BAB I

PENDAHULUAN

1.1 Latar Belakang

Kejahatan dunia maya setiap tahunnya mengalami peningkatan yang sangat pesat, hal ini dikarenakan semakin berkembangnya teknologi komputer yang berdampak pada kehidupan manusia. Banyak cara yang dilakukan untuk mempermudah kegiatan kejahatan yang melibatkan teknologi komputer ini salah satunya adalah memanfaatkan kelemahan sistem jaringan komputer dengan menyusupkan program yang digunakan sebagai media untuk mencuri informasi dari sebuah sistem komputer, program ini disebut sebagai *malware* (Kurniawan, 2014).

Malware diantaranya seperti *virus* (komputer), *trojans*, *spyware*, dan *worm*. *Virus* komputer bekerja dengan cara menempel pada suatu *file* komputer yang biasanya berupa *file executable*, *trojan* bekerja dengan cara melakukan *social engineering files* berbahaya dengan menampilkannya seperti *files* yang terlihat tidak berbahaya, *spyware* adalah perangkat lunak yang disisipi kode untuk mendapatkan informasi penting dari pengguna seperti akun *bank*, *password*, dan informasi lainnya yang diinginkan oleh pembuatnya, sedangkan *worm* adalah perangkat lunak jahat yang dibuat dengan memanfaatkan celah lubang keamanan pada sistem operasi untuk tujuan tertentu (Septiani, 2016).

Zeus trojan adalah salah satu *malware* yang pernah menjadi sangat fenomenal karena menyebabkan kerugian yang besar serta melibatkan

banyak negara sebagai korbannya. *Zeus Trojan* secara khusus dirancang untuk mencuri informasi yang terkait dengan perbankan dimana cara infeksinya adalah melalui perpindahan dari *drive* ke *drive* ataupun *phising*. Kendali komponen *trojan Zeus* telah ditemukan di 196 negara, termasuk negara terisolasi seperti Korea Utara. Lima negara yang paling terinfeksi adalah Mesir, Amerika Serikat, Meksiko, Arab Saudi, dan Turki (Raditya, 2013).

Etaher dalam *From Zeus to Zitmo: Trends in Banking Malware* (2015) menyatakan bahwa *Zeus* merupakan *Trojan* yang mencuri data rahasia, untuk dijual yang menawarkan layanan kepada klien, dengan perbaikan bug ke basis kode *Zeus* pertama dan dengan fitur yang berbeda, misalnya, perekaman video dan deteksi *sandbox*. Komunitas keamanan sekarang memiliki kemampuan untuk melacak *server* perintah ini dan memblokirnya. *Bot Zeus* telah ditemukan bertanggung jawab atas 44% infeksi *malware online* selama transaksi keuangan dan sekitar 90% dari penipuan perbankan global. Ada sekitar 3,6 juta komputer yang terinfeksi oleh *Zeus* di AS saja selama periode 2009 dan 2010. Era ini dianggap sebagai periode paling produktif untuk *Zeus*.

Penelitian ini adalah sebuah upaya untuk memberikan gambaran solusi dalam penanganan atas serangan *malware* dengan cara melakukan analisis terhadap *malware zeus* yang telah berhasil melakukan serangan, dengan menggunakan metode analisis dinamis dan *reverse engineering*.

Penelitian yang dilakukan oleh Damodaran (2015) menyatakan bahwa metode analisis dinamis sangat efektif apabila digunakan untuk melakukan analisis perilaku atau aktivitas dari berbagai jenis *Malware*, termasuk *Zeus Trojan*. Namun, metode analisis dinamis hanya dapat dilakukan apabila *malware* dijalankan secara langsung, sehingga dapat mengakibatkan sistem yang dipakai untuk uji coba dapat terkena infeksi dari *malware* tersebut. (Damodaran, 2015)

Penelitian yang dilakukan oleh H. Binsalleeh menyatakan bahwa metode *reverse engineering* pada *malware zeus* menjelaskan proses pembuatan dan pemasangan *bot* dan mengekstrak kunci enkripsi dari *malware* serta penggunaannya untuk mendekripsi komunikasi jaringan dan informasi konfigurasi *botnet*.

