BAB I
PENDAHULUAN

1.1. Latar Belakang

Penggunaan *Smartphone android* sekarang ini meningkat secara signifikan di seluruh dunia. Menurut survei Databoks pengguna *smartphone* diprediksi akan mencapai 89% populasi di tahun 2025, dan akan terus meningkat seiring berjalannya waktu. Ini dikarenakan ponsel pintar semakin terjangkau, sehingga meningkatkan minat dari para penggunanya juga [1]. Karena jumlah yang banyak ini, muncul kasus-kasus tentang keamanan privasi dan informasi, sebab kurangnya kesadaran diri mengenai *malware, spam, spoofing/phising*, hingga mengunggah tentang hal yang bersifat pribadi seperti nomor telepon, dan alamat rumah [2].

Dalam era teknologi saat ini, internet telah menjadi bagian yang umum dalam kehidupan sehari-hari, membantu manusia dalam berbagai kegiatan dan aktivitas. Kemudahan yang ditawarkan oleh internet telah menghubungkan berbagai perangkat seperti komputer dan *smartphone*, memungkinkan mereka saling berinteraksi melalui jaringan ini. Manfaat internet sangat besar bagi kehidupan manusia, namun di balik segala keuntungannya, internet juga dapat membawa bencana bagi para penggunanya, khususnya melalui penyebaran *malware*. *Malware* adalah bentuk kejahatan yang sering muncul dalam jaringan komputer. Salah satunya adalah "*backdoor*", yang merupakan jenis virus *Trojan Horse*. *Backdoor* ini bisa berkembang di dalam perangkat yang terinfeksi dan memungkinkan penyerang untuk masuk ke sistem tanpa sepengetahuan pemiliknya. Biasanya, *malware* yang diinstal di dalam *backdoor* dikenal sebagai "*Remote Access Trojan*" (RAT). Jenis *malware* ini menjadi ancaman serius karena dapat mengambil alih kendali perangkat pengguna dan bahkan mencuri data pribadi atau informasi sensitif lainnya. Keberadaan *backdoor* memberi kesempatan kepada penyerang untuk secara

diam-diam mencuri informasi, merusak sistem, atau melakukan aksi jahat lainnya tanpa sepengetahuan pemilik perangkat [3].

Salah satu bentuk kejahatan siber yang semakin sering terjadi adalah penipuan melalui file berekstensi *Android Package Kit* (APK). APK merupakan format aplikasi yang digunakan pada perangkat berbasis *Android*. Penipuan ini biasanya dilakukan melalui *chat* atau obrolan di platform media sosial seperti *WhatsApp*, dengan berbagai modus yang sangat beragam, seperti modus undangan pernikahan, cek resi paket, tagihan BPJS Kesehatan, surat tilang kepolisian, dan modus lainnya. Kronologisnya, penipuan ini melibatkan pengiriman file APK yang menjanjikan hal-hal menarik atau penting kepada calon korban. Begitu calon korban mengunduh dan menginstal aplikasi tersebut, pelaku akan mendapatkan akses ilegal ke perangkat korban. Dengan akses ini, pelaku dapat dengan mudah menyadap data penting, seperti kode *One Time Password* (OTP), pin, dan *password* dari layanan perbankan mobile atau dompet digital *(e-wallet)* milik korban. Dampaknya sangat merugikan, karena begitu pelaku mendapatkan data sensitif korban, mereka akan menyalahgunakannya untuk mencuri seluruh saldo yang ada di akun perbankan mobile atau *e-wallet* korban. Hal ini dapat menyebabkan kerugian finansial yang besar bagi korban dan mengganggu keamanan serta privasi pribadi mereka [4].

Dalam penelitian ini, akan dilakukan analisis *malware* yang disisipkan pada sebuah aplikasi. Aplikasi yang digunakan pada penelitian ini adalah aplikasi Whatsapp GB. Aplikasi ini adalah hasil modifikasi dari pihak ketiga. Aplikasi inilah yang akan digunakan untuk melakukan eksploitasi pada *smartphone android* menggunakan alat bernama AhMyth. AhMyth adalah sebuah alat Administrasi Jarak Jauh atau *Remote Administration Tool* (RAT) sumber terbuka yang kuat, dirancang untuk mengakses data informatif dari perangkat *android*. AhMyth ini juga yang digunakan sebagai *malware* untuk melakukan pengujian ekslpoitasi ini.

Metode yang digunakan dalam penelitian ini adalah *Reverse Engineering*, adalah proses untuk memahami dan mengungkap cara kerja sebuah aplikasi dengan menganalisis cara operasinya, serta mempelajari struktur dan fungsinya [5]. Selanjutnya, hasil penelitian dianalisis dengan mengidentifikasi perbedaan dalam kode program, baik secara manual maupun otomatis. Analisis otomatis dilakukan menggunakan MobSF (Mobile Security Framework) dengan pendekatan analisis statis.

1.2. Rumusan Masalah

Keamanan sistem operasi pada smartphone menjadi aspek vital karena memungkinkan serangan terhadap perangkat pengguna kapan saja dan di mana saja. Salah satu ancaman utama adalah malware yang disematkan melalui aplikasi Android, yang dapat membuka akses tidak sah ke perangkat target. Dalam penelitian ini, analisis dilakukan menggunakan teknik reverse engineering untuk mengkaji backdoor yang disisipkan pada perangkat Android melalui aplikasi yang telah dimodifikasi. Selanjutnya, analisis ini akan mengevaluasi kemampuan malware dalam mengeksploitasi data dan fungsi perangkat target, serta membandingkan hasil pemindaian otomatis menggunakan Mobile Security Framework (MobSF) dengan analisis manual menggunakan JADX.

1.3. Pertanyaan Penelitian

Berdasarkan rumusan masalah di atas, maka pertanyaan pada penelitian ini adalah:

1. Bagaimana kemampuan *malware AhMyth* setelah terpasang pada sistem operasi Android?
2. Bagaimana perubahan kode pada aplikasi sebelum dan sesudah disusupi *malware AhMyth*?

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengetahui kemampuan *Malware AhMyth* setelah terpasang pada perangkat Android.
2. Menganalisa perubahan kode pada aplikasi sebelum dan sesudah disusupi *malware AhMyth*.

1.5. Batasan Masalah

Batasan Masalah Penelitian ini adalah:

1. Pengujian dilakukan dengan menggunakan AhMyth.
2. Backdoor yang digunakan adalah AhMyth.
3. Menggunakan aplikasi WhatsappGB sebagai alat untuk pengujian.
4. Menggunakan JADX untuk membandingkan perubahan sebelum dan sesudah disisipkan malware.
5. Menggunakan MobSF untuk melakukan scanning secara otomatis.
6. Menggunakan android versi 13 selama pengujian.
7. Menggunakan satu jaringan yang sama.
8. Menggunakan Whatsapp GB sebagai aplikasi perantara untuk eksploitasi.
9. Menggunakan port default dari AhMyth 42474.

1.6. Manfaat Penelitian

Manfaat Penelitian ini adalah:

1. Memahami kemampuan malware AhMyth setelah diinstal pada perangkat Android serta mengetahui berbagai aksi yang bisa dilakukan oleh malware tersebut.
2. Mengetahui perubahan kode dalam aplikasi sebelum dan sesudah malware AhMyth disisipkan.
3. Dapat menjadi referensi bagi penelitian selanjutnya.