JIIC: JURNAL INTELEK INSAN CENDIKIA
https://jicnusantara.com/index.php/jiic
Vol : 3 No: 7, Juli 2026
E-ISSN : 3047-7824

Satu Klik Bisa Menghancurkan Segalanya: Memahami Ancaman Siber di Era Digital

One Click Can Destroy Everything: Understanding Cyber Threats in the Digital Age

Gita, Ismanita, Rayyan Firdaus
Universitas Malikussaleh
Email: gita240420068@mhs.unimal.ac.id[1], ismanita.240420058@mhs.unimal.ac.id[2], Rayyan@gmail.com[3]

Article Info

Article history:
Received : 08-07-2026
Revised : 10-07-2026
Accepted : 12-07-2026
Pulished : 14-07-2026

Abstract

The spread of digital technology in Indonesia is accompanied by an increase in cybersecurity threats. The purpose of this article is to identify the trends, classifications, sources, and impacts of cyber threats in Indonesia, as well as to develop relevant mitigation strategies for individuals and organizations. The research method used is descriptive qualitative. This study uses literature research to collect data and official reports from authorized institutions such as the National Cyber and Crypto Agency (BSSN), the Financial Services Authority (OJK), the Indonesia Anti-Scam Center (IASC), the Ministry of Communication and Digital, as well as private institutions such as Kaspersky, AwanPintar.id, and ITSEC Asia from 2025 to 2026. This study shows a drastic increase in cyberattacks in Indonesia BSSN estimated 5.5 billion cyberattacks throughout 2025, most of which were based on malware and phishing caused by user negligence when interacting with suspicious links or attachments. Artificial intelligence-based threats such as deepfakes have increased by 550 percent in the last five years. Digital fraud has caused financial losses exceeding Rp2.6 trillion by May 2025. According to this research, human error remains the most dominant security factor. Therefore, improving digital literacy, system update policies, and a proactive security culture are essential steps to mitigate cyber threats in Indonesia.

Keywords: cyber threats, digital security, digital literacy

Abstrak

Penyebaran teknologi digital di Indonesia seiring dengan peningkatan ancaman keamanan siber. Tujuan dari artikel ini adalah untuk mengidentifikasi tren, klasifikasi, sumber, dan dampak ancaman siber di Indonesia serta mengembangkan strategi mitigasi yang relevan bagi individu dan organisasi. Metode penelitian ini adalah kualitatif deskriptif. Penelitian ini menggunakan penelitian desk research untuk mengumpulkan data dan laporan resmi dari lembaga resmi seperti Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), Pusat Anti-Scam Indonesia (IASC), Kementerian Komunikasi dan Digital, serta lembaga swasta seperti Kaspersky, AwanPintar.id, dan ITSEC Asia dari tahun 2025 hingga2026. Kajian menunjukkan peningkatan drastis dalam serangan siber di Indonesia BSSN memperkirakan 5,5 miliar serangan siber sepanjang tahun 2025, sebagian besar berbasis malware dan phishing yang disebabkan oleh kelalaian pengguna saat berinteraksi dengan tautan atau lampiran mencurigakan. Ancaman berbasis kecerdasan buatan seperti deepfake telah meningkat sebesar 550 persen dalam lima tahun terakhir. Penipuan digital telah menyebabkan kerugian finansial yang melampaui Rp2,6 triliun hingga Mei 2025. Menurut penelitian ini, kesalahan manusia juga dikenal sebagai kesalahan manusia masih merupakan faktor keamanan yang paling dominan. Oleh karena itu, meningkatkan literasi digital, kebijakan pembaruan sistem, dan budaya keamanan proaktif adalah langkah penting untuk mengurangi ancaman siber di Indonesia.

Kata Kunci: ancaman siber, keamanan digital, literasi digital

PENDAHULUAN

Cara masyarakat Indonesia berinteraksi, bertransaksi, dan bekerja telah diubah oleh transformasi digital. Di sisi lain, kemudahan tersebut membawa dampak berupa perluasan permukaan serangan (surface attack), yang dapat dimanfaatkan oleh pelaku kejahatan siber. Serangan yang berdampak luas, seperti pencurian data pribadi, kerugian finansial, dan penundaan layanan publik, dapat dimulai dengan tindakan sederhana yang tampak sepele, seperti mengklik tautan pada pesan singkat atau surel yang tidak dikenal.

