awanpintar.id
CLOUD SECURITY ENGINE

INDONESIA WASPADA

Laporan ancaman digital di Indonesia

SEMESTER 1

2023

Green
OPEN

Daftar Isi

Ringkasan Eksekutif

Ketegangan keamanan siber selalu menjadi topik yang menarik bagi para pakar keamanan, bisnis, dan masyarakat umum. Semester pertama tahun 2023 memberikan gambaran kritis tentang berbagai tantangan keamanan siber yang dihadapi organisasi dan individu di seluruh Indonesia.

Dalam Laporan Ancaman Digital Semester Pertama 2023, AwanPintar.id mengeksplorasi tren, statistik, dan peristiwa penting yang terjadi pada periode Januari sampai Juni 2023. Data pada laporan diharapkan dapat menjadi pertimbangan Profesional IT Security untuk mengantisipasi dan meminimalisir dampak kerugian pada organisasinya.

Beberapa isu penting yang disorot dalam laporan ini meliputi serangan malware yang semakin tertarget, serangan peretasan baru yang ditemukan, tindakan kejahatan siber yang terkoordinasi, dan kelemahan keamanan jaringan dan perangkat lunak yang masih rentan.

Melalui Laporan Ancaman Digital Semester Pertama 2023, kami berharap dapat meningkatkan kesadaran dan pemahaman tentang tantangan keamanan digital yang semakin meluas di tengah masyarakat. Dalam upaya untuk mendorong kolaborasi dan kerja sama, kita harus mengambil tindakan yang tepat untuk melindungi sistem dan data dari ancaman dan serangan yang semakin kompleks dan menguat.

Semoga kehadiran AwanPintar.id dapat membantu merealisasikan Kedaulatan Digital yang disampaikan Presiden Republik Indonesia, Bpk. Joko Widodo, karena data sangat tidak ternilai harganya.

Tentang

awanpintar.id

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

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

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

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

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

AwanPintar.id menyediakan sensor 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 dapat diakses di www.awanpintar.id.

Metodologi

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

1. Pengumpulan Data

AwanPintar.id menggunakan sejumlah sensor yang tersebar di jaringan internet Indonesia dan mengumpulkan seluruh data dari tiap sensornya untuk diolah menjadi BigData. Tiap sensor 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.

Sensor AwanPintar.id bersifat pasif dan mandiri, yang berarti sebagai sensor hanya menerima masukan yang berupa serangan dari seluruh dunia yang diarahkan ke tiap sensor secara spesifik. Sensor 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 sensor di jaringan internet Indonesia dilakukan untuk melakukan sampling dari banyak IP dari beragam AS Number agar mendapatkan distribusi data yang komprehensif.

2. Pemilihan Data

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

3. Analisis Data

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

Metode analisa deskriptif dan korelatif digunakan untuk mendapatkan pemahaman yang lebih detail dari setiap data yang disajikan. Sangat dimungkinkan tiap topik menggunakan metode yang berbeda mengikuti kebutuhannya. Penamaan nama kota dan negara didapat berdasarkan alamat IP yang terdeteksi.

4. Evaluasi Risiko

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

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

5. Visualisasi Data

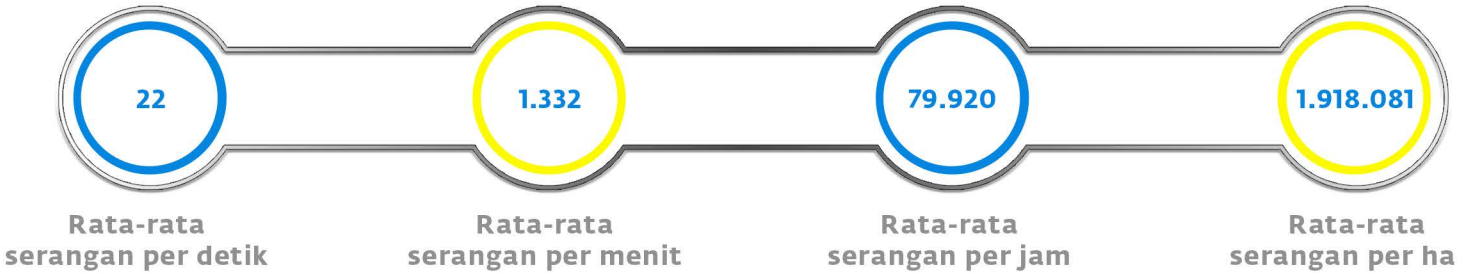
Untuk mempermudah membaca data yang ada, data keamanan siber diekstraksi dan disajikan dalam bentuk visualisasi data. Ini berguna untuk memperjelas informasi keamanan siber dan memudahkan pemahaman tentang sifat dan sumber serangan. Visualisasi data biasanya berupa grafik, diagram, atau peta.

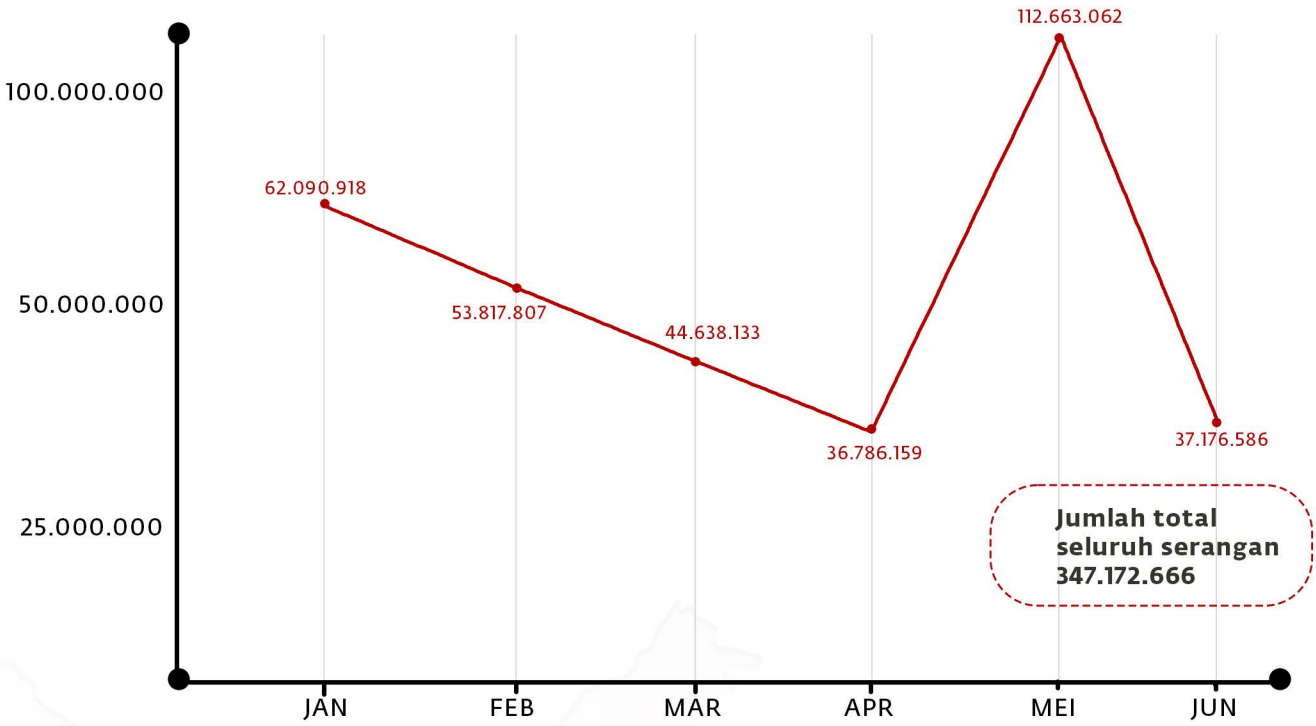
Skala dalam visualisasi mungkin saja disesuaikan untuk memberikan gambaran yang menarik saat melihat data yang disajikan tanpa mengurangi informasi yang diberikan.

