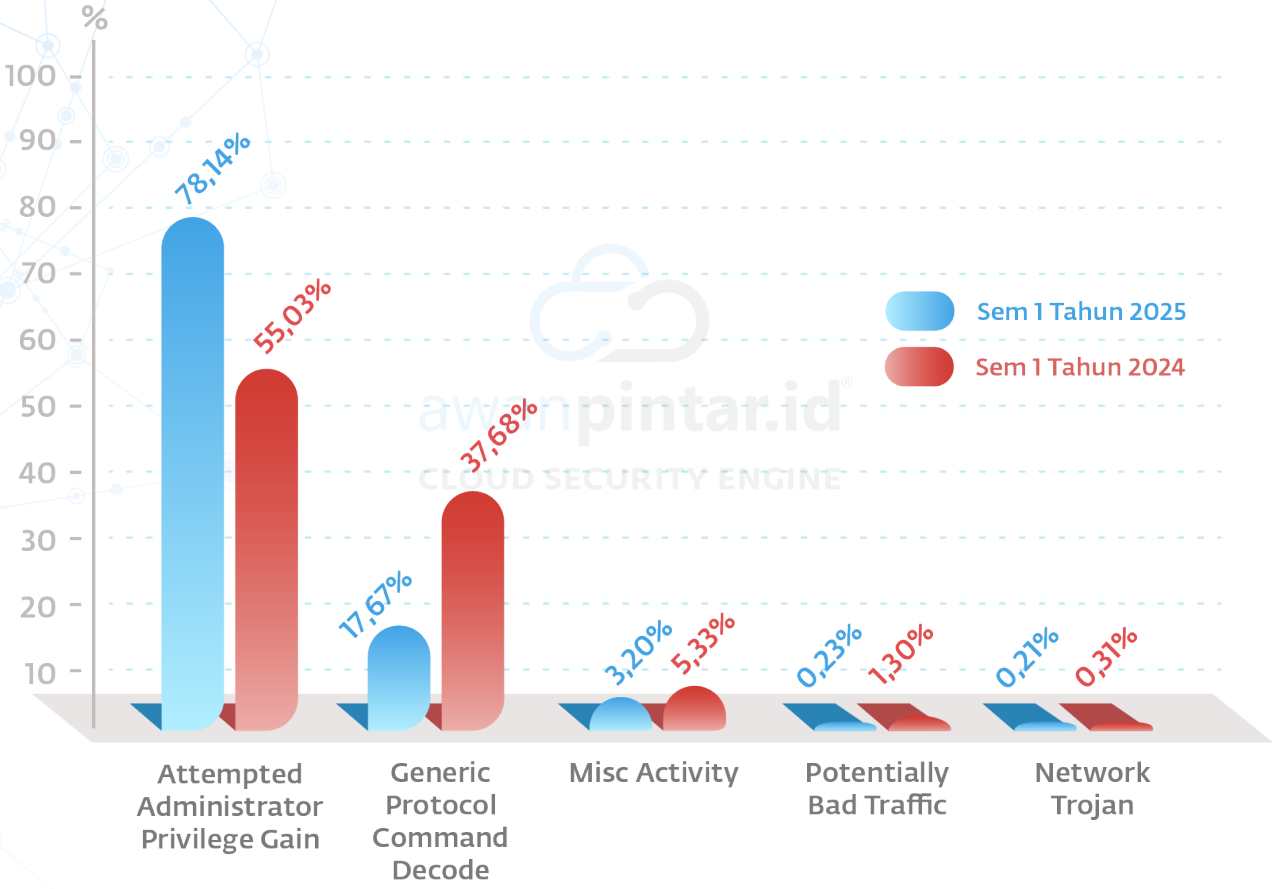
Penurunan sebesar 1,07% ini merupakan indikator positif dalam lanskap keamanan siber. Hal ini mungkin mencerminkan peningkatan efektivitas sistem pertahanan dalam mengidentifikasi dan memitigasi lalu lintas yang berpotensi membahayakan, atau adanya perubahan metode dari penyerang yang kini menggunakan teknik yang lebih sulit dideteksi dalam upaya penyusupan. Meskipun demikian, kewaspadaan tetap harus tinggi mengingat dampak serius dari jenis serangan ini.

Serangan Trojan (Network Trojan)

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

Semester 1 Tahun 2025: 0,21%
Semester 1 Tahun 2024: 0,31%

Data dari AwanPintar.id® menunjukkan adanya penurunan dalam deteksi Serangan Trojan (Network Trojan). Penurunan sebesar 0,10% tersebut, meskipun kecil, bisa mengindikasikan peningkatan efektivitas pertahanan terhadap Trojan, atau pergeseran fokus penyerang ke jenis malware lain. Meskipun demikian, ancaman Trojan tetap relevan dan memerlukan kewaspadaan berkelanjutan mengingat dampaknya yang berpotensi merusak.

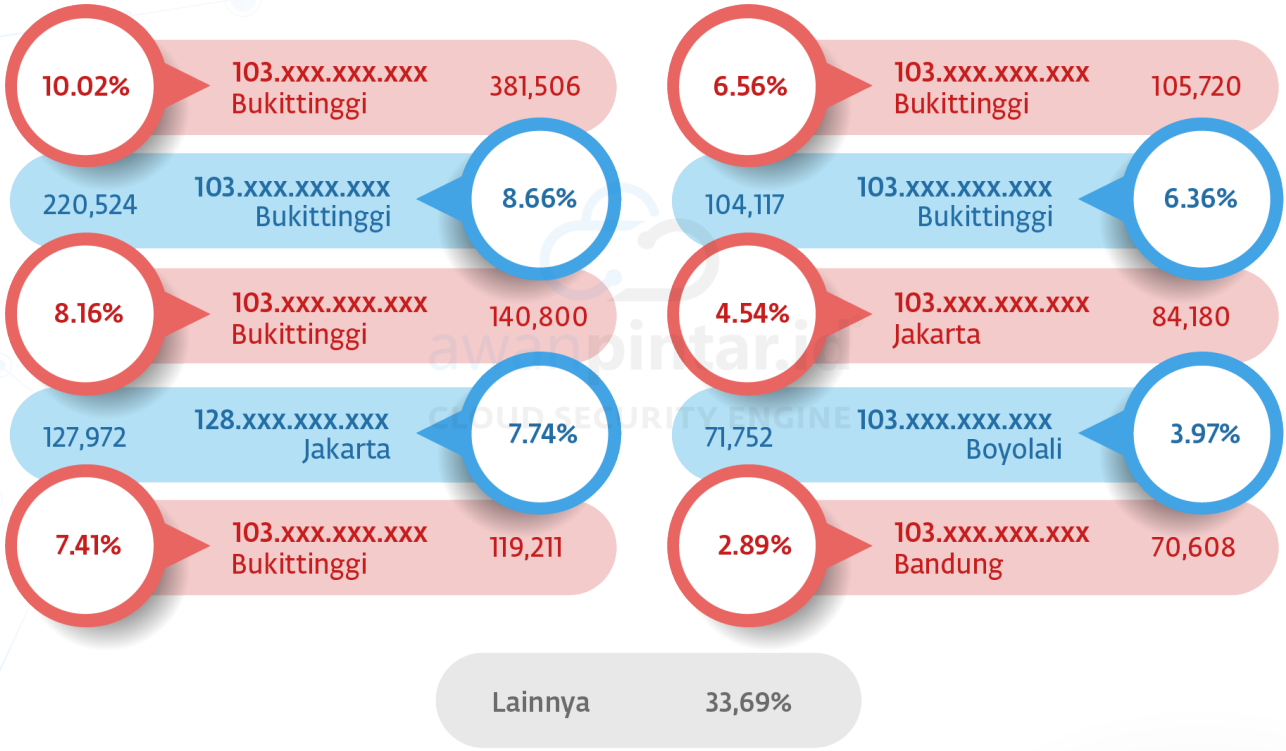

%
100
90
80
70
60
50
40
30
20
10
78,14%
55,03%
17,67%
37,68%
3,20%
5,33%
0,23%
1,30%
0,21%
0,31%
Sem 1 Tahun 2025
Sem 1 Tahun 2024
Attempted Administrator Privilege Gain
Generic Protocol Command Decode
Misc Activity
Potentially Bad Traffic
Network Trojan

Green
OPEN

IP Penyerang dari Dalam Negeri

Memahami dari mana sebuah serangan siber berasal adalah langkah awal dalam membangun pertahanan yang efektif. Dalam konteks keamanan siber di Indonesia, data mengenai alamat IP penyerang yang berasal dari dalam negeri menjadi sangat penting.

AwanPintar.id® telah melakukan analisis mendalam terhadap data ini selama semester pertama tahun 2025, memberikan gambaran jelas tentang titik-titik asal serangan yang terjadi di dalam batas negara kita sendiri. Wawasan ini membantu kita tidak hanya dalam mengidentifikasi sumber ancaman, tetapi juga dalam merancang strategi mitigasi yang lebih terfokus untuk melindungi ruang siber nasional.



Data yang dihimpun AwanPintar.id® untuk Semester 1 tahun 2025 memberikan gambaran tentang asal-usul serangan siber yang berasal dari dalam negeri Indonesia.

Temuan Kunci

Berdasarkan data di atas, beberapa temuan kunci dapat diidentifikasi:

Dominasi Asal Serangan dari Bukittinggi: Tujuh dari sepuluh IP penyerang teratas berasal dari Bukittinggi, Sumatera Barat. IP ini menyumbang total persentase serangan yang sangat signifikan: 47.17% dari total 10 IP teratas. Ini menunjukkan adanya konsentrasi aktivitas penyerangan yang tinggi dari wilayah tersebut.

Blok IP yang Berdekatan: Beberapa serangan menunjukkan berada dalam satu blok atau rentang IP yang berdekatan. Ini bisa mengindikasikan bahwa serangan berasal dari satu penyedia layanan internet (ISP) atau bahkan satu jaringan botnet yang terkonsentrasi di area tersebut.

Jakarta Sebagai Pusat Kedua: Jakarta menyumbang dua IP dalam daftar, dengan total 12.28% dari persentase serangan 10 IP teratas. Mengingat Jakarta adalah kota metropolitan besar dengan banyak koneksi internet, kemunculannya wajar, meskipun tidak sedominan Bukittinggi dalam data ini.

Variasi Lokasi Lain: Boyolali dan Bandung menunjukkan bahwa aktivitas penyerangan tersebar di beberapa wilayah lain di Indonesia, meskipun dengan kontribusi yang lebih kecil dibandingkan Bukittinggi dan Jakarta.

Sifat Serangan: Data ini hanya menunjukkan IP penyerang dan persentase, tanpa detail mengenai jenis serangan yang dilakukan (misalnya, DDoS, brute force, scanning, dll.).

Implikasi

Temuan-temuan kunci di atas memiliki beberapa implikasi penting:

- Peningkatan Pemantauan di Bukittinggi: ISP dan organisasi keamanan siber perlu meningkatkan pemantauan dan analisis terhadap lalu lintas jaringan yang berasal dari wilayah Bukittinggi, terutama dari IP yang teridentifikasi. Ini bisa menjadi hotspot aktivitas siber berbahaya.
- Investigasi Potensi Botnet/Jaringan Kompromi: Konsentrasi IP yang berdekatan di Bukittinggi sangat mungkin menunjukkan adanya jaringan botnet atau sejumlah besar perangkat yang telah terkompromi (misalnya, perangkat IoT, komputer pribadi, atau server yang rentan) dan kini digunakan untuk meluncurkan serangan. Diperlukan investigasi lebih lanjut untuk mengidentifikasi akar masalahnya.
- Kolaborasi dengan ISP: AwanPintar.id® dan lembaga terkait perlu berkolaborasi dengan ISP yang mengelola blok IP tersebut (terutama di Bukittinggi) untuk menyelidiki aktivitas mencurigakan, mengidentifikasi sumber kompromi, dan mengambil tindakan mitigasi seperti pembersihan malware atau pembatasan lalu lintas berbahaya.
- Peningkatan Kesadaran Keamanan: Tingginya jumlah serangan dari berbagai kota di Indonesia mengindikasikan perlunya peningkatan kesadaran keamanan siber di kalangan pengguna internet dan organisasi di seluruh negeri. Banyak serangan mungkin berasal dari perangkat yang tidak terlindungi atau kurang di-patch.
- Pentingnya Geoblokir Selektif: Bagi organisasi yang mengalami serangan dari IP-IP ini, pertimbangan geoblokir selektif atau pemblokiran rentang IP tertentu dapat menjadi langkah mitigasi sementara, namun harus dilakukan dengan hati-hati agar tidak memblokir pengguna yang sah.

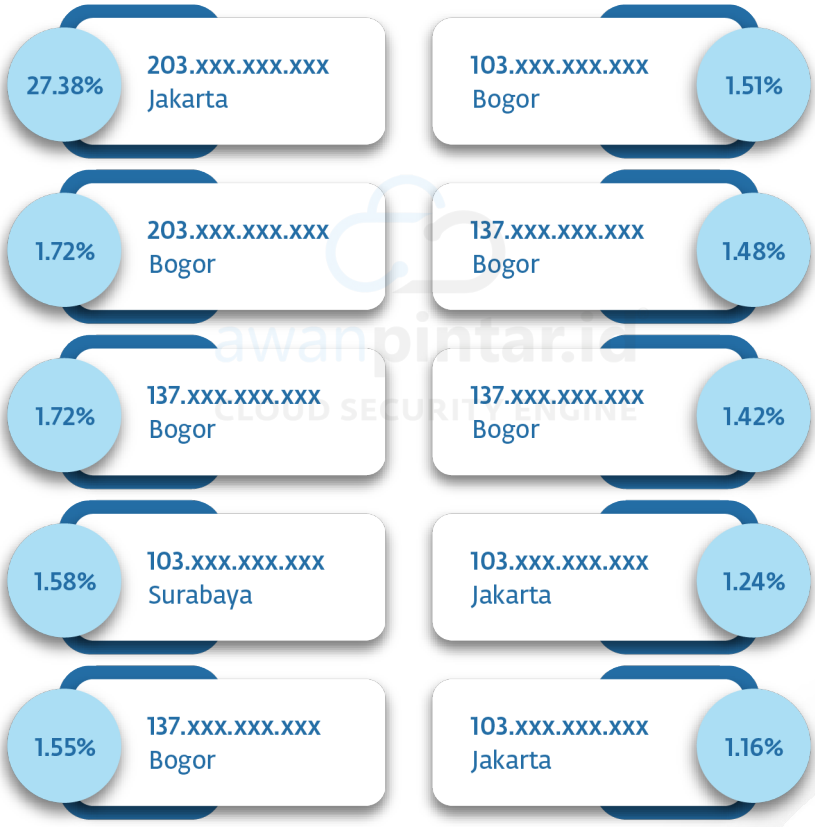
Green
OPEN

IP Spam dan Malware di Indonesia

Di tengah perkembangan pesat dunia digital Indonesia, tantangan keamanan siber semakin kompleks. Untuk memberikan gambaran mendalam tentang ancaman yang paling sering kita hadapi, AwanPintar.id® telah menganalisis data alamat IP pengirim spam dan malware yang beroperasi di Indonesia selama semester pertama tahun 2025.

Hasil analisis ini mengungkap pola dan sumber-sumber utama di balik gelombang spam dan serangan malware yang menyasar pengguna di tanah air. Pemahaman mengenai jejak IP ini sangat krusial bagi individu, bisnis, maupun pemerintah dalam memperkuat strategi pertahanan siber nasional.

IP Spam di Indonesia



Data dari AwanPintar.id® ini menampilkan 10 IP Spam teratas yang terdeteksi menjadi ancaman spam yang menargetkan Indonesia pada Semester 1 Tahun 2025

Temuan Kunci:

Jakarta Mendominasi menyumbang persentase terbesar secara signifikan, yaitu 27.38% dari total serangan. Ini mengindikasikan adanya satu sumber tunggal yang sangat aktif di Jakarta.

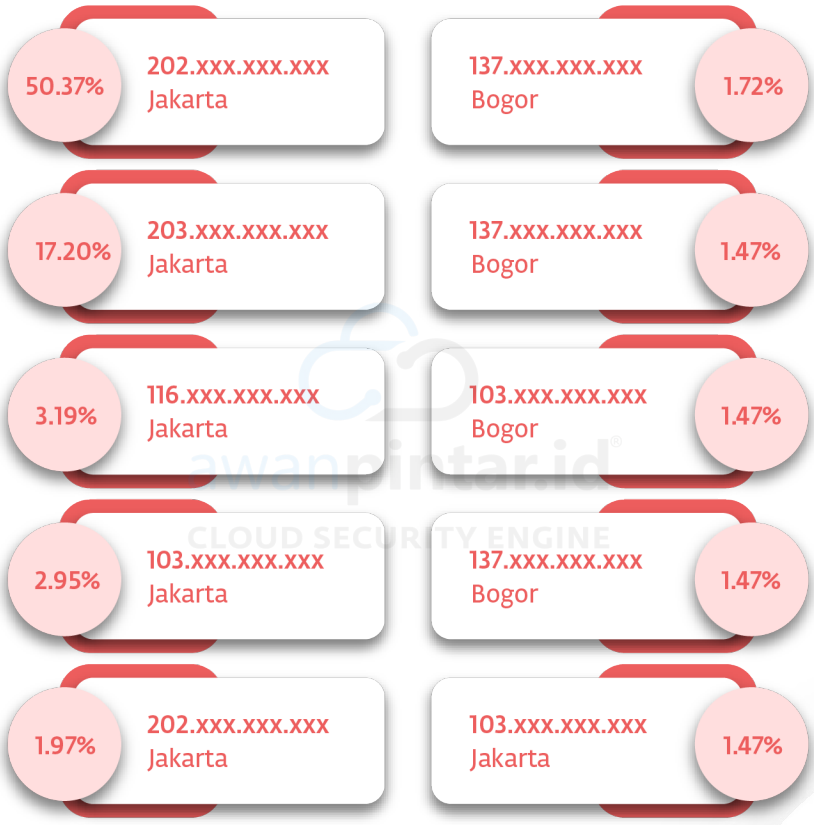
Konsentrasi di Bogor: Lima IP teratas berikutnya (peringkat 2, 3, 5, 6, 7, 8) berasal dari Bogor, dengan total kontribusi sekitar 9.46%. Hal ini menunjukkan adanya kluster aktivitas penyerangan yang signifikan di Bogor.

Surabaya sebagai Kontributor Lain: Surabaya menyumbang 1.58%.

Implikasi:

Data ini menyoroti bahwa serangan siber cenderung terkonsentrasi pada beberapa IP dan lokasi geografis tertentu. Dominasi satu IP di Jakarta menunjukkan potensi adanya server yang disalahgunakan atau sistem yang sangat terinfeksi yang bertanggung jawab atas sebagian besar aktivitas.

IP Malware di Indonesia



Data terbaru dari AwanPintar.id® menyoroti lebih mendalam terkait IP malware dari dalam negeri mengungkapkan beberapa fakta yang bisa kita cermati sebagi berikut:

Temuan Kunci:

Jakarta Mendominasi Secara Absolut: 6 dari 10 IP teratas berasal dari Jakarta, menyumbang total 77.75% dari seluruh IP malware terdeteksi dalam daftar ini. Secara spesifik, Jakarta sangat dominan, menyumbang persentase terbesar. Ini menunjukkan Jakarta adalah pusat utama distribusi malware dari dalam negeri.

Bogor sebagai Hotspot Sekunder: 4 IP berasal dari Bogor, secara kolektif menyumbang 6.13% dari total IP malware teratas. Ini menempatkan Bogor sebagai kontributor penting kedua setelah Jakarta.

Konsentrasi Tinggi: Sebagian besar aktivitas malware berasal dari sejumlah kecil IP yang terkonsentrasi di dua kota utama.

Implikasi:

Data ini dengan jelas menunjukkan bahwa Jakarta adalah episentrum utama penyebaran malware dari dalam negeri, dengan satu IP saja yang bertanggung jawab atas separuh lebih dari aktivitas yang terdeteksi.

IP ini kemungkinan besar adalah server yang disusupi, botnet aktif, atau infrastruktur lain yang disalahgunakan untuk hosting dan mendistribusikan malware. Fokus mitigasi harus diarahkan pada identifikasi, pembersihan, dan pemblokiran IP serta jaringan terkait di Jakarta dan Bogor.

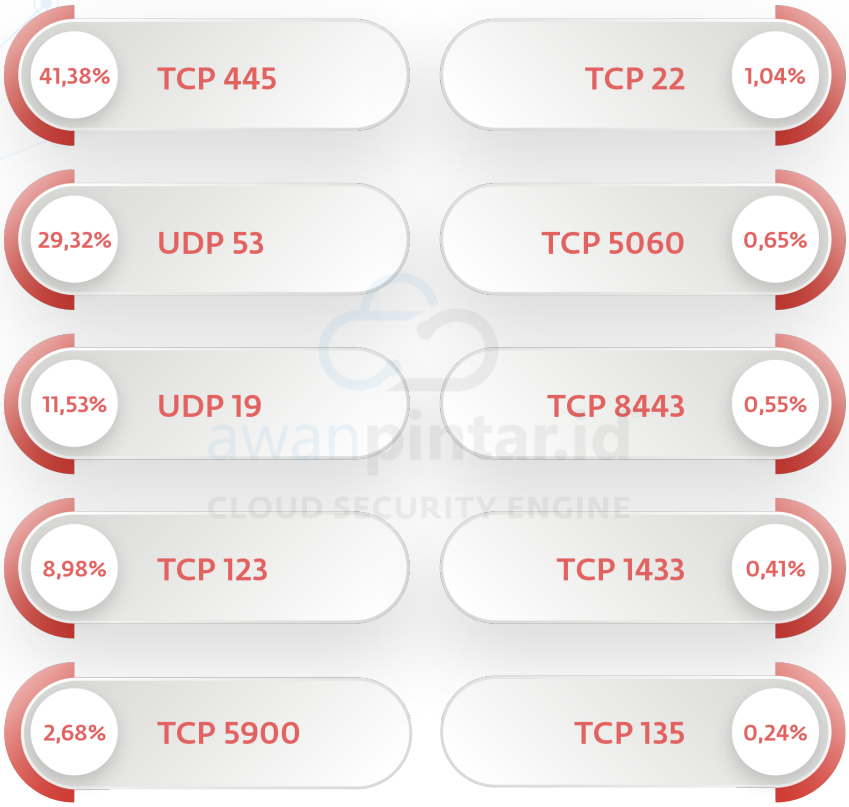
Serangan Port Dalam Negeri

Di dunia siber, "port" bisa diibaratkan sebagai pintu masuk atau keluar data pada sebuah sistem atau jaringan. Serangan yang menargetkan port ini menjadi ancaman serius, terutama jika berasal dari dalam negeri. Untuk menguak pola dan intensitas ancaman ini, AwanPintar.id® telah menganalisis data serangan port dalam negeri selama paruh pertama tahun 2025.

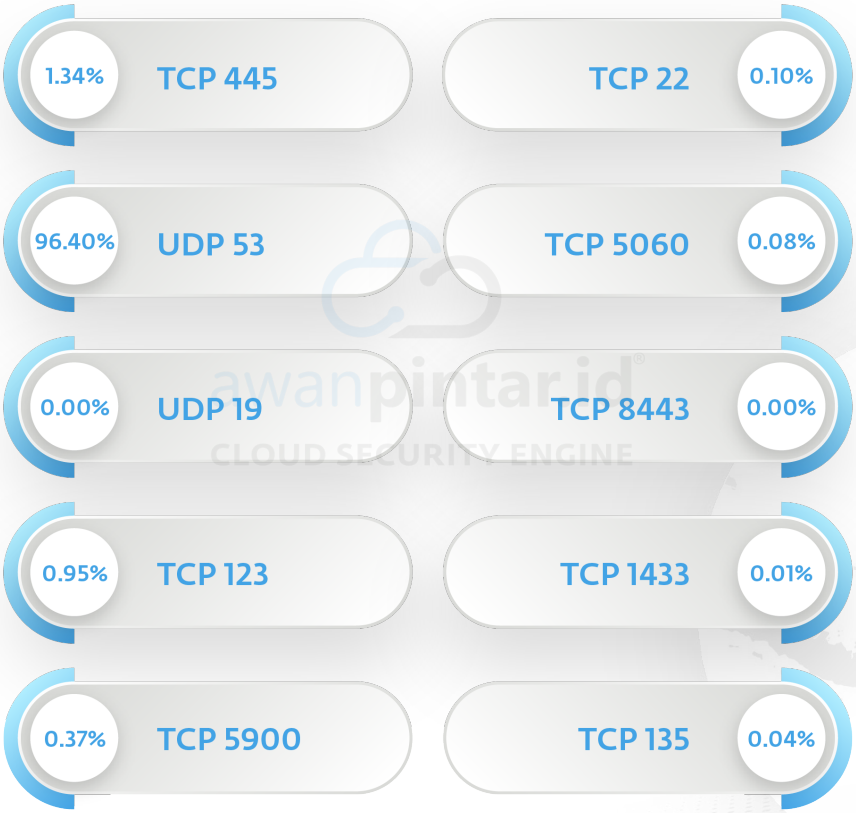
Wawasan ini sangat penting untuk memahami bagaimana celah-celah ini dieksploitasi di lingkungan lokal, memungkinkan kita untuk menutup pintu-pintu yang rentan dan memperkuat pertahanan jaringan di seluruh Indonesia.

Green
OPEN

Semester 1 Tahun 2025

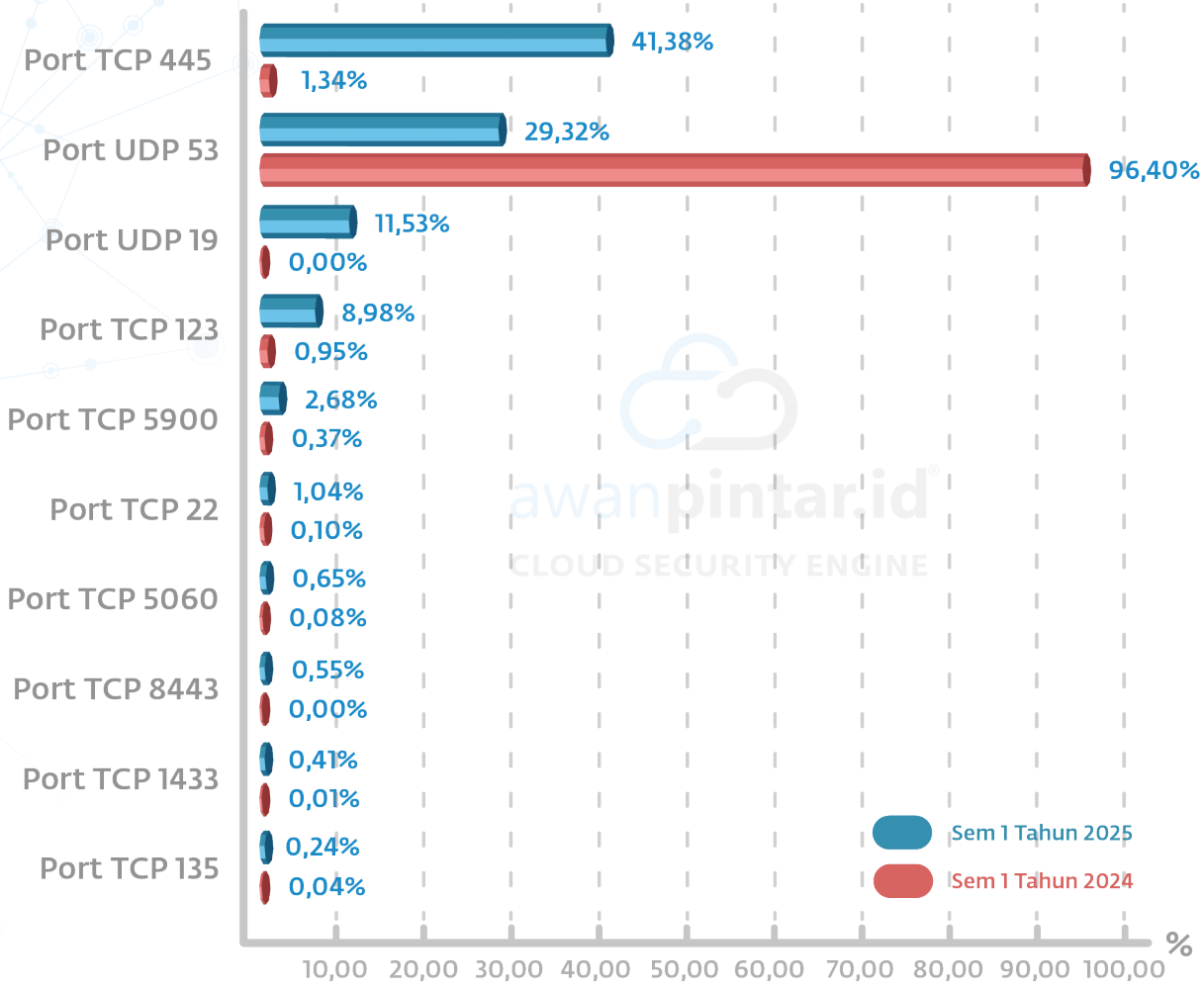


Semester 1 Tahun 2024



Green
OPEN

Komparasi Serangan Port Dalam Negeri Semester 1 Tahun 2024 & Semester 1 Tahun 2024



Port TCP 445
Mengalami Peningkatan 40,04%

Port UDP 53
Mengalami Penurunan -67,08%

Port UDP 19
Serangan Port Baru 11,53%

Port TCP 123
Mengalami Peningkatan 8,03%

Port TCP 5900
Mengalami Peningkatan 2,31%

Port TCP 22
Mengalami Peningkatan 0,94%

Port TCP 5060
Mengalami Peningkatan 0,57%

Port TCP 8443
Serangan Port Baru 0,55%

Port TCP 1433
Serangan Port Baru 0,40%

Port TCP 135
Serangan Port Baru 0,20%

Data AwanPintar.id® mengungkapkan perubahan signifikan pada port yang menjadi target serangan siber dari dalam negeri antara Semester 1 Tahun 2024 dan Semester 1 Tahun 2025.

Pergeseran Prioritas Serangan Port

Dominasi Baru Port TCP 445 (SMB): melonjak drastis dari 1,34% menjadi 41,38% (+40,04%). Ini menjadi port yang paling sering diserang atau disalahgunakan, sangat terkait dengan ancaman seperti ransomware dan pergerakan lateral.

Penurunan Signifikan Port UDP 53 (DNS): yang sebelumnya dominan menyerang dengan teknik DNS Poisoning, turun tajam dari 96,40% menjadi 29,32% (-67,08%). Ini menunjukkan penyerang beralih dari serangan berbasis DNS yang umum.

Munculnya Port Amplification DDoS Baru: Port UDP 19 (CHARGEN) (11,53%), TCP 123 (NTP) (8,98%), dan TCP 8443 (HTTPS) (0,55%) muncul atau meningkat cukup besar secara relatif. Ini adalah protokol yang rentan disalahgunakan untuk serangan DDoS amplification yang lebih canggih.

Peningkatan Serangan Akses & Layanan: Port TCP 5900 (VNC) (2,68%), TCP 22 (SSH) (1,04%), TCP 135 (RPC) (0,0,24%), TCP 5060 (SIP) (+0,57% menjadi 0,65%), dan TCP 1433 (SQL Server) (0,41%) semuanya menunjukkan peningkatan atau kemunculan sebagai target. Ini menandakan upaya penyerang mendapatkan akses melalui layanan-layanan ini.

Implikasi

Pola serangan port ini menunjukkan evolusi taktik penyerang dari dalam negeri. Mereka kini secara agresif menargetkan kerentanan SMB, yang menjadi indikator utama ancaman ransomware atau penyebaran malware di jaringan lokal.

Penurunan serangan DNS mengisyaratkan perpindahan ke metode DDoS amplification yang lebih bervariasi atau terfokus. Peningkatan pada port akses (SSH, VNC, SQL Server) menegaskan bahwa upaya untuk mengkompromikan sistem melalui layanan yang terekspos terus meningkat. Organisasi perlu memperkuat keamanan SMB, menutup atau mengamankan port yang tidak perlu, serta memitigasi risiko DDoS amplification dari sumber internal dan eksternal.

Green
OPEN

LIPUTAN KHUSUS

Common Vulnerability & Exposure Global Semester 1 Tahun 2025

Pada laporan kali ini, mulai ditambahkan laporan terkait diterbitkannya Common Vulnerability & Exposure secara Global yang merupakan data CVE yang dirangkum melalui platform CSIRTradar dan terhubung dengan AwanPintar.id® yang khusus merekam dan menyimpan setiap kerentanan baru yang terjadi pada perangkat lunak dan perangkat keras di seluruh dunia, termasuk Indonesia di dalamnya.

Data ini terus di-update secara real time sesuai dengan kerentanan yang berhasil ditemukan dan telah dikodekan sesuai prosedur, berikut data-data terkini terkait CVE global tahun 2025.

Informasi terkait data CVE penting untuk diketahui pemangku kepentingan di dunia IT Security, hal ini terkait dengan Attack Surface Monitoring (ASM) terkait aset digital yang dimiliki. Common Vulnerability Scoring System (CVSS) memiliki kaitan erat dengan ASM dalam upaya mengelola risiko keamanan siber.

Peran CVSS dengan Attack Surface Monitoring:

CVSS berperan krusial dalam tahapan vital dari Attack Surface Monitoring, yaitu analisis dan prioritisasi kerentanan. Berikut adalah detail kaitannya:

1. **Identifikasi Kerentanan:** ASM bertujuan untuk menemukan semua aset yang terekspos dan potensi kerentanannya. Setelah aset dan kerentanan teridentifikasi (misalnya, melalui pemindaian kerentanan), di sinilah CVSS masuk.
2. **Penilaian Tingkat Keparahan (Severity):** Setiap kerentanan yang ditemukan oleh ASM akan dievaluasi menggunakan CVSS. Skor CVSS memberikan gambaran standar dan objektif tentang seberapa parah kerentanan tersebut dari perspektif teknis. Ini memungkinkan tim keamanan untuk memahami potensi dampak jika kerentanan tersebut dieksploitasi.
3. **Prioritisasi Risiko:** Salah satu manfaat terbesar CVSS dalam konteks ASM adalah membantu dalam prioritisasi. Tidak semua kerentanan memiliki tingkat risiko yang sama, dan tim keamanan jarang memiliki sumber daya tak terbatas untuk mengatasi semuanya sekaligus.
4. **Manajemen Risiko:** Meskipun CVSS memberikan skor teknis, ASM juga menekankan pentingnya konteks. Dalam ASM, skor CVSS tidak hanya dilihat sebagai angka absolut, tetapi juga dipertimbangkan bersama dengan faktor-faktor lain.
5. **Pelaporan dan Kepatuhan:** Penggunaan CVSS dalam proses ASM membantu organisasi memenuhi persyaratan kepatuhan regulasi dan standar audit yang mengharuskan identifikasi dan penanganan risiko keamanan.

Green
OPEN

Fungsi nilai (score) pada CVSS

Nilai pada Common Vulnerability Scoring System (CVSS) memiliki fungsi utama sebagai metrik standar untuk mengukur tingkat keparahan teknis suatu kerentanan. Skor numerik ini, yang berkisar antara 0.0 hingga 10.0, membantu dalam mengkuantifikasi seberapa parah dampak potensial jika sebuah kerentanan berhasil dieksploitasi, serta seberapa mudah kerentanan tersebut dapat dieksploitasi. Dengan adanya nilai standar ini, berbagai pihak, mulai dari peneliti keamanan, vendor perangkat lunak, hingga tim operasional IT, dapat berkomunikasi dan memahami tingkat keparahan kerentanan secara konsisten, terlepas dari konteks atau organisasi mereka. Ini memungkinkan perbandingan objektif antara kerentanan yang ditemukan pada produk atau sistem yang berbeda.

Fungsi krusial lainnya dari nilai CVSS adalah membantu organisasi dalam memprioritaskan upaya remediasi. Dalam lingkungan yang penuh dengan ribuan kerentanan yang dilaporkan setiap tahun, tim keamanan membutuhkan cara yang efisien untuk menentukan mana yang paling mendesak untuk ditangani. Nilai CVSS, bersama dengan faktor-faktor lain seperti konteks bisnis dan kemungkinan eksploitasi di dunia nyata, memungkinkan organisasi untuk fokus pada kerentanan dengan skor tinggi yang memiliki potensi dampak paling merusak atau paling mudah diserang. Dengan demikian, nilai CVSS menjadi alat vital dalam manajemen kerentanan, membantu alokasi sumber daya yang tepat dan pengurangan risiko keamanan secara keseluruhan.

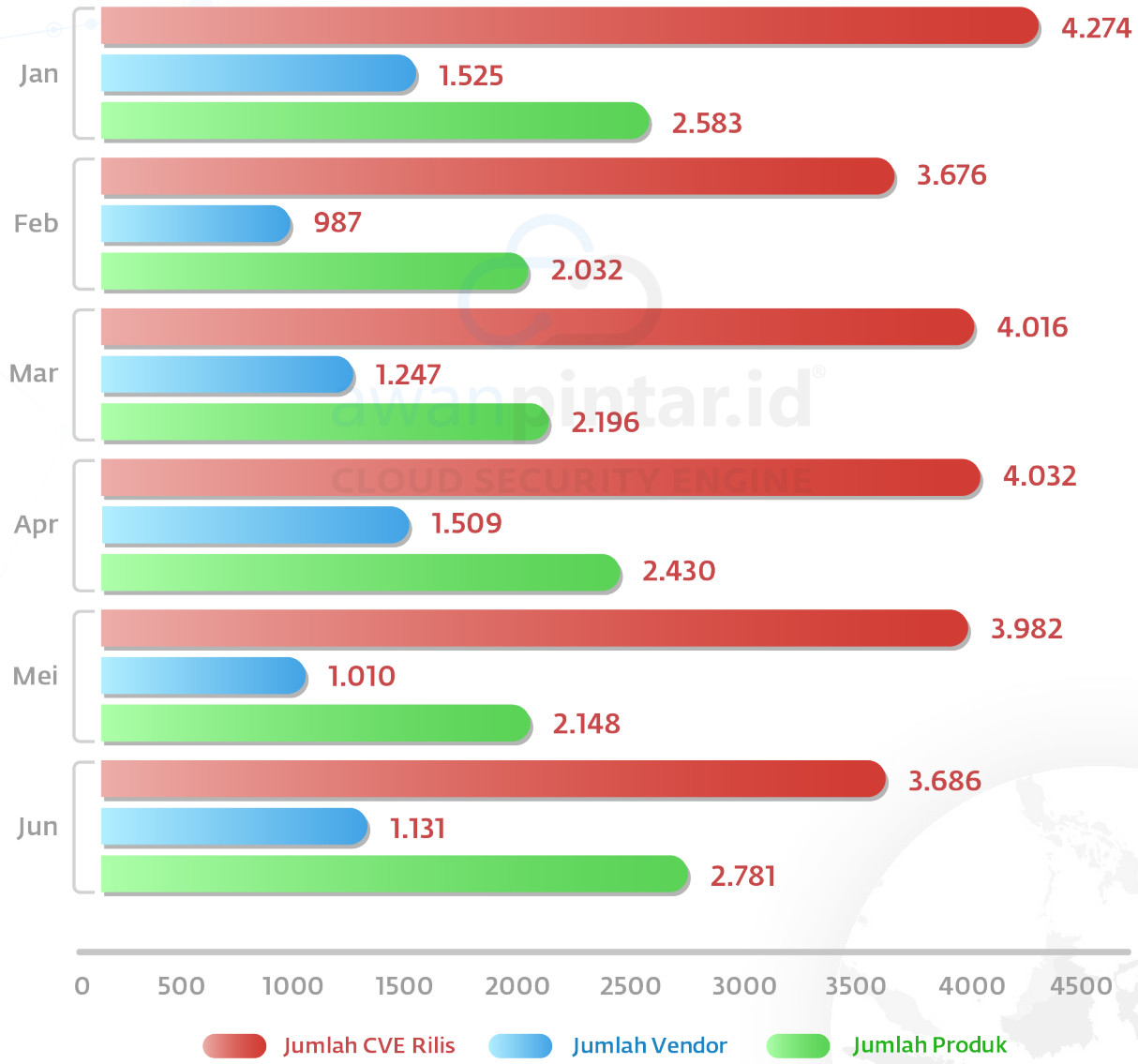
Secara umum peta kerentanan (Heat Map) terkait nilai CVSS dapat digambarkan sesuai tabel di di bawah ini.

