JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 13 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i3.6556

# ANALISIS SAMPEL MALWARE PADA SISTEM OPERASI WINDOWS 10 MENGGUNAKAN CUCKOO SANDBOX

**Muhammad Rifki Adiyatma[1*], Herri Setiawan[2], Tasmi[3]**

[1,2]Teknik Informatika, Universitas Indo Global Mandiri
[3]Sistem Komputer, Universitas Indo Global Mandiri
Jalan Jend. Sudirman Km.4 No. 62, Kota Palembang, Indonesia

**Keywords:**
Windows OS 10;
Cuckoo Sandboox;
Analysis Dynamic;
Sample Malware.

**Corespondent Email:**
2022110055p@students.uigm.ac.id

**Abstrak.** Analisis malware merupakan langkah penting dalam mendeteksi, memahami, dan mengurangi dampak perangkat lunak berbahaya terhadap sistem komputer. Penelitian ini berfokus pada analisis sampel malware pada sistem operasi Windows menggunakan *Cuckoo Sandbox*, sebuah platform open-source yang dirancang untuk menganalisis perilaku malware secara otomatis. Proses analisis dilakukan dengan mengisolasi sampel dalam lingkungan virtual yang terkendali, sehingga memungkinkan pemantauan aktivitas berbahaya tanpa risiko terhadap sistem host. Penelitian ini melibatkan tahapan pengumpulan sampel malware, konfigurasi lingkungan pengujian, eksekusi sampel, dan analisis hasil. Berdasarkan hasil analisis, ditemukan bahwa sampel malware memiliki kemampuan untuk memodifikasi file sistem, memanipulasi entri registry, dan melakukan komunikasi jaringan dengan server perintah dan kontrol. Tingkat deteksi berdasarkan VirusTotal menunjukkan bahwa sebagian besar sampel dikategorikan sebagai malware berbahaya, dengan tingkat deteksi mencapai 67%. Temuan ini menegaskan efektivitas metode analisis dinamis dalam mengungkap pola serangan malware serta pentingnya penggunaan lingkungan virtual dalam pengujian malware untuk meningkatkan keamanan dan mitigasi risiko



**Abstract.** Malware analysis is a crucial step in detecting, understanding, and mitigating the impact of malicious software on computer systems. This study focuses on analyzing malware samples on the Windows operating system using Cuckoo Sandbox, an open-source platform designed to automatically analyze malware behavior. The analysis was carried out by isolating the samples within a controlled virtual environment, allowing malicious activities to be monitored without risking the host system. The research involved several stages, including malware sample collection, testing environment configuration, sample execution, and result analysis. Based on the findings, the analyzed malware samples exhibited capabilities such as modifying system files, manipulating registry entries, and establishing network communications with command and control servers. Detection rates from VirusTotal indicated that most samples were classified as malicious, with a detection ratio of 67%. These results emphasize the effectiveness of dynamic analysis methods in revealing malware attack patterns and highlight the importance of using virtual environments in malware testing to enhance security and risk mitigation.

Vol. 13 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i3.6556

## 1. PENDAHULUAN

Di era digital saat ini, *malware* menjadi salah satu ancaman utama terhadap keamanan sistem komputer di seluruh dunia. *Malware* seperti *virus*, *worm*, *trojan*, dan *ransomware* mampu merusak data, mengganggu operasional sistem, dan menyebabkan kerugian besar baik di sektor individu maupun organisasi [1]. Sistem operasi Windows, sebagai salah satu sistem operasi dengan tingkat adopsi tertinggi, menjadi sasaran empuk berbagai serangan *malware* yang memanfaatkan celah-celah keamanan yang ada. Kondisi ini menuntut pengembangan metode analisis yang mampu mengidentifikasi dan memahami perilaku *malware* secara efektif guna meningkatkan sistem pertahanan siber [2].

Permasalahan yang dihadapi dalam konteks ini adalah bagaimana melakukan analisis terhadap sampel *malware* secara aman tanpa membahayakan sistem utama. Sistem operasi Windows telah dilengkapi berbagai fitur keamanan seperti Windows Defender dan Windows Firewall, namun varian *malware* baru terus bermunculan dengan teknik serangan yang semakin kompleks [3]. Salah satu tantangan penting adalah mengungkap aktivitas tersembunyi *malware* yang hanya dapat diamati melalui eksekusi langsung dalam lingkungan yang terkendali. Oleh karena itu, diperlukan pendekatan yang mampu merekam perilaku *malware* dengan risiko minimal terhadap kerusakan system [4].

Penelitian terdahulu telah banyak membahas teknik analisis *malware* menggunakan pendekatan statis dan dinamis. Manoppo et al. menunjukkan bahwa *dynamic analysis* memberikan hasil yang lebih mendalam dibandingkan *static analysis* dalam mengamati perilaku aktual *malware* [1]. Studi oleh Rahayu dan Trianto memperkenalkan penggunaan *Cuckoo Sandbox* sebagai platform analisis otomatis untuk memantau aktivitas file, registry, dan jaringan. Sementara itu [2], Kurniawan membuktikan bahwa *sandboxing* mampu mengisolasi eksekusi *malware* sehingga analisis dapat dilakukan tanpa membahayakan sistem utama [3]. Namun, sebagian besar penelitian sebelumnya masih terbatas pada jenis *malware* tertentu dan belum banyak yang mengkaji analisis varian *ransomware* seperti WannaCry secara spesifik pada Windows 10.

Untuk menjawab tantangan tersebut, penelitian ini menggunakan metode *dynamic analysis* berbasis *Cuckoo Sandbox* versi 2.0.7. Sampel *malware* yang diuji diunduh dari sumber tepercaya dan dijalankan di lingkungan virtual yang telah dikonfigurasi dengan kontrol ketat [5]. Selama eksekusi, seluruh aktivitas yang dilakukan oleh *malware* seperti modifikasi file sistem, manipulasi registry, dan komunikasi jaringan dicatat dan dianalisis. Pendekatan ini dipilih karena mampu memberikan gambaran perilaku *malware* yang mendekati kondisi aktual di dunia nyata tanpa membahayakan perangkat utama [6].

Penelitian ini bertujuan untuk mengidentifikasi karakteristik perilaku *malware* pada sistem operasi Windows 10, memahami mekanisme serangan yang digunakan, serta mengevaluasi efektivitas penggunaan *Cuckoo Sandbox* dalam analisis otomatis. Selain itu, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan teknik mitigasi serangan *malware* melalui pendekatan berbasis lingkungan terisolasi. Dengan memahami pola aktivitas *malware*, langkah-langkah pencegahan dan respons insiden dapat dirancang dengan lebih baik.

Hasil penelitian menunjukkan bahwa *Cuckoo Sandbox* mampu mendeteksi berbagai aktivitas berbahaya yang dilakukan oleh sampel *malware* dengan akurasi yang tinggi. Analisis terhadap sampel *ransomware* WannaCry, *trojan* generik, dan *ransomware downloader* memperlihatkan adanya upaya modifikasi file sistem, perubahan entri registry, serta komunikasi dengan server eksternal. Temuan ini mempertegas pentingnya penggunaan *sandboxing* dalam upaya mendeteksi dan menganalisis *malware* di lingkungan yang aman, sekaligus memperkaya pemahaman tentang ancaman siber yang terus berkembang.

## 2. TINJAUAN PUSTAKA

### *2.1 Malware*

*Malware* merupakan singkatan dari *malicious software*, yaitu perangkat lunak yang dirancang untuk melakukan aktivitas merusak, mencuri data, atau mengganggu operasional sistem komputer [7]. Jenis-jenis *malware* yang umum meliputi *virus*, *worm*, *trojan*, *spyware*, *adware*, dan *ransomware*. Setiap jenis memiliki karakteristik serangan yang berbeda, namun

seluruhnya menimbulkan risiko serius terhadap integritas dan keamanan data [8].

### *2.2 Metode Analisis Malware*

Metode analisis *malware* terbagi menjadi dua pendekatan utama, yaitu *static analysis* dan *dynamic analysis* [9]. *Static analysis* dilakukan tanpa mengeksekusi file, dengan cara memeriksa struktur kode, signature, atau menggunakan fungsi hash seperti MD5 dan SHA-1. Sebaliknya, *dynamic analysis* dilakukan dengan mengeksekusi *malware* di lingkungan terkendali untuk mengamati perubahan file sistem, registry, dan komunikasi jaringan. Pendekatan *dynamic* memungkinkan pengamatan terhadap perilaku aktual *malware* yang aktif [10].