Tren serangan terkini

AKUMULASI SERANGAN DIGITAL DI INDONESIA

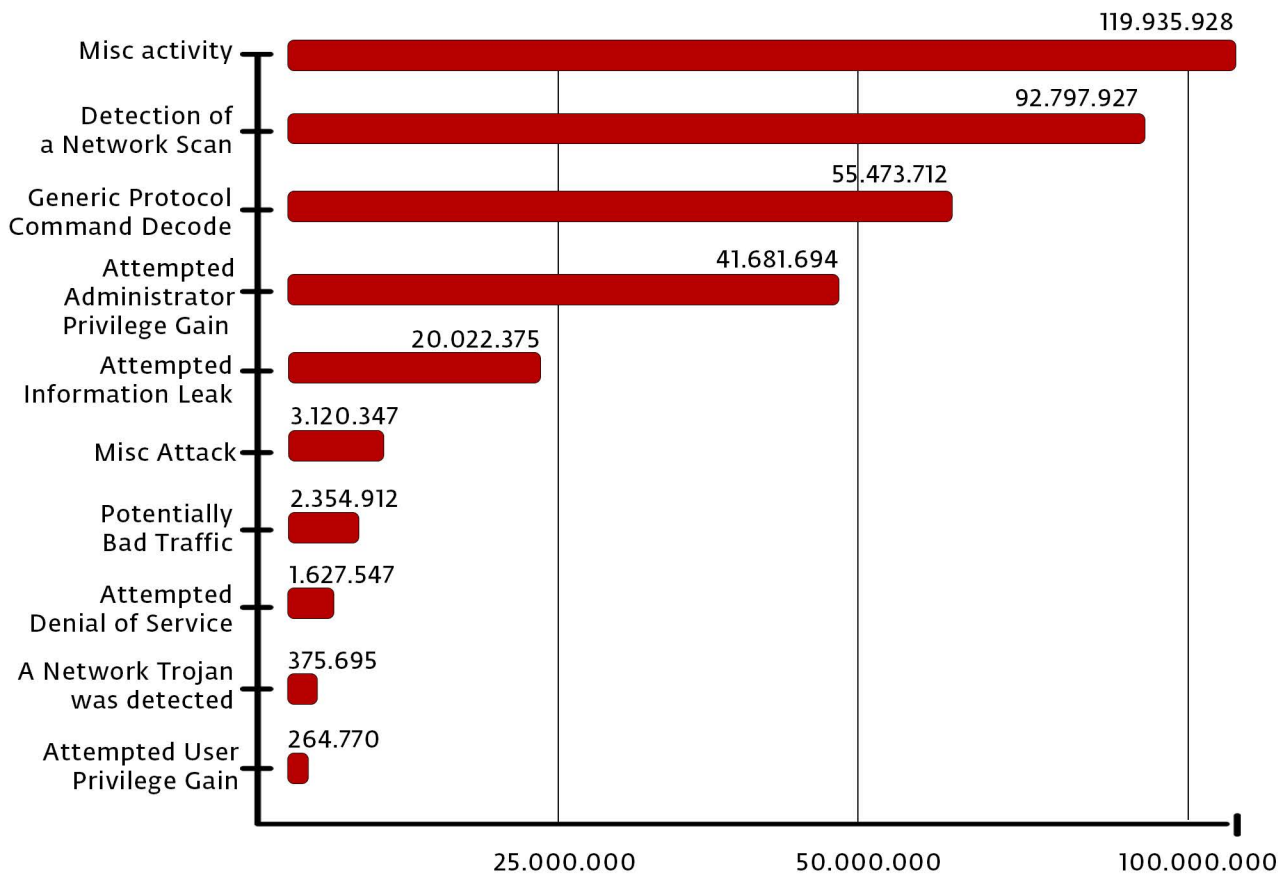
Berikut ini merupakan data yang diambil secara rata-rata pada sebuah sensor.





Total rata-rata serangan per sensor sepanjang paruh pertama tahun 2023 mencapai 347.172.666 serangan. Jumlah serangan tersebut mengalami fluktuasi setiap bulannya. Sejak memasuki bulan Januari sampai dengan April 2023 jumlah serangan siber yang masuk Indonesia terus mengalami penurunan yang cukup signifikan. Namun, di bulan Mei ancaman ini melesat jauh hingga mencapai 112.663.062. Lonjakan signifikan terjadi seiring dengan insiden ransomware LockBit yang menggegerkan Indonesia pada bulan tersebut.

10 Jenis serangan siber teratas



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.

Detection of a Network Scan

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

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.

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.

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.

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.

Attempted Denial of Service

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

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.

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 termasuk email phishing, drive by download, dan unduhan perangkat lunak dari sumber yang tidak tepercaya.

Attempted 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.

10 Negara kontributor serangan siber

Serangan siber saat ini menjadi ancaman besar bagi dunia digital, dan banyak negara yang berkontribusi dalam melakukan serangan tersebut. Berdasarkan hasil olah data dari AwanPintar.id. Negara-negara ini merupakan negara yang melakukan serangan siber yang lebih terprogram, berskala besar, dan terfokus.

451.527.897
BRASIL

150.630.838
IRAN

77.598.982
HONGKONG

70.816.348
KOREA SELATAN

43.740.243
PERANCIS

361.946.530
AMERIKA SERIKAT

109.223.074
TIONGKOK

75.616.566
BELANDA

55.621.858
JERMAN

38.880.881
SINGAPURA

Brasil, Amerika Serikat dan Tiongkok merupakan negara yang secara konsisten menjadi negara yang paling sering melakukan serangan siber terhadap Indonesia. Dari dalam negeri, ancaman yang datang juga tidak main-main, 38.572.455 serangan siber selama 6 bulan terakhir. Namun angka tersebut bukan berarti pelaku serangan dari negara itu. Pelaku bisa saja dari luar memanfaatkan IP negara tersebut dan melakukan serangan dengan aset yang mereka kuasai di Indonesia.

Dapat dikatakan asal penyerang merupakan IP yang lemah monitoring atau tingkat keamanannya sehingga dapat dimanfaatkan untuk melakukan penyerangan.

5 Daerah penyerang teratas di Indonesia

AwanPintar.id mencatat Indonesia masuk dalam peringkat 11 dari negara penyerang. Ini berarti alamat IP Indonesia digunakan secara aktif untuk melakukan serangan ke sesama server di Indonesia.

Daerah yang aktif melakukan serangan adalah:

Jakarta	11.283.243
Depok	2. 423.383
Tangerang	1.275.688
Bogor	911.036
Jatikramat	843.193

Lima daerah yang melakukan serangan siber terbanyak di Indonesia diperoleh dari hasil pemantauan sensor yang tersebar di seluruh Indonesia. Berdasarkan data di atas, terlihat bahwa daerah dengan persentase serangan terbanyak adalah Jakarta, sejumlah 11.283.243 juta kali serangan.

Dari lima daerah tersebut, didominasi oleh daerah-daerah di kisaran Jabodetabek, hal ini bisa diasumsikan karena Jabodetabek menurut Indeks Masyarakat Digital dari Kementerian Komunikasi dan Informatika (Kominfo) pada tahun 2022 masuk sebagai daerah dengan infrastruktur dan ekosistem digital terbaik nasional.

