BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan yang pesat pada teknologi informasi mempengaruhi kehidupan umat manusia sedari dari anak-anak sampai dengan orang dewasa karena rasa ingin tahu akan hal baru membuat eskalasi teknologi yang tak bisa dibendung, sehingga dapat memberi dampak yang positif ataupun negative bagi pengguna itu sendiri, semakin canggih suatu teknologi menyebabkan kenaikan angka resiko kejahatan di dunia maya yang diterima oleh pengguna[1]. Di Indonesia Sistem Operasi *Desktop* yang banyak digunakan adalah *Windows* dengan 79.63%, *Unknown* 13.3%, OS X 4.9%, Linux 2.02%, Chrome OS 0.07%, dan FreeBSD sebesar 0% pada bulan Mei 2021 [2].

Banyaknya pengguna *windows* tidak mengimbangi dengan menggunakan produk yang asli dari *developer*, mendownload aplikasi secara sembarangan melalui website yang tidak dipercaya, atau mengklik sebuah link maupun aplikasi pada sebuah email dari orang yang tidak dikenal. Sehingga secara tidak sadar banyak celah pada aplikasi yang di download tersebut sehingga memungkinkan pengguna tidak mengetahui bahwa pada *software* tersebut terdapat *malware* yang disisipkan sehingga banyak terjadi kasus pencurian data, pada statistik tahun 2019 sebanyak 80% dari perusahaan Indonesia menggunakan software bajakan dan menjadi yang tertinggi di Asia tenggara, sehingga celah itu dapat dimanfaatkan oleh *hacker* untuk melakukan pencurian data melalui aplikasi yang disusupi *malware* tersebut [3].

Malware atau *Malicious Software* merupakan sebuah aplikasi yang digunakan untuk melakukan aktivitas yang bahaya maupun merusak *software* yang lain, *malware* diklasifikasikan menjadi 5 menurut penelitian yang dominan menyerang komputer yaitu Virus, Worm, Trojan Horse, Spyware dan Backdoor [4]. *Malware* diciptakan untuk melakukan pencurian data sampai merusak sistem dengan cara melakukan penyusupan pada komputer korban. Salah satu jenis *malware* yang digunakan untuk melakukan pencurian data adalah *Remote Access*

Trojan yang masuk kategori *backdoor* karena bisa memberikan akses penuh komputer korban melalui *backdoor* tanpa sepengetahuan pengguna saat terhubung dengan internet [5].

Analisis memori bisa sangat berguna dalam menganalisis *malware*. Sebuah *malware* pasti meninggalkan beberapa jejak yang bisa dianalisis dengan cara mengakuisisi akuisisi memori RAM secara langsung. Analisis memori berperan penting dalam bidang forensik digital. Karena itu kita dapat memastikan karakter dan alur proses sebuah *malware* saat berjalan di latar belakang dalam sistem operasi. Analisis memori juga bisa memperoleh sebuah password dan data yang tidak disimpan di *hard drive* sistem juga dapat diperoleh dengan teknik ini [6]. Yara Rule merupakan sebuah tools penunjang yang bertujuan untuk membantu seorang peneliti untuk mengidentifikasi dan mengklasifikasikan sebuah sample *malware*, Yara rule dibuat berdasarkan jenis *malware* dan Indicator of Compromise(IOC) atau string *malware* tersebut [7][8].

Metode memori forensik dan *Yara Rule* merupakan beberapa metode yang bertujuan untuk menganalisa aktivitas sebuah *malware* yang tersimpan dalam RAM. Memori forensik dan *Yara Rule* pada analisis *malware* bertujuan untuk melakukan analisis aktivitas *malware* pada jaringan, perubahan *registry*, perubahan data yang berjalan pada sistem operasi dan menganalisa *string malware* agar bisa mengetahui pola kerja dari sebuah *malware*.

1.2 Rumusan Masalah

Untuk mengarahkan dan memperjelas penelitian ini agar bisa mendapatkan hasil yang sesuai dengan topik pembahasan, maka masalah yang dirumuskan adalah mengakuisisi RAM pada sebuah komputer yang terinfeksi *malware*, yang kemudian peneliti melakukan analisis aktivitas *malware* yang berjalan pada memori RAM dengan metode memori forensic, dan peneliti melakukan analisa string sample *malware* RAT (*Remote Access Trojan)* menggunakan metode *Yara Rule*.

1.3 Batasan Masalah

Agar masalah di dalam penelitian ini tidak keluar dari konteks penelitian, maka lingkup masalah dalam penelitian ini meliputi

a. VirtualBox menjadi tempat instalasi sistem operasi.
b. *Windows* 10 sebagai sistem operasi *victim* dan tempat instalasi *malware* RAT jenis *redline stealer*.
c. Kali Linux sebagai sistem operasi untuk melakukan analisis *malware*.
d. Menggunakan metode *Memory Forensic* dan *Yara Rule*.
e. *FTK Imager* menjadi *tools* yang digunakan untuk akuisisi RAM.
f. *File Image* hasil *dump* RAM adalah *.mem*.
g. *Tools* yang dipakai untuk guna analisis memori adalah *volatility*.
h. *Tools* yang dipakai untuk guna analisis *string malware* adalah *Yara Rule*.

1.4 Tujuan Penelitian

Tujuan yang ingin digapai pada penelitian ini adalah mendapatkan data dari memori yang diakuisisi kemudian dilakukan analisis menggunakan *volatility* dengan mengimplementasikan metode *Memory Forensic* dan *Yara Rule* agar diketahui karakteristik dan perilaku dari *malware* yang disisipkan pada aplikasi GCleaner. Diinginkan dari penelitian ini bisa digunakan untuk referensi bagi peneliti yang melakukan analisis *malware* selanjutnya.

1.5 Manfaat Penelitian

Manfaat yang bisa diberikan dari penelitian ini bisa dilihat sebagai berikut:

a. Memberikan cara dalam melakukan analisa sebuah *malware* menggunakan metode Memori Forensik dan *Yara Rule*
b. Menjadi dasar referensi kepada peneliti selanjutnya dalam melakukan analisis *malware*.

1.6 Sistematika Penulisan

Pada skripsi ini, peneliti dipresentasikan dalam lima bab menggunakan sistematika pembahasan berikut ini:

Bab I Pendahuluan

Bab ini menjelaskan tentang latar belakang, perumusan masalah, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Tinjauan Pustaka dan Landasan Teori

Bab ini menjelaskan tentang rujukan jurnal dan teori yang dipakai sebagai landasan penelitian guna menyelesaikan masalah yang digunakan pada penelitian ini. Bagian ini membahas tentang *malware* pada system operasi *windows*.

Bab III Metodologi Penelitian

Bab ini menggambarkan gambaran umum, tahapan penelitian, masalah pada objek penelitian, spesifikasi alat yang digunakan, mengumpulkan data, merancang dan mensimulasikan rencana penelitian.

Bab IV Pembahasan

Bab ini menggambarkan tentang implementasi, analisis *malware RAT*, dan hasil dari penulisan skripsi ini.

Bab V Penutup

Bab ini menggambarkan kesimpulan pada hasil akhir penilaian penelitian, dan saran.

DAFTAR PUSTAKA

Bab ini menjelaskan tentang sumber referensi yang digunakan oleh penulis untuk membantu menyelesaikan penelitian ini