BAB I
PENDAHULUAN

1.1 Latar Belakang

Ancaman keamanan siber terus meningkat seiring dengan berkembangnya teknologi informasi dan ketergantungan terhadap sistem komputer. Salah satu malware yang masih menjadi ancaman serius adalah Trojan Emotet. Malware ini memiliki tingkat kompleksitas tinggi dan secara khusus menargetkan sistem operasi Windows [1]. Awalnya dikenal sebagai banking trojan, Emotet telah berevolusi menjadi malware modular yang mampu memuat berbagai *payload* berbahaya serta mempertahankan komunikasi berkelanjutan dengan server *Command and Control (C2)* melalui jaringan [2].

Dominasi penggunaan sistem operasi Windows pada perangkat individu maupun organisasi menjadikan platform ini sasaran utama infeksi Emotet. Infeksi tersebut dapat menimbulkan berbagai risiko keamanan, seperti kompromi sistem dan pencurian data. Selain itu, Emotet sering dimanfaatkan sebagai pintu masuk bagi serangan lanjutan yang memperluas dampak ancaman siber [3]. Oleh karena itu, perlindungan terhadap sistem operasi Windows dari ancaman seperti Emotet menjadi hal yang sangat penting [4].

Karakteristik utama Trojan Emotet tercermin pada aktivitas komunikasinya di lapisan jaringan. Malware ini secara aktif menghasilkan lalu lintas jaringan untuk menjaga koneksi C2, menyebarkan modul tambahan, dan mentransmisikan data korban. Oleh karena itu, analisis lalu lintas jaringan menjadi kunci dalam memahami perilaku dan ancaman Emotet [5].

Permasalahan muncul karena lalu lintas jaringan Emotet dirancang menyerupai trafik normal melalui enkripsi dan pola komunikasi yang samar, sehingga aktivitas berbahaya sulit terdeteksi meskipun sistem Windows tampak berfungsi normal [6].

Dalam keamanan sistem, lalu lintas jaringan merepresentasikan interaksi antara sistem terinfeksi dan infrastruktur penyerang. Setiap paket data berpotensi

memuat indikator kompromi yang dapat mengancam integritas dan kerahasiaan sistem Windows. Oleh karena itu, analisis lalu lintas jaringan menjadi penting dalam mengidentifikasi ancaman keamanan [7].

Packet analysis merupakan teknik forensik jaringan untuk menganalisis paket data secara rinci guna mengidentifikasi aktivitas jaringan yang tidak terdeteksi melalui pemantauan sistem konvensional, sehingga penting dalam mengungkap aktivitas malware tersembunyi [8].

Wireshark sebagai *packet analyzer* bersifat *open-source* memungkinkan analisis lalu lintas jaringan berdasarkan data paket aktual. Melalui Wireshark, perilaku komunikasi malware dapat diamati secara langsung dan sistematis [9]. Namun, penggunaan Wireshark dalam penelitian keamanan jaringan masih umumnya terbatas pada deteksi anomali lalu lintas, tanpa mengaitkan hasil packet analysis dengan dampak keamanan pada sistem operasi yang terinfeksi [10].

Penelitian berbasis packet analysis telah mampu mengidentifikasi pola komunikasi C2 Trojan Emotet, namun umumnya belum mengaitkan aktivitas jaringan tersebut dengan dampak keamanan sistem operasi Windows secara komprehensif [11].

Secara global, penelitian Emotet lebih menitikberatkan pada evolusi dan penyebaran malware serta teknik evasi, sehingga analisis lalu lintas jaringan masih bersifat pendukung dan belum terintegrasi [12]. Hingga kini, kajian empiris yang mengaitkan karakteristik paket jaringan Trojan Emotet dengan kompromi keamanan pada sistem operasi Windows masih terbatas, meskipun lalu lintas jaringan Emotet berperan langsung dalam ancaman seperti eksfiltrasi data dan koneksi jarak jauh tidak sah [13].

Meskipun demikian, aktivitas jaringan Emotet berkontribusi langsung pada berbagai bentuk kompromi keamanan, seperti eksfiltrasi data, pembukaan koneksi jarak jauh yang tidak sah, dan pembukaan jalan bagi masuknya malware yang lebih lanjut. Kerugian keamanan sistem operasi Windows sulit diidentifikasi secara menyeluruh tanpa memahami karakteristik lalu lintas jaringan tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah penulis paparkan diatas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara mendeteksi aktivitas atau trafik malware Emotet pada jaringan sistem operasi Windows berdasarkan hasil *packet analysis* menggunakan Wireshark?
2. Bagaimana dampak aktivitas lalu lintas jaringan yang dihasilkan oleh Trojan Emotet terhadap keamanan sistem operasi Windows berdasarkan hasil packet analysis menggunakan Wireshark?

1.3 Batasan Masalah

1. Penelitian ini hanya membahas Trojan Emotet pada sistem operasi Windows.
2. Analisis dibatasi pada lalu lintas dan fitur paket jaringan yang dihasilkan oleh Emotet.
3. Packet analysis menggunakan Wireshark digunakan sebagai satu-satunya metode analisis.

1.4 Tujuan Penelitian

1. Menganalisis pola lalu lintas jaringan akibat infeksi Trojan Emotet pada OS Windows.
2. Mengidentifikasi karakteristik lalu lintas jaringan Trojan Emotet pada sistem operasi Windows berdasarkan hasil *packet analysis* menggunakan Wireshark.
3. Memberikan gambaran empiris mengenai peran *packet analysis* dalam mengkaji dampak malware berbasis jaringan terhadap keamanan sistem operasi Windows.

1.5 Manfaat Penelitian

Manfaat yang ingin dicapai di penelitian ini Adalah:

1. Menambah pemahaman akademik tentang dampak lalu lintas jaringan

Trojan Emotet pada keamanan sistem Windows.

2. Memberikan kontribusi kajian mengenai penggunaaan *packet analysis* dalam analisis malware berbasis jaringan.
3. Membantu mahasiswa memahami keterkaitan antara fitur paket jaringan dan indikasi kompromi keamanan sistem.

1.6 Sistematika Penulisan

Untuk mempermudah dalam memahami skripsi ini, maka penulis materi disusun dengan sistematika sebagai berikut:

BAB I PENDAHULUAN, Berisi latar belakang penelitian, rumusan masalah, Batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematik penulisan.

BAB II TINJAUAN PUSTAKA, Memabahas teori dan konsep yang berkaitan dengan malware, Trojan Emotet, sistem operasi Windows, keamanan jaringan, Wireshark, serta penelitian terdahulu yang relevan.

BAB III METODOLOGI PENELITIAN, Menjelaskan metode penelitian yang digunakan, skenario pengujian, lingkungan sistem, teknik pengumpulan data lalu lintas jaringan, serta tahapan analisis packet menggunakanWireshark.

BAB IV HASIL DAN PEMBAHASAN, Menyajikan hasil analisis lalu lintas jaringan Trojan Emotet, pembahasan karakteristik paket jaringan, serta keterkaitannya dengan dampak kompromi keamanan pada sistem operasi sistem Windows.

BAB V KEESIMPULAN DAN SARAN, Berisi kesimpulan berdasarkan hasil penelitian serta saran untuk pengembangan penelitian selanjutnya.