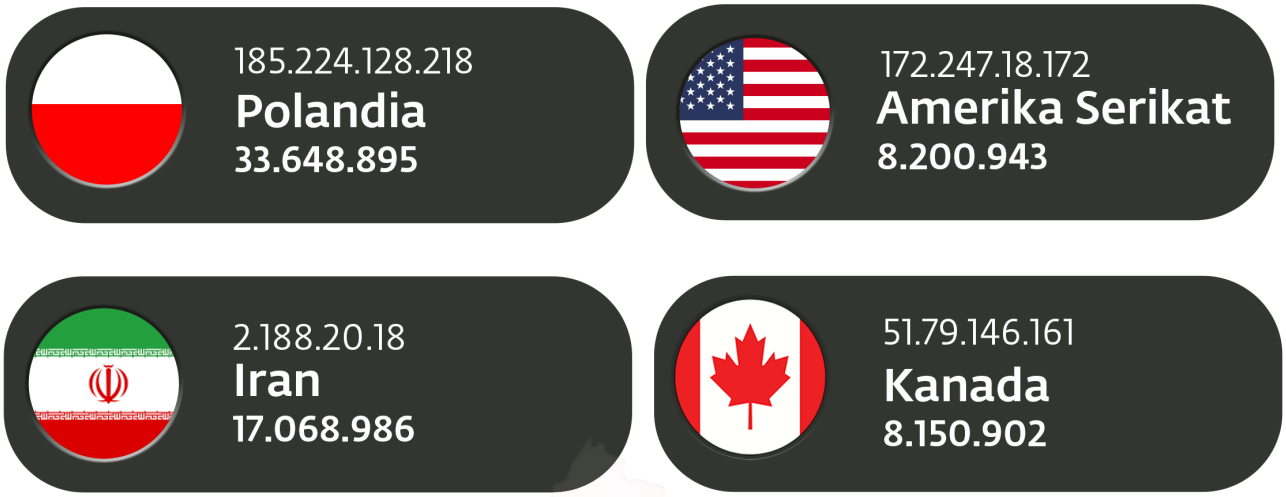
Serangan siber membutuhkan infrastruktur dan akses internet yang baik, daerah seperti Depok dengan 2.423.383 serangan, kemudian Tangerang di posisi ketiga dengan 1.275.688 ancaman merupakan daerah-daerah yang memiliki infrastruktur internet yang baik, begitu pula Bogor dengan 911.036 serangan dan Jatikramat yang merupakan bagian dari Bekasi dengan 843.193 serangan sibernya.

Kelima daerah tersebut berdasarkan agregasi data yang diperoleh AwanPintar.id selama enam bulan pertama di tahun 2023 sebagai daerah paling sering melakukan serangan domestik, meski sebagian dari serangan tersebut pemicunya bisa saja berasal dari negara luar.

10 IP penyerang teratas

Berdasarkan catatan log dari AwanPintar.id terdapat 10 IP address yang aktif melakukan serangan terhadap sistem jaringan di Indonesia. Hal ini menimbulkan potensi kerusakan dan keamanan yang serius bagi operasi bisnis. Berikut adalah sepuluh IP penyerang teratas yang terdeteksi.

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



173.29.67.198
Amerika Serikat
6.903.274

103.135.35.154
India
5.744.198

104.192.86.39
Amerika Serikat
6.230.423

23.231.151.191
Amerika Serikat
5.734.798

154.82.100.66
Tiongkok
6.093.438

23.224.129.146
Amerika Serikat
5.685.717

Ancaman pencurian kredensial

Penjahat dunia maya mencuri kredensial menggunakan berbagai teknik, taktik, dan prosedur. Data yang dikompromikan memiliki berbagai kegunaan dan memungkinkan penyerang untuk menembus perusahaan dan mencuri informasi sensitif.

Yang diperlukan hanyalah satu kredensial yang baik untuk mendapatkan akses ke infrastruktur perusahaan dan menyebabkan pelanggaran data yang berujung pada rusaknya reputasi dan kerugian finansial yang besar.

Untuk mendapatkan kredensial yang dibutuhkan sebagai vektor serangan, ada lima metode utama: Eksploitasi kredensial, kerentanan dan eksploitasi, kesalahan konfigurasi, malware serta sosial engineering. Metode tersebut juga digunakan dalam serangan siber yang dilakukan di Indonesia selama 6 bulan terakhir.

1. Administrator Privilege gain

• Backdoor DoublePulsar	38.894.349
• Bypass Autentikasi RDP	739.368
• FortiOS SSL VPN	562.188
• Eksploitasi Mikrotik Winbox	254.835
• Eksploitasi Kerentanan	121.044
• Serangan Buffer Overflow	75.703
• Brute Force Admin Login	23.937
• Eksploitasi Realtek eCos RSDK/MSDK	15.234

Backdoor DoublePulsar (Backdoor DoublePulsar installing communication)

Kredensial adalah barang berharga di dunia maya. Sehingga kredensial selalu menjadi komoditas utama bagi para peretas untuk diperoleh. Di Indonesia ancaman nomor satu terhadap kredensial berasal dari backdoor DoublePulsar.

Backdoor DoublePulsar digunakan untuk menyuntikkan dan menjalankan kode berbahaya pada sistem yang terinfeksi dan diinstal serta digunakan oleh EternalBlue. EternalBlue adalah eksploit SMBv1 (Server Message Block 1.0) yang dapat memicu RCE dan menyerang layanan berbagi file SMB.

Begitu dominannya serangan DoublePulsar menunjukkan masih banyak port SMB di tanah air yang masih terbuka sehingga menjadi incaran penjahat siber untuk melewati sistem keamanan PC dan mengakses sistem tanpa terdeteksi. Setelah mendapatkan akses ke sistem, penyerang dapat menanam malware, atau mencuri data pribadi penggunanya.

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

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

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

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

Penyerang lokal yang tidak diautentikasi dapat mengeksploitasi kerentanan ini untuk mendapatkan akses ke sesi RDP yang aman.

Network Level Authentication (NLA) digunakan untuk meningkatkan keamanan sesi RDP dengan meminta pengguna untuk mengautentikasi sebelum sesi dibuat. Di beberapa versi Windows, penanganan sesi RDP menggunakan NLA telah berubah.

Jika pemutusan RDP sementara dipicu, sesi akan mencoba menyambung kembali secara otomatis. Jika berhasil, sesi akan dipulihkan dalam keadaan tidak terkunci, terlepas dari keadaan yang tersisa sebelum pemutusan.

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

Eksploitasi Mikrotik Winbox (EXPLOIT Mikrotik Winbox RCE Attempt)

Perhatikan bahwa meskipun Winbox digunakan sebagai titik serangan, kerentanannya ada di RouterOS. Masalah ini kemudian diberi pengidentifikasi universal CVE-2018-14847.

Cara kerjanya: Kerentanan memungkinkan alat khusus untuk terhubung ke port Winbox, dan meminta file basis data pengguna sistem.

Versi yang Terpengaruh

- Mempengaruhi semua rilis perbaikan bug dari 6.30.1 hingga 6.40.7, diperbaiki pada 6.40.8 pada 23-Apr-2018
- Mempengaruhi semua rilis saat ini dari 6.29 hingga 6.42, diperbaiki pada 6.42.1 pada 23-Apr-2018
- Mempengaruhi semua rilis RC dari 6.29rc1 ke 6.43rc3, diperbaiki di 6.43rc4 pada 23-Apr-2018

Sebagai penyedia solusi murah untuk fungsi router, jumlah pengguna MikroTik di Indonesia sangat besar yaitu 199.381, dengan pengguna mikrotik Winbox sebesar 54.051, sumber: shodan.io.

Eksploitasi Kerentanan (EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read)

Validasi input yang tidak benar dalam komponen IPv6 saat menangani paket yang dikirim oleh penyerang jaringan. Kerentanan ini memungkinkan out-of-bounds Read dan kemungkinan Denial of Service.

Produk membaca data setelah akhir atau sebelum awal dari buffer yang dimaksud. Biasanya, ini memungkinkan penyerang membaca informasi sensitif dari lokasi memori lain atau menyebabkan kerusakan.

Serangan Buffer Overflow (GPL EXPLOIT ntpdx overflow attempt)

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

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

Brute Force Admin Login (POLICY FTP Frequent Admin Login Attempts)

Satu kemungkinan kerentanan untuk server adalah serangan kata sandi brute force melalui layanan FTP. Karena akun yang digunakan untuk FTP seringkali merupakan akun pengguna fisik pada sistem operasi host, secara teori dimungkinkan untuk menebak nama pengguna administratif setelah Anda menentukan jenis server FTP.

Setelah nama akun ditemukan, klien jahat dapat terhubung ke server dan mencoba serangan brute-force pada akun tersebut. Misalnya: "administrator" untuk sistem Windows atau "root" untuk sistem UNIX.

Eksploitasi Realtek eCos RSDK/MSDK (EXPLOIT Realtek eCos RSDK/MSDK Stack-based Buffer Overflow Attempt Inbound (CVE-2022-27255)

Pada eksploitasi Realtek pelaku ancaman cenderung mengeksploitasi kerentanan ini untuk mengeksekusi kode berbahaya pada perangkat, memodifikasi pengaturan, mencegat lalu lintas jaringan, dan memindai perangkat lain di jaringan lokal, beberapa di antaranya mungkin merupakan aset perusahaan.

Kerentanan ini juga dikenal sebagai CVE-2022-27255, yang tidak memerlukan autentikasi atau interaksi korban dan dapat mencapai eksekusi kode jarak jauh. Kerentanan tersebut pernah memengaruhi ratusan ribu, bahkan jutaan, perangkat yang menggunakan Software Development Kit (SDK) Realtek untuk eCos OS.

2. Information Leak

• INFO User-Agent (python-requests)	9.305.842
• POLICY CURL User Agent	4.114.891
• SCAN MS Terminal Server Traffic on Non-standard Port	3.938.883
• SCAN NMAP sS window 1024	1.017.778
• SCAN Potential VNC Scan 5900-5920	863.217
• FTP FTP PWD command attempt without login	133.992
• FTP FTP CWD command attempt without login	104.739
• SCAN Potential SSH Scan	31.549
• FTP FTP NLST command attempt without login	15.126

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

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

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

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

User Agent (POLICY CURL User Agent)

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

RDP Brute Force (SCAN MS Terminal Server Traffic on Non-standard Port)

Ini bisa menjadi tanda port dipindai dari dunia luar. Tidak jarang pemindaian port mencoba mengidentifikasi layanan apa yang tersedia di setiap port. Ini berarti ada sesuatu yang menguji port RDP non-standar untuk melihat apakah RDP berjalan.

Deteksi ini bisa jadi merupakan tanda serangan RDP Brute Force dari alamat IP yang tidak diinginkan.

SCAN NMAP -sS window 1024

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

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

Eksploitasi VNC (SCAN Potential VNC Scan 5900-5920)

VNC adalah singkatan dari Virtual Network Computing yang merupakan sistem berbagi desktop grafis yang digunakan untuk mengoperasikan perangkat lain dari jarak jauh. Ini berbagi pembaruan visual grafis sambil menyampaikan input mouse dan keyboard dari satu perangkat ke perangkat lainnya melalui internet.

Protokol Remote Frame Buffer digunakan oleh Virtual Network Computing. VNC umumnya digunakan di dunia komputasi, dan aktor jahat telah menemukan banyak cara untuk mengeksploitasi kerentanan yang menyertai VNC. Mengekspos VNC ke internet telah lama dianggap sebagai risiko keamanan. Di Indonesia port ini rutin mendapat ancaman setiap bulannya.

Brute Force SSH

(SCAN Potential SSH Scan)

SSH adalah salah satu protokol yang paling umum digunakan dalam infrastruktur teknologi informasi modern. Dan karenanya, dapat menjadi vektor serangan yang berharga bagi peretas. Salah satu cara paling andal untuk mendapatkan akses SSH ke server adalah dengan brute force kredensial.

Comment Attempt without login

FTP tidak dibangun untuk keamanan. Ini umumnya dianggap sebagai protokol yang tidak aman karena bergantung pada nama pengguna dan kata sandi teks-jelas untuk otentikasi dan tidak menggunakan enkripsi. Data yang dikirim melalui FTP rentan terhadap serangan sniffing, spoofing, dan brute force, di antara metode serangan dasar lainnya.

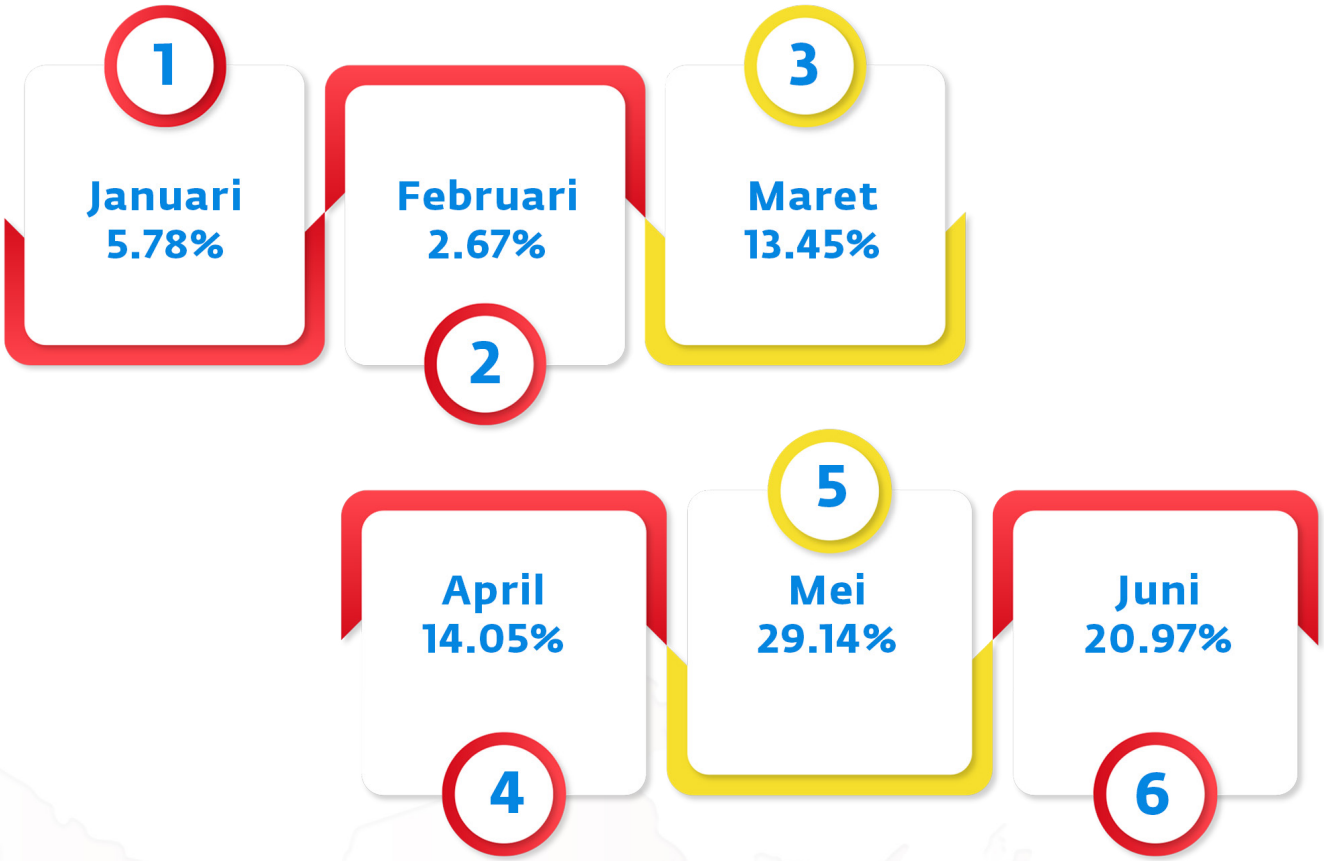
Spam & Malware

Meskipun internet dan email membawa berbagai manfaat, mereka juga menimbulkan sejumlah potensi ancaman keamanan. Email merupakan cara paling mudah dan murahuntuk mengawali suatu serangan siber sehingga sering digunakan penjahat dunia maya dalam aktivitas peretasan.

Beberapa ancaman keamanan email yang paling umum salah satunya spam dan malware, keduanya bisa menjadi kombinasi serangan mematikan. Spam adalah junk email yang merupakan penyalahgunaan sistem pesan elektronik untuk mengirim berbagai hal secara massal.

Spam email sering dimanfaatkan untuk menyebarluaskan malware dengan cara disusupkan secara rahasia dalam lampiran yang disertakannya, yang dapat membahayakan perangkat pengguna. Berikut adalah data spam dan malware yang dikompilasi oleh AwanPintar.id.

