ANALISIS *HYBRID* DAN *REVERSE ENGINEERING* UNTUK DETEKSI MALWARE *ZEUS* MENGGUNAKAN *YARA RULES*

SKRIPSI

IVAN HARRY CAHYADI 2007422008

KONSENTRASI KEAMANAN SISTEM INFORMASI

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2024

ANALISIS *HYBRID* DAN *REVERSE ENGINEERING* UNTUK DETEKSI MALWARE *ZEUS* MENGGUNAKAN *YARA RULES*

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

IVAN HARRY CAHYADI

2007422008

KONSENTRASI KEAMANAN SISTEM INFORMASI

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2024

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Ivan Harry Cahyadi

NIM : 2007422008

Jurusan/Program Studi : T.Informatika dan Komputer / T.Multimedia dan Jaringan

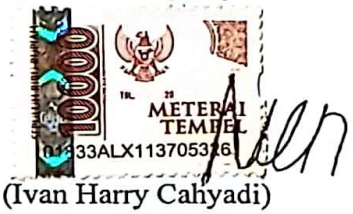
Judul skripsi : Analisis *Hybrid* dan *Reverse Engineering* Untuk Deteksi Malware *Zeus* Menggunakan *Yara Rules*

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 17 Juli 2024

Yang membuat pernyataan



(Ivan Harry Cahyadi)

NIM 2007422008

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Ivan Harry Cahyadi

NIM : 2007422008

Program Studi : Teknik Multimedia dan Jaringan

Judul Skripsi : Analisis *Hybrid* dan *Reverse Engineering* Untuk Deteksi Malware *Zeus* Menggunakan *Yara Rules*

Telah diuji oleh tim penguji dan pembimbing dalam Sidang Skripsi pada hari Selasa, Tanggal 30, Bulan Juli, Tahun 2024, dan dinyatakan **LULUS.**

Disahkan Oleh

Pembimbing I : Defiana Arnaldy, S.Tp., M.Si. ( )

Penguji I : Dr. Indra Hermawan, M.Kom ( )

Penguji II : Ayu Rosyida Zain, S.ST, M.T ( )

Penguji III : Iik Muhamad Malik Matin, S.Kom. M.T. ( )

Mengetahui :

Jurusan Teknik Informatika dan Komputer

Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.

NIP 197908032003122003

KATA PENGANTAR

Puji syukur saya sampaikan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan skripsi ini yang berjudul *Analisis Hybrid dan Reverse Engineering Untuk Deteksi Malware Zeus Menggunakan Yara Rules*. Penulisan ini dilakukan untuk memenuhi salah satu syarat untuk mencapai gelar Diploma Empat Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbigan dari berbagai pihak, mulai dari masa perkuliahan hingga penyusunan laporan skripsi ini, penulis tidak akan mampu menyelesaikannya. Oleh karena itu, penulis mengucapkan terima kasih kepada semua pihak yang telah mendukung, terutama kepada:

1. Bapak Defiana Arnaldy, S.Tp., M.Si., selaku dosen pembimbing, yang telah menyediakan waktu, tenaga, dan pandangan untuk membimbing penulis dalam penyusunan laporan skripsi ini.
2. Ketua jurusan Teknik Informatika dan Komputer Ibu Dr. Anita Hidayati, S.Kom., M.Kom., dan Kepala program studi Teknik Multimedia dan Jaringan Ibu Ayu Rosida Zain, S.ST., M.T..
3. Bapak Dr. Indra Hermawan. M.Kom., selaku dosen mata kuliah Seminar dan Metodologi Penelitian, yang telah membantu penulis dalam penyusunan laporan skripsi ini.
4. Hardi Cahyadi dan Clara Monica Effendi yang telah membantu dan mendukung penulis dalam pengerjaan skripsi.
5. Orang tua dan keluarga serta teman-teman CCIT Security yang telah memberikan bantuan dukungan moral dan material.

Semoga Tuhan Yang Maha Esa membalas segala kebaikan dari semua pihak yang telah membantu.