Fenomena ini telah menjadi fenomena yang sangat umum dan bukan lagi ancaman yang mungkin. Menurut data yang dikumpulkan oleh Badan Siber dan Sandi Negara (BSSN), jumlah anomali dan serangan siber di Indonesia terus meningkat dari tahun ke tahun, bahkan mencapai miliaran insiden dalam beberapa bulan. Peningkatan ini juga disebabkan oleh tingginya penetrasi internet yang tidak diimbangi oleh pengetahuan yang cukup tentang keamanan digital di kalangan masyarakat dan lembaga.

Artikel ini ditulis untuk menjawab beberapa pertanyaan penelitian: (1) tren dan skala ancaman siber di Indonesia dari tahun 2025 hingga 2026 (2) jenis ancaman siber apa yang paling dominan (3) faktor apa yang menyebabkan kerentanan digital tinggi di Indonesia dan (4) strategi mitigasi apa yang dapat digunakan untuk menekan risiko. Untuk membantu pembaca umum, pelaku usaha, dan pengambil kebijakan memahami dan menangani ancaman siber dengan lebih baik, penelitian ini bertujuan untuk memberikan gambaran lengkap yang didasarkan pada data resmi dan terbaru.

METODE PENELITIAN

Penelitian ini disusun menggunakan pendekatan kualitatif deskriptif dengan melakukan penelusuran pustaka daring. Dibandingkan dengan mengumpulkan data baru melalui wawancara atau survei di lapangan, pendekatan ini dipilih karena tujuan tulisan adalah untuk memetakan tren dan pola ancaman siber yang sedang berlangsung berdasarkan data yang sudah dipublikasikan.

Data yang digunakan sebagian besar berasal dari publikasi yang tersedia untuk umum dari Juli 2025 hingga Juni 2026. Sebagian data didasarkan pada pernyataan resmi dari lembaga pemerintah seperti Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), Pusat Anti-Scam Indonesia (IASC), Kementerian Komunikasi dan Digital, dan Kantor Staf Kepresidenan, yang dikutip ulang oleh media. Sebagian lainnya berasal dari laporan penelitian yang dibuat oleh perusahaan keamanan siber seperti Kaspersky, AwanPintar.id, dan ITSEC Asia. Laporan ini juga didistribusikan melalui berita di media dan artikel ringkasan data di beberapa portal teknologi.

Untuk memastikan bahwa angka yang dikutip konsisten satu sama lain dan benar-benar dapat diakses, proses pengumpulan melibatkan membaca secara menyeluruh setiap artikel dari sumber-sumber tersebut melalui mesin pencari. Setelah data dikumpulkan, mereka dikelompokkan ke dalam beberapa tema diskusi, seperti skala ancaman, jenis serangan yang dominan, faktor penyebab kerentanan, dampak yang ditimbulkan, dan langkah mitigasi. Kemudian, untuk mengetahui apakah tren antar-sumber konsisten atau berbeda, perbandingan antar-sumber dilakukan.

Metode ini memiliki keterbatasan, harus diakui. Sumber-sumber tertentu adalah artikel media atau blog perusahaan yang mengutip data resmi, bukan dokumen resmi itu sendiri. Karena

itu, makna data mungkin tidak banyak berubah saat dikutip berulang kali. Selain itu, masing-masing lembaga dan organisasi penelitian kadang-kadang menggunakan istilah yang berbeda untuk hal-hal yang serupa misalnya, "anomali trafik" tidak selalu identik dengan "serangan" atau "insiden". Akibatnya, angka-angka yang disajikan lebih tepat dianggap sebagai representasi skala dan tren daripada angka mutlak yang dapat dibandingkan secara ketat. Pembaca disarankan untuk mengunjungi situs web bssn.go.id, ojk.go.id, atau komdigi.go.id secara langsung jika mereka membutuhkan informasi resmi untuk keperluan akademik resmi.

HASIL DAN PEMBAHASAN

Skala dan Tren Ancaman Siber di Indonesia

Menurut data BSSN, jumlah serangan siber di Indonesia akan mencapai 5,5 miliar insiden pada tahun 2025. Tren ini berlanjut pada awal 2026, dengan tercatat 1,52 miliar serangan hanya dari 1 Januari hingga 15 April 2026. Selain itu, menurut penelitian ITSEC Asia, dari Januari hingga November 2025, terjadi lebih dari 5,16 miliar anomali trafik, setara dengan 182 percobaan serangan per detik, menempatkan Indonesia di antara negara-negara Asia Pasifik dengan tingkat ancaman digital tertinggi.

