BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan pesatnya penetrasi jaringan *global* dan kemajuan *mobile* internet di Indonesia, semakin menambah kerentanan keamanan informasi sebuah organisasi dari ancaman siber (Islami, 2017). *Malware* didefinisikan sebagai semua perangkat lunak jahat, program komputer jahat, atau perangkat lunak jahat, seperti virus (komputer), *trojans*, *spyware, dan worm.*

Dampak yang terjadi apabila PC terinfeksi *malware* yaitu PC akan berjalan semakin lambat mesikpun menggunakan spesifikasi PC dengan *processor* bagus dan RAM dengan jumlah banyak, akan tetapi jika PC terinfeksi *malware* akan berjalan lambat dan pada performa *network* tidak stabil (Elanda, 2015).

Menurut hasil penelitian dari (Technologies, 2016) telah menemukan varian baru yang tersembunyi dari *malware HummingBad* di lebih dari 20 aplikasi di *Google Play*. *HummingBad* muncul sebagai *malware* yang sangat canggih dan berkembang dengan baik, yang menggunakan taktik *rootkit* dan *chain-attack* untuk mendapatkan kontrol penuh atas perangkat yang terinfeksi. Ponsel yang terinfeksi menampilkan iklan ilegal dan memasang aplikasi palsu pada saat setelah ponsel dihidupkan layarnya, dihidupkan ulang atau dimatikan ponselnya, dan melakukan perubahan dalam konektivitas internet. Hal tersebut dilakukan dengan menggunakan perangkat yang terinfeksi untuk meniru klik pada tombol instal, beli, dan terima. Indonesia menempati urutan keempat dalam hal infeksi *malware HummingBad* terhadap ponsel dengan sistem operasi *Android* dengan jumlah sebanyak 489.336 perangkat yang terinfeksi.

Penelitian berjudul "*Bio-inspired for Features Optimization and Malware Detection*" yang dilakukan oleh (Bacci, et al., 2018) menyebutkan bahwa metode *Particle Sward Optimization* (PSO) berbasis *AdaBoost* memberikan performa yang baik untuk memprediksi infeksi *malware HummingBad* dengan persentase akurasi sebesar 95,6%, walaupun tingkat akurasinya cukup besar, tetapi penelitian tersebut dilakukan berdasarkan perspektif data mining classification and prediction yang membangun fungsi menggambarkan dan membedakan kelas atau konsep presiksi, sehingga perilaku ataupun aktivitas dari *malware* tersebut dapat dipantau secara langsung dan pola serangannya bisa diidentifikasi. (Razak, Anuar, & Othman, 2017).

Penelitian lain berjudul "*Impact of Code Obfuscation on Android Malware Detection based on Static and Dynamic Analysis*" yang dilakukan (Bacci, et al., 2018) menerangkan bahwasannya metode deteksi *malware* berbasis analisis statis pada dasarnya tidak efektif pada malware yang dikaburkan dibandingkan dengan metode dinamis, walaupun demikian, metode analisis dinamis sangat efektif apabila digunakan untuk melakukan analisis perilaku atau aktivitas dari berbagai jenis *malware*, termasuk *malware HummingBad*.

Analisis *malware* dengan menggunakan *reverse engineering* akan mendapatkan *source code* dari *malware* tersebut (Triantoro, Widiyasono, & Gunawan, 2021). *Source code* ini dapat mempelajari cara kerja *malware*, karakteristiknya, teknik infeksi yang digunakan dan lain-lain. Keuntungan melakukan *reverse engineering* pada analisis *malware* adalah *malware* tidak dijalankan (*execute*) sehingga meminimalisir kemungkinan komputer terinfeksi *malware* tersebut. Implementasi *Reverse Engineering* dalam analisis *malware* menjadi masalah tersendiri.

Berdasarkan permasalahan-permasalahan dan latar belakang yang telah dipaparkan di atas, maka diusulkan suatu penelitian yang berjudul **Analisis *Malware "HummingBad"* pada Perangkat *Smartphone* Menggunakan Metode Hybrid**".

