BAB I
PENDAHULUAN

1.1. Latar Belakang

Pada era modern ini hampir semua orang menggunakan *smartphone* karena kemudahan akses informasi, banyaknya aplikasi, dan koneksi internet yang cepat, sehingga menjadikannya alat yang sangat diperlukan dalam kehidupan sehari-hari[1]. Di Indonesia perangkat *smartphone* terutama yang menggunakan sistem operasi Android, mendominasi pasar dengan *market share* 88,46% pada tahun 2024, jauh melampaui iOS yang hanya memiliki 11,4%[2]. *Smartphone* telah membantu banyak orang berkomunikasi, bekerja, dan mengakses berbagai layanan dengan mudah. Namun, seiring dengan meningkatnya penggunaan *smartphone*, terdapat risiko keamanan siber yang signifikan karena perangkat ini menyimpan banyak data pribadi dan informasi sensitif yang rentan terhadap serangan digital[3].

Berdasarkan survei nasional yang melibatkan 1.700 responden dari 34 provinsi di Indonesia, diperkuat dengan *Focus Group Discussion* (FGD) bersama 20 responden terpilih, lebih dari 98,3% responden pernah menerima pesan penipuan digital. Salah satu modus pesan penipuan yang banyak mereka terima adalah pengiriman tautan yang berisi *malware* atau *virus* (65,2%). Salah satu jenis penipuan yang banyak memakan korban yaitu pengiriman tautan yang mengandung *malware* (33,8%), situs web dan aplikasi palsu (27,4%)[4]. Media komunikasi yang digunakan dalam penipuan paling banyak dilakukan melalui SMS atau Telepon, media sosial, dan aplikasi chat. Serangan *malware* merupakan bentuk ancaman yang menggunakan berbagai metode untuk menyusup ke dalam perangkat pengguna dengan maksud mencuri data pribadi, mengganggu kinerja perangkat, atau bahkan mengakses sistem secara ilegal[5]. Sejak akhir tahun 2022 hingga 2023, masyarakat dihebohkan dengan penyebaran luas aplikasi Android yang dimodifikasi untuk melakukan penipuan, termasuk serangan *phishing* menggunakan *malware* yang viral melalui pesan singkat WhatsApp[6].

WhatsApp telah menjadi platform komunikasi utama bagi mayoritas pengguna internet di Indonesia. Data menunjukkan bahwa pada Januari 2024,

sebanyak 90,9% dari mayoritas pengguna internet berusia 16 hingga 64 tahun memilih WhatsApp sebagai platform komunikasi utama[7]. Hal ini menunjukkan bahwa WhatsApp memiliki pengaruh yang besar dalam kehidupan sehari-hari masyarakat Indonesia, Sebagai platform komunikasi yang banyak digunakan, WhatsApp sering menjadi target bagi para pelaku kejahatan dunia maya untuk menyebarkan *malware* dan melakukan serangan siber lainnya[6]. Situasi ini menimbulkan tantangan besar dalam melindungi pengguna *smartphone* dari ancaman keamanan siber yang semakin kompleks, terutama terkait dengan analisis dan deteksi serangan *malware*.

Penelitian ini bertujuan untuk menghadapi tantangan-tantangan yang timbul dalam konteks ini, dengan memanfaatkan metode *hybrid analysis*. *Hybrid analysis* adalah metode yang menggabungkan analisis statis dan dinamis untuk mendapatkan gambaran lengkap tentang perangkat lunak atau *malware*[8]. Analisis statis mengidentifikasi struktur dan potensi kerentanan tanpa menjalankan kode, sementara analisis dinamis mengamati perilaku perangkat lunak saat dijalankan di lingkungan terkendali. Kombinasi ini memungkinkan deteksi ancaman yang lebih efektif dan memberikan informasi yang lebih mendalam untuk mitigasi ancaman siber[9].

Berdasarkan permasalahan diatas, penelitian ini menganalisis malware dalam file undangan pernikahan, yaitu malware yang banyak beredar melalui pesan WhatsApp. Penelitian ini diharapkan dapat memberikan gambaran cara kerja malware, dampak yang diakibatkannya terhadap sistem Android dan informasi apa saja yang bisa didapatkan saat malware tersebut terpasang di perangkat android dengan memanfaatkan data dan temuan langsung dari skenario serangan yang telah disusun. Oleh karena itu, disusun penelitian pada skripsi yang berjudul "Analisis *Malware Trojan* Dalam File Undangan Pernikahan.Apk Pada *Smartphone* Android Dengan Metode *Hybrid Analysis*".

1.2. Rumusan Masalah

Peningkatan jumlah pengguna *smartphone* Android diiringi tingginya insiden penipuan digital di Indonesia, terutama melalui aplikasi komunikasi seperti WhatsApp. Salah satu serangan yang sering terjadi dan menimbulkan kerugian besar bagi pengguna *smartphone* android adalah melalui *malware* yang menyamar sebagai aplikasi undangan pernikahan. Serangan ini dilakukan melalui pengiriman file dengan format APK melalui pesan WhatsApp yang ketika diklik oleh pengguna, akan menginstal malware di perangkat. Maka dari itu, penelitian ini dilakukan untuk menganalisis serangan *malware* undangan pernikahan pada perangkat Android menggunakan metode *hybrid analysis*. Analisis ini bertujuan untuk memahami secara mendalam karakteristik dan perilaku dari *malware* undangan pernikahan tersebut, aktivitas yang dilakukan setelah instalasi, dan jenis data sensitif yang dapat diakses atau dicuri oleh penyerang.

1.3. Pertanyaan Penelitian

Berdasarkan rumusan masalah diatas, maka pertanyaan peneliti dalam melakukan penelitian ini yaitu:

1. Bagaimana perilaku *malware* undangan pernikahan setelah terpasang pada perangkat Android?
2. Data apa saja yang dapat diakses dan dikumpulkan oleh penyerang setelah *malware* undangan pernikahan berhasil terpasang, serta bagaimana data tersebut dapat dieksploitasi?

1.4 Batasan Masalah

Penelitian ini memiliki batasan untuk memfokuskan pada aspek-aspek tertentu, yaitu:

1. Penelitian ini hanya menganalisis *malware* undangan pernikahan
2. Menggunakan *tools* APKTool untuk decompile dan modifikasi file apk.
3. Menggunakan *tools* JADX untuk analisis source code.
4. Menggunakan *smartphone* dengan versi android 11 untuk pengujian

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah, dapat dijabarkan tujuan penelitian sebagai berikut:

1. Mengetahui perilaku *malware* undangan pernikahan setelah terpasang pada perangkat Android
2. Mengetahui data apa saja yang dapat diakses dan dikumpulkan oleh penyerang setelah *malware* undangan pernikahan berhasil terpasang, serta bagaimana data tersebut dapat dieksploitasi.

1.6 Manfaat Penelitian

Berdasarkan rumusan masalah, batasan masalah dan tujuan penelitian yang telah diuraikan diatas, maka dapat diketahui manfaat dari penelitian ini adalah:

1. Dapat mengetahui kemampuan *malware* undangan pernikahan setelah terpasang pada perangkat Android dan mengidentifikasi serangkaian tindakan yang dilakukan *malware* tersebut.
2. Dapat mengetahui informasi spesifik yang berhasil diakses dan dikumpulkan oleh penyerang setelah *malware* undangan pernikahan berhasil terpasang, serta bagaimana data tersebut dapat dieksploitasi.
3. Dapat menjadi referensi bagi penelitian selanjutnya.