Fakta ini diperkuat oleh Laporan AwanPintar.id, yang mencatat 234.528.187 serangan siber sepanjang semester kedua tahun 2025, peningkatan 75,76% dari semester pertama tahun yang sama. Lebih dari 90 juta serangan terjadi dalam satu bulan pada Desember 2025 mungkin karena banyaknya transaksi online di akhir tahun. Selain itu, Indonesia tercatat sebagai penyumbang terbesar dari lalu lintas berbahaya global, dengan kontribusi 56,29%, dan penyumbang malware terbesar, dengan kontribusi 61,32%.

Jenis Ancaman Siber yang Dominan

Sebanyak 83,68 persen dari anomali siber berbasis malware, yang dihasilkan melalui tautan phishing, lampiran surel berbahaya, dan aplikasi palsu. Malware ini biasanya digunakan sebagai tahap awal untuk mencuri kredensial atau membuka akses admin sebelum pelaku melakukan serangan lanjutan seperti ransomware. Suara.com melaporkan bahwa backdoor jenis DoublePulsar mendominasi hampir seluruh serangan sejenisnya, karena karakteristiknya yang sangat tersembunyi sehingga korban sering tidak menyadarinya sampai kerusakan terjadi.

Selain malware konvensional, ancaman berbasis kecerdasan buatan juga meningkat pesat. Menurut Kementerian Komunikasi dan Digital, jumlah konten deepfake di Indonesia telah meningkat sebesar 550 persen dalam lima tahun terakhir. Menurut laporan tersebut, kerugian per insiden deepfake korporat rata-rata mencapai 250.000 USD. Di industri perbankan dan fintech, deepfake banyak digunakan untuk memalsukan identitas selama proses verifikasi digital onboarding. Akibatnya, metode verifikasi tradisional berbasis wajah atau suara menjadi kurang aman.

Selain itu, Kaspersky mencatat munculnya pola ancaman baru berupa serangan rantai pasok (supply chain attack), yang akan dialami oleh sekitar 20 persen perusahaan di Indonesia hingga tahun 2025. Serangan ini menyusup melalui mitra bisnis atau vendor dengan standar keamanan yang kurang, sehingga perusahaan dengan sistem internal yang kuat sekalipun dapat menjadi korban jika mitra kerjanya lengah.

Faktor Penyebab Tingginya Kerentanan Digital

Ada sejumlah penyebab kerentanan siber yang tinggi di Indonesia. Pertama, eksploitasi celah keamanan (CVE) meningkat dengan cepat. Menurut laporan AwanPintar.id, banyak CVE yang dirilis pada tahun 2025 langsung dieksploitasi pada bulan yang sama, terutama pada sistem komunikasi dan perangkat Internet of Things (IoT). Ini menunjukkan bahwa perusahaan yang tidak melakukan pembaruan sistem dengan cepat menjadi sasaran CVE. Kedua, menurut Yudhi Kukuh, pendiri AwanPintar.id, pola serangan telah berubah dari individu menjadi kelompok yang lebih terorganisir dan menyasar target strategis seperti layanan publik dan platform ekonomi digital.

Ketiga, dan paling penting, dasar sebagian besar serangan siber tetap pada faktor kesalahan manusia. Mengklik tautan tanpa verifikasi, penggunaan kata sandi yang buruk, dan kurangnya instruksi tentang keamanan digital di tempat kerja menyebabkan lapisan pertahanan teknis menjadi buruk. Kondisi ini menunjukkan bahwa tanpa instruksi pengguna yang memadai, investasi dalam teknologi keamanan tidak akan cukup untuk menekan risiko secara signifikan.

Dampak Ancaman Siber

Ancaman siber di Indonesia benar-benar berdampak pada sektor keuangan. Menurut OJK dan Indonesia Anti-Scam Center (IASC), penipuan online telah mengakibatkan kerugian yang melampaui Rp2,6 triliun hingga Mei 2025. Sementara itu, ekonomi siber secara keseluruhan tercatat mencapai Rp18 triliun pada tahun 2024, menurut BSSN. Sebagaimana disampaikan dalam pernyataan resmi Kantor Staf Kepresidenan, dampak di luar aspek finansial juga mencakup gangguan operasional layanan publik, keterlambatan sistem, kebocoran data pribadi, dan penurunan kepercayaan masyarakat terhadap ekosistem digital nasional.

Upaya Mitigasi

Untuk mengurangi ancaman, beberapa tindakan dapat disarankan pada tingkat individu maupun organisasi, tergantung pada pola ancaman yang diidentifikasi. Salah satunya adalah memverifikasi tautan dan pengirim pesan sebelum melakukan klik, terutama untuk pesan yang bernada mendesak atau meminta data sensitif.

