BAB 1
PENDAHULUAN

1.1 Latar Belakang

Kemudahan yang dirasakan dengan berkembang nya zaman, membuat setiap manusia juga dimudahkan dalam setiap urusannya. Kemajuan teknologi tidak dipungkiri selalu menjadi kebutuhan yang berdampingan dalam kegiatan setiap manusia kesehariannya. Namun terkadang kemudahan tersebut dapat dimanfaatkan oleh beberapa pihak yang tidak bertanggung jawab dan dijadikan suatu keuntungan individu atas pihak yang dirugikan.

Baru-baru ini, situs web phising semakin berbahaya dan menjadi masalah yang serius dibidang keamanan jaringan. Penyerang menggunakan banyak pendekatan untuk menanamkan *Ransomware* ke host target untuk memblok akses korban terhadap data mereka dan memeras korban dengan melakukan pembayaran uang atau sebagai tebusan untuk membuka akses kembali data atau *file* korban. *Ransomware* hadir dalam berbagai bentuk, misalnya mengunci layar pada sebuah perangkat atau perangkat lunak yang berbasis kripto yang mengenkripsi *file* target atau dengan algoritma kriptografi canggih.

Tujuan para pelaku yang berperan sebagai penyerang yaitu untuk mengambil keuntungan dari kelalaian korban yang sering mencari program bajakan di internet. Dengan demikian banyak cara yang dilakukan oleh seorang penyerang, salah satunya adalah dengan pendekatan yang menghasilkan sebuah keuntungan. *Attacker* atau penyerang menjual *Alat*, yang digunakan untuk eksploitasi dan menginfeksi korban dengan cara *drive–by-download*, mereka beroperasi secara *exploit-as-a-service* yaitu membangun dan menyewakan *botnet*. Bahkan menawarkan sebuah jasa pembuatan bot dan menjual bot atau sebuah virus disusun bagaikan buku dalam rak(IKHSAN et al., 2021).

Metode analisis statis untuk menganalisis *Malware* ini tidak akan mengaktifkan *file Malware* secara langsung melainkan ditelusuri dan diteliti serta dianalisis terhadap kode sumber yang dituliskan didalam program dengan melakukan tahapan pembedahan program *Malware* tersebut, sehingga informasi yang didapatkan sangatlah lengkap dan bisa memberikan gambaran

yang sangat detail tentang mekanisme kerja *Malware* tersebut secara keseluruhan(Cahyanto et al., 2017).

Sedangkan untuk analisis dinamis dilakukan dengan menjalankan sampel *Malware* dan dimonitor selama program berjalan. Pada kasus seperti ini, analisis dinamis adalah cara terbaik untuk mengidentifikasi fungsionalitas *Malware*(Virgiawan A. Manoppo, Arie S. M. Lumenta, 2020).

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang masalah di atas dapat dibuat rumusan masalah berikut:

1) Bagaimana mengidentifikasi *Ransomware* dengan menggunakan metode analisis statis dan dinamis?
2) Bagaimana cara mencegah serangan *Ransomware* ?

1.3 Batasan Masalah

Batasan masalah dalam penulisan ini sebagai berikut :

1) Menggunakan sistem operasi ubuntu 18.04 dan menggunakan windows 7 ultimate untuk mengeksekusi *Malware* melalui virtualbox.
2) Menggunakan data dari *Ransomware* tipe STOP/DJVU.

1.4 Manfaat

Manfaat yang didapat diantara lain:

1) Dapat memahami cara kerja *Ransomware*.
2) Dapat mengetahui cara antisipasi kalau mengunjungi website yang kemungkinan terdapat *malware*.

1.5 Tujuan Penulisan

Tujuan yang ingin dicapai dalam penulisan ini adalah:

1) Menerapkan metode *static analysis* dan *dynamic analysis* untuk menganalisis *Malware*.
2) Dapat mengidentifikasi jenis *Ransomware* .
3) Dapat mencegah serangan *Ransomware* tersebut.

1.6 Sistematika Penulisan

Berikut ini adalah penulisan sistematis untuk memperjelas apa yang ingin dicapai oleh penulis dan untuk memastikan bahwa pembaca memahami apa yang ingin penulis lakukan:

BAB 1 PENDAHULUAN

Pada bab ini akan dijelaskan latar belakang masalah, rumusan masalah, batasan masalah, manfaat penulisan, tujuan penulisan, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Dalam bab ini berisi penjelasan mengenai landasan teori yang berhubungan dengan materi yang dibuat oleh penulis. Teori tersebut antara lain tentang pengertian malware, sejarah malware, jenis-jenis malware, stop ransomware, dan teknik analisis untuk melakukan identifikasi malware.

BAB 3 METODOLOGI PENULISAN

Pada bab ini terdapat kumpulan dari metode bagaimana penulis mengumpulkan data untuk penulisan, tahapan dalam penulisan, serta metode analisis malware.

BAB 4 HASIL DAN PEMBAHASAN

Dalam bab ini menjelaskan terkait hasil yang didapatkan berupa pembahasan dari hasil analisis malware yang dijelaskan dalam bentuk gambar dan tabel.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini berisi uraian tentang kesimpulan yang didapat dari penulisan yang telah dilakukan serta saran untuk pembaca terkait pengembangan penulisan lebih lanjut.