### *2.3 Cuckoo Sandbox*

*Cuckoo Sandbox* merupakan platform open-source yang dirancang untuk menganalisis perilaku *malware* secara otomatis di lingkungan virtual [3]. Platform ini mampu mendeteksi aktivitas seperti pembuatan file baru, modifikasi registry, hingga koneksi ke server eksternal. Selain itu, *Cuckoo Sandbox* mendukung integrasi dengan layanan eksternal seperti VirusTotal untuk memperkaya hasil analisis [11].

### *2.4 Keamanan Sistem Operasi Windows*

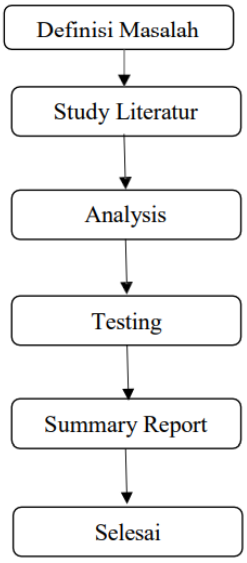
Sistem operasi Windows, meskipun telah dilengkapi berbagai fitur keamanan seperti Windows Defender, Windows Firewall, dan pembaruan otomatis, tetap menjadi sasaran utama serangan *malware* [12]. Pemahaman tentang mekanisme pertahanan Windows serta kelemahannya menjadi penting dalam rangka menyusun strategi analisis dan mitigasi yang efektif terhadap ancaman *malware*.

### *2.5 Relevansi terhadap Penelitian*

Penggunaan kombinasi metode *dynamic analysis* melalui *Cuckoo Sandbox* dan analisis terhadap arsitektur keamanan Windows menjadi dasar penelitian ini. Fokus penelitian diarahkan pada identifikasi perilaku *malware* jenis *ransomware* WannaCry dan *trojan* generik, untuk memberikan pemahaman yang lebih mendalam tentang pola serangan dan teknik mitigasi yang relevan terhadap sistem operasi Windows 10.

## 3. METODE PENELITIAN

Penelitian ini menggunakan metode *dynamic analysis* untuk menganalisis perilaku sampel *malware* pada sistem operasi Windows 10. Metode ini dilakukan dengan mengeksekusi sampel *malware* di lingkungan virtual terkontrol menggunakan *Cuckoo Sandbox* versi 2.0.7, sehingga seluruh aktivitas berbahaya dapat diamati tanpa membahayakan sistem utama. Proses penelitian meliputi pengumpulan sampel, persiapan lingkungan pengujian, eksekusi sampel, observasi aktivitas, dan analisis hasil [13]- [16]. Rancangan tahapan penelitian secara umum ditunjukkan pada Gambar 1.




**Gambar 1.** Tahapan Penelitian Analisis Malware

Sampel *malware* yang digunakan dalam penelitian ini diperoleh dari repositori terbuka di GitHub [1]. Tiga jenis sampel yang dipilih adalah *ransomware* WannaCry, *trojan* generik, dan *ransomware downloader*. Untuk memastikan keaslian dan validitas sampel, setiap file diverifikasi menggunakan fungsi hash MD5 dan SHA-1.

Spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini disajikan pada Tabel 1. Mesin virtual menggunakan sistem operasi Windows 10 Home 64-bit dengan RAM 16 GB dan prosesor AMD A8, sedangkan untuk kebutuhan analisis digunakan *Cuckoo Sandbox* dan layanan VirusTotal.

**Tabel 1.** Spesifikasi Lingkungan Pengujian

| Komponen | Spesifikasi |
|---|---|

| | |
|---|---|
| Sistem Operasi | Windows 10 Home 64-bit |
| Prosesor | AMD A8 |
| RAM | 16 GB |
| Virtualisasi | VirtualBox |
| Sandbox | Cuckoo Sandbox v2.0.7 |

Tahap implementasi penelitian dimulai dengan konfigurasi lingkungan virtual. Setelah sistem *Cuckoo Sandbox* siap, sampel *malware* diunggah untuk kemudian dieksekusi secara otomatis. Selama proses ini, *sandbox* memonitor aktivitas file, perubahan registry, aktivitas jaringan, dan proses-proses yang berjalan. Data hasil monitoring diekstraksi dalam format JSON dan HTML untuk dianalisis lebih lanjut.