Rating	Score	Deskripsi
CRITICAL	9.0-10	Kerentanan yang paling parah dan memiliki dampak yang menghancurkan pada kerahasiaan, integritas, atau ketersediaan sistem. Kerentanan kritis seringkali sangat mudah dieksploitasi (misalnya, melalui jaringan tanpa otentikasi atau interaksi pengguna), dan dapat menyebabkan kompromi sistem yang lengkap atau denial of service (DoS) yang parah. Kerentanan dalam kategori ini harus segera ditangani.
HIGH	7.0-8.9	Kerentanan yang memiliki dampak serius pada kerahasiaan, integritas, atau ketersediaan sistem. Kerentanan ini seringkali lebih mudah dieksploitasi, mungkin memerlukan sedikit atau tanpa interaksi pengguna, dan dapat menyebabkan kerugian yang signifikan. Prioritas penanganannya tinggi.
MEDIUM	4.0-6.9	Kerentanan yang memiliki dampak sedang. Eksploitasi mungkin memerlukan beberapa kondisi yang tidak biasa, seperti interaksi pengguna, atau akses tertentu. Dampaknya bisa berupa hilangnya sebagian kerahasiaan, integritas, atau ketersediaan. Ini adalah kategori yang paling umum untuk banyak kerentanan.
LOW	0.1-3.9	Kerentanan dengan dampak yang sangat terbatas pada kerahasiaan, integritas, atau ketersediaan sistem. Eksploitasi mungkin memerlukan kondisi yang sangat spesifik, interaksi pengguna yang tinggi, atau hak akses yang signifikan, sehingga menjadikannya kurang mungkin untuk dieksploitasi secara luas atau dengan dampak besar.
NONE	0	Kerentanan ini tidak memiliki dampak keamanan yang signifikan atau tidak dapat dieksploitasi untuk menyebabkan kerugian. Ini adalah kerentanan yang paling tidak parah.

CVSS Versi 3.1

CVSS versi 3.1 dirilis pada Juni 2019 dan merupakan penyempurnaan dari CVSS 3.0. Secara spesifik, CVSS versi 3.1 hadir sebagai kerangka kerja yang lebih matang dan komprehensif dibandingkan pendahulunya, menyediakan metrik terperinci untuk menghitung tingkat keparahan (severity) kerentanan berdasarkan faktor-faktor seperti kemampuan eksploitasi, dampak terhadap kerahasiaan, integritas, dan ketersediaan, serta tingkat remediasi yang diperlukan. Data CVSS 3.1 oleh karena itu menjadi informasi esensial bagi organisasi dan profesional keamanan untuk memprioritaskan upaya mitigasi, mengalokasikan sumber daya secara efektif, dan pada akhirnya memperkuat postur keamanan siber mereka.

Jumlah Total CVE, Vendor dan Produk CVSS 3.1

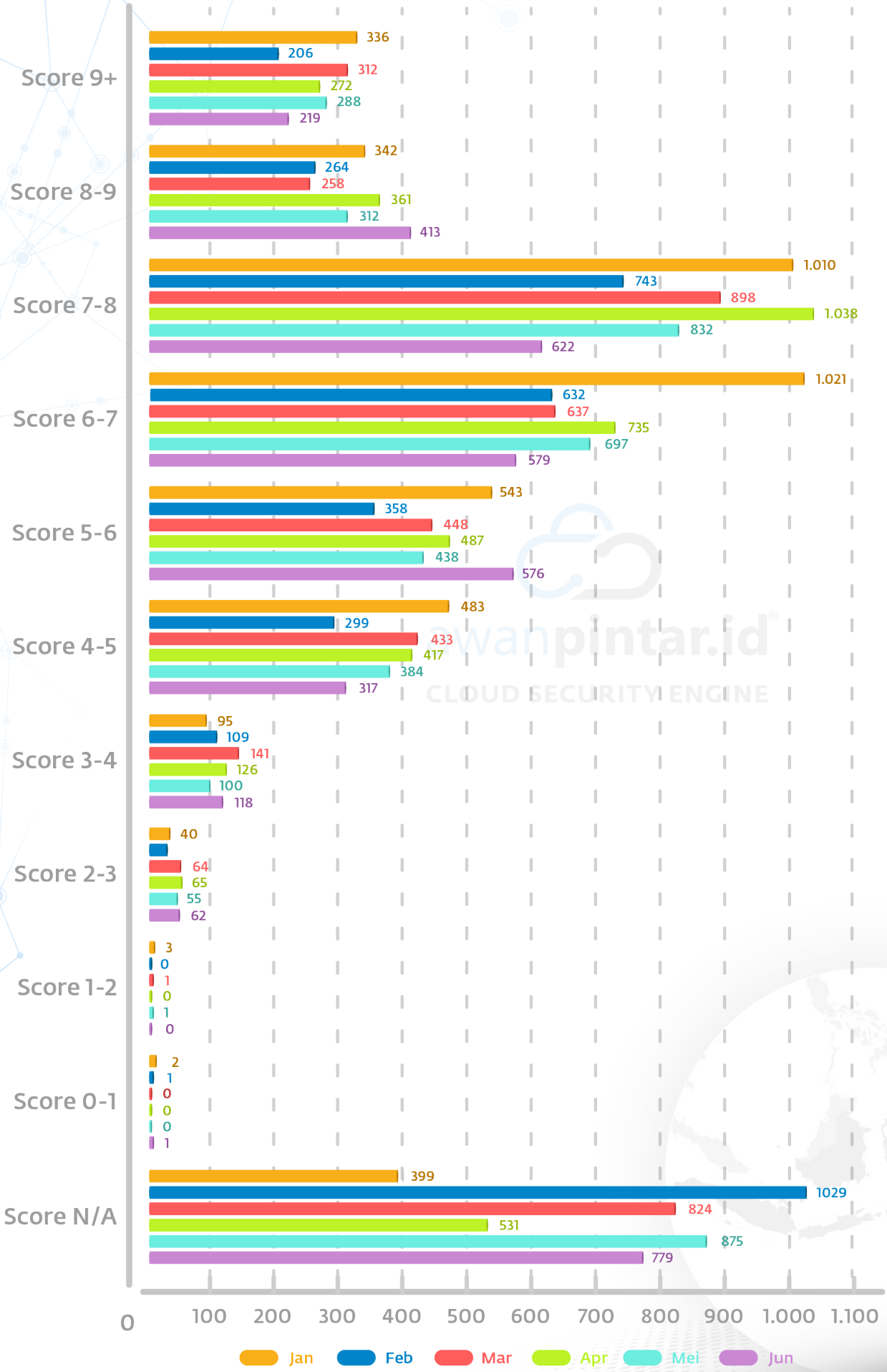


	Jumlah CVE Rilis	Jumlah Vendor	Jumlah Produk
Total	23.666	7.409	14.170
Rata-Rata	3.945	1.235	2.362

Green

OPEN

Sebaran CVE Score CVSS 3.1



Green
OPEN

Total dan Rata-rata CVSS Score Versi 3.1

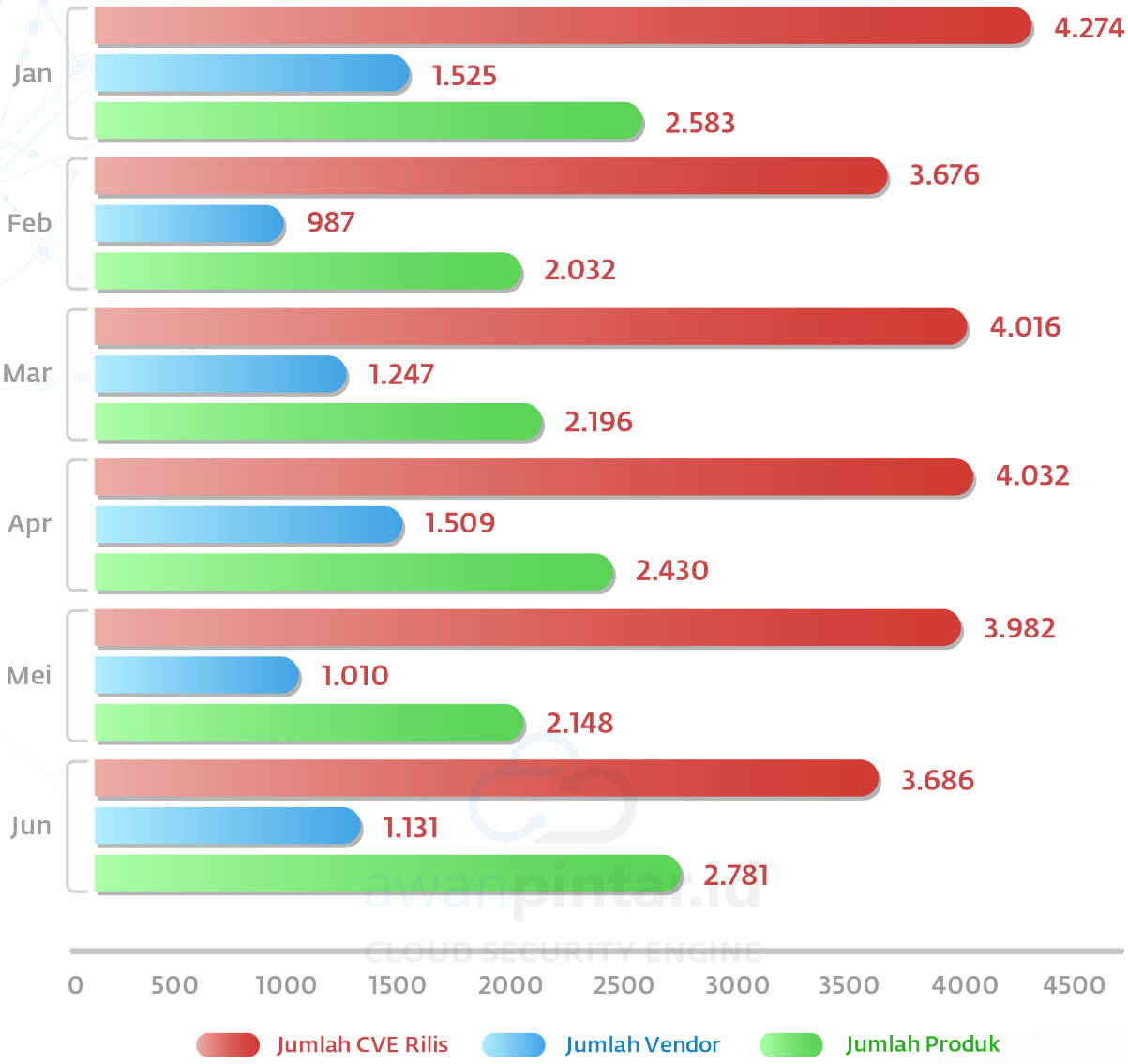
	CVSS Score										
	9	8-9	7-8	6-7	5-6	4-5	3-4	2-3	1-2	0-1	N/A
Total	1.632	1.950	5.143	4.301	2.850	2.333	689	322	5	4	4.437
Rata-Rata	272	325	858	717	475	389	115	54	1	1	740

CVSS Versi 4.0

CVSS versi 4.0 adalah generasi terbaru dari standar ini, yang dirilis pada tahun 2023. Versi ini dirancang untuk memberikan penilaian kerentanan yang lebih akurat, bernuansa, dan sesuai konteks, dengan fokus yang lebih besar pada kecerdasan ancaman (threat intelligence) dan dampak spesifik.

Hasil penilaian CVSS versi 4.0 berbeda dengan versi sebelumnya. Pada kolom nilai N/A (Not Available) menunjukkan angka yang tinggi, umumnya ini dikarenakan banyaknya CVE yang memiliki informasi terbatas untuk dinilai menggunakan metode perhitungan versi 4.0. Alasan ini menjadikan versi 3.1 lebih sering menjadi acuan penilaian.

Jumlah Total CVE, Vendor dan Produk CVSS 4.0

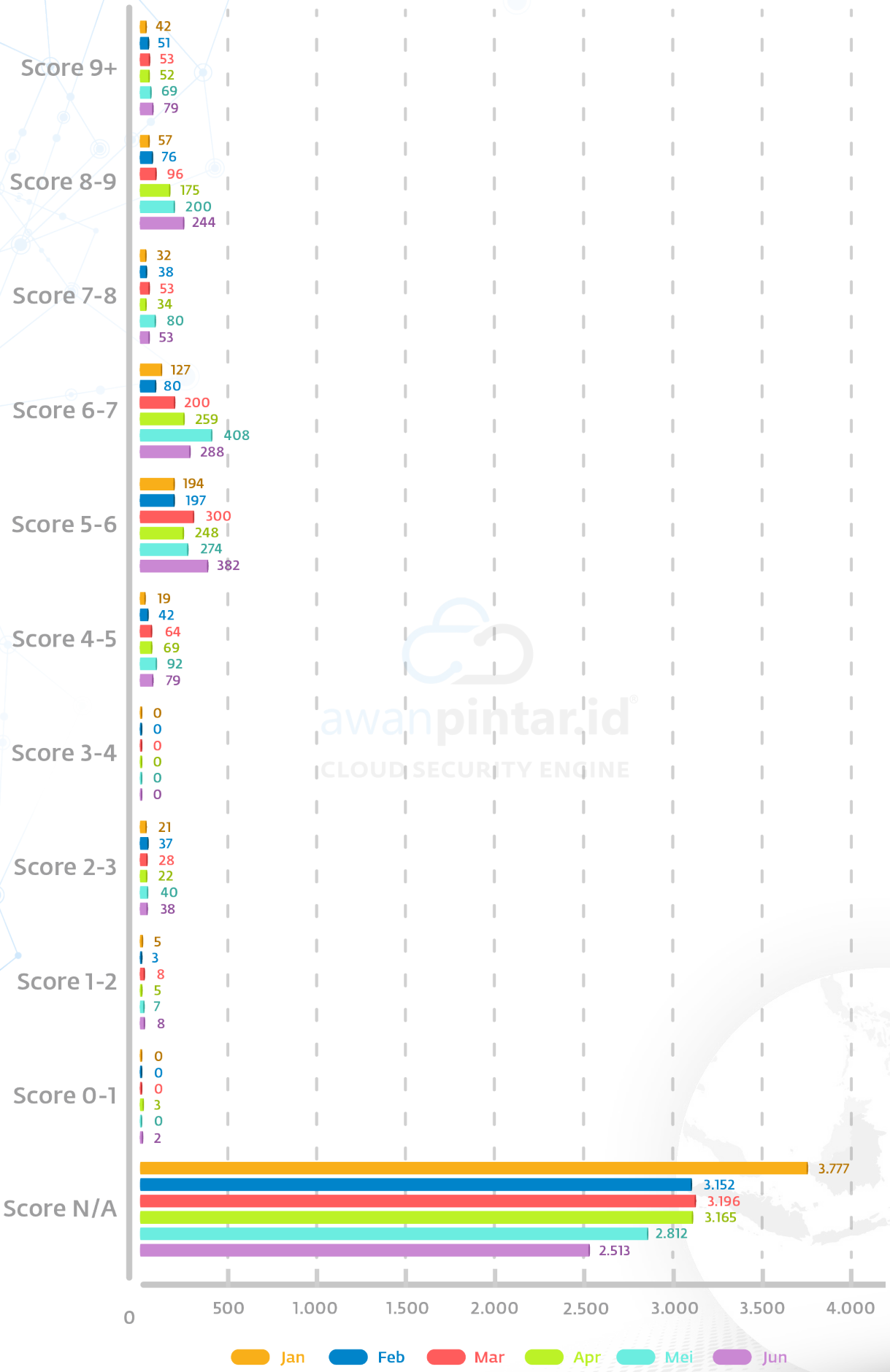


	Jumlah CVE Rilis	Jumlah Vendor	Jumlah Produk
Total	23.666	7.409	14.170
Rata-Rata	3.945	1.235	2.362