Analisis *malware* dengan menggunakan *reverse engineering* akan mendapatkan *source code* dari *malware* tersebut. *Source code* ini dapat mempelajari cara kerja *malware*, karakteristiknya, teknik infeksi yang digunakan dan lain-lain. Keuntungan melakukan *reverse engineering* pada analisis *malware* adalah *malware* tidak dijalankan (*execute*) sehingga meminimalisir kemungkinan komputer terinfeksi *malware* tersebut. (Ismail, 2018)

Penelitian ini dilakukan dengan cara analisis dinamis dan *reverse engineering*. Proses analisis dinamis dibutuhkan mesin virtual sebagai *tools* bantuan yang digunakan untuk proses uji coba, sehingga meminimalisir adanya infeksi *malware* pada sistem yang asli. Proses

reverse engineering dilakukan dengan dua acara yaitu *disassembler* dan *hashing* untuk mendapatkan informasi yang ada didalam *malware* sehingga dapat diketahui bagaimana *malware* tersebut bekerja .

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka rumusan masalah yaitu:

- a. Bagaimana melakukan proses identifikasi serangan *Malware Zeus* menggunakan metode analisis dinamis?
- b. Bagaimana cara kerja *Malware Zeus* dengan melakukan *reverse engineering* menggunakan proses *disassembler*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas maka tujuan penelitian yaitu:

- a. Melakukan proses identifikasi serangan *Malware Zeus* menggunakan metode analisis dinamis.
- b. Mengetahui cara kerja *Malware Zeus* dengan melakukan *reverse engineering* menggunakan proses *disassembler*.

1.4 Batasan Masalah

Adapun batasan masalah dari penelitian yaitu:

- a. Analisis yang dilakukan merupakan *reverse engineering*.
- b. Penelitian yang dilakukan dalam Mode *Virtual*
- c. Penelitian dilakukan pada sistem operasi *Windows*.
- d. Aplikasi yang digunakan untuk analisis berbasis *freeware*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini yaitu agar hasil dari penelitian dapat dimanfaatkan dan digunakan oleh sebagai berikut:

- a. Bagi Ilmu Pengetahuan
 1. Menambah wawasan tentang cara kerja *malware* khususnya pada *malware Zeus*.
 2. Mengetahui proses identifikasi *malware Zeus*.
- b. Bagi Masyarakat Umum
 1. Mengetahui tanda-tanda sistem yang terserang oleh *malware Zeus*.
 2. Mengetahui cara pencegahan *malware Zeus*.

1.6 Metodologi

Metode penelitian menjelaskan mengenai tahapan atau prosedur penelitian untuk menganalisa suatu *malware* komputer, *malware* yang ada di lakukan analisis dengan melakukan *Reverse Engineering* dengan kombinasi *tools* yang bersifat *freeware* dan dilakukan dalam lingkungan aman yaitu pengujian dalam model *virtual*.

1.7 Sistematika Penulisan

Sistematika penulisan untuk memahami lebih jelas isi laporan, materi-materi yang tertera pada laporan skripsi ini dikelompokkan menjadi beberapa sub bab dengan sistematika penyampaian sebagai berikut:

BAB I PENDAHULUAN

Berisi tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisikan kajian dari penelitian terdahulu dan teori yang berupa pengertian dan definisi yang diambil dari kutipan jurnal, web, ataupun buku serta beberapa *literature review* yang berkaitan dengan penyusunan laporan skripsi ini.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan metodologi penelitian yang memberikan gambaran dan alur dari penelitian yang dilakukan, menjelaskan dari metodologi penelitian, kajian teori, analisis dinamis dan *reverse engineering*.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil analisa *malware* dan pembahasan yang diusulkan dan yang diimplementasikan, pembahasan secara detail mengenai analisis *malware Zeus* dengan melakukan *reverse engineering*.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang berkaitan dengan analisa berdasarkan yang telah diuraikan pada bab-bab sebelumnya.