
2025
10 - 16 Maret 2025
HASHCAT
Kamsib Indonesia
on Paper
Edisi 6
Tetap Aman
Bersama Kamsib
Kamsib Indonesia on Paper adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital.

Kamsib Indonesia on Paper

Edisi 6
10 – 16 Maret 2025

Organisasi disarankan untuk menerapkan zero-trust security, meningkatkan pelatihan, serta memperbarui sistem.

Serangan Siber Terbaru: BLACK BASTA, FRIGIDSTEALER, dan Eksploitasi Microsoft 365

Penulis: **Anton Lepari**

Pada pekan ini, ancaman siber terus berkembang dengan teknik yang semakin canggih. Salah satu tren utama adalah keterkaitan antara *ransomware* BLACK BASTA dan CACTUS. Afiliasi BLACK BASTA diketahui menggunakan modul BackConnect (BC) untuk mengendalikan sistem yang terinfeksi, mencuri data, serta mengeksekusi perintah jarak jauh. Selain itu, taktik *phishing* semakin kompleks dengan penggunaan *fake CAPTCHA* dan *SEO poisoning*. Peretas memanfaatkan pencarian dokumen PDF untuk menjebak korban. Serangan ini menggunakan Webflow CDN untuk mendistribusikan *malware*. Hal ini menandakan bahwa adanya peningkatan strategi manipulasi dalam pencarian daring.

Serangan berbasis eksploitasi *HTTP client tools* juga meningkat, terutama terhadap lingkungan Microsoft 365. Peneliti dari Proofpoint mengungkapkan bahwa 78% *tenant* Microsoft 365 telah menjadi target *account takeover*, naik 7% dalam enam bulan terakhir. Di sisi lain, skema penipuan pekerja IT dari Korea Utara semakin meluas, di mana individu yang berpura-pura sebagai pekerja lepas berupaya mengumpulkan dana untuk DPRK. Serangan ini menyoroti pentingnya perusahaan untuk melakukan verifikasi menyeluruh terhadap pekerja jarak jauh guna menghindari risiko keamanan data.

Di sektor kerentanan perangkat lunak, Broadcom merilis *patch* keamanan untuk tiga kerentanan hypervisor VMWare yang telah masuk dalam katalog CISA Known Exploited Vulnerabilities. Selain itu, *malware* baru bernama FRIGIDSTEALER menargetkan pengguna macOS melalui teknik *web injects* dan *fake updates*. *Malware* ini dirancang untuk mencuri *browser cookies*, file sensitif, dan Apple Notes, menandai tren baru dalam serangan berbasis macOS. Keterlibatan kelompok KTA420 (TA2727) dalam penyebaran FRIGIDSTEALER menunjukkan bahwa ancaman ini semakin berkembang dengan metode penyebaran yang lebih terstruktur.

Kroll juga membahas mengenai *ransomware roundup*, kelompok BIANLIAN terdeteksi mengirimkan surat fisik berisi permintaan tebusan dalam Bitcoin senilai $150.000-$500.000 kepada berbagai organisasi. Sementara itu, KTA421 (OX THIEFS) semakin aktif dengan membangun situs kebocoran data yang merinci informasi korban, termasuk kerugian yang dialami. Meningkatnya tren serangan ini menunjukkan bahwa organisasi harus lebih

waspada terhadap berbagai vektor serangan siber yang berkembang pesat. Laporan ini diungkapkan oleh Kroll melalui kanal YouTube mereka pada video berjudul *March 10, 2025 Cyber Threat Intelligence Briefing*.

BLACK BASTA

Black Basta adalah kelompok *ransomware* yang beroperasi dengan model *Ransomware-as-a-Service* (RaaS) dan pertama kali terdeteksi pada April 2022. Kelompok ini dikenal karena menggunakan teknik *double extortion*. Mereka tidak hanya mengenkripsi data korban tetapi juga mengancam untuk merilisnya jika tebusan tidak dibayarkan. Versi awal Black Basta memiliki banyak kemiripan dengan Conti Ransomware, menunjukkan kemungkinan adanya keterkaitan atau pengaruh dalam pengembangannya.