Green

OPEN

Sebaran CVE Score CVSS 4.0



Green
OPEN

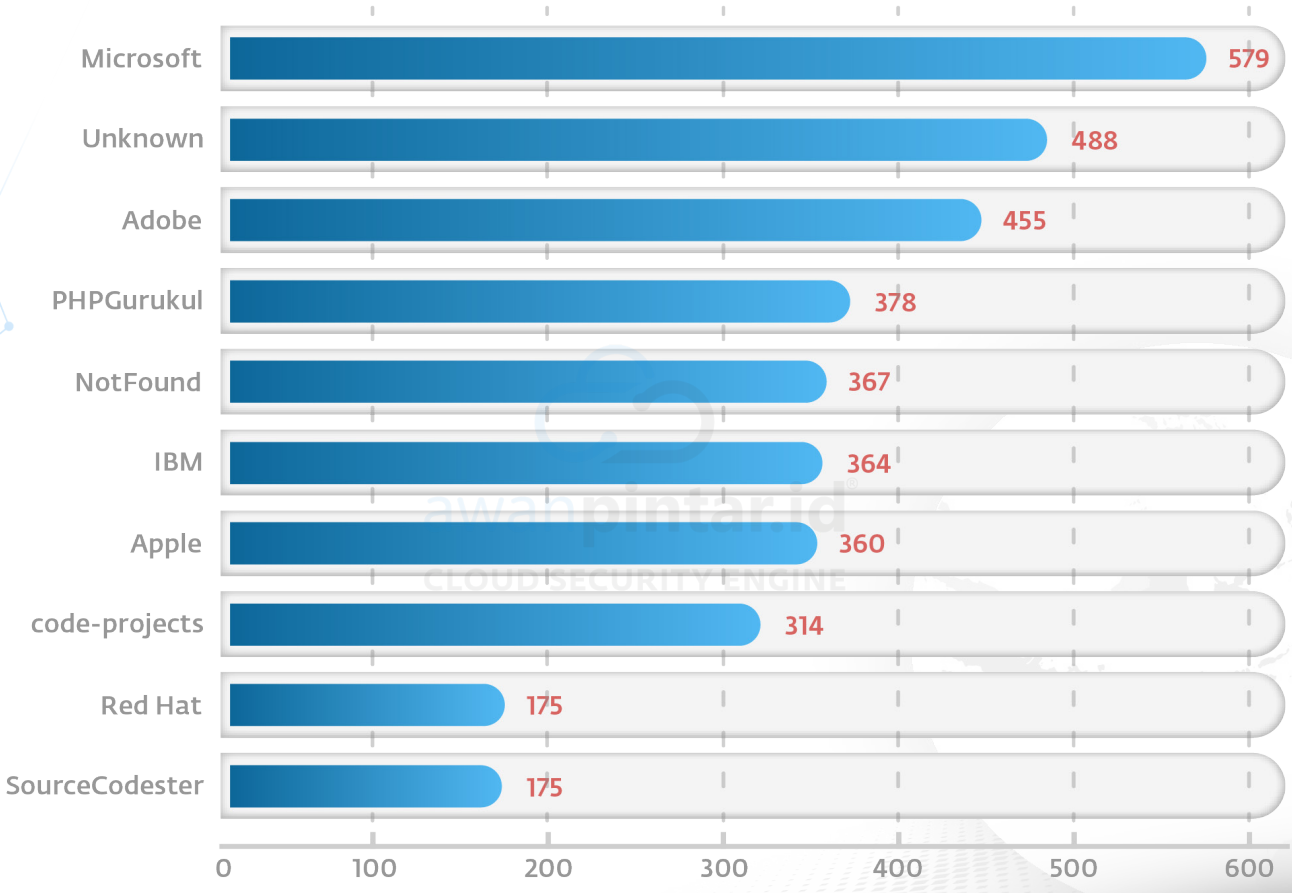
Total dan Rata-rata CVSS Score Versi 4.0

	CVSS Score										
	9	8-9	7-8	6-7	5-6	4-5	3-4	2-3	1-2	0-1	N/A
Total	346	848	308	1.362	1.595	365	0	186	36	5	18.615
Rata-Rata	58	142	52	227	266	61	0	31	6	1	3.103

Prioritas Penanganan

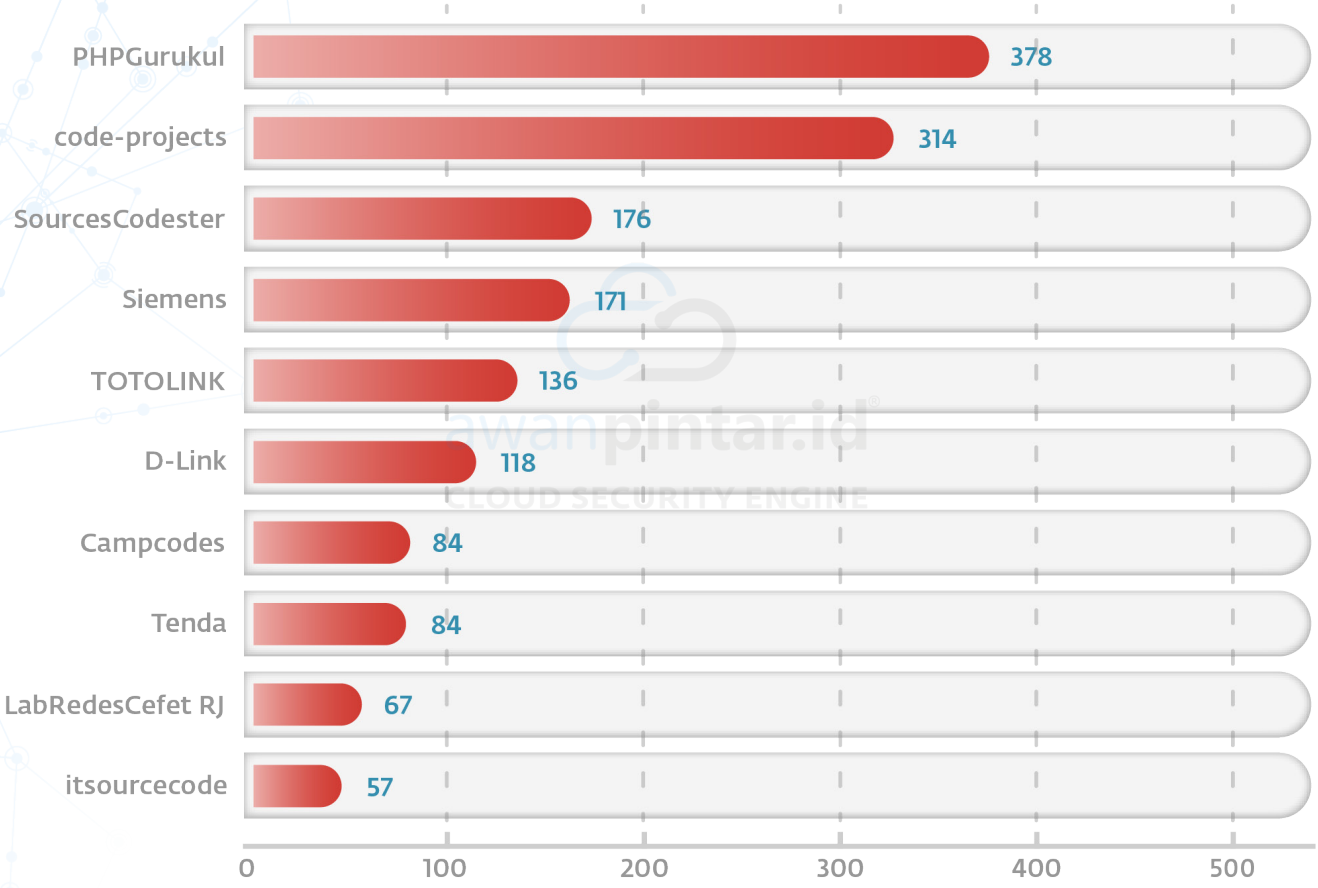
Dalam ekosistem keamanan siber yang terus bergejolak, kerentanan merupakan titik masuk potensial bagi penyerang untuk merusak sistem, mencuri data, atau mengganggu layanan. Fokus khusus pada kerentanan dengan skor CVSS Tinggi (7.0-8.9) dan Kritikal (9.0-10.0) menjadi sangat penting karena keduanya merepresentasikan ancaman dengan potensi dampak serius. Kerentanan kritikal adalah prioritas utama karena biasanya mudah dieksploitasi dan dapat menyebabkan kerugian parah, seperti kompromi sistem total atau pengungkapan data sensitif skala besar. Sementara itu, kerentanan tinggi, meskipun mungkin memerlukan upaya lebih untuk dieksploitasi atau memiliki dampak yang sedikit lebih rendah dari kritikal, tetap dapat mengakibatkan gangguan operasional signifikan, pelanggaran integritas data, atau kerugian finansial yang substansial. Mengabaikan salah satu kategori ini dapat menempatkan organisasi pada risiko yang tidak perlu, sehingga respons yang cepat dan terkoordinasi terhadap kedua skala ini sangat vital untuk menjaga postur keamanan yang kuat.

