BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan dan kemajuan teknologi informasi dan komunikasi sekarang sudah sangat modern ,sehingga banyak sektor yang beralih menggunakan teknologi komputerisasi. Perkembangan dan kemajuan tersebut juga memaksa masyarakat untuk melakukan perubahan dalam segala aspek bidangnya. Berdasarkan data yang dikeluarkan oleh badan pusat statistik, penggunaan Teknologi Informasi dan Komunikasi (TIK) mengalami perkembangan yang pesat sejak lima tahun terakhir. Perkembangan paling pesat terlihat terlihat pada penggunaan internet dalam rumah tangga yang mencapai angka 78,18% , sedangkan untuk kepemilikan komputer dalam rumah tangga mengalami kenaikan sebesar 18,83% pada tahun (Tri dkk., 2020).

Perkembangan dan kemajuan teknologi tidak hanya membawa dampak yang positif bagi masyarakat, tetapi perkembangan dan kemajuan teknologi juga membawa dampak negatif, salah satunya adalah dengan munculnya berbagai macam tindak kejahatan *cyber*, seperti penyebaran *malware* (Virgiawan, Lumenta dan Karouw, 2020). *Malware* merupakan suatu program yang digunakan untuk kejahatan *cyber*crime dengan berbagai tujuan diantaranya untuk mencari kesenangan dan mencari keuntungan seperti melakukan penyadapan serta pencurian informasi pribadi. *Malware* dapat berisi kode berbahaya seperti Virus, *Worm*, *Trojan Horse*, juga bisa membuat *BackDoor* yang dapat melakukan

pencurian informasi pribadi atau mengambil kendali sistem komputer seseorang (Pajar Setia, Widiyasono dan Putra Aldya, 2018).

Malware pada umumnya dibuat untuk merusak atau membobol suatu software atau sistem operasi melalui script yang dirahasiakan atau dalam arti lain disisipkan secara tersembunyi oleh pembuat *malware* tersebut(Virgiawan, Lumenta dan Karouw, 2020). *Malware* pada saat ini sudah berkembang pesat ,sehingga mengharuskan pengguna komputer untuk lebih waspada dalam menjaga informasi ataupun *file* penting di komputer supaya tidak diambil dan disalah gunakan oleh orang yang tidak berhak (Adenansi dan Novarina, 2017).

Analis *Proofpoint* menemukan *variant malware* baru yang disebut *Redline Stealer* pada awal maret 2020 (Saleous dkk., 2022). *Malware* ini telah mendapat ketenaran berkat kemampuannya yang dapat menghindari deteksi dan mencuri informasi sensitif dari perangkat yang terinfeksi. *Malware Redline stealer* mencuri informasi data login, dan kartu kredit dari aplikasi *browser* (Alrabaee dan Manna, 2021). *Malware Redline Stealer* merupakan *malware* yang mengancam keamanan privasi data pada era digital, hal ini cukup mengkhawatirkan sehingga diperlukan lebih banyak lagi penelitian di bidang *malware* khususnya terhadap *Redline Stealer*.

Analisis *malware* umumnya dapat dilakukan dengan 2 metode yaitu *Dynamic Analysis* dan *Static Analysis* (Cahyanto, Wahanggara dan Ramadana, 2017). *Static Analysis* dilakukan dengan cara mengamati secara langsung *source code malware* tanpa menjalankan *malware* tersebut, sedangkan *Dynamic Analysis* dilakukan dengan cara mengamati kerja *malware* saat *malware* dijalankan pada suatu sistem(Adenansi dan Novarina, 2017). Penggabungan metode *Static* dan

Dynamic banyak dilakukan oleh para analis *malware* karena luasnya cakupan dan banyaknya *tools* yang tersedia sehingga dapat menghasilkan analisis yang detail dan menyeluruh (Yusirwan, Prayudi dan Riadi, 2015).

Penelitian ini menggunakan *malware Redline Stealer* sebagai objek analisis. Metode analisis *malware* yang digunakan pada penelitian ini yaitu *static analysis* dan *dynamic analysis*. Analisis *malware* pada penelitian ini dilakukan pada *virtual lab* yang terisolasi untuk menghindari penyebaran *malware* pada komputer. Penggunaan metode *static analysis* telah digunakan pada beberapa penelitian sebelumnya di antaranya dilakukan oleh (Megira, Pangesti dan Wibowo, 2018; Hazri, 2020). Penggunaan metode *static analysis* juga telah digunakan pada beberapa penelitian sebelumnya di antaranya dilakukan oleh (Virgiawan, Lumenta dan Karouw, 2020), sedangkan penggunaan metode *static analysis* dan *dynamic analysis* telah dilakukan oleh (Yusirwan, Prayudi dan Riadi, 2015; Cahyanto, Wahanggara dan Ramadana, 2017; Gunawan dan Ferriyan, 2017; Pajar Setia, Widiyasono dan Putra Aldya, 2018; Rusdi, Widiyasono dan Sulastri, 2019). Dari semua penelitian tersebut, belum ada penelitian yang membahas penggunaan metode analisis *static* dan *dynamic* yang menggunakan objek *malware Redline Stealer,* sehingga penelitian ini menjadi peluang penelitian yang baik untuk dilakukan.

Berdasarkan permasalahan dan latar belakang yang telah dipaparkan di atas, maka diusulkan suatu penelitian yang berjudul " Analisis *Malware* Redline Stealer Menggunakan Metode *Static Analysis* dan *Dynamic Analysis*".

1.2 Rumusan Masalah

Merujuk pada latar belakang penelitian di atas, maka dapat dirumuskan rumusan masalah pada penelitian ini yaitu:

1. Bagaimana proses investigasi dan analisis serangan *malware Redline Stealer* dengan menggunakan metode statis dan dinamis?
2. Bagaimana penanganan serangan *malware* Redline Stealer pada perangkat komputer?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini yaitu:

1. Pengujian dilakukan pada aplikasi virtual box dengan konfigurasi *NAT*.
2. Analisis dilakukan pada sistem operasi *Windows* tanpa *antivirus*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini yaitu:

1. Memahami proses investigasi dan analisis serangan *malware Redline Stealer* dengan menggunakan metode statis dan dinamis.
2. Melakukan penanganan serangan *malware Redline Stealer* pada perangkat komputer.

1.5 Manfaat Penelitian

Manfaat penelitian ini yaitu :

1. Menambah wawasan tentang karakteristik *malware* pada komputer, khususnya *malware Redline Stealer.*
2. Menjadi rujukan bagi penelitian lebih lanjut dan dapat menjadi dasar untuk pembuatan anti-*malware* untuk jenis *malware* serupa.

1.6 Metodologi Penelitian

Metodologi penelitian menjelaskan tentang apa saja tahapan yang dilalui selama proses penelitian. Tahapan – tahapan tersebut diantaranya adalah studi literatur, pengumpulan data, menyiapkan sistem, analisa *Malware Redline stealer* dan penarikan kesimpulan.

1.7 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini dibagi menjadi 5 bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan kajian dari penelitian terdahulu dan teori yang berupa pengertian dan definisi yang diambil dari berbagai sumber referensi yang berkaitan dengan penyusunan laporan tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang metodologi penelitian yang memberikan gambaran dan alur dari penelitian yang dilakukan, menjelaskan dari metodologi penelitian, kajian teori, analisis dinamis.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil analisa *malware* dan pembahasan yang diusulkan dan yang diimplementasikan, pembahasan secara detail mengenai analisis *malware Redline stealer* dengan melakukan analisis dinamis dan statis.

BAB V SIMPULAN DAN SARAN

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