Analisis Perilaku Malware Malware Menggunakan Metode Analisis Dinamis

1st Khalif Ibrahim
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
khalifi@student.telkomuniversity.ac.id

2nd Favian Dewanta
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
favian@telkomuniversity.ac.id

3rd Niken Dwi Wahyu Cahyani
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
nikencahyani@telkomuniversity.ac.id

***Abstrak* — Malware merupakan sebuah perangkat lunak atau software yang diciptakan untuk menyusup atau merusak sistem komputer. Penyebaran malware saat ini begitu mudah baik melalui iklan-iklan tertentu pada website, USB flashdrive, dan media lainnya. Semuanya sangat erat kaitannya dengan tindak kejahatan seperti pencurian file, internet banking, kartu kredit dan lain sebagainya. Berkaitan dengan hal tersebut, ada suatu bidang yang menangani tindak kejahatan yaitu forensik digital. Salah satu tahapan dalam forensik digital yaitu melakukan analisis terhadap barang bukti digital, dalam hal ini adalah malware. Untuk membuktikan suatu software dikatakan malware adalah dengan mengetahui cara kerja program tersebut pada sistem komputer. Metode pengujian malware dengan analisis dinamis merupakan metode yang paling akurat untuk menganalisa cara kerja malware. Pada Tugas Akhir ini, digunakan metode Malware Analisis Dinamis melalui pengujian Regshot dan Wireshark untuk menganalisa 6 sample malware yang tersedia, yaitu Poison Ivy, Gen Variant Johnnie 97338, Trojan GenericKD 40427213, Dropped:Trojan.AgentWDCR. PZW, 32.Trojan.Raasmd.Auto dan Gen:Variant.Strictor.171520. Dari pengujian tersebut diperoleh hasil melalui metode Regshot terdapat perubahan Registry terbanyak oleh malware Dropped:Trojan.AgentWDCR.PZW yaitu 163 Registry. Sedangkan dalam Metode Wireshark, malware yang mengirimkan protocol paling banyak adalah Gen:Variant.Strictor.171520 sebanyak 1998 protocol.**

***Kata kunci*— Forensik Digital; Analisis Malware; Dynamic Analysis; Trojan; Gen; Poison Ivy; Wireshark; Regshot; Protocol.**

I. PENDAHULUAN

Perkembangan teknologi pada saat ini begitu pesat, semakin canggih teknologi maka semakin tinggi tingkat kejahatan di dunia maya maupun digital. Penyalahgunaan kecanggihan teknologi yang pesat salah satunya yaitu pengambilan data infomasi tanpa sepengetahuan pemiliknya. Saat sekarang salah satu ancaman yang sangat besar dan sangat merugikan bagi seseorang yaitu malicious software atau yang dikenal dengan sebutan malware. Pada penelitian sebelumnya yang dilakukan oleh Virgiawan A. Manoppo1 , Arie S. M Lumenta2 , dan Stanley D. S. Karouw3 (2020) telah dilakukan penelitian analisis malware menggunakan analisis dinamis menggunakan Cuckoo Sandbox pada Jaringan Universitas Sam Ratulangi. Penelitian mereka melakukan simulasi perilaku dari program malware pada sebuah Jaringan di dalam Universitas dan dianalisa menggunakan Cuckoo Sandbox lalu bisa terlihat tingkat malicious malware berdasarkan hasil yang didapatkan dalam VirusTotal [2].

Dengan adanya penelitian sebelumnya, pada tugas akhir ini dikembangkan penelitian dengan menambahkan 5 buah file malware baru untuk dianalisis selain Poison Ivy, yaitu : Trojan GenericKD 40427213, 32.Trojan.Raasmd.Auto, Dropped:Trojan.AgentWDCR.PZW, Gen:Variant.Strictor. 171520, dan Gen Variant Johnnie 97338. Metode yang akan digunakan adalah analisis malware dinamis dengan menggunakan Regshot dan Wireshark agar dapat diketahui bagaimana perilaku malware saat dijalankan.

II. KAJIAN TEORI

A. Malware

Malware (malicious software) merupakan program yang dirancang untuk disusupkan ke dalam sebuah sistem dengan tujuan untuk melakukan beraneka ragam ditimbulkan dapat berkisar mulai dari sekedar memperlambat kinerja sistem hingga merusak bahkan menghancurkan data penting yang tersimpan dalam sistem yang dimaksud.

