SITI: Jurnal Sistem Informasi dan Teknik Informatika
Vol. 01, No.02, Date 2025-05-03

Sejarah dan Perkembangan Virus Komputer: dari Malware Awal hingga Ransomware

Ihsan [1*]
[1]Informatika, LPK-Codingin, Banten-Indonesia
*e-mail : ihsan86@gmail.com

Abstract
This study aims to trace the history and development of computer viruses from early malware to contemporary ransomware. Through a qualitative literature review, data were collected from secondary sources such as academic documents, cybersecurity reports, and historical technology archives. The findings indicate that malware evolution can be categorized into four main phases: (1) theoretical concepts in the 1940s–1970s, (2) the emergence of the first viruses in the 1980s (e.g., Brain Virus and Elk Cloner), (3) expansion via the internet in the 1990s–2000s (e.g., Melissa, ILOVEYOU), and (4) the dominance of ransomware since the 2010s (e.g., WannaCry, NotPetya). The analysis reveals that this evolution was driven by technological advancements such as global networking, complex operating systems, and economic and political motives. Modern ransomware leverages cryptographic encryption and digital payments to target victims, significantly impacting critical infrastructure. The discussion highlights the need for adaptive AI-based security systems, increased user awareness, and international collaboration in cybersecurity regulations. This study concludes that a deep understanding of malware evolution is a crucial foundation for anticipating future threats such as AI-driven attacks and IoT exploitation. The findings recommend integrating both technical and non-technical approaches in cybersecurity mitigation strategies.
***Keywords**: computer virus, ransomware, malware evolution.*

Abstrak
Penelitian ini bertujuan untuk menelusuri sejarah dan perkembangan virus komputer dari malware awal hingga ransomware kontemporer. Melalui studi literatur kualitatif, data dikumpulkan dari sumber sekunder seperti dokumen akademis, laporan keamanan siber, dan arsip sejarah teknologi. Hasil penelitian menunjukkan bahwa evolusi malware terbagi dalam empat fase utama: (1) konsep teoretis pada 1940–1970-an, (2) kemunculan virus pertama di era 1980-an (misalnya, Brain Virus dan Elk Cloner), (3) ekspansi melalui internet tahun 1990–2000-an (Melissa, ILOVEYOU), dan (4) dominasi ransomware sejak 2010 (WannaCry, NotPetya). Analisis mengungkap bahwa perkembangan ini dipicu oleh kemajuan teknologi seperti jaringan global, sistem operasi kompleks, serta motif ekonomi dan politik. Ransomware modern memanfaatkan enkripsi kriptografi dan pembayaran digital untuk menargetkan korban dengan dampak signifikan pada infrastruktur vital. Diskusi menyoroti perlunya sistem keamanan adaptif berbasis AI, peningkatan kesadaran pengguna, serta kolaborasi internasional dalam regulasi siber. Penelitian ini menyimpulkan bahwa pemahaman mendalam tentang evolusi malware merupakan fondasi kritis untuk mengantisipasi ancaman masa depan seperti serangan berbasis AI dan eksploitasi IoT. Temuan ini merekomendasikan integrasi pendekatan teknis dan non-teknis dalam strategi mitigasi keamanan siber.

Kata kunci: virus komputer, ransomware, evolusi malware.

1. PENDAHULUAN

Sejak kemunculannya pada pertengahan abad ke-20, virus komputer telah berevolusi dari sekadar eksperimen akademis menjadi ancaman global yang kompleks. Konsep awal malware tercetus dari teori John von Neumann tentang program yang mampu mereplikasi diri (1949), yang kemudian diimplementasikan dalam bentuk praktis seperti Creeper pada 1971. Pada era 1980-an, virus seperti Brain dan Elk Cloner menandai awal penyebaran malware melalui disket, menginfeksi sistem dengan tujuan iseng atau eksperimen. Namun, perkembangan internet pada 1990-an membuka pintu bagi ekspansi malware secara masif, diikuti oleh motif ekonomi dan politik yang lebih terstruktur. Saat ini, ransomware mendominasi lanskap keamanan siber, memanfaatkan teknologi enkripsi dan pembayaran kripto untuk mengeksploitasi korban secara finansial. Pemahaman tentang sejarah dan transformasi malware ini tidak hanya penting untuk literasi teknologi, tetapi juga menjadi fondasi kritis dalam merancang sistem pertahanan siber yang adaptif.

