JSAI : Journal Scientific and Applied Informatics
Vol. 08, No. 2, Juni 2025, hal. 311~320
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

Analisis *Malware* Archer.exe untuk Identifikasi Potensi Ancaman pada Sistem Operasi Menggunakan Metode *Hybrid Analysis*

[1]Juan Haniful Kahfi, [2] Johannes Hamonangan Siregar
[1,2]Universitas Pembangunan Jaya, Indonesia
[1]juan.hanifulkahfi@student.upj.ac.id; [2] johannes.siregar@upj.ac.id;

Article Info

Article history:

Received, 2025-05-22
Revised, 2025-05-26
Accepted, 2025-06-3

Kata Kunci:

Malware
Analisis Dinamis
Analisis Hibrida
Analisis Statis
RAT

ABSTRAK

Keamanan siber menjadi perhatian utama dalam era digital, terutama terhadap serangan *malware* yang menargetkan sistem operasi Windows 10. Penelitian ini bertujuan untuk menganalisis malware jenis Remote Access Trojan (RAT) bernama archer.exe yang diperoleh dari situs *Any.run*. Metode yang digunakan adalah *hybrid analysis*, yaitu kombinasi antara *static analysis* dan *dynamic analysis* untuk memperoleh gambaran menyeluruh mengenai struktur dan perilaku malware. Hasil analisis statis menunjukkan bahwa archer.exe merupakan file berformat *Portable Executable* (PE) dengan ukuran 829,35 KB dan menggunakan teknik *packing* untuk menyembunyikan *payload*-nya. Sementara itu, analisis dinamis mengungkap bahwa malware ini melakukan modifikasi registry, membuat proses turunan seperti rundll32.exe dan cmd.exe, serta melakukan koneksi jaringan ke Command and Control (C2) server dengan alamat IP 192.169.69.26 melalui domain dominoduck2101.duckdns.org. Temuan ini menunjukkan bahwa archer.exe memiliki potensi ancaman untuk mengakses sistem dari jarak jauh, mencuri data, dan menjalankan aktivitas berbahaya tanpa diketahui pengguna. Penelitian ini membuktikan bahwa metode *hybrid analysis* efektif dalam mengidentifikasi ancaman dan perilaku tersembunyi dari *malware* jenis RAT pada sistem operasi Windows 10.

Keywords:

Malware
Dynamic Analysis
Hybrid Analysis
Static Analysis
RAT

ABSTRACT

Cybersecurity has become a primary concern in the digital era, particularly regarding malware attacks targeting the Windows operating system. This study aims to analyze a Remote Access Trojan (RAT)-type malware named archer.exe, obtained from the Any.run platform. The method used is hybrid analysis, a combination of static analysis and dynamic analysis, to provide a comprehensive understanding of the malware's structure and behavior. Static analysis results show that archer.exe is a Portable Executable (PE) file with a size of 829.35 KB and employs packing techniques to conceal its payload. Meanwhile, dynamic analysis reveals that the malware modifies system registry keys, spawns child processes such as rundll32.exe and cmd.exe, and establishes a network connection to a Command and Control (C2) server at IP address 192.169.69.26 via the domain dominoduck2101.duckdns.org. These findings indicate that archer.exe poses a high risk of remote system access, data theft, and malicious background activity without user awareness. This study demonstrates that the hybrid analysis method is effective in identifying hidden threats and malicious behavior of RAT-type malware on Windows 10 systems.

Penulis Korespondensi:

Johannes Hamonangan Siregar
Program Studi Sistem Informasi,
Universitas Pembangunan Jaya,
Email: johannes.siregar@upj.ac.id

1. PENDAHULUAN

Pada era digital saat ini, pemanfaatan teknologi informasi telah merambah ke berbagai sektor kehidupan termasuk ekonomi, pendidikan, dan pemerintahan. Perkembangan digital ini memberikan banyak kemudahan serta

meningkatkan efisiensi, namun di sisi lain, juga memperbesar risiko terhadap keamanan siber terutama dalam keamanan data [12]. Salah satu ancaman terbesar yang dihadapi saat ini adalah serangan malware, khususnya yang menargetkan sistem operasi Windows 10 melalui *file* yang berformat *executable* (.exe). Salah satu jenis *malware* yang sangat berbahaya adalah *Remote Access Trojan* (RAT) karena berisiko pelaku serangan siber untuk mengakses sistem dari jarak jauh serta melakukan berbagai aktivitas berbahaya tanpa sepengetahuan pengguna [10]. Akibatnya, sistem bisa digunakan untuk mencuri data, memantau aktivitas korban, bahkan merusak sistem dan mengunci perangkat.

Untuk mengetahui cara kerja malware dan potensi bahayanya, dapat menggunakan dua metode, yaitu *static analysis* dan *dynamic analysis*. *Static analysis* dilakukan dengan memeriksa struktur file malware, seperti struktur *file* dan *hash*, tanpa menjalankannya. Sedangkan *dynamic analysis* dilakukan dengan mengamati perilaku malware saat dijalankan di lingkungan aman seperti mesin virtual. Gabungan dari kedua metode tersebut disebut *hybrid analysis*, yang dianggap lebih efektif karena mampu memberikan gambaran lengkap—baik dari sisi teknis file maupun dampak yang ditimbulkan saat dijalankan. Penelitian terdahulu, Setiadji menunjukkan bahwa metode ini mampu mendeteksi perubahan registry serta aktivitas komunikasi jaringan yang dilakukan oleh *malware* secara tersembunyi [21].