Persentase Jumlah SPAM & Malware terhadap total email masuk



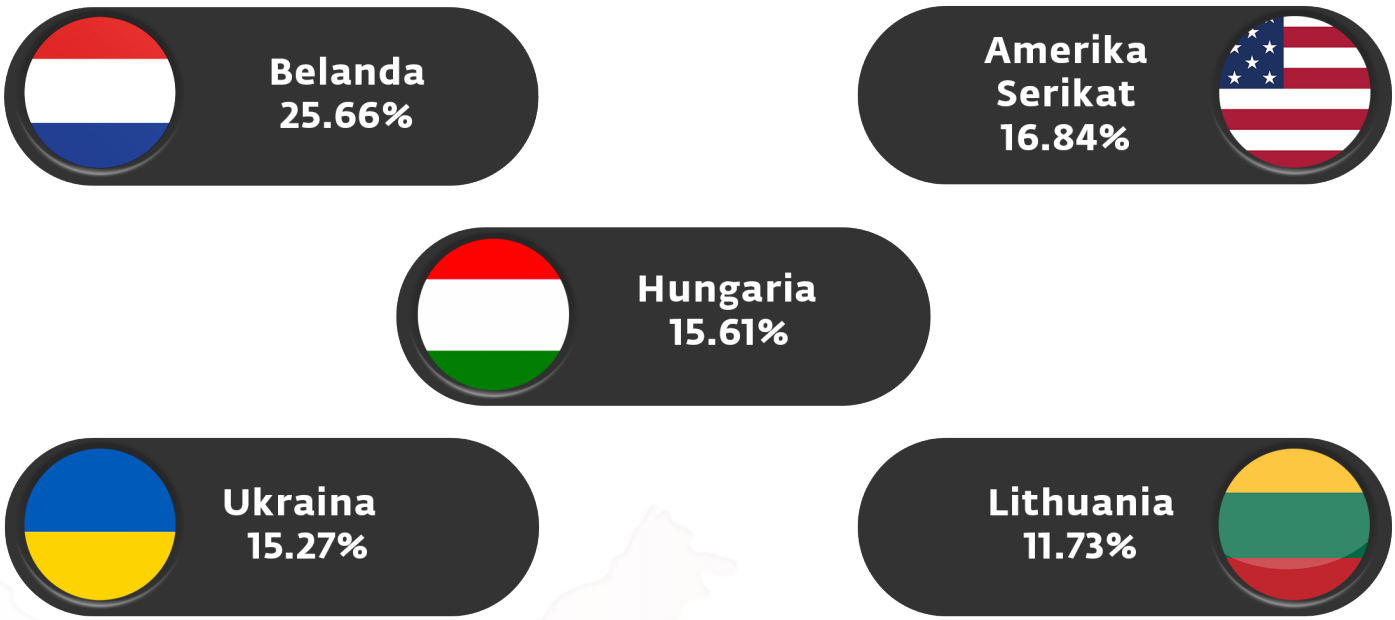
Secara umum serangan spam malware di awal tahun cenderung fluktuatif, namun seiring waktu berjalan ancaman tersebut semakin meningkat. Lonjakan persentasenya bisa hingga beberapa kali lipat dan mencapai puncaknya di bulan Mei.

Bulan Mei ditandai sebagai bulan terburuk dalam semester pertama keamanan siber di Indonesia, karena di bulan ini ransomware LockBit sedang naik daun di tanah air seiring dengan munculnya kasus yang ada dan pemberitaan yang masif. Email sendiri merupakan sarana paling mudah untuk mengirimkan ransomware, cara paling sederhana namun mematikan.

Pada bulan akhir semester pertama persentase spam dan malware di Indonesia memang terjadi penurunan sekitar 9 persen, meski demikian secara keseluruhan masih menduduki posisi kedua sebagai serangan email terbesar.

Yang perlu menjadi sorotan lainnya adalah Business Email Compromise (BEC) salah satu kejahatan lain yang sering dilancarkan melalui email. Meskipun beberapa serangan BEC melibatkan penggunaan malware, banyak yang mengandalkan teknik manipulasi psikologis, di mana antivirus, filter spam, atau daftar putih email tidak efektif.

5 Negara Pengirim Malware

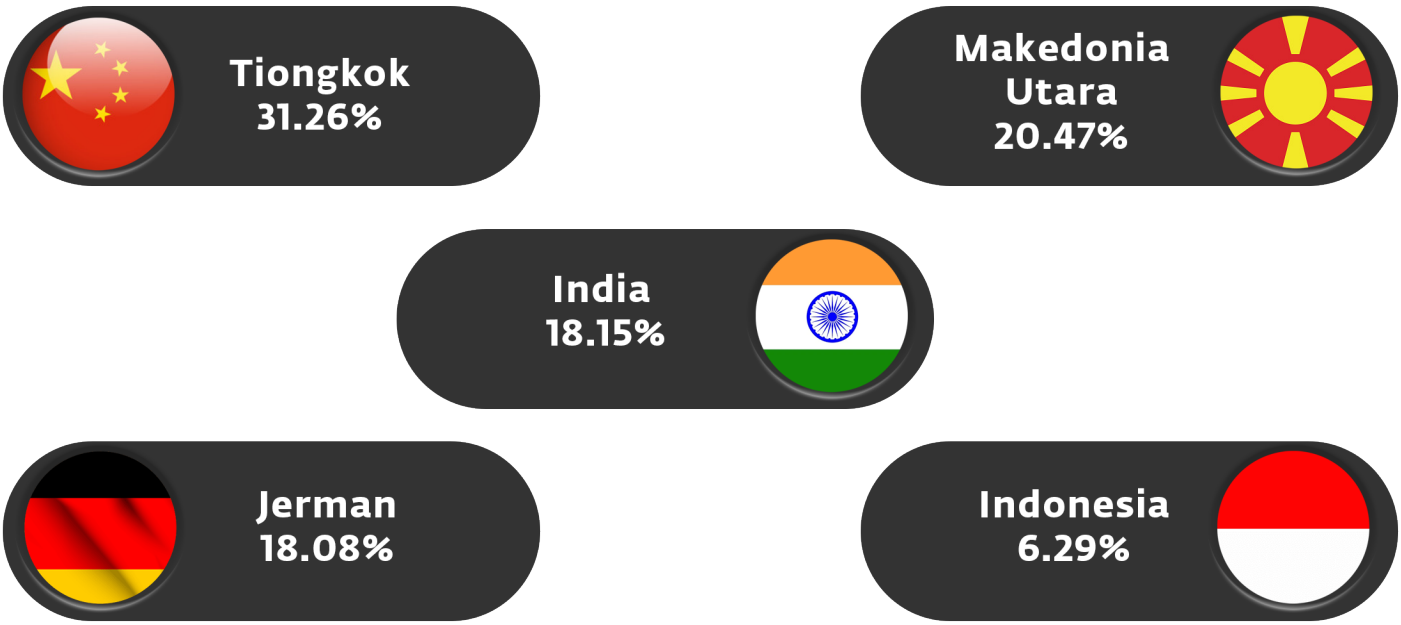


Dalam serangan melalui email, malware menjadi komoditas utamanya, malware memiliki banyak varian seperti ransomware, adware, spyware dan banyak lagi. Dan yang paling berbahaya dari varian-varian malware adalah ransomware dan spyware.

Secara keseluruhan ancaman digital yang masuk di paruh pertama tahun ini, Amerika Serikat dan Belanda masuk dalam 10 negara kontributor serangan siber terbesar di Indonesia. Sehingga tidak lagi menjadi kejutan jika kemudian keduanya mencuat sebagai negara pengirim malware terbanyak.

Yang menjadi perhatian adalah empat negara lainnya yang berasal dari benua Eropa seperti Belanda, Hungaria, Ukraina dan Lithuania yang tidak memiliki rekam jejak signifikan dalam serangan digital ke Indonesia mampu menjadi 5 besar penyumbang malware terbanyak.

5 Negara Pengirim SPAM Terbanyak



Email spam selalu menjadi pandemi ancaman digital di belahan dunia mana pun, penjahat digital mana yang tidak tergoda melancarkan serangan secara masif minim biaya namun efektif dan efisien dalam meraih hasil.

Yang paling umum dalam spam email adalah phising, kejahatan digital yang menargetkan informasi atau data sensitif korban melalui email, unggahan media sosial, atau pesan teks.

Pelaku phising biasanya menampakkan diri sebagai pihak atau institusi yang berwenang. Mereka menyisipkan tautan di dalam narasi yang disebarkan, dan menggiring korban agar mengeklik tautan tersebut (link phising).

Data yang menjadi sasaran phising adalah data pribadi (nama, usia, alamat), data akun (username dan password), dan data finansial (informasi kartu kredit atau rekening bank).