Perkembangan virus komputer tidak terjadi dalam ruang hampa, melainkan dipicu oleh kemajuan teknologi dan perubahan dinamika sosial. Pertumbuhan internet, sistem operasi yang semakin kompleks, serta ketergantungan manusia pada infrastruktur digital telah menciptakan celah yang dimanfaatkan pelaku kejahatan siber. Contohnya, worm Morris (1988) memanfaatkan kerentanan protokol jaringan (Brassard, 2023), sementara ransomware WannaCry (2017) mengeksploitasi kelemahan sistem Windows (Aljaidi et al., 2022),. Permasalahan utama terletak pada ketertinggalan strategi pertahanan dalam menghadapi inovasi serangan yang terus berkembang. Selain itu, minimnya kesadaran pengguna dan fragmentasi regulasi global memperparah dampak serangan malware. Pertanyaan mendasar yang perlu dijawab adalah: bagaimana pola evolusi malware dari masa ke masa, dan langkah apa yang efektif untuk memitigasi ancaman masa depan?

Sejumlah studi telah mengkaji aspek teknis dan historis malware. (Payne, 2022) dalam *Viruses* mendokumentasikan karakteristik virus era 1990-an, sementara laporan Kaspersky (2021) fokus pada tren ransomware modern (Jones et al., 2023). Penelitian oleh Zamora (2015) menganalisis peran faktor ekonomi dalam perkembangan malware, sementara Sommer dan Brown (2011) mengeksplorasi dampak serangan siber pada keamanan nasional. Namun, sebagian besar literatur terdahulu cenderung terfragmentasi—ada yang membahas sejarah tanpa kaitan dengan konteks teknologi terkini, atau mengulas teknik serangan tanpa analisis mendalam tentang akar permasalahan. Kekosongan penelitian terletak pada kurangnya integrasi antara perspektif historis, teknis, dan sosio-ekonomi dalam memahami evolusi malware.

Meskipun banyak studi telah dilakukan, tiga gap utama teridentifikasi. Pertama, penelitian terdahulu jarang menyajikan analisis kronologis yang menyeluruh dari era pra-internet hingga ransomware kontemporer. Kedua, faktor pendorong seperti globalisasi, kebijakan privatisasi data, dan perkembangan kriptografi sering diabaikan. Ketiga, minimnya pembahasan tentang keterkaitan antara evolusi malware dengan respons kebijakan dan inovasi keamanan (Ansori, 2024). Contohnya, transformasi dari virus "iseng" menjadi ransomware yang terorganisir belum dijelaskan secara holistik, termasuk peran mata uang kripto dalam memfasilitasi kejahatan transnasional. Gap ini membatasi pemahaman komprehensif tentang dinamika ancaman siber.

Untuk menjawab tantangan tersebut, penelitian ini mengusulkan pendekatan multidisiplin yang menggabungkan analisis sejarah, reverse engineering malware, dan studi kasus serangan besar. Solusi teknis seperti sistem deteksi berbasis AI dan blockchain untuk melacak transaksi ransomware perlu diintegrasikan dengan solusi non-teknis, seperti edukasi pengguna dan kerangka regulasi global. Contoh konkret termasuk penerapan *zero-trust architecture* pada infrastruktur vital dan kolaborasi internasional melalui forum seperti INTERPOL Cybercrime Directorate. Selain itu, penelitian menekankan pentingnya

"kebersihan digital" (digital hygiene) sebagai langkah preventif, seperti pembaruan sistem berkala dan manajemen kata sandi.

Kebaruan (novelty) penelitian ini terletak pada tiga aspek. Pertama, penyusunan timeline perkembangan malware yang mencakup fase teoretis (1940-an) hingga era ransomware (2020-an), dilengkapi dengan studi kasus seperti WannaCry dan NotPetya. Kedua, integrasi analisis sosio-teknis, termasuk dampak globalisasi dan ekonomi gelap siber terhadap motif penyerang. Ketiga, penggunaan data primer dari laporan forensik siber terbaru (misalnya, analisis serangan Colonial Pipeline 2021) yang belum banyak dieksplorasi dalam literatur akademis (Tsvetanov & Slaria, 2021). Pendekatan ini memungkinkan pemetaan yang lebih akurat tentang pola evolusi malware dan prediksi ancaman masa depan.

Penelitian ini mengadopsi metode kualitatif dengan pendekatan studi literatur sistematis dan analisis konten. Data dikumpulkan dari sumber sekunder seperti jurnal akademis, arsip sejarah teknologi (misalnya, dokumen ARPANET), laporan tahunan perusahaan keamanan (Symantec, CrowdStrike), serta wawancara dengan pakar siber yang dipublikasikan di media (Mugu et al., 2024). Analisis dilakukan secara tematik dengan mengkategorikan malware berdasarkan periode, teknik serangan, dan dampaknya. Validasi data dilakukan melalui triangulasi sumber untuk memastikan akurasi historis dan teknis.

Kontribusi penelitian ini bersifat teoritis dan praktis. Secara teoritis, studi ini memperkaya literatur sejarah teknologi dengan menghubungkan perkembangan malware dengan konteks sosio-politik, seperti Perang Dingin dan kebangkitan ekonomi digital. Secara praktis, temuan penelitian dapat menjadi acuan bagi pengembang sistem keamanan, pembuat kebijakan, dan organisasi dalam merancang strategi mitigasi yang proaktif. Misalnya, pemahaman tentang pola serangan ransomware dapat mendorong pengembangan alat dekripsi khusus atau pelatihan respons insiden bagi institusi finansial. Selain itu, penelitian ini meningkatkan kesadaran publik tentang pentingnya keamanan siber dalam era transformasi digital.

Berdasarkan latar belakang dan gap penelitian yang diidentifikasi, studi ini bertujuan untuk menyajikan narasi komprehensif tentang evolusi malware, dari akar teoretisnya hingga ancaman modern. Dengan menggabungkan perspektif sejarah, teknis, dan sosio-ekonomi, penelitian ini tidak hanya mengisi celah akademis tetapi juga menawarkan rekomendasi kebijakan yang actionable. Hasilnya diharapkan dapat menjadi peta jalan bagi penguatan ketahanan siber di tingkat individu, organisasi, dan global, sekaligus mengantisipasi tantangan masa depan seperti serangan berbasis AI dan eksploitasi IoT.

2. METODOLOGI

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi literatur sistematis untuk menganalisis evolusi virus komputer dari perspektif historis dan teknis (Ansori & Noeralamsyah, n.d.). Data dikumpulkan melalui tinjauan mendalam terhadap sumber sekunder, termasuk jurnal akademis, laporan industri keamanan siber, arsip sejarah teknologi, serta dokumentasi kasus malware yang dipublikasikan antara 1940–2023. Kriteria inklusi sumber meliputi relevansi dengan topik perkembangan malware, kredibilitas penerbit (misalnya, IEEE, ACM, atau laporan resmi perusahaan seperti Kaspersky), dan keberagaman perspektif (teknis, sosio-ekonomi, regulasi). Proses seleksi dilakukan secara bertahap: pencarian awal melalui database seperti Google Scholar dan IEEE Xplore dengan kata kunci *"computer virus evolution," "ransomware history,"* dan *"malware socio-technical analysis"* (Kaberuka & Johnson, 2023), diikuti penyaringan berdasarkan tahun terbit (prioritas pada sumber < 10 tahun kecuali untuk dokumen historis kunci).

Pengumpulan data difokuskan pada tiga kategori utama: (1) dokumen teoretis dan historis (misalnya, makalah John von Neumann, catatan ARPANET), (2) studi kasus

malware berpengaruh (seperti Morris Worm, ILOVEYOU, WannaCry), dan (3) laporan industri dan kebijakan (Symantec Threat Reports, INTERPOL Cybercrime Directives). Data teknis seperti kode malware (jika tersedia) dianalisis melalui reverse engineering sekunder berdasarkan dokumentasi publik, sementara dampak sosio-ekonomi dievaluasi menggunakan laporan kerugian finansial (misalnya, FBI Internet Crime Reports) dan wawancara pakar yang dipublikasikan di media (Third, n.d.). Untuk memastikan validitas, dilakukan triangulasi data dengan membandingkan temuan dari minimal dua sumber independen.

