ANALISA MALWARE PADA TRAFFIC JARINGAN BERBASIS POLA LALU LINTAS DATA MENGGUNAKAN METODE ANOMALY

Jian Malik Hidayat[1], Herri Setiawan[2], Tasmi[3]
[1,2,3] Universitas Indo Global Mandiri, Jian Malik Hidayat
e-mail: [1]2022110039P@students.uigm.ac.id, [2]herri@uigm.ac.id, [3]tasmi@uigm.ac.id,

ABSTRACT

Network security is a major challenge in the era of increasingly rapid digitalization. PDF files, which are widely used for sharing information, are often exploited by cybercriminals to insert malware. This research aims to analyze the impact of malware in PDF files on network traffic using Wireshark software. With a traffic pattern-based approach and anomaly detection, this research identifies malicious activities such as connections to servers, data exfiltration, traffic spikes, and the use of obfuscation techniques. The malware in the PDF file shows suspicious traffic patterns that include increased volume of outgoing data, and repeated data packets to certain destinations. Additionally, these activities cause significant disruption to network performance, open security gaps, and increase the risk of sensitive data leakage. Wireshark is used to capture, analyze and identify traffic anomalies in real-time. The research results show that pattern and anomaly-based analysis using Wireshark effectively improves the accuracy of PDF malware detection at the network level. These findings support the importance of applying traffic analysis methods to detect hidden cyber threats. In addition, this research makes an important contribution to the development of network analysis-based cyber attack mitigation strategies, helping organizations respond to threats more quickly and reduce potential losses. With this approach, network security can be strengthened to deal with evolving threats.

Keywords: *Analysis, Anomaly, Network Traffic.*

INTISARI

Keamanan jaringan menjadi tantangan utama di era digitalisasi yang semakin berkembang pesat. File PDF, yang secara luas digunakan untuk berbagi informasi, sering dimanfaatkan oleh pelaku kejahatan siber untuk menyisipkan malware. Penelitian ini bertujuan untuk menganalisis dampak malware dalam file PDF terhadap lalu lintas jaringan menggunakan perangkat lunak Wireshark. Dengan pendekatan berbasis pola lalu lintas dan deteksi anomali, penelitian ini mengidentifikasi aktivitas berbahaya seperti koneksi ke server,eksfiltrasi data, lonjakan lalu lintas, dan penggunaan teknik *obfuscation.* Malware dalam file PDF menunjukkan pola lalu lintas mencurigakan yang mencakup peningkatan volume data keluar, dan paket data berulang ke tujuan tertentu. Selain itu, aktivitas ini menyebabkan gangguan signifikan terhadap kinerja jaringan, membuka celah keamanan, dan meningkatkan risiko kebocoran data sensitif. Wireshark digunakan untuk menangkap, menganalisis, dan mengidentifikasi anomali lalu lintas secara real-time. Hasil penelitian menunjukkan bahwa analisis berbasis pola dan anomali menggunakan Wireshark secara efektif meningkatkan akurasi deteksi malware PDF di tingkat jaringan. Temuan ini mendukung pentingnya penerapan metode analisis lalu lintas untuk mendeteksi ancaman siber yang tersembunyi. Selain itu, penelitian ini memberikan kontribusi penting dalam pengembangan strategi mitigasi serangan siber berbasis analisis jaringan, membantu organisasi merespons ancaman lebih cepat dan mengurangi potensi kerugian. Dengan pendekatan ini, keamanan jaringan dapat diperkuat untuk menghadapi ancaman yang terus berkembang.

Kata Kunci: Analisis, Anomali, Lalu Lintas Jaringan.

1. PENDAHULUAN

1.1 LATAR BELAKANG

Dengan pesatnya pertumbuhan teknologi informasi, kehadiran malware telah menjadi ancaman serius terhadap keamanan sistem dan data. Malware, yang merupakan singkatan dari malicious software, dirancang untuk merusak atau mengakses informasi tanpa izin (Suhaemin, Amin & Muslih, 2023). Analisis ini berfokus pada jenis malware tertentu yang telah menembus sistem perusahaan di berbagai industri. Berbagai kejahatan yang menggunakan teknologi komputer dan internet sebagai media tindak pidananya umumnya disebut sebagai "Cyber Crime." Tindakan ini dapat berdampak langsung kepada korban atau menjangkau korban melalui jaringan internet, sehingga menimbulkan kerugian baik langsung maupun tidak langsung. Salah satunya adalah penggunaan malware untuk melakukan kejahatan siber terhadap korbannya (Matin & Rahardjo, 2020).

Malware adalah program yang dapat dijalankan di komputer untuk menemukan kerentanan pada perangkat lunak. Jenis-jenis malware mencakup virus, Trojan horse, worm, dan adware (Amdani & Iqbal, 2021). Penyebaran malware dapat menyebabkan gangguan jaringan, mengganggu komunikasi yang sedang berlangsung antar komputer di jaringan, dan

menyebabkan anomali jaringan. Analisis malware merupakan bagian penting dari upaya memerangi ancaman ini (Nasution & Laksono, 2020). Pemahaman mendalam tentang cara kerja malware, cara penyebarannya, dan kemungkinan kerentanannya merupakan dasar untuk mengembangkan strategi keamanan yang efektif.

