Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 693−700
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2908

Analisis Karakteristik Antivirus Berdasarkan Aktivitas *Malware* Menggunakan Analisis Dinamis

Ma'arij Haritsah, Adityas Widjajarto*, Ahmad Almaarif

Fakultas Rekayasa Industri, Program Studi S1 Sistem Informasi, Telkom University, Bandung
Jl. Telekomunikasi. 1, Terusan Buahbatu - Bojongsoang, Telkom University, Sukapura, Kec. Dayeuhkolot, Kabupaten Bandung, Jawa Barat, Indonesia
Email: [1]haritsah@student.telkomuniversity.ac.id, [2,*]adtwjrt@telkomuniversity.ac.id, [3]ahmadalmaarif@telkomuniversity.ac.id
Email Penulis Korespondensi: adtwjrt@telkomuniversity.ac.id
Submitted: **11/01/2023**; Accepted: **31/01/2023**; Published: **31/01/2023**

Abstrak− *Malware*, kependekan dari *"Malicious Software"*, merupakan sebuah program yang dirancang khusus untuk melakukan sebuah aktivitas yang dapat membahayakan perangkat lunak pada perangkat korban. Contoh *malware* yang umum ditemukan seperti *trojan, ransomware dan downloader*. Penting bagi pengguna komputer untuk mengenali dan menghindari *malware* ketika sedang menggunakan perangkat komputer. oleh karena itu, pengguna komputer dapat mengatasi serangan *malware* menggunakan perangkat lunak proteksi yang dikhususkan untuk perangkat komputer menggunakan perangkat lunak Antivirus yang dirancang untuk mencegah, mencari, mendeteksi, dan menghapus jenis *malware* yang telah disebutkan sebelumnya. Pada penelitian ini, metode analisis dinamis digunakan untuk mengetahui aktivitas *malware* dengan cara menjalankannya dan memonitor aktivitas yang terjadi. Metode ini biasanya digunakan untuk mengidentifikasi tindakan yang dilakukan oleh *malware* ketika dijalankan. Hasil penelitian menunjukan bahwa semakin tinggi jumlah aktivitas *malware*, maka semakin tinggi pula metrik yang diuji pada antivirus seperti *CPU, memory, disk,* dan waktu *scan*. Pada fitur *removable drive protection*, antivirus Avast relatif lebih efisien dibandingkan dengan antivirus lain karena memiliki rata-rata penggunaan *CPU, memory* yang rendah, tingkat deteksi yang cukup tinggi, dan waktu *scan* yang cepat. Antivirus Kaspersky relatif paling ampuh dalam mendeteksi sampel *malware* dengan tingkat deteksi 100%. Sedangkan pada antivirus Windows Defender relatif paling lemah dari segi tingkat deteksi karena memiliki tingkat deteksi yang paling rendah.

Kata Kunci: Analisis Dinamis *Malware*; Antivirus; Karakteristik Antivirus; *Malware*; *Removable Drive Protection*; Tingkat Deteksi Antivirus

Abstract− *Malware, short for "Malicious Software", is a program specifically designed to perform an activity that can harm software on a victim's device. Examples of commonly found malware include trojans, ransomware and downloaders. It is important for computer users to recognize and avoid malware when using computer devices. Therefore, computer users can overcome malware attacks by using protection software specifically for computer devices using Antivirus software designed to prevent, find, detect, and remove the types of malware that have been mentioned previously. In this study, the dynamic analysis method is used to determine malware activity by running it and monitoring the activity that occurs. This method is usually used to identify the actions that malware performs when it runs. The results showed that the higher the number of malware activities, the higher the metrics tested on the antivirus, such as CPU, memory, disk, and scan time. Regarding the removable drive protection feature, Avast antivirus is relatively more efficient compared to other antiviruses because it has an average CPU usage, low memory, a fairly high detection rate, and fast scan times. Kaspersky Antivirus is relatively the most effective in detecting malware samples with the highest detection rate of 100%. Meanwhile, the Windows Defender antivirus is relatively the weakest in terms of detection rate because it has the lowest detection rate.*

Keywords: *Antivirus; Antivirus Characteristics; Antivirus Detection Rate; Dynamic Malware Analysis; Malware; Removable Drive Protection.*

1. PENDAHULUAN

Malicious software atau *malware* adalah sebuah program yang dirancang khusus untuk melakukan sebuah aktivitas yang dapat membahayakan perangkat lunak pada perangkat korban seperti *trojan*, *ransomware*, *dan downloader* [1]. *Malware* merupakan program yang sengaja dibuat untuk membahayakan dan merugikan sistem operasi atau data pada komputer [2]. Dengan demikian, dapat dikatakan bahwa *malware (Malicious software)* merupakan program yang dirancang untuk mengganggu kinerja atau dapat juga membahayakan sistem pada komputer.

Untuk mengetahui apa yang dilakukan oleh *malware*, dibutuhkan analisis untuk mengetahui aktivitas apa saja yang dilakukan oleh *malware* dan fungsi apa saja yang digunakan pada sistem setelah *malware* tersebut dieksekusi [3]. Salah satu analisis yang akan dibahas dalam identifikasi *malware* ini adalah metode analisis dinamis. Analisis dinamis dilakukan dengan menjalankan sampel *malware* pada sebuah *environment* yang terkontrol dan ter *monitor* selama proses analisis [4]. Tindakan preventif juga berperan penting dalam mengurangi aktivitas serangan *malware* yang menginfeksi sistem komputer, salah satunya adalah dengan memanfaatkan program antivirus pada perangkat komputer [5]. Antivirus juga dapat melakukan deteksi *signature based* dan *heuristic based* pada sistem menggunakan fitur *scanning* yang terdapat pada *software* itu sendiri [6] [7].

Perangkat lunak antivirus adalah program yang dirancang untuk mencegah, mendeteksi, dan menghapus infeksi *malware* pada perangkat komputasi individu [8]. Antivirus disebut juga sebagai perangkat lunak perlindungan dari serangan *malware*, program ini dapat melindungi perangkat menggunakan beberapa fitur yang

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 693−700
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2908

dimilikinya, salah satunya fitur *removable drive protection*. *Removable drive protection* adalah fitur yang terdapat pada beberapa antivirus yang memungkinkan pengguna untuk memindai perangkat penyimpanan sekunder, seperti *flash drive, hard drive* eksternal, atau kartu *memory*, untuk mencari tahu apakah terdapat *malware* yang menyebar melalui perangkat tersebut sekaligus membersihkan *malware* yang bersarang di dalamnya [9].

Sebelumnya penulis telah mempelajari beberapa penelitian terdahulu yang terkait dengan penelitian yang penulis lakukan. Salah satunya yaitu, "*Comparative Performance Analysis of Anti-virus Software*" oleh Noel Dogonyaro pada tahun 2021, dimana pada penelitian tersebut membahas mengenai bagaimana teknik penghindaran dan pendeteksian *malware* yang berfokus pada analisis kinerja komparatif dari beberapa perangkat lunak antivirus. Hasil analisis tersebut berupa pengukuran parameter yang menawarkan kinerja maksimal dengan mempertimbangkan deteksi *malware*, tingkat penghapusan, dan waktu peluncuran antarmuka paling cepat.

Pada penelitian ini, parameter yang digunakan untuk mengenali karakteristik antivirus yaitu berupa sumber daya komputasi, waktu *scanning* dan tingkat deteksi pada beberapa antivirus menggunakan metode analisis dinamis. metode analisis dinamis digunakan untuk mengevaluasi perilaku *malware* dengan cara menjalankannya dan memonitor aktivitas yang terjadi. Metode ini biasanya digunakan untuk mengidentifikasi tindakan yang dilakukan oleh *malware* ketika dijalankan. Jumlah aktivitas tersebut akan digunakan untuk mengetahui karakteristik antivirus pada fitur *removable drive protection.* Ketika menjalankan fitur *removable drive protection* pada antivirus, performa antivirus sangat penting untuk diperhatikan. Hal ini dikarenakan jika antivirus memiliki performa yang buruk, maka proses pemindaian akan berlangsung lama dan menyebabkan kinerja sistem komputer menjadi terhambat. Selain itu, tingkat deteksi antivirus juga menjadi hal utama dalam melindungi perangkat dari serangan *malware.*

2. METODOLOGI PENELITIAN

Untuk metode pengumpulan data yang mendukung penelitian ini adalah sebagai berikut:

