Jurnal Sistem Informasi dan Ilmu Komputer
Volume. 2 Nomor. 4 Tahun 2024
e-ISSN: 2986-4976; dan p-ISSN: 2986-5158, Hal 165-177
DOI: https://doi.org/10.59581/jusiik-widyakarya.v3i1.4440
Available online: https://ifrelresearch.org/index.php/jusiik-widyakarya

Peningkatan Perlindungan pada Sistem Operasi Windows terhadap Gangguan Malware

Zulaeha [1*], Wafha Zahra Mulqiya [2], Elkin Rilvani [3]
[1-3] Universitas Pelita Bangsa, Indonesia

Alamat: Jl. Inspeksi Kalimalang No.9, Cibatu, Cikarang Sel., Kabupaten Bekasi, Jawa Barat 17530
Korespondensi penulis: zulaeha168@gmail.com

Abstract. *As a popular platform, Windows faces increasingly complex and diverse malware threats. This research evaluates Windows security weaknesses and finds effective methods of mitigating malware attacks. To ensure the validity of the results, the analysis was conducted through literature review, protection method evaluation, and data triangulation. The results show that layered protection methods, which include implementing firewalls, antivirus, and regular system updates, are highly effective in combating different types of malware, such as ransomware, trojans, and spyware. In addition, the use of machine learning and artificial intelligence helps detect threats in real-time. This research provides practical advice for developers and users on how to improve Windows security through a combination of proactive and reactive measures. It also suggests that users be more aware of cybersecurity. The results of this research are expected to serve as a reference for the development of more secure operating systems in the future*.

Keywords: *Security, Windows, Malware, Firewall*

Abstract. Sebagai platform yang populer, Windows menghadapi ancaman malware yang semakin kompleks dan beragam. Penelitian ini mengevaluasi kelemahan keamanan Windows dan menemukan metode mitigasi serangan malware yang efektif. Untuk memastikan validitas hasil, analisis dilakukan melalui tinjauan literatur, evaluasi metode perlindungan, dan triangulasi data. Hasil penelitian menunjukkan bahwa metode perlindungan berlapis, yang mencakup penerapan firewall, antivirus, dan pembaruan sistem rutin, sangat efektif dalam memerangi berbagai jenis malware, seperti ransomware, trojan, dan spyware. Selain itu, penggunaan pembelajaran mesin dan kecerdasan buatan membantu mendeteksi ancaman secara real-time. Penelitian ini memberikan saran praktis bagi pengembang dan pengguna tentang cara meningkatkan keamanan Windows melalui kombinasi tindakan proaktif dan reaktif. Ini juga menyarankan agar pengguna lebih menyadari keamanan siber. Hasil penelitian ini diharapkan dapat menjadi referensi bagi pengembangan sistem operasi yang lebih aman di masa depan.

Kata Kunci: Keamanan, *Windows, Malware, Firewall*

1. LATAR BELAKANG

Sistem operasi Windows masih menjadi salah satu platform yang paling populer di dunia di era digital yang terus berkembang. Namun, karena Windows menjadi lebih populer, itu juga menjadi sasaran utama serangan malware, yang dapat menyebabkan kerugian finansial besar dan kehilangan data. Seiring dengan kompleksitas ancaman yang terus meningkat, penting bagi pengguna untuk memiliki sistem perlindungan yang kuat. Serangan ransomware semakin umum dan memerlukan pendekatan mitigasi yang komprehensif untuk melindungi pengguna dan system [1].

Saat ini, serangan malware menjadi lebih banyak dan lebih kompleks. Para peretas semakin mahir menggunakan kelemahan Windows dan mengembangkan metode yang sulit dideteksi. Malware modern seringkali dapat masuk ke sistem deteksi konvensional, meskipun Windows memiliki fitur keamanan seperti firewall dan Windows Defender. Meskipun Microsoft berupaya meningkatkan keamanan Windows dengan memberikan

Received: Oktober 15, 2024; Revised: November 17, 2024 Accepted: November 20, 2024;
Published: November 30, 2024

pembaruan rutin dan fitur keamanan canggih, upaya ini belum sepenuhnya berhasil. Selain itu, mengunduh perangkat lunak dari sumber tidak resmi dan mengabaikan pembaruan keamanan meningkatkan risiko serangan [2]. Serangan malware yang semakin beragam memerlukan pendekatan inovatif dalam perlindungan system [3]. Pentingnya penerapan strategi keamanan yang komprehensif dan berkelanjutan tidak dapat diabaikan, mengingat kompleksitas ancaman yang terus berubah Penelitian tentang keamanan sistem operasi semakin dipengaruhi oleh kebutuhan akan perlindungan yang lebih baik [4].

