BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

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.

Selama penyebaran COVID-19 terus berlanjut dan menyebar ke seluruh dunia, semakin bertambah tingkat ancaman dan serangan yang mengeksploitasi dan memanfaatkan pandemi. Dilaporkan bahwa COVID-19 digunakan dalam berbagai aktivitas online dengan tujuan berbahaya atau jahat yang termasuk dalam email *scam*, *ransomware*, dan *malicious domains*[2]. Dengan jumlah kasus terkonfirmasi yang terus bertambah, maka daya tarik dalam penggunaan atau pemanfaatan *Coronavirus* untuk aktivitas online berbahaya dan jahat terus meningkat.

Smartphone, sebagai salah satu cara yang paling banyak digunakan dalam melacak dan mencari status terkini pandemi, dan bahkan menerima notifikasi sehingga menjadikan target utama dalam serangan yang memanfaatkan pandemi ini. Sebagaimana virus *Corona* terus meningkat di seluruh dunia, orang lebih cenderung menggunakan aplikasi seluler untuk mencari informasi dan pengamanan untuk menghindari infeksi, pembaharuan terkait COVID-19 dan layanan medis. Dengan demikian, pengembang jahat memanfaatkan peluang ini dalam memikat pengguna *smartphone* agar mengunduh dan instalasi aplikasi yang telah disisipkan program jahat. Beberapa laporan berita menunjukkan bahwa perkembangan dari program berbahaya yang memanfaatkan COVID-19 telah

diamati, dan ribuan dari pengguna *smartphone* yang terkena dampak dalam banyak cara[3].

Smartphone dengan sistem operasi *android* menjadi favorit utama bagi pengembang aplikasi jahat atau *malware*, hal ini dapat dilihat dengan jumlah pengguna *smartphone android* di dunia mencapai 72,92% dan hanya menyisakan 26,53% untuk sistem operasi iOS pada bulan Oktober 2020[4]. Beberapa faktor selain dari pengguna awam *smartphone* yang lengah terhadap faktor keamanan, didukung juga dengan banyaknya aplikasi *third-party* sebagai media penyebaran *malware* menyebabkan tren *malware* dengan tema *Coronavirus* terus meningkat.

Oleh karena itu perlu diketahui bagaimana penyebaran *malware* dapat terjadi, maka dalam penelitian ini aplikasi *android* dengan tema *Coronavirus* akan dilakukan penyisipan *malware* menggunakan metode *reverse engineering* baik dalam proses infeksi maupun analisis, serta teknik infeksi *malware* yang digunakan adalah *repackaging attack*. Teknik *repackaging attack*, yaitu metode yang digunakan dengan melakukan perubahan dan penyusupan pada aplikasi *android*, aplikasi dengan format APK akan dilakukan *reverse engineering* dan menambahkan *payload* atau perintah berbahaya yang disusupkan dalam aplikasi. Hasil dari aplikasi yang terinfeksi *malware* dilakukan analisis statis untuk melihat apakah *malware* telah berhasil disisipkan dengan melakukan uji deteksi menggunakan VirusTotal dan *framework* MobSF. Analisis dinamis dilakukan dengan menjalankan aplikasi yang telah disisipkan *malware*, sehingga dapat mengetahui hasil kerja dari *malware* tersebut. Maka dengan mengetahui aktivitas *malware* dapat memberikan manfaat bagi pengguna baik dalam menjaga *smartphone android* dari infeksi *malware*, maupun menambah informasi tentang keamanan dari sebuah aplikasi *android*.

1.2 Rumusan Masalah

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

a. Bagaimana teknik melakukan infeksi atau penyusupan *malware* pada aplikasi *android* dengan tema COVID-19?

b. Bagaimana teknik melakukan analisis statis pada aplikasi *android* menggunakan *tool* VirusTotal dan *framework* MobSF?
c. Bagaimana melakukan analisis dinamis pada aplikasi *android*?
d. Bagaimana hasil perbandingan analisis anatara aplikasi *android* dengan tema COVID-19 sebelum dan sesudah dilakukan infeksi malware?