Tujuan dari penelitian ini adalah untuk melakukan analisis rinci terhadap pola lalu lintas data terhadap malware yang terdeteksi di lingkungan perusahaan pada area traffic jaringan, dengan fokus pada hasil analisis dan mengidentifikasi kerentanan yang dapat dieksploitasi untuk lebih melindungi sistem. Network anomaly adalah suatu peristiwa di mana suatu objek mempunyai nilai unik atau nilai yang berbeda dengan benda lainnya (Pressman, 2021). Anomali jaringan dapat mendeteksi serangan pada jaringan karena paket yang berisi serangan berbeda dengan paket data yang seharusnya dieksekusi pada port jaringan (Solomon & Maunder, 2021).

Dalam jaringan, sulit untuk mendeteksi malware yang mengenkripsi paket masuk dan keluar dengan benar. Hal ini karena malware terenkripsi mendependekan paket yang diterima oleh malware yang dieksekusi oleh host, sedangkan malware yang mengenkripsi paket yang dikirim dan diterima tidak mendependekankan paket tersebut secara langsung. Jika mengetahui isi paket yang dikirim ke klien yang terinfeksi, dapat mengenkripsinya; namun, untuk menemukan paket yang dikirim oleh malware memerlukan aplikasi lain untuk dapat mengenali kode malware (Alhassan, Bock, & Bozkurt, 2022).

Solusi untuk menemukan aktivitas malware pada file Pcap dalam penelitian ini adalah dengan mencari aktivitas port yang digunakan malware tersebut untuk menemukan aktivitas pada komputer yang terinfeksi (Akhtar & Feng, 2022). Dengan memeriksa aktivitas paket yang dikirim dan diterima pada port yang digunakan jaringan , dapat mengklasifikasikan jenis serangan yang dilakukan oleh malware. Setelah mengklasifikasikan serangan yang dilakukan oleh malware tersebut, dampak dari masing-masing malware dapat diklasifikasikan.

Investigasi ini dapat digunakan untuk mengidentifikasi aktivitas pola lalu lintas jaringan yang dilakukan oleh malware menggunakan metode anomali pada port yang digunakan. Keuntungan menggunakan teknik anomali adalah dapat mendeteksi pola yang tidak biasa dalam jaringan komputer (Liao & Chiu, 2021; Zhang & Lee, 2021). Teknik anomali dapat membantu mengenali aktivitas malware dengan lebih mudah dan cepat.

Berdasarkan latar belakang tersebut, rumusan masalah yang akan dibahas pada penelitian ini adalah sebagai berikut:
1. Bagaimana mendeteksi malware kategori *mail server* dan *File Pdf* yang berjalan pada lalu lintas data jaringan?
2. Bagaimana menganalisis tingkah laku *mail server* dan *File Pdf* saat berjalan pada lalu lintas data jaringan?
3. Bagaimana dampak yang ditimbulkan *mail server* dan *File Pdf* terhadap *traffic* lalu lintas data jaringan?

Berdasarkan rumusan masalah pada penelitian ini, tujuan dilakukannya penelitian ini adalah sebagai berikut:
1. Mendeteksi keberadaan *mail server* dan *File Pdf* yang aktif dalam lalu lintas jaringan.
2. Mengetahui tingkah laku *mail server* dan *File Pdf* saat berjalan pada jaringan.
3. Mengetahui dampak yang ditimbulkan *mail server* dan *File Pdf* terhadap traffic jaringan.

Adapun batasan masalah pada penelitian ini sebagai berikut:
1. Data yang diambil dari penelitian ini menggunakan jaringan Perusahaan Peneliti.
2. Penelitian ini menggunakan metode analisis secara anomaly yang berfokus pada malware neris secara statis menggunakan Wireshark.

Terdapat Tinjauan pusataka berdasakan latar belakang diatas:
1. Pendahuluan tentang Malware dan Ancaman Keamanannya
   Seiring dengan pesatnya pertumbuhan teknologi informasi, kehadiran malware telah menjadi ancaman serius terhadap keamanan sistem dan data. Malware, atau perangkat lunak berbahaya, dirancang untuk merusak atau mengakses informasi tanpa izin (Suhaemin, Amin & Muslih, 2023) Berbagai jenis malware seperti virus, Trojan horse, worm, dan adware menjadi fokus perhatian para peneliti dan praktisi keamanan siber karena dampaknya yang luas pada sistem informasi di berbagai industri (Amdani & Iqbal, 2021).
2. Cyber Crime dan Dampaknya
   Tindakan kejahatan siber, yang mencakup penggunaan teknologi komputer dan internet sebagai media, dapat menyebabkan kerugian langsung dan tidak langsung bagi korban (Matin & Rahardjo, 2020). Dalam konteks ini, malware sering digunakan sebagai alat untuk melancarkan serangan siber, yang semakin kompleks dan canggih. Oleh karena itu, analisis terhadap malware menjadi sangat penting dalam memahami dan mengatasi ancaman ini.
3. Penyebaran Malware dan Analisisnya
   Penyebaran malware dapat menyebabkan gangguan dalam jaringan, mengganggu komunikasi antar komputer, dan menciptakan anomali jaringan. Analisis malware merupakan langkah krusial dalam memerangi ancaman ini, karena pemahaman yang mendalam tentang cara kerja dan penyebaran malware dapat menjadi dasar untuk