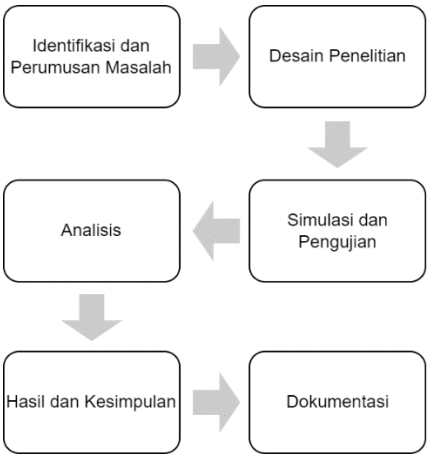
2.1 Metode Kepustakaan

Metode keupstakaan adalah metode dalam mencari, mengumpulkan, serta menganalisis sumber data untuk diolah. Sumber data bisa melalui buku, jurnal, *e-book*, dan modul yang berhubungan dengan penelitian ini [10].

2.2 Sistematika Penelitian

Sistematika penelitian merupakan bagan yang menjelaskan tahapan yang harus dilakukan untuk menyelesaikan penelitian, tahapan yang dilakukan dalam penelitian ini sesuai dengan metode yang telah ditentukan sebelumnya yaitu metode analisis berdasarkan eksperimen [11].

Tahapan-tahapan pada sistematika penelitian yang dilakukan dapat dilihat pada gambar berikut:



Gambar 1. Alur Tahapan Penelitian

2.3 Pengumpulan Data

Dalam penelitian ini pengumpulan data diperoleh dari hasil eksperimen dengan menjalankan atau mengeksekusi *malware* pada sistem, setelahnya dapat dilakukan *monitoring* terhadap sistem yang telah di injeksi *malware* menggunakan metode analisis dinamis berdasarkan aktivitas *malware* yang terdeteksi menggunakan *tools* khusus analisis dinamis, dimana *tools* yang akan digunakan seperti Regshot, Process Explorer, dan SpyStudio berdasarkan *registry changes*, total *DLL* yang digunakan, dan fungsi *API call* yang dijalankan [12] [13] [14].

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 693−700
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2908

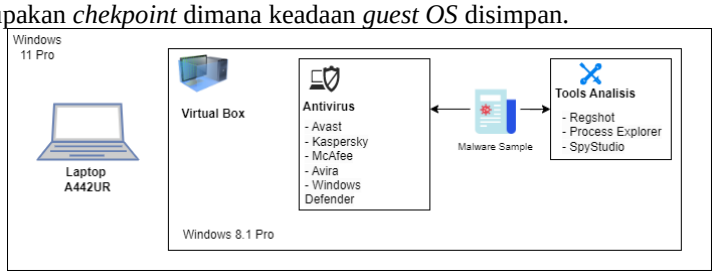
Kemudian antivirus akan menjalankan metode pemindaian pada fitur *removable drive scan* untuk mengetahui karakteristik antivirus [15]. Selanjutnya, proses *scanning* dilakukan pemantauan pada sumber daya komputasi seperti penggunaan *CPU*, dan *memory* serta waktu *scan*, dan tingkat deteksi pada antivirus [16]. Hasil monitoring diukur dan dianalisis guna mengetahui karakteristik antivirus dan menbandingkan karakteristiknya dengan antivirus lain yang diuji [17].

2.4 Pengolahan Data

Berdasarkan temuan pada hasil deteksi *malware* menggunakan metode analisis dinamis dan hasil deteksi pemindaian oleh perangkat lunak antivirus, dilakukan analisis dan diproses untuk dapat mengetahui karakteristik antivirus [18] [19]. Selanjutnya hasil deteksi dari kedua proses tersebut dapat diperoleh data kuantitatif berupa penggunaan sumber daya, waktu *scanning* dan tingkat deteksi terhadap *malware* berdasarkan total aktivitas *malware* menggunakan metode analisis dinamis.

2.5 Desain Lingkungan Virtual

Gambar di bawah ini menunjukkan desain lingkungan *virtual machine* yang terdiri dari beberapa komponen utama, yaitu *core operating system*, virtualBox, sampel *malware*, *tools* analisis dinamis dan *software* antivirus yang dipisahkan menggunakan snapshot. VirtualBox merupakan lingkungan yang terisolasi yang dapat menjalankan sistem operasi dan aplikasi seperti sebuah komputer fisik [20]. Sistem operasi *core* merupakan sistem operasi utama dimana VirtualBox di pasang, sedangkan sistem operasi *guest* merupakan sistem operasi yang di instal di dalam VirtualBox, *tools* analisis dinamis dan antivirus merupakan aplikasi yang di install di dalam *guest OS*, dan *snapshot* merupakan *chekpoint* dimana keadaan *guest OS* disimpan.



