JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Analisis Pola Penyebaran dan Dampak Virus Trojan Horse terhadap Keamanan Sistem Komputer

Gilang Akbar Hadikosyah[1*], Nurul Firzatul Zannah[2], Sara Yulistia[3], M Rizky Febrian[4], Fhadli Maulana[5], Rianda Sulthan[6]
[1,2,3,4,5,6] Program Studi Teknik Informatika, Fakultas Teknik,Universitas Malikussaleh, Indonesia
[1]gilang.240170133@mhs.unimal.ac.id, [2]nurul.240170217@mhs.unimal.ac.id , [3]sara.240170238@mhs.unimal.ac.id, [4]rizky.240170024@mhs.unimal.ac.id, [5]fhadli.220170158@mhs.unimal.ac.id , [6]rianda.210170150@mhs.unimal.ac.id

ABSTRACT

The rapid advancement of information technology has significantly increased the use of computer systems in daily activities. Alongside these developments, cyber threats have also grown, one of the most prevalent being the Trojan Horse virus. Trojan Horse is a type of malware that disguises itself as a legitimate program in order to deceive users and gain unauthorized access to computer systems. This study aims to analyze the patterns of Trojan Horse virus propagation, examine its impacts on computer system security, and identify effective prevention and mitigation strategies. The research method used is a literature review by analyzing books, scientific journals, and credible online sources related to Trojan Horse malware and information system security. The results show that Trojan Horse viruses commonly spread through email attachments, malicious downloads, fake software, and social engineering techniques. The impacts include data theft, system performance degradation, unauthorized remote access, and disruption of organizational operations. Therefore, comprehensive security measures combining technical controls and user awareness are essential to minimize Trojan Horse attacks.

Keywords:
Trojan Horse, computer virus, system security, malware, cyber threat

PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk pendidikan, pemerintahan, bisnis, dan layanan publik. Hampir seluruh aktivitas pengolahan data saat ini bergantung pada sistem komputer dan jaringan internet. Ketergantungan yang tinggi terhadap teknologi tersebut membuat keamanan sistem komputer menjadi aspek yang sangat penting. Namun, kemajuan teknologi juga diiringi dengan meningkatnya ancaman keamanan siber. Salah satu ancaman yang paling sering ditemui adalah malware, khususnya virus Trojan Horse. Trojan Horse menjadi berbahaya karena mampu menyamar sebagai program yang sah sehingga sering kali dijalankan secara tidak sadar oleh pengguna. Serangan Trojan Horse dapat menyebabkan kerugian besar, baik bagi individu maupun organisasi. Kerugian tersebut meliputi pencurian data pribadi, kebocoran informasi rahasia, kerusakan sistem, hingga gangguan operasional. Oleh karena itu, analisis mengenai pola penyebaran dan dampak virus Trojan Horse sangat diperlukan sebagai upaya meningkatkan kesadaran dan keamanan sistem komputer.

TINJAUAN PUSTAKA

Definisi dan Karakteristik Trojan Horse

Trojan Horse adalah jenis malware yang menyamar sebagai program yang dapat dipercaya, dan jika orang menginstalnya tanpa menyadarinya, peretas dapat mengendalikan komputer secara jarak jauh, mencuri data rahasia, atau melakukan tugas-tugas jahat lainnya (Xiao et al., 2025). Berbeda dengan virus atau *worm* yang memiliki kemampuan untuk mereplikasi diri (*self-replicating*) dan menyebar secara mandiri melalui jaringan atau media penyimpanan, Trojan Horse tidak dapat memperbanyak dirinya sendiri. Karakteristik utama Trojan adalah penggunaan teknik social engineering untuk memanipulasi korban dan membuka "pintu belakang" (*backdoor*) bagi penyerang untuk mendapatkan akses tidak sah ke sistem korban.

Mekanisme Kerja Trojan Horse

Menurut Maulana (2022), mekanisme kerja Trojan Horse merupakan proses strategis yang kompleks dan tidak melakukan replikasi otomatis, melainkan sangat bergantung pada interaksi pengguna melalui beberapa tahapan utama. Tahapan tersebut meliputi:

- Penyebaran (*Delivery*): Trojan disampaikan kepada target melalui berbagai vektor seperti email *phishing*, situs web yang dikompromikan (*drive-by download*), unduhan perangkat lunak bajakan, hingga iklan digital berbahaya.
- Instalasi (*Installation*): Trojan memanfaatkan rekayasa sosial untuk memancing pengguna melakukan aksi aktif,

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

seperti membuka lampiran dokumen yang mengandung makro berbahaya atau mengklik tombol instal pada program palsu. Setelah dijalankan, Trojan akan beroperasi di latar belakang untuk menyembunyikan dirinya dari sistem keamanan.

