ANALISIS *MALICIOUS TRAFFIC* PADA PONSEL PADA PONSEL ANDROID *"CHINA BRAND"* MENGGUNAKAN MALTRAIL

Paskalis Rivaldianus Tagang[1], Dedy Hariyadi [2], Arief Ikhwan Wicaksono [3]

INTISARI

Latar Belakang: Malicious Traffic merupakan lalu lintas jaringan yang tidak normal dan memiliki dampak berbahaya, sering kali disebabkan oleh malfungsi perangkat. Trafik berbahaya ini dapat menyebabkan berbagai masalah keamanan seperti malwer, phising, spam, dan serangan Ddos. Berdasarkan data dari Badan Ciber dan Sandi Negara (BSSN) pada tahun 2023, terdeteksi 403.990.813 anomali dengan kasus tertinggi adalah Generic Troja RAT. Peningkatan penjualan ponsel Android "China Brand" di Indonesia, seperti Xiaomi, OPPO, Vivo, dan Realme, mengindikasikan adanya data leakage. Penelitian ini menggunakan Maltrail dan *Network Development Life Cycle* (NDLC) untuk mendeteksi Malicious traffic pada ponsel tersebut. Fokusnya adalah identifikasi anomali yang dapat menyebabkan serangan, terutama karena adanya bloatware yang mengganggu kinerja ponsel

Tujuan: Penelitian ini bertujuan 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

Metode Penelitian: Metode yang digunakan adalah *port mirroring,* ini adalah teknik penyalinan jaringan *traffic* dari port yang dilalui lalu lintas utama ke media lain. Penyalinan *traffic* menggunakan teknik *port mirroring* dilakukan dengan penyalinan *traffic* dari *acess point* yang sebelumnya sudah saling terkoneksi dengan ponsel Android *"China Brand"*.

Hasil: Pengujian dari ponsel android "*China Brand*" tidak ditemukan *Malicious traffic,* pada aplikasi Maltrail, hanya nomor IP Raspberry yang terdeteksi *Malicious traffic*nya

Kesimpulan: Sistem monitoring *Malicious traffic* telah berhasil dirancang dan dibangun. Proses pendeteksian *Malicious traffic* pada ponsel android *"China Brand"* dengan menggunakan metode *port mirroring* tidak ditemukan *Malicious traffic* secara langsung, seperti hasil yang di tampilkan dibagian pembahasan, pendeteksian *Malicious traffic* tidak temukan trafik pada aplikasi Maltrail, hanya nomor IP Raspberry yang terdeteksi *Malicious traffic*, sehingga tidak memiliki *Malicious traffic* dan terbukti bahwa ponsel android *"China Brand"* tidak memiliki *malware* yang sengaja ditanamkan. Dapat disumpulkan ponsel android *"China Brand"* aman.

Kata-kunci: *Malicious Traffic, Maltrail, Malware, China Brand*

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

ANALISIS *MALICIOUS TRAFFIC* PADA PONSEL PADA PONSEL ANDROID *"CHINA BRAND"* MENGGUNAKAN MALTRAIL

Paskalis Rivaldianus Tagang[1], Dedy Hariyadi [2], Arief Ikhwan Wicaksono [3]

ABSTRACT

***Background**: Malicious traffic is abnormal network traffic and has a harmful impact, often caused by device malfunctions. This malicious traffic can cause various security issues such as malwer, phishing, spam, and DDoS attacks. Based on data from the State Cyber and Cryptography Agency (BSSN) in 2023, 403,990,813 anomalies were detected with the highest case being Generic Troja RAT. The increase in sales of "China Brand" Android phones in Indonesia, such as Xiaomi, OPPO, Vivo, and Realme, indicates the existence of data leakage. This study uses Maltrail and Network Development Life Cycle (NDLC) to detect malicious traffic on the phone. The focus is on identifying anomalies that can lead to attacks, especially due to the presence of bloatware that interferes with the performance of the phone*

***Objective**: This study aims to add a blacklist of malicious traffic detection on "China Brand" Android devices and add new insights to users to be more aware of cyber attacks that not only occur in attacks from the outside but can be attacked from within that are deliberately implanted*

***Method:** The method used is port mirroring, this is a technique of copying network traffic from the port that the main traffic passes to other media. Traffic copying using the port mirroring technique is carried out by copying traffic from acess points that have previously been interconnected with "China Brand" Android phones*

***Results:** Testing of "China Brand" android phone did not find Malicious traffic, on the Maltrail application, only the Raspberry IP number was detected Malicious traffic*

***Conclusion:** The Malicious traffic monitoring system has been successfully designed and built. The process of detecting Malicious traffic on "China Brand" android phones using the port mirroring method did not find Malicious traffic directly, as shown in the discussion section, Malicious traffic detection did not find traffic on the Maltrail application, only the Raspberry IP number was detected Malicious traffic, so it did not have Malicious traffic and it was proven that the "China Brand" Android phone did not have malware that was deliberately implanted. Can be collected "China Brand" android phone is safe.*

***Keyword**: Malicious Traffic, Maltrail, Malware, China Brand*

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA