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 dikehidupan manusia (Septani et al., 2016). Hasil survey yang dilaksanakan oleh IDCERT tahun 2015, Negara Indonesia menjadi negara yang paling sering diserang *malware* (Wahidin et al., 2022).

Malicious software atau yang lebih dikenal sebagai *malware* merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktivitas berbahaya atau perusak perangkat lunak lainnya seperti *Trojan, Ransomware, Virus, Spyware* dan *Exploit.* Dibutuhkan analisa untuk menentukan apakah aplikasi dalam komputer itu teridentifikasi adalah sebuah *malware* dan untuk mengetahui karakteristik dari *malware* tersebut dan dampak sistem setelah *malware* tersebut dieksekusi (Manoppo et al., 2020).

Serangan *ransomware WannaCry* yang dimulai pada 12 Mei 2017, dan skalanya belum pernah terjadi sebelumnya dengan cepat memengaruhi lebih dari 200.000 komputer di lebih dari 150 negara (Wijaya, 2019). Secara umum, sindikat kejahatan transnasional “mengadaptasi model bisnis mereka dengan menggunakan apa yang disebut *'ransomware'* untuk mendapatkan kendali atas jaringan komputer dan kemudian meminta pembayaran sebagai imbalan untuk pemulihan.” Virus *WannaCry* mengeksploitasi kerentanan di *Microsoft Windows* yang awalnya

dikembangkan oleh Badan Keamanan Nasional AS dan beroperasi dengan mengenkripsi data korban dan menuntut pembayaran tebusan sebagai imbalan pemulihan data (Wahidin et al., 2022).

Malware yang berjenis *Ransomware WannaCry* telah melakukan serangan secara masif ke seluruh penjuru dunia termasuk Negara Indonesia (Kurniawan et al., 2021). *Malware* tersebut bekerja dengan cara melakukan *enkripsi file* dengan cepat serta menyebar data servernya, serta melakukan pemindaian port TCP dan UDP 139 dan 445 (SMB) dari komputer, apabila *port* tersebut terbuka, maka *malware* akan menyebar secara otomatis yang dapat merugikan kinerja pengguna. *Enkripsi file* yang digunakan pada *malware* tersebut adalah jenis RSA-2048 sehingga sangat sulit untuk menemukan kode enkripsinya (Wahidin et al., 2022).

Perbedaan antara *malware* biasa dengan *ransomware* yaitu, jika *malware* aktivitasnya cenderung bersembunyi dan tidak mau menampakkan diri. Sedangkan, *ransomware* lebih menampakkan aktivitasnya sebagai *virus.* Merujuk perbedaannya pengguna dapat mengetahui apabila dirinya sedang terinfeksi oleh *ransomware* (Wahidin et al., 2022).

Teknik *malware analysis* dapat membantu penelitian dalam memahami risiko dan bahaya dari *malware* tersebut. Salah satu cara metode yang dapat digunakan ada dengan *signature-based detection.* (Nugraha et al., 2019)

Penelitian yang telah dilakukan sebagai dasar penelitian ini diantaranya, Penelitian metode *reverse engineering* dengan teknik *string analysis* berhasil menunjukkan 12 *function* yang terdapat pada sample *malware flawed ammyy rat* ini menunjukkan bahwa penelitian sebelumnya telah menunjukkan hasil *reverse*

engineering dengan *disassembly* telah teridentifikasi tidak ada *function* yang terlewat, jadi sebaiknya untuk melakukan *reverse engineering* sebaiknya dilakukan terlebih dahulu string analisis untuk mengetahui *function* atau mengetahui proses *load* dari *malware* kemudian dilakukan *disassembly* untuk mengetahui *source code* yang terdapat pada *malware*. Metode *sandbox* online menunjukkan *file section* dan *file import* dari *malware* tersebut (Setia et al., 2019).

Terdapat penelitian lain identifikasi *malware* dilakukan dengan mencari API *call memory* dan hasil *signature*. Berdasarkan data yang diperoleh, hasil API *call memory* dengan hasil *signature* saling terkait. Hasil *signature* dihasilkan dari beberapa API *call memory* yang dijalankan oleh *malware* (Setiawan et al., 2021). Hasil *API call memory* dan hasil *signature* didapatkan dengan menggunakan *tools static analysis* yang digunakan selama pengujian berlangsung (Nugraha et al., 2019).

Berdasarkan ciri khas *ransomware* yang meminta tebusan secara terang-terangan (Ferdiansyah, 2018), maka dalam penelitian ini dilakukan analisis *ransomware WannaCry* menggunakan metode *reverse engineering* dan *signature-based detection* tersebut pada pola *byte*, kode instruksi sehingga didapatkan pola *byte*, kode instruksi, pola serangan pada *malware* ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan, perumusan masalah untuk penelitian yang akan dilakukan adalah, bagaimana cara melakukan investigasi dan

analisis terhadap *signature malware wannacry* menggunakan metode *reverse engineering* dan *signature-based detection* ?

1.3 Tujuan Penelitian

Tujuan dari penelitian adalah melakukan proses investigasi *malware WannaCry* degan menggunakan metode *Reverse Engineering* dan *Signature-based Detection* pada pola *byte* dan kode instruksinya.

1.4 Batasan Masalah

Berdasarkan rumusan masalah yang penulis buat, untuk menghindari pembahasan yang melebar dari seharusnya, oleh karena itu penulis membuat batasan dalam melakukan penelitian yaitu:

a. Melakukan *investigasi malware ransomware* dikhususkan hanya pada *malware WannaCry.*
b. *Signature* yang di teliti hanya berupa sample pola *byte*, atau kode instruksi yang terdapat di *malware WannaCry* diantaranya MD5, *File Name*, *string Signature*, pemanggilan fungsi khusus, instruksi *assembly, networking*, enkripsi dekripsi.
c. Penelitian dilakukan dalam *Virtual Machine mode.*
d. Penelitian dilakukan pada *system operasi windows.*
e. Aplikasi yang digunakan untuk analisis berbasis *freeware.*

1.5 Manfaat Penelitian

Manfaat dalam penelitian ini adalah sebagai berikut:

a. Mengetahui pola serangan *malware WannaCry* dalam kehidupan sehari – hari dengan analisis *signature* daripada *WannaCry*.
b. Mengetahui cara kerja *malware* khususnya *WannaCry*
c. Meminimalisir *system* dalam penanganan serangan *malware WannaCry* maupun sejenisnya.
d. Berkontribusi dalam bidang analisis *malware* sebagai dokumentasi dimasa mendatang.
e. Relevansi bagi para peneliti yang juga ingin meneliti terkait *malware WannaCry* atau *malware* lainnya.
f. Benih suka membaca, menulis, menganalisis, dan informasi berharga.
g. Memahami berbagai masalah dan meningkatkan kesadaran pengguna digital.
h. Mendapatkan ilmu pengetahuan dan informasi baru.
i. Mencari solusi atas sebuah permasalahan.

1.6 Metode Penelitian

Sistematika penulisan yang digunakan dalam penelitian ini adalah 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 literatur 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 ataupun statis, dan prosedur analisis data.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil studi analisa *malware* dan pembahasan yang diusulkan dan yang diimplementasikan, pembahasan secara detail mengenai analisa *malware WannaCry* menggunakan *reverse engineering* dan *signature-based detection.*

BAB V SIMPULAN DAN SARAN

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