1. Pembaruan rutin sistem dan perangkat lunak untuk menutup celah keamanan (patch management) sebelum sempat digunakan
2. Implementasi autentikasi berlapis (multi-factor authentication) untuk mengurangi risiko pengambilalihan akun
3. Audit keamanan terhadap vendor dan mitra bisnis untuk mengurangi risiko serangan rantai pasok
4. Pencadangan data (backup) yang rutin dan terenkripsi sebagai lapisan terakhir perlindungan terhadap ransomware.
5. Secara teratur, karyawan dan masyarakat umum diberi pelatihan kesadaran keamanan siber karena sebagian besar insiden berasal dari kesalahan pengguna.

Penguatan sistem teknis dan peningkatan literasi digital masyarakat menjadi kunci utama dalam mencegah laju pertumbuhan insiden siber di Indonesia ke depan.

KESIMPULAN

Hasil penelitian menunjukkan tren yang signifikan dalam volume, kompleksitas, dan konsekuensi finansial ancaman siber di Indonesia. Ancaman berbasis kecerdasan buatan seperti

deepfake tumbuh pesat dan menambah kompleksitas mitigasi, tetapi phishing dan malware tetap menjadi jenis ancaman paling umum. Sebagian besar insiden disebabkan oleh kesalahan manusia, menunjukkan bahwa keamanan siber bukan hanya masalah teknologi tetapi juga perilaku dan kesadaran pengguna.

SARAN

Sangat disarankan agar orang memperhatikan dan memverifikasi setiap tautan atau permintaan data sebelum melakukan apa pun. Mereka juga harus terus mengetahui modus penipuan digital terbaru. Disarankan agar perusahaan dan bisnis mengalokasikan dana yang seimbang untuk teknologi keamanan (seperti sistem manajemen akses dan deteksi ancaman) dan program pelatihan keamanan siber untuk karyawan. Penguatan regulasi terkait perlindungan data pribadi dan kolaborasi lintas sektor antara pemerintah, industri, dan masyarakat diperlukan untuk melindungi ekosistem digital dari ancaman siber di masa mendatang.

DAFTAR PUSTAKA

AwanPintar.id (Prosperita Group). (2026). Indonesia Waspada: Laporan Ancaman Digital di Indonesia Semester 2 Tahun 2025. Dikutip dalam CSIRT.or.id, Serangan Siber RI Meledak, 234 Juta Insiden dalam 6 Bulan. https://csirt.or.id/berita/serangan-siber-ri-dalam-6-bulan

CNBC Indonesia. (2026, 2 Juni). Serangan Siber di RI Menggila, Melonjak Sampai 714%, Awal 2026 Segini. https://www.cnbcindonesia.com/tech/20260602203559-37-739562/serangan-siber-di-ri-menggila-melonjak-sampai-714-awal-2026-segini/amp

CyberHub.id. (2025). Ancaman Digital 2025: 133,4 Juta Serangan Siber Terjadi di RI. https://cyberhub.id/berita/ancaman-digital-2025-serangan-siber-ri

IT Proxsis Group. (2025, 3 Juli). Tren Ancaman Siber di Indonesia Meningkat? Berikut Fakta yang Harus Diketahui. https://it.proxsisgroup.com/tren-ancaman-siber-di-indonesia-meningkat-berikut-fakta-yang-harus-diketahui/

ManageEngine. (2026). Serangan Siber Indonesia 2026: Dari Statistik ke Strategi Kesiapan IT. https://www.manageengine.com/id/blog/siem/statistik-serangan-siber-indonesia.html

SMJTimes. (2026, 10 April). Kaspersky Laporkan 50 Juta Serangan Siber Terdeteksi di Indonesia pada 2025.https://smjtimes.com/2026/04/10/kaspersky-laporkan-50-juta-serangan-siber-terdeteksi-di-indonesia-pada-2025/

Suara.com. (2026, 9 Juni). 182 Serangan Siber per Detik Menghantam Indonesia, ITSEC Asia Soroti Ancaman Digital. https://amp.suara.com/tekno/2026/06/09/154358/182-serangan-siber-per-detik-menghantam-indonesia-itsec-asia-soroti-ancaman-digital

Verihubs. (2026, 22 Maret). Statistik Cybercrime Indonesia 2025-2026: Data dan Tren Terbaru. https://verihubs.com/blog/statistik-cybercrime-indonesia