- Eksekusi (*Execution*): Pada tahap ini, fungsi jahat mulai dijalankan, yang dapat bervariasi mulai dari membuka akses pintu belakang (*backdoor*), mencuri kredensial dan data sensitif, hingga mengambil alih kontrol sistem secara penuh melalui *Remote Access Trojan* (RAT). Menurut Damanik et al. (2023), Trojan juga dapat membentuk file malware baru serta mengubah atau merusak file asli yang ada pada sistem komputer.
- Pembersihan Jejak dan Pergerakan Lateral: Untuk menghindari deteksi, Trojan sering menyimpan instruksinya dalam bentuk terenkripsi pada tempat yang tidak biasa seperti kunci registri Windows. Selanjutnya, Trojan dapat melakukan pergerakan lateral untuk mencari dan menyerang perangkat lain yang terhubung dalam jaringan yang sama.

Secara ringkas, Trojan bekerja dengan menyamar sebagai perangkat lunak sah guna mengelabui pengguna agar menginstalnya tanpa curiga, yang kemudian memberikan kemampuan bagi peretas untuk memanipulasi komputer secara jarak jauh dan mencuri informasi sensitif.

Klasifikasi dan Varian Modern Trojan Horse

Terdapat berbagai jenis Trojan yang diklasifikasikan berdasarkan tujuan serangan dan metode eksekusinya, sebagaimana dirangkum dalam Tabel 1.

Tabel 1. Klasifikasi Jenis-Jenis Trojan Horse

Jenis Trojan	Tujuan Utama	Metode Eksekusi Umum	Contoh Trojan Terkenal
Backdoor	Memberikan akses permanen dan jarak jauh ke perangkat korban.	Membuka jalur di firewall serta menyiapkan komunikasi dengan server pengendali (C2).	Back Orifice, Gh0st RAT, ValleyRAT
Banking Trojan	Mengambil informasi finansial dan data login perbankan milik korban.	Melakukan pencatatan tombol, penyadapan formulir, dan tangkapan layar untuk mencuri data.	Zeus, Emotet, AZORult, Coyote
Downloader/Dropper	Mengunduh atau menyalurkan malware lain ke sistem yang terinfeksi.	Terhubung ke server C2 untuk mengunduh muatan tambahan (payload).	Emotet, Ursnif, AZORult
FakeAV	Menipu pengguna agar membayar layanan keamanan palsu.	Menampilkan peringatan fiktif tentang adanya infeksi pada sistem.	Trojan-FakeAV, variasi lainnya
RAT (Remote Access Trojan)	Memberikan penyerang kendali penuh terhadap komputer korban.	Mengaktifkan modul jarak jauh dan menyediakan akses ke terminal sistem	Netbus, Gh0st RAT, SubSeven
Ransom Trojan	Mengenkripsi data korban dan meminta pembayaran tebusan.	Menerapkan enkripsi kuat serta menyembunyikan salinan data yang asli.	CryptoLocker, WannaCry, Crysis
Exploit Trojan	Menyusup dengan mengeksploitasi celah keamanan tanpa perlu interaksi pengguna.	Memakai exploit kit guna memanfaatkan kelemahan pada plugin atau browser.	Beragam varian menggunakan RIG/Kaspersky kits, Operation Aurora
Infostealer/Spy	Mengambil informasi pribadi seperti kredensial, histori, dan data sensitif lainnya.	Melakukan keylogging, menyalin isi clipboard, dan mengekstrak data dari browser.	AZORult, Skygofree, Infostealer Trojan
DDoS Trojan	Membangun jaringan botnet untuk menyerang target secara massal.	Menunggu instruksi dari server C2 untuk menjalankan serangan bersamaan.	Aisuru, Mirai, Gafgyt, XorDDoS

Sumber: Diadaptasi dari Maulana (2022)

Dampak Trojan Horse terhadap Segitiga Keamanan (*CIA Triad*)

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Harahap et al. (2023) menjelaskan bahwa *CIA Triad* merupakan pilar fundamental dalam manajemen risiko keamanan informasi yang terdiri dari tiga indikator utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Keberadaan *Trojan Horse* secara langsung mengancam ketiga pilar tersebut melalui berbagai mekanisme serangan yang merusak. Pada aspek kerahasiaan, Trojan berfungsi sebagai alat utama untuk mencuri informasi sensitif seperti kredensial login, data perbankan, dan nomor kartu kredit tanpa otoritas pengguna. Dampak nyata terlihat pada serangan Trojan perbankan seperti Zeus yang secara masif mencuri data finansial penggunanya. Terkait pilar integritas, Trojan dapat merusak keakuratan data dengan memodifikasi registri sistem atau merubah file-file asli menjadi format yang tidak dapat digunakan. Penelitian Damanik et al. (2023) terhadap sampel Trojan Ryuk.bin membuktikan bahwa malware ini secara aktif membentuk file baru sambil menghancurkan file original pada sistem yang terinfeksi. Akhirnya, pada pilar ketersediaan, Trojan mengganggu operasional sistem dengan membentuk *botnet* untuk serangan DDoS atau mengonsumsi daya CPU yang sangat tinggi sehingga mengakibatkan sistem menjadi lambat dan tidak responsif. Dampak nyata dari gangguan ketersediaan ini terlihat pada serangan siber terhadap *Health Service Executive* (HSE) Irlandia yang memaksa penghentian seluruh sistem TI selama tiga minggu, sehingga melumpuhkan layanan medis nasional (Faul et al., 2022). Kesalingterkaitan ketiga elemen ini sangat penting karena hilangnya satu faktor saja akibat serangan Trojan akan membuat keamanan sistem sangat berisiko dan merusak struktur pertahanan secara keseluruhan.

METODE PENELITIAN

Penelitian ini dilaksanakan dengan rancangan studi kepustakaan (*literature review*) untuk menganalisis karakteristik, pola penyebaran, dan dampak virus Trojan Horse. Pendekatan ini dipilih untuk menyintesis bukti-bukti empiris dan konsep teoritis dari berbagai sumber tanpa melakukan eksperimen laboratorium secara langsung.

Ruang Lingkup dan Objek Penelitian

Objek utama penelitian ini adalah *malware* jenis Trojan Horse dengan fokus pada mekanisme infeksi dan ancamannya terhadap aspek keamanan sistem komputer. Ruang lingkup analisis mencakup varian Trojan yang berkembang dalam periode satu dekade terakhir hingga tahun 2025, serta relevansinya terhadap kerangka kerja keamanan CIA Triad (*Confidentiality, Integrity, Availability*).

Bahan dan Alat Utama

Bahan penelitian terdiri dari data sekunder yang bersumber dari jurnal ilmiah nasional dan internasional bereputasi, laporan riset keamanan siber, dan buku teks akademik. Alat bantu yang digunakan meliputi perangkat lunak manajemen referensi untuk pengorganisasian literatur dan basis data akademik daring seperti ResearchGate, ScienceDirect, dan direktori jurnal nasional.

Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui dokumentasi literatur dengan langkah-langkah sistematis sebagai berikut:

- Pencarian literatur menggunakan kata kunci spesifik: "Trojan Horse analysis", "CIA Triad impact", dan "cybersecurity threats".
- Seleksi sumber berdasarkan kriteria inklusi, yaitu publikasi yang diterbitkan antara tahun 2019–2025 untuk menjamin kemutakhiran data, serta memiliki relevansi langsung dengan topik Trojan Horse dan keamanan sistem.
- Ekstraksi informasi kunci mengenai definisi, klasifikasi, mekanisme teknis, dan studi kasus serangan.

Teknik Analisis

Data yang terkumpul dianalisis menggunakan teknik analisis isi (*content analysis*) secara kualitatif. Proses analisis mencakup tiga tahapan: (1) reduksi data untuk memilah informasi yang esensial; (2) sintesis data untuk mengintegrasikan temuan dari berbagai referensi seperti Damanik et al. (2023) dan Xiao et al. (2025); serta (3) penarikan kesimpulan untuk merumuskan pola umum penyebaran Trojan dan rekomendasi mitigasi yang efektif bagi pengguna sistem komputer.

