BAB I

PENDAHULUAN

1.1. Latar Belakang

Malware-malware baru terus bermunculan seiring dengan perkembangan teknologi, baik dari segi *platform* maupun sistem operasi, dengan memanfaatkan celah keamanan dan kelalaian pengguna. *Malware* dapat menyusup ke sistem operasi sehingga dapat merusak sistem operasi, memanfaatkan sumber daya tanpa sepengetahuan pemilik perangkat, bahkan mengumpulkan informasi pribadi untuk dibagikan ke pihak ketiga tanpa persetujuan pengguna. *Malware* mencakup *Trojan Horse, Adware, Spyware, Ransomware* dan perangkat lunak lainnya yang bertujuan merusak dan merugikan sasarannya. (Kunang, 2014).

Kebutuhan akan mobilitas membuat masyarakat di seluruh belahan dunia marak menggunakan *gadget* seperti *tablet* dan *smartphone* dengan berbagai macam sistem operasi. Sistem operasi untuk perangkat *smartphone* yang paling banyak digunakan adalah Android yakni sebanyak 76,82% dari total *market share* (StatCounter, 2018).

Malware pada platform Android menyusup lewat layanan distribusi aplikasi, baik resmi (*Google Play Store*) maupun milik pihak ketiga, dengan menyamar menjadi aplikasi sah seperti pemutar video, permainan dan utilitas sistem (McAfee Inc., 2018). Beberapa jenis *malware* yang banyak beredar di layanan distribusi aplikasi Android diantaranya adalah *Adware*, *Banking Trojan* dan *Cryptocurrency-mining malware*. *Adware* merupakan salah satu *malware* yang

paling banyak menyerang pengguna *Google Play Store* dan terus mengalami peningkatan hingga 36% sejak tahun 2016. Selain itu, serangan *Banking Trojan* juga meningkat hingga 12% sedangkan *Crypto-Mining* terjadi peningkatan sebesar 5% bersamaan dengan melambungnya harga *Bitcoin* pada saat itu (McAfee Inc., 2018).

Praktisi keamanan teknologi informasi perlu melakukan suatu proses investigasi forensik analisis *malware* untuk mengidentifikasi, mengamankan, mengamati, dan menyajikan fakta dan opini dari informasi *malware*. Beberapa metode dan teknik dalam melakukan analisis *malware* yaitu analisa secara statis (*Static Analysis*) dan analisa secara dinamis (*Dynamic Analysis*), dimana keduanya memiliki kelemahan dan kelebihan masing-masing (Gadhiya & Bhavsar, 2013). *Hybrid Analysis* merupakan gabungan dari *Static* dan *Dynamic Analysis* yang efektif untuk mendeteksi infeksi *malware* secara akurat (Zalavadiya & Sharma, 2017).

Berdasarkan latar belakang diatas maka dilakukan sebuah penelitian dengan judul "Analisis Infeksi *Malware* pada Perangkat Android dengan *Hybrid Analysis*". Penelitian ini mencoba menganalisis *malware Judy*, yaitu *adware* yang banyak beredar di *Google Play Store*, dan *Marcher*, yaitu salah satu *banking trojan* yang mengambil informasi *e-banking* nasabah, dengan menggunakan metode *hybrid analysis*. Penelitian ini diharapkan dapat memberikan gambaran cara kerja kedua *malware* tersebut dan dampak yang diakibatkan terhadap sistem Android serta langkah pencegahan agar terhindar dari serangan *malware*.

1.2. Rumusan Masalah

Adapun rumusan masalah dari latar belakang tersebut yaitu:

1. Bagaimana proses analisis *malware* dengan menggunakan metode *hybrid analysis*?
2. Bagaimana karakteristik dari sampel *malware* Judy dan Marcher?
3. Bagaimana langkah pencegahan agar terhindar dari infeksi *malware* pada perangkat Android?

1.3. Batasan Masalah

Adapun batasan masalah yang digunakan yaitu:

1. Penelitian ini hanya dilakukan untuk pengamatan terhadap sampel *malware* dan dampak serangannya, bukan untuk memperbaiki sistemnya.
2. Penelitian dilakukan pada dua sampel *malware* yaitu Judy dan Marcher.
3. Tidak terpasang anti-*malware* pada platform Android.
4. Proses eksekusi *malware* dilakukan pada Android Emulator versi 5.1 (Lollipop).

1.4. Tujuan Penelitian

Adapun tujuan dari penelitian ini yaitu:

1. Mengetahui proses analisis *malware* dengan menggunakan metode *hybrid analysis*.
2. Mengetahui karakteristik dari sampel *malware* Judy dan Marcher.
3. Memberikan informasi langkah pencegahan agar terhindar dari infeksi *malware* pada perangkat Android.

1.5. Manfaat Penelitian

Manfaat yang didapat dari hasil penelitian ini diantaranya:

1. Menambah wawasan tentang karakteristik *malware* pada platform Android, khususnya *malware* Judy dan Marcher.
2. Meningkatkan tingkat pendeteksian *malware* serupa pada platform Android dengan melihat karakteristiknya.
3. Menjadi rujukan untuk melakukan pengembangan penelitian lebih lanjut dan dapat menjadi dasar untuk pembuatan anti-*malware* untuk jenis *malware* serupa.

1.6. Metodologi Penelitian

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

1.6.1 Perumusan Masalah

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

1.6.2 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.

1.6.3 Tahap Analisis

Tahap ini melakukan analisis Hybrid dengan menggabungkan analisis Statis dan Dinamis. Analisis Hybrid dimulai dengan melihat kemungkinan adanya *malicious code* yang ditanam pada objek yang diteliti, menjalankan objek *malware* yang diteliti guna melihat efek yang ditimbulkan oleh *malware* terhadap sistem.

1.6.4 Dokumentasi

Tahap ini merupakan kumpulan data-data dan informasi hasil dari analisis yang dilakukan terhadap objek *malware* yang diteliti yang kemudian disusun kedalam laporan tugas akhir.

1.7. Sistematika Penulisan

Penulisan dalam laporan tugas akhir ini memakai sistematika pembahasan sebagai berikut:

BAB I PENDAHULUAN

Bab ini memuat latar belakang, rumusan masalah, batasan masalah, maksud dan tujuan, metodologi 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 METODOLOGI PENELITIAN

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

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan kebutuhan sistem dan hasil analisis *malware* sample dengan menggunakan metode *hybrid analysis*.

BAB V KESIMPULAN DAN SARAN

Bab terakhir memuat kesimpulan dan saran keseluruhan dari bab sebelumnya sebagai hasil yang diperoleh yang diharapkan dapat bermanfaat dalam penelitian selanjutnya.