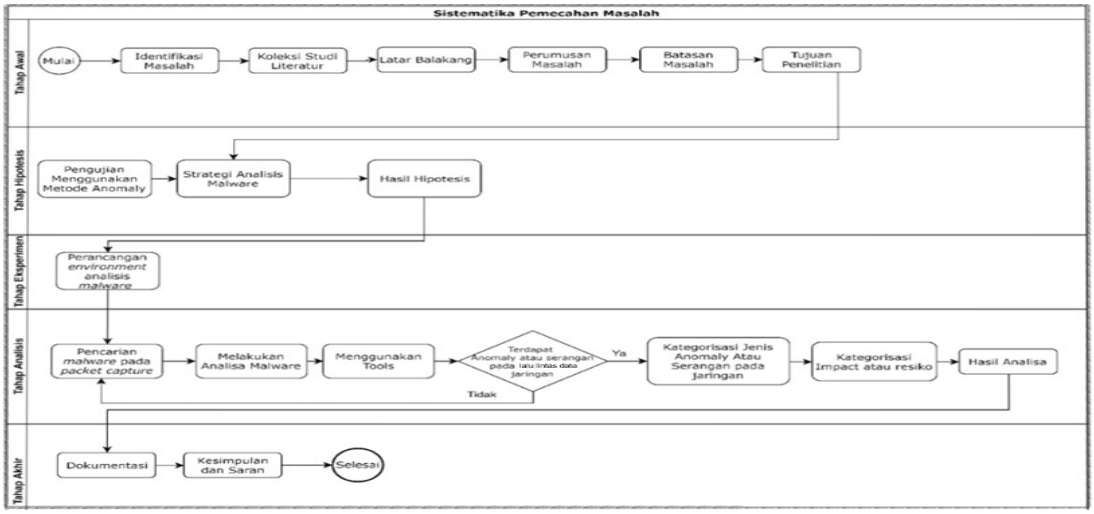
mengembangkan strategi keamanan yang lebih efektif (Nasution & Laksono, 2020).

4. Network Anomaly dan Deteksi Malware
   Anomali jaringan adalah peristiwa di mana suatu objek menunjukkan nilai unik atau berbeda dibandingkan dengan objek lainnya (Pressman, 2021). Teknik deteksi anomali memungkinkan identifikasi serangan pada jaringan melalui perbedaan paket data yang seharusnya dieksekusi. Metode ini efektif dalam mendeteksi aktivitas malware yang mengenkripsi paket, meskipun ada tantangan dalam mengidentifikasi paket tersebut secara langsung (Solomon & Maunder, 2021).
5. Tantangan Deteksi Malware Terenkripsi
   Deteksi malware yang mengenkripsi paket masuk dan keluar merupakan tantangan tersendiri. Malware terenkripsi sering kali bergantung pada paket yang diterima oleh host, sehingga memerlukan aplikasi khusus untuk mengenali kode malware yang tersembunyi di dalamnya (Alhassan, Bock, & Bozkurt, 2022). Upaya untuk mengidentifikasi aktivitas malware melalui analisis paket menjadi penting dalam mendeteksi dan mengklasifikasikan jenis serangan.
6. Metode dan Solusi Deteksi Malware
   Dalam penelitian ini, solusi untuk menemukan aktivitas malware pada file Pcap melibatkan pencarian aktivitas port yang digunakan oleh malware tersebut (Akhtar & Feng, 2022). Dengan memeriksa aktivitas paket yang dikirim dan diterima pada port yang teridentifikasi, dapat dilakukan klasifikasi terhadap jenis serangan yang dilancarkan. Hasil analisis ini berpotensi memberikan pemahaman lebih dalam tentang dampak dari masing- masing malware.
7. Keuntungan Teknik Anomali dalam Deteksi Malware
   Teknik anomali menawarkan keuntungan dalam mendeteksi pola yang tidak biasa dalam jaringan komputer (Liao & Chiu, 2021; Zhang & Lee, 2021). Penggunaan metode ini dalam mengidentifikasi aktivitas pola lalu lintas yang dilakukan oleh malware dapat mempercepat proses deteksi dan mitigasi serangan, sehingga meningkatkan keamanan sistem secara keseluruhan.

2. METODE PENELITIAN

2.1 SISTEMATIKA PEMECAHAN MASALAH

Pemecahan masalah yang sistematis menggambarkan bagaimana alur penelitian dapat terjadi dan berjalan secara logis. Pemecahan masalah yang sistematis digunakan untuk menciptakan gambaran suatu solusi yang dapat memecahkan masalah yang dihadapi dan mencapai tujuan penelitian yang baik. Sistem itu sendiri terdiri dari fase- fase dimana identifikasi masalah dimulai. Setelah menemukan masalahnya, dapat memutuskan solusi dari masalah yang temui. Tahap desain lingkungan yang digunakan dalam penelitian ini kemudian dapat ditentukan. Berikutnya adalah tahap pengujian yang digunakan dalam penelitian ini.



Gambar 2.1 Sistematika Pemecahan Masalah

Gambar 2.1, dijelaskan alur sistematika penelitian yang terdiri dari beberapa tahap, yaitu tahap awal, tahap desain, tahap pengumpulan data, dan tahap akhir.