HASIL DAN PEMBAHASAN

Pola Penyebaran Virus Trojan Horse

Analisis data terbaru menunjukkan bahwa teknik rekayasa sosial (*social engineering*) tetap menjadi vektor serangan paling dominan. Berdasarkan *Cyber Security Breaches Survey 2025* yang dirilis oleh Pemerintah Inggris, 85%

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

bisnis melaporkan mengalami serangan phishing dalam 12 bulan terakhir. Angka ini jauh melampaui jenis serangan teknis lainnya seperti malware spesifik (18%) atau ransomware (6%), sebagaimana terlihat pada Gambar 1.

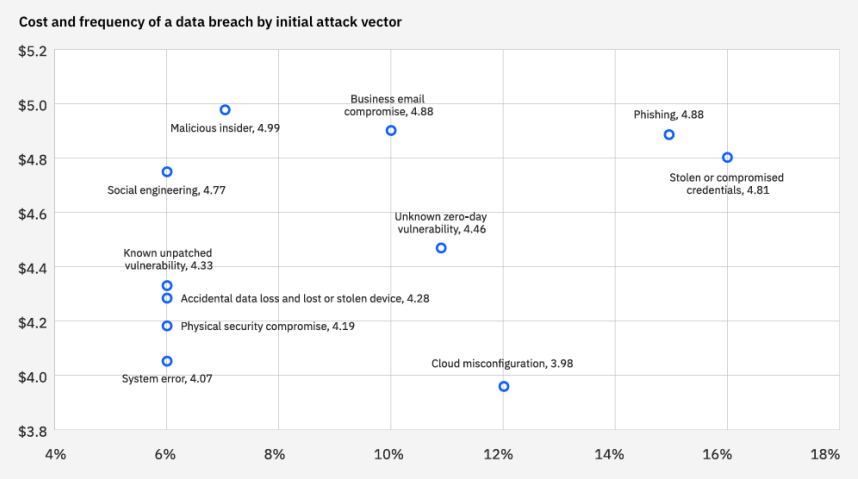
Gambar 1. Proporsi Jenis Serangan Siber yang Dialami Bisnis Tahun 2025 (Sumber: Departement for Science, Innovation and Technology, 2025)

Dampak Trojan Horse terhadap Keamanan Sistem

Infeksi Trojan Horse tidak sekadar gangguan teknis, melainkan serangan strategis yang meruntuhkan tiga pilar keamanan informasi (CIA Triad) secara simultan. Analisis mendalam terhadap mekanisme varian Trojan modern menunjukkan pola kerusakan sebagai berikut:

Analisis Dampak Finansial dan Vektor Serangan

Dalam Cost of a Data Breach Report 2024, IBM (2024) mengungkapkan bahwa Trojan sering kali menjadi pintu masuk utama melalui pencurian kredensial. Sebagaimana terlihat pada Gambar 2, vektor serangan yang melibatkan kredensial curian (*stolen credentials*) menyumbang 16% dari total insiden global dengan rata-rata kerugian mencapai USD 4,81 juta. Angka ini berkorelasi erat dengan maraknya Trojan tipe *Infostealer* (seperti Azorult) yang secara spesifik dirancang untuk mencuri *login* pengguna.



Gambar 2. Biaya dan Frekuensi Pelanggaran Data Berdasarkan Vektor Serangan Awal (Sumber: IBM, 2024)

Kerahasiaan (Confidentiality)

Dampak paling kritis terlihat pada pelanggaran privasi. Trojan mengeksploitasi kredensial yang dicuri untuk memberikan akses tidak sah kepada penyerang. Data IBM (2024) juga mencatat bahwa serangan berbasis kredensial ini membutuhkan waktu paling lama untuk diidentifikasi, yaitu rata-rata 292 hari. Selama periode "diam" ini, Trojan terus menerus memanen data sensitif korban tanpa terdeteksi.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Integritas (*Integrity*) dan Ketersediaan (*Availability*)

Dari sisi integritas, Trojan memanipulasi *registry* sistem untuk memastikan persistensi, membuat sistem tidak lagi dapat dipercaya. Sementara itu, dari sisi ketersediaan, perangkat yang terinfeksi sering direkrut menjadi jaringan *botnet* untuk serangan DDoS, yang menghabiskan sumber daya komputasi dan melumpuhkan layanan. Kerugian akibat gangguan bisnis ini berkontribusi besar terhadap lonjakan total biaya pelanggaran data yang mencapai rekor tertinggi USD 4,88 juta pada tahun 2024 (IBM, 2024).