Depok, 17 Juli 2024

(Ivan Harry Cahyadi)

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama : Ivan Harry Cahyadi

NIM : 2007422008

Jurusan/ProgramStudi : T.Informatika dan Komputer / T.Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

Analisis *Hybrid* dan *Reverse Engineering* Untuk Deteksi Malware *Zeus* Menggunakan *Yara Rules*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalih mediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, 17 Juli 2024

Yang Menyatakan

(Ivan Harry Cahyadi)

NIM 2007422008

ANALISIS *HYBRID* DAN *REVERSE ENGINEERING* UNTUK DETEKSI MALWARE *ZEUS* MENGGUNAKAN *YARA RULES*

ABSTRAK

Kejahatan siber terus meningkat pesat, dan malware menjadi salah satu alat utama yang digunakan. Malware adalah program jahat yang dirancang untuk menyusup dan merusak sistem komputer yang dapat menyebabkan kerugian besar bagi individu dan organisasi. Salah satu jenis malware yang paling banyak beredar adalah Trojan. Contoh yang paling populer adalah Malware Zeus, yang termasuk dalam kategori Banking Trojan. Malware Zeus telah mencuri informasi sensitif seperti email, kata sandi, data keuangan, dan nomor kartu kredit dari pengguna di hampir 200 negara, dan menyebabkan kerugian finansial besar bagi institusi keuangan seperti Bank of America. Analisis malware diperlukan untuk mengetahui dan melawan malware tersebut. Analisis ini dilakukan untuk mengidentifikasi, memahami cara kerja dan mendeteksi malware tersebut pada sistem komputer. Penelitian ini menggunakan Malware Analysis Lab FlareVM sebagai ruang isolasi yang digunakan untuk melakukan analisis malware dengan aman. Metode yang digunakan pada penelitian ini yaitu metode analisis hybrid, reverse engineering dan penggunaan YARA Rules untuk pendeteksian. Hasil dari analisis statis berupa data kuantitatif terkait file malware, seperti jumlah library yang digunakan dan frekuensi kemunculan string tertentu. Analisis dinamis menghasilkan indikator berbasis host seperti jumlah proses yang dihasilkan oleh malware, serta indikator berbasis jaringan yang menunjukkan jumlah koneksi yang dilakukan oleh malware. Data hasil analisis yang diperoleh digunakan untuk merancang YARA Rules yang efektif dan efisien untuk mendeteksi malware zeus pada sistem komputer.

Kata kunci: Analisis *Hybrid*, *Malware Analysis Lab*, Malware *Zeus*, *Reverse Engineering*, *YARA Rules*

DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME i
LEMBAR PENGESAHAN ii
KATA PENGANTAR iii
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS iv
ABSTRAK v
DAFTAR ISI vi
DAFTAR GAMBAR viii
DAFTAR TABEL ix
BAB I 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan dan Manfaat 3
1.5 Sistematika Penulisan 4
BAB II 5
2.1 Malware 5
2.2 Analisis Malware 5
2.3 Malware Analysis Environment and Repository (MAER) 6
2.4 Alat-alat Analisis Malware 7
2.5 Penelitian Sejenis 10
BAB III 12
3.1 Rancangan Penelitian 12
3.2 Tahapan Penelitian 13
3.3 Skenario Analisis 14
3.4 Skenario Pengujian 18
BAB IV 20
4.1 Analisis Kebutuhan Sistem 20
4.2 Perancangan Sistem 21
4.3 Implementasi Sistem 21

4.4 Analisis 27
4.5 YARA Rules 49
4.6 Hasil 52
BAB V 60
5.1 Kesimpulan 60
5.2 Saran 61
DAFTAR PUSTAKA 62
DAFTAR RIWAYAT HIDUP 64

DAFTAR GAMBAR

Gambar 1.1 Diagram Penyebaran Malware Berdasarkan Sistem Operasi 1
Gambar 1.2 Diagram Penyebaran Malware Pada Sistem Operasi Windows 2
Gambar 3.1 Rancangan Penelitian 13
Gambar 3.2 Flowchart Skenario Analisis 14
Gambar 3.3 Flowchart Skenario Pengujian 18
Gambar 4.1 Topologi Jaringan Laboratorium 21
Gambar 4.2 Mengunduh REMnux 22
Gambar 4.3 Mengunduh Windows 10 22
Gambar 4.4 Mengunduh FlareVM 22
Gambar 4.5 Memasang REMnux 23
Gambar 4.6 Memasang Windows 10 23
Gambar 4.7 Menonaktifkan Windows Defender 24
Gambar 4.8 Menonaktifkan Real Time Protection Secara Permanen 25
Gambar 4.9 Menonaktifkan Windows Defender Secara Permanen 25
Gambar 4.10 Memasang FlareVM 26
Gambar 4.11 Berhasil Memasang FlareVM 26
Gambar 4.12 Konfigurasi Jaringan Laboratorium 27
Gambar 4.13 Hasil Pemindaian Malware Zeus Menggunakan VirusTotal 28
Gambar 4.14 Bagian Malware Zeus 30
Gambar 4.15 Magic Byte Malware Zeus 32
Gambar 4.16 String Tidak Aman Malware Zeus 32
Gambar 4.17 String Berbahaya Malware Zeus 33
Gambar 4.18 Ekstrak String Malware Zeus 38
Gambar 4.19 String Domain Malware Zeus 39
Gambar 4.20 Kemampuan Malware Zeus 40
Gambar 4.21 Graph Pertahanan Evasion Malware Zeus 42
Gambar 4.22 Disassembly Pertahanan Evasion Malware Zeus 42
Gambar 4.23 String Acak 43
Gambar 4.24 Disassembly String Acak 43
Gambar 4.25 Menjalankan INetSim 45
Gambar 4.26 Pohon Proses Malware Zeus 1 45
Gambar 4.27 Pohon Proses Malware Zeus 2 46
Gambar 4.28 Memantau Proses Malware Zeus 46
Gambar 4.29 Tangkapan Paket Jaringan Malware Zeus 47
Gambar 4.30 Follow TCP Stream Paket Protokol HTTP Malware Zeus 48
Gambar 4.31 YARA Rules Malware Zeus 50
Gambar 4.32 Hasil Deteksi Langsung File Malware Zeus 56
Gambar 4.33 Compiled YARA Rules 57
Gambar 4.34 Hasil Deteksi Pada Sistem Komputer 58
Gambar 4.35 Hasil Deteksi Berdasarkan Karakteristik Malware yang Sama 59

DAFTAR TABEL

Tabel 2.1 Penelitian Sejenis 10
Tabel 4.1 Informasi Umum Malware Zeus 29
Tabel 4.2 Persentase Jenis File Executeable Malware Zeus 29
Tabel 4.3 Persentase Jenis File Data Malware Zeus 31
Tabel 4.4 Library Malware Zeus 32
Tabel 4.5 String Berbahaya Malware Zeus 34
Tabel 4.6 Teknik String Malware Zeus 37
Tabel 4.7 Tipe String Malware Zeus 39
Tabel 4.8 Distribusi Pengaruh Malware Zeus (Berbasis-host) 47
Tabel 4.9 Distribusi Pengaruh Malware Zeus (Berbasis-jaringan) 48
Tabel 4.10 Hasil Analisis 52
Tabel 4.11 Frekuensi Kemunculan String 56
Tabel 4.12 Sampel Pengujuian Malware 58

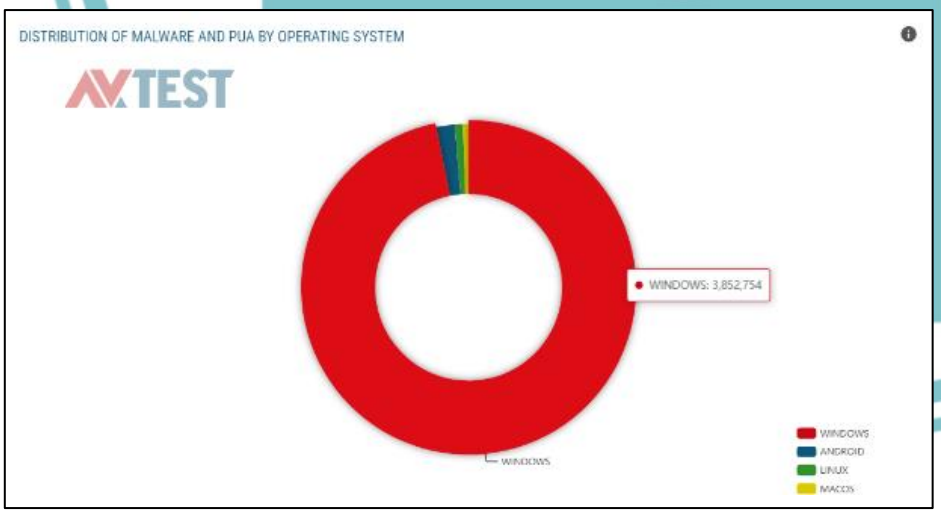
BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa tahun terakhir, hampir setiap masyarakat telah menggunakan internet untuk kehidupan sehari-hari. Kehadiran internet memberikan kemudahan dalam interaksi sosial dan perbankan online. Namun, seiring dengan pesatnya perkembangan internet, kejahatan *cyber* juga semakin meningkat. Para pelaku kejahatan memanfaatkan perangkat lunak berbahaya, yang dikenal sebagai malware untuk meluncurkan serangan terhadap perangkat korban. (Aslan and Samet, 2020) Malware berbentuk program yang dapat mengeksploitasi file-file penting dalam komputer. Ada bermacam-macam jenis malware yaitu *Worm, Trojan, Ransomware, Backdoor,* dan lainnya. (Ilhamdi and Kunang, 2020)

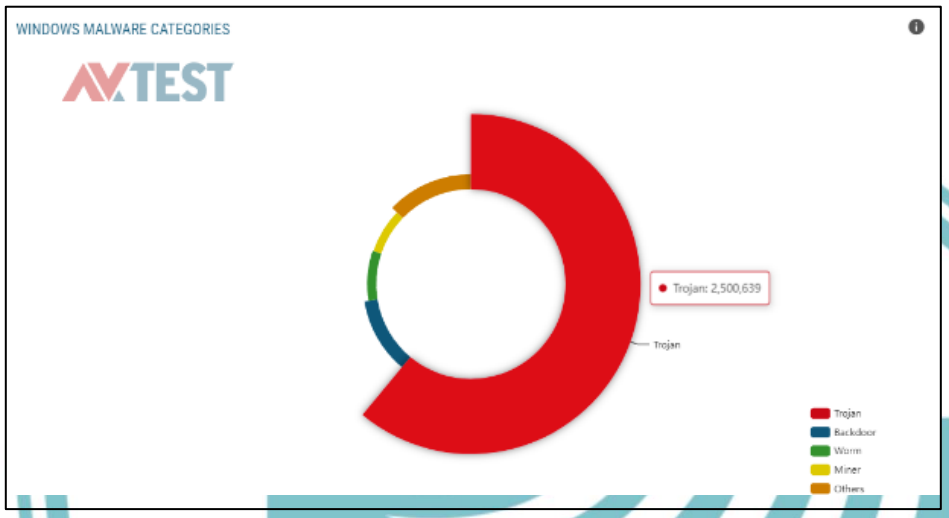
Berdasarkan informasi terbaru yang dikutip dari situs portal.av-atlas.org, jumlah penyebaran malware tertinggi terjadi pada sistem operasi Windows dengan total 3.852.754 kasus. Diagram data tersebut dapat dilihat pada gambar 1.1 dibawah:



Gambar 1.1 Diagram Penyebaran Malware Berdasarkan Sistem Operasi

Sumber: AV-ATLAS - Malware & PUA, 2024

Jenis malware yang paling banyak beredar pada sistem operasi Windows adalah *trojan*, dengan total 2.500.639 kasus. Data ini merupakan statistik terbaru hingga bulan Januari 2024. Diagram data tersebut dapat dilihat pada gambar 1.2 dibawah:



