BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Malicious traffic merupakan kejadian yang tidak normal yang terjadi pada lalu lintas jaringan dan memiliki dampak yang berbahaya. Salah satu penyebab adanya *Malicious traffic* yaitu adanya aktivitas atau serangan yang timbul dari malfungsi pada perangkat. *Malicious traffic* dapat membawa serta masalah keamanan lainnya seperti *malware*, *phising*, *spam,* dan serangan DDoS. Berdasarkan data yang didapat dari Badan Siber dan Sandi Negara (BSSN) selama tahun 2023 terdapat 403.990.813 anomali dengan anomali tertinggi yaitu *Generic Trojan RAT* yang mengindikasikan adanya *backdoor communication* antara perangkat dengan *domain Malicious* (BSSN, 2023) Penjualan ponsel Android *"China Brand"* di Indonesia semakin meningkat, dengan pertumbuhan yang sangat pesat pada beberapa tahun terakhir ini. Ponsel Android *"China Brand"* seperti Xiaomi, OPPO, Vivo, dan X4, telah menarik perhatian konsumen Indonesia dengan produk mereka yang inovatif dan terjangkau. Menurut data dari *Counterpointresearch* jumlah penjualan Ponsel Android *"China Brand"* di Indonesia pada tahun 2023 yaitu, OPPO 20%, Vivo 17% Xiaomi 16%, dan Realme 11% (Team Counterpoint, 2024). Namun, berdasarkan penelitian sebelumnya ditemukan ponsel tersebut memiliki indikasi *Malicious traffic* sebagai data *leakage* (Hariyadi et al., 2023)

Malicious traffic dapat di sebabkan oleh aplikasi yang tidak diinginkan seperti aplikasi yang didapat dari *pay-per-install* pada aplikasi yang tersedia di tempat download alternatif dan resmi(Kotzias et al., 2020). Selain itu, penyebaran *malware* disebarkan melalui tempat *download* resmi maupun alternatif. *Malware* yang dibawa dapat masuk tanpa disadari melalui update aplikasi dan *malware* tersebut dapat terbawa ke perangkat baru melalui backup otomatis dari *malware* tersebut. Berdasarkan masalah keamanan tersebut maka perlu diketahui cara untuk melihat keamanan ponsel *"China Brand".* Dengan demikian, masalah dari

keamanan data akibat *Malicious traffic* dapat diatasi. Masalah keamanan menjadi hal yang sangat penting karena adanya *malware* yang terdeteksi pada perangkat Android*"China Brand".*

Pada penelitian sebelumnya, seperti yang dilakukan oleh (Hudzaifah, 2023), dijelaskan bahwa untuk mengetahui normal atau tidaknya jaringan perlu dilakukan pengawasan dengan menggunakan sistem *monitoring*. Setelah diketahui normal atau tidaknya jaringan terdapat dua ancaman yaitu ancaman dari dalam *(insider threat)* dan ancaman dari luar *(outsider threat)* seperti yang dijelaskan pada penelitian oleh (Hariyadi & Finansia, 2023).

Dalam mengetahui normal atau tidaknya jaringan maka dilakukan pengawasan dengan menggunakan Maltrail seperti yang dijelaskan pada penelitian yang dilakukan oleh (Hudzaifah, 2023). Dilakukan Pembangunan sistem monitoring *Malicious traffic* di jaringan. Maltrail digunakan untuk mengawasi lalu lintas pada jaringan yang berbahaya dengan jejak statis yang di kumpulkan dari laporan anti-virus. Pada penelitian tersebut dimanfaatkan daftar domain public. Kemudian pada penelitian yang dilakukan oleh (Hariyadi & Finansia, 2023) diterapkan metode Network Development Life Cycle (NDLC). Penerapan NDLC dibantu dengan teknik *port mirroring* pada router. Namun, penerapannya menggunakan perancangan Mikrotik dan Maltrail sebagai sensor deteksi *Malicious traffic*. Dengan analisis tersebut maka dapat dilihat jenis ancaman yang berasal dari dalam atau dari luar. Selain itu juga dapat diusulkan analisis serangan siber yang bersumber dari jaringan internal menggunakan teknik *Switched Port Analyzer* atau *port mirroring* ekosistem rumah cerdas.