Serangan Black Basta telah berdampak pada berbagai industri serta infrastruktur kritis di Amerika Utara, Eropa, dan Australia. Hingga saat ini, lebih dari 500 organisasi telah menjadi korban serangan yang dilakukan oleh afiliasi Black Basta. Metode akses awal yang umum digunakan termasuk *phishing*, penyebaran *malware* Qakbot, Cobalt Strike, serta eksploitasi kerentanan keamanan yang sudah diketahui. Setelah berhasil masuk ke dalam jaringan, peretas akan bergerak lateral untuk mengidentifikasi sistem dan data penting sebelum akhirnya meluncurkan *ransomware*.

Selain itu, Black Basta dikaitkan dengan kelompok FIN7, salah satu aktor ancaman siber (*threat actor*). Keterkaitan ini terlihat dari modul khusus yang digunakan untuk menghindari deteksi *Endpoint Detection and Response* (EDR). Dengan kemampuan adaptasi yang tinggi dan strategi serangan yang canggih, Black Basta tetap menjadi ancaman utama bagi organisasi di seluruh dunia.

Untuk melindungi sistem dari serangan Black Basta, organisasi disarankan untuk menerapkan *zero-trust security*, meningkatkan pelatihan kesadaran keamanan siber, serta memastikan sistem selalu diperbarui dengan *patch* terbaru. Deteksi dini melalui pemantauan anomali jaringan dan respons cepat terhadap insiden juga menjadi kunci dalam menghadapi ancaman ransomware ini.

CACTUS

Cactus Ransomware adalah salah satu varian *ransomware* terbaru yang muncul pada Maret 2023 dan telah menargetkan berbagai entitas komersial serta korban profil tinggi. Dengan menggunakan teknik *double extortion*, Cactus tidak hanya mengenkripsi data korban tetapi juga mengancam untuk membocorkan data jika tebusan tidak dibayarkan. Berdasarkan laporan Darkfeed, hingga April 2024, *ransomware* ini telah menyerang lebih dari 100 organisasi. Keunikan Cactus terletak pada penggunaan OpenSSL library untuk enkripsi menggunakan kombinasi algoritma AES_CBC_256 dan RSA_4096, yang membuatnya sulit untuk didekripsi tanpa kunci yang tepat.

Salah satu metode utama yang digunakan oleh Cactus untuk mendapatkan akses awal adalah dengan mengeksploitasi kerentanan VPN (CVE-2023-38035). Peretas menargetkan Fortinet VPN untuk masuk ke jaringan internal perusahaan. Setelah mendapatkan akses, mereka memasang *backdoor SSH* yang dikendalikan dari server *Command and Control* (C2) serta menjadwalkan tugas otomatis untuk mempertahankan akses dalam jangka panjang. Dengan menggunakan alat seperti SoftPerfect Network Scanner dan PSNmap,

penyerang memetakan jaringan target, mengidentifikasi pengguna, serta menentukan perangkat yang aktif untuk memperluas infeksi *ransomware*.

Untuk memperkuat kendali atas sistem yang telah terinfeksi, pelaku serangan menggunakan teknik *credential dumping* seperti *LSASS credential dumping* untuk mencuri kredensial dari browser dan file di dalam disk. Selain itu, alat seperti AnyDesk dan Splashtop dipasang di perangkat korban guna menjaga akses jarak jauh. Setelah mendapatkan kendali penuh, penyerang menghapus antivirus dan menciptakan akun admin baru menggunakan skrip otomatis. Data korban kemudian dieksfiltrasi ke layanan *cloud* menggunakan RClone, sebelum akhirnya *ransomware* dijalankan untuk mengenkripsi file dan menghapus cadangan sistem agar tidak dapat dipulihkan.

Cactus menggunakan strategi unik dalam proses enkripsinya, di mana file yang lebih besar dari 7.7MB hanya dienkripsi sebagian untuk mempercepat proses. File yang telah dienkripsi akan diberi ekstensi khusus, dan sebuah *ransom note* akan ditinggalkan di setiap folder.

Sumber

- Kroll. 10 Maret 2025. *March 10, 2025 Cyber Threat Intelligence Briefing*. Tautan: https://www.youtube.com/watch?v=fG_nxZcOwSQ
- Abhinav Paliwal. 19 September 2024. *Black Basta Ransomware: What You Need to Know.* Tautan: https://blog.qualys.com/vulnerabilities-threat-research/2024/09/19/black-basta-ransomware-what-you-need-to-know. Qualys Blog.
- Aishwarya Gentyal. 11 Juli 2024. Cactus Ransomware: New strain in the market. Tautan: https://www.trellix.com/blogs/research/cactus-ransomware-new-strain-in-the-market/. Trellix Blog.

Jaringan nirkabel telah menjadi infrastruktur utama dalam berbagai aspek kehidupan.

Bagaimana Hacker Mengeksploitasi Kelemahan Jaringan Nirkabel?

Penulis: **Anton Lepari**

Jaringan nirkabel telah menjadi infrastruktur utama dalam berbagai aspek kehidupan. Teknologi ini tidak hanya mencakup WiFi, tetapi juga berbagai sistem komunikasi lain seperti Bluetooth, NFC, Zigbee, Li-Fi, WiMAX, serta jaringan seluler 4G dan 5G. WiFi, yang berbasis standar IEEE 802.11, merupakan teknologi paling umum yang digunakan untuk koneksi internet di rumah, kantor, serta tempat umum. Sementara itu, Bluetooth memungkinkan komunikasi jarak pendek antar perangkat seperti ponsel dan *earphone*, NFC mendukung transaksi digital, sedangkan Zigbee dan Z-Wave sering digunakan dalam otomatisasi rumah berbasis IoT. Selain itu, Li-Fi menawarkan konektivitas berbasis cahaya LED dengan kecepatan tinggi, dan WiMAX menyediakan akses internet broadband di daerah terpencil. Perkembangan jaringan seluler seperti 4G dan 5G semakin memperluas akses internet, memungkinkan komunikasi nirkabel yang lebih efisien.

Di antara berbagai teknologi jaringan nirkabel, WiFi memegang peranan penting dalam kehidupan sehari-hari. Dalam dunia kerja, WiFi mendukung

produktivitas dengan memungkinkan komunikasi jarak jauh melalui surel, *video conference*, serta akses ke layanan *cloud computing*. Dalam sektor pendidikan, teknologi ini memfasilitasi pembelajaran online dan akses ke sumber daya digital yang mempercepat proses belajar-mengajar. Dalam aspek sosial, WiFi menjadi tulang punggung media sosial, layanan *streaming video*, serta komunikasi instan melalui berbagai aplikasi pesan. Bahkan dalam kehidupan rumah tangga, berbagai perangkat smart home seperti kamera keamanan, lampu pintar, dan perangkat IoT lainnya sangat bergantung pada konektivitas WiFi.

Namun, di balik manfaatnya, WiFi juga rentan terhadap berbagai ancaman keamanan. Serangan seperti *Evil Twin Attack* memungkinkan penyerang menciptakan jaringan palsu untuk mencuri kredensial pengguna. Ada pula *Deauthentication Attack* yang dapat memutuskan koneksi perangkat dengan mengirimkan *frame deauthentication* secara paksa. Selain itu, *Man-in-the-Middle (MitM) Attack* memungkinkan peretas mencegat serta memodifikasi lalu lintas data. Serta *KRACK Attack* mengeksploitasi kelemahan dalam protokol WPA2 untuk mendekripsi lalu lintas jaringan. Serangan lainnya seperti *WPS PIN Brute-Force Attack* juga dapat digunakan untuk mendapatkan akses ke jaringan WiFi dengan menebak PIN WPS secara sistematis.

Dengan meningkatnya ancaman keamanan ini, pengguna WiFi perlu meningkatkan kesadaran akan risiko serta menerapkan langkah-langkah mitigasi, seperti menggunakan enkripsi WPA3, menghindari koneksi ke jaringan publik tanpa VPN, serta memperbarui firmware perangkat secara berkala. Dengan memahami tantangan keamanan yang ada, kita dapat lebih waspada dalam memanfaatkan teknologi WiFi secara aman dan optimal.

Standar dan Frekuensi pada *Wireless Fidelity*

WiFi (*Wireless Fidelity*) adalah teknologi jaringan nirkabel yang memungkinkan perangkat seperti komputer, smartphone, dan perangkat IoT terhubung ke internet atau jaringan lokal tanpa menggunakan kabel fisik. WiFi bekerja berdasarkan standar IEEE 802.11 yang dikembangkan oleh *Institute of Electrical and Electronics Engineers* (IEEE) untuk memastikan komunikasi data nirkabel yang aman dan efisien. Teknologi ini banyak digunakan di rumah, perkantoran, tempat umum, serta dalam berbagai perangkat pintar seperti kamera keamanan dan perangkat otomatisasi rumah (*smart home*).