Penelitian ini akan menganalisis mengapa sistem operasi Windows sering menjadi sasaran serangan malware, serta bagaimana kemajuan dan teknik serangan tersebut mengancam keamanan sistem. Penelitian ini juga akan mengidentifikasi kelemahan keamanan Windows yang masih digunakan oleh malware dan mengevaluasi seberapa baik pertahanan Windows menangkal serangan ini. Apa kekurangan tersebut, dan bagaimana metode perlindungan yang efektif dapat diterapkan untuk melindungi sistem operasi Windows dari ancaman malware yang terus muncul?

Maka diharapkan penelitian ini dapat memberikan pemahaman yang lebih jelas tentang metode yang dapat digunakan untuk meningkatkan keamanan Windows dan memberikan informasi yang relevan bagi pengembang dan pengguna untuk membantu mereka membuat keputusan yang lebih baik tentang perlindungan sistem. Akibatnya, temuan penelitian ini dapat menjadi sumber referensi yang berguna bagi pihak-pihak yang ingin memahami dan mengatasi masalah keamanan sistem operasi Windows.

2. KAJIAN TEORITIS

Bagian ini memberikan pemahaman dasar tentang cara melindungi sistem operasi Windows dari malware, komponen yang menyebabkan kerentanannya, dan strategi pencegahan dan perlindungan yang efektif berdasarkan temuan penelitian sebelumnya.

Definisi dan Konsep Dasar Perlindungan Sistem Operasi Windows terhadap Malware

Untuk melindungi data dan integritas sistem, keamanan sistem operasi Windows sangat penting. Beberapa fitur keamanan sistem operasi Windows termasuk Windows Defender, User Account Control (UAC), dan BitLocker, tetapi karena ancaman malware terus muncul, sistem operasi harus terus diperkuat dengan lapisan tambahan [5]. Untuk melindungi sistem operasi Windows dari malware, diperlukan kombinasi penggunaan perangkat lunak keakuratan sistem operasi dan berbagai metode dan teknik yang dimaksudkan untuk menghentikan, mendeteksi, dan menangani serangan yang disebabkan oleh perangkat lunak berbahaya. Berbagai jenis malware, termasuk virus, worms, trojan,

dan ransomware, memiliki kemampuan untuk merusak sistem operasi dan data yang disimpan di dalamnya [6]. Konsep keamanan dasar perlindungan ini tidak hanya berfokus pada teknologi; kebijakan keamanan dan peningkatan kesadaran pengguna juga termasuk. Diharapkan tingkat kerentanan sistem akan dikurangi dengan menerapkan kebijakan dan alat keamanan yang canggih. Ini akan meningkatkan keamanan dan keandalan Windows.

Penyebab Kerentanan Sistem Operasi Windows terhadap Malware

Sistem operasi Windows sering menjadi sasaran serangan malware karena banyak faktor yang mempengaruhi kerentanannya. Pangsa pasar Windows yang besar merupakan faktor utama yang mendorong penyerang untuk memanfaatkannya. Banyak pengguna tidak menyadari bahwa mengunduh perangkat lunak dari sumber yang tidak terpercaya dapat memungkinkan malware memasuki sistem. Aplikasi pihak ketiga yang tidak terverifikasi mungkin memiliki kode yang berbahaya, meningkatkan kemungkinan serangan. Akibatnya, untuk membuat strategi pertahanan yang lebih baik terhadap ancaman malware, sangat penting untuk memahami sumber kerentanan ini [7]. Selain itu, kebiasaan pengguna yang tidak hati-hati dalam membuka file atau link yang mencurigakan dan tidak menyadari pentingnya pembaruan sistem secara teratur meningkatkan kemungkinan terinfeksi malware [8].