Pada penelitian sebelumnya belum ditemukan *Malicious traffic* atau aktivitas anomali pada perangkat IoT (Hariyadi & Finansia, 2023). Kemudian pada penelitian selanjutnya terdapat kekurangan dalam penggunaan Maltrail yang belum terintegrasi dengan *firewall* (Hudzaifah, 2023). Pada penelitian tersebut masih bisa dikembangkan untuk mengintegrasi Mailtrail dengan *firewall.* Dalam sebuah penelitian, terdapat berbagai cara untuk mengatasi masalah *Malicious traffic.* Yang dianataranya, melakukan deteksi *Malicious traffic* berbasis *Machine Learning* (ML). Mengidentifikasi *Malicious traffic* juga dilakukan dengan mengevaluasi

pendekatan menggunakan kumpulan data Bot dan empat algoritma *Machine Learning* (ML) yang berbeda. Namun, deteksi berbasis *Machine Learning* (ML) mencapai akurasi deteksi yang rendah dan *throughput* yang rendah, akibat ekstraksi fitur lalu lintas menjadi tidak efisien dan deteksi serangan tidak terjadi secara realtime (Fu et al., 2021; Shafiq et al., 2020). Penelitian lain melakukan rancangan model jaringan konvolusional HexCNN-1D yang menggabungkan mekanisme pemrosesan dan dinormalisasi. Dengan menambahkan modul mekanisme *Global Attention Block* (GAB) dan *Category Attention Block* (CAB), kemudian digunakan untuk mengklasifikasikan dan mengenali *Malicious traffic* jaringan(He et al., 2021).

Dari berbagai upaya penanganan *Malicious traffic* diatas, peneliti bermaksud melakukan penelitian yang berbeda. Hal yang menjadi pembeda yaitu pada ponsel Android *"China Brand",* sebagai objek penelitian yang akan dianalisis *Malicious traffic* menggunakan Maltrail. Masalah lain yang menjadi motivasi untuk mengangkat topik penelitian ini adalah pada sebuah penelitian yang menyebutkan bahwa *bloatware* merupakan *malware* yang sengaja ditanam pada ponsel Android untuk membuat sumber daya batrai, memori, ruang disk dan lainya menjadi terganggu dan mengakibatkan penyimpanan cepat penuh (Ozbay & Bicakci, n.d.). Sehingga penulis melakukan fokus pendeteksian, yang dilakukan untuk mengetahui adanya aktifitas anomali yang bersumber dari ponsel Android *"China Brand"* yang kemungkinan digunakan untuk melakukan penyerangan kepada pihak yang lain..

1.1.1 Perumusan Masalah

Penelitian ini terkait analisis *Malicious traffic* pada ponsel Android *"China Brand"* menggunakan Maltrail. Peneliti menjelaskan proses implementasi Maltrail dalam menganalisis *Malicious traffic* untuk mengetahui adanya aktivitas tidak wajar dan berpotensi mengganggu sistem jaringan yang bersumber dari perangkat ponsel Android*"China Brand"*.

1.1.2 Manfaat Hasil Penelitian

Manfaat yang diperoleh dari penelitian ini adalah untuk mengungkap fakta baru terkait aktivitas tidak wajar perangkat Android, khususnya pada merek *"China*

Brand". Mengingat Android merupakan perangkat yang menjadi sangat penting dalam kehidupan sehari-hari, dan di bandingkan dengan merek lain, *"China Brand"* relatif murah dalam segi harga. Sehingga kemungkinan besar memiliki banyak pengguna. Oleh karena itu peneliti melakukan analisis adanya potensi *Malicious traffic* pada jaringan perangkat Android *"China Brand*" melalui jaringan nirkabel 2.4Ghz. Penelitian ini diharapkan dapat memberikan wawasan dan kewaspadaan tentang ancaman *Malicious traffic* yang di timbulkan oleh perkembangan teknologi Android *"China Brand"* atau perihal yang merugikan pihak lain akibat *malware* baik yang sengaja ditanam atau pun adanya aktivitas pengendalian sehinnga dapat merugikan bagi penggunanya.

1.1.3 Pertanyaan Penelitian

Berdasarkan perumusan masalah diatas, dapat di uraikan menjadi beberapa pertanyaan.

1. Bagaimana cara mengimplementasikan Maltrail dalam menganalisis *Malicious traffic*?
2. Bagaimana sistem dapat mengetahui adanya *Malicious traffic* pada perangkat Android *"China Brand"*?

1.2 TUJUAN PENELITIAN

Tujuan penelitian ini yaitu untuk menambahkan daftar hitam deteksi *Malicious traffic* pada perangkat Android *"China Brand"* dan menambah *insight* baru pada pengguna agar lebih waspada terhadap serangan siber yang tidak hanya terjadi pada serangan dari luar tapi dapat diserang dari dalam yang sengaja ditanamkan.