BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Internet kini menjadi teknologi yang vital di berbagai belahan penjuru dunia. Keberhasilan dalam menyebarkan informasi secara global menjadi aspek yang krusial, namun hal ini dapat berdampak positif maupun negatif. Dengan kelebihan yang dimiliki ini, banyak pengusaha memanfaatkan internet dalam mempromosikan produk melalui iklan *online* untuk mendapatkan jangkauan pangsa pasar yang lebih luas dengan lebih efisien dan biaya yang lebih ekonomis dibandingkan metode konvensional (Bermudez-Villalva et al., 2020). Namun, kejahatan siber ini dapat terjadi di berbagai tempat, termasuk pemanfaatan iklan *online* sebagai umpan dalam menarik *audiens*. Dari data BSSN sepanjang tahun 2023, total trafik anomali di Indonesia sebanyak 403.990.813 anomali serta adanya laporan dalam "kategori aduan" terbanyak dari *stakeholder* pada layanan aduan siber adalah *cybercrime* dengan persentase 86% (1.417). Tingginya persentase *cybercrime*, iklan *online* dapat menjadi sumber dan target eksploitasi penyerangan, terutama ketika dibuat secara berlebihan sehingga mengganggu kenyamanan pengguna. Iklan *online* dapat disusupi oleh para pelaku kejahatan siber dengan menyematkan *malware* di dalamnya untuk menyerang perangkat korban. Kejahatan yang memanfaatkan iklan *online* disebut dengan *malicious advertising* atau *malvertising* (Rolon et al., 2019).

Malvertising merupakan aktifitas kejahatan siber yang menyuntikan malware kedalam iklan *online* yang memanfaatkan kerentanan browser sebuah browser (Bermudez-Villalva et al., 2020). *Malvertising* menjadi berbahaya karena mempunyai sebuah mekanisme penyebaran *malware* melalui perantara iklan, yang membawa kepercayaan tersirat antara pihak yang terlibat dalam penayangan iklan tersebut (Dwi Anggana et al., 2022). Dalam kegiatan yang dilakukan oleh para pelaku kejahatan pada ranah *malvertising* ini yaitu menggunakan sebuah trik penipuan klik atau *click fraud* untuk memicu klik iklan palsu secara terprogram,

dan pada saat di klik hal ini dapat mengarahkan pengguna ke halaman yang berisi unduhan *drive-by-downloads* atau serangan yang memungkinkan *malware* diunduh dan diinstal tanpa persetujuan atau sepengetahuan pengguna (Chen et al., 2019). Beberapa situs terkemuka yang sudah dimanfaatkan untuk praktik *malvertising* meliputi Spotify, London Stock Exchange, dan The Network Times (P Pillai et al., 2022). Dampak negatif dari *malvertising* dapat menjadi ancaman serius bagi pengguna ponsel Android yang mempunyai sebuah masalah dengan munculnya iklan yang berlebih. Sementara itu, pengguna ponsel Android di Indonesia selalu mengalami kenaikan selama periode tahun 2015-2021 dengan rata-rata sebanyak 7,02 juta/tahun. Kenaikan yang signifikan dari tahun ke tahun, membuat brand ponsel Android asing masuk ke Indonesia. Salah satunya merupakan ponsel Android *"China Brand"* berhasil mendominasi pangsa pasar di Indonesia. Hal ini terjadi karena pengalaman merek *(brand experience)* yang tinggi, sehingga berperan penting dalam membangun kepercayaan merek *(brand trust)* tersebut (Ari Pamungkas & lshak, 2023). Namun, ponsel Android *"China Brand"* ini memiliki sebuah masalah, yaitu seringnya kemunculan iklan *online* yang berlebih. Dilain sisi pemanfaatan dari AdBlocker juga tidak dapat bekerja maksimal dikarenakan kustomisasi *blacklist* iklan pada peramban yang terbatas dan sepenuhnya dikelola oleh peramban (Satriawan & Hari Trisnawan, 2021). Sehingga hal ini dikhawatirkan, adanya indikasi bahwasanya pada iklan *online* yang muncul telah tersisipi oleh *malware* serta hal tersebut juga memberikan dampak yang mengganggu dan merugikan pengalaman pengguna.

Dari penjelasan diatas bisa diketahui bahwa *malvertising* ini dapat menyerang ke sebuah ponsel Android tanpa diketahui oleh pengguna. Oleh sebab itu diperlukannya sebuah solusi terhadap penanganan *malvertising.* Seperti halnya penelitian yang dilakukan oleh Joshua rolon terkait solusi serangan *malvertising,* dengan *SpartanShield* sebagai alat pertahanan. *SpartanShield* ini merupakan sebuah konfigurasi browsing web yang terdiri dari browser brave, ekstensi pemblokiran iklan uBlock Origin, dan DNS *sinkhole* Pi-Hole yang bertujuan untuk memberikan pertahanan dari serangan *malvertising* serta membantu dalam meningkatkan kinerja web browser secara keseluruhan (Rolon et al., 2019). Penelitian lain yang dilakukan

