JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Nomor** 2, November 2026

Analisis Mekanisme Pertahanan Sistem Operasi Terhadap Berbagai Variasi Virus Komputer Modern

Habib Habsyi Al-Qudsyi[1*], Syifa Ul Qalbi[2], Nur Amelia Sofiyani[3], Ahmat Fahri Matondang[4], Ariifah Yaasir Harahap[5], Vanes Jaya Sandria[6]
[1,2,3]Universitas Malikussaleh, Indonesia
[1]vanes.240170137@mhs.unimal.ac.id

ABSTRACT

Evolusi ancaman siber yang pesat telah mengubah virus komputer sederhana menjadi entitas yang sangat canggih, seperti malware polimorfik dan serangan tanpa file (fileless). Penelitian ini bertujuan untuk memberikan analisis mendalam mengenai mekanisme pertahanan internal pada sistem operasi (OS) modern. Metodologi penelitian melibatkan evaluasi teknis terhadap beberapa lapis perlindungan, termasuk integritas memori, keamanan berbasis virtualisasi, dan integrasi algoritma pembelajaran mesin untuk deteksi perilaku. Hasil penelitian menunjukkan bahwa meskipun deteksi berbasis tanda tangan (signature) tradisional mulai usang, kombinasi antara keamanan berbasis perangkat keras (TPM) dan analisis heuristik dinamis menawarkan perlindungan yang kokoh terhadap eksploitasi zero-day. Penelitian ini menyimpulkan bahwa sinergi antara isolasi tingkat kernel dan kecerdasan berbasis awan (cloud) sangat penting untuk menjaga integritas sistem di era ancaman yang terus berkembang secara persisten.

Kata Kunci: Keamanan Sistem Operasi, Mitigasi Virus, Deteksi AI, Perlindungan Kernel, Pertahanan Siber

PENDAHULUAN

Sistem operasi (OS) merupakan fondasi dari seluruh aktivitas komputasi, menjadikannya target utama bagi pengembang perangkat lunak berbahaya. Dalam satu dekade terakhir, virus komputer telah bermutasi dari program replikasi diri yang mengganggu menjadi alat serangan siber yang terorganisir untuk pencurian data, pemerasan (ransomware), dan sabotase sistem infrastruktur kritis.

Fenomena yang paling mengkhawatirkan saat ini adalah munculnya serangan *fileless malware*. Berbeda dengan malware konvensional, serangan ini beroperasi tanpa menyimpan file berbahaya pada media penyimpanan dan memanfaatkan memori serta skrip sistem yang sah, sehingga sulit terdeteksi oleh antivirus tradisional *(Kaspersky Lab, 2021)*. Oleh karena itu, penelitian ini akan menguraikan bagaimana mekanisme pertahanan OS berevolusi dari model pasif menjadi proaktif, serta bagaimana teknologi AI digunakan untuk membedakan antara proses sistem yang sah dan aktivitas virus yang disamarkan secara kompleks.

Perkembangan teknologi informasi yang sangat pesat sejalan dengan meningkatnya ketergantungan manusia terhadap sistem komputer dan perangkat digital. Kondisi ini menjadi keamanan sistem operasi sebagai aspek krusial, mengingat hampir seluruh aktivitas penting mulai dari komunikasi, tranksaksi keuangan, hingga pengelolaan data strategis yang berjalan diatas sistem operasi. Serangan virus komputer modern tidak lagi bersifat sporadis, melainkan terstruktur dan berkelanjutan (persistent threat), dengan tujuan jangka panjang seperti penguasaan sistem, pencurian data sensitif, serta gangguan terhadap layanan kritis.

Di sisi lain, sistem operasi modern terus mengalami peningkatan kemampuan pertahanan melalui integrasi teknologi keamanan berbasis perangkat keras dan kecerdasan buatan. Mekanisme seperti Virtualization-Based Security (VBS), Trusted Platform Module (TPM), serta deteksi berbasis perilaku (behavior-based detection) menjadi pendekatan utama dalam menghadapi virus generasi baru yang mampu menghindari metode deteksi konvensional. Namun demikian, efektivitas mekanisme tersebut menjadi perdebatan, Evolusi malware modern juga ditandai dengan meningkatnya eksploitasi celah *zero-day*, di mana kerentanan dimanfaatkan sebelum tersedia mekanisme penambalan resmi *(Bilge & Dumitraş, 2012)*.

Oleh karena itu, penelitian ini menjadi relavan untuk dilakukan guna menganalisis sejauh mana mekanisme pertahanan sistem operasi mampu menghadapi berbagai variasi virus komputer modern. Penelitian ini diharapkan dapat memberikan gambaran komprehenshif mengenai kekuatan, keterbatasan, serta potensi pengembangan sistem pertahanan sistem operasi dimasa mendatang.

