BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Indonesia merupakan salah satu Negara yang menjadi pengguna *smartphone* terbanyak di Dunia. Hal ini sebagaimana dilaporkan oleh data Newzoo yang dikutip dari situs dataindonesia.id, tercatat pengguna *smartphone* di Indonesia pada tahun 2023 mencapai 192,15 juta pengguna[1]. Penggunaan *smartphone* ini bertujuan untuk memudahkan masyarakat dalam berkomunikasi satu sama lain baik itu berkirim pesan dan melakukan panggilan suara. Bahkan dapat pula menghubungkan satu orang dengan lainnya menggunakan media sosial. Dikutip dari dataindonesia.id, menurut We Are Social menunjukkan jumlah pengguna aktif media sosial di Indonesia tercatat sebanyak 167 juta orang pada bulan Januari 2023 jumlah tersebut setara dengan 60,4% jumlah populasi dalam Negeri[2]. Meskipun memiliki tujuan utama sebagai alat komunikasi, namun pada perkembangannya *smartphone* dapat digunakan untuk mencari informasi-informasi terkini dari mancanegara serta sebagai alat transaksi pembayaran online. Sejalan dengan adanya kecanggihan fitur pada smartphone, namun tak jarang juga ditemui beberapa masalah yang muncul pada sistem operasi[3]. Permasalahan sistem operasi yang dimaksud merupakan adanya serangan *malware* sehingga memberikan peluang adanya kegiatan *cybercrime*, *phishing*, pencurian data sensitif atau pengaksesan data pribadi dan lain sebagainya. Munculnya beberapa kejahatan tersebut tentunya dipengaruhi oleh adanya beberapa faktor internal dan eksternal. Hal ini disampaikan oleh Efvy Zam dalam bukunya yang berjudul "Phising Teknik Mudah Penyadapan Password dan Pencegahannya" yang menyebutkan bahwa kejahatan phising dapat terjadi karena minimnya tingkat pendidikan dan pengetahuan masyarakat terhadap teknologi keamanan dan sikap lalai serta kurang telitinya masyarakat dalam membaca saat adanya pesan masuk[4].

Tercatat berdasarkan laporan perusahaan keamanan siber Kaspersky Labs, dari bulan Januari hingga September 2019 perusahaan telah memblokir 632.451 upaya serangan *mobile* malware ke *smartphone* di Indonesia. Hal ini sekaligus menjadikan Indonesia sebagai Negara dengan jumlah ancaman android terdeteksi terbanyak se-Asia Tenggara[5]. Berdasarkan data tersebut maka dapat dilihat juga bahwa serangan *malware* terhadap *smartphone* sendiri mengalami peningkatan dari tahun ke tahun. Pada tahun 2023 terjadi peningkatan hingga 50% serangan siber pada smartphone di Indonesia dibandingkan dengan tahun 2022, yang mana pada tahun 2023 terdapat 33.790.599 serangan sedangkan pada tahun 2022 hanya terdapat 22.255.956 serangan. Mayoritas ancaman siber ini ialah ancaman malware yang mencakup 40,8% dari seluruh ancaman yang terdeteksi[6]. Salah satu contoh kasus serangan *malware* yang sering terjadi di Indonesia adalah adanya pengiriman *malware* berupa aplikasi kepada pengguna *smartphone* yang akan menjadi korban melalui media sosial baik itu *whatsapp* ataupun *direct message*. Biasanya penyerang akan berpura-pura menjadi oknum kurir pengiriman yang akan memberikan informasi kedatangan paket. Namun, untuk dapat menerima paket tersebut, calon korban diwajibkan membaca terlebih dahulu serta mengonfirmasi informasi dalam file terlampir. Pada saat calon korban mengunduh dan membuka lampiran, maka *malware* secara otomatis akan terunduh juga ke smartphone korban. Penyerang menggunakan sebuah file aplikasi yang sudah disusupi *malware* dan *script remote administrative trojan* yang dapat dimodifikasi lagi dengan *metasploit* sehingga penyerang bisa mendapatkan seluruh data penting korban beserta aset yang ada di dalam perangkat android korban. Dalam contoh kasus tersebut, peretas menggunakan RAT dikarenakan membuka peluang bagi peretas untuk mendapatkan seluruh kendali atas smartphone target yang telah terpasang aplikasi modifikasi tersebut.

Dikutip dari merdeka.com, menurut Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri, pada bulan Desember tahun 2022 terdapat sebanyak 483 orang yang telah menjadi korban kejahatan *phising* aplikasi

tersebut dengan kerugian yang ditaksir mencapai 12 miliar rupiah[7]. Serangan tersebut mengakibatkan banyaknya data-data penting hilang tanpa adanya penyebab yang pasti, bahkan penyerang dapat mengambil tabungan korban melalui aplikasi *mobile banking* yang terinstal di perangkatnya. Serangan *malware* tidak hanya mengakibatkan adanya kejahatan *phising* yang merugikan pengguna *smartphone*, namun juga kejahatan lain seperti *cybercrime* atau kejahatan siber. Menurut laporan data tahun 2017 dari CNBC, akibat adanya kejahatan siber maka Indonesia mengalami kerugian tahunan mencapai 600 miliar USD atau setara dengan 8,160 triliun rupiah[8]. Untuk dapat mencegah dan melindungi smartphone dari adanya serangan *malware fatrat* maka harus dilaksanakan beberapa upaya seperti dilakukannya pengujian eksploitasi menggunakan metode *reverse engineering*.

