ANALISIS *MALICIOUS TRAFFIC* PADA LAMPU CERDAS MENGGUNAKAN APLIKASI MALTRAIL

Velisia Amanda Khafid [1], Dedy Haryadi [2]

INTISARI

Dari banyaknya obyek perangkat IoT, lampu cerdas menjadi alat yang banyak digunakan dalam aktivitas rumah tangga. Sehingga lampu cerdas tersebut menjadi salah satu pemeran dalam peningkatan aktivitas IoT. Seiring meningkatnya perkembangan IoT, resiko tingkat keamanan beresiko merugikan pengguna, terutama jaringan yang bersifat nirkabel. Sehingga diperlukan sistem keamanan sebagai upaya penanggulangan serangan kejahatan siber. Pendeteksian *malicious traffic* berfokus pada mengidentifikasi malware yang sengaja ditanam pada lampu cerdas.

Tujuan dari penelitaian ini yaitu untuk menambah daftar hitam deteksi *malicious traffic* pada lampu cerdas dan menambah *insight* baru keamanan siber kepada pengguna lampu cerdas. Metode yang digunakan menggunakan *port mirroring* atau SPAN. *Port mirroring* merupakan teknik penyalinan *traffic* dengan melakukan ekspor trafik dari router yang sudah saling terkoneksi dengan lampu cerdas. Untuk mengoneksikan hal tersebut dilakukan rangkaian setingan MikroTik untuk mengambil nomor IP pada masing masing *device*, kemudian dilakukan analisis menggunakan aplikasi Maltrail. *Device* yang digunakan yaitu 5 (lima) buah lampu cerdas dengan merek yang berbeda.

Dari hasil perancangan pendeteksi *malicious traffic* pada lampu cerdas melalui aplikasi Maltrail, tidak ditemukan adanya *malicious traffic* secara sengaja ditanam dalam lampu cerdas tersebut. Serangan hanya ditemukan pada router. Sehingga dapat disimpulkan bahwa sistem aktivitas lampu cerdas berbasis nirkabel tersebut aman dari serangan kejahatan siber.

Kata-kunci: IoT, *Malicious Traffic*, Maltrail, lampu cerdas, *Port Mirroring*.

1

2

ANALYSIS OF MALICIOUS TRAFFIC ON SMART LIGHTS USING THE MALTRAIL APPLICATION

Velisia Amanda Khafid[1], Dedy Haryadi [2]

ABSTRACT

Of the many IoT device objects, smