BAB I
PENDAHULUAN

1.1 Latar Belakang

Pandemi virus Corona (COVID-19) yang dimulai pada tahun 2019 sudah menjadi peristiwa krisis global, dengan dampak karantina masal yang dirasakan seluruh negara di dunia. Pada saat penulisan, Organisasi Kesehatan Dunia (WHO) melalui *Coronavirus Disease* (COVID-19) *Dashboard* melaporkan lebih dari 33 juta kasus yang dikonfirmasi dan lebih dari 1 juta kematian secara global[1]. Saat COVID-19 menyebar ke seluruh dunia, ada ancaman lain yang meningkat dan dirasakan dampaknya secara signifikan dalam bidang teknologi; yaitu, *Cybercrime, Cyberattacks* dan banyak serangan dunia maya yang menyerang secara acak maupun serangan yang ditargetkan[2].

Domain dari situs *coronavirusapp.site* adalah sebuah situs yang awalnya berisi data mengenai penyebaran virus Corona yang mana data ini diambil langsung dari *infection2020.com* (situs web dari pengembang *independen* untuk melacak berita COVID-19 yang berada di AS)[3]. Halaman utama dari *website coronavirusapp.site* dapat dilihat pada Gambar 1, dan spanduk kecil di bagian atas *website* bertujuan untuk yang mendorong orang yang melihat untuk memasangkan aplikasi mobile dari *website* ini agar pembaruan data lebih *realtime*.

Kemudian jika dilihat dari informasi domain yang didapatkan, domain situs *coronavirusapp.site* awalnya terdaftar pada 8 Maret 2020 menggunakan pengaturan *privasi* domain untuk mengaburkan detail dari identitas pendaftar[4]. Situs ini di-hosting oleh *Wrathost*, sebuah penyedia hosting dengan biaya murah. Sehingga domain tersebut berada pada *range* alamat IP dengan lebih dari 100 *domain* lain yang tidak terkait. Namun dilihat lihat sertifikat SSLnya, situs ini menggunakan sertifikat SSL dari *Let's Encrypt*. Ketika dilihat pada *Let's Encrypt SSL*,

Gambar 1. Halaman Utama *coronavirusapp.site*

Nama aplikasi *mobile* yang dapat diunduh dari *website* ini adalah *"Coronavirus_Tracker.apk"*. Aplikasi ini merupakan aplikasi yang ditujukan kepada pengguna *mobile Android*. Aplikasi *Android* tersebut kemudian dilakukan *analisis Statik, analisis Dinamik* untuk mengetahui *karakteristik* dan jenis *malware* yang disisipkan pada Aplikasi tersebut.

Gambar 1.1. Bukti adanya transaksi BTC

Dari gambar 1.1 dapat dilihat bahwa adanya pengiriman yang dilakukan terhadap korban dengan nilai 0.01 BTC.

Oleh karena itu perlu diketahui bagaimana penyebaran *malware* dapat terjadi, maka peneliti memuat sebuah topik penelitian yang berjudul **" ANALISIS COVIDLOCK RANSOMWARE MENGUNAKAN METODE HYBRID ANALISIS"**. sebuah metode *analisis statis* yang bertujuan untuk membuka, membaca, dan menemukan kode yang terdeteksi *malware* tersebut, *Reverse engineering* dalam analisis malware berguna untuk interaksi data yang memuat informasi yang ada didalam *malware*.

1.2 Perumusan masalah

Berdasarkan latar belakang yang ditemukan di atas, maka dapat dirumuskan sebuah permasalahan sebagai berikut:

a. Bagaimana cara melakukan analisis statis menggunakan metode reverse engineering pada aplikasi *Covid-19 Tracker* ?
b. Bagaimana cara melakukan analisis dinamis pada aplikasi *Covid-19 Tracker* ?
c. Bagaimana hasil dari kode tersebut ?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian adalah :

a. Membangun lingkungan penelitian berbasis linux
b. Melakukan analisis statis dan analisis dinamis terhadap sampel aplikasi android dengan tema *Covid-19*.
c. Mendapatkan sebuah kode *enkripsi*.

1.4 Batasan Masalah

Dalam menganalisa sebuah malware android pada Covid-19 ini diberikan beberapa batasan masalah, dengan tujuan agar pembahasan tidak melebar dan lebih terperinci, Adapun ruang lingkup permasalahan sebagai berikut:

a. Analisis statis menggunakan metode *reverse engineering.*

b. Analisis statis dilakukan pada area source code aplikasi dan mendapatkan code ***enkripsi.***
c. Penelitian ini hanya mengambil satu sampel aplikasi yaitu aplikasi *Covid-19 Tracker.apk*
d. Analisis dinamis dilakukan dengan menjalankan secara real *device* menggunakan Smartphone *Oppo A3s* dalam kondisi diberikan akses seluruh permission (*google play*)guna mengetahui kinerja malware maksimal.

1.5 Sistematika Penulisan

Sitematika penulisan dalam laporan skripsi ini bertujuan untuk mempermudah isi sebagaimana skripsi dapat dipahami dalam garis besar. Adapun penulisannya sebagai berikut :

Bab I Pendahuluan

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

Bab II Landasan Teori

Bab ini menjelaskan mengenai malware, dan penjelasan tentang hal-hal yang terkait dengan pemecahan masalah yang berhubungan dan digunakan untuk mendukung penulisan penelitian ini.

Bab III Metodologi Penelitian

Bab ini membahas tentang penjelasan gambaran umum penelitian, masalah yang terdapat pada objek, spesifikasi alat yang digunakan,pengumpulan data, perancangan dan simulasi serta rencana alur penelitian.

Bab IV Pembahasan

Bab ini membahas mengenai hasil proses analisa *malware* pada aplikasi *Covid-19*, uji coba pengujian, dan hasil dari penelitian.

Bab V Penutup

Bab ini menjelaskan mengenai kesimpulan dan hasil penelitian dan sebagai bahan peninjauan selanjutnya.