Dalam penelitian ini dilakukan *exploitation testing* terhadap sistem android dengan aplikasi baidu browser sebagai perantara serangan *malware*. Penggunaan android 10 dalam penelitian ini dikarenakan erdasarkan data yang dikutip dari GSM Arena pada tahun 2021, laporan dari Android Studio menunjukkan bahwasanya jumlah persentase pengguna android 10 saat ini 26, 5% secara global sementara untuk pengguna android 11 berada di urutan kedua dengan jumlah 24,2% pengguna. Penggunaan Baidu browser dalam penelitian ini dikarenakan Baidu browser dipilih untuk digunakan pada penelitian ini karena baidubrowser merupakan sebuah aplikasi bawaan yang marak ditemukan pada smartphone besutan china seperti *Xiaomi* yang mana aplikasi bawaan pada smartphone Xiaomi tidak . Serangan *malware* dilakukan dengan membuat *backdoor* menggunakan *fatrat*. *Fatrat* merupakan sebuah *tools* yang digunakan untuk menginfeksi aplikasi android dengan *payload* meterpreter. Penelitian ini menggunakan metode *reverse engineering*, dan MobSF, JADX, serta TheFatRat sebagai tools. MobSF digunakan untuk melakukan analisa secara otomatis, analisis secara manual menggunakan JADX, sedangkan TheFatRat digunakan untuk melakukan injeksi *malware metasploit* berjenis RAT. Pemilihan penggunaan ketiga *tools* tersebut dikarenakan adanya manfaat yang diberikan. TheFatRat berfungsi untuk menginject sebuah *script malware*

dari metasploit ke dalam sebuah file aplikasi original dengan satu kali klik, sehingga dapat memudahkan pelaksanaan penelitian. MobSF dapat membantu pengguna dengan menyediakan analisis risiko otomatis. Di samping itu, MobSF membantu pengguna dalam menyeleksi aplikasi yang mungkin berbahaya atau berubah menjadi berbahaya di beberapa titik. Selain MobSf, JADX juga digunakan untuk mengetahui perubahan struktur dari program sebelum dan sesudah dilakukan injeksi *malware* ke dalam aplikasi android. Maka dengan adanya penggunaan MobSF dan JADX sebagai *tools* dapat memudahkan peneliti untuk mengetahui perbandingan banyaknya anomali pada analisis otomatis dengan analisis manual. Harapan dari penelitian ini dapat mengetahui bagaimana serangan *malware* berjalan dan mengetahui celah keamanan yang dapat dimanfaatkan oleh hacker, sehingga dapat dilakukan tindak lanjut yang tepat untuk mengamankan *smartphone* ataupun perangkat bersistem operasi android lainnya. Diharapkan penelitian ini dapat memberikan kontribusi terhadap pengembangan keamanan yang ada di sistem operasi android dan memberikan solusi serta saran kepada pengguna android untuk dapat mengoptimalkan keamanan perangkat.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang masalah di atas, maka rumusan dalam penelitian ini adalah :

1. Bagaimana perilaku atau kemampuan *malware* fatrat Ketika berhasil disisipkan pada aplikasi BaiduBrowser.
2. Bagaimana MobSF dapat mengindentifikasi adanya *malware* pada aplikasi Baidu Browser setelah disisipi *malware*.

1.3 Pertanyaan Penelitian

Berdasarkan latar belakang di atas, maka pertanyaan yang ada pada penelitian ini adalah :

1. Apakah terjadi perubahan pada struktur aplikasi Baidu browser sebelum dan setelah dilakukan injeksi malware?

2. Apakah MobSF dapat mengidentifikasi adanya malware pada aplikasi Baidu Browser?

1.4 Tujuan Penelitian

Adapun tujuan penelitian sebagai berikut :

1. Mengetahui perilaku, karakteristik dan kemampuan malware fatrat yang disisipkan ke dalam aplikasi baidu browser.
2. Mendalami pengujian yang dilakukan secara manual dan pengujian yang dilakukan secara otomatis menggunakan MobSF.

1.5 Batasan Penelitian

Batasan penelitian yang digunakan pada penelitian ini adalah sebagai berikut :

1. Pengujian dilakukan dengan menggunakan tools Metasploit.
2. Menggunakan aplikasi baidu browser sebagai objek yang disisipi malware fatrat.
3. Menggunakan JADX untuk melakukan analisis perbandingan manual terhadap struktur kode pada aplikasi sebelum dan sesudah dilakukan penyisipan malware.
4. Menggunakan MobSF untuk melakukan scanning secara otomatis.
5. Penelitian dilakukan dengan memanfaatkan android 10.

1.6 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Manfaat Teoritis

   Penelitian ini diharapkan dapat menambah wawasan dan ilmu pengetahuan tentang analisis keamanan sistem android, khususnya yang berkaitan dengan malware metasploit dan RAT menggunakan metode Reverse

Engineering dan dapat bermanfaat sebagai bahan untuk penelitian lebih lanjut.

2. Manfaat Praktis
   a. Pembaca dapat mengetahui bagaimana cara menganalisis sistem keamanan pada android.
   b. Dapat mempelajari cara kerja aplikasi seperti perizinan hak akses aplikasi.
   c. Sebagai pengetahuan bagi pengguna Android agar lebih berhati-hati memasang aplikasi yang tidak dikenal *store.*
   d. Dengan adanya penelitian ini diharapkan dapat menambah wawasan kepada setiap pembaca jika suatu saat mendapati aplikasi tidak dikenal agar dapat melakukan *scanning* secara keseluruhan menggunakan MobSF dan dilakukan analisa secara mendalam menggunakaan JADX.
   e. Hasil penelitian ini diharapkan dapat memberikan kesempatan bagi penulis dan pembaca untuk menambah pengetahuan dan wawasan dalam bidang IT *Securty*, khususnya tentang serangan *malware* pada Android.