Gambar 2. Desain Lingkungan Virtual

2.5 Sampel *Malware*

Gambar Sampel *malware* yang digunakan pada penelitian ini merupakan *file* yang memiliki format *exe*. Sampel *malware* tersebut akan dijalankan pada *virtual machine* Windows 8.1 dan digunakan untuk mengetahui kemampuan antivirus dalam menangani infeksi *malware*. Berikut daftar sampel *malware* yang digunakan pada penelitian ini:

Tabel 1. Sampel *Malware*

Hash	Tanggal Dibuat	Nama CVE	Nama Sampel
046419ffc6e587f8a631	02-01-2018	CVE-2022-4258	Sampel 1 *Trojan*
97437cdf7f697beb41d5	28-01-2018	CVE-2015-8264	Sampel 2 *Trojan*
348902db5e72113a54b	06-02-2018	CVE-2022-23714	Sampel 3 *Ransomware*
21957bfa277e386c9967	05-02-2018	CVE-2022-23714	Sampel 4 *Ransomware*
db825e1f70c6f9b265be	31-01-2018	CVE-2017-15956	Sampel 5 *Downloader*
a1b5a5cd5410656eb13	11-09-2012	CVE-2012-5188	Sampel 6 *Downloader*

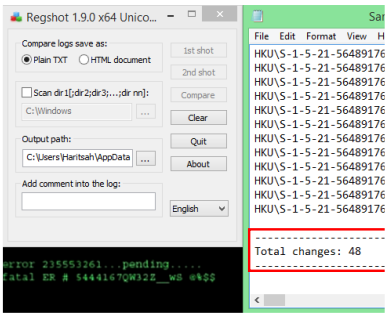
3. HASIL DAN PEMBAHASAN

3.1 Pengujian Analisis Dinamis

Bagian analisis sampel pada *malware* ini merupakan pengujian yang dilakukan oleh peneliti untuk mendapatkan hasil temuan atau aktivitas pada sampel *malware*. Berikut merupakan hasil analisis pada temuan aktivitas *malware:*

1) Pengujian Menggunakan Regshot

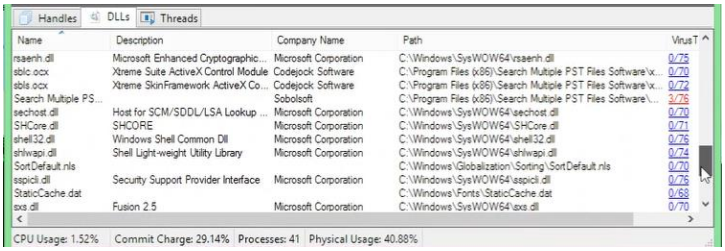
Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 693−700
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2908



Gambar 3. Pengujian Regshot Sampel 1

Gambar 3 merupakan hasil analisis menggunakan Regshot pada sampel 1 *trojan*. Regshot menampilkan hasil bahwa terdapat adanya penambahan 2 *registry key*, 24 *value added*, dan 22 *value modified*, sehingga terdapat total 48 perubahan pada *registry* ketika sampel dijalankan pada sistem *virtual machine*.

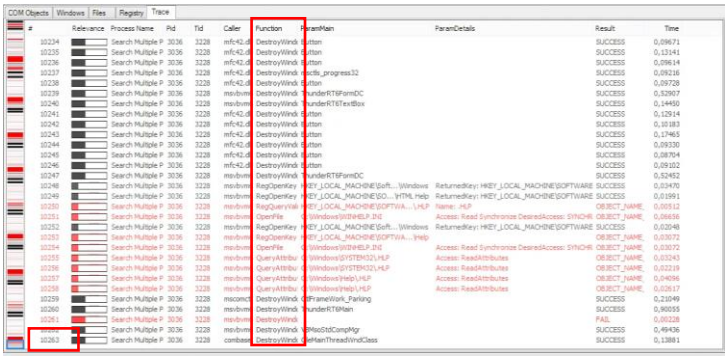
2) Pengujian Menggunakan Process Explorer