Analisis data dilakukan dengan mengamati perubahan signifikan yang terjadi pada sistem selama eksekusi *malware*. Aktivitas yang diamati meliputi pembuatan file baru, modifikasi registry, serta percobaan koneksi jaringan ke server eksternal atau alamat IP mencurigakan. Data jaringan yang diperoleh diperiksa menggunakan tools tambahan seperti Wireshark untuk memvalidasi adanya koneksi ke server perintah dan kontrol (*command and control servers*).

Lingkungan pengujian dirancang agar dapat menjamin keamanan serta menghindari penyebaran *malware* ke sistem utama. Penggunaan mesin virtual memberikan keuntungan berupa kemampuan *snapshot* untuk mengembalikan sistem ke kondisi semula dengan cepat jika terjadi infeksi.

Data hasil analisis kemudian dibandingkan dengan database VirusTotal untuk mengidentifikasi dan mengonfirmasi jenis *malware* berdasarkan signature yang dikenali oleh berbagai antivirus. Sampel yang dianalisis juga diperiksa indikasi keberadaan teknik anti-detection atau teknik pengelakan, seperti deteksi terhadap lingkungan virtual atau penggunaan metode enkripsi terhadap payload.

Dalam penelitian ini, keamanan sistem operasi Windows juga diperhatikan dengan mengaktifkan Windows Firewall, mengandalkan antivirus terpercaya, serta menerapkan backup data rutin sebagai tindakan preventif. Dengan kombinasi pendekatan *dynamic analysis* berbantuan *sandbox* serta pemeriksaan berbasis signature eksternal, penelitian ini berupaya memperoleh pemahaman komprehensif mengenai perilaku *malware* pada sistem operasi Windows 10.

## 4. HASIL DAN PEMBAHASAN

### 4.1 Hasil

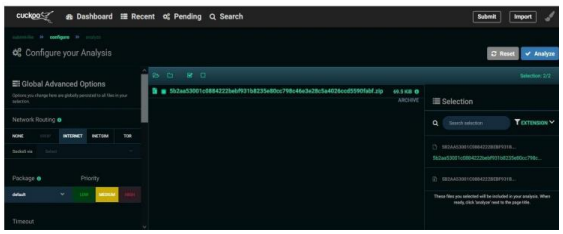
Penelitian ini bertujuan untuk menganalisis perilaku *malware* terhadap sistem operasi Windows 10 menggunakan metode *dynamic analysis* berbasis *Cuckoo Sandbox*. Ancaman terhadap sistem operasi Windows yang semakin kompleks menuntut pendekatan analisis yang komprehensif untuk memahami mekanisme serangan serta mengembangkan strategi mitigasi. Pada tahap awal penelitian, dilakukan identifikasi terhadap permasalahan utama yaitu kemampuan *malware* dalam memanfaatkan celah keamanan untuk mencuri data, merusak file sistem, dan mengganggu kinerja komputer pengguna.

Sampel *malware* diperoleh dari sumber terpercaya dan diverifikasi menggunakan hash MD5 dan SHA256 untuk menjamin integritas file. Proses analisis dilakukan dalam lingkungan mesin virtual yang telah dikonfigurasi dengan *Cuckoo Sandbox*. Hasil pengujian menunjukkan bahwa seluruh sampel yang dianalisis memperlihatkan perilaku berbahaya, meliputi modifikasi terhadap file sistem, perubahan pada entri registry, serta upaya koneksi ke domain atau alamat IP eksternal yang mencurigakan. Tabel 4.1 menyajikan identitas file sampel yang dianalisis, yang menunjukkan bahwa dua task dengan status "running" telah berhasil dijalankan dalam *sandbox*.