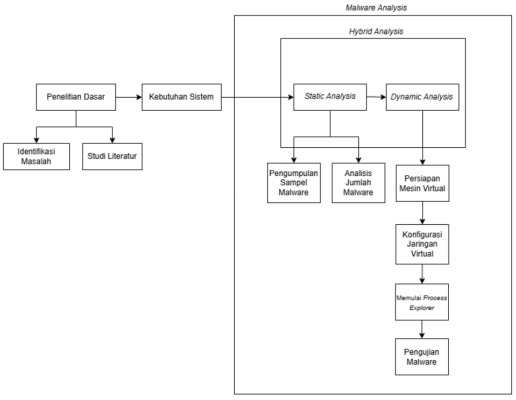
Namun, di Indonesia, masih banyak organisasi dan individu yang belum memahami cara menerapkan metode analisis ini secara optimal. Rendahnya kesadaran dan keterampilan teknis menjadi hambatan utama dalam menghadapi serangan *malware*. Oleh karena itu, penelitian ini dilakukan untuk memberikan pemahaman yang praktis mengenai bagaimana menganalisis *malware* menggunakan pendekatan *hybrid analysis*, dengan fokus pada *malware* bernama archer.exe yang berbasis RAT [4].

Tujuan utama dari penelitian ini adalah untuk mengetahui bagaimana perilaku malware archer.exe saat dijalankan pada sistem operasi Windows 10, serta mengidentifikasi potensi ancaman yang ditimbulkan. Penelitian ini juga bertujuan untuk meningkatkan pemahaman pengguna TI dalam melakukan analisis malware dengan pendekatan yang tepat dan aman. Kontribusi yang dihasilkan dari penelitian ini berupa panduan teknis bagi pengguna TI dalam mendeteksi dan menganalisis *malware*, serta memberikan kasus nyata mengenai aktivitas *malware* berjenis RAT dalam sistem operasi Windows 10. Hasil dari penelitian ini diharapkan dapat menjadi referensi bagi akademisi maupun praktisi dalam menyusun strategi pencegahan dan penanggulangan ancaman siber [2].

Sebagai bagian dari metodologi yang digunakan dalam penelitian ini, serangkaian langkah dilakukan untuk menganalisis *malware*. Langkah pertama adalah pengumpulan sampel *malware*, yang diambil dari situs *Any.run*. Selanjutnya, dilakukan analisis jumlah *hash malware*, dengan mengidentifikasi struktur file *malware*, seperti ukuran *file* dan nilai *hash* MD5 (*Message-Digest Algorithm* 5), menggunakan berbagai alat, yaitu HashCalc, CFF *Explorer*, dan *Detect It Easy* (DIE). Untuk melakukan analisis malware secara aman, persiapan mesin virtual dilakukan dengan menggunakan aplikasi VMware *Workstation* yang menyediakan ruang virtual yang terisolasi. Pada tahap berikutnya, dilakukan konfigurasi jaringan virtual menggunakan perangkat lunak ApateDNS yang diperlukan dalam analisis *malware*. Setelah itu, memulai *Process Explorer* dilakukan untuk menampilkan informasi mengenai proses yang aktif di latar belakang sistem operasi Windows 10 menggunakan *Process Monitor* (ProcMon). Terakhir, pengujian *malware* dilakukan dalam lingkungan virtual untuk memastikan bahwa *malware* tidak menginfeksi perangkat fisik, memungkinkan analisis dilakukan dengan aman [9].

2. METODE PENELITIAN

Sampel *malware* archer.exe yang digunakan dalam penelitian ini diperoleh dari *website* Any.run. Metode *hybrid analysis* adalah kombinasi antara *static* dan *dynamic analysis*, di mana langkah pertama melibatkan pemeriksaan tanda tangan *(signature)* yang ada pada *malware*, kemudian dilanjutkan dengan pengamatan terhadap perilaku *malware* dalam sistem yang terinfeksi [10]. Metode penelitian diterapkan secara berkelanjutan untuk melihat setiap tahap dalam proses penelitian [11].



Gambar 1. Langkah-langkah penelitian

Penelitian Dasar

Penelitian dasar adalah langkah awal dalam proses penelitian [12]. Pada penelitian ini terdapat 2 (dua) cara yang digunakan dalam tahap awal penelitian, yaitu identifikasi masalah, sampel *malware* yang digunakan pada penelitian ini termasuk kedalam kategori RAT (*Remote Access Trojan*) yang memiliki kemampuan untuk mengambil, memodifikasi, atau mengontrol perangkat yang terinfeksi dari jarak jauh. Studi Literatur dilakukan setelah mengidentifikasi masalah, tahap berikutnya adalah mencari referensi yang relevan mengenai cara kerja *malware* serta metode yang diterapkan dalam penelitian ini. Proses ini melibatkan pencarian literatur yang memberikan wawasan tentang bagaimana *malware* beroperasi di dalam sistem dan metode analisis untuk mengidentifikasi perilaku malware. Referensi tersebut mencakup artikel ilmiah dan sumber lainnya yang memastikan penelitian ini didasarkan pada informasi yang valid dan relevan [15].

Kebutuhan Sistem

Setelah penelitian dasar, kebutuhan sistem didefinisikan untuk menentukan komponen yang dibutuhkan dalam menjalankan kegiatan analisis *malware*, termasuk perangkat keras (*hardware*) dan perangkat lunak (*software*). Sistem yang sedang berjalan akan dievaluasi guna mengidentifikasi kelemahan atau kekurangan yang perlu diperbaiki. Proses identifikasi kebutuhan sistem ini bertujuan untuk menemukan solusi terhadap permasalahan yang ada serta menentukan langkah-langkah perbaikan yang harus dilakukan agar sistem dapat berfungsi lebih optimal [13].