KAJIAN LITERATUR

Bagian ini menguraikan dasar-dasar teknis yang menopang sistem pertahanan sistem operasi modern:

Mekanisme Keamanan Memori (ASLR dan DEP): Mekanisme keamanan memori seperti Address Space Layout Randomization (ASLR) dan Data Execution Prevention (DEP) dirancang untuk meminimalkan keberhasilan eksploitasi

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Nomor** 2, November 2026

berbasis memori dengan membatasi eksekusi kode pada area data dan mengacak lokasi alamat memori proses *(Microsoft, 2023)*.

Konsep Sandboxing dan Isolasi Proses: Kajian literatur menunjukkan bahwa prinsip *least privilege* (hak istimewa terendah) merupakan konsep krusial dalam keamanan sistem operasi. Sistem operasi modern seperti Windows dan macOS menerapkan mekanisme sandboxing, di mana aplikasi dijalankan dalam lingkungan terisolasi dengan hak akses terbatas untuk mencegah dampak penyebaran malware *(Saltzer & Schroeder, 1975)*.

Heuristik dan Machine Learning: Pendekatan deteksi malware berbasis *machine learning* dikembangkan untuk mengatasi keterbatasan metode signature-based yang tidak efektif terhadap malware polimorfik dan metamorfik *(Gilbert et al., 2020)*.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif-deskriptif dengan analisis teknik pada arsitektur sistem operasi.

Objek Penelitian:

Objek penelitian difokuskan pada kernel sistem operasi Windows NT yang digunakan pada Windows 11, khususnya komponen keamanan seperti Antimalware Scan Interface (AMSI), Virtualization-Based Security (VBS) (Microsoft, 2023), serta perlindungan berbasis perangkat keras seperti Trusted Platform Module (TPM) dan Secure Boot (Trusted Computing Group, 2022). **Ruang Lingkup :** Pengamatan dilakukan pada interaksi antara virus modern dengan lapisan pertahanan *Antimalware Scan Interface* (AMSI) dan *Virtualization-Based Security* (VBS). Ruang Lingkup Penelitian Pengamatan dilakukan pada interaksi antara virus komputer modern dengan lapisan pertahanan sistem operasi dalam lingkungan laboratorium yang terkendali (sandbox environment).

Teknik Analisis:

Data dikumpulkan melalui pemantauan alur pemanggilan API sistem, aktivitas memori, serta upaya modifikasi registry dan injeksi proses yang dilakukan oleh sampel malware. Data tersebut dianalisis untuk mengevaluasi kemampuan sistem operasi dalam mendeteksi dan menghentikan aktivitas berbahaya.

Alur Penelitian:

Gambar 1. Alur Metode Penelitian

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Nomor** 2, November 2026

Penjelasan Tahapan Penelitian:

Tahapan Penelitian Tahapan penelitian dimulai dengan studi literatur untuk mengidentifikasi konsep dan perkembangan terbaru terkait virus komputer modern serta mekanisme pertahanan sistem operasi. Literatur yang dikaji meliputi jurnal ilmiah, buku rujukan sistem operasi, serta dokumentasi resmi pengembang sistem operasi.

Tahap selanjutnya adalah perancangan skenario pengujian secara kualitatif dalam lingkungan laboratorium yang terkendali (sandbox environment). Pada tahap ini, peneliti tidak berfokus pada pengukuran kuantitatif, melainkan pada observasi perilaku sistem operasi ketika berhadapan dengan aktivitas malware modern. Skenario pengujian dirancang untuk merepresentasikan pola serangan umum, seperti upaya injeksi memori, pemanggilan API berulang yang mencurigakan, serta percobaan modifikasi registry.

Tahap pengamatan dilakukan dengan memantau respons sistem operasi terhadap setiap skenario serangan, termasuk mekanisme pemblokiran proses, isolasi aplikasi, dan pencegahan eskalasi hak akses. Hasil pengamatan dicatat secara deskriptif untuk menggambarkan efektivitas masing-masing lapisan pertahanan.

Tahap akhir penelitian adalah analisis dan interpretasi hasil pengamatan. Pada tahap ini, peneliti membandingkan temuan observasi dengan konsep dan teori yang dibahas dalam kajian literatur guna menarik kesimpulan mengenai kekuatan dan keterbatasan mekanisme pertahanan sistem operasi dalam menghadapi variasi virus komputer modern.

HASIL DAN PEMBAHASAN

Hasil analisis menunjukkan bahwa sistem operasi saat ini menerapkan strategi pertahanan berlapis *(defense-in-depth)*.

Tabel 1. Analisis Ketahanan Lapis Pertahanan Sistem Operasi

Lapisan Pertahanan	Jenis Ancaman	Respon Teknis Sistem	Efektivitas
Integritas memori (ASLR/DEP)	Eksploitasi memori	Pemutusan proses (termination)	Tinggi
Sandbox / isolasi	Ransomware	Penolakan akses tulis ke disk	Sangat tinggi
Analisis heuristik (AI)	Virus polimorfik	Pemblokiran berdasarkan skor risiko	Menengah
Root of Trust Perangkat Keras (TPM/Secure Boot)	Rootkit / bootkit	Kegagalan booting pada kode tidak valid	Sangat tinggi

PEMBAHASAN

Pembahasan: Mekanisme pertahanan memiliki yang paling signifikan dalam tiga tahun terakhir adalah pemanfaatan virtualisasi untuk keamanan. Sebagai contoh, Windows 11 menggunakan Hardware-Enforced Stack Protection yang memanfaatkan fitur perangkat keras CPU untuk mencegah modifikasi alur eksekusi program oleh malware, sebagaimana dijelaskan dalam arsitektur keamanan kernel Windows modern (Russinovich et al., 2021)..

Secara logis, pertahanan ini bekerja dengan memisahkan fungsi-fungsi keamanan inti ke dalam kontainer berbasis virtualisasi yang tidak dapat diakses oleh komponen sistem operasi lainnya, sehingga meningkatkan ketahanan terhadap eskalasi hak akses (Microsoft, 2023). Jadi,jika sebuah virus berhasil mendapatkan hak akses ”Administrator” melalui serangan *social engineering,* virus tersebut tetap akan terhalang oleh lapisan virtualisasi kernel. Namun, pembahasan ini juga mengidentifikasi celah pada “Analisis AI”, di mana virus yang sangat canggih dapat meniru perilaku manusia (seperti mengetik atau menggerakkan kursor) untuk menipu deteksi heuristik.

KESIMPULAN

Berdasarkan analisis di atas, dapat disimpulkan bahwa mekanisme pertahanan sistem operasi terhadap virus modern telah bergeser dari sekadar pemindaian file menjadi pemantauan aktivitas sistem *secara real-time* dan mendalam. Sinergi antara perlindungan berbasis perangkat keras seperti Trusted Platform Module (TPM) dan algoritma kecerdasan buatan merupakan standar keamanan baru yang tidak dapat diabaikan dalam menghadapi ancaman siber modern (Trusted Computing Group, 2022)

Manfaat penelitian ini adalah memberikan pemahaman bahwa keamanan komputer tidak cukup hanya dengan menginstal perangkat lunak tambahan, melainkan harus memaksimalkan fitur keamanan bawaan OS. Rekomendasi untuk penelitian selanjutnya adalah mengkaji lebih dalam mengenai serangan berbasis "AI vs AI"’ di mana virus menggunakan kecerdasan buatan pertahanan sistem yang juga berbasis kecerdasan buatan.

REFERENSI

Bilge, L., & Dumitraș, T. (2012). *Before we knew it: An empirical study of zero-day attacks*. ACM Conference on Computer and Communications Security. https://link.springer.com/article/10.1007/s11416-019-00353-0

Gilbert, D., Mateu, C., & Planes, J. (2020). *The rise of machine learning for malware detection*. Journal of Computer

E-ISSN: 3090-739X
Volume 2, **Nomor** 2, November 2026

Virology and Hacking Techniques. https://link.springer.com/article/10.1007/s11416-019-00353-0

Kaspersky Lab. (2021). *Fileless malware: Attacks without files*. https://www.kaspersky.com/resource-center/definitions/fileless-malware

Microsoft. (2023). *Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) overview*. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/vbs

Microsoft. (2023). *Virtualization-Based Security (VBS) in Windows 11*. https://learn.microsoft.com/en-us/windows/win32/memory/data-execution-prevention

Russinovich, M., Solomon, D., & Ionescu, A. (2021). *Windows Internals* (7th ed.). Microsoft Press. https://learn.microsoft.com/en-us/sysinternals/resources/windows-internals

Saltzer, J. H., & Schroeder, M. D. (1975). *The protection of information in computer systems*. IEEE. https://ieeexplore.ieee.org/document/1451869

Trusted Computing Group. (2022). *TPM 2.0: A brief introduction*. https://trustedcomputinggroup.org/resource/tpm-library