**Tabel 2.** Identitas Sampel Malware

| Task ID | Date | Filename/URL | Package | Status |
|---|---|---|---|---|
| 569483 | 11/13/2020 /14:22 | 58aa530f1088422fb97b1346254bbce79b6e2a4e5c3a9f1ce055f590df | Exe | Running |
| 569484 | 11/13/2020 /14:22 | 58aa530f1088422fb97b1346254bbce79b6e2a4e5c3a9f1ce055f590df | 7z | Running |

Setelah proses upload, tampilan file sampel malware dapat dilihat pada Gambar 2, yang memperlihatkan antarmuka dashboard *Cuckoo Sandbox* saat analisis berlangsung.



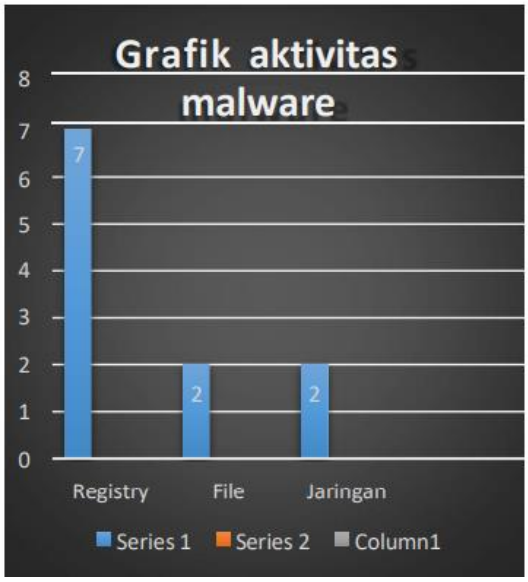

**Gambar 2.** Tampilan Dashboard Setelah Upload Sampel Malware

Analisis lebih mendalam terhadap registry sistem menunjukkan bahwa malware melakukan manipulasi terhadap entri registry seperti *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider\HwOrder*. Perubahan ini bertujuan untuk mempengaruhi urutan layanan jaringan dan mempertahankan kontrol terhadap sistem yang terinfeksi. Data aktivitas registry yang diamati dirangkum dalam Tabel 3.

**Tabel 3.** Aktivitas Registry Akibat Infeksi Malware

| Registry Key | Aksi |
|---|---|
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider\HwOrder | Modifikasi |
| HKEY_LOCAL_MACHINE\Software\Malicious App | Penambahan entri |

Selain perubahan terhadap sistem file dan registry, aktivitas jaringan yang dilakukan oleh malware juga tercatat intensif. Gambar 3 memperlihatkan intensitas aktivitas jaringan, termasuk upaya koneksi ke server eksternal melalui protokol HTTP, yang menjadi salah satu indikator keberadaan komunikasi ke server perintah dan kontrol (*command and control server*).




**Gambar 3.** Intensitas Aktivitas Jaringan Sampel Malware

Hasil pemeriksaan lebih lanjut dengan menggunakan layanan VirusTotal menunjukkan bahwa tingkat deteksi terhadap file sampel mencapai 67%. Hal ini mengindikasikan bahwa file yang diuji telah diklasifikasikan sebagai *malicious trojan* oleh sebagian besar mesin antivirus.

Analisis terhadap ransomware WannaCry menunjukkan kecenderungan untuk memanipulasi pengaturan jaringan melalui modifikasi registry serta upaya untuk berkomunikasi dengan domain-domain asing yang tidak dikenali. Aktivitas jaringan ransomware tersebut dirangkum dalam Tabel 4 dan aktivitas registry spesifik terhadap pengaturan proxy dan koneksi internet dijelaskan dalam Tabel 4.

**Tabel 4.** Koneksi Jaringan yang Dilakukan oleh Malware

| API Call | IP Address | Port | Tujuan |
|---|---|---|---|
| Connect | 209.27.16.165 | 445 | SMB Communication |

**Tabel 5.** Aktivitas Registry Ransomware WannaCry

| Waktu | API | Registry Key | Tujuan |
|---|---|---|---|
| 27-Feb-25 | RegOpenKeyExW | HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad | Membaca pengaturan WPAD |

Analisis statis terhadap file executable memperlihatkan adanya entropi tinggi, yang mengindikasikan kemungkinan penggunaan teknik enkripsi atau packing untuk menghindari deteksi antivirus. Hasil analisis string menunjukkan penggunaan fungsi API standar Windows seperti GetTickCount, ReadFile, dan CreateFileA, yang sering digunakan dalam malware untuk melakukan interaksi dengan file sistem dan memori. Gambar 4. dan Gambar 5 memperlihatkan hasil analisis sections dan data resources dari file sampel malware.