Malware Analysis

Pada tahap ini, dilakukan penerapan hasil penelitian dasar yang berkaitan dengan metode yang digunakan dalam analisis *malware*. Proses ini terdiri dari 6 (enam) langkah, yaitu [14]:

1) Pengumpulan Sampel *Malware*: Sampel *malware* diambil dari website Any.run [15].
2) Analisis Jumlah *Hash Malware*: Melakukan identifikasi terhadap karakteristik dasar *malware* seperti informasi ukuran dan nilai *hash* MD5 (*Message-Digest Algorithm* 5) menggunakan *tools HashCalc*, CFF *Explorer,* dan *Detect It Easy* (DIE) [16].
3) Persiapan Mesin Virtual: Ruang lingkup virtual yang dipakai untuk eksekusi *malware* dengan aman. Aplikasi yang digunakan adalah VMware Workstation [18].
4) Konfigurasi Jaringan Virtual: Pada tahap ini, digunakan perangkat lunak ApateDNS untuk mengatur lingkungan jaringan virtual yang diperlukan dalam analisis *malware* [19].
5) Memulai *Process Explorer*: Tahap ini bertujuan untuk menampilkan informasi mengenai proses yang aktif di latar belakang sistem operasi. Perangkat lunak yang digunakan dalam analisis ini adalah *Process Monitor* (ProcMon) [20].
6) Pengujian *Malware*: Pengujian dilakukan dalam lingkungan virtual guna mencegah *malware* menginfeksi perangkat fisik, sehingga analisis dapat dilakukan dengan aman [21].

3. HASIL DAN ANALISIS

Penelitian ini berfokus pada analisis *file malware* bernama archer.exe, yang diperoleh melalui situs https://any.run/. *File* tersebut menjadi objek utama dalam studi ini, dan sejumlah informasi awal terkait sampel *malware* berhasil dikumpulkan. Adapun pendekatan yang digunakan dalam penelitian ini adalah analisis terhadap *malware* berbasis RAT, dengan metode *hybrid analysis*, yaitu gabungan antara *static analysis* dan *dynamic analysis*. Untuk menunjang proses analisis, digunakan berbagai perangkat lunak pendukung seperti ApateDNS, HashCalc, DIE (*Detect It Easy*), CFF *Explorer*, *Process Monitor*, *Wireshark*, serta VMware *Workstation* sebagai lingkungan uji.

Kebutuhan Sistem diperlukan untuk mendukung proses analisis *malware*, sistem yang digunakan diklasifikasikan menjadi dua jenis kebutuhan (*requirement*), yaitu *Hardware Requirement* dan *Software Requirement.* Rincian spesifikasi perangkat keras (*hardware*) yang digunakan dalam proses pengujian *malware* archer.exe disajikan pada tabel 1.

Tabel 1. *Hardware Requirement*

Processor	**Intel Core i5-12500H CPU @ 2.50GHz**
RAM	16 GB DDR4
Storage	SSD 512GB

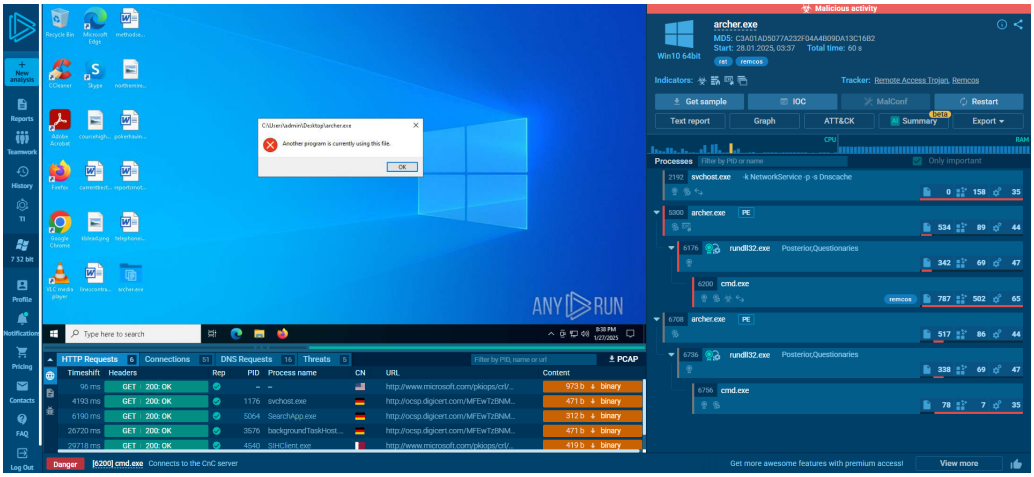
Rincian spesifikasi perangkat lunak (*software*) yang dibutuhkan dalam proses pengujian *malware* archer.exe disajikan pada tabel 2.

JSAI : Journal Scientific and Applied Informatics
Vol. 08, No. 2, Juni 2025, hal. 311~320
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

Tabel 2. *Software Requirement*

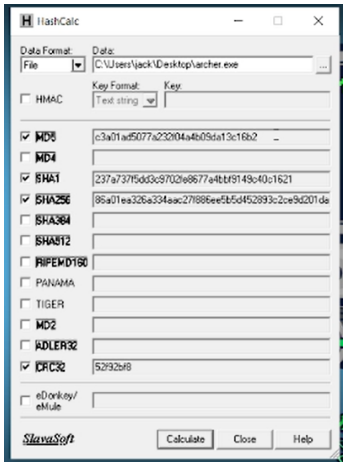
Type	*Spesification*
Operating System	Windows 11 *Home Single Language* 24H2
Virtual Machine Software	VMWare *Workstation Pro v*17.6.0
Virtual Network Software	ApateDNS *v*1.0
Hashing Software	*HashCalc* v2.0, CFF Explorer *v*8.0
Process Monitor	*Process Monitor v*4.01
PE Analyzer	*Detect It Easy v*.3.10

Malware analysis dilakukan dari tahapan pertama yaitu **pengumpulan sampel *malware*** dimulai dengan memperoleh sampel malware yang menjadi objek penelitian. Untuk memperoleh sampel *malware* archer.exe, dilakukan dengan menekan tombol *get sample*, sehingga file *malware* secara otomatis akan diunduh dalam format .rar. File *malware* yang terkompresi tersebut kemudian diekstrak selama proses analisis untuk pengujian *malware*. Proses memperoleh sampel *malware* archer.exe melalui situs *Any.run* dapat dilihat pada gambar 2.



Gambar 2. Tampilan Situs *Any.run*

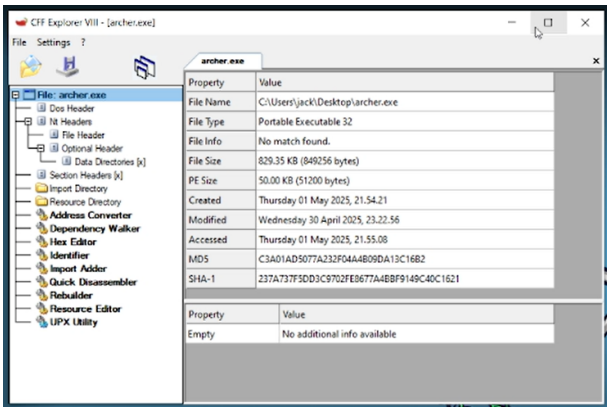
Analisis jumlah *hash malware* menggunakan Hashcalc untuk mengetahui nilai *hash* (*Message Digest Algorithm 5*) MD5 dari *malware* archer.exe. Kegiatan ini bertujuan untuk memverifikasi integritas dari sampel *malware* yang telah diunduh dari situs *Any.run* [9]. Sehingga dapat diketahui bahwa *file* yang telah diunduh tersebut ketika diekstrak tidak mengalami perubahan dan tetap sama saat proses pengumpulan sampel *malware*. Pada gambar 3 merupakan hasil dari kalkulasi Hashcalc menunjukkan file archer.exe mempunyai nilai hash MD5 c3a01ad5077a232f04a4b09da13c16b2.



Gambar 3. Tampilan Hashcalc *Malware* Archer.exe

Analisis terhadap *file* archer.exe menggunakan *software* CFF Explorer berfungsi untuk memeriksa struktur internal dari file yang berformat *Portable Executable* (PE) [16]. Tampilan hasil analisis dapat dilihat pada gambar 4.

JSAI : Journal Scientific and Applied Informatics
Vol. 08, No. 2, Juni 2025, hal. 311~320
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085



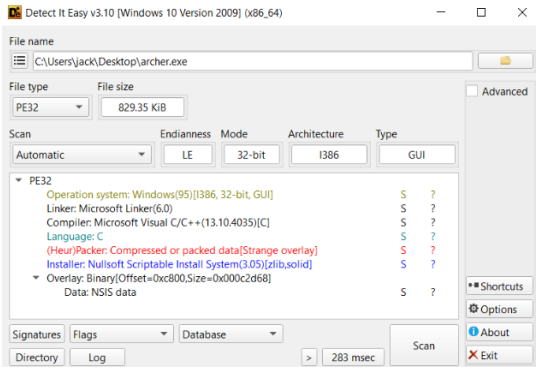
Gambar 4. Tampilan Hasil CFF *Explorer*

Berikut hasil *Static analysis* yang berupa informasi dan jumlah *hash* dari *malware* archer.exe menggunakan *tools* Hashcalc dan CFF Explorer disajikan pada tabel 3:

Tabel 3. *Information about Malware* Archer.exe

Malware Name	archer.exe
MD5	c3a01ad5077a232f04a4b09da13c16b2
File Size	829,35 KB
File Type	*Portable Executable*
PE Size	50,00 KB

Hasil dari *static analysis* dengan menggunakan *tools* Hashcalc dan CFF Explorer ini menunjukkan bahwa *malware* Archer.exe merupakan *malware* yang berformat *Portable Executable* (PE) dengan ukuran file 829,35 KB. Identitas *hash* MD5 dari *malware* archer.exe adalah c3a01ad5077a232f04a4b09da13c16b2 yang digunakan untuk integritas *file* atau memastikan bahwa *file* yang dianalisis sesuai dengan *file* aslinya dan tidak berubah. Perbedaan antara *file size* yang tercatat sebesar 829,35 KB dan *PE size* yang hanya 50,00 KB menunjukkan bahwa sebagian besar ukuran *file* terkompresi. Hal ini mengindikasikan penggunaan teknik *packing*, yang sering kali digunakan oleh *malware* untuk menyembunyikan *payload* berbahaya untuk menghindari deteksi dari *antivirus*. Selanjutnya, dengan menggunakan *tools* analisis *Detect It Easy* (DIE) teridentifikasi bahwa file archer.exe benar menggunakan teknik *packing* yang berfungsi untuk mengompresi atau menyembunyikan data asli di dalam *file* [21]. Temuan ini dapat dilihat melalui *tools Detect It Easy* (DIE), sebagaimana ditunjukkan dalam gambar 5.