Studi Kasus Serangan Trojan Horse

Studi kasus yang paling merepresentasikan kompleksitas Trojan modern adalah Emotet. Penelitian longitudinal oleh Boyarchuk et al. (2023), menunjukkan bahwa Emotet telah bertransformasi dari sekadar Banking Trojan menjadi infrastruktur botnet multi-lapis yang sangat tangguh. Dalam analisis telemetri mereka pada tahun 2022, ditemukan bahwa Emotet menggunakan rantai eksekusi (execution chains) yang terus berubah untuk menghindari deteksi, mulai dari penggunaan makro Excel 4.0 hingga file Microsoft HTML Application (HTA).

Lebih jauh, Boyarchuk et al. (2023) menegaskan peran Emotet sebagai distributor utama dalam model bisnis *Malware-as-a-Service (MaaS)*. Emotet tidak hanya mencuri data, tetapi secara aktif menyewakan akses ke mesin korban untuk mendistribusikan muatan berbahaya lainnya, termasuk TrickBot dan Ransomware Ryuk. Mekanisme ini menciptakan serangan bertingkat (*multi-stage attack*) di mana satu infeksi awal yang tampaknya sepele dapat berujung pada kelumpuhan total jaringan organisasi akibat enkripsi ransomware beberapa minggu kemudian.

Strategi Mitigasi dan Penanggulangan Berbasis Network-Based Intrusion Response

Grammatikakis et al. (2021) menekankan bahwa evolusi Trojan seperti Emotet yang menggunakan enkripsi berlapis dan teknik anti-analisis canggih membuat solusi keamanan berbasis host (seperti antivirus tradisional) menjadi kurang efektif. Oleh karena itu, diperlukan strategi pertahanan yang lebih proaktif dan berlapis

Pendekatan Keamanan Hibrida (*Multi-layer Security*)

Menghadapi lanskap komputasi heterogen saat ini, pertahanan tidak bisa lagi hanya mengandalkan pemindaian file di sisi klien. Grammatikakis et al. (2021) mengusulkan integrasi *Intelligent Intrusion Response System (iIRS)* yang menggabungkan solusi berbasis *host* dengan pemantauan jaringan tingkat lanjut. Sistem ini bekerja dengan memodelkan graf keamanan jaringan (*Graphical Network Security Model*) untuk memprediksi jalur serangan potensial dan memblokir komunikasi *Command & Control (C2)* secara otomatis sebelum data sensitif dicuri.

Deteksi Anomali Jaringan (*Network Anomaly Detection*)

Karena Trojan modern menggunakan protokol terenkripsi (seperti HTTPS) untuk menyembunyikan komunikasi jahatnya, deteksi berbasis tanda tangan (*signature-based*) sering kali gagal. Solusinya adalah beralih ke analisis perilaku jaringan yang mampu mendeteksi pola komunikasi mencurigakan, seperti koneksi berulang ke domain tak dikenal atau lonjakan trafik terenkripsi yang tidak wajar pada jam-jam non-operasional (Grammatikakis et al., 2021).

Mitigasi Otomatis dan Isolasi

Untuk meminimalkan dampak penyebaran lateral, sistem pertahanan harus mampu merespons secara otonom. Dalam simulasi yang dilakukan oleh (Grammatikakis et al., 2021), penerapan aturan *firewall* dinamis yang secara otomatis mengisolasi *host* terinfeksi terbukti efektif menghentikan eksfiltrasi data tanpa perlu menunggu intervensi manusia, selaras dengan prinsip *Zero Trust* yang membatasi kepercayaan pada setiap entitas di dalam jaringan.