10 Besar Vendor CVSS 3.1 Semester 1 Tahun 2025



Green
OPEN

10 Besar Vendor CVSS 4.0 Semester 1 Tahun 2025

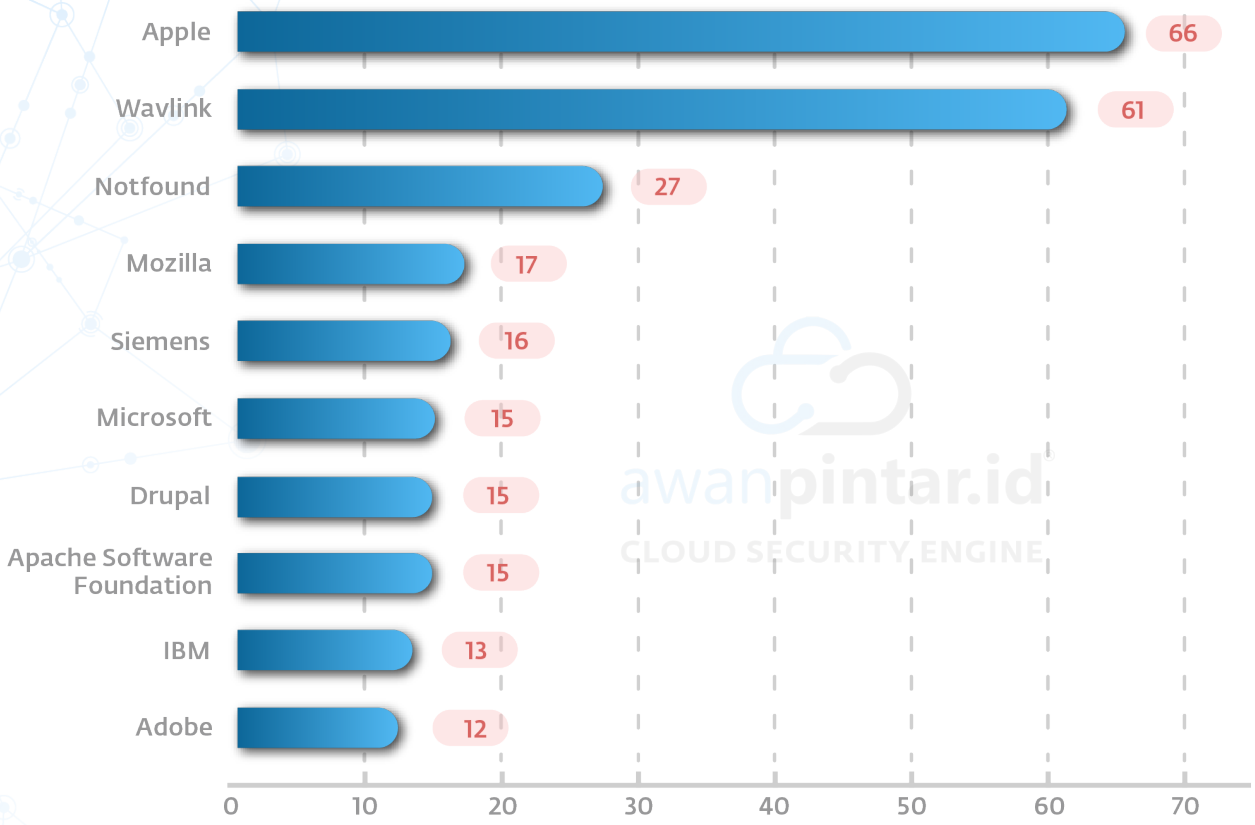


10 Vendor terbanyak mencatatkan nilai 0 hingga 10.

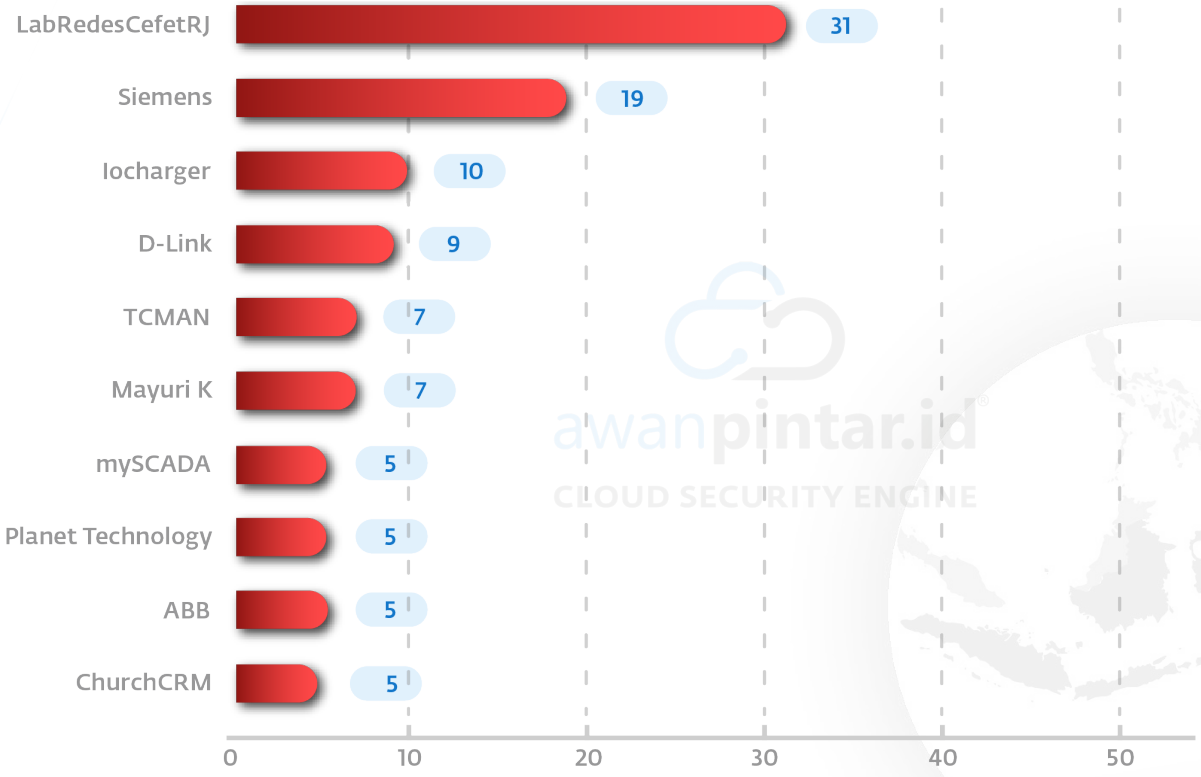
Dari data diatas dapat dilihat, vendor dengan produk populer yang sering kita dengar dalam dunia digital menempati rangking 10 besar. Namun perlu diketahui, bukan berarti nama vendor yang disebutkan memiliki tingkat kerentanan kritikal yang tinggi, karena nilai yang dikumpulkan adalah 0 hingga 10. Secara skala prioritas, data di bawah merupakan nilai dengan status Kritikal.

Green
OPEN

Top 10 Vendor CVSS Score 9-10 CVSS 3.1



Top 10 Vendor CVSS Score 9-10 CVSS 4-0

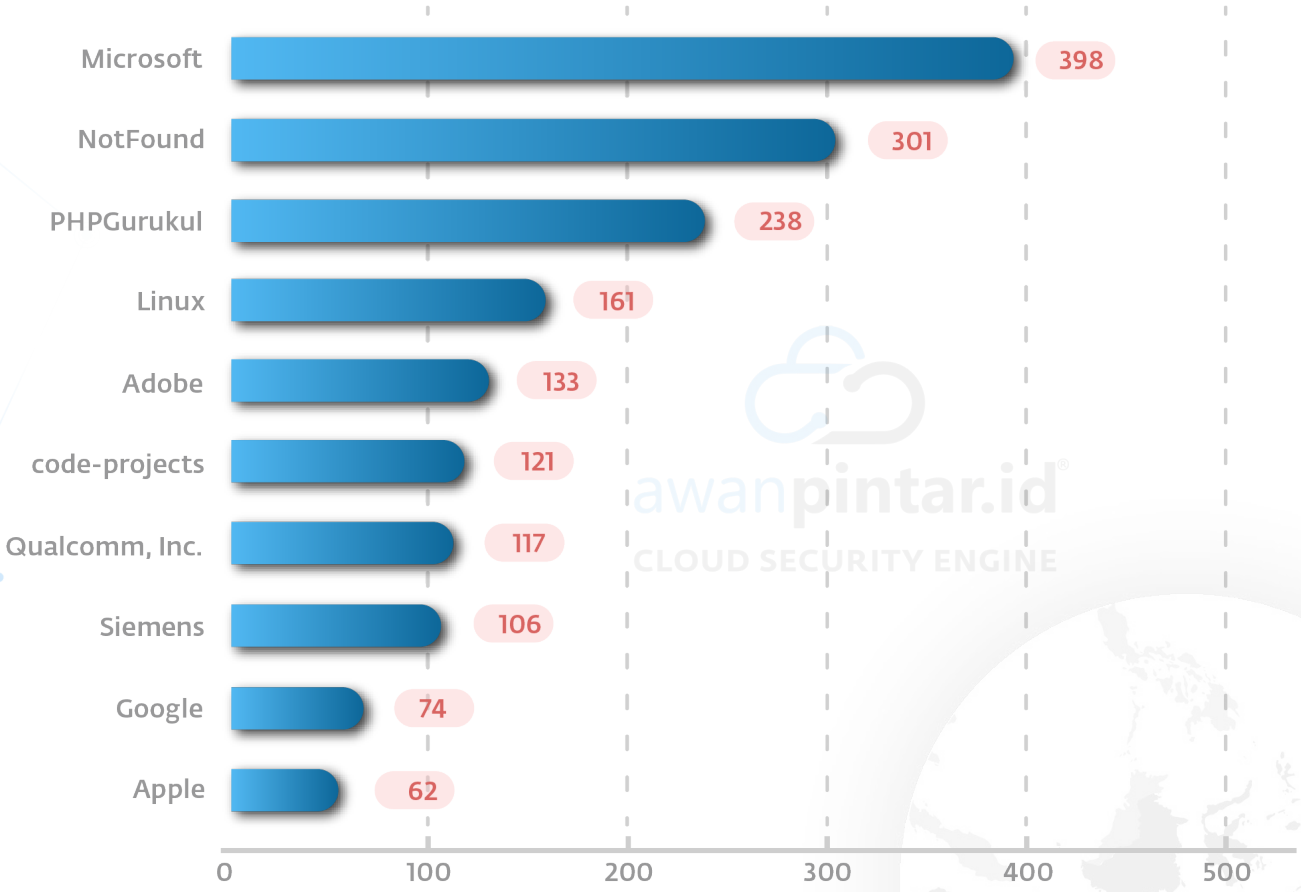


10 Vendor terbanyak mencatatkan nilai 9 hingga 10 (Critical)

Dari data sebelumnya, dapat dilihat vendor yang membutuhkan perhatian lebih tekait kerencanan yang dimiiliki karena sudah masuk kategori kritis. Kerentanan yang mendapatkan nilai CVSS kritikal (umumnya 9.0-10.0) menandakan adanya potensi dampak yang sangat parah terhadap kerahasiaan, integritas, atau ketersediaan sistem, serta kemudahan eksploitasi yang tinggi. Oleh karena itu, respon cepat terhadap kerentanan CVSS kritikal bukan hanya rekomendasi terbaik, melainkan sebuah keharusan mendesak untuk melindungi aset digital vital, menjaga reputasi bisnis, dan mencegah kerugian finansial maupun operasional yang masif akibat pelanggaran keamanan.

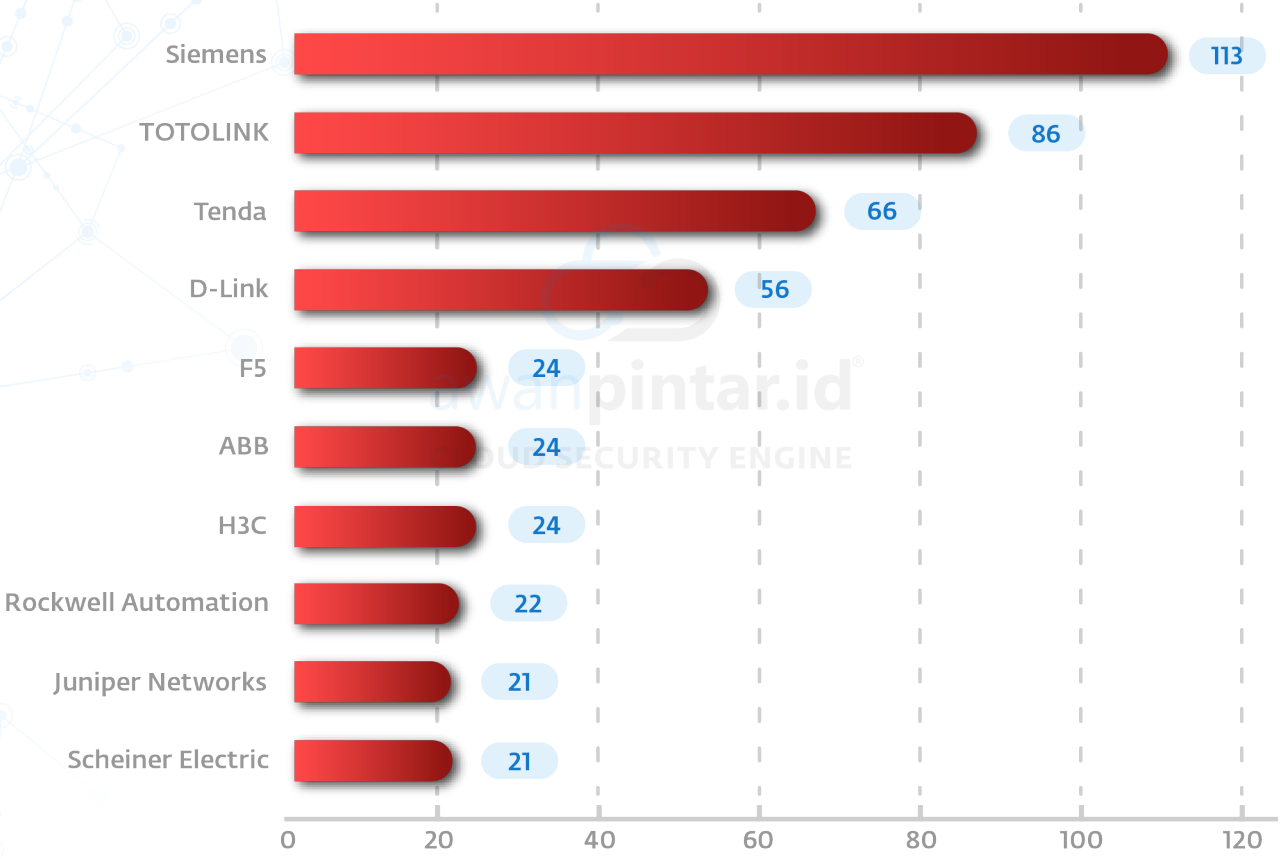
Catatan khusus, Dalam daftar CVE, penunjukan vendor "Not Found" biasanya menunjukkan bahwa vendor yang bertanggung jawab atas produk yang rentan tersebut tidak ada, tidak dikenal publik, atau telah memilih untuk tidak diasosiasikan dengan catatan CVE spesifik tersebut. Hal ini juga dapat terjadi jika produk atau versi yang dimaksud sudah tidak lagi didukung oleh vendor dan mereka tidak ingin dikaitkan dengan kerentanan tersebut.

Top 10 Vendor CVSS Score 7-8.9
CVSS 3.1



Green
OPEN

Top 10 Vendor CVSS Score 7-8.9
CVSS 4.0



10 Vendor terbanyak mencatatkan nilai 7 hingga 8.9 (High)

Kerentanan yang mendapatkan nilai CVSS tinggi (umumnya 7.0-8.9) menandakan adanya potensi dampak yang signifikan terhadap kerahasiaan, integritas, atau ketersediaan sistem, serta kemudahan eksploitasi yang tidak dapat diabaikan. Meskipun tidak se-kritis kerentanan "kritikal", kerentanan dengan skor tinggi masih dapat menyebabkan kerugian substansial, termasuk pelanggaran data, gangguan layanan, dan dampak finansial. Oleh karena itu, respon cepat terhadap kerentanan CVSS tinggi adalah langkah proaktif yang penting untuk meminimalkan risiko, melindungi aset digital, dan menjaga kelangsungan operasional di tengah ancaman siber yang terus-menerus.

Green
OPEN

Open Source Vulnerability Global Semester 1 Tahun 2025

Dalam lanskap pengembangan perangkat lunak modern, penggunaan komponen sumber terbuka (open source) telah menjadi praktik yang sangat umum dan bahkan esensial. Dari sistem operasi hingga pustaka kode spesifik, perangkat lunak sumber terbuka menawarkan kecepatan, fleksibilitas, dan inovasi yang tak tertandingi.

