BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Serangan yang ditargetkan adalah APK (Application Package File) yang secara khusus menargetkan individu atau organisasi dan sering kali berisi beberapa elemen rekayasa sosial dalam upaya untuk membuatnya tampak seperti dari sumber yang sah, dan dengan demikian memikat pengguna yang ditargetkan untuk APK. Jenis serangan ini umumnya kurang signifikan jumlahnya dibandingkan dengan jenis serangan lain dalam statistik kami karena sifatnya, mereka hanya mempengaruhi satu atau sangat sekelompok kecil orang. Agar serangan yang ditargetkan berhasil, penyerang melakukan penelitian dan perencanaan sebelumnya untuk mengumpulkan informasi tentang individu atau organisasi tertentu dan, bergantung pada informasi yang dikumpulkan, konten manipulasi psikologis dipilih untuk digunakan dalam penyerangan[1].].

Malware Onion adalah software berbahaya yang tidak diinginkan, dan dirancang khusus untuk merugikan pengguna atau sistem target. Ini dapat mencakup jumlah jenis malware seperti virus, trojan, backdoors, spyware, cryptolocker dan ransomware. Namun, malware tidak terbatas pada ini, Malware bisa diklasifikasikan menurut fungsinya dan tujuan. Ini dapat dibagi menjadi empat kategori menurut jenis perilaku seperti penyebaran, infeksi, ketekunan, dan muatan. Perilaku kebanyakan adalah salah satu serangan yang paling umum metode perangkat lunak berbahaya dan merujuk mekanisme untuk menyebarkan malware ketika ada komunikasi melalui Internet atau ada hak akses didalamnya. Dan ini perilaku tentang infeksi bagaimana malware menginfeksi sistem target[2].

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 terus meningkat.[3]

Oleh karena itu perlu diketahui bagaimana penyebaran malware dapat terjadi, maka dalam penelitian ini aplikasi android 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 masalah diatas, maka dapat dirumuskan permasalahanyang akan dibahas yaitu tentang, Bagaimana menganalisis dan deteksi malware onion pada platfrom android menggunakan metode anasilis static?

1.3 Batasan Masalah

Adapun batasan masalah yang akan digunakan yaitu:

a. Peneliti ini hanya dilakukan untuk pengamatan sample malware dan dampak serangannya, bukan untuk memperbaiki sistemnya.
b. Peneliti tidak menangani lebih jauh tentang pencegahan dan penanganan terhadap malware
c. Hanya menganalisis malware yang terdapat pada platfrom android
d. Proses eksekusi malware dijalankan diplatfrom Android.
e. Analisis statis menggunakan Tools VirusTotal, dan Mobsf

f. Sistem Operasi yang di gunakan yaitu linux Remnux.

1.4 Tujuan Penelitian

Berdasarkan Adapun tujuan penelitian ini sebagai berikut:

a. Mengetahui proses analisis malware dengan menggunakan motode static analysis.
b. Mendeteksi keberadaan malware android yang ada pada kode sebuah program aplikasi
c. Memberikan informasi langkah pencegahan agar terhindar dari infeksi malware pada platfrom android.

1.5 Metode Penulisan

Metode penelitian dalam penulisan tugas akhir ini menggunakan metode static analysis yaitu penelitian yang dilakukan untuk mengetahui akibat yang ditimbulkan dari malware yang telah dieksekusi pada platform android. Tahapan penelitian ini diantaranya :

1. Perumusan Masalah,Tahapan ini memuat permasalahan yang menjadi landasan dilakukannya penelitian demi menjawab suatu masalah yang berkenaan dengan penelitian ini.

Pengumpulan Data, Tahap ini merupakan proses pengumpulan data yang berkaitan dengan objek malware yang akan diteliti.

a. Studi Literatur Tahap ini merupakan proses mempelajari dan mengumpulkan data dari sumber yang relevan dan mendukung terhadap penelitian ini.
b. Observasi Tahap ini merupakan proses pengumpulan informasi dengan mengamati fenomena yang terjadi secara real di lapangan yang terkait dengan penelitian ini. Informasi yang didapat berupa statistik tingkat serangan malware yang terjadi dan sampel malware yang dijadikan objek penelitian.

Tahap Analisis , Tahap ini melakukan analisis malware dengan menganalisis Statis. 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.

Dokumentasi, Tahap ini merupakan kumpulan data-data dan informasi hasil dari analisis yang dilakukan terhadap objek malware yang diteliti yang kemudian disusun kedalam laporan skripsi

1.6 Sistematika Penulisan

Dalam penelitian ini, penulis disajikan dalam lima bab dengan sistematika pembahasan sebagai berikut :

Bab I Pendahulan

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

Bab II Landasan Teori

Bab ini berisikan kajian dari penelitian terdahulu dan teori berupa pengertian dan definisi yang diambil dari kutipan jurnal, web, ataupun buku serta beberapa literature review yang berkaitan dengan penyusunan laporan tugas akhir ini.

Bab III Metode Penelitian

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

Bab IV Pembahasan

Bab ini menjelaskan kebutuhan sistem dan hasil analisis malware onion dengan menggunakan metode static analysis.

Bab V Penutup

Bab ini berisi tentang kesimpulan dari hasil akhir penelitian dan saran.