B. Model Analisis Malware

Pada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Oleh karena itulah maka model analisis yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu : bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak. [4]:

1. Analisis Dinamis (Dynamic Analysis)

Analisis malware dinamis merupakan sebuah proses untuk mempelajari perilaku malware dengan menjalankannya pada lingkungan yang diawasi. Tipe analisis ini memerlukan lingkungan yang aman, seperti virtual machine dan sandbox, untuk mencegah penyebaran malware. Dalam desain lingkungan analisis malware harus ada beberapa tools yang bisa mengcapture setiap gerakan malware secara detail dan bisa memberikan feedback yang

relevan. Virtual Sistem biasa digunakan untuk menjalankan percobaan tersebut. Analisis dinamis dilakukan dengan menjalankan sampel malware pada sebuah ruang lingkup yang dikontrol dan dimonitor selama ia berjalan. Pada beberapa kasus, analisis statis tidak menampilkan informasi yang banyak dikarenakan obfuscation, dan packing. Pada kasus seperti ini, Analisis Dinamis adalah cara terbaik untuk mengidentifikasi fungsionalitas malware. Analisis dinamis pada penelitian ini dilakukan dengan menggunakan metode Regshot dan Wireshark.

III. METODE

A. Desain Sistem

Pada tahap ini proses mendeteksi dan menganalisis malware dugunakan metode analisis dinamis akan melalui beberapa tahapan yang terdiri dari membangun Virtual Lab, Menjalankan Malware, Analisis Perilaku Malware, dan Analisis Malware Otomatis (Regshot). Perancangan sistem ini dilakukan bertujuan untuk melakukan identifikasi dan analisis apa saja yang dilakukan oleh malware

B. Membangun Virtual Lab

Proses analisis malware memerlukan sebuah lingkungan yang aman (virtual lab, dimana peneliti dapat dengan bebas melakukan analisa terhadap malware, tanpa harus khawatir malware tersebut akan menyebar dan menimbulkan kerusakan terhadap komputer. Virtual lab yang dimaksud dalam penelitian ini adalah sebuah mesin virtual yang didalamnya sudah terinstal berbagai macam tools yang diperlukan untuk kegiatan analisa. Program untuk mesin virtual yang digunakan dalam penelitian ini adalah Virtualbox.

C. Menjalankan Malware

Dalam tahap ini dilakukan pengujian dengan menjalankan sampel file malware (Poison Ivy, Gen, Trojan) pada virtual lab. Proses menjalankan malware berbeda beda untuk setiap malware. Pertama setelah didapatkan malware dari website dasmalwerk.eu dilakukan ekstraksi pada file ZIP yang telah diunduh, setelah itu dilakukan konversi file pada setiap malware yang telah diunduh agar dapat dijalankan, contohnya mengubah ekstensi file menjadi html atau exe, setelah itu malware dijalankan dengan dilakukan double click pada file malware yang telah dikonversi sehingga dapat menghasilkan informasi mengenai perilaku apa saja yang dilakukan oleh malware terhadap sistem ketika file tersebut dijalankan

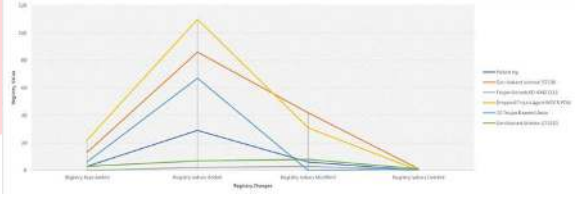
D. Analisis Perilaku Malware

Dalam proses analisis akan diperiksa secara keseluruhan proses yang berjalan pada komputer seperti perubahan registry, aktivitas komunikasi jaringan dan peristiwa janggal lainnya yang terjadi ketika telah terinfeksi oleh malware. Proses analisis terhadap perubahan pada sistem registry menggunakan program pendukung Regshot, yang mana dengan program regshot ini Peneliti akan melakukan analisis pada sistem registry dengan cara membandingkan snapshot dari registry sebelum malware diaktifkan dan snapshot dari registry setelah program malware diaktifkan sehingga akan dapat diketahui perbedaan dan aktifitas apa saja yang telah dilakukan oleh malware terhadap perubahan registry sistem. Sedangkan Wireshark dalam penelitian ini digunakan untuk menganalisa kinerja jaringan, tujuannya agar didapatkan informasi mengenai kemungkinan adanya indikasi yang ditimbulkan oleh perilaku malware terhadap sistem jaringan.

