BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Malware atau *malicious software* adalah suatu program yang dibuat khusus untuk menginfeksi perangkat lunak atau aplikasi atau dokumen yang tersimpan dalam sebuah sistem. Sistem operasi yang terinfeksi malware dapat mengalami kerusakan sistem, file atau kehilangan data-data penting. [1]

Salah satu jenis malware adalah *ransomware*. *Ransomware* bekerja dengan cara menyerang jaringan internet. Selain itu, *ransomware* juga mengenkripsi komputer korban. Untuk dapat mengakses komputernya lagi, korban diminta untuk menebus (*ransom)* dengan sejumlah uang dalam bentuk Bitcoin. Berdasarkan data Q3 2020 dari *Kaspersky*, serangan *ransomware* mencapai 121.579 korban, di antaranya menyerang pada bidang pendidikan, perawatan kesehatan, tata kelola, dan keuangan [2].

GandCrab merupakan salah satu geng dari *ransomware* yang paling terkenal dan ganas karena mengklaim telah mendapatkan uang tebusan lebih dari US$ 2 miliar dalam waktu 18 bulan. GandCrab sempat menyatakan pensiun pada pertengahan tahun 2019 yang lalu, namun virusnya masih banyak tersebar luas.

Oleh karena itu, analisis statis pada GandCrab merupakan salah satu tindakan yang diperlukan untuk mengetahui karakteristik dari *ransomware* ini. Analisis statis adalah salah satu metode analisis yang dilakukan dengan cara memahami fungsi *source code* dari malware untuk mendapatkan informasi yang lengkap dan gambaran detail mekanisme kerja sebuah malware. Para peneliti malware perlu mengetahui metode ini. Peneliti tertarik melakukan penelitian untuk memahami metode analisis ini lebih lanjut, dan membuat sebuah topik penelitian dengan judul **"Analisis Malware GandCrab Ransomware Pada Windows Menggunakan Metode Statis".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan sebelumnya, maka pokok masalah yang akan dibahas dalam penelitian ini adalah: "Bagaimana cara melakukan analisis statis pada *Malware Gandcarb Ransomware*?"

1.3 Batasan Masalah

Agar dalam penyusunan Tugas Akhir ini tidak terlalu jauh dan menyimpang dari pokok permasalahan, maka penulis membatasi permasalahan yang meliputi :

1. Analisis *Malware Gandcarb Ransomware* menggunakan analisis statis
2. Analisis statis dilakukan pada *strings* malware
3. Penelitian ini hanya melakukan analisis malware dan tidak membuat anti-*malware*.
4. Tool yang digunakan untuk analisis ini adalah Dependency walker, PEStudio, Exeinfo PE, dan PEexplorer.

1.4 Tujuan Penelitian

Tujuan yang ingin diraih dalam pembuatan laporan skripsi ini adalah:

a. Untuk mengetahui karakteristik dan sistem kerja dari *ransomware gandcrab*
b. Membuktikan metode statis dapat digunakan untuk mendeteksi perilaku *malware gandcrab ransomware*.

1.5 Sistematika Penulisan

Untuk memudahkan pemahaman terhadap penelitian ini, maka pembahasan dibagi dalam beberapa bab sesuai dengan pokok permasalahan, yaitu:

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini terdapat tinjauan penelitian yang penah dilakukan peneliti lain sebelumnya, landasan teori yang menjelaskan tentang

malware, metode, tools, dan penjelasan tentang teori-teori pemecahan masalah yang berkaitan dan digunakan sebagai pendukung penulisan penelitian ini.

BAB III METODOLOGI PENELITIAN

Pada bab ini akan dijelaskan mulai dari gambaran umum *Malware Gandcarb Ransomware*, alur penelitian, kebutuhan alat dan bahan penelitian.

BAB IV PEMBAHASAN

Pada bab ini menjelaskan tentang analisis malware dan hasil dari penelitian ini.

BAB V PENUTUP

Merupakan bagian akhir dari penulisan yang berisi kesimpulan tentang hasil analisa dan pembahasan serta saran-saran untuk penelitian selanjutnya.