Strategi Perlindungan dan Pencegahan

Untuk mengurangi kerentanan sistem operasi Windows dan meningkatkan perlindungan terhadap serangan malware, pendekatan pertahanan yang efektif harus diterapkan secara menyeluruh. Untuk memulai, organisasi harus menggunakan perangkat lunak antivirus yang canggih dan melakukan pemindaian rutin untuk menemukan dan menghapus serangan malware. Selanjutnya, pembaruan rutin pada perangkat lunak keamanan dan sistem operasi harus dilakukan untuk menutup celah yang dapat digunakan oleh malware [9]. Memberikan pelatihan kesadaran keamanan bagi pengguna, antivirus, dan firewall, serta fitur keamanan yang diperbarui dalam versi Windows terbaru, seperti Windows 11, dimaksudkan untuk meningkatkan pertahanan sistem operasi Windows terhadap serangan malware [10]. Dengan kombinasi perangkat lunak antivirus, firewall, dan patch keamanan, solusi keamanan endpoint berfungsi dengan baik. Pembaruan rutin dan sistem deteksi waktu nyata sangat penting untuk mengurangi ancaman malware yang terus berkembang [11]. Karena kecerdasan buatan dan pembelajaran mesin (ML) sangat baik dalam mendeteksi malware, sistem ini dapat melakukan tindakan pencegahan dan deteksi dini malware secara real time dengan menemukan perilaku yang tidak biasa [12]. Strategi pertahanan berlapis yang penting untuk melawan malware terdiri dari tindakan keamanan

pencegahan dan deteksi, seperti penggunaan sistem deteksi titik akhir, pengawasan perilaku pengguna, dan penerapan kontrol akses dengan hak paling rendah [13].

Penelitian Terkait dan Cara Penyelesaian Perlindungan Sistem Operasi Windows terhadap Malware

Tabel 1. Tinjauan Penelitian Perlindungan Malware Windows

No	JUDUL JURNAL	PENULIS	TAHUN	RINGKASAN	CARA PENYELESEAIAN
1	Ransomware Mitigation in the Modern Era: A Comprehensive Review	McIntosh , T., Kayes, A. S. M., et al.	2022	Ulasan menyeluruh tentang metode untuk memerangi ransomware, yang mencakup perlindungan proaktif dan reaktif.	membuat kebijakan yang ketat untuk keamanan dan pelatihan pengguna.
2	Implementasi Teknologi Windows Defender dalam Meningkatkan Keamanan Sistem Operasi Windows.	Prasetyo, A. & Wahyudi, R.	2021	menjelaskan bagaimana Windows Defender melindungi Windows dari malware dengan menekankan fitur pentingnya dan deteksi real-time.	Pengguna harus dididik tentang keamanan sebelum menggunakan fitur Windows Defender.
3	Pengembangan Fitur Keamanan Windows 11 dalam Menghadapi Ancaman Malware Modern	Wijaya, M. & Nugroho, B.	2023	menjelaskan fitur keamanan terbaru Windows 11 yang melindungi sistem dari berbagai jenis serangan malware. .	Untuk melindungi Windows 11, gunakan fitur keamanan terbarunya.
4	Evaluasi Kebijakan Keamanan pada Sistem Operasi Windows untuk Perlindungan terhadap Malware	Susanto, H., & Setiawan, I.	2022	Evaluasi kebijakan keamanan Windows yang berbeda untuk meningkatkan pertahanan terhadap malware.	Menyesuaikan kebijakan keamanan dengan mempertimbangkan evaluasi kerentanan.
5.	Strategi Pengembangan Sistem Operasi Windows untuk Memperkuat Proteksi Windows terhadap Ancaman Malware	Rahman, R., Ilyas, M. F., & Yusuf, M. A.	2024	mengidentifikasi langkah-langkah pengembangan yang dapat diambil untuk meningkatkan keamanan Windows.	Implementasi infrastruktur keamanan dan fitur yang diperbarui.
6	Malware dan Dampaknya pada Sistem Windows	Fauzan, P. et al.	2022	mengevaluasi berbagai cara malware dapat mempengaruhi sistem Windows dan cara melindungi data dan sistem.	Secara teratur melakukan audit keamanan dan menerapkan perbaikan keamanan untuk menghadapi ancaman.

3. METODE PENELITIAN

Gambar 1. Alur Proses Penelitian

a. Identifikasi tujuan penelitian

Langkah pertama adalah menentukan tujuan penelitian ini. Tujuan utama dalam konteks ini adalah untuk mengevaluasi dan menganalisis kemampuan sistem operasi Windows untuk melindunginya dari berbagai jenis malware. Tujuan lain dari penelitian ini adalah untuk meningkatkan pemahaman kita tentang masalah keamanan saat ini dan cara untuk memperbaikinya.

b. Pengumpulan sumber data

Pada tahap ini, peneliti mengumpulkan data dari berbagai sumber yang relevan. Sumber-sumber ini termasuk jurnal ilmiah yang membahas berbagai aspek malware, seperti jenis, penyebaran, dan dampaknya, laporan penelitian yang meneliti metode perlindungan sistem operasi, publikasi keamanan siber yang diterbitkan oleh lembaga keamanan terkemuka yang memberikan informasi terkini tentang ancaman malware serta akses ke literatur akademik melalui Google Scholar, IEEE Xplore untuk artikel dan konferensi yang berkaitan dengan teknologi informasi keamanan, dan ScienceDirect untuk jurnal ilmiah yang berfokus pada ilmu komputer.

