JIKUM
JURNAL ILMU KOMPUTER

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

Kajian Ancaman Malware dan Upaya Pencegahan melalui Penguatan Keamanan Sistem Komputer

Khaira Ulvi[1], Garwira Rasikha[2*], Raudatul Aulia[3] , Shella Rika[4] , Maulida Hidayani[5]
[1,2,3,4,5]Universitas Malikusssaleh, Indonesia
[1]khaira.240170059@mhs.unimal.ac.id,[2]garwita.240170041@mhs.unimal.ac.id,[3]raudatul.240170033@mhs.unimal.ac.id,
[4]shella.240170032@mhs.unimal.ac.id ,[5]maulida.240170143@mhs.unimal.ac.id

ABSTRACT

Malware is one of the most significant threats to computer system security and continues to evolve alongside rapid advances in information technology. The increasing reliance on digital systems in various sectors has made organizations and individuals more vulnerable to malware attacks, which can result in data breaches, system failures, financial losses, and operational disruptions. This study aims to examine the various types of malware threats and to analyze prevention strategies through strengthening computer system security. The research method employed is a systematic literature review by analyzing scientific journal articles, books, and official cybersecurity reports published between 2018 and 2024. The results indicate that malware such as viruses, worms, trojans, ransomware, and spyware exhibit different attack vectors, behaviors, and impacts. Effective prevention measures include the implementation of updated antivirus software, firewalls, regular system and application updates, data backup mechanisms, user awareness training, and the enforcement of organizational security policies. A comprehensive approach to strengthening computer system security is essential to reducing malware risks and enhancing overall information security resilience.

Keywords: *malware, computer security, cyber threats, system protection*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era digital telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk pendidikan, pemerintahan, bisnis, dan industri. Pemanfaatan sistem komputer dan jaringan internet yang semakin luas memberikan kemudahan dalam pengolahan data, komunikasi, serta penyimpanan informasi. Namun, kemajuan tersebut juga diiringi dengan meningkatnya ancaman keamanan siber yang semakin kompleks, salah satunya adalah malware.

Malware merupakan perangkat lunak berbahaya yang dirancang untuk menyusup ke dalam sistem komputer dengan tujuan merusak sistem, mencuri data, memata-matai aktivitas pengguna, atau mengambil alih kendali sistem tanpa izin. Penyebaran malware dapat terjadi melalui berbagai media, seperti email phishing, unduhan aplikasi tidak resmi, situs web berbahaya, serta eksploitasi celah keamanan pada sistem operasi dan aplikasi. Dampak serangan malware tidak hanya bersifat teknis, tetapi juga dapat menimbulkan kerugian finansial, gangguan operasional, dan kebocoran data sensitif.

Seiring meningkatnya ketergantungan terhadap sistem komputer dan layanan digital, keamanan informasi menjadi aspek yang sangat krusial. Banyak pengguna dan organisasi masih memiliki tingkat kesadaran keamanan siber yang rendah, sehingga sistem yang digunakan rentan terhadap serangan malware. Selain itu, perkembangan malware modern yang semakin canggih, seperti ransomware dan fileless malware, membuat metode pengamanan konvensional menjadi kurang efektif.

Oleh karena itu, diperlukan kajian yang komprehensif mengenai ancaman malware serta upaya pencegahan yang dapat dilakukan melalui penguatan keamanan sistem komputer. Penelitian ini bertujuan untuk mengkaji jenis-jenis malware yang umum ditemukan, menganalisis dampak serangan malware terhadap sistem komputer, serta mengidentifikasi strategi pencegahan yang efektif guna meningkatkan keamanan sistem komputer.

TINJAUAN PUSTAKA

Konsep dan Definisi Malware

Malware merupakan istilah umum untuk berbagai perangkat lunak berbahaya yang dirancang untuk mengganggu, merusak, atau memperoleh akses tidak sah ke sistem komputer. Menurut Stallings (2018), malware memanfaatkan kelemahan sistem keamanan dan sering kali beroperasi tanpa disadari pengguna. Penyebarannya dapat melalui file, jaringan, maupun media penyimpanan eksternal.