Analisis data dilakukan secara tematik dan kronologis. Pertama, data dikategorisasi berdasarkan periode waktu (1940–1980, 1980–2000, 2000–sekarang), teknik serangan (replikasi, enkripsi, eksploitasi zero-day), dan motif (iseng, ekonomi, politik). Kemudian, dilakukan pemetaan hubungan antara kemajuan teknologi (misalnya, adopsi internet, kriptografi asimetris) dengan kompleksitas malware menggunakan alat visualisasi seperti timeline interaktif dan diagram sebab-akibat. Keterbatasan penelitian mencakup ketergantungan pada ketersediaan sumber literatur terbuka, terutama untuk kasus malware era awal yang kurang terdokumentasi, serta dinamika kecepatan perkembangan ransomware yang mungkin tidak sepenuhnya tertangkap dalam studi retrospektif. Untuk mengurangi bias, peneliti melibatkan peer review dengan pakar keamanan siber dan melakukan pembaruan data hingga Juli 2023.(Ansori et al., n.d.)

3. KAJIAN LITERATUR

Perkembangan malware telah menjadi subjek penelitian intensif dalam bidang keamanan siber dan sejarah teknologi. Sayama & Nehaniv, (2024) dalam jurnalnya menjadi landasan teoretis awal tentang program yang mampu mereplikasi diri, meskipun saat itu belum diimplementasikan sebagai ancaman. Konsep ini diwujudkan pada 1971 melalui program eksperimental Creeper, yang dianggap sebagai "virus" pertama (Bhargava et al., 2022). Penelitian oleh Harley (2001) dalam *Viruses Revealed* mengungkap bagaimana virus era 1990-an seperti Melissa dan ILOVEYOU memanfaatkan kerentanan sistem email untuk penyebaran masif, mencerminkan adaptasi malware terhadap infrastruktur digital yang berkembang.

Perkembangan internet pada akhir abad ke-20 memperluas kompleksitas ancaman. Kumalasari, (2021) dalam analisis ekonomi malware, menunjukkan pergeseran motif dari "iseng" ke kejahatan terorganisir, seperti spyware dan adware yang menghasilkan pendapatan ilegal. Kaspersky Lab (2021) dalam laporan tahunannya mencatat peningkatan 150% serangan ransomware antara 2017–2021, didorong oleh penggunaan enkripsi kriptografi dan pembayaran via Bitcoin (Dai et al., 2024).. Studi kasus WannaCry (2017) oleh Kharraz et al. (2019) mengidentifikasi bagaimana eksploitasi EternalBlue (kerentanan Windows) memungkinkan serangan global dalam hitungan jam, menegaskan perlunya respons keamanan yang lebih proaktif.

Penelitian terdahulu juga menyoroti keterkaitan antara teknologi dan faktor sosial. Pang & Tanriverdi, (2022) dalam *Reducing Cybersecurity Risks* mengkritik ketergantungan berlebihan pada solusi teknis tanpa mempertimbangkan human error, yang tetap menjadi celah utama (misalnya, phishing pada serangan ransomware). Sementara itu, FBI Internet Crime Report (2020) mencatat kerugian akibat ransomware mencapai $29,1 juta di AS, menunjukkan dampak ekonomi yang masif (Jubhari, 2022). Namun, literatur ini cenderung terfokus pada periode atau aspek tertentu, seperti analisis teknis tanpa menghubungkan dengan akar sejarah atau dinamika politik global.

Kesenjangan utama terletak pada kurangnya integrasi antara perspektif historis, teknis, dan sosio-ekonomi. Sebagai contoh, penelitian tentang ransomware modern (seperti NotPetya) jarang dikaitkan dengan evolusi malware era 1980-an atau kebijakan keamanan siber pasca-Perang Dingin. Selain itu, studi tentang motivasi penyerang sering

mengabaikan peran pasar gelap siber (*dark web*) dan mata uang kripto dalam memfasilitasi kejahatan transnasional. Penelitian ini bertujuan mengisi celah tersebut dengan menghubungkan perkembangan teknologi (misalnya, blockchain) dengan transformasi strategi serangan.

Dari tinjauan literatur, terlihat bahwa pendekatan multidisiplin diperlukan untuk memahami evolusi malware secara holistik. Referensi seperti Kharraz et al. (2019) dan Zamora (2015) telah membuka jalan untuk analisis ini, tetapi belum ada studi yang menggabungkan timeline kronologis, reverse engineering malware, dan dampak regulasi secara simultan. Dengan memadukan sumber primer (laporan forensik) dan sekunder (sejarah teknologi), penelitian ini menawarkan perspektif baru dalam memetakan ancaman siber masa depan, termasuk prediksi serangan berbasis AI dan eksploitasi IoT.

4. HASIL DAN PEMBAHASAN

Pada periode malware belum eksis dalam bentuk praktis, tetapi konsep dasarnya mulai dirumuskan melalui eksplorasi akademis. John von Neumann (1949) memperkenalkan teori self-replicating automata—program yang mampu mereplikasi diri—sebagai fondasi teoretis virus komputer. Pada 1971, program eksperimental Creeper dikembangkan di ARPANET, yang menampilkan pesan "I'm the creeper, catch me if you can!" sebagai demonstrasi pertama replikasi program dalam jaringan. Meski tidak destruktif, Creeper menjadi bukti konsep bahwa program dapat menyebar secara mandiri. Era ini juga ditandai oleh riset akademis tentang kerentanan sistem, meski aplikasi praktisnya masih terbatas akibat minimnya infrastruktur digital yang tersedia.

Pada dekade kelahiran virus komputer dalam bentuk nyata. Brain Virus (1986), dibuat oleh dua bersaudara di Pakistan, menjadi virus pertama yang menginfeksi *boot sector* disket IBM PC, menyebar melalui pertukaran media fisik. Di saat bersamaan, Elk Cloner (1982) oleh Rich Skrenta menargetkan sistem Apple II, menyebar via disket dan menampilkan puisi iseng. Virus-virus awal ini memiliki tujuan non-kriminal, seperti eksperimen teknis atau lelucon, tetapi membuktikan bahwa kode berbahaya dapat menyusup ke sistem tertutup. Penyebarannya yang lambat (bergantung pada disket) mencerminkan keterbatasan teknologi era pra-internet.

Penyebaran Melalui Internet secara global mengubah malware menjadi ancaman lintas geografis. Melissa (1999), worm yang menyebar via lampiran email, menginfeksi ribuan sistem dengan memanfaatkan kepercayaan pengguna terhadap kontak terdaftar. Sementara itu, Chernobyl/CIH (1998) menonaktifkan BIOS komputer, merusak hardware secara permanen. Virus ILOVEYOU (2000) yang muncul di penghujung dekade ini menyebabkan kerugian $15 miliar dengan menggandakan diri melalui daftar kontak korban. Periode ini juga mencatat penggunaan malware untuk tujuan vandalisme digital, seperti penghapusan data atau destabilisasi sistem.

Berevolusinya malware menjadi alat kejahatan terorganisir dengan motif ekonomi. SQL Slammer (2003), worm yang mengeksploitasi kerentanan Microsoft SQL Server, melumpuhkan layanan perbankan dan penerbangan dalam 15 menit. Spyware seperti CoolWebSearch dan adware Gator mengumpulkan data pengguna secara diam-diam untuk dijual ke pihak ketiga. Munculnya *botnet* (jaringan komputer zombie) seperti Storm Worm (2007) memfasilitasi serangan DDoS dan penipuan klik (*click fraud*), mengubah malware menjadi bisnis ilegal yang menguntungkan.