Namun, di balik segala keunggulannya, terdapat sebuah tantangan signifikan yang seringkali terabaikan: kerentanan sumber terbuka. Kerentanan ini adalah cacat atau kelemahan dalam kode sumber terbuka yang dapat dieksploitasi oleh pihak jahat untuk tujuan tidak sah, seperti pencurian data, gangguan layanan, atau bahkan kontrol penuh atas sistem yang terinfeksi. Mengingat sebagian besar aplikasi saat ini dibangun di atas fondasi sumber terbuka, pemahaman dan pengelolaan kerentanan ini menjadi krusial.

Penyebab utama munculnya kerentanan sumber terbuka bervariasi. Seringkali, kerentanan tersebut muncul karena kesalahan pemrograman yang tidak disengaja oleh pengembang. Komunitas sumber terbuka yang besar dan tersebar juga berarti bahwa kode mungkin ditinjau oleh banyak mata, namun tidak semua mata memiliki tingkat keahlian atau niat yang sama dalam mengidentifikasi potensi kelemahan.

Open Source Vulnerability (OSV) adalah tantangan yang tidak dapat dihindari dalam ekosistem perangkat lunak terbuka saat ini. Namun, dengan pendekatan yang komprehensif, mencakup identifikasi, pemantauan, mitigasi, dan manajemen yang berkelanjutan, organisasi dapat secara signifikan mengurangi risiko yang terkait dengan penggunaan komponen sumber terbuka. Investasi dalam alat dan proses keamanan, serta pengembangan budaya keamanan yang kuat di antara tim, akan menjadi kunci untuk memanfaatkan keuntungan besar dari sumber terbuka sambil menjaga integritas dan keamanan aplikasi dan data.

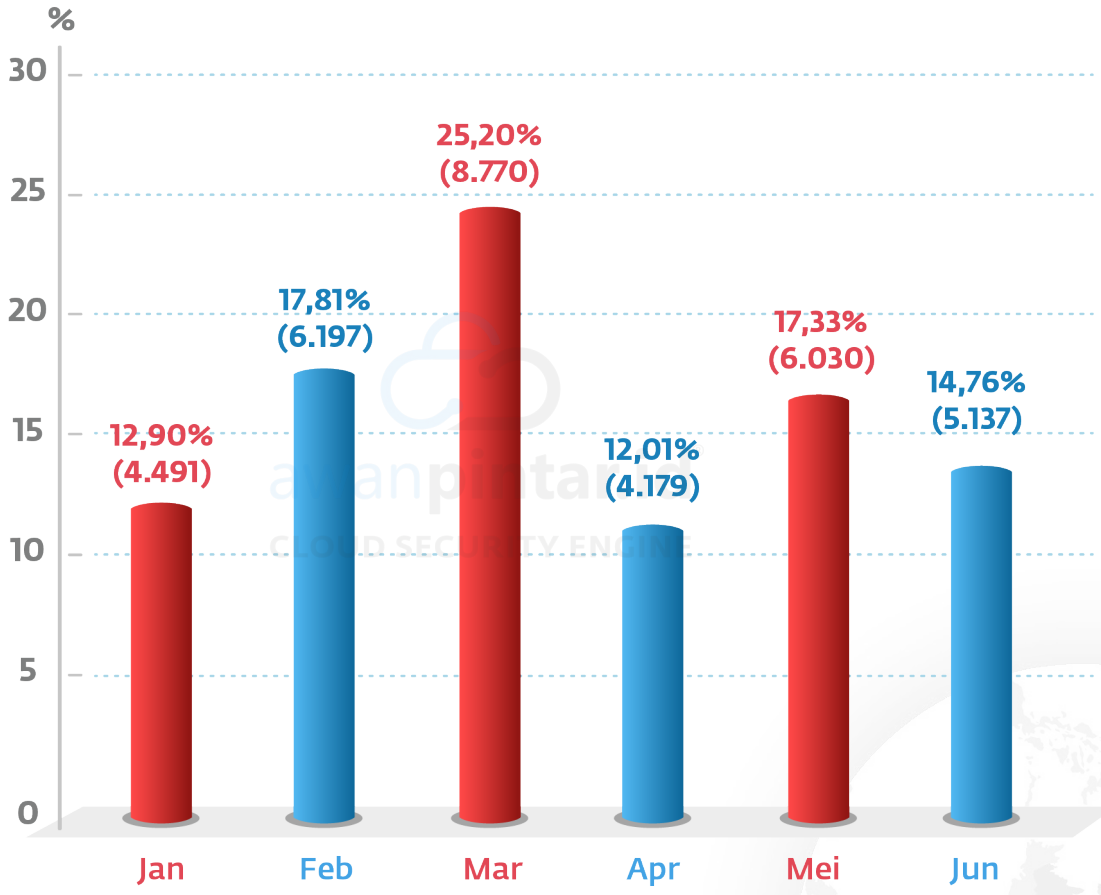
Seperti halnya CVSS,Informasi terkait data OSV penting untuk diketahui pemangku kepentingan di dunia IT Security, hal ini terkait dengan Attack Surface Monitoring (ASM) terkait aset digital yang dimiliki. Monitoring OSV secara berkala akan membantu menutup celah keamanan yang ada. Berikut beberapa manfaat terkait ASM.

1. **Identifikasi Komponen Sumber Terbuka:** Tahap awal ASM adalah menemukan semua aset. Di dalam aset-aset ini, terutama aplikasi web dan layanan, terdapat banyak komponen sumber terbuka. OSV membantu mengidentifikasi dan memetakan komponen-komponen ini.
2. **Pemindaian Kerentanan yang Spesifik:** Setelah komponen sumber terbuka teridentifikasi (seringkali melalui Software Bill of Materials - SBOM), data dari OSV dapat digunakan untuk secara otomatis memindai dan memverifikasi apakah ada kerentanan yang diketahui yang memengaruhi versi spesifik dari komponen tersebut. Ini lebih akurat daripada hanya mengandalkan basis data kerentanan umum.
3. **Supply Chain Security:** OSV secara langsung mendukung manajemen rantai pasokan perangkat lunak, yang merupakan bagian krusial dari Attack Surface Monitoring. Dengan mengetahui

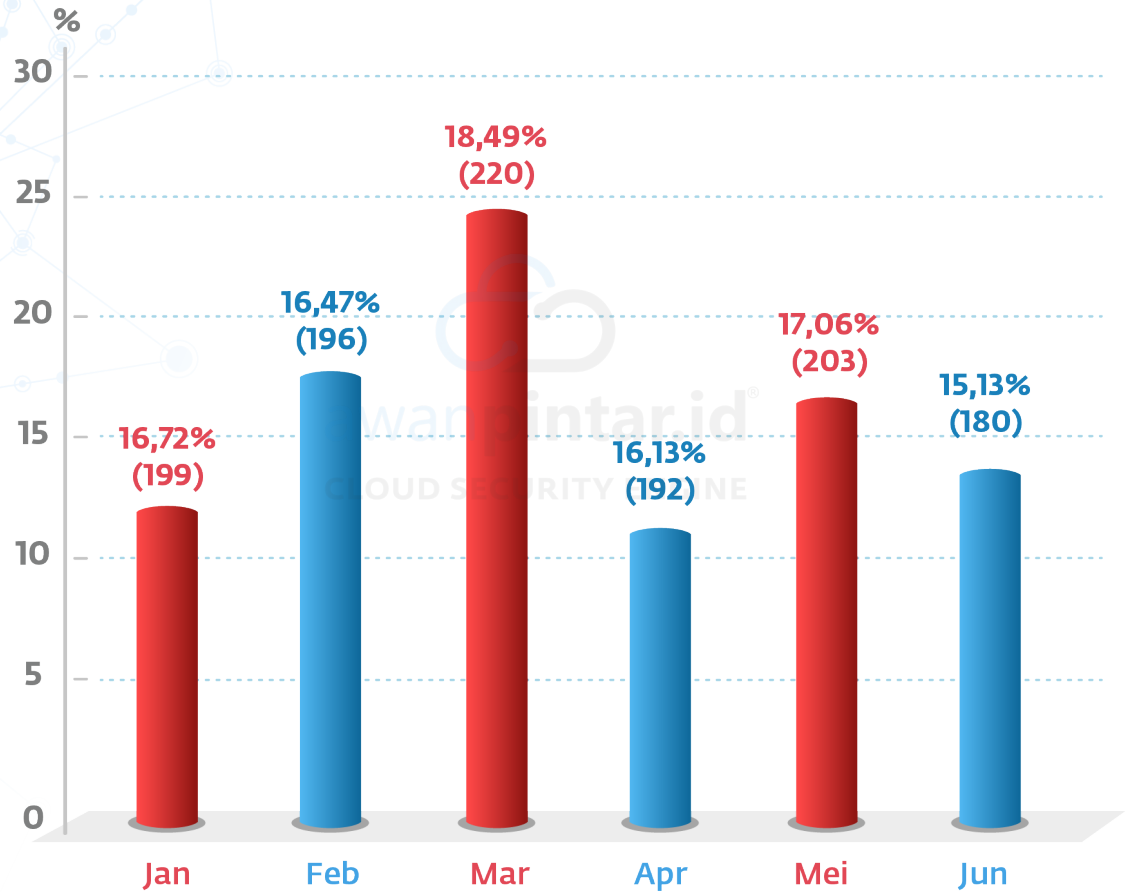
kerentanan dalam dependensi sumber terbuka, sehingga dapat mencegah masuknya kerentanan dan melakukan prioritisasi remediasi yang lebih Baik.

4. **Mengurangi "Shadow IT" dalam Konteks Open Source:** Seringkali, pengembang menggunakan pustaka open source tanpa sepengetahuan tim keamanan, menciptakan "shadow IT" dalam bentuk dependensi yang rentan. ASM, dengan bantuan OSV, dapat mengungkap dan mengelola risiko-risiko tersembunyi ini.
5. **Visibilitas yang Lebih Akurat:** Integrasi data OSV ke dalam alat ASM memberikan visibilitas yang jauh lebih akurat terhadap risiko yang ditimbulkan oleh komponen sumber terbuka dalam ekosistem digital organisasi. Ini memungkinkan tim keamanan untuk tidak hanya melihat apa yang terekspos secara eksternal tetapi juga apa yang rentan di dalamnya.

Sebaran OSV Semester 1 Tahun 2025



Sebaran Ekosistem OSV Semester 1 Tahun 2025



Data menunjukkan tren rilis kerentanan Open Source (OSV) sepanjang paruh pertama tahun ini. Angka ini mencerminkan aktivitas penemuan dan pengungkapan kerentanan pada proyek-proyek open source yang penting untuk dipantau oleh tim keamanan siber.

Temuan Kunci

Puncak Rilis di Bulan Maret: Bulan Maret mencatat jumlah rilis OSV tertinggi secara signifikan, yaitu 25,20% dari total rilis selama enam bulan. Ini mengindikasikan adanya lonjakan penemuan kerentanan atau pengungkapan bug bounty yang besar pada periode tersebut.

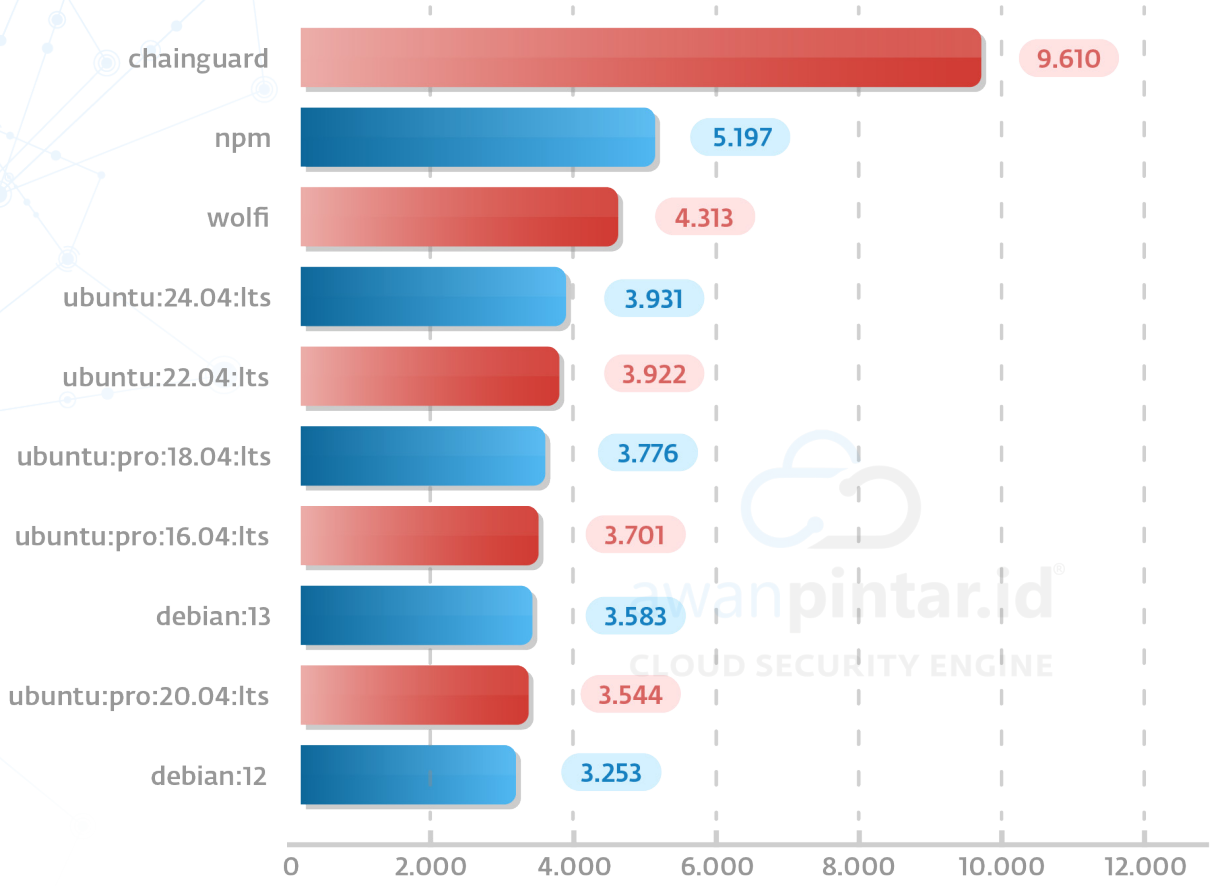
Aktivitas Rilis yang Tinggi di Awal Tahun: Tiga bulan pertama (Januari, Februari, Maret) secara kumulatif menyumbang lebih dari separuh total rilis OSV, yaitu sekitar 55,91%.