Gambar 4. Pengujian Process Explorer Sampel 1

Gambar 4 merupakan hasil analisis menggunakan Process Explorer pada sampel *malware* 1 *trojan*. Process Explorer menampilkan satu *process* yang dijalankan oleh sampel bernama *Search Multiple PST Files Software*, pada kolom Virus Total menunjukkan bahwa *process* tersebut terindikasi sebagai *malware* pada 3 dari 76 antivirus. Pada panel bawah *tab DLLs*, *process* tersebut menautkan sebanyak 60 *DLL* pada sistem, diantaranya terdapat 2 *DLL* yang terindikasi *malware* antara lain MFC42.*DLL*.mui sejumlah 1 dari 75 antivirus, *Search Multiple PST Files Software* sejumlah 3 dari 76 antivirus pada Virus Total.

3) Pengujian Menggunakan SpyStudio



Gambar 5. Pengujian SpyStudio Sampel 1

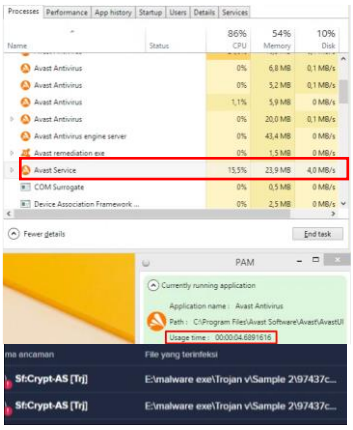
Gambar 5 merupakan hasil analisis menggunakan SpyStudio pada sampel 1 *trojan*. Pada *tab* utama SpyStudio menampilkan hasil data *trace* sejumlah 10263 baris. Pada fitur *statistics* di dalam *tab By Function* menampilkan daftar *API call*s yang dipanggil oleh sampel selama *process execute and hook*, dengan fungsi terbanyak yang dipanggil adalah *RegOpenKey* berjumlah 2556. Jumlah total dari keseluruhan *API call*s yang dipanggil oleh sampel berjumlah 10089 selama dilakukannya pengujian.

3.2 Pengujian Antivirus

Bagian analisis antivirus ini merupakan pengujian yang dilakukan oleh peneliti untuk mendapatkan hasil berupa *profiling* pada fitur *removable drive protection* pada antivirus. Pada penelitian ini, antivirus yang akan diujikan untuk melakukan analisis fitur *removable drive protection* adalah Avast, Kaspersky, Avira, McAfee, dan Windows Defender.

1) Antivirus Avast

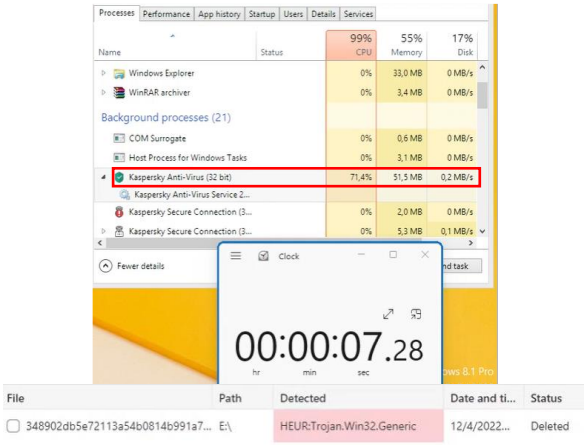
Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 693−700
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2908



Gambar 6. Pengujian pada Sampel 2

Gambar 6 merupakan hasil Pengujian fitur *removable drive protection* antivirus Avast pada sampel 2 *trojan* yang sudah disiapkan dan dianalisis sebelumnya. Beberapa indikator yang diujikan dan dipantau pada sampel tersebut merupakan sumber daya yang digunakan oleh antivirus ketika melakukan proses *scanning* dan bagaimana antivirus menampilkan hasil deteksi *file* ketika proses *scanning* telah selesai.