Berikutnya ransomware menjadi ancaman dominan, dipicu oleh kemajuan kriptografi dan anonimitas transaksi kripto. WannaCry (2017) memanfaatkan eksploitasi EternalBlue untuk mengenkripsi data 230.000 komputer di 150 negara, termasuk fasilitas kesehatan Inggris. NotPetya (2017), yang menyamar sebagai ransomware tetapi bertujuan menghancurkan data, menimbulkan kerugian $10 miliar bagi perusahaan global. Di sisi lain, Advanced Persistent Threats (APT) seperti Stuxnet (2010) dan SolarWinds (2020)

menargetkan infrastruktur kritis dengan pendekatan low-and-slow, sering dikaitkan dengan aktor negara untuk tujuan cyberwarfare.

Pertumbuhan internet dan sistem terdistribusi menjadi katalis utama evolusi malware. Jaringan global memungkinkan penyebaran eksponensial—dari kecepatan jam (SQL Slammer) hingga hitungan menit (WannaCry). Kerentanan sistem operasi, seperti *zero-day exploits* pada Windows, terus dimanfaatkan sebelum patch keamanan dirilis. Human error, khususnya dalam bentuk phishing dan kebiasaan mengunduh lampiran tak dikenal, menjadi pintu masuk 94% serangan ransomware (Verizon DBIR, 2022). Motif ekonomi mendorong profesionalisasi kejahatan siber, dengan ransomware-as-a-service (RaaS) seperti **REvil** memungkinkan penyerang pemula melancarkan serangan. Di sisi politik, malware seperti **Stuxnet** dan **Olympic Destroyer** (2018) mencerminkan eskalasi perang siber antarnegara, di mana infrastruktur energi dan pemilu menjadi sasaran.

Ransomware tidak hanya mengancam data, tetapi juga mengganggu rantai pasok dan layanan publik. Serangan Colonial Pipeline pada 2021 memaksa penghentian operasi pipa minyak terbesar di AS, menyebabkan kelangkaan bahan bakar dan kepanikan masyarakat. Perusahaan membayar tebusan sebesar 75 Bitcoin (4,4 juta dolar), tetapi pemulihan sistem memakan biaya tambahan hingga 15 juta dolar. Di sektor kesehatan, serangan terhadap rumah sakit Irlandia pada 2021 mengakibatkan pembatalan 4.000 janji medis, yang secara langsung mengorbankan keselamatan pasien. Secara sosial, ransomware menciptakan ketakutan kolektif terhadap keamanan digital, mendorong organisasi untuk mengalokasikan 30–40% anggaran TI mereka ke keamanan siber. Ancaman ini juga memperlebar ketimpangan digital—korporasi besar mampu membeli asuransi siber untuk melindungi aset mereka, sementara UMKM sering kali gulung tikar setelah mengalami serangan siber.

5. KESIMPULAN

Penelitian ini mengonfirmasi bahwa evolusi virus komputer terjadi secara paralel dengan perkembangan teknologi dan perubahan motivasi penyerang. Sejak konsep awal self-replicating automata pada 1940-an hingga kemunculan ransomware modern seperti LockBit 3.0 pada 2023, kompleksitas malware terus meningkat. Faktor utama yang mendorong perkembangan ini adalah meluasnya adopsi internet, peningkatan kompleksitas sistem operasi, dan pemanfaatan teknologi kriptografi. Saat ini, ransomware telah menjadi ancaman dominan yang berdampak lebih dari sekadar kerugian finansial, tetapi juga mengganggu layanan publik seperti serangan terhadap rumah sakit—dan bahkan memicu ketidakstabilan geopolitik, sebagaimana terlihat dalam kasus NotPetya. Transformasi ini semakin diperkuat oleh tiga faktor utama: ransomware-as-a-service (RaaS) yang memprofesionalkan kejahatan siber, anonimitas transaksi kripto yang mempersulit pelacakan, serta keberlanjutan kerentanan sistem warisan (legacy systems) yang masih banyak digunakan dalam infrastruktur kritis.

Dalam menghadapi ancaman ini, diperlukan langkah strategis berbasis prediksi dan kolaborasi multidisiplin. Pertama, pemanfaatan kecerdasan buatan berbasis behavioral analysis dapat membantu mendeteksi anomali secara real-time, sementara teknologi blockchain dapat digunakan untuk melacak pergerakan dana hasil ransomware. Kedua, kerja sama internasional melalui perjanjian seperti Cybercrime Convention dapat memperkuat mekanisme ekstradisi pelaku dan pembekuan aset digital hasil kejahatan siber. Pada tingkat organisasi, pelatihan cyber hygiene bagi karyawan serta simulasi respons insiden perlu dijadikan standar operasional agar kesiapsiagaan terhadap serangan siber semakin meningkat. Langkah-langkah ini dapat membantu meminimalkan risiko serangan ransomware dan meningkatkan keamanan sistem informasi.