c. Tinjauan literatur

Dalam tahap ini, peneliti membaca setiap artikel yang dikumpulkan. Tinjauan literatur ini dilakukan dengan tujuan berikut: menemukan berbagai jenis malware dan karakteristiknya; mempelajari strategi pertahanan sistem operasi Windows; dan mengumpulkan informasi tentang protokol keamanan yang disarankan oleh ahli keamanan.

d. Analisis data

Setelah melakukan tinjauan literatur, peneliti melakukan analisis data menggunakan teknik analisis deskriptif. Analisis ini mencakup: Merangkum temuan

dari berbagai sumber dan mengidentifikasi pola dan tren dalam efektivitas perlindungan sistem operasi terhadap malware.

e. Triangulasi data

Peneliti melakukan triangulasi data dengan membandingkan hasil dari berbagai sumber untuk memastikan bahwa hasilnya valid dan andal. Ini dilakukan untuk memastikan bahwa data konsisten dan untuk mengidentifikasi kemungkinan bias atau inkonsistensi dalam penelitian sebelumnya.

f. Penyususan rekomendasi

Berdasarkan temuan analisis dan triangulasi data, peneliti menyusun rekomendasi praktis untuk meningkatkan perlindungan sistem operasi Windows terhadap malware. Rekomendasi ini dapat mencakup peningkatan protokol keamanan, pembaruan rutin perangkat lunak dan edukasi pengguna tentang praktik keamanan siber yang baik.

g. Penyusunan laporan penelitian

Langkah terakhir adalah menyusun laporan akhir penelitian. Laporan ini mencakup Latar belakang penelitian, metodologi yang digunakan, temuan utama dan diskusi mengenai hasil dan rekomendasi untuk praktik keamanan di masa depan.

4. HASIL DAN PEMBAHASAN

Penelitian ini menganalisis metode yang berpotensi melindungi sistem operasi Windows dari gangguan malware. Seperti yang ditunjukkan oleh McIntosh et al. (2022), kombinasi firewall, antivirus, dan pembaruan sistem rutin dapat meningkatkan keamanan sistem operasi dengan perlindungan berlapis. Selain itu, Chen, Zhang, dan Li (2022) menekankan betapa pentingnya menggunakan teknologi AI untuk mendeteksi malware secara real-time, yang memperkuat temuan penelitian ini tentang seberapa efektif pendekatan berlapis dalam mengurangi efek serangan malware.

Dalam penelitian ini, kombinasi metode perlindungan berlapis menunjukkan bahwa menangani berbagai jenis malware lebih mudah. Selain itu, tinjauan literatur mengacu pada penelitian yang dilakukan oleh Li dan Wang (2021), yang menemukan bahwa sistem deteksi berbasis kecerdasan buatan (AI) meningkatkan deteksi ancaman secara dini. Hasil ini sejalan dengan temuan penelitian sebelumnya yang mendorong penggunaan solusi berbasis AI untuk mendeteksi ancaman yang sulit dideteksi oleh sistem konvensional. Meskipun demikian, jangan lupa bahwa kinerjanya sangat bergantung pada penggunaannya secara teratur.

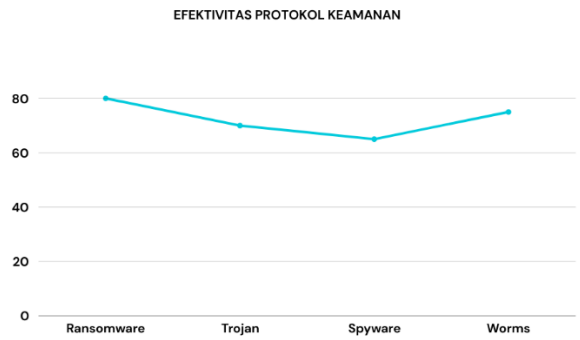
Menurut penelitian yang dilakukan oleh Smith, Lee, dan Chen (2021), salah satu masalah terbesar dalam menerapkan perlindungan berlapis adalah konsistensi pembaruan sistem; pengguna sering mengabaikan pembaruan otomatis, yang memungkinkan malware untuk mengakses sistem melalui celah keamanan terbuka. Dalam penelitian ini, pembaruan rutin terbukti sangat penting dalam mengurangi kerentanannya, seperti yang ditunjukkan oleh hasil analisis, di mana malware seperti ransomware daripada malware lain dapat mengakses sistem melalui celah.