2.2 TAHAPAN ANALISA MENGGUNAKAN METODE ANOMALY

Tahap ini memindai malware dan mengambil sampel paket, menganalisis dampak malware pada lalu lintas jaringan, dan mendeteksi jaringan yang dikirim melalui mail server dan dikirimkan dengan format file pdf terinfeksi malware dalam lingkungan yang dibuat. Untuk melakukan analisisnya, memerlukan alat analisis paket yaitu Wireshark.Setelah hasil analisis dampak malware pada jaringan diperoleh, maka anomali yang terjadi di dalam jaringan dan jenis serangan

(payload) terhadap malware yang dianalisis diklasifikasikan, dan dampak atau risiko malware yang dianalisis diklasifikasikan. Tahap ini mencari malware dalam penangkapan paket dan menganalisis dampaknya terhadap lalu lintas jaringan. Pencarian ini sering kali melibatkan mata-mata pada jaringan yang terinfeksi untuk mendeteksi aktivitas mencurigakan. Langkah-langkah untuk level ini adalah:

1. Pencarian Malware pada Packet Capture:
   Packet Capture CC & IRC Gunakan alat atau platform seperti Wireshark untuk melakukan penangkapan paket dari jaringan yang ingin dianalisis. Identifikasi Aktivitas Mencurigakan: Analisis paket untuk mengidentifikasi pola atau aktivitas yang mencurigakan yang mungkin disebabkan oleh malware.
2. Sniffing pada Jaringan yang Terinfeksi:
   Gunakan Sniffing Tools: Wireshark adalah contoh alat yang umum digunakan untuk sniffing pada jaringan. Analisis Paket yang Disniff: Analisis paket yang telah disniff untuk mendeteksi perilaku atau pola tertentu yang menunjukkan adanya malware.
3. Analisis Dampak Malware Terhadap Traffic Jaringan:
   Identifikasi Perubahan Trafik: Periksa perubahan dalam pola lalu lintas jaringan yang mungkin disebabkan oleh malware. Tinjau jumlah dan jenis komunikasi yang dilakukan oleh sistem terinfeksi.
4. Analisis Kategori Anomaly di Jaringan:
   Penggunaan Wireshark untuk Analisis Anomali: Wireshark dapat digunakan untuk mengidentifikasi anomali dalam paket dan lalu lintas jaringan. Fokus pada pola yang tidak biasa atau tidak sesuai dengan profil normal jaringan.
5. Analisis Jenis Serangan (Payload) pada Malware:
   Pendeteksian Payload Malware: Identifikasi payload atau kode berbahaya yang dikirim oleh malware. Perhatikan karakteristik unik yang dapat membantu dalam mengklasifikasikan jenis serangan.
6. Kategorisasi Impact atau Risiko:
   Penggunaan Informasi Analisis untuk Kategorisasi: Gunakan hasil analisis untuk menentukan tingkat risiko atau dampak yang diakibatkan oleh malware. Kategorisasikan risiko berdasarkan skala yang telah ditentukan (rendah, sedang, tinggi).
7. Pelaporan Hasil Analisis:
   Dokumentasikan Temuan: Buat laporan yang mencakup hasil analisis, temuan malware, dampaknya terhadap jaringan, dan kategorisasi risiko. Sertakan informasi tentang payload, serangan, dan anomali yang terdeteksi.
8. Langkah Selanjutnya:
   Reaksi dan Mitigasi: Tentukan langkah-langkah reaksi yang perlu diambil untuk mengatasi malware dan dampaknya. Rancang strategi mitigasi untuk mencegah penyebaran lebih lanjut dan mengurangi risiko.
9. Pembaruan dan Evaluasi:
   Pembaruan Sistem Keamanan: Berdasarkan temuan, lakukan pembaruan pada sistem keamanan untuk mengatasi kelemahan yang mungkin telah dieksploitasi oleh malware. Tingkatkan kebijakan keamanan jika diperlukan.

Langkah-langkah ini membantu dalam mengidentifikasi, menganalisis, dan mengatasi malware serta dampaknya terhadap jaringan. Penting untuk menjaga keamanan jaringan dengan merespons secara cepat terhadap temuan dan mengimplementasikan tindakan mitigasi yang diperlukan.

2.3 KOMPONEN PENGUJIAN

Untuk mencapai tujuan penelitian ini, berbagai skenario harus dirancang dan diuji dengan cermat untuk memastikan bahwa hasil yang diinginkan tercapai. Setiap skenario dirancang untuk mengeksplorasi berbagai kondisi dan variabel yang dapat mempengaruhi hasil akhir penelitian. Proses ini mengumpulkan beberapa sampel data dengan menangkap paket capture (PCAP) dalam pola lalu lintas. Pengumpulan data ini dilakukan dengan menggunakan teknik sniffing. Suatu proses yang memantau dan mengumpulkan data yang dikirim melalui jaringan pada port TCP/IP tertentu.

Tujuan dari teknik sniffing ini adalah untuk mencatat dan menganalisis lalu lintas yang terjadi dengan harapan dapat mengidentifikasi pola tertentu yang relevan untuk tujuan penelitian. Dengan menerapkan skenario pengujian berbeda, penelitian ini bertujuan untuk menemukan pola, anomali, atau indikator tertentu yang dapat dijadikan acuan untuk analisis lebih lanjut. Hasil pengujian skenario yang berbeda diharapkan dapat memberikan wawasan yang lebih baik dan mendukung pencapaian tujuan utama penelitian yang dilakukan.

2.4 TAHAP AKHIR

Tahap ini merupakan fase terakhir dari serangkaian penyelidikan yang menyeluruh dan sistematis. Pada tahap ini, seluruh hasil yang diperoleh selama proses penelitian dirangkum dan disusun dalam bentuk laporan yang komprehensif. Laporan ini tidak hanya berfungsi sebagai referensi utama untuk merefleksikan temuan investigasi, namun juga sebagai dokumen yang memberikan rincian terkait setiap langkah selama proses investigasi dan temuan, khususnya analisis malware yang dilakukan.