**Gambar 4.** Analisa Sections Malware

gambar di atas memperlihatkan struktur *sections* dalam file *malware*. Terlihat adanya tiga *section* utama, yaitu .text, .data, dan .rdata, serta satu tambahan bernama .pdata. Masing-masing memiliki alamat virtual, ukuran, dan entropi yang cukup tinggi. Entropi yang tinggi (misalnya 7.9921875 pada .pdata) mengindikasikan kemungkinan bahwa bagian tersebut telah mengalami kompresi atau enkripsi, yang merupakan teknik umum dalam *malware packing* untuk menyembunyikan muatan jahat.


**Gambar 5** Analisis Data Resources Malware

Selanjutnya, gambar *resources* menunjukkan dua entri penting yang mengindikasikan file ini mengandung *embedded data* dengan bahasa default *LANG_ENGLISH* dan sub-bahasa *SUBLANG_ENGLISH_US*. Salah satunya bertipe *RT_VERSION* dan lainnya adalah file dengan keterangan *data*, yang berpotensi menyimpan konfigurasi tersembunyi, *payload*, atau *command-and-control (C2)* trigger.

Keseluruhan hasil ini memperkuat hipotesis bahwa malware modern mengombinasikan berbagai teknik pengelakan deteksi, baik melalui perubahan perilaku pada registry, manipulasi sistem file, maupun koneksi jaringan tersembunyi.

### 4.2 Pembahasan

#### *1. Interpretasi Hasil Analisis Malware*

Hasil analisis perilaku *malware* menggunakan *Cuckoo Sandbox* menunjukkan bahwa metode *dynamic analysis* efektif dalam mendeteksi berbagai aktivitas berbahaya pada sistem operasi Windows 10. Sampel *malware* yang diuji memperlihatkan kemampuan untuk memodifikasi file sistem, mengubah entri registry, serta melakukan koneksi ke server eksternal. Modifikasi terhadap registry, khususnya pada kunci *NetworkProvider/HwOrder*, menunjukkan upaya malware untuk mempertahankan persistensinya di dalam sistem. Aktivitas komunikasi jaringan melalui protokol HTTP ke domain acak juga mengindikasikan adanya komunikasi dengan server perintah dan kontrol (*command and control*), yang merupakan ciri khas serangan malware modern.

Analisis statis lebih lanjut terhadap struktur file executable memperlihatkan adanya entropi tinggi pada beberapa bagian file, menunjukkan kemungkinan penggunaan teknik *packer* atau enkripsi untuk menghindari deteksi antivirus. String analysis juga menemukan pemanfaatan fungsi API Windows standar untuk melakukan operasi terhadap file dan memori sistem, memperkuat indikasi bahwa malware berusaha mengakses sumber daya penting di dalam komputer korban.

#### 2. Perbandingan dengan Penelitian Sebelumnya

Temuan dalam penelitian ini konsisten dengan hasil penelitian sebelumnya yang dilakukan oleh Rahayu dan Trianto, di mana malware modern tidak hanya mengandalkan eksekusi file, tetapi juga melakukan perubahan konfigurasi sistem untuk memperkuat keberadaan mereka. Penggunaan teknik komunikasi jaringan sederhana melalui HTTP, seperti yang ditemukan dalam penelitian ini, juga telah diidentifikasi dalam studi Zimba et al. [2] sebagai salah satu metode umum dalam operasi malware untuk menghindari deteksi firewall atau sistem deteksi intrusi tradisional.

Selain itu, kemampuan ransomware WannaCry untuk memodifikasi pengaturan jaringan dan mengakses registry sistem mendukung laporan yang disampaikan oleh Adi dan Hartanto [3], yang menunjukkan bahwa WannaCry memiliki mekanisme adaptif dalam memastikan konektivitas ke server C2, bahkan di jaringan yang terbatas.