Standar IEEE 802.11 pertama kali diperkenalkan pada tahun 1997 dengan kecepatan maksimal 2 Mbps. Seiring berkembangnya kebutuhan akan konektivitas yang lebih cepat dan stabil, muncul berbagai versi seperti 802.11a dan 802.11b pada tahun 1999, diikuti oleh 802.11g pada tahun 2003 yang menawarkan kecepatan hingga 54 Mbps. Pada tahun 2009, standar 802.11n mulai diperkenalkan dengan teknologi *Multiple Input Multiple Output* (MIMO), yang meningkatkan kecepatan hingga 600 Mbps. Kemudian, muncul 802.11ac (WiFi 5) yang mendukung kecepatan hingga 6.9 Gbps, dan yang terbaru adalah 802.11ax (WiFi 6 dan WiFi 6E) yang mampu mencapai kecepatan hingga 9.6 Gbps dengan efisiensi jaringan lebih tinggi dan latensi lebih rendah.

WiFi beroperasi pada beberapa pita frekuensi utama, yaitu 2.4 GHz, 5 GHz, dan yang terbaru 6 GHz. Frekuensi 2.4 GHz memiliki jangkauan lebih luas dan dapat menembus hambatan seperti dinding, tetapi rentan terhadap interferensi dari perangkat lain seperti *microwave* dan Bluetooth. Sementara itu, frekuensi

5 GHz dan 6 GHz menawarkan kecepatan lebih tinggi dengan latensi rendah, meskipun jangkauannya lebih pendek dibandingkan 2.4 GHz. Dengan inovasi terbaru, WiFi terus berkembang untuk mendukung kebutuhan komunikasi modern, mulai dari keperluan pribadi hingga penggunaan di sektor industri dan IoT.

Eksplotasi Wi-Fi

WiFi sering menjadi target serangan karena sifatnya yang terbuka dan menggunakan komunikasi nirkabel. Berikut lima metode eksploitasi yang umum digunakan oleh peretas untuk menyerang jaringan WiFi:

1. **Evil Twin Attack**
   Serangan ini melibatkan pembuatan jaringan WiFi palsu dengan nama (SSID) yang sama dengan jaringan asli. Ketika pengguna tidak sadar dan terhubung ke jaringan palsu ini, penyerang dapat mencegat lalu lintas jaringan dan mencuri data sensitif seperti kredensial login dan informasi kartu kredit.

2. **Deauthentication Attack**
   Serangan ini mengeksploitasi kelemahan dalam protokol IEEE 802.11 dengan mengirimkan paket deauthentication ke klien dan *access point* (AP). Akibatnya, perangkat pengguna akan terputus dari jaringan dan dipaksa untuk mencoba terhubung kembali, sering kali ke jaringan palsu yang dikendalikan penyerang (*Evil Twin*).

3. **KRACK Attack (Key Reinstallation Attack)**
   KRACK mengeksploitasi kelemahan dalam proses handshake WPA2. Dengan serangan ini, penyerang dapat memaksa klien untuk menggunakan kembali kunci enkripsi yang sudah digunakan sebelumnya, memungkinkan mereka untuk mendekripsi lalu lintas jaringan dan mencuri data yang dikirim melalui WiFi.

4. **WPS PIN Brute Force Attack**
   WiFi Protected Setup (WPS) sering digunakan untuk mempermudah koneksi perangkat ke jaringan WiFi tanpa perlu memasukkan kata sandi. Namun, fitur ini memiliki kelemahan serius, di mana penyerang dapat menggunakan metode *brute force* untuk menebak PIN WPS dan mendapatkan akses ke jaringan WiFi dalam hitungan jam.

5. **Man-in-the-Middle (MitM) Attack**
   Serangan ini memungkinkan penyerang untuk mencegat dan memodifikasi lalu lintas data antara klien dan *router*. Dengan teknik seperti *ARP spoofing* atau *DHCP spoofing*, penyerang dapat membaca dan mengubah komunikasi jaringan, termasuk informasi sensitif seperti login dan transaksi keuangan.