Penurunan di April, Lalu Sedikit Kenaikan Kembali: Setelah lonjakan di Maret, terjadi penurunan tajam di April, namun kemudian diikuti oleh sedikit kenaikan di Mei dan kembali menurun di Juni. Ini menunjukkan pola fluktuatif namun tetap dengan volume rilis yang substansial setiap bulannya.

Total Rilis yang Besar: Selama enam bulan pertama, ada total 34.804 rilis OSV. Ini menunjukkan besarnya volume kerentanan open source yang ditemukan dan diungkapkan secara terus-menerus.

Green
OPEN

10 Ekosistem OSV Tertinggi Semester 1 Tahun 2025



Implikasi

Pentingnya Pemantauan Berkelanjutan: Volume rilis OSV yang tinggi, terutama lonjakan di bulan-bulan tertentu, menggarisbawahi pentingnya pemantauan kerentanan open source secara berkelanjutan dan otomatis. Organisasi yang banyak menggunakan komponen open source dalam produk atau infrastruktur mereka harus memiliki sistem untuk melacak rilis OSV dan dampaknya.

Manajemen Risiko Proaktif: Lonjakan rilis di bulan Maret bisa jadi merupakan hasil dari kampanye bug bounty besar, temuan penelitian keamanan, atau pengungkapan kerentanan yang terkoordinasi. Tim keamanan harus siap untuk menghadapi gelombang kerentanan baru dan memiliki proses yang efisien untuk menilai, memprioritaskan, dan menambal kerentanan tersebut.

Pengaruh Ekosistem Open Source: Tren ini juga mencerminkan dinamika dalam ekosistem open source itu sendiri. Peningkatan jumlah rilis bisa jadi indikasi meningkatnya jumlah kontributor yang mencari kerentanan, atau adanya proyek open source baru yang rentan yang menjadi populer.

Dampak pada Supply Chain Security: Mengingat banyak aplikasi modern dibangun di atas tumpukan open source, rilis OSV ini memiliki dampak langsung pada keamanan rantai pasokan perangkat lunak (software supply chain security). Setiap rilis kerentanan bisa berpotensi menjadi risiko bagi banyak pengguna di seluruh dunia.

Kesimpulan: Data rilis OSV ini menjadi pengingat kritis bagi organisasi untuk memiliki strategi manajemen kerentanan open source yang kuat. Ini termasuk menggunakan Software Composition Analysis (SCA) tools untuk mengidentifikasi komponen open source yang rentan, memantau feed kerentanan secara real-time, dan memiliki proses patching yang cepat.

Vulnerability Manajemen dalam Pemenuhan Kepatuhan (Compliance)

NIST dan ISO 27001-2022

Dengan adanya ID CVE yang unik, organisasi dapat secara seragam mengidentifikasi, melacak, dan membahas kerentanan di seluruh produk dan platform, memfasilitasi komunikasi yang jelas antara vendor, peneliti, dan pengguna akhir. Ini menjadi fondasi bagi fungsi "Identifikasi" (Identify (ID)) dalam kerangka NIST, memungkinkan organisasi untuk membangun pemahaman yang komprehensif tentang risiko keamanan siber yang terkait dengan sistem dan aset mereka.

Open Source Vulnerability (OSV) melengkapi pendekatan ini dengan menyediakan database kerentanan yang secara spesifik berfokus pada komponen open source. Mengingat ketergantungan yang semakin besar pada perangkat lunak open source di hampir setiap lingkungan TI modern, kemampuan untuk dengan cepat dan akurat mengidentifikasi kerentanan dalam pustaka atau dependensi open source sangatlah penting. Dengan menggabungkan informasi dari CVE dan OSV, organisasi dapat memenuhi persyaratan kepatuhan NIST yang mendorong manajemen risiko berkelanjutan, deteksi ancaman, dan respons insiden. Keduanya memungkinkan tim keamanan untuk secara proaktif memantau, menilai, dan memitigasi risiko kerentanan, memastikan bahwa kontrol keamanan yang relevan diterapkan dan dipertahankan untuk mencapai postur keamanan yang kuat dan sesuai dengan standar yang ditetapkan.

Annex A.8.8 pada ISO 27001-2022 terkait Pengendalian Manajemen Kerentanan Teknis (Management of Technical Vulnerabilities) secara spesifik menekankan peran perlilndungan aset terhadap kemungkinan eksploitasi kerentanan yang ada. Informasi terkait CVE dan OSV dapat membantu organisasi dalam kaitan sebagai berikut:

1. **Sumber Informasi Kerentanan**
   Annex A.8.8 secara eksplisit menyatakan bahwa organisasi harus "mendapatkan informasi tentang kerentanan teknis dari sistem informasi yang digunakan." Pemberitahuan kerentanan (vulnerability alerts), baik dari vendor perangkat lunak, penyedia layanan, lembaga penelitian keamanan, atau bahkan dari pihak ketiga yang melaporkan (melalui program vulnerability disclosure), adalah sumber utama dari informasi ini.
2. **Identifikasi dan Penilaian**
   Setelah menerima "vulnerability alert", organisasi diharapkan untuk:
   - Mengidentifikasi keberadaan kerentanan dalam produk dan layanan mereka, termasuk komponen eksternal yang digunakan.
   - Mengevaluasi eksposur organisasi terhadap kerentanan tersebut. Ini melibatkan penilaian risiko untuk memahami potensi dampak dan kemungkinan eksploitasi.
3. **Pengambilan TIndakan yang Tepat**
   Berdasarkan penilaian kerentanan, organisasi harus "mengambil tindakan yang tepat" untuk menanganinya. Ini bisa mencakup:
   - Menerapkan patch atau pembaruan keamanan.
   - Mengkonfigurasi ulang sistem atau jaringan.
   - Menerapkan kontrol keamanan tambahan (misalnya, firewall, virtual patching).
   - Meningkatkan pemantauan untuk mendeteksi serangan.
   - Meningkatkan kesadaran pengguna terhadap kerentanan tersebut.
4. **Manajemen Pengungkapan Kerentanan (Vulnerability Disclosure Management)**
   ISO 27001:2022 juga menekankan pentingnya memiliki prosedur untuk mengelola pengungkapan kerentanan. Ini termasuk saluran formal bagi pihak internal dan eksternal (misalnya, peneliti keamanan) untuk melaporkan kelemahan keamanan. Pemberitahuan kerentanan yang diterima melalui saluran ini harus diproses dan ditangani sesuai dengan kebijakan yang ditetapkan.
5. **Pendekatan Berbasis Risiko**
   ISO 27001 secara keseluruhan didasarkan pada pendekatan berbasis risiko. Setiap "vulnerability alert" yang diterima harus diintegrasikan ke dalam proses penilaian risiko organisasi. Tidak semua kerentanan memiliki tingkat risiko yang sama, sehingga prioritas penanganannya harus didasarkan pada tingkat risiko yang ditimbulkan terhadap aset informasi.

Kepatuhan di Indonesia

Berbagai peraturan dan kebijakan keamanan siber di Indonesia secara implisit menuntut organisasi untuk memanfaatkan informasi pendukung seperti CVE dan OSV sebagai bagian dari praktik manajemen risiko dan kepatuhan.

Berikut adalah beberapa peraturan dan kerangka kerja di Indonesia yang secara tidak langsung memerlukan penggunaan informasi CVE dan OSV:

1. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).
   - UU PDP mewajibkan pengendali data dan prosesor data untuk menerapkan langkah-langkah keamanan yang memadai untuk melindungi data pribadi dari risiko keamanan, termasuk kebocoran, kehilangan, dan penyalahgunaan.

- Untuk memenuhi kewajiban ini, organisasi perlu mengidentifikasi dan memitigasi kerentanan pada sistem, aplikasi, dan infrastruktur yang memproses data pribadi. CVE dan OSV adalah sumber daya utama untuk mengidentifikasi kerentanan tersebut. Kegagalan dalam memitigasi kerentanan yang diketahui dapat dianggap sebagai kelalaian dalam menjaga keamanan data pribadi, yang berpotensi menimbulkan sanksi administratif atau pidana.

2. Peraturan Presiden
   - Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV).
   - Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

   Perpres ini mewajibkan penyelenggara IIV untuk menerapkan langkah-langkah pelindungan terhadap serangan siber dan insiden siber. Ini termasuk pengelolaan risiko kerentanan yang seringkali sangat kompleks dan melibatkan banyak sistem, termasuk open source. Penggunaan CVE dan OSV sangat penting untuk secara proaktif mengidentifikasi dan menambal kerentanan yang dapat membahayakan operasional IIV untuk keamanan siber nasional.
3. Peraturan Badan Siber dan Sandi Negara (BSSN)
   - Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber 20024-2028.
   - Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber.
   - Nomor 8 Tahun 2023 tentang Pelindungan Infrastruktur Informasi Vital (IIV)

   Panduan ini menekankan pentingnya identifikasi, penilaian, dan mitigasi kerentanan. CVE dan OSV adalah alat fundamental untuk melaksanakan rekomendasi tersebut.
4. Peraturan di Sektor Khusus (misalnya, Perbankan).
   - Peraturan Bank Indonesia (PBI)
     - Nomor 2 tahun 2024 tentang Keamanan SIstem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, Seta Pihak Lain yang Diatur dan Diawasi Bank Indonesia.
   - Otoritas Jasa Keuangan (OJK)
     - POJK Nomor 11 tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.
     - SEOJK Nomor 20 Tahun 2022 tentang Ketahanan dan Keamanan Siber Bagi Bank Umum.

   Lembaga keuangan diwajibkan untuk menerapkan sistem keamanan informasi yang kuat sebagai bagian dari kerangka manajemen risiko TI mereka. CVE dan OSV adalah alat standar industri untuk tujuan ini.

Green
OPEN

PENUTUP

Laporan ini memberikan gambaran yang jelas mengenai lanskap ancaman digital di Indonesia pada semester pertama tahun 2025. Penurunan signifikan dalam serangan siber yang terarah dan canggih, serta munculnya tren-tren baru yang mengkhawatirkan, menggarisbawahi perlunya tindakan segera dan terkoordinasi dari seluruh pemangku kepentingan. Pemahaman yang mendalam mengenai pola dan karakteristik serangan yang dipaparkan dalam laporan ini diharapkan dapat menjadi dasar bagi pengembangan strategi pertahanan siber yang lebih efektif.

Ancaman siber terus berkembang dan berevolusi, sehingga upaya untuk melindungi ruang digital Indonesia harus bersifat dinamis dan adaptif. Kolaborasi yang erat antara pemerintah, sektor swasta, akademisi, dan masyarakat sipil sangat penting dalam membangun ekosistem keamanan siber yang tangguh. Investasi dalam pengembangan sumber daya manusia di bidang keamanan siber, peningkatan kesadaran publik, dan penerapan teknologi keamanan yang inovatif merupakan langkah-langkah krusial yang harus diambil.

Pemerintah perlu memperkuat regulasi dan kebijakan keamanan siber, serta meningkatkan kapasitas lembaga-lembaga yang bertanggung jawab dalam penanganan insiden siber. Sektor swasta harus memprioritaskan keamanan siber dalam setiap aspek operasional mereka, dan mengadopsi kepatuhan dan praktik-praktik terbaik dalam pengelolaan risiko siber. Masyarakat perlu meningkatkan kesadaran mengenai ancaman siber dan mengambil langkah-langkah proaktif untuk melindungi diri mereka sendiri di ruang digital.

Dengan upaya bersama dan komitmen yang kuat, Indonesia dapat menghadapi tantangan keamanan siber dengan lebih percaya diri dan membangun masa depan digital yang aman, nyaman, dan produktif bagi seluruh masyarakat. Laporan ini diharapkan dapat menjadi kontribusi yang berharga dalam upaya tersebut, dan mendorong tindakan nyata untuk memperkuat pertahanan siber nasional.

Ancaman siber yang kian canggih mengharuskan organisasi untuk bertindak proaktif dalam melindungi sistem dan data. Seiring dengan evolusi serangan siber, pendekatan keamanan konvensional tidak lagi memadai. Diperlukan investasi pada teknologi keamanan siber mutakhir yang tidak hanya mampu mendeteksi, tetapi juga merespons ancaman secara efektif dan otomatis. Adopsi solusi canggih seperti SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), dan UEBA (User and Entity Behavior Analytics) menjadi krusial. Teknologi ini bekerja secara sinergis untuk memberikan visibilitas yang lebih baik terhadap aktivitas jaringan, mengotomatisasi respons terhadap insiden, serta mengidentifikasi anomali perilaku yang mungkin mengindikasikan adanya serangan, bahkan dari dalam sistem sekalipun.

Green
OPEN

Selain itu, pertahanan siber harus diperkuat dengan solusi threat intelligence yang terintegrasi, terutama yang memiliki fokus pada lanskap ancaman di Indonesia. Dengan menganalisis dan memantau serangan yang menargetkan wilayah spesifik, organisasi dapat mempersiapkan diri secara lebih baik terhadap Taktik, Teknik, dan Prosedur (TTP) yang umum digunakan oleh penyerang siber di Indonesia. Integrasi threat intelligence ini memungkinkan sistem keamanan untuk mendeteksi indikator kompromi (IoC) yang relevan, sehingga respons dapat dilakukan dengan lebih cepat dan terarah. Dengan kombinasi teknologi canggih dan data intelijen yang spesifik, organisasi dapat membangun postur keamanan yang lebih kuat dan tangguh dalam menghadapi serangan siber yang terus berkembang.