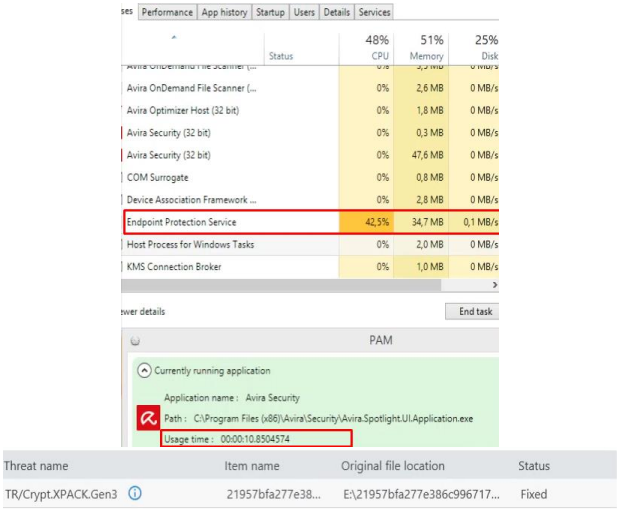
2) Antivirus Kaspersky



Gambar 7. Pengujian pada Sampel 3

Gambar 7 merupakan hasil Pengujian fitur *removable drive protection* antivirus Kaspersky pada sampel 3 *ransomware* yang sudah disiapkan dan dianalisis sebelumnya.

3) Antivirus Avira

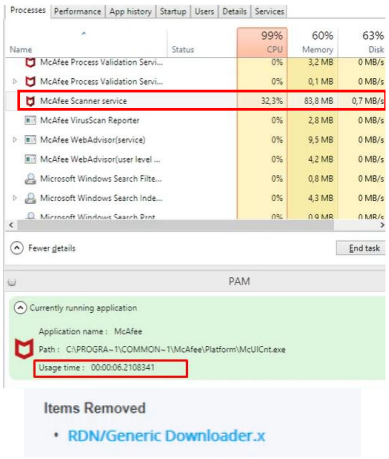


Gambar 8. Pengujian pada Sampel 4 *Ransomware*

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 693−700
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2908

Gambar 8 merupakan hasil Pengujian fitur *removable drive protection* antivirus Avira pada sampel 4 *ransomware* yang sudah disiapkan dan dianalisis sebelumnya.

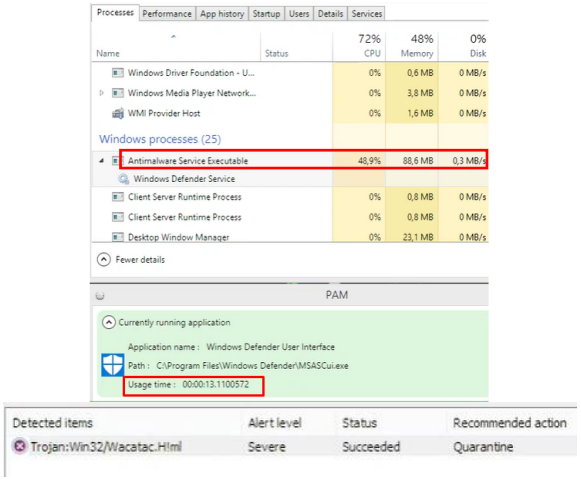
4) Antivirus McAfee



Gambar 9. Pengujian pada Sampel 5

Gambar 9 merupakan hasil Pengujian fitur *removable drive protection* antivirus McAfee pada sampel 5 *downloader* yang sudah disiapkan dan dianalisis sebelumnya.

5) Antivirus Windows Defender

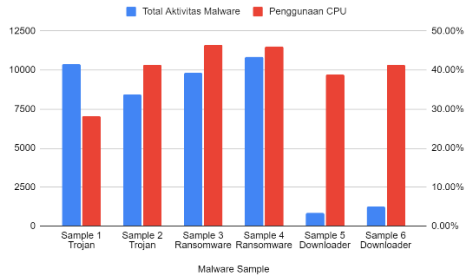


Gambar 10. Pengujian pada Sampel 6

Gambar 10 merupakan hasil Pengujian fitur *removable drive protection* antivirus Windows Defender pada sampel 6 *downloader* yang sudah disiapkan dan dianalisis sebelumnya.