Gambar 1.2 Diagram Penyebaran Malware Pada Sistem Operasi Windows
Sumber: AV-ATLAS - Malware & PUA, 2024

Didalam perkembangannya, *trojan* merupakan salah satu malware paling berbahaya yang pernah dikembangkan. *Trojan* dapat mencuri informasi pribadi, menghapus file, memodifikasi file, mengendalikan sistem korban bahkan dapat menjadi jalur untuk memasang sejumlah malware tambahan di dalam sistem korban. *Trojan* sangat sulit dideteksi karena bersembunyi sebagai *software* atau proses yang biasanya tidak diketahui oleh orang pada umumnya, dapat menyebar melalui berbagai metode seperti *Social Engineering, File Download Fraud, Email Phishing, dan Malvertising,* untuk menipu korban dan menginfeksinya. (Victorius *et al.*, 2019)

Malware *Zeus*, juga dikenal dengan sebutan *Zbot*, sebagai salah satu malware berbahaya yang memberikan dampak signifikan terhadap sektor keuangan. *Trojan* perbankan ini pertama kali muncul pada tahun 2007. Pada bulan Mei 2011, kode sumber lengkap untuk malware ini secara tidak sengaja tersebar di berbagai situs internet. Ketersediaan kode sumber ini menjadi pemicu utama bagi munculnya varian-varian baru dari malware *zeus*. (Etaher, Weir and Alazab, 2015)

1.2 Rumusan Masalah

Berdasarkan hal-hal yang telah disampaikan pada latar belakang di atas, berikut rumusan masalahnya:

Bagaimana cara merancang dan mengimplementasikan lingkungan yang aman dan terkendali untuk pengujian serta analisis malware?

Bagaimana mengetahui cara kerja Malware *Zeus* melalui metode analisis statis dan dinamis berdasarkan indikator berbasis *host* dan jaringan?

Bagaimana cara merancang *YARA Rules* yang efektif dan efisien untuk mendeteksi Malware *Zeus*?

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang disusun agar ruang lingkup penelitian lebih terfokus, adalah:

a. Analisis ini hanya berfokus pada Malware *Zeus* sebagai objek utama.
b. Penelitian dilakukan dalam *Mode Virtual* untuk memastikan keamanan dan kontrol lingkungan analisis.
c. Analisis difokuskan pada sistem operasi Windows.
d. Pendeteksian hanya dilakukan menggunakan *YARA rules*.
e. Pendeteksian dilakukan menggunakan 3 sampel Malware *Zeus* yang mewakili varian utama.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah:

a. Mengetahui teknik, fitur dan cara kerja malware *zeus*.
b. Merancang, mengimplementasikan, dan mengevaluasi YARA rules yang efektif dan efisien untuk mendeteksi Malware *Zeus* di sistem komputer.

1.4.2 Manfaat

Manfaat penelitian ini adalah:

Memahami cara merancang dan mengimplementasikan lingkungan yang aman untuk menguji dan menganalisis malware.

Memahami cara menganalisis malware menggunakan metode analisis statis dan dinamis (*hybrid*).

Memahami cara merancang dan mengimplementasikan *YARA Rules* yang efektif dan efisien untuk pendeteksian malware.

Meningkatkan keamanan pada sistem komputer.

1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan dalam membuat laporan penelitian ini:

1. BAB I PENDAHULUAN

   Bab ini adalah bab pertama dalam penelitian ini, yang berisi latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.
2. BAB II TINJAUAN PUSTAKA

   Bab ini adalah bab kedua dalam penelitian ini, yang berisi landasan teori yang digunakan dan menguraikan penelitian-penelitian terkait.
3. BAB III METODE PENELITIAN

   Bab ini adalah bab ketiga dalam penelitian ini, yang berisi penjelasan mengenai rancangan penelitian, tahapan penelitian, dan skenario analisis yang digunakan.
4. BAB IV HASIL DAN PEMBAHASAN

   Bab ini adalah bab keempat dalam penelitian ini, yang berisi analisis kebutuhan sistem, perancangan dan implementasi sistem, serta analisis aturan dan hasil yang diperoleh.
5. BAB V PENUTUP

   Bab ini adalah bab terakhir dalam penelitian ini, yang berisi kesimpulan dari hasil analisis serta saran-saran untuk penelitian selanjutnya.