Dalam konteks penggunaan lingkungan pengujian, hasil penelitian ini juga sejalan

dengan studi Ahmed et al. [4] yang menyatakan bahwa sandbox berbasis mesin virtual memberikan isolasi optimal terhadap malware, memungkinkan analisis yang aman tanpa risiko infeksi terhadap sistem utama. Namun, fenomena sandbox evasion, yaitu kemampuan malware mendeteksi lingkungan virtual dan mengubah perilakunya, sebagaimana dilaporkan oleh Manoppo et al. [5], tetap menjadi tantangan yang perlu diantisipasi dalam analisis dinamis.

### 3. Implikasi Teoretis dan Praktis

Implikasi teoretis dari hasil penelitian ini menguatkan teori tentang pentingnya pendekatan analisis perilaku (*behavior-based analysis*) dalam deteksi malware. Sementara analisis berbasis signature masih memiliki peran penting, pendekatan analisis perilaku memungkinkan pendeteksian malware varian baru yang belum dikenali dalam database antivirus. Penelitian ini juga menunjukkan bahwa kombinasi analisis statis dan dinamis menghasilkan pemahaman yang lebih komprehensif terhadap perilaku malware di sistem target.

Secara praktis, penggunaan lingkungan mesin virtual terbukti lebih aman dan fleksibel dibandingkan pengujian di sistem operasi Windows asli. Lingkungan virtual memungkinkan rollback sistem dengan mudah melalui penggunaan snapshot, sehingga mempercepat siklus pengujian dan mengurangi risiko kerusakan permanen akibat infeksi malware.

Dengan demikian, penelitian ini tidak hanya memperkuat pemahaman mengenai perilaku malware terhadap sistem Windows, tetapi juga memberikan rekomendasi teknis untuk praktik terbaik dalam analisis malware, khususnya dalam konteks pengujian aman dan respons insiden di dunia nyata.

## 5. KESIMPULAN

Penelitian ini telah berhasil menganalisis perilaku sampel *malware* pada sistem operasi Windows 10 menggunakan metode *dynamic analysis* berbasis *Cuckoo Sandbox*. Hasil pengujian menunjukkan bahwa malware memiliki kemampuan untuk memodifikasi file sistem, memanipulasi entri registry, serta melakukan komunikasi jaringan dengan server eksternal, yang mengindikasikan ancaman serius terhadap integritas dan keamanan sistem. Penggunaan mesin virtual sebagai lingkungan pengujian terbukti memberikan keunggulan dalam aspek keamanan, fleksibilitas rollback, dan isolasi sistem, meskipun masih terdapat keterbatasan terkait potensi pengelakan (*sandbox evasion*) oleh malware canggih. Metode analisis dinamis yang diterapkan dalam penelitian ini memiliki kelebihan dalam mendeteksi aktivitas malware secara real-time, namun di sisi lain memerlukan sumber daya sistem yang lebih besar dan waktu analisis yang lebih panjang dibandingkan metode statis. Untuk pengembangan penelitian selanjutnya, disarankan untuk mengintegrasikan teknik analisis berbasis *machine learning* guna meningkatkan akurasi deteksi serta memperluas cakupan terhadap malware varian baru yang menggunakan teknik pengelakan lebih kompleks, sekaligus memperkuat konfigurasi lingkungan virtual agar lebih menyerupai sistem nyata guna mengurangi risiko deteksi oleh malware.

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan, bantuan, dan fasilitas selama pelaksanaan penelitian ini, sehingga penelitian mengenai analisis perilaku malware menggunakan metode *dynamic analysis* berbasis *Cuckoo Sandbox* dapat diselesaikan dengan baik.

## DAFTAR PUSTAKA

[1] Chandra, S., Hutauruk, Y., Yulianto, F. A., and Satrya, G. B., "Malware analysis pada Windows operating system untuk mendeteksi trojan," unpublished, 2016.

[2] Deldar, F., and Abadi, M., "Deep Learning for Zero-day Malware Detection and Classification: A Survey," *ACM Computing Surveys*, vol. 56, no. 2, 2023, doi: https://doi.org/10.1145/3605775.