Gambar 5. Tampilan Hasil Alat Analisis *Detect It Easy*

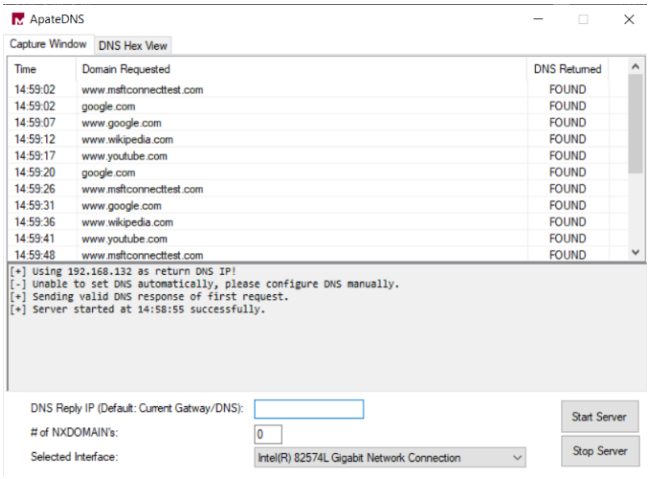
Persiapan mesin virtual dilakukan untuk membuat *virtual machine* sebagai fasilitas pengujian *malware archer.exe* dilingkungan yang terisolasi dengan menggunakan *software* VMware *Workstation*. Mesin virtual dijalankan dengan sistem operasi Windows 10 yang berfungsi serupa dengan komputer fisik pada umumnya serta kompatibel dengan jenis *malware archer.exe* ini [9]. Selain itu, konfigurasi jaringan NAT dapat menghubungkan mesin virtual ke internet melalui *host* fisik dengan tetap menjaga isolasi yang diperlukan, sehingga mencegah *malware* menyebar lebih lanjut ke perangkat fisik. Spesifikasi dari mesin virtual yang digunakan dalam pengujian *malware* archer.exe dapat dilihat pada tabel 4.

JSAI : Journal Scientific and Applied Informatics
Vol. 08, No. 2, Juni 2025, hal. 311~320
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

Tabel 4. *Virtual Machine Spesification*

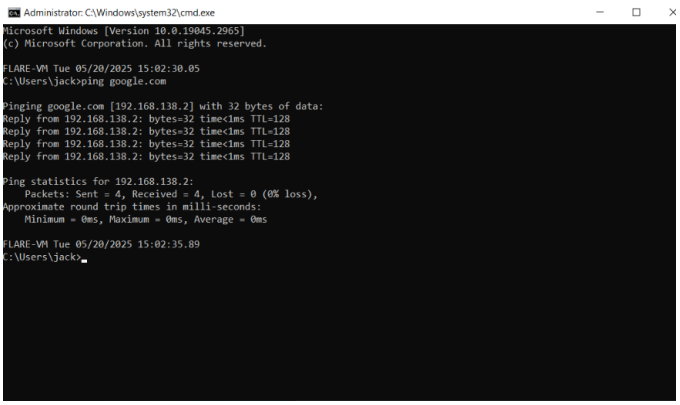
Operating System (Virtual Machine)	Windows 10
RAM	4 GB
Processor	2 Core
Storage	64 GB
Network	*NAT*

Konfigurasi jaringan virtual pada tahapan ini bertujuan untuk membangun jaringan virtual yang dapat dideteksi oleh *malware* saat dijalankan di latar belakang sistem operasi. Jaringan ini meskipun terlihat terhubung ke internet, sebenarnya diisolasi untuk menghindari interaksi langsung dengan jaringan sesungguhnya. Saat tombol *Start Server* ditekan, ApateDNS secara otomatis aktif untuk membentuk *virtual server*, dan mengubah alamat IP localhost menjadi 127.0.0.1, sebagaimana diilustrasikan pada gambar 6. Dengan konfigurasi ini, *malware* yang melakukan koneksi jaringan akan diarahkan ke lingkungan virtual yang terisolasi [9].



Gambar 6. Tampilan ApateDNS Aktif

Untuk memastikan ApateDNS berjalan dengan baik, dilakukan pemeriksaan koneksi menggunakan *Command Prompt* (CMD) dengan menjalankan perintah ping, seperti yang terlihat pada gambar 7. Hasilnya menunjukkan bahwa *software* ApateDNS sudah aktif, dengan melakukan ping ke *domain* google.com, sehingga jaringan perangkat *virtual machine* seperti terkoneksi dengan internet [9].