BAB V
PENUTUP

5.1 Kesimpulan

Berikut adalah poin-poin kesimpulan berdasarkan penelitian yang telah dilakukan:

1. Lingkungan aman untuk pengujian dan analisis malware dirancang menggunakan mesin virtual dengan fitur *snapshot*, sehingga memudahkan pemulihan sistem ke kondisi semula jika terjadi perubahan. Jaringan dikonfigurasi menggunakan *host-only adapter* dan INetSim untuk mencegah malware terhubung ke jaringan utama. Lingkungan ini juga perlu dilengkapi dengan alat analisis malware, dengan *menginstal* FlareVM dan REMnux, berbagai alat yang diperlukan untuk analisis sudah tersedia.
2. Melalui analisis statis, cara kerja malware zeus diungkap dengan mengekstraksi dan menganalisis string, fungsi, dan API yang digunakan tanpa harus menjalankannya. Analisis string menunjukkan bahwa malware zeus menggunakan fungsi seperti "GetClipboardData" untuk mencuri data sensitif dari clipboard pengguna, dengan memanggil API Windows melalui interrupt INT 2Eh (untuk kernel-mode) atau menggunakan stdcall untuk memanggil fungsi dari "kernel32.dll" atau "user32.dll". Pada analisis dinamis berbasis host, malware zeus terlihat melakukan perubahan pada sistem file, proses, dan registri. Sedangkan pada analisis dinamis berbasis jaringan, terungkap perilaku aktivitas jaringan yang dilakukan malware zeus, seperti mengunduh Flash Player dari internet.
3. YARA rules yang efektif dirancang dengan mengidentifikasi string unik dalam malware zeus, seperti signature khusus, fungsi API, atau karakteristik lainnya. Dengan menggunakan kondisi yang relevan dan optimasi menggunakan *wildcard* serta pola hex, diterapkan untuk meningkatkan fleksibilitas dan kemampuan mendeteksi berbagai varian malware zeus. Setelah rule dibuat, dilakukan pengujian pada berbagai sampel malware, termasuk malware zeus dan malware lain dengan karakteristik serupa, guna memastikan rule tersebut dapat mendeteksi malware target dengan konsisten tanpa menghasilkan *false positives*. Setelah berhasil dirancang, YARA rules kemudian dikompilasi menggunakan yarac untuk meningkatkan efisiensi deteksi dan mempercepat proses scanning pada jumlah file yang lebih besar.

5.2 Saran

Berdasarkan hasil penelitian ini, terdapat beberapa saran yang dapat diterapkan untuk pengembangan lebih lanjut:

Integrasikan *YARA Rules* yang telah dibuat dengan sistem *Endpoint Detection and Response (EDR)* untuk deteksi *real-time* dan respons otomatis terhadap ancaman malware zeus di *endpoint*.

Publikasikan *YARA Rules* yang telah dibuat di *Malware Information Sharing Platform (MISP)* untuk berbagi informasi dengan komunitas keamanan siber.

Hubungkan *YARA Rules* dengan Yextend untuk meningkatkan kemampuan dalam mendeteksi malware yang tersembunyi dalam file yang dikompresi.

Gunakan *sandbox* malware seperti VMRay dan ANY.RUN untuk melakukan analisis dinamis. Sandbox ini secara otomatis memberikan laporan terperinci tentang perilaku malware.

Perbarui *YARA Rules* secara berkala agar tetap dapat mendeteksi malware baru yang terus berkembang.

DAFTAR PUSTAKA

Amiruddin, A. *et al.* (2021) 'Utilizing Reverse Engineering Technique for A Malware Analysis Model', *Scientific Journal of Informatics*, 8(2), pp. 222–229. Available at: https://doi.org/10.15294/sji.v8i2.24755.