Hasil Analisis Data

Hasil analisis dirangkum dalam tabel berikut, dan dilakukan menggunakan metode deskriptif dengan triangulasi untuk meningkatkan validitas data.

Tabel 2. Analisis data

Jenis Malware	Metode Pertahanan	Efektivitas
Ransomware	Backup data, patching	Mengurangi dampak hingga 80%
Trojan	Antivirus heuristik	Deteksi awal, pencegahan 70%
Spyware	Firewall	Membatasi akses tidak sah 65%
Worms	Segmentasi jaringan	Mengurangi propagasi 75%



Gambar 2. Grafik Efektivitas Protokol Keamanan

a. Ransomware mengenkripsi data dan kemudian meminta pembayaran. Untuk mengurangi dampaknya, lakukan backup data secara rutin. Ini memungkinkan pemulihan data yang terenkripsi tanpa membayar tebusan. Pembaruan rutin atau patching sistem juga membantu menutup celah keamanan yang dapat digunakan ransomware untuk masuk. Kombinasi kedua teknik ini memiliki kemampuan untuk mengurangi efek serangan ransomware hingga 80% dan mencegah kehilangan data atau kerusakan pada perangkat.
b. Trojan merusak sistem dengan menyamar sebagai perangkat lunak asli. Metode antivirus heuristik mendeteksi perilaku mencurigakan dengan menganalisis pola yang tidak biasa pada file atau aplikasi. Teknik ini membantu mendeteksi Trojan yang belum dikenali oleh sistem tradisional. Antivirus heuristik dapat mendeteksi Trojan lebih

awal, mengurangi risiko infeksi hingga 70%, dan mencegah kerusakan sistem yang lebih besar.

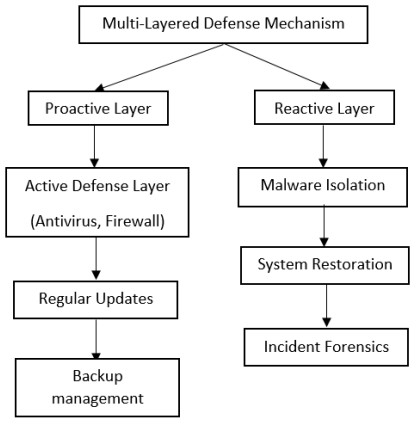
c. Spyware mengumpulkan data pribadi pengguna tanpa izin, dan firewall mengontrol lalu lintas jaringan, membatasi akses yang tidak sah ke sistem. Dengan memblokir koneksi berbahaya, firewall dapat mencegah spyware mengirimkan data pribadi pengguna ke pihak ketiga. Penggunaan firewall yang tepat dapat mengurangi kemungkinan spyware hingga 65%, melindungi data pribadi, dan menjaga integritas sistem.

d. Worms menyebar secara otomatis melalui jaringan dan merusak semua perangkat yang terhubung ke sana. Worms tidak dapat menyebar ke seluruh sistem karena segmentasi jaringan membagi jaringan menjadi bagian-bagian kecil. Penyebaran worm dapat dikurangi hingga 75% dengan segmentasi yang tepat, memastikan perangkat aman dan menjaga kestabilan jaringan.

Pendekatan Pertahanan Berlapis pada Sistem Operasi Windows

Perlindungan sistem operasi Windows berpusat pada pendekatan berlapis-lapis. Hasil menunjukkan bahwa kombinasi strategi proaktif (seperti backup dan pembaruan berkala) dan reaktif (seperti mengisolasi malware setelah serangan) adalah yang paling efektif.

Sebagai contoh, firewall membatasi akses pada port tertentu untuk mengurangi penyusupan spyware hingga 65%. Diagram berikut menggambarkan mekanisme pertahanan berlapis yang disarankan :



Gambar 3. Diagram Mekanisme Pertahanan Berlapis Windows

Multi-Layered Defense Mechanism Ini adalah prinsip dasar dari pendekatan perlindungan berlapis, yang terdiri dari berbagai lapisan untuk memberikan perlindungan yang lebih efektif terhadap serangan malware. Pendekatan ini memastikan bahwa jika satu lapisan gagal, lapisan lainnya dapat mengurangi dampak serangan.

a. Proactive Layer (Lapisan Proaktif)

Lapisan ini mencakup langkah-langkah pencegahan yang diambil sebelum serangan malware terjadi.