IV. HASIL DAN PEMBAHASAN

A. Hasil Analisis

Malware pada Regshot Hasil pengujian Regshot penelitian ini dapat dilihat pada Gambar 4.2 Grafik Hasil Pengujian Regshot. Grafik tersebut menunjukkan kemampuan setiap malware dalam melakukan perubahan registry. Dari grafik tersebut terlihat bahwa sacara umum kemampuan malware pada setiap jenis attack pada registry cukup konsisten dengan Dropped:Trojan.AgentWDCR.PZW adalah malware paling berbahaya, diikuti oleh malware Gen Variant Johnnie 97338 dan 32.Trojan.Raasmd.Auto sebagai malware berbahaya peringkat 2 dan 3 pada penelitian ini.



GAMBAR 4.2.
Grafik Perbandingan Hasil Pengujian Regshot

Hasil pengujian analisis dinamis metode Regshot penelitian ini dapat dilihat pada Tabel 4.1. Hasil Pengujian Regshot 6 Sampel Malware Penelitian. Tabel 4.1 menampilkan kemampuan setiap malware dalam menambah key registry (registry keys added), menambah nilai registry (registry values added), mengubah nilai registry (registry values modified), dan menghapus nilai registry (registry values deleted).

Tabel 4.1 Hasil Pengujian Regshot 6 Sampel Malware Penelitian menunjukkan hasil pengujian yang dilakukan menggunakan teknik Regshot bahwa malware Dropped:Trojan.AgentWDCR.PZW memiliki perubahan registry yang paling dominan diantara malware lain yaitu dengan 22 penambahan registry keys, 110 perubahan jumlah registry, dan 31 registry yang dimodifikasi. Hasil ini menunjukkan bahwa malware Dropped:Trojan.AgentWDCR.PZW merupakan malware yang paling berbahaya karena memiliki kemampuan mengubah registry paling kuat.

TABEL 4.1
Hasil Pengujian Regshot 6 Sampel Malware Penelitian

No	Malware	Registry Keys Added	Registry Values Added	Registry Values Modified	Registry Values Deleted
1	Poison Ivy	3	29	6	0
2	Gen Variant Johnnie 97338	13	86	42	1
3	Trojan GenericKD 40427213	0	2	3	0

4	Dropped:Trojan.AgentWDCR.PZW	22	110	31	0
5	32.Trojan.Raasmd.Auto	6	67	0	1
6	Gen:Variant.Strictor.171520	3	7	8	1

B. Hasil Analisis Malware pada Wireshark

Hasil pengujian Wireshark penelitian ini dapat dilihat pada Tabel 4.2. Protocol menunjukkan tipe data yang dapat ditransmisikan dan kode perintah untuk mengirim dan menerima data, serta bagaimana transfer data terkonfirmasi. Protocol mirip dengan bahasa pemrograman dan setiap protocol memiliki rules dan vocabulary sendiri. Tipe protocol terbagi 4 yaitu: Transmission Control Protocol (TCP), Internet Protocol (IP), User Datagram Protocol (UDP), dan Post office Protocol (POP). Wireshark memiliki library yang mampu menganalisis 3000 protocol. Hasil pengujian Wireshark pada Tabel 4.2 menunjukkan bahwa malware Gen:Variant.Strictor.171520 merupakan malware yang paling berbahaya karena memiliki kemampuan untuk melakukan intersepsi dan transmisi data pada 1993 protocol, terbanyak diantara malware lainnya.