JIKUM
JURNAL ILMU KOMPUTER

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

Jenis-Jenis Malware

Virus menyebar dengan menempel pada file atau program dan aktif ketika file dijalankan. Worm mampu menyebar secara mandiri melalui jaringan. Trojan horse menyamar sebagai aplikasi sah untuk mengelabui pengguna. Spyware memantau aktivitas pengguna dan mencuri informasi sensitif. Ransomware mengenkripsi data korban dan meminta tebusan; Behl dan Behl (2017) menyebutnya sebagai ancaman serius karena dapat melumpuhkan sistem. Adware menampilkan iklan berlebihan yang mengganggu kinerja.

Dampak Malware terhadap Sistem Komputer

Dampak serangan malware meliputi penurunan kinerja, kerusakan data, kebocoran informasi, hingga gangguan layanan. Pada organisasi, malware dapat menghentikan operasional dan menurunkan kepercayaan pengguna, sehingga perlindungan menyeluruh menjadi kebutuhan utama.

METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur sistematis. Data diperoleh dari berbagai sumber pustaka yang relevan, meliputi jurnal ilmiah nasional dan internasional, buku teks keamanan komputer, serta laporan resmi dari lembaga keamanan siber. Proses pencarian literatur dilakukan melalui basis data seperti Google Scholar, IEEE Xplore, dan ScienceDirect dengan kata kunci "malware", "computer security", dan "cyber threats".

Sebanyak 20 artikel dan sumber pustaka yang diterbitkan dalam rentang tahun 2018 hingga 2024 dipilih berdasarkan relevansi dan kredibilitasnya. Tahapan penelitian meliputi identifikasi literatur, klasifikasi jenis malware, analisis dampak serangan malware, serta evaluasi upaya pencegahan yang telah diusulkan oleh penelitian sebelumnya. Data yang diperoleh dianalisis secara deskriptif dan komparatif untuk menghasilkan gambaran komprehensif mengenai ancaman malware dan strategi penguatan keamanan sistem komputer.

HASIL DAN PEMBAHASAN

Perkembangan Ancaman Malware

Ancaman malware berkembang seiring kemajuan teknologi dan konektivitas. Malware modern seperti polymorphic dan fileless malware mampu menghindari deteksi tradisional, meningkatkan risiko serangan pada individu dan organisasi.

Dampak Serangan Malware terhadap Sistem Komputer

Serangan malware menyebabkan kerusakan sistem, pencurian data, penurunan kinerja jaringan, dan gangguan operasional. Ringkasan jenis malware dan dampaknya disajikan pada Tabel 1.

Tabel 1. Jenis Malware dan Dampaknya terhadap Sistem Komputer

Jenis Malware	Cara Kerja / Penyebaran	Dampak terhadap Sistem
Virus	Menempel pada file atau program dan aktif saat dijalankan	Kerusakan file dan penurunan kinerja sistem
Worm	Menyebar secara mandiri melalui jaringan	Membebani jaringan dan mempercepat penyebaran serangan
Trojan	Menyamar sebagai aplikasi legal	Pengambilalihan sistem dan pencurian data
Spyware	Memantau aktivitas pengguna secara diam-diam	Kebocoran data pribadi dan kredensial
Ransomware	Mengenkripsi data dan meminta tebusan	Kehilangan akses data dan gangguan operasional

Berdasarkan Tabel 1, setiap jenis malware memiliki karakteristik serangan dan dampak yang berbeda. Oleh karena itu, strategi pengamanan sistem komputer harus disesuaikan dengan jenis ancaman yang dihadapi.