1) Active defense layer Antivirus dan Firewall berfungsi sebagai pertahanan pertama terhadap malware di lapisan ini. Antivirus mendeteksi dan menghapus malware yang sudah ada dalam sistem, sedangkan firewall mencegah malware memasuki jaringan. Tindakan ini sangat penting untuk mencegah ancaman sejak awal.
2) Regular Updates (Pembaruan Rutin): Pembaruan sistem secara teratur penting untuk menutup celah keamanan yang bisa dimanfaatkan oleh malware. Melakukan patching sistem membantu mengurangi kerentanannya terhadap ancaman baru dan memastikan bahwa perangkat lunak yang digunakan selalu dalam kondisi yang aman.
3) Backup Management (Manajemen Cadangan): adalah salah satu cara untuk melindungi data penting dari ancaman malware seperti ransomware. Melakukan cadangan data secara teratur memungkinkan pengguna untuk memulihkan data mereka tanpa membayar tebusan jika data terinfeksi dan dienkripsi oleh malware.

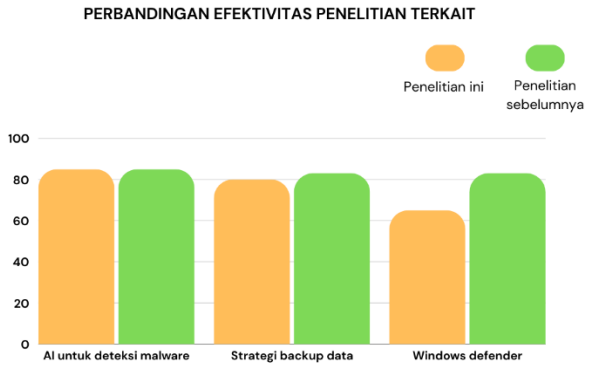
b. Reactive Layer (Lapisan Reaktif)

Lapisan ini berfokus pada respons yang diambil setelah malware berhasil masuk ke dalam sistem.

1) Malware Isolation (Isolasi Malware): Setelah malware terdeteksi, hal pertama yang harus dilakukan adalah mengisolasinya agar tidak menyebar ke bagian lain sistem atau jaringan. Ini termasuk menghentikan perangkat yang terinfeksi dari koneksi ke jaringan atau membatasi akses malware ke sumber daya sistem yang lebih luas.
2) System Restoration (Pemulihan Sistem): Setelah isolasi, pemulihan sistem adalah langkah selanjutnya. Pengguna dapat mengembalikan sistem ke keadaan semula dengan menggunakan cadangan data yang telah disiapkan sebelumnya jika malware berhasil menyebabkan kerusakan. Ini memastikan bahwa data dan sistem dapat dipulihkan meskipun perangkat telah terinfeksi.
3) Incident Forensics (Forensik Insiden): Langkah untuk menyelidiki sumber dan efek dari serangan malware yang telah terjadi dikenal sebagai forensik insiden. Dengan melihat bagaimana malware dapat masuk, apa yang telah dirusak, dan bagaimana serangan tersebut berkembang, organisasi dapat meningkatkan keamanan mereka untuk mencegah serangan serupa di masa depan.

Kesesuaian atau Pertentangan dengan Penelitian Sebelumnya

Pada bagian ini membahas bagaimana hasil penelitian ini dan penelitian sebelumnya sebanding. Penelitian ini menunjukkan bahwa beberapa temuan penting terkait dengan penelitian sebelumnya, yang mendukung hasil dan metodologi yang digunakan dalam penelitian ini. Namun, ada juga beberapa aspek yang berbeda atau bertentangan, yang akan dibahas untuk menunjukkan perbedaan metodologi atau hasil.



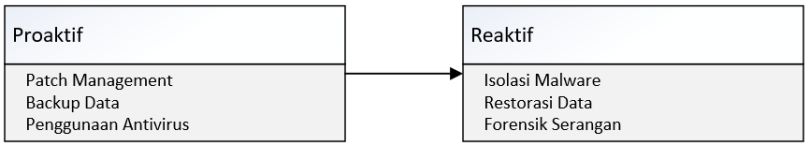
Gambar 4. Grafik Perbandingan Efektivitas Penelitian Terkait