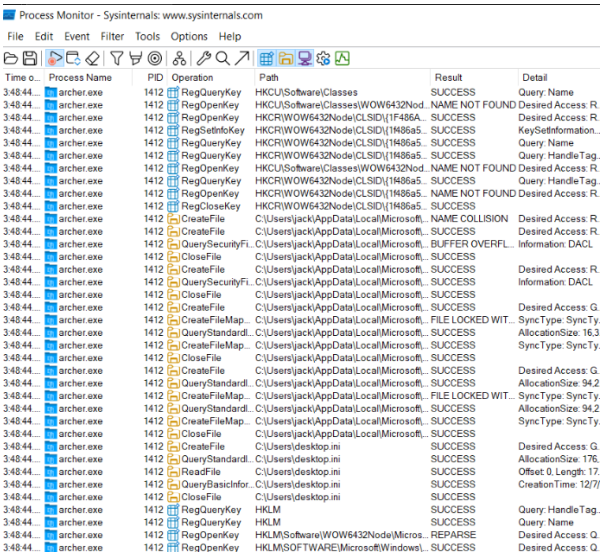


Gambar 7. Tampilan Hasil Ping dari CMD

Memulai *process explorer* dengan alat *Process Monitor* (ProcMon) yang berfungsi untuk memantau dan merekam segala aktivitas atau proses yang berlangsung di latar belakang sistem operasi Windows 10. ProcMon dilengkapi dengan fitur filter yang membantu untuk menyaring dan menampilkan proses-proses tertentu. Merujuk pada gambar 8, ditampilkan log aktivitas dari proses *archer.exe* dengan PID 1412, *malware archer.exe* melakukan operasi *create*

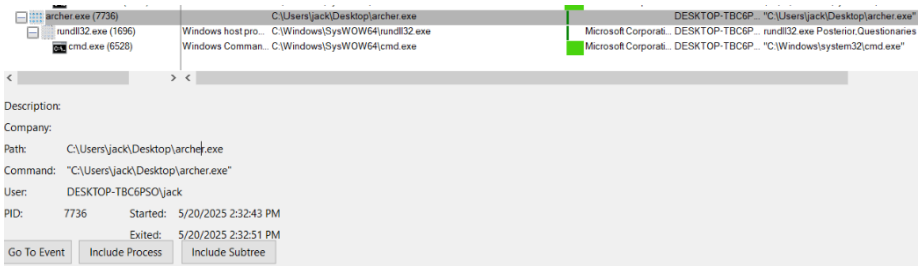
JSAI : Journal Scientific and Applied Informatics
Vol. 08, No. 2, Juni 2025, hal. 311~320
E-ISSN: 2614-3054; P-ISSN: 2614-3062, accredited by Kemenristekdikti, Sinta 4
DOI: 10.36085

file, *read file*, dan *query file* serta melakukan operasi membuka dan memodifikasi *registry key* pada direktori sensitif seperti HKCU, HKCR, dan HKLM.



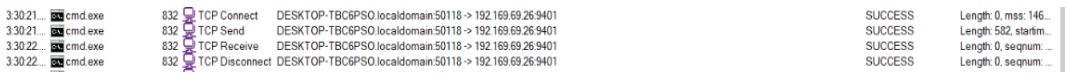
Gambar 8. Tampilan ProcMon

Berdasarkan pengamatan dengan menggunakan fitur *Process Tree* pada ProcMon terhadap eksekusi *file malware* archer.exe, ditemukan indikasi kuat yang menunjukkan aktivitas berbahaya yang konsisten dengan karakteristik *malware*. *Malware* archer.exe membuat proses turunan atau *child process* yaitu program rundll32.exe dan cmd.exe, kedua program ini adalah komponen sistem Windows yang sah. Hal ini dilakukan *malware* ini untuk mengecoh korban maupun *antivirus* agar menganggap proses tersebut merupakan bagian dari aktivitas normal yang sah. Hasil temuan ini dapat dilihat pada gambar 9.



Gambar 9. Tampilan *Process Tree* dari ProcMon

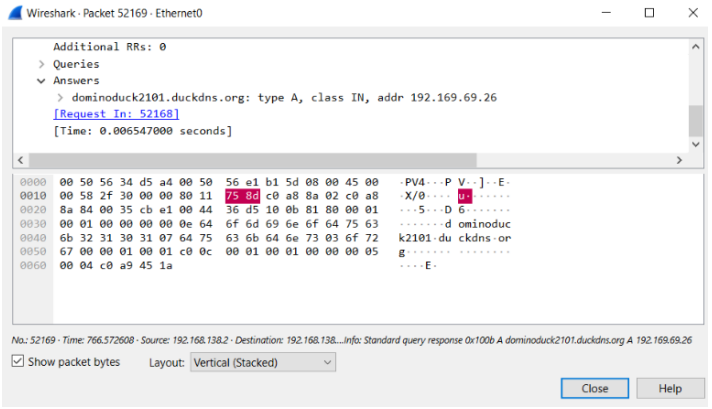
Selanjutnya, pada gambar 10 didapatkan temuan juga bahwa *malware* archer.exe menggunakan program cmd.exe untuk melakukan koneksi internet lewat protokol TCP ke alamat IP 192.169.69.26 pada port 9401. Koneksi ini melibatkan pengiriman dan penerimaan data antara sistem dan server eksternal, yang mengindikasikan adanya komunikasi dua arah. Proses aktivitas jaringan ini berpotensi mengarah pada komunikasi *Command and Control Server* (C2) untuk mengirim perintah, menerima data, dan mengelola *malware* secara *remote* sehingga *malware* dapat melakukan pencurian data, memantau aktivitas korban, serta melakukan kerusakan pada sistem operasi Windows 10 yang terinfeksi.