1.3 Batasan Masalah

Dalam analisis infeksi *malware android* pada aplikasi COVID-19 ini diberikan beberapa batasan masalah, dengan tujuan agar pembahasan tidak melebar dan lebih terperinci. Adapun ruang lingkup permasalahan sebagai berikut :

a. Yang akan dibahas dalam penelitian ini adalah proses infeksi *malware* pada aplikasi *android* dengan tema COVID-19 dari awal hingga uji hasil *malware*.
b. Aplikasi dengan tema COVID-19 adalah aplikasi *third-party* yang tersebar di internet dan belum terinfeksi *malware*.
c. Aplikasi COVID-19 berformat APK.
d. Proses infeksi *malware* dilakukan setelah mendapatkan aplikasi dengan tema COVID-19 dengan teknik *repackaging attack*.
e. Analisis statis menggunakan *tool* VirusTotal dan *framework* MobSF yang berfokus pada *permission* yang diminta oleh aplikasi android COVID-19.
f. *Malware* yang disisipkan pada aplikasi dengan tema COVID-19 dibuat menggunakan *framework* Metasploit.
g. *Malware* berupa Payload dengan tipe reverse_tcp yang akan menjalankan exploit
h. Analisis dinamis dilakukan dengan menjalankan *malware* dalam kondisi diberikan akses seluruh *permission* guna mengetahui kinerja *malware* secara maksimal.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian adalah :

a. Membangun lingkungan peneliian berbasis Linux untuk melakukan implementasi menggunakan *framework* Metasploit dan analisis menggunakan *framework* MobSF.
b. Mengimplementasikan teknik *repackaging attack* menggunakan *tool* Apktool dan *framework* MobSF.
c. Melakukan analisis statis dan analisis dinamis terhadap sampel aplikasi *android* dengan tema COVID-19.
d. Membandingkan hasil analisis statis dari sampel aplikasi android dengan tema COVID-19 yang dilakukan infeksi atau penyusupan malware menggunakan *tool* VirusTotal dan *framework* MobSF, serta analisis dinamis dengan eksekusi sampel aplikasi *android* yang diinfeksi *malware* untuk mengetahui dampak *malware* dan informasi-informasi perbedaan yang didapatkan.

1.5 Metode Penelitian

Adapun metode penelitian yang digunakan adalah sebagai berikut :

1. Studi pustaka

   Teknik mengumpulkan data dan informasi dengan cara membaca serta mempelajari tentang analisis *malware, reverse engineering, penetration-testing* dan hal-hal yang berkaitan dengan proses infeksi dan deteksi *malware* pada platform *android* untuk digunakan sebagai referensi dalam penelitian ini. Sumber studi pustaka dapat berupa, paper, buku, jurnal, atau makalah dan referensi lainnya.
2. Membangun *environment* dengan melakukan instalasi modul serta *library* yang akan dibutuhkan oleh *tools* agar dapat dijalankan untuk melakukan analisis sampel aplikasi *android* dalam penelitian ini.
3. Implementasi

Mengimplementasikan teknik *repackaging attack* untuk menyusupkan *malware* pada aplikasi *android* dengan tema COVID-19 menggunakan *tool* Apktool dan framework Metasploit.

4. Analisis Data

   Kegiatan analisis dilakukan terhadap objek penelitian yaitu aplikasi *android* dengan tema COVID-19 menggunakan analisis statis dan analisis dinamis.

5. Penulisan laporan

   Pada tahap ini, semua temuan yang didapat selama proses analisis statis dan analisis dinamis akan dimasukkan kedalam laporan akhir.

1.6 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 infkesi maware pada android dengan aplikasi tema COVID-19 serta penjelasan tentang beberapa tools yang digunakan.

Bab III Metodologi Penelitian, bab ini membahas mengenai analisis infeksi malware, dari persiapan, pencarian dan metode yang digunakan baik dari proses infeksi malware hingga analisa hasil, dan gambaran umum mengenai alur proses seperti flowchart.

Bab IV Pembahasan, bab ini membahas mengenai hasil proses infeksi malware android pada aplikasi COVID-19, analisa yang dilakukan sebelum dan setelah proses infeksi untuk menguji hasil malware.

Bab V Penutup, bab ini menjelaskan mengenai kesimpulan dan hasil penelitian dan sebagai bahan peninjauan selanjutnya.