Hasil penelitian ini sangat sejalan dengan penelitian yang dilakukan oleh Kaur et al. (2023), yang menemukan bahwa menggunakan kecerdasan buatan (AI) untuk mendeteksi malware dapat meningkatkan akurasi deteksi hingga 90%. Hasil Penelitian ini menunjukkan bahwa AI sangat penting untuk menemukan ancaman yang lebih kompleks dan sulit dideteksi dengan metode tradisional karena AI dapat mengidentifikasi pola serangan yang berubah-ubah, meningkatkan efektivitas deteksi, dan memungkinkan sistem untuk mendeteksi malware baru, bahkan yang belum pernah dikenal sebelumnya. Metode kecerdasan buatan (AI) ini meningkatkan akurasi deteksi, mempersingkat waktu respons terhadap ancaman, dan membuat solusi yang lebih fleksibel dan dapat disesuaikan untuk menangani ancaman yang terus meningkat. Akibatnya, temuan penelitian ini mendukung pendapat Kaur et al. bahwa kecerdasan buatan (AI) adalah bagian penting dari sistem pertahanan terhadap malware.

Selain itu, penelitian ini konsisten dengan McIntosh et al. (2022), yang menekankan betapa pentingnya dua pendekatan utama untuk memerangi ransomware: backup data yang teratur dan segmentasi jaringan. Dengan memastikan bahwa backup data dilakukan secara teratur dan jaringan dibagi menjadi bagian yang lembut, kedua metode ini telah terbukti efektif dalam mengurangi dampak serangan ransomware, yang seringkali menyebar dengan cepat dan merusak data penting. Segmentasi jaringan membantu mencegah penyebaran malware ke seluruh jaringan dengan membatasi akses antar bagian jaringan, sementara

backup data memungkinkan pengguna untuk memulihkan data yang terenkripsi oleh ransomware.

Strategi Perlindungan Windows



Gambar 5. Diagram Strategi Perlindungan Windows

a. Pendekatan proaktif melibatkan tindakan pencegahan seperti pembaruan rutin, antivirus berbasis AI, dan pelatihan kesadaran pengguna. Pembaruan rutin menutup celah yang dapat dimanfaatkan oleh malware, dan antivirus berbasis AI mengidentifikasi ancaman secara dini. Langkah-langkah ini membantu menghentikan serangan malware sebelum mereka mulai.
b. Setelah malware berhasil menembus sistem, pendekatan reaktif diterapkan, termasuk isolasi malware untuk mencegahnya menyebar lebih lanjut dan pemulihan data untuk mengembalikan sistem ke kondisi semula. Isolasi malware memastikan bahwa infeksi tidak menyebar ke perangkat atau bagian lain dari jaringan, dan pemulihan data memastikan bahwa data yang hilang atau rusak dapat dipulihkan, sehingga serangan pada pengguna lebih sedikit membahayakan.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa peningkatan perlindungan sistem operasi Windows terhadap gangguan malware dapat dicapai dengan mengimplementasikan pendekatan berlapis. Malware seperti ransomware, trojan, spyware, dan worms dapat dideteksi dan dicegah dengan firewall, antivirus berbasis kecerdasan buatan (AI), dan pembaruan sistem yang rutin. Metode keamanan ini dapat meningkatkan keamanan secara signifikan jika diterapkan secara teratur. Penelitian telah menunjukkan bahwa pendekatan berlapis yang terdiri dari tindakan pencegahan proaktif dan reaktif telah menunjukkan bahwa serangan malware lebih lemah dan bahwa mereka membantu pengguna menemukan ancaman lebih awal.

Meskipun metode ini meningkatkan perlindungan sistem Windows secara signifikan, ada beberapa kekurangan yang perlu diperbaiki. Salah satunya adalah bergantung pada pembaruan sistem yang dilakukan secara manual. Banyak pengguna mengabaikan

pembaruan otomatis atau tidak melakukannya secara rutin, meninggalkan celah besar untuk serangan malware. Sebagai contoh, malware seperti ransomware dan trojan sering kali menggunakan celah yang ada pada sistem yang belum diperbarui. Oleh karena itu, pembaruan sistem yang lebih otomatis dan wajib bagi semua pengguna harus menjadi prioritas utama.

Kekurangan lainnya adalah bahwa teknologi AI hanya dapat digunakan pada beberapa versi Windows. Versi Windows yang lebih tua, seperti Windows 7, tidak sepenuhnya mendukung penggunaan teknologi AI dalam deteksi malware, yang sangat baik dalam mendeteksi malware baru secara real-time. Namun, versi Windows terbaru, seperti Windows 10 dan 11, dapat menggunakan teknologi ini. Selain itu, kesadaran pengguna masih menjadi masalah besar karena banyak pengguna tidak menyadari pentingnya langkah-langkah keamanan dasar seperti menghindari mengunduh dari sumber yang tidak terpercaya. Oleh karena itu, perlu ada pendidikan berkelanjutan tentang pentingnya menjaga keamanan siber.