Gambar 10. Tampilan *Network Process* dari ProcMon

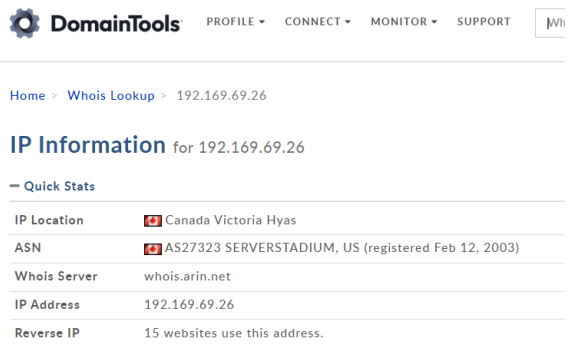
Untuk memperoleh informasi lengkap mengenai aktivitas jaringan tersebut, digunakan *software Wireshark* untuk menangkap paket data yang berkomunikasi dengan sistem [10][17]. Hasil pengamatan dari *Wireshark* menunjukkan bahwa ketika file archer.exe dijalankan pada sistem operasi Windows, terdapat komunikasi antara IP 192.169.69.26 kepada sistem, serta menerima layanan dari alamat *domain host* dominoduck2101.duckdns.org. Karena *malware*

melakukan komunikasi aktivitas jaringan secara berulang dengan memanggil alamat *domain host* dengan alamat IP yang sama, maka alamat dominoduck2101.duckdns.org terindikasi sebagai alamat C2 *Server* dari *malware* archer.exe. Temuan tersebut dapat dilihat pada gambar 11 dibawah ini.



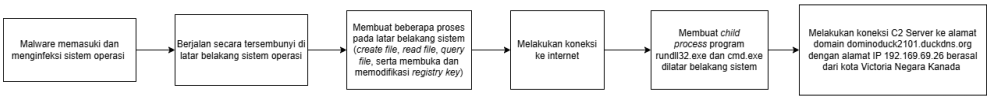
Gambar 11. Tampilan *Detail Wireshark Archer.exe*

Temuan alamat IP yang didapatkan dari *Process Monitor,* selanjutnya dilacak menggunakan *tools whoislookup* dari *domaintools* yang menampilkan hasil informasi dari alamat IP 192.169.69.26 memiliki nama terdaftar AS27323 *SERVERSTADIUM* yang berasal dari negara Kanada dengan alamat kota Victoria, Hyas yang dapat dilihat pada gambar 12.



Gambar 12. Tampilan Hasil *Domaintools*

Berdasarkan temuan dari penelitian yang telah dilakukan, alur perilaku dari *malware archer.exe* saat menginfeksi sistem operasi yaitu berjalan secara tersembunyi di latar belakang sistem operasi dan menjalankan aktivitas seperti membuat, membaca, serta memeriksa file, termasuk melakukan modifikasi pada *registry* sistem operasi Windows 10. Setelah terhubung ke internet, *malware* ini kemudian membuat proses turunan pada program rundll32.exe dan cmd.exe untuk menyamarkan aktivitas berbahayanya sebagai proses sistem yang sah. Setelah itu, *malware* melakukan koneksi jaringan ke *domain host* dominoduck2101.duckdns.org, yang merujuk pada alamat *Command and Control* (C2) *server* dengan alamat IP 192.169.69.26 yang terdaftar di kota Victoria, Kanada. Koneksi ini terindikasi sebagai jalur komunikasi antara penyerang dan sistem yang terinfeksi, sehingga dapat berpotensi *malware* melakukan pencurian data dan mengakses sistem dari jarak jauh (*remote*). Hal ini juga dapat merusak sistem operasi yang terinfeksi oleh *malware* archer.exe ini dikarenakan membuat proses dan operasi yang berbahaya pada latar belakang sistem operasi Windows 10. Alur perilaku ini ditampilkan secara visual pada gambar 13.



Gambar 13. Alur Perilaku dari *Malware* Archer.exe

4. KESIMPULAN

Malware archer.exe teridentifikasi sebagai *file Portable Executable* (PE) yang berukuran 829,35 KB dengan identitas *hash* MD5 c3a01ad5077a232f04a4b09da13c16b2. *Malware* ini juga terindikasi menggunakan teknik *packing*, yang umum digunakan untuk menyembunyikan *payload* berbahaya dari deteksi *antivirus*. Ditemukan alur perilaku berbahaya dari *malware* archer.exe yaitu dengan menginfeksi sistem operasi yang berjalan secara tersembunyi di latar belakang. Setelah itu, *Malware* membuat proses dan operasi berbahaya seperti membuat, membaca, serta memodifikasi *file* dan *registry* pada Windows 10. Setelah terhubung ke internet, malware ini membuat proses turunan menggunakan rundll32.exe dan cmd.exe untuk menyamarkan aktivitasnya. *Malware* kemudian menghubungkan sistem operasi yang terinfeksi ke *C2 server* melalui *domain host* dominoduck2101.duckdns.org dan alamat IP 192.169.69.26. Koneksi ini berpotensi digunakan untuk pencurian data, memantau aktivitas korban secara *remote*, serta dapat merusak sistem operasi. Dengan *hybrid analysis*, penelitian ini berhasil mengidentifikasi karakteristik, perilaku *malware*, serta pola komunikasi berbahaya, yang membuktikan bahwa metode *hybrid analysis* dapat mengidentifikasi potensi ancaman dari *malware* archer.exe yang berjenis RAT pada sistem operasi Windows 10.