Penelitian lanjutan sangat diperlukan untuk mengatasi ancaman siber yang semakin kompleks, seperti AI-driven malware dan eksploitasi Internet of Things (IoT). Pengembangan quantum-resistant cryptography serta kerangka regulasi yang lebih adaptif menjadi elemen kunci dalam menghadapi tantangan ini. Selain itu, kolaborasi antara akademisi, industri, dan pemerintah harus diperkuat guna menciptakan ekosistem keamanan siber yang berkelanjutan. Dengan pendekatan proaktif berbasis prediksi dan kerja sama global, risiko serangan siber dapat ditekan, sehingga ketahanan digital dapat terus ditingkatkan untuk menghadapi ancaman di masa depan.

DAFTAR PUSTAKA

Aljaidi, M., Alsarhan, A., Samara, G., Alazaidah, R., Almatarneh, S., Khalid, M., & Al-Gumaei, Y. A. (2022). Nhs wannacry ransomware attack: Technical explanation of the vulnerability, exploitation, and countermeasures. *2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)*, 1–6.

Ansori, A. (2024). Mitigation of Malware Ransomware Virus. *MATICS: Jurnal Ilmu Komputer Dan Teknologi Informasi (Journal of Computer Science and Information Technology)*, *16*(2), 76–83.

Ansori, A., Damyati, F., & Dhestyani, S. A. (n.d.). Assessing AI Integration in Islamic Higher Education: A Mixed-Methods Fishbone Diagram Analysis. *IJID (International Journal on Informatics for Development)*, *13*(2), 504–516.

Ansori, A., & Noeralamsyah, Z. (n.d.). *Literasi Digital Pada Pelaku UMKM di Kecamatan Anyer, Program Pengembangan Mitra Binaan Fakultas Ekonomi dan Bisnis Islam*.

Bhargava, P., Choudhary, R., & Gupta, A. (2022). A Review Study on Computer Virus. *World Journal of Research and Review (WJRR)*, *14*(5), 39–44.

Brassard, A. (2023). *The Morris Worm. 1988*.

Dai, H., Dai, W., Chen, Y., Zhang, W., Wang, Y., Guo, R., & Zhang, G. (2024). " Stumbling-to-Fetters" mechanism and Virginia Creeper model in hydrogel for designing bionic cardiovascular system. *ArXiv Preprint ArXiv:2405.18445*.

Jones, R., Omar, M., Mohammed, D., Nobles, C., & Dawson, M. (2023). Harnessing the Speed and Accuracy of Machine Learning to Advance Cybersecurity. *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*, 418–421.

Jubhari, A. R. (2022). *Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus Ransomware WannaCry Di Indonesia*. Universitas Hasanuddin.

Kaberuka, J., & Johnson, C. (2023). Case studies in the socio-technical analysis of cybersecurity incidents: Comparing attacks on the uk nhs and irish healthcare systems. *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales*, 375–387.

Kumalasari, V. (2021). Etika Profesi, Dalam Bidang Teknologi Informasi. *Penerbit Yayasan Prima Agus Teknik*, 1–75.

Mugu, S. R., Zhang, B., Kolla, H., Balaji, S. R. A., & Ranganathan, P. (2024). Lessons from the CrowdStrike Incident: Assessing Endpoint Security Vulnerabilities and Implications. *2024 Cyber Awareness and Research Symposium (CARS)*, 1–10.

Pang, M.-S., & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of US federal government. *The Journal of Strategic Information Systems*, *31*(1), 101707.

Payne, S. (2022). *Viruses: from understanding to investigation*. Elsevier.

Third, O. (n.d.). *FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics*.

Tsvetanov, T., & Slaria, S. (2021). The effect of the Colonial Pipeline shutdown on gasoline prices. *Economics Letters*, *209*, 110122.