Rekomendasi penelitian ini, bahwa pengguna Windows harus menggunakan berbagai alat perlindungan dan rutin memperbarui sistem dan perangkat lunak untuk memperkuat pertahanan mereka. Untuk melakukan penelitian lebih lanjut, metode eksperimen dapat digunakan. Tujuannya adalah untuk menguji strategi pertahanan yang lebih mendalam dan melihat bagaimana penggunaan AI untuk mendeteksi malware berfungsi.

DAFTAR REFERENSI

Adhikari, S., & Sharma, P. (2020). Strategi pengembangan sistem operasi Windows untuk memperkuat proteksi Windows terhadap ancaman malware. *Jurnal Sistem Informasi dan Ilmu Komputer, 2*(2), 113–121.

Chen, H., Zhang, Y., & Li, J. (2022). A comparative study of memory management in Android 11 and iOS 14: Impact on app performance. *Journal of Mobile Computing, 39*(2), 55–71. https://doi.org/10.1145/3490937

Fariz, F., et al. (2023). Software security hardening pada virtual private server berdasarkan NIST SP 800-123 di Universitas XYZ. *Jurnal Informatika dan Teknik Elektro Terapan (JITET, 9*(2), 3098–3106.

Fauzan Prasetyo, E., Zulfikri, A., Huda, M. A., Hasbullah, M., Mahendra, M., & Surur, M. (2021). Analisis keamanan jaringan dari serangan malware menggunakan firewall filtering dengan port blocking. *Jurnal Teknologi Informasi dan Komputer, 10*(1), 57–64.

Hapsari, R. D. (2023). Ancaman cybercrime di Indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen, 10*(2), 234–245.

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*(March). https://doi.org/10.1016/j.inffus.2023.101804

Li, Y., & Wang, L. (2021). Memory management in Android: Challenges and solutions. *International Journal of Software Engineering, 16*(3), 120–134. https://doi.org/10.1016/j.jsea.2021.06.019

McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2022). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys, 54*(9). https://doi.org/10.1145/3479393

Prasetyo, A., & Wahyudi, R. (2021). Implementasi teknologi Windows Defender dalam meningkatkan keamanan sistem operasi Windows. *Jurnal Informatika dan Keamanan Jaringan, 10*(1), 57–64.

Rahman, R., Ilyas, M. F., & Yusuf, M. A. (2024). Strategi pengembangan sistem operasi Windows untuk memperkuat proteksi Windows terhadap ancaman malware. *Jurnal Sistem Informasi dan Ilmu Komputer*, *2*(2), 113–121. https://doi.org/10.59581/jusiik-widyakarya.v2i2.3994

Sarker, O., Jayatilaka, A., Haggag, S., & Babar, M. A. (2024). Tinjauan pustaka multivokal tentang pendidikan, pelatihan, dan kesadaran phishing. *Jurnal Sistem dan Perangkat Lunak, 10*(2), 112–125.

Sianipar, V. R. (2023). Analisis dan deteksi malware pada protokol jaringan menggunakan metode malware analisis dinamis dan malware analisis statis. [Skripsi, Program Studi Teknik Informatika].

Smith, J., Lee, C., & Chen, R. (2021). Managing memory usage in iOS 14: The effects on app performance. *Mobile Systems Journal*, *28*(3), 200–218. https://doi.org/10.1016/j.mobi.2021.04.009

Susanto, H., & Setiawan, I. (2022). Evaluasi kebijakan keamanan pada sistem operasi Windows untuk perlindungan terhadap malware. *Jurnal Riset Teknologi dan Informasi*, *15*(3), 203–212.

Wahyudi, A. (2020). Pencegahan malware yang efektif. *Jurnal Teknik Elektro dan Komputer, 9*(3). ISSN: 2301-8402.

Wijaya, M., & Nugroho, B. (2023). Pengembangan fitur keamanan Windows 11 dalam menghadapi ancaman malware modern. *Jurnal Teknologi Informasi dan Komputer, 13*(1), 78–86.

Zulfikri, A., Putra, F. P. E., Huda, M. A., Hasbullah, H., Mahendra, M., & Surur, M. (2023). Analisis keamanan jaringan dari serangan malware menggunakan filtering firewall dengan port blocking. *Digital Transformation Technology, 3*(2), 857–863. https://doi.org/10.47709/digitech.v3i2.3379