oleh Muhamad Apriyatna, yaitu memanfaatkan Raspberry Pi 4 menggunakan OPNSense DHCP dengan metode PPDIOO yang bertujuan untuk DNS lokal sebagai satu-satunya jalur koneksi data, sementara DNS terlepas dari OPNSense digunakan untuk menerapkan filtrasi iklan di situs web. Raspberry Pi dengan sistem Pi-Hole bertindak sebagai pemfilter data dan iklan, serta OPNSense memberikan lapisan keamanan ekstra sebagai DNS Resolver (Apriyatna & Fikri Zulfikar, 2023). Penelitian lain yang membahas pemblokiran iklan juga dilakukan oleh Lukmanulhakim bin Ngah, memanfaatkan Raspberry Pi 3 B yaitu dengan Ras3Guard dan Pi Hole sebagai *software engine* yang digunakan. Ras3Guard ini memungkinkan untuk mengelola dan memantau semua aktivitas internet dengan mudah dan efektif, serta memfilter situs web yang tidak diinginkan hingga memblokir iklan *online* (Bin Ngah et al., 2021). Adapun penelitian lain yang membahas solusi untuk *malvertising* ini yang dilakukan oleh Arya P Pillai, dengan memanfaatkan penggunaan antivirus, *AdBlocker*, pembaruan browser dan plugin secara teratur. Selain itu, penulis memperhatikan jalur pengiriman, menambah fitur keamanan tambahan, dan melakukan pemindaian secara berkala untuk mendeteksi *malware* dan melawan *malvertising* (P Pillai et al., 2022).

Dari penelitian yang dilakukan oleh Arya P Pillai, mengenai solusi yang berkaitan dengan melawan *malvertising* ini terlalu kompleks karena banyak solusi yang diimplementasikan sehingga dapat menimbulkan kebingungan dan pendekatan yang tidak fokus. Oleh sebab itu, untuk mengurangi risiko serangan *malvertising* dengan solusi yang lebih simple dan terfokus, penulis bermaksud dalam penelitian ini memanfaatkan AdGuardHome sebagai solusi perangkat lunaknya dengan ponsel Android *"China Brand"* sebagai objeknya. Langkah ini melibatkan penerapan router dalam jaringan lokal untuk mengalihkan penggunaan AdGuardHome sebagai DNS *Query*, memastikan bahwa semua *client* yang menggunakan DHCP secara otomatis terhubung dengan AdGuardHome. Dengan demikian, upaya dalam membangun sistem pemblokiran iklan *online* yang tersebar melalui situs web, diharapkan dapat meminimalisir potensi serangan *malvertising*.

1.2 PERUMUSAN MASALAH

Berdasarkan latar belakang yang dipaparkan, dapat ditarik sebuah permasalahan penelitian, yaitu serangan siber dapat terjadi di berbagai tempat, salah satunya upaya pemanfaatan iklan *online* dalam penyebaran *malware* atau juga disebut dengan *malvertising*. Gangguan *malvertising* tidak hanya terbatas pada penyebaran *malware*, namun juga menurunkan tingkat efektivitas pada situs *web* itu sendiri, karena adanya gangguan dalam aktivitas browsing yang dilakukan. Ponsel Android *"China Brand"* menjadi salah satu produk yang memiliki permasalahan akan kemunculan iklan *online* yang berlebih. Meskipun sudah adanya upaya yang dilakukan dengan menggunakan AdBlockers tetapi solusi ini tidak selalu berfungsi dengan baik ketika ekstensi AdBlocker tidak menghentikan semua iklan. Hal ini diperlukan kustomisasi *blacklist* iklan terbatas pada peramban bawaan yang sepenuhnya dikelola oleh pengembang peramban, sehingga pengguna tidak dapat mengatur *blacklist* iklan ketika menemukan iklan yang lolos dari AdBlocker.

1.3 PERTANYAAN PENELITIAN

Berdasarkan perumusan masalah, maka dapat diuraikan menjadi beberapa pertanyaan penelitian, antara lain adalah sebagai berikut:

1. Bagaimana AdGuard Home dapat digunakan sebagai sistem pertahanan dalam memerangi *malvertising*?
2. Bagaimana efektivitas AdGuard Home dalam melawan serangan *malvertising* pada ponsel Android *"China Brand"*?

1.4 TUJUAN PENELITIAN

Penelitian ini bertujuan membangun sebuah sistem keamanan pada infrastruktur utama jaringan, dari serangan *malvertising* dan kejahatan yang terjadi pada internet dengan menggunakan AdGuardHome. Penelitian ini akan diujikan pada 5 ponsel Android *"China Brand"* dengan kondisi"*fresh install"* atau "modul setelan pabrik", yang mempunyai sebuah masalah terkait dengan iklan *online* yang muncul. Hal ini perlu diwaspadai adanya indikasi bahwa iklan *online* tersebut berpotensi disisipi sebuah *malware*.

1.5 MANFAAT HASIL PENELITIAN

Penelitian ini memberikan manfaat dalam mengurangi aktivitas serangan siber yang dilakukan melalui iklan *online* dalam menyebarkan *malware* atau *malvertising* pada saat mengakses *web* dan aplikasi *mobile* pada ponsel Android*"China Brand"*. Dengan adanya pemanfaatan AdGuardHome ini, dapat memberikan pengalaman pengguna yang lebih baik dan lebih terjaga dari serangan *malware* yang berpotensi merusak pada saat melakukan aktivitas berselancar di internet. Penelitian ini juga dapat menjadi sebuah sumbangan pada keamanan digital, terkhusus dalam konteks pencegahan *malvertising.*