Dari olah data yang diperoleh AwanPintar.id, pada serangan spam email terbanyak ada beberapa hal menarik, selain Tiongkok sebagai salah satu negara kontributor serangan terbesar di indonesia, empat negara lainnya tidak termasuk di dalamnya.

Yang menjadi sorotan tentu saja Indonesia, yang berada di posisi kelima sebagai negara paling banyak melakukan serangan melalui spam email. Serangan domestik seperti ini bisa saja melalui akun-akun yang disusupi atau server yang sudah dikuasai dari luar Indonesia.

Port favorit peretas

Port dapat didefinisikan sebagai saluran komunikasi antara dua perangkat dalam jaringan komputer. Port terbuka yang tidak diinginkan dapat menjadi tidak aman untuk jaringan.

Port terbuka dapat memberikan akses pelaku ancaman ke lingkungan teknologi informasi (TI) jika tidak cukup dilindungi atau dikonfigurasi dengan benar. Contoh kasus: pada tahun 2017, penjahat dunia maya mengeksploitasi port 445 untuk menyebarkan ransomware WannaCry.

- Port 53 DNS 292.769.669
- Port 445 SMB 19.364.539
- Port 1900 SSDP 18.535.283
- Port 5900 VNC 8.199.265
- Port 5060 SIP 2.890.105
- Port 22 SSH 1.727.581
- Port 110 1.291.843
- Port 3389 (RDP) 739.812
- Port 25565 (Minecraft) 419.495
- Port 21 (FTP) 337.087

10 Port paling rentan di Indonesia

Di zaman meningkatnya jumlah serangan siber, port jaringan terbuka patut diperhatikan karena sangat rentan untuk dieksploitasi oleh peretas. Dan melalui olah data yang diperoleh dari seluruh Indonesia ada begitu banyak ancaman yang masuk melalui port.

1. Port 53 DNS (Domain Name Sistem)

Port 53 digunakan oleh Domain Name System (DNS), sebuah layanan yang mengubah nama yang dapat dibaca manusia seperti Prosperita.com menjadi alamat IP yang dimengerti oleh komputer. Karena port 53 biasanya terbuka, program jahat sering masuk melaluinya.

Kerentanan dalam DNS Bypass Firewall Rules adalah kerentanan berisiko yang merupakan salah satu yang paling sering ditemukan di jaringan di seluruh dunia. Masalah ini telah ada setidaknya sejak tahun 1990 tetapi telah terbukti sulit untuk dideteksi.

Satu eksploitasi umum yang menggunakan port DNS adalah Denial Distributed of Service (DDoS). Namun yang paling berbahaya adalah ancaman DNS Hijacking, yang membajak DNS korban dan mengarahkan ke server yang berbahaya.

2. Port 445 SMB

Port 445 adalah port jaringan tradisional Microsoft yang terkait dengan layanan NetBIOS asli yang ditemukan di versi OS Windows sebelumnya. Saat ini, port 445 digunakan oleh Microsoft Directory Services untuk Active Directory (AD) dan untuk protokol Server Message Block (SMB) melalui TCP/IP. SMB adalah protokol komunikasi yang dibuat oleh Microsoft untuk menyediakan akses berbagi file dan printer di seluruh jaringan.

Agar berbagi sumber daya dan komunikasi berfungsi, port harus terbuka dan dapat diakses. Ini berarti mereka terbuka untuk berbagi sumber daya yang sah tetapi juga menjadi target terbuka dan selalu siap untuk penyerang. Dan yang perlu menjadi perhatian dari kerentanan SMB adalah kerentanan Wannacry yang berjalan di EternalBlue.

3. Port 1900 SSDP

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

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

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

4. Port 5900 VNC

VNC singkatan dari “Virtual Network Computing”. 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.

Melihat fungsionalitasnya, tidak mengherankan jika port ini mendapat serangan dalam jumlah besar selama semester pertama tahun 2023 dan terlihat jelas penjahat siber ingin mendapatkan ikan besar dalam sekali kail dengan membombardir port ini.

5. Port 5060 SIP

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

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

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

6. Port 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 diotentikasi 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.

7. Port 110

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

Pop3 "post office protocol" digunakan oleh klien email untuk pengambilan email mereka dari server "kantor pos" email yang ditunjuk. Klien Email seperti Microsoft Outlook, Netscape, Eudora, dan banyak lainnya, terhubung ke port 110 dari server email jarak jauh, kemudian menggunakan protokol pop3 untuk mengambil email mereka.

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

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

8. Port 3389 RDP

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

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

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

9. Port 25565 Minecraft

Port khusus yang biasanya digunakan untuk menghubungkan game Minecraft ke internet, sehingga pemain dapat bermain dalam mode multiplayer dengan pemain lain dari seluruh dunia. Untuk memungkinkan akses ke server Minecraft dari luar jaringan, maka diperlukan konfigurasi port forwarding pada router atau firewall yang digunakan.

Port forwarding juga dikenal sebagai manajemen port, memungkinkan server dan perangkat jarak jauh di internet dapat mengakses perangkat yang ada di jaringan pribadi. Peretas yang masuk melalui celah port ini dapat mempengaruhi banyak perangkat para pemain Minecraft untuk tujuan DDoS.

10. Port 21 FTP

Port 21 umumnya dikaitkan dengan FTP. FTP telah ditetapkan ke Port 21 oleh Internet Assigned Numbers Authority (IANA). IANA juga mengawasi alokasi alamat IP global.

FTP sering dianggap sebagai protokol transfer file yang "tidak aman". Ini terutama karena FTP mengirim data dalam teks yang jelas dan menawarkan opsi anonim tanpa memerlukan kata sandi. FTP adalah protokol standar, yang berarti bahwa banyak sistem mengaktifkannya secara default.

Pelaku dapat mengeksploitasi port ini untuk mendapatkan akses tidak sah ke file, kredensial, dan informasi lain yang melewati FTP ditransmisikan dalam teks jelas tanpa enkripsi.

Mitigasi Kerentanan

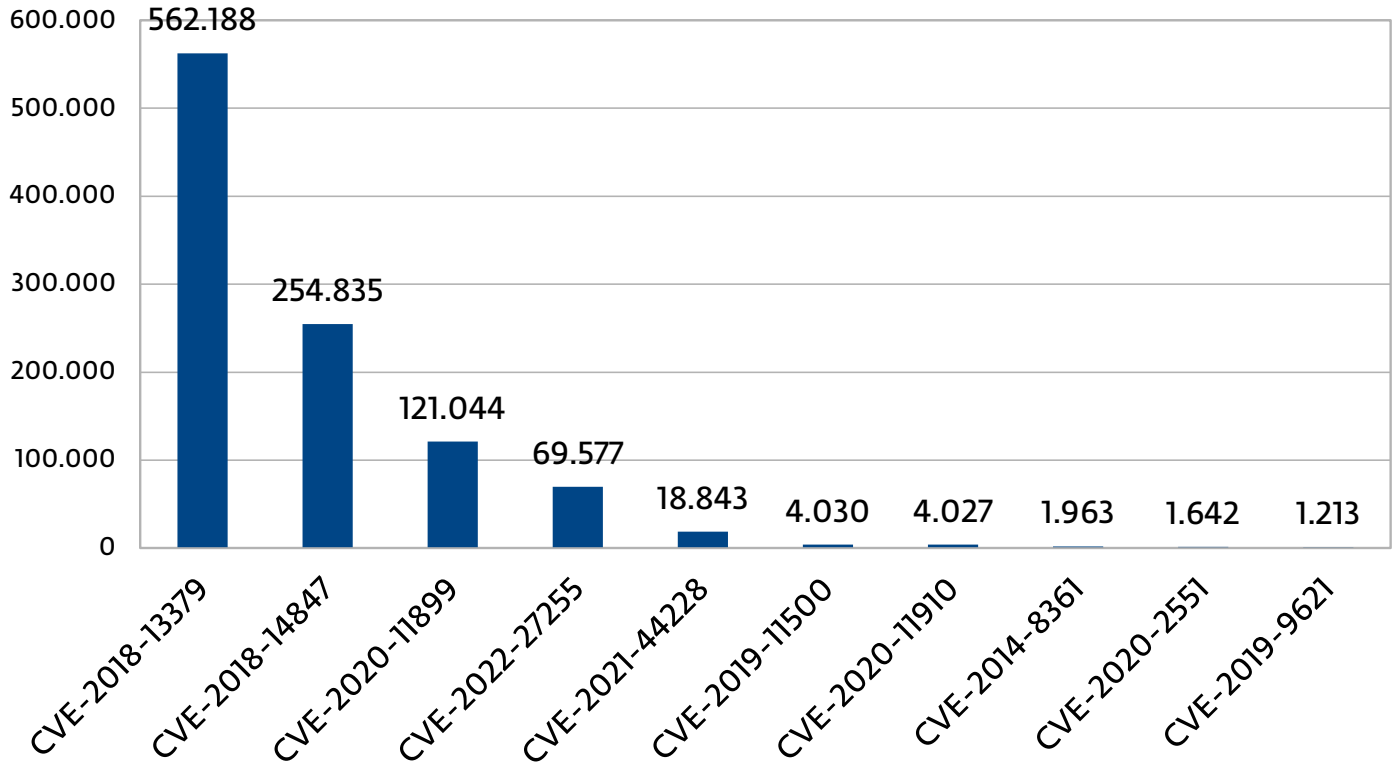
Port komputer adalah komponen penting dalam pemrograman aplikasi dan jaringan karena menyediakan titik dok sentral untuk bertukar informasi antara dua entitas. Firewall yang tepat memastikan bahwa port tidak terbuka untuk serangan oleh penjahat dunia maya.