3.3 Perbandingan Total Aktivitas Malware dengan Metrik Antivirus

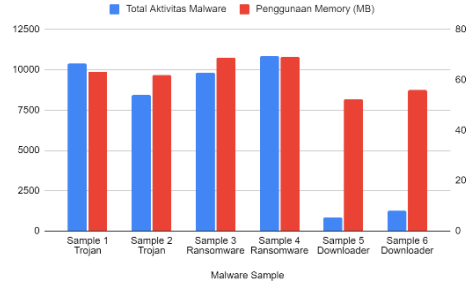
Berikut ini merupakan perbandingan hasil analisis dari total aktivitas *malware* dengan metrik antivirus pada hasil pengujian:



Gambar 11. Total Aktivitas *Malware* dan Penggunaan *CPU* Antivirus

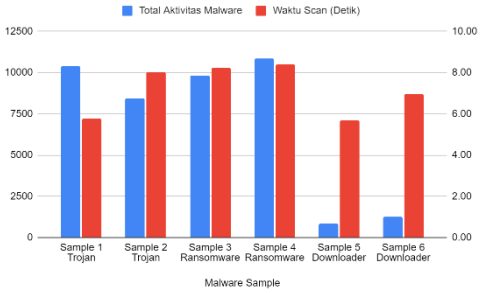
Gambar 11 merupakan perbandingan total aktivitas *malware* dengan Penggunaan *CPU* Antivirus. Jika diperhatikan, gambar menunjukan bahwa semakin tinggi jumlah aktivitas *malware*, maka semakin tinggi pula tingkat penggunaan *CPU* yang dibutuhkan.

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 693−700
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2908



Gambar 12. Total Aktivitas *Malware* dan Penggunaan *Memory* Antivirus

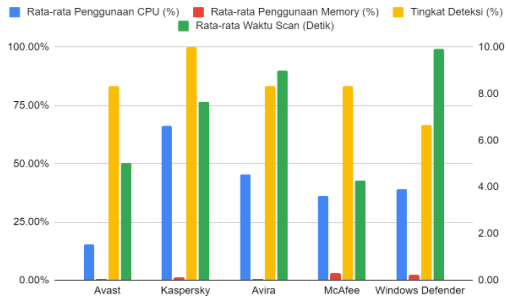
Gambar 12 merupakan perbandingan total aktivitas *malware* dengan Penggunaan *memory* Antivirus. Dari gambar tersebut, terlihat bahwa semakin besar total aktivitas *malware*, maka semakin tinggi penggunaan *memory* yang digunakan untuk melakukan *scanning* pada *malware* tersebut.



Gambar 13. Total Aktivitas *Malware* dan Waktu *Scan* Antivirus

Gambar 13 merupakan perbandingan total aktivitas *malware* dengan waktu *scan* antivirus. Dari gambar tersebut, terlihat bahwa semakin besar total aktivitas *malware*, maka semakin lama waktu yang diperlukan untuk melakukan *scanning* pada *malware* tersebut.

3.4 Perbandingan Software Antivirus



Gambar 14. Perbandingan Antivirus

Pada perbandingan antivirus dalam mendeteksi *malware* pada fitur *removable drive protection*, antivirus Avast merupakan antivirus yang relatif lebih efisien dibandingkan dengan antivirus lain yang diuji karena memiliki rata-rata penggunaan *CPU* dan *memory* yang rendah, tingkat deteksi yang cukup tinggi, dan waktu *scan* yang cepat. Antivirus Kaspersky merupakan antivirus yang relatif paling ampuh dalam mendeteksi sampel *malware* karena memiliki tingkat deteksi 100%.

4. KESIMPULAN

Setelah dilakukannya pengujian dan memperoleh hasil analisis karakteristik antivirus berdasarkan aktivitas *malware* menggunakan analisis dinamis, dapat diambil kesimpulan bahwa perbandingan total aktivitas *malware* dengan metrik antivirus didapatkan bahwa semakin tinggi jumlah aktivitas *malware*, maka semakin tinggi pula metrik yang diuji pada antivirus seperti *CPU, memory, disk dan waktu scan.* Pada perbandingan antivirus dalam mendeteksi *malware*, antivirus Avast merupakan antivirus yang relatif lebih efisien dibandingkan dengan antivirus lain yang diuji karena memiliki rata-rata penggunaan *CPU* dan *memory* yang rendah, tingkat deteksi yang cukup tinggi, dan waktu *scan* yang cepat. Antivirus Kaspersky merupakan antivirus yang relatif paling ampuh dalam mendeteksi sampel *malware* karena memiliki tingkat deteksi 100%. Antivirus Avira dan McAfee merupakan antivirus yang cukup tinggi dalam mendeteksi *malware*. Sedangkan pada antivirus Windows Defender merupakan antivirus yang relatif paling rendah dibandingkan dengan antivirus lain.