Laporan ini merinci beberapa temuan utama dari penelitian ini, termasuk data kualitatif dan kuantitatif yang mendukung kesimpulan penelitian. Selain itu, laporan ini memberikan analisis terperinci tentang pola dan karakteristik malware yang terdeteksi serta dampaknya terhadap sistem keamanan yang diselidiki. Laporan penelitian juga memuat kesimpulan

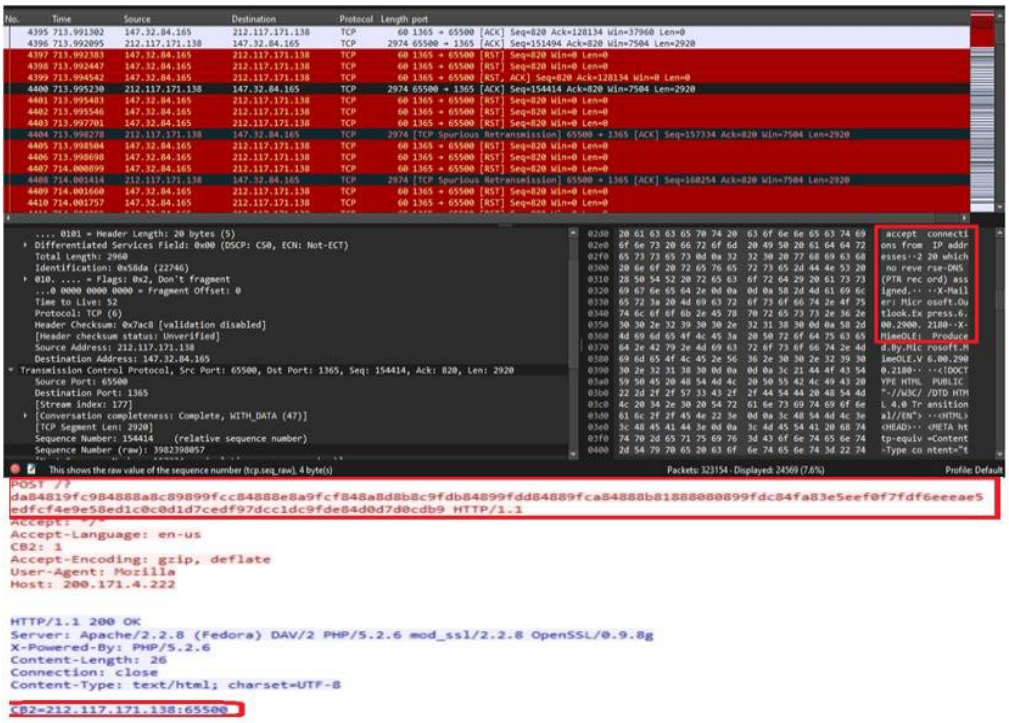
yang merangkum seluruh temuan dan rekomendasi yang dibuat berdasarkan temuan dan analisis yang dilakukan selanjutnya.

Rekomendasi ini diharapkan dapat menjadi panduan bagi langkah selanjutnya dalam pencegahan dan pengelolaan malware serta berkontribusi positif terhadap kemajuan ilmu pengetahuan dan teknologi keamanan siber.

3. HASIL DAN PEMBAHASAN

3.1 DETEKSI MALWARE PADA POLA LALU LINTAS DATA

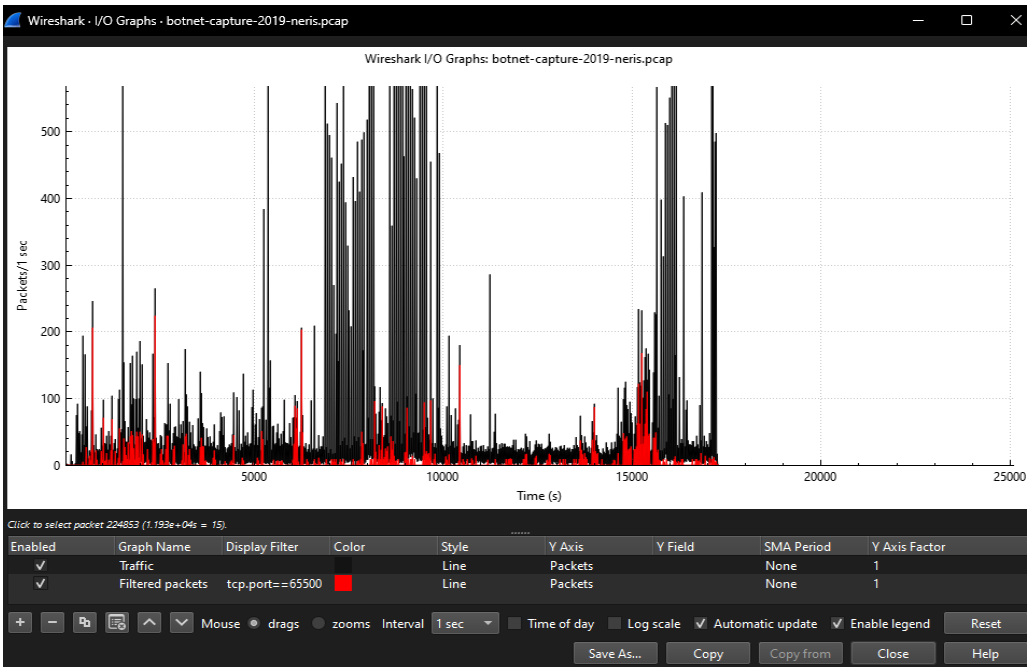
Dalam penelitian ini, kami menggunakan metode anomali untuk melakukan analisis malware pada lalu lintas jaringan berdasarkan pola lalu lintas. Data yang digunakan adalah data lalu lintas jaringan yang diperoleh dari perusahaan peneliti. Data lalu lintas jaringan terdiri dari data paket TCP/IP yang diproses menggunakan Wireshark. Data lalu lintas jaringan kemudian dihasilkan menjadi kumpulan data dan diekspor dalam format CSV. Menentukan pola lalu lintas data yang dapat digunakan untuk mendeteksi malware. Pola-pola ini termasuk CC dan IRC. Dalam C&C melalui IRC, CC mewakili jumlah koneksi di jaringan Wireshark. Jumlah koneksi adalah jumlah koneksi yang dibuat oleh perangkat di jaringan. Jumlah koneksi dapat digunakan untuk memantau aktivitas jaringan dan mendeteksi anomali. IRC adalah singkatan dari Internet Relay Chat. IRC adalah protokol komunikasi yang digunakan untuk bertukar pesan dan file secara real time. Penyerang memiliki server yang menjalankan layanan IRC yang memungkinkan klien yang terinfeksi berkomunikasi menggunakan protokol IRC, mendistribusikan spa, dan mencuri informasi seperti kredit.