Firewall juga mencegah akses tidak sah ke jaringan komputer, sehingga mencegah serangan dunia maya seperti terjadinya serangan terhadap port yang terbuka. Oleh karena itu, port dibuka untuk interval waktu terbatas dan setelah itu port ditutup sambil tetap memeriksa dengan pemantauan konstan terhadap port perangkat komputer.

10 Kerentanan tertinggi

Di dunia digital saat ini, serangan siber menjadi semakin umum dan canggih. Penjahat siber menggunakan berbagai teknik untuk mengeksploitasi kerentanan dalam sistem komputer, jaringan, dan aplikasi. Common Vulnerabilities and Exposures atau CVE memainkan peran penting dalam mengidentifikasi dan memitigasi kerentanan ini.

Dalam operasi AwanPintar.id menjaring aktivitas lalu lintas jaringan yang masuk ke Indonesia ditemukan 10 kerentanan tertinggi datang melalui Common Vulnerability and Exposures (CVE) yang dapat memengaruhi pengguna di seluruh Indonesia.



CVE-2018-13379

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

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

Sistem yang terdampak:

- FortiOS versi 5.4.12 hingga 5.6.0
- FortiOS versi 5.6.3 hingga 5.6.7
- FortiOS versi 6.0.0 hingga 6.0.4
- FortiProxy versi 1.0.0 hingga 1.0.7
- FortiProxy versi 1.1.0 hingga 1.1.6
- FortiProxy versi 1.2.0 hingga 1.2.8

FortiProxy versi 2.0.0 yang menggunakan SSL-VPN

CVE Numbering Authority (CNA): 9.1 (critical)

Mitigasi Kerentanan

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

CVE-2018-14847

Perhatikan bahwa meskipun Winbox digunakan sebagai titik serangan, kerentanannya ada di RouterOS. Masalah ini kemudian diberi pengidentifikasi universal CVE-2018-14847.

Cara kerjanya: Kerentanan memungkinkan alat khusus untuk terhubung ke port Winbox, dan meminta file basis data pengguna sistem.

Versi yang terpengaruh

- Mempengaruhi semua rilis perbaikan bug dari 6.30.1 hingga 6.40.7, diperbaiki pada 6.40.8 pada 23-Apr-2018
- Mempengaruhi semua rilis saat ini dari 6.29 hingga 6.42, diperbaiki pada 6.42.1 pada 23-Apr-2018
- Mempengaruhi semua rilis RC dari 6.29rc1 ke 6.43rc3, diperbaiki di 6.43rc4 pada 23-Apr-2018

Sebagai penyedia solusi murah untuk fungsi router, jumlah pengguna MikroTik di Indonesia sangat besar yaitu 198.533, sementara khusus pengguna mikrotik Winbox adalah 54.000, sumber: Shodan.io.

CVE-2020-11899

Kerentanan ini diketahui pada 16 Juni 2020. Kerentanan dikenal sebagai adanya Tumpukan Treck TCP/IP sebelum 6.0.1.66 memiliki IPv6 Out-of-bounds Read.

Out of bounds read adalah jenis kesalahan perangkat lunak yang dapat terjadi saat membaca data dari memori. Pembacaan di luar batas dapat menyebabkan crash atau kerentanan tak terduga lainnya, dan memungkinkan penyerang membaca informasi sensitif yang seharusnya tidak dapat mereka akses.

Kerentanan tersebut secara kolektif dikenal sebagai Ripple20. Eksploitasi kerentanan ini dapat mengakibatkan eksekusi kode jarak jauh, penolakan layanan (DoS), atau pengungkapan informasi, bergantung pada kerentanan tertentu.

Dampak

Dampak dari kerentanan ini akan bervariasi karena kombinasi opsi build dan runtime yang digunakan saat mengembangkan sistem tertanam yang berbeda. Keanekaragaman implementasi dan kurangnya visibilitas rantai pasokan telah memperparah masalah dalam menilai secara akurat dampak dari kerentanan ini. Singkatnya, penyerang jarak jauh yang tidak diautentikasi mungkin dapat menggunakan paket jaringan yang dibuat khusus untuk menyebabkan penolakan layanan, mengungkapkan informasi, atau mengeksekusi kode arbitrer.

Produk yang terdampak

Banyak vendor di seluruh dunia terpengaruh oleh kerentanan yang berasal dari CVE-2020-11899 seperti di antaranya adalah Caterpillar, Cisco, Dell, HP, Intel dan masih banyak lagi. Namun vendor-vendor tersebut juga sudah merilis pembaruan atau patching untuk produk mereka yang terpengaruh.

Mitigasi Kerentanan

Perbarui ke versi stabil terbaru dari perangkat lunak tumpukan IP Treck (6.0.1.67 atau lebih baru).

Pertimbangkan memblokir serangan jaringan melalui inspeksi paket mendalam. Dalam beberapa kasus, switch, router, dan firewall modern akan menjatuhkan paket yang cacat tanpa konfigurasi tambahan. Disarankan agar fitur keamanan tersebut tidak dinonaktifkan. Di bawah ini adalah daftar kemungkinan mitigasi yang dapat diterapkan sesuai dengan lingkungan jaringan Anda.

- Normalisasikan atau tolak paket terfragmentasi IP (IP Fragments) jika tidak didukung di lingkungan Anda
- Nonaktifkan atau blokir tunneling IP, baik tunneling IPv6-in-IPv4 atau IP-in-IP jika tidak diperlukan
- Blokir perutean sumber IP dan semua fitur IPv6 yang tidak digunakan lagi seperti header perutean (lihat juga VU#267289)
- Terapkan pemeriksaan TCP dan tolak paket TCP yang cacat
- Blokir pesan kontrol ICMP yang tidak digunakan seperti MTU Update dan Address Mask update
- Normalisasikan DNS melalui server rekursif yang aman atau firewall lapisan aplikasi
- Pastikan Anda menggunakan peralatan OSI layer 2 (Ethernet) yang andal
- Berikan keamanan DHCP/DHCPv6 dengan fitur seperti pengintaian DHCP
- Nonaktifkan atau blokir multicast IPv6 jika tidak digunakan dalam infrastruktur switching

CVE-2022-27255

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

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

Dampak

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

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

Produk yang terdampak

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

CVE Numbering Authority (CNA): 8.5 (High)

Mitigasi Kerentanan

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

Secara khusus, perusahaan harus:

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

CVE-2021-44228

CVE-2021-44228 adalah kerentanan eksekusi kode jarak jauh yang memengaruhi banyak versi library Apache Log4j. Kerentanan ini sangat kritis karena CVE-2021-44228 memungkinkan pelaku ancaman untuk mengambil kendali penuh atas server tanpa memerlukan otentikasi apa pun. Dalam hal tingkat keparahan, Log4Shell diberi peringkat 10 dari 10 tingkat kerentanan.

