BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era tekhnologi seperti ini. banyak sekali pihak yang tidak bertanggung jawab dalam memanfaatkan situasi seperti ini untuk mendapatkan keuntungan dengan cara mengunci *file* atau system korban, sampai korban tersebut membayar tagihan yang diberikan dengan mata uang bitcoin. Dengan menggunakan bitcoin memungkinkan penjahat dunia maya menerima dana dengan tingkat anonimitas yang tinggi, membuat transaksi sulit dilacak. [1]

Ransomware merupakan tipe *malware* yang menginfeksi sebuah sistem, kemudian mengunci atau mengenkripsi data-data penting, untuk meminta tebusan. Penyerang akan memberikan tawaran dengan menyediakan *decrypt* untuk membuka *file* yang terkunci dengan membayar sejumlah uang dalam waktu singkat [2]. Terdapat 2 jenis *ransomware* dalam penyerangannya yaitu *Crypto Ransomware* dan *Locker Ransomware*. *Crypto Ransomware* merupakan jenis *Ransomware* yang mengenkripsi sebuah *file-file* penting di dalam sebuah komputer korban sehingga menjadi tidak dapat digunakan. Penjahat Cyber yang memanfaatkan serangan *crypto-ransomware* menghasilkan pendapatan dengan menyimpan *file* untuk tebusan dan menuntut korban membayar uang tebusan untuk memulihkan *file* mereka [3]. Tidak seperti *Crypto Ransomware*, *Locker Ransomware* mengunci perangkat korban dari perangkat mereka. Terkadang yang dikunci adalah *file* atau perangkat lunak [4].

Analisa *malware* secara umum dapat dilakukan dengan dua cara yaitu Analisa Static dan Analisa Dynamic. Meskipun kedua cara tersebut sama-sama menganalisa sebuah *malware*, akan tetapi dalam metodenya terdapat perbedaan. Analisa static digunakan untuk mencari source codenya lalu memahami kode tersebut sedangkan analisa dynamic dilakukan dengan cara mengeksekusi *malware* tersebut di sebuah virtual machine atau di sebuah device khusus untuk dipelajari perilaku yang ditimbulkan oleh *malware* tersebut.

Riset perusahaan keamanan siber Kaspersky menyebutkan bahwasannya sumber utama ancaman komputer di Indonesia antara lain internet, *malware* yang berasal dari removable media, dan *file* berbahaya dari tautan / link email. Sehingga *ransomware* rentan tersebar melwati media internet dan lain-lainnya.

Atas dasar-dasar masalah diatas maka peneliti membuat sebuah topik penelitian yang berjudul **"Analisis Perbandingan *Crypto Ransomware* dan *Locker Ransomware* Menggunakan Metode Dynamic"**. Dengan menggunakan dynamic analisis kita bisa membuka dan melihat sifat dari *malware* jenis *ransomware* ketika dijalankan pada suatu *device*.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka permasalahan yang dapat dirumuskan yakni "Bagaimana hasil analisis dynamic antara *ransomware crypto* dan *ransomware locker* ? "

1.3 Batasan Masalah

Mengingat permasalahan yang komplek serta menghindari meluasnya ruang lingkup masalah, perlu adanya baasan masalah pada penelitian ini, diantaranya:

a. Perbandingan *crypto ransomware* dan *locker ransomware*
b. Analisis dynamic pada *ransomware crypto* dan *locker* menggunakan dynamic analisis
c. Penelitian ini hanya mengambil satu *malware* yaitu *ransomware* dengan jenis *crypto* dan *locker*
d. Analisa dnamic menggunakan VirtualBox dengan *windows* 10-64bit, ram 2048 dan hardisk 20 Gb
e. *Crypto Ransomware* menggunakan jenis VoidCrypt
f. *Locker Ransomware* menggunakan jenis Virlock

1.4 Tujuan Penelitian

Adapun tujuan dari hasil penelitian ini adalah :

a. mengetahui proses analisis dynamica pada *crypto ransomware* dan *locker ransomware*
b. Menganalisa cara kerja serangan *ransomware crypto* dan *locker*
c. Memberikan informasi pencegahan terhadap ancaman *ransomware*

1.5 Manfaat Penelitian

Diharapkan dalam manfaat penelitian ini dapat memberikan pemahaman kepada pengguna perangkat agar lebih berhati - hati dalam mengakses internet dan mengetahui cara menganalisanya terhadap *ransomware* tersebut.

1.6 Sistematika Penulisan

Dalam penelitian ini, penulis menyajikan dalam lima bab dengan sistematika pembahasan sebagai berikut:

1. **BAB I PENDAHULUAN**

   Bab ini berisi tentang latar belakang, rumusan masalah, Batasan masalah, tujuan penelitian dan sistematika penulisan

2. **BAB II LANDASAN TEORI**

   Bab ini berisi tentang teori-teori pemecahan masalah yang berhubungan dan digunakan untuk mendukung penulisan penelitian ini.

3. **BAB III METODOLOGI PENELITIAN**

   Bab ini berisi tentang penjelasan gambaran umum penelitian, masalah yang terdapat pada objek, spesifikasi alat yang digunakan, Pengumpulan data, perancangan dan simulasi serta rencana alur penelitian.

4. **BAB IV PEMBAHASAN**

   Bab ini berisi tentang impleentasi, Analisa *malware*, uji coba pegujian, dan hasil dari penelitian ini.

5. **BAB V PENUTUP**

   Bab ini berisi tenatang kesimpulan dari hasil akhir penelitian dan saran.

6. **DAFTAR PUSTAKA**

   Pada bagian ini akan dipaparkan tentang sumber-sumber yang digunakan dalam penulisan penelitian ini.