Gambar 3.1 Hasil Aktivitas *Anomaly* C&C IRC Malware neris Port 65500

Gambar 3.1 menunjukkan koneksi menggunakan protokol IRC,Klien yang terinfeksi menggunakan layanan IRC untuk mengirim POST ke server menggunakan nilai kunci IP dan port 65500, menyatakan bahwa lalu lintas adalah anomali. Data ini digunakan untuk mengirim file PDF malware. Malware File Pdf dapat digunakan untuk mengirim iklan, penipuan, spam, dan konten yang tidak relevan ke penerima email. Ada juga email spam dengan niat jahat untuk menyebarkan virus dan malware ke perangkat berbahaya lainnya. Ini terjadi segera setelah pengguna membuka email.

P - ISSN: 1979-911X
E - ISSN: 2541-528X



Gambar 3.2 Hasil Analisis *Graph* Malware Neris pada port 65500

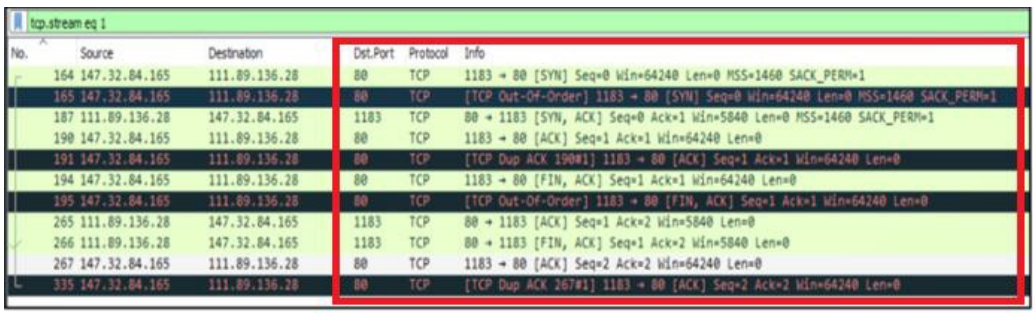
Pada gambar di atas, dapat melihat peningkatan lalu lintas pada port 65500 karena malware melonjak tinggi traffic melewati port 65500. Hal ini dapat mempengaruhi lalu lintas dan menyebabkan anomali lalu lintas.

3.2 ANALISA PORT MENGGUNAKAN METODE ANOMALY

Pada sub-bab ini akan menjelaskan hasil dari port *activity* dengan menggunakan Wireshark, Dalam analisis ini, akan dijelaskan metode dan algoritma yang digunakan untuk mengidentifikasi anomali dalam lalu lintas jaringan. Analisis tingkah laku malware dapat mencakup aspek pada protocol, termasuk penggunaan TCP scanning oleh malware untuk mengeksplorasi dan menyebarkan diri. Berikut adalah beberapa poin penting terkait analisis tingkah laku malware terkait TCP scanning.

3.2.1 TCP *SCAN*

TCP (Transmission Control Protocol) Scan adalah metode pemindaian jaringan yang digunakan untuk mengidentifikasi status port pada perangkat dalam jaringan. Protokol ini beroperasi di layer transport, memungkinkan pengguna untuk mengirimkan paket-paket khusus, seperti SYN, ACK, FIN, dan RST, untuk mendapatkan informasi tentang port yang terbuka, tertutup, atau terfilter oleh firewall.