Upaya Pencegahan melalui Penguatan Keamanan Sistem

Upaya pencegahan malware perlu dilakukan melalui penguatan keamanan sistem komputer secara menyeluruh, baik dari aspek teknis maupun non-teknis. Pencegahan yang efektif harus diterapkan secara berlapis untuk meminimalkan peluang masuknya malware serta mengurangi dampak serangan.

JIKUM
JURNAL ILMU KOMPUTER

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

Tabel 2. Strategi Pencegahan Malware pada Sistem Komputer

Strategi Pencegahan	Implementasi	Manfaat
Antivirus dan Anti-Malware	Instalasi dan pembaruan rutin perangkat lunak keamanan	Mendeteksi dan menghapus malware secara otomatis
Firewall	Konfigurasi firewall pada sistem dan jaringan	Memblokir akses tidak sah dan serangan dari luar
Pembaruan Sistem	Update sistem operasi dan aplikasi secara berkala	Menutup celah keamanan yang dapat dieksploitasi malware
Backup Data	Pencadangan data secara terjadwal	Memulihkan data saat terjadi serangan ransomware
Edukasi Pengguna	Pelatihan keamanan siber dan kesadaran phishing	Mengurangi risiko serangan berbasis kesalahan manusia

Berdasarkan Tabel 2, dapat disimpulkan bahwa pencegahan malware harus dilakukan secara menyeluruh dan berkelanjutan. Kombinasi antara teknologi keamanan, kebijakan yang jelas, serta kesadaran pengguna merupakan kunci utama dalam memperkuat keamanan sistem komputer. Organisasi yang menerapkan strategi ini secara konsisten cenderung memiliki tingkat risiko serangan malware yang lebih rendah.

KESIMPULAN

Malware merupakan salah satu ancaman serius terhadap keamanan sistem komputer yang terus berkembang seiring dengan kemajuan teknologi informasi. Setiap jenis malware memiliki karakteristik serangan dan dampak yang berbeda-beda, mulai dari kerusakan sistem hingga pencurian data sensitif. Oleh karena itu, keamanan sistem komputer tidak dapat ditangani secara parsial, melainkan harus diperkuat melalui pendekatan yang komprehensif.

Penguatan keamanan sistem komputer dapat dilakukan melalui penerapan teknologi keamanan seperti antivirus, firewall, dan pembaruan sistem secara berkala, serta didukung oleh kebijakan keamanan organisasi yang jelas. Selain itu, peningkatan kesadaran dan edukasi pengguna memiliki peran penting dalam mencegah serangan malware, khususnya yang memanfaatkan rekayasa sosial. Dengan penerapan strategi keamanan yang terpadu, risiko serangan malware dapat diminimalkan dan ketahanan sistem komputer dapat ditingkatkan.

Penelitian ini diharapkan dapat menjadi referensi dalam memahami ancaman malware dan upaya pencegahan yang efektif. Penelitian selanjutnya disarankan untuk mengkaji implementasi penguatan keamanan sistem komputer secara empiris pada lingkungan tertentu guna memperoleh hasil yang lebih spesifik dan aplikatif.

REFERENSI

Behl, A., & Behl, K. (2017). Cyberwar: The next threat to national security and what to do about it. Oxford University Press.

Kaspersky. (2022). What is malware? https://www.kaspersky.com

National Institute of Standards and Technology. (2020). Guide to malware incident prevention and handling (SP 800-83 Rev.1). NIST.

Pressman, R. S. (2015). Software engineering: A practitioner’s approach (8th ed.). McGraw-Hill.

Stallings, W. (2018). Effective cybersecurity: A guide to using best practices and standards. Addison-Wesley.

Szor, P. (2005). The art of computer virus research and defense. Addison-Wesley.

Tanenbaum, A. S., & Bos, H. (2015). Modern operating systems (4th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning.

Yadav, S., & Rao, S. (2016). Malware detection and prevention techniques. International Journal of Computer Applications, 144(5), 1–5.

Zimba, A., & Wang, Z. (2021). Cyber security threats and malware attacks. Journal of Information Security, 12(2), 85–97.