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

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

Dampak

Beberapa pengguna mungkin khawatir bahwa Log4j versi 1.x dipengaruhi oleh kerentanan. Untungnya, tidak demikian karena penyebaran Log4J ini tidak menawarkan mekanisme pencarian JNDI di tingkat pesan.

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

Produk terdampak

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

Mitigasi Kerentanan

Intinya dengan mengikuti saran mitigasi yang diberikan oleh Apache:

- Identifikasi aplikasi yang menggunakan dependensi log4j di bawah 2.15.0 (seperti di atas).
- Tingkatkan dependensi log4j ke setidaknya versi 2.17.0(2.15.0 dan 2.16.0 telah mengetahui kerentanan Denial of Service [DoS], dikutip dalam CVE-2021-45046 dan CVE-2021-45105, jadi rekomendasi dari Apache adalah menggunakan 2.17.0 dan yang lebih baru.).

CVE-2019-11500

CVE-2019-11500 dipublikasikan pada 28 Agustus 2019. Cacat ditemukan di dovecot. Pengurai protokol IMAP dan ManageSieve tidak menangani byte NULL dengan benar pada sistem operasi Linux Red Hat.

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

Dampak

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

Produk yang terdampak

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

Mitigasi Kerentanan

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

CVE-2020-11910

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

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

Dampak

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

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

Produk terdampak

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

Mitigasi Kerentanan

Vendor perangkat akan memiliki pendekatan yang berbeda dari operator jaringan. Secara umum, kami merekomendasikan langkah-langkah berikut:

- Semua organisasi harus melakukan penilaian risiko yang komprehensif sebelum menerapkan tindakan defensif.
- Pertama-tama terapkan tindakan defensif dalam mode "Alert" pasif.

Mitigasi untuk vendor perangkat:

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

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

Mitigasi bagi operator dan jaringan:
(berdasarkan penasehat CERT/CC dan CISA ICS-CERT)

- Mitigasi pertama dan terbaik adalah memperbarui ke versi yang ditambal dari semua perangkat.
- Jika perangkat tidak dapat diperbarui, langkah-langkah berikut disarankan:
  1. Minimalkan eksposur jaringan untuk perangkat tertanam dan kritis, pertahankan eksposur seminimal mungkin, dan pastikan bahwa perangkat tidak dapat diakses dari Internet kecuali benar-benar penting.
  2. Pisahkan jaringan dan perangkat OT di belakang firewall dan isolasi dari jaringan bisnis.
  3. Aktifkan hanya metode akses jarak jauh yang aman.
  4. Blokir lalu lintas IP anomali.
  5. Blokir serangan jaringan melalui inspeksi paket menda lam, untuk mengurangi risiko pada perangkat Anda yang mendukung TCP/IP tersemat Treck.

CVE-2014-8361

Kerentanan ini diidentifikasi pada 20 Oktober 2014, ditemukan di Realtek SDK, dan telah diklasifikasikan kritis. Ini memengaruhi beberapa pemrosesan yang tidak diketahui dari Layanan SOAP komponen miniigd. Manipulasi sebagai bagian dari Permintaan NewInternalClient mengarah ke kerentanan validasi masukan.

Dampak

Layanan SOAP miniigd di Realtek SDK memungkinkan penyerang jarak jauh untuk mengeksekusi kode arbitrer melalui permintaan NewInternalClient yang dibuat. Signature ini mendeteksi upaya untuk mengeksploitasi kerentanan eksekusi kode jarak jauh di Realtek rtl81xx SDK.

Realtek rtl81xx SDK rentan terhadap kerentanan eksekusi kode jarak jauh karena gagal membersihkan data yang diberikan pengguna dengan benar saat menangani permintaan NewInternalClient. Secara khusus, masalah ini memengaruhi layanan SOAP 'miniigd'. Penyerang dapat mengeksploitasi masalah ini untuk mengeksekusi kode arbitrer dengan hak akses root.

Penyerang dapat mengeksploitasi masalah ini untuk mengeksekusi kode arbitrer dalam konteks aplikasi yang terpengaruh. Upaya eksploitasi yang gagal akan menghasilkan kondisi denial-of-service.

Produk terdampak

Ini menunjukkan upaya serangan untuk mengeksploitasi kerentanan Eksekusi Perintah di beberapa router D-Link. Kerentanan disebabkan oleh kesalahan yang terjadi saat perangkat lunak yang rentan menangani file SOAP/XML berbahaya.

D-Link DIR-501 miniigd v1.08 dan sebelumnya
D-Link DIR-515 miniigd v1.08 dan sebelumnya
D-Link DIR-600L miniigd v1.08 dan sebelumnya
D-Link DIR-605L miniigd v1.08 dan sebelumnya
D-Link DIR-615 miniigd v1.08 dan sebelumnya
D-Link DIR-619L miniigd v1.08 dan sebelumnya
D-Link DIR-809 miniigd v1.07 dan sebelumnya
D-Link DIR-900L miniigd v1.08 dan sebelumnya
D-Link DIR-905L miniigd v1.08 dan sebelumnya
Trendnet TEW-731BR miniigd v1.08 dan sebelumnya

Mitigasi Kerentanan

Disarankan untuk mengganti objek yang terpengaruh dengan produk alternatif. Selain itu, dimungkinkan untuk mendeteksi dan mencegah serangan semacam ini dengan solusi keamanan yang komprehensif.

CVE-2020-2551

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

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

Dampak

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

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

Produk terdampak

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

CVE Numbering Authority (CNA): 9.8 (Critical)

Mitigasi Kerentanan

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

CVE-2019-9621

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

Dampak

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

Produk terdampak

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

CVE Numbering Authority (CNA): 7.5

Mitigasi Kerentanan

Untuk mengamankan versi Zimbra yang didukung (8.7 dan 8.8)

- Pengguna Zimbra yang menjalankan versi 8.8 harus meningkatkan ke 8.8.10 Patch 7 atau 8.8.11 Patch 3
- Pengguna Zimbra yang menjalankan versi dukungan jangka panjang (LTS) 8.7.11 harus meningkatkan ke 8.7.11 Patch 10

Untuk mengamankan versi Zimbra yang tidak didukung (8.6 dan sebelumnya)

- Pengguna yang menjalankan 8.6 harus meningkat kan ke Patch 13.
- Zimbra versi lama rentan hingga ditingkatkan ke versi yang didukung.

PENUTUP

Dalam semester pertama tahun 2023, aktivitas serangan siber cenderung menurun, kecuali anomali yang terjadi di bulan Mei dengan jumlah serangan siber yang yang jauh lebih besar dari bulan lainnya. Seiring dengan penggunaan teknologi yang semakin berkembang dan luas diadopsi oleh masyarakat. Berbagai metode serangan siber, seperti ransomware, phising, dan cryptojacking terus berkembang dan semakin sulit dideteksi oleh sistem keamanan.

Pada semester pertama tahun 2023, terdapat beberapa ancaman siber yang cukup signifikan, seperti serangan DDoS, hacking, dan exploit pada aplikasi atau sistem yang rentan. Selain itu, sering ditemui para pelaku serangan menyamarkan dirinya atau menyembunyikan identitas dan melakukan serangan secara terorganisir terhadap lalu lintas jaringan.

Oleh karena itu, perusahaan harus meningkatkan sistem keamanan mereka dengan mengimplementasikan teknologi keamanan terbaru dan melatih karyawan dalam mengidentifikasi dan merespons ancaman siber. Selain itu, perusahaan juga harus memperbarui sistem keamanan mereka secara teratur, melakukan pemantauan lalu lintas jaringan, dan melakukan analisis terhadap aktivitas yang mencurigakan untuk memastikan keamanan dan keutuhan sistem mereka.

Kesadaran dan tindakan proaktif dalam mengatasi ancaman siber merupakan kunci untuk mengurangi risiko kerugian akibat dari serangan siber. Dengan adanya kerjasama antara perusahaan dan pemerintah dalam meningkatkan keamanan siber, keamanan jaringan dan data dapat terjamin dan terus ditingkatkan untuk menghadapi ancaman siber yang semakin kompleks dan berbahaya di masa depan.

Terima Kasih