BAB I

PENDAHULUAN

A. LATAR BELAKANG

Malware berasal dari kata *malicious* dan *software* yang merupakan perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer. Perangkat lunak yang dianggap sebagai perangkat perusak berdasarkan maksud yang terlihat dari pencipta dan bukan berdasarkan ciri-ciri tertentu, mencakup *Virus Computer, Trojan Horse,* perangkat pengintai (*spyware)*, perangkat iklan (*adware*) yang tidak jujur, perangkat jahat (*crimeware*) dan perangkat lunak lainnya yang berniat jahat dan tidak diinginkan (G.Kaur, 2012). *Malware* dibuat dengan sengaja yang disisipkan pada sebuah sistem *android* untuk mencuri data informasi dan bahkan dapat merusak sebuah sistem *android*. *Malware* sangat berbahaya, karena sangat sulit untuk dideteksi oleh sistem yang sedang bekerja, sehingga hal yang sangat mungkin dilakukan adalah menganalisa terkait aktivitas dari *malware* tersebut. *Trojan.Android.GMobi* merupakan salah satu jenis *malware* yang berbahaya karena kemampuannya yang mampu mencuri data pengguna dan perangkat dan mengirimnya kembali ke server C & C. *Gmobi* mengumpulkan email pengguna, info perangkat, status ketersediaan roaming, GPS atau koordinat jaringan seluler, serta apakah aplikasi Google Play yang dipasang di perangkat. (*securityaffairs*)

Perkembangan *malware* yang semakin variatif menimbulkan dampak yang cukup berbahaya pada penggunaan *software*, untuk itu analisa *malware* diperlukan untuk mempelajari bagaimana cara kerja *malware* sebagai bentuk perlawanan pada jenis *malware* yang semakin berbahaya. Beberapa kejahatan yang diantaranya dengan memanfaatkan celah pada aplikasi yang disisipi *malware* jenis *spyware, adware* yang selanjutnya dimanfaatkan untuk mendapatkan keuntungan pribadi atau kelompok.

Konsep penelitian yang digunakan pada penelitian ini menggunakan teknik *reverse engineering* seperti yang dilakukan oleh kunang (2014) dengan membongkar struktur file .apk dan menganalisa *source code* dari aplikasi untuk mengetahui kode *malware* jahat apa yang terdapat pada aplikasi. Selain itu peneliti juga menggunakan teknik analisa dinamis seperti yang dilakukan oleh Nugroho dan Prayudi (2015), mereka meneliti bagaimana cara kerja *malware Biscuit* yang dilakukan dengan proses *reverse engineering*. Ditemukan bagaimana mekanisme kerja *malware*, yaitu dengan mengirimkan *auto request* pada koneksi IP tertentu dan mendeteksi perintah-perintah tertentu pada program yang tidak seharusnya ada. Beberapa fakta tentang *malware* ini menjadikannya topik menarik untuk diangkat menjadi tema sebuah penelitian karena penanganan tindak kejahatan yang melibatkan teknologi perangkat *smartphone* masih sangat awam untuk saat ini.

Hasil implementasi ini adalah melakukan uji analisa *malware* dengan konsep *reverse engineering* yang melibatkan teknik analisa statis dan dinamis pada aplikasi yang terinfeksi *malware* seperti yang dilakukan oleh Nugroho dan

Prayudi (2014) pada *malware Biscuit* dengan tipe *Trojan* untuk perangkat PC. Teknik ini melakukan analisa *malware* secara statis dan dinamis dimana akan dianalisa bukti kejahatan *malware* dengan menganalisa *source code malware* dan mempelajari aktifitas *malware* pada lingkungan *virtual* yang dimaksudkan untuk mengetahui bagaimana *malware* bekerja, pengaruhnya pada sistem dan data apa saja yang berhasil dicuri. Teknik ini diharapkan dapat menjawab bagaimana mekanisme kerja *malware* serta mengetahui dampak apa saja yang timbul dari kerusakan *malware* pada aplikasi *android*.

B. RUMUSAN MASALAH

Dari latar belakang dan permasalahan di atas, dapat dirumuskan beberapa hal yang akan dilakukan dalam penelitian ini:

1. Bagaimana cara menganalisis *malware* pada aplikasi *android* ?
2. Bagaimana cara mendapatkan artefak digital pada aplikasi yang terinfeksi *malware* untuk dijadikan bukti kejahatan *cybercrime*?
3. Bagaimana memahami alur cara kerja *malware* menggunakan *tools malware analysis?*

C. BATASAN MASALAH

Dari rumusan masalah tersebut dibuat batasan-batasan masalah yang akan dilakukan, batasan-batasan itu antara lain:

1. *Malware* yang digunakan adalah jenis *malware Trojan.Android.GMobi.*
2. Mengidentifikasi artefak digital pada *malware Trojan.Android.GMobi* sebagai barang bukti dengan menggunakan *tools malware analysis*.

3. Pembuktian alur cara kerja *malware* berupa analisis statis dan dinamis sehingga dapat digunakan untuk menelusuri jejak kode *malware* jahat yang disisipkan pada aplikasi yang terinfeksi.
4. Pengujian sampel dilakukan pada perangkat *android* dengan *OS lollipop* dan *emulator* dengan OS *lollipop*.

.