Journal of Information System Research (JOSH)
Volume 4, No. 2, Januari 2023, pp 693−700
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i2.2908

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada Dosen pembimbing Universitas Telkom yang telah mendukung penelitian ini serta segenap rekan-rekan penulis dalam memberikan semangat dan motivasi dalam penelitian ini.

REFERENCES

[1] S. Kramer and J. C. Bradfield, "A general definition of malware," *Journal in Computer Virology*, vol. 6, no. 2, pp. 105–114, May 2010, doi: 10.1007/s11416-009-0137-1.

[2] M. Siddiqui, M. C. Wang, and J. Lee, "A survey of data mining techniques for malware detection using file features," *Proceedings of the 46th Annual Southeast Regional Conference on XX - ACM-SE 46*, 2008, doi: 10.1145/1593105.1593239.

[3] N. Kaur and A. Kumar, "A Complete Dynamic Malware Analysis," *Int J Comput Appl*, vol. 135, no. 4, pp. 20–25, Feb. 2016, doi: 10.5120/ijca2016908283.

[4] 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, pp. 181–188, Jan. 2020, doi: 10.35793/jtek.9.3.2020.29567.

[5] O. Whitehouse, "Antivirus Software," *Engineering & Technology Reference*, Jan. 2014, doi: 10.1049/etr.2014.0006.

[6] A. Bastian, "Improving Antivirus Signature For Detection Ransomware Attacks With Machine Learning," *Smart Comp :Jurnalnya Orang Pintar Komputer*, vol. 10, pp. 30–34, Jan. 2021, doi: 10.30591/smartcomp.v10i1.2190.

[7] Kaspersky, "Apa itu Analisis Heuristik?" 2019. [Online]. Available: https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis

[8] L. Rosencrance, "What is antivirus software (antivirus program)?" Jan. 2017. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/antivirus-software

[9] Techslang, "What is Antivirus Software? — Definition by Techslang." Jan. 2019. [Online]. Available: https://www.techslang.com/definition/what-is-antivirus-software/

[10] J. Danandjaja, "Metode Penelitian Kepustakaan," *Antropologi Indonesia*, vol. 0, no. 52, Jul. 2014, doi: 10.7454/ai.v0i52.3318.

[11] A. A. Pradipta, Y. A. Prasetyo, and N. Ambarsari, "Pengembangan Web E-Commerce Bojana Sari Menggunakan Metode Prototype," *eProceedings of Engineering*, vol. 2, Jan. 2015, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/2726

[12] G. Wagener, A. Dulaunoy, and T. Engel, "An Instrumented Analysis of Unknown Software and Malware Driven by Free Libre Open Source Software." pp. 597–605, Jan. 2008. doi: 10.1109/SITIS.2008.57.

[13] M. Sikorski and A. Honig, *Practical malware analysis : the hands-on guide to dissecting malicious software*. San Francisco No Starch Press, 2012.

[14] O. Aslan and R. Samet, "Investigation of possibilities to detect malware using existing tools," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, Mar. 2018, vol. 2017-October, pp. 1277–1284. doi: 10.1109/AICCSA.2017.24.

[15] Kaspersky, "Removable drives scan." Jan. 2022. [Online]. Available: https://support.kaspersky.com/KES4Linux/11/en-us/193947.htm

[16] A. S. Tanenbaum and H. Bos, *Modern operating systems*, 4th ed. Pearson Education, 2015.

[17] K. Shihab and H. Ramadhan, "Tuning of computer systems using heuristics and system performance tools," *Expert Syst Appl*, vol. 36, pp. 5230–5239, Jan. 2009, doi: 10.1016/j.eswa.2008.06.139.

[18] M. Egele, T. Scholte, E. Kirda, and C. Kruegel, "A Survey on Automated Dynamic Malware-analysis Techniques and Tools," *ACM Comput Surv*, vol. 44, pp. 1–42, Jan. 2012, doi: 10.1145/2089125.2089126.

[19] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, "Dynamic malware analysis in the modern era—A state of the art survey," *ACM Comput Surv*, vol. 52, no. 5, Sep. 2019, doi: 10.1145/3329786.

[20] P. Dash, *Getting started with Oracle VM VirtualBox : build your own virtual enviroment from scratch using VirtualBox*. Packt Pub, 2013.