Sumber

- Choi, Min-Kyu & Rosslin, John & Robles, Rosslin & Hong, Chang-Hwa & Kim, Tai-Hoon. (2008). *Wireless Network Security: Vulnerabilities, Threats and Countermeasures*. International Journal of Multimedia and Ubiquitous Engineering. 3.
- O'Sullivan, J. *How we made the wireless network*. Nat Electron 1, 147 (2018). https://doi.org/10.1038/s41928-018-0027-y

- Sonawane, Sachin & Mane, Prof & Vanjale, Prof. (2013). *A Survey on Evil Twin Detection Methods for Wireless Local Area Network.*
- Mathy Vanhoef and Frank Piessens. 2017. *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Association for Computing Machinery, New York, NY, USA, 1313–1328. https://doi.org/10.1145/3133956.3134027
- L. R and R. M. Bommi, "Deauthentication Attack Detection in the Wi-Fi network by Using ML Techniques," *2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE),* Bengaluru, India, 2022, pp. 1-6, doi: 10.1109/ICSTCEE56972.2022.10099975.

Banyak pengguna melaporkan bahwa mereka tidak dapat mengakses layanan dengan normal.

Serangan Siber pada Platform X (sebelumnya Twitter)

Penulis: **Anton Lepari**

Pada 10 Maret 2025, platform media sosial X mengalami gangguan layanan yang signifikan. Elon Musk, pemilik platform tersebut, mengklaim bahwa X menjadi target serangan siber besar-besaran yang melibatkan sumber daya substansial, kemungkinan melibatkan kelompok terkoordinasi besar atau negara tertentu. Serangan ini menyebabkan dua lonjakan besar dalam keluhan pengguna dan mengakibatkan downtime yang signifikan, terutama mempengaruhi pengguna di wilayah pesisir AS. Sebagai jejaring sosial yang sebelumnya dikenal sebagai Twitter, banyak pengguna melaporkan bahwa mereka tidak dapat mengakses layanan dengan normal, terutama karena postingan gagal dimuat.

Menurut Downdetector, platform pemantau gangguan layanan, masalah ini pertama kali terjadi sekitar pukul 5.45 pagi, dengan ribuan laporan pengguna yang mengalami kendala. Meskipun sempat membaik, gangguan kembali meningkat menjelang siang, terutama berdampak pada aplikasi seluler. Pengguna yang mengalami kegagalan memuat tweet menerima pesan kesalahan yang menyatakan "ada yang tidak beres" dan disarankan untuk mencoba kembali.

Sumber

- Nick Robins-Early. 10 Maret 2025. *Elon Musk claims 'massive cyber-attack' caused X outages.* Tautan: https://www.theguardian.com/technology/2025/mar/10/elon-musk-cyberattack-x-outages. The Guardian.
- Fajar Nugraha. 11 March 2025. *Musk Sebut X Mengalami Serangan Siber Besar-besaran*. Tautan: https://www.metrotvnews.com/read/NG9CQrj6-musk-sebut-x-mengalami-serangan-siber-besar-besaran. Metro TV.
- Michelle Chapman dan Barbara Ortutay. 11 Maret 2025. *Elon Musk claims X being targeted in 'massive cyberattack' as service goes down*. Tautan: https://apnews.com/article/x-musk-twitter-outage-california-0268a8b035aaa277c0287e7c82b6081e. AP News.

GitHub telah menjadi standar industri dalam pengembangan perangkat lunak modern.

Mengenal Serangan pada GitHub Supply Chain pada Perangkat Lunak

Penulis: **Anton Lepari**

GitHub Supply Chain Attack adalah serangan terhadap rantai pasokan perangkat lunak (*software*) yang memanfaatkan ekosistem GitHub. Ini termasuk repositori kode, dependensi, dan *pipeline CI/CD*. Serangan ini bertujuan untuk menyisipkan kode berbahaya ke dalam proyek perangkat lunak yang digunakan oleh banyak pengembang. Karena GitHub menjadi pusat kolaborasi bagi berbagai proyek *open-source* dan komersial, serangan ini dapat berdampak luas dengan menginfeksi banyak pengguna sekaligus.

Metode yang digunakan dalam serangan ini beragam, mulai dari pengambilalihan repositori, eksploitasi *GitHub Actions*, hingga *poisoning code contribution* melalui *Pull Request* berbahaya. Salah satu teknik yang sering digunakan adalah *Dependency Confusion*, di mana penyerang mengunggah paket dengan nama mirip dependensi asli ke registri publik seperti npm atau PyPI. Akibatnya, sistem yang secara otomatis memperbarui dependensi dapat mengunduh versi berbahaya tanpa disadari. Selain itu, penyerang juga dapat mencuri kredensial pengembang melalui *phishing* atau *credential stuffing* untuk mendapatkan akses ke proyek penting.