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka rumusan masalah yaitu bagaimana melakukan identifikasi serangan drive-by-download Malware HummingBad pada perangkat Android menggunakan metode hybrid.

1.3 Batasan Masalah

Adapun batasan masalah dari penelitian yaitu:

a. *Malware* yang diteliti yang terfokus pada *malware HummingBad* yang menyerang perangkat android.
b. Bantuan yang dilakukan untuk melakukan analisis dinamis adalah Phoenix OS.
c. Penelitian ini menggunakan mesin virtual dan emulator android sebagai eksekutor *malware HummingBad.*

1.4 Tujuan Penelitian

Berdasakan rumusan masalah maka tujuan penelitian yaitu melakukan identifikasi serangan drive-by-download Malware HummingBad pada perangkat Android menggunakan metode hybrid.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini yaitu agar hasil dari penelitian dapat dimanfaatkan dan digunakan oleh sebagai berikut:

a. Bagi Ilmu Pengetahuan

1. Menambah wawasan tentang cara kerja malware khususnya pada *malware HummingBad*.
2. Mengetahui perilaku dan aktivitas serangan malware HummingBad.

b. Bagi Masyarakat Umum

1. Mengetahui tanda-tanda sistem yang terserang oleh *malware HummingBad*
2. Mengetahui cara pencegahan *malware HummingBad.*

1.6 Metodologi

Metodologi penelitian menjelaskan mengenai jenis penelitian eksperimental. Metode eksperimen ini meliputi perumusan masalah, data *collection, System Preparation, Study Case Malware HummingBad, Analisis Dinamis, Reverse Engineering,* dan Documentation & Reporting.

a. Perumusan Masalah

Langkah awal untuk memulai penelitian adalah proses merumuskan masalah yang akan diteliti. Tahap ini merupakan tahap yang paling penting dalam penelitian karena semua jalannya penelitian akan dituntun oleh perumusan masalah.

b. Data Collection

Data *Collection* merupakan tahap kedua dari penelitian ini. Permasalahan yang sebelumnya dirumuskan, kemudian dicari solusi pemecahan masalahnya.

c. System Preparation

Sistem ini harus disiapkan terlebih dahulu agar nantinya dapat dilakukan analisis terhadap *malware HummingBad*.

d. Study Case Malware HummingBad

Tahap ini dilakukan proses penyelidikan atau pemeriksaan secara mendalam, terperinci, dan detail pada *Malware Hummingbad*.

e. Analisis Dinamis

Tahapan ini dilakukan Analisa dinamis pada malware hummingbad sehingga dapat diketahui bagaimana malware hummingbad berjalan pada system.

f. *Reverse Engineering*

Reverse Engineering dilakukan pada tahap ini untuk menegmbalikan malware menjadi kode program sehingga dapat dilakukan analisis malware yang lebih baik.

g. Documentation & Reporting

Tahapan terakhir adalah *Documentation & Reporting* dimana pada tahap ini proses analisis yang telah dilakukan kemudian didokumentasikan untuk disimpan dan diterapkan pada laporan penelitian.

1.7 Sistematika Penulisan

Sistematika penulisan untuk memahami lebih jelas isi laporan, materi-materi yang tertera pada laporan skripsi ini dikelompokkan menjadi beberapa sub bab dengan sistematika penyampaian sebagai berikut:

BAB I PENDAHULUAN

Berisi tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

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

BAB III METODOLOGI PENELITIAN

Bab ini berisikan metodologi penelitian yang memberikan gambaran dan alur dari penelitian yang dilakukan, menjelaskan dari metodologi penelitian, kajian teori, analisis dinamis.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil analisa *malware* dan pembahasan yang diusulkan dan yang diimplementasikan, pembahasan secara detail mengenai analisis *malware HummingBad* dengan melakukan analisis dinamis.

BAB V SIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang berkaitan dengan analisa berdasarkan yang telah diuraikan pada bab-bab sebelumnya.