KESIMPULAN

Penelitian ini berhasil mengidentifikasi bahwa Trojan Horse telah berevolusi menjadi ancaman strategis yang mengeksploitasi celah kolaborasi manusia-mesin, dengan 85% serangan bermula dari teknik rekayasa sosial (*phishing*). Dari hasil yang diperoleh, dampak serangan tidak hanya terbatas pada kerugian finansial masif (rata-rata USD 4,88 juta), tetapi juga merusak pilar resiliensi organisasi. Kour et al. (2024) menyoroti bahwa di era Industri 5.0, serangan siber seperti Trojan tidak hanya mengancam data, tetapi juga keberlanjutan (*sustainability*) operasional industri yang semakin bergantung pada interkonektivitas AI dan *Internet of Things* (IoT).

Manfaat utama penelitian ini adalah memberikan landasan bagi penerapan strategi pertahanan hibrida yang mengintegrasikan aspek teknis (*Zero Trust*) dan aspek manusia. Namun, penelitian ini masih memiliki keterbatasan karena belum mendalami dampak serangan terhadap ekosistem *supply chain* yang saling terhubung. Oleh karena itu, penelitian selanjutnya perlu ditingkatkan untuk mengembangkan kerangka kerja "User-Friendly Security" yang dapat meminimalkan kesalahan manusia tanpa menghambat produktivitas.

Berdasarkan temuan tersebut, rekomendasi utama penelitian ini adalah perlunya pergeseran fokus dari sekadar "deteksi ancaman" menjadi "pembangunan resiliensi siber". Sebagaimana disarankan oleh Kour et al. (2024), organisasi harus mengadopsi model keamanan yang menempatkan manusia sebagai sentral pertahanan (*human-centric approach*),

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

mengingat manusia sering kali menjadi mata rantai terlemah sekaligus pertahanan terakhir dalam menghadapi serangan Trojan yang semakin canggih.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Teknik Informatika Universitas Malikussaleh yang telah memberikan dukungan fasilitas dan lingkungan akademik selama proses penelitian ini. Ucapan terima kasih juga disampaikan kepada rekan-rekan mahasiswa yang telah memberikan masukan, referensi tambahan, serta dukungan diskusi sehingga penyusunan jurnal ini dapat diselesaikan dengan baik.

REFERENSI

Boyarchuk, O., Mariani, S., Ortolani, S., & Vigna, G. (2023). Keeping Up with the Emotets: Tracking a Multi-infrastructure Botnet. *Digital Threats: Research and Practice*, *4*(3). https://doi.org/10.1145/3594554

Damanik, A. R., Seta, H. B., & Theresiawati, T. (2023). Analisis Trojan Dan Spyware Menggunakan Metode Hybrid Analysis. *Jurnal Ilmiah Matrik*, *25*(1), 89–97. https://doi.org/10.33557/jurnalmatrik.v25i1.2327

Departement for Science, I. and T. (2025). *Cyber Security Breaches Survey 2025*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

Faul, C., Robinson, J., Carey, J., McArdle, O., Ryan, L., Woods, R., & McClean, B. (2022). Effect of the Cyberattack Targeting the Irish Health System in May 2021 on Radiation Treatment at St. Luke's Radiation Oncology Network. *Advances in Radiation Oncology*, *7*(5), 100993. https://doi.org/10.1016/j.adro.2022.100993

Grammatikakis, K. P., Koufos, I., Kolokotronis, N., Vassilakis, C., & Shiaeles, S. (2021). Understanding and mitigating banking trojans: From Zeus to emotet. *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021*, *July*, 121–128. https://doi.org/10.1109/CSR51186.2021.9527960

Harahap, A. H. H., Andani, C. D., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen Dan Pemasaran Digital*, *1*(2), 73–83. https://doi.org/10.38035/jmpd.v1i2.34

IBM. (2024). Cost of a Data Breach Report Table of contents. *IBM Report*.

Kour, R., Karim, R., Dersin, P., & Venkatesh, N. (2024). Cybersecurity for Industry 5.0: trends and gaps. *Frontiers in Computer Science*, *6*(July). https://doi.org/10.3389/fcomp.2024.1434436

Maulana, M. S. (2022). *Laporan Riset Mendalam: Analisis Komprehensif tentang Trojan Pengenalan dan Sejarah Trojan*. https://www.researchgate.net/publication/394511234

Xiao, W., Xu, X., Chen, J., Zhang, H., & Zhang, Y. (2025). *Trojan Virus Detection and Classification Based on Graph Convolutional Neural Network Algorithm*. *3*(2), 2–6.