Dampak dari serangan ini bisa sangat luas, terutama jika kode berbahaya berhasil masuk ke dalam perangkat lunak yang digunakan oleh banyak pihak. Misalnya, jika suatu proyek *open-source* populer terinfeksi, maka semua aplikasi yang bergantung pada proyek tersebut juga berisiko. Oleh karena itu, penting bagi pengembang untuk menerapkan langkah-langkah keamanan, seperti memverifikasi dependensi, menggunakan autentikasi dua faktor (2FA), serta memantau aktivitas repositori secara rutin agar dapat mendeteksi ancaman sejak dini.

Apa itu GitHub?

GitHub adalah platform berbasis *cloud* yang digunakan untuk menyimpan, mengelola, dan berkolaborasi dalam pengembangan perangkat lunak menggunakan sistem kontrol versi Git. Dengan GitHub, pengembang dapat bekerja sama dalam suatu proyek, melacak perubahan kode, serta mengelola revisi secara efisien. Platform ini banyak digunakan oleh individu, komunitas *open-source*, dan perusahaan untuk membangun serta mengelola perangkat lunak secara terstruktur.

Salah satu fitur utama GitHub adalah repositori, yang berfungsi sebagai tempat penyimpanan kode sumber, dokumentasi, dan file terkait proyek. Pengguna dapat berkontribusi melalui *Pull Request*, yang memungkinkan mereka mengusulkan perubahan sebelum kode digabungkan ke dalam proyek utama. Selain itu, GitHub menyediakan fitur seperti *Issue Tracker* untuk melaporkan *bug* dan mendiskusikan pengembangan, serta *GitHub Actions* untuk otomatisasi alur kerja CI/CD.

GitHub juga memiliki berbagai alat keamanan dan manajemen proyek, seperti *Dependabot* untuk mendeteksi kerentanan dalam dependensi dan *Code Scanning* untuk menemukan potensi *bug* dalam kode. Dengan dukungan integrasi ke berbagai layanan dan ekosistem yang luas, GitHub telah menjadi

standar industri dalam pengembangan perangkat lunak modern, baik untuk proyek *open-source* maupun komersial.

Sumber

- Benedetti, Giacomo & Verderame, Luca & Merlo, Alessio. (2022). *Automatic Security Assessment of GitHub Actions Workflows*. 37-45. 10.1145/3560835.3564554.
- Silva, Edson & Rodrigues, Rodolfo & Oliveira, Johnatan & Boechat, Danilo & Tavares, Cleiton. (2024). *Evaluating Test Quality in GitHub Repositories: A Comparative Analysis of CI/CD Practices Using GitHub Actions*. 45-55. 10.5753/vem.2024.3842.
- Ghouri, Arsalan. (2025). *View of Management Information System and Digital Supply Chain Influence on Supply Chain Resilience through Supply Chain Risk Management. International Journal of Construction Supply Chain Management*. 14. 96-118. 10.2139/ssrn.5081694.

Kamsib Indonesia
Jakarta, Indonesia
hubungi@kamsib.id

Kamsib ID *adalah sebuah platform edukasi yang berfokus pada keamanan informasi dan siber dalam bahasa Indonesia. Kehadiran Kamsib dipicu oleh lonjakan pesat penggunaan internet yang tidak diimbangi dengan kesadaran akan pentingnya keamanan di dunia maya. Fenomena ini juga menjadi salah satu pemicu dari banyaknya kasus penipuan, kebocoran data, dan insiden dalam sistem elektronik, baik yang dimiliki oleh pemerintah maupun swasta.*

Kamsib Indonesia on Paper *adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital. Diterbitkan secara berkala, majalah ini menyajikan artikel mendalam, studi kasus, serta wawancara dengan para ahli untuk memberikan wawasan bagi profesional keamanan siber, peneliti, dan penggemar dunia siber. Dengan pendekatan yang informatif dan analitis, Kamsib Indonesia on Paper bertujuan menjadi referensi utama bagi siapa saja yang ingin memahami dan menghadapi tantangan di dunia siber yang terus berkembang.* [at]kamsib_id