[3] Febiola, A., Manalu, R., Ajeng, R., Said, K., Gunawan, I., and Satria, H., "Analisis sistem keamanan pada sistem operasi Windows," *Jikomnus*, vol. 1, no. 1, pp. 48–55, 2024, doi: https://doi.org/10.260396/jikomnus.

[4] Iqbal, M., and Khaera Arifin, A., "Analisis aktivitas dan pola serangan Eternalblue dan

Wannacry ransomware yang beraksi pada jaringan Prodi D3 Teknologi Telekomunikasi Universitas Telkom," *Journal of Telecommunication Technology*, vol. 6, no. 2, pp. 2274–2293, 2020.

[5] Kusuma, G. H. A., "Implementasi Volatility dalam menganalisa malware pada memory dump," *Journal of Informatics*, vol. 4, no. 1, pp. 36–43, 2023. [Online]. Available: https://journal.univpancasila.ac.id/index.php/jiac/article/view/5491

[6] M. Nasution, R., "Implementasi metode Secure Hash Algorithm (SHA-1) untuk mendeteksi orisinalitas file audio," *Bulletin of Computer Science Research*, vol. 2, no. 3, pp. 73–84, 2022, doi: https://doi.org/10.47065/bulletincsr.v2i3.140.

[7] Mulqiya, W. Z., and Rilvani, E., "Peningkatan perlindungan pada sistem operasi Windows terhadap gangguan malware," in *Proceedings*, pp. 165–177, 2024.

[8] Nainggolan, S., "Implementasi algoritma SHA-256 pada aplikasi Duplicate Document Scanner," *Resolusi: Rekayasa Teknik Informatika dan Informasi*, vol. 2, no. 5, pp. 201–213, 2022. [Online]. Available: https://djournals.com/resolusi

[9] Novansyah, H., and Sutabri, T., "Analisis malware dengan metode dinamik menggunakan framework Cuckoo Sandbox," *Blantika: Multidisciplinary Journal*, vol. 2, no. 1, 2023. [Online]. Available: https://blantika.publikasiku.id/

[10] Praptono, A., and Yusuf, H., "Tinjauan kriminologi terhadap pelaku kejahatan pemerasan dengan menggunakan virus, ransomware Wannacry sebagai suatu kejahatan modern," *Jurnal Intelek dan Cendikiawan Nusantara*, pp. 1530–1539, 2024. [Online]. Available: https://jicnusantara.com/index.php/jicn/article/view/192

[11] Puji Rahayu, Y. D., and Trianto, N., "Analisis malware menggunakan metode analisis statis dan dinamis untuk pembuatan IOC berdasarkan STIX versi 2.1," *Info Kripto*, vol. 15, no. 3, pp. 105–111, 2021, doi: https://doi.org/10.56706/ik.v15i3.30.

[12] Rahim, I., Anwar, N., Widodo, A. M., Karsono Juman, K., and Setiawan, I., "Komparasi fungsi hash MD5 dan SHA256 dalam keamanan gambar dan teks," *Ikraith-Informatika*, vol. 7, no. 2, pp. 41–48, 2022, doi: https://doi.org/10.37817/ikraithinformatika.v7i2.2249.

[13] Rahman, R., Mulyadi, and Imran, A., "Optimalisasi keamanan data pada sistem operasi Windows melalui penerapan teknologi kriptografi modern," *Jurnal Sistem Informasi dan Ilmu Komputer*, vol. 2, no. 3, pp. 146–166, 2024.

[14] S, S. Y., "Analisis malware tt.exe menggunakan metode static analysis dan dynamic analysis," in *Proceedings*, pp. 860–865, 2015.

[15] Virgiawan A. Manoppo, Arie S. M. Lumenta, and Stanley D. S. Karouw, "Analisa malware menggunakan metode dynamic analysis pada jaringan," *Jurnal Teknik Elektro dan Komputer*, vol. 9, no. 3, pp. 181–188, 2020.

[16] Wahidin, G. W., Syaifuddin, S., and Sari, Z., "Analisis ransomware Wannacry menggunakan aplikasi Cuckoo Sandbox," *Jurnal Repositor*, vol. 4, no. 1, pp. 83–94, 2022, doi: https://doi.org/10.22219/repositor.v4i1.1373.