Tabel 4.2. Hasil Pengujian Metode Wireshark 6 Sampel

No	*Malware*	*Protocol*
1	Poison Ivy	0
2	Gen Variant Johnnie 97338	0
3	Trojan GenericKD 40427213	0
4	Dropped:Trojan.AgentWDCR.PZW	1922
5	32.Trojan.Raasmd.Auto	136
6	Gen:Variant.Strictor.171520	1993

C. KESIMPULAN

A. Kesimpulan

Berdasarkan pengujian yang telah dilakukan di penelitian Tugas Akhir ini dapat disimpulkan bahwa :

1. Malware yang paling berbahaya dari 6 sampel penelitian menggunakan metode Regshot adalah Dropped:Trojan.AgentWDCR.PZW dengan 22 registry keys added, 110 registry values added, dan 31 registry values modified. Malware yang paling aktif mengirimkan data ke pemilik malware dengan metode Wireshark adalah Gen:Variant.Strictor.171520 yaitu 1993 protocol.
2. Analisis dinamis terhadap malware dilakukan dengan menjalankan sampel malware pada sebuah ruang lingkup yang terkendali dan perilaku malware diuji dengan metode Regshot dan Wireshark.
3. Analisis dinamis metode Regshot dilakukan dengan men-capture registry sebuah sistem sebelum diinjeksi malware, lalu malware dimasukan kedalam sistem, setelah itu dilakukan capture untuk yang kedua kali untuk membandingkan perubahan registry yang dilakukan oleh malware.
4. Analisis dinamis metode Wireshark adalah dengan men-capture protocol apa saja yang dikeluarkan oleh suatu malware untuk melihat apakah malware mengirimkan packet kepada pemilik malware.

B. Saran

Berdasarkan pengujian yang telah dilakukan teridentifikasi saran pengembangan lanjutan dari penelitian ini saran dari penelitian Analisis dan Deteksi Malware Menggunakan Metode Analisis Dinamis sebagai berikut: 1. Pengujian dilakukan pada sistem operasi dan sandbox yang berbeda untuk menganalisis dependensi perilaku malware terhadap sistem operasi maupun lingkungan pengujian. 2. Pengujian dilakukan dengan menggunakan tool yang berbeda untuk menganalisis perbandingan kemampuan tool pada analisis dinamis.

REFERENSI

[1] Kramer, S., Bradfield, J.C.: A general definition of malware. Journal in Computer Virology. 6, 105–114 (2010). https://doi.org/10.1007/s11416-009-0137-1.

[2] Cahyanto, T.A., Wahanggara, V., Ramadana, D.: Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis. Justindo, Jurnal Sistem & Teknologi Informasi Indonesia. 2, 19–30 (2017).

[3] Manoppo, V.A., Lumenta, A.S.M., Karouw, S.D.S.: Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. Jurnal Teknik Elektro Dan Komputer. 9, 181–188 (2020).

[4] Eze, A O., & Chuwonoso, C. (2018). "Malware Analysis and Mitigation in Information Preservation." IOSR Journal of Computer Engineering (IOSRJCE),20(04), 1st ser., 53-62 (accessed Jan 24.2023).

[5] "Pengguna Windows XP Lebih Rentan Terinfeksi Ransomware WannaCry.", https://tekno.tempo.co/read/875272/pengguna-windows-xp-lebih-rentan-terinfeksi-ransomware wannacry (accessed Jan. 29, 2023).

[6] "US military still using Windows XP with a floppy disk to launch missiles.", https://www.defenceview.in/us-military-still-using-windows-xp-with-a-floppy-disk-to-launch missiles/ (accessed Jan. 29, 2023).

[7] "Windows XP remains the dominant OS — at least in one part of the world", https://www.windowscentral.com/windows-xp-remains-dominant-operating-system-least-one-part world (accessed Jan. 29, 2023).

[8] "IT threat evolution in Q3 2022. Non-mobile statistics", https://securelist.com/it-threat evolution-in-q3-2022-non-mobile-statistics/107963/ (accessed Jan 29, 2023).

[9] "Desktop Windows Version Market Share Armenia", https://gs.statcounter.com/windows version-market-share/desktop/armenia/2022 (accessed Jan 29, 2023).

[10] EC-Council. (2020). Certified Ethical Hacker(CEH) Version 11. [[VitalSource Bookshelf version]]. Retrieved from vbk://9781635675337

[11] "Removal instructions for Trojan.Win32.Generic virus", https://www.pcrisk.com/removal guides/15213-trojan-win32-generic-virus (accessed Feb 2, 2023) [12] "Trojan.GenericKD.3016333", https://www.f-secure.com/v descs/trojan_w32_generickd_3016333.shtml (accessed Feb 3, 2023)