REFERENSI

[1] A. Muhammad, G. Mandar, & M. Hamid, "Analisis penggunaan packer perangkat lunak berbahaya(malware) menggunakan teknik reverse engineering", Jurnal Teknik Informatika (J-Tifa), vol. 5, no. 1, p. 6-10, 2021. https://doi.org/10.52046/j-tifa.v5i1.1400

[2] A. N. Yusril, I. Larasati, and P. al Zukri, “SISTEMASI: Jurnal Sistem Informasi Systematic Literature Review Analisis Metode Agile dalam Pengembangan Aplikasi Mobile.” [Online]. Available: http://sistemasi.ftik.unisi.ac.id

[3] A. Triantoro, N. Widiyasono, and R. Gunawan, “Hack. exe Malware Analysis and Investigation Using Memory Forensics,” Ojs.Unud.Ac.Id, vol. 6, no. 2, pp. 94–99, 2021, [Online]. Available: https://ojs.unud.ac.id/index.php/ijeet/article/download/IJEET.2021.v06.i01.p16/39911

[4] B. A. Saputro, L. I. Alfitra, and R. B. Oktaviaji, “Analisis Malware Android Menggunakan Metode Reverse Engineering,” Jurnal Repositor, vol. 2, no. 10, pp. 41–53, 2024, doi: 10.22219/repositor.v2i10.31842.

[5] D. Prayitno, “Systematic Literature Review: Implementasi Metode Statis Dan Dinamis Pada Analisa Malware,” Simetris, vol. 16, no. 2, pp. 53–57, 2022.

[6] F. Bahtiar, N. Widiyasono, and A. P. Aldya, “Memory Volatile Forensik Untuk Deteksi Malware Menggunakan Algoritma Machine Learning,” Jurnal Teknik Informatika dan Sistem Informasi, vol. 4, pp. 242–253, 2018.

[7] Faliandy, M. Y. Lazuardi, and T. Sutabri, "Analisis kesadaran keamanan siber pada pengguna aplikasi e-court di lingkungan pengadilan", Jurnal Ilmiah Binary Stmik Bina Nusantara Jaya Lubuklinggau, vol. 5, no. 2, p. 101-107, 2023. https://doi.org/10.52303/jb.v5i2.106

[8] H. Chotimah, "Tata kelola keamanan siber dan diplomasi siber indonesia di bawah kelembagaan badan siber dan sandi negara [cyber security governance and indonesian cyber diplomacy by national cyber and encryption agency]", Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, vol. 10, no. 2, p. 113-128, 2019. https://doi.org/10.22212/jp.v10i2.1447

[9] H. N. Aditya, N. Widiyasono, and A. Rahmatulloh, “Analisis Malware Aquvaprn.exe Untuk Investigasi Sistem Operasi Dengan Metode Memory Forensics,” Jurnal Teknik Informatika dan Sistem Informasi, vol. 10, no. 2, pp. 161–172, Aug. 2024, doi: 10.28932/jutisi.v10i2.6562.

[10] I. Gunawan and A. Ferriyan, “Analisis Malware Botnet Proteus Pendekatan Static dan Dinamic,” JR : JURNAL RESPONSIVE Teknik Informatika, vol. 1, no. 1, pp. 12–17, 2017, doi: 10.36352/jr.v1i1.91.

[11] M. Machlul, "Peningkatan kualitas sdm melalui pelatihan cyber security pada anggota polisi daerah jawa timur", Parta Jurnal Pengabdian Kepada Masyarakat, vol. 4, no. 2, p. 150-155, 2024. https://doi.org/10.38043/parta.v4i2.4655

[12] M. O. Hoshmand and S. Ratnawati, “Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity,” 2023. [Online]. Available: https://jurnal.politap.ac.id/index.php/aicoms

[13] M. R. Fadli, “Memahami desain metode penelitian kualitatif,” Humanika, vol. 21, no. 1, pp. 33–54, 2021, doi: 10.21831/hum.v21i1.38075.

[14] N. Zalavadiya and Dr. P. Sharma, "A Methodology of Malware Analysis, Tools and Technique for windows platform – RAT Analysis," International Journal of Innovative Research in Computer and Communication Engineering, vol. 5, no. 3, pp. 5042–5054, 2017, doi: 10.15680/IJIRCCE.2017.

[15] S. Almarri and P. Sant, "Optimised Malware Detection in Digital Forensics," International Journal of Network Security & Its Applications, vol. 6, no. 1, pp. 1–15, 2014, doi: 10.5121/ijnsa.2014.6101.

[16] S. Megira, A. R. Pangesti, and F. W. Wibowo, "Malware Analysis and Detection Using Reverse Engineering Technique," Journal of Physics: Conference Series, vol. 1140, no. 1, 2018, doi: 10.1088/1742-6596/1140/1/012042.

[17] S. Yusirwan, Y. Prayudi, and I. Riadi, "Implementation of Malware Analysis using Static and Dynamic Analysis Method," International Journal of Computer Applications, vol. 117, no. 6, pp. 11–15, 2015, doi: 10.5120/20557-2943.

[18] V. A. Manoppo, A. S. M. Lumenta, and S. D. S. Karouw, "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi," Jurnal Teknik Elektro dan Komputer, vol. 9, no. 3, pp. 181–188, Sep.-Des. 2020. Available: https://ejournal.unsrat.ac.id/index.php/elekdankom.

[19] Y. D. Puji Rahayu and Nanang Trianto, "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: 10.56706/ik.v15i3.30.

[20] Y. Herdiana, Z. Munawar, & N. Putri, "Mitigasi ancaman resiko keamanan siber di masa pandemi covid-19", Jurnal Ict Information Communication & Technology, vol. 20, no. 1, p. 42-52, 2021. https://doi.org/10.36054/jict-ikmi.v20i1.305

[21] Y. Setiadji, "Identifikasi malware berdasarkan artefak registry windows 10 menggunakan regshot dan cuckoo", Jurnal Edukasi Dan Penelitian Informatika (Jepin), vol. 8, no. 3, p. 482, 2022. https://doi.org/10.26418/jp.v8i3.57208