Anastasios, C. (2023) *Master of Science Cybersecurity Malware Analysis and Reverse Engineering*.

Aslan, O. and Samet, R. (2020) 'A Comprehensive Review on Malware Detection Approaches', *IEEE Access*. Institute of Electrical and Electronics Engineers Inc., pp. 6249–6271. Available at: https://doi.org/10.1109/ACCESS.2019.2963724.

AV-ATLAS - Malware & PUA (2024). Available at: https://portal.av-atlas.org/malware/statistics (Accessed: 29 January 2024).

Balci, A. (2020) *Malware Reverse Engineering Handbook*. Available at: www.ccdcoe.org.

Cutter (2024). Available at: https://cutter.re/ (Accessed: 5 February 2024).

Damanik, A., Seta, H. and Theresiawati (2023) '2327-Article Text-6898-1-10-20230523', *Jurnal Ilmiah MATRIK*, 25(1).

Download Windows 10 (2024). Available at: https://www.microsoft.com/en-us/software-download/windows10 (Accessed: 24 April 2024).

Dwi, Y. *et al.* (2021) *Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1*.

Etaher, N., Weir, G. and Alazab, M. (2015) 'Etaher_etal_IEEE_TrustCom_2015_From_ZeuS_to_Zitmo_Trends_in_banking', *The 14th IEEE International Conference* [Preprint].

Fujii, S., Yamagishi, R. and Yamauchi, T. (2022) 'Survey and Analysis on ATT&CK Mapping Function of Online Sandbox for Understanding and Efficient Using', *Journal of Information Processing*, 30, pp. 807–821. Available at: https://doi.org/10.2197/ipsjjip.30.807.

Get the Virtual Appliance | REMnux Documentation (2024). Available at: https://docs.remnux.org/install-distro/get-virtual-appliance (Accessed: 24 April 2024).

Hamdi, Y. and Kunang, Y.N. (2020) 'ANALISIS MALWARE PADA SISTEM OPERASI WINDOWS MENGGUNAKAN TEKNIK FORENSIK', *Bina Darma Conference on Computer Science* [Preprint].

Or-Meir, O. *et al.* (2019) 'Dynamic malware analysis in the modern era—A state of the art survey', *ACM Computing Surveys*, 52(5). Available at: https://doi.org/10.1145/3329786.

Prayitno, D. *et al.* (2022) *Systematic Literature Review: Implementasi Metode Statis Dan Dinamis Pada Analisa Malware*.

Riadi, I., Sunardi and Aprilliansyah, D. (2023) 'Analysis of Anubis Trojan Attack on Android Banking Application Using Mobile Security Labware', *International Journal of Safety and Security Engineering*, 13(1), pp. 31–38. Available at: https://doi.org/10.18280/ijsse.130104.

Talukder, S. (2020) *Tools and Techniques for Malware Detection and Analysis*. Available at: https://www.researchgate.net/publication/339301928.

Victorius, E.J. *et al.* (2019) *ANALISIS DETEKSI MALWARE REMOTE ACCESS TROJAN MENGGUNAKAN DYNAMIC MALWARE ANALYSIS DETECTION TOOLS BERBASIS BEHAVIOUR MALWARE DETECTION ANALYSIS OF REMOTE ACCESS TROJAN WITH BEHAVIOUR-BASED DYNAMIC MALWARE ANALYSIS DETECTION TOOLS*.

DAFTAR RIWAYAT HIDUP

Ivan Harry Cahyadi

Lahir di Bekasi pada 11 Februari 2002. Lulus dari MI Tarbiyatul Falah tahun 2014, SMP Yadika 11 tahun 2017, SMA Hutama tahun 2020. Pendidikan Profesi CEP-CCIT di Fakultas Teknik Universitas Indonesia (2020-2022) program studi Network Administrator Professional. Saat ini, sedang menyelesaikan studi D4 Teknik Informatika dan Komputer di Politeknik Negeri Jakarta (2020-2024) program studi Teknik Multimedia dan Jaringan, konsentrasi keamanan sistem informasi.