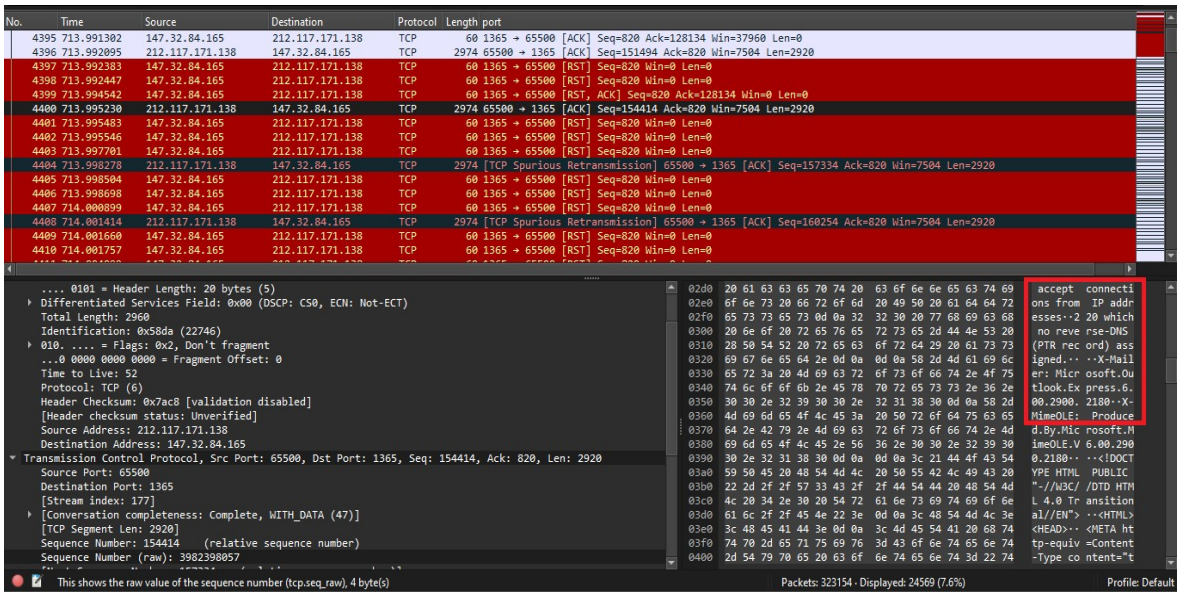


Gambar 3.3 Hasil aktifitas *scanning*

Pada Gambar 3.3 di atas, klien yang terinfeksi malware melakukan jabat tangan tiga arah, yaitu (SYN, SYN/ACK, ACK), dengan target yang dipindai dan klien yang terinfeksi. Ketika target yang dipindai mengirimkan paket SYN/ACK, kita mengetahui bahwa port tempat koneksi dibuat terbuka. Berdasarkan hasil analisa di atas terlihat bahwa target yang

dipindai memiliki port 80 yang terbuka. Jika port ditutup, sambungan jabat tangan 3 arah tidak akan dibuat.

Berdasarkan tambahan tentang perilaku malware di file PDF diperoleh melalui analisis statis menggunakan Wireshark. Hasilnya menunjukkan pola aktivitas yang khas seperti mencari kerentanan keamanan, mengumpulkan informasi sensitif, dan berkomunikasi dengan server kontrol. Data ini memberikan informasi mendalam tentang modus operandi malware file PDF yang teridentifikasi.



Gambar 3.4 Aktifitas downloading executable file pcap malware neris

Gambar 3.4 menunjukkan adanya anomaly pada file yang diunduh oleh malware tanpa sepengetahuan pengguna. Pada port 65500, aplikasi email dan Microsoft Outlook untuk mengirim file PDF terinfeksi malware parah, dan komputer yang terinfeksi malware mengirimkan virus malware ke berbagai tujuan email yang ditujukan untuk file PDF, Ada penjelasan enkripsi yang menunjukkan bahwa mengirim email spam, kirim email dari pengirim yang sama dan gunakan IP tujuan yang sama.

3.3 RELEVANSI DAMPAK TERHADAP TRAFFIC JARINGAN

Dampak yang terukur pada traffic jaringan menunjukkan bahwa malware File Pdf bukan hanya ancaman virtual tetapi juga memiliki konsekuensi nyata terhadap kinerja jaringan. Ini menekankan pentingnya implementasi kebijakan keamanan yang proaktif, termasuk pembaruan rutin, pemantauan aktif, dan reaksi cepat terhadap ancaman yang teridentifikasi.

Tabel 3.1 Analisis dampak malware

Malware	*Threat*	*Port*	**Deskripsi risk**
Neris	C&C HTTP	80	Dalam aktivitas ini, malware berkomunikasi dengan server dan memungkinkan server mengeluarkan perintah yang dapat dijalankan oleh klien yang terinfeksi malware di komputer (alamat IP). Hal ini dimungkinkan karena dalam aktivitas ini, server mengirimkan perintah dalam paket terenkripsi. Sulit untuk mengetahui apa yang ada di dalam paket.

	C&C IRC	6667	Selama aktivitas ini, malware berkomunikasi dengan server sehingga dapat mengeluarkan perintah yang dapat dijalankan oleh klien yang terinfeksi. Dampaknya pada aktivitas server adalah perintah dikirimkan untuk memeriksa file PDF dari malware.
	Malware File Pdf	65500	Dalam aktivitas ini, malware mengirimkan email ke pengguna acak, sehingga memperlambat bandwidth dan kinerja klien yang terinfeksi.
	Identity Theft	80	Dalam aktivitasnya, malware memberikan informasi seperti nama komputer, alamat IP, dan alamat MAC agar pengguna mengetahui di mana mereka dilacak.
	Downloading Executable File	80, 81, 82, 88, 1389, 2012	Dalam aktivitas ini, malware mengunduh file executable yang terinfeksi malware dan menyamarkan ekstensi file dari file tersebut, meskipun sebenarnya file tersebut adalah file executable. Dampak dari aktivitas ini pada komputer selama pengunduhan meningkatkan beban pada komputer dan membuka pintu belakang, menjadikan klien yang terinfeksi semakin rentan terhadap malware
Rbot	C&C IRC	6667	Selama aktivitas ini, malware berkomunikasi dengan server sehingga dapat mengeluarkan perintah yang dapat dijalankan oleh klien yang terinfeksi. Efek dari aktivitas ini adalah server mengirimkan perintah untuk melakukan TCP Scan, SYN flood, dan ICMP flood.
	Dos Attack	22, 80	Dalam aktivitas ini, malware melakukan DoS pada port 22 (SYN flood) dan port 80 (ICMP flood). Dampak dari aktivitas ini adalah dapat mengurangi bandwidth internet, menghambat pengiriman paket, dan memperlambat sistem komputer.
	Network Scanning	80	Pada aktivitas ini malware melakukan scanning terhadap port 80 yang digunakan oleh server. Dampak dari aktivitas ini adalah malware mengetahui port yang terbuka sehingga dapat malware melakukan DDoS.
Arid Viper	C&C HTTP	80	Pada aktivitas ini malware melakukan komunikasi dengan server, sehingga server dapat memberi perintah yang bisa dieksekusi oleh client yang terinfeksi, dan juga mengirim identitas nama komputer pada client yang terinfeksi.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan terkait deteksi dan analisis malware File Pdf pada lalu lintas data jaringan, dapat diambil beberapa kesimpulan yaitu:

1. Mendeteksi Keberadaan Malware File Pdf pada pola lalu lintas data:
   Anomali pola lalu lintas yang dikirim melalui file PDF yang berisi malware tipe Neris diteruskan ke port 65500.
2. Analisis Tingkah Laku Malware File Pdf:
   Dengan menggunakan metode analisis malware secara statis menggunakan metode anomaly yang terdapat pada lalu lintas data pada port jaringan, penelitian ini memberikan wawasan mendalam tentang tingkah laku malware File Pdf saat berjalan pada jaringan.
3. Dampak Terhadap Traffic Jaringan:
   Hasil penelitian menunjukkan bahwa malware File Pdf memiliki dampak yang signifikan terhadap traffic lalu lintas data jaringan dengan mempengaruhi besaran traffic pada port 65500 yang di lalui malware neris. Pemahaman lebih lanjut tentang dampak ini dapat membantu organisasi untuk meningkatkan keamanan jaringan mereka dan merespon dengan lebih cepat terhadap potensi ancaman dengan mengindentifikasi bahwa malware neris file pdf akan melewati port 65500.

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Allah SWT atas rahmat dan karunia-Nya sehingga penelitian ini dengan judul "Analisis Malware pada Traffic Jaringan Berbasis Pola Lalu Lintas Data Menggunakan Metode Anomaly" dapat diselesaikan. Naskah publikas ini disusun berdasarkan hasil penelitian yang telah dilakukan. Selama pelaksanaan penelitian dan penyusunan laporan, penulis mendapatkan banyak bantuan, bimbingan, dan dukungan dari berbagai pihak, mulai dari proses pengumpulan data hingga tahap akhir penyusunan. Penulis menyadari bahwa naskah publikasi ini masih memiliki kekurangan, baik dari segi materi maupun penyajiannya. Oleh karena itu, kritik dan saran yang konstruktif dari pembaca sangat diharapkan guna penyempurnaan di masa mendatang. Semoga penelitian ini dapat memberikan manfaat bagi semua pihak yang membutuhkan.

DAFTAR PUSTAKA

Suhaemin, Amin., & Muslih. (2023). *Karakteristik Cybercrime di Indonesia. Edulaw: Journal of Islamic Law and Jurisprudance.* Vol. 5. No. 2.

Matin., & Rahardjo., (2020) *Malware detection using honeypot and machine learning.* IEEE. 7(2). 1-4

Amdani, R.T., & Iqbal, M. (2021). *Analisis Dan Deteksi Malware Poison Ivy Malware Analisis Statis Analysis And Detection Of Malware Poison Ivy With Malware Dynamic Analysis Method And Malware Static Analysis,* 7(2), Pp. 178–191.

Nasution, M.A.H. & Laksono, A.T. (2020). *'Investigasi Serangan Backdoor Remote Access Trojan (Ra) Terhadap Smartphone',* 7(4), Pp. 505-510. Https://Doi.Org/10.30865/Jurikom.V7i4.2301.

Pressman, & R. S. (2021). *Rekayasa Perangkat Lunak: Pendekatan Praktisi Yogyakarta:* Andi. (Edisi 7, hal. 45-78).

Solomon, R., & Maunder, S. (2021). *TCP/IP Analysis and Troubleshooting.* Springer. pp. 45-78.

Alhassan, I., Bock, C., & Bozkurt, S. (2022). *Malware Detection using Anomaly Detection Algorithms.* IEEE Xplore.

Liao, Y., & Chiu, H. (2021). *Network Traffic Anomaly Detection: A Comprehensive Survey.* Wiley.

Akhtar, M. S., & Feng, T. (2022). *Malware Analysis and Detection Using Machine Learning Algorithms.* Symmetry, 14(11), 2304.

Zhang, T., & Lee, J. (2021). *Advanced Techniques in Intrusion Detection and Anomaly Detection for Computer Networks.* Academic Press.