BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

VLC Player adalah perangkat lunak pemutar media *open source* dengan lebih dari 4 miliar unduhan yang terus akan bertambah, saat ini digunakan di *platfrom* utama, termasuk *Windows, MacOS. Linux,* serta Android dan iOS [1]. Menurut informasi dari badan keamanan siber Jerman *CERT-Bund* metemukan celah keamanan yang beresiko tinggi [2], celah keamanan ini ditemukan di *VLC* versi Windows yang di idenfikasi sebagai *CVE-2019-5439* [3].

Keamanan *VLC* yang rentan ini dimanfaatkan peretas dengan cara membuat Video dengan format .mkv yang akan disisipkan malware sehingga dapat memicu *double free* pada *zlib_decompress_extra()* dan dapat menyebapkan *crash* pada VLC*[3]* yang nantinya dapat dimanfaatkan oleh peretas untuk mengambil alih kendali perangkat *computer* dari jarak jauh dengan menggunakan Teknik *Remote Code Execution (RCE)* [2].

Masyarakat umum perlu mengetahui kinerja malware jenis ini, dan mewaspadai dampak yang ditimbulkan. Para peneliti dapat melakukan analisis lebih mendalam terkait penyebaran malware jenis ini, karena dalam keterbatasan penelitian saat ini, peneliti belum menemukan adanya analisis lengkap tentang malware *MKV* yang menyerang *VLC Player* dengan metode analisis *dynamic*.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, dapat dirumuskan permasalahan yang akan di bahas yaitu: analisa terhadap-malware *MKV* yang menyerang *VLC Player* menggunakan *System Oprasi* Remnux dan metode analisis *dynamic*.

1.3 Batasan Masalah

1. Penelitian ini melakukan pengamatan serangan malware dan dampak serangannya,

2. Hasil penelitian ini bukan untuk memperbaiki *system* yang terinfeksi malware
3. Skenario serangan yang digunakan dalam penelitian, mengasumsikan, tidak terpasang antivirus pada *OS windows* yang dijadikan target serangan
4. Proses exploit dilakukan pada OS windows pada *virual box*
5. Injeksi video yang sudah terinfeksi malware menggunakan kali linux
6. Analisis dilakukan menggunakan tools Prosess explorer dan REMnux.

1.4 Tujuan Penelitian

Tujuan dari penelitian sebagai berikut

1. Mengetahui cara kerja malware yang menginfeksi file video
2. Hasil penelitian menerapkan *dynamic* analisis untuk mengamati dan menilai kinerja malware trojan yang menyerang *VLC Player*.
3. Dengan melakukan analisis terhadap Video *MKV* yang berbahaya dapat memberikan manfaat bagi pengguna agar terhindar dari peretas dan menambah informasi tentang keamanan dari sebuah file.

1.5 Metode penelitian

Metode penelitian dalam tugas akhir ini menggunakan metode *dynamic* analysis. Tahapan penelitian diantaranya:

1. **Studi Literatur**

   Studi literature dilakukan dengan cara membaca dan mempelajari sejumlah refrensi dan literature yang berhubungan dengan pembuatan malware.

2. **Observasi**

   Tahap ini merupakan proses pengumpulan informasi dengan mengamati kenerja malware yang terjadi secara real.

3. **Analisa Data**

   Tahap ini melakukan analisis malware dengan menganalisis Dynamic. Analisis malware ini dimulai dengan melihat kemungkinan adanya file yang diinfeksi malware pada objek yang diteliti, menjalankan objek

malware yang diteliti guna melihat efek yang ditimbulkan oleh malware terhadap sistem file.

1.6 Sistematika Penulisan

Penulisan Tugas Akhir ini disusun dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pendahuluan berisi latar belakang masalah, perumusan masalah, tujuan dan manfaat studi, ruang lingkup studi, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini memuat tentang hasil studi pustaka mengenai teori serta konsep. Menjelaskan materi yang tersedia yang berhubungan erat dengan topik laporan Tugas Akhir. Tinjauan pustaka berisi beberapa referensi dari hasil penelitian yang relevan dengan topik tugas akhir yang disajikan, yang diperoleh dari berbagai sumber.

BAB III METODOLOGI PENELITIAN

Bab ini mencakup metodologi penelitian yang memberikan gambaran dan alur dari penelitian yang dilakukan.

BAB IV PEMBAHASAN

Bab IV berisi rancangan proyek, implementasi malware serta evaluasi rancangan. Selanjutnya alur pengerjaan proyek, metode testing, hingga hasil akhir penelitian dan pembahasan analisis hasil akhir penelitian, termasuk pembahasan hasil-hasil uji coba (testing). Data hasil akhir pengujian dapat berupa grafik, table, data monitoring, log system, dan lain-lain, dengan pembahasan.

BAB V PENUTUP

Bab V berisi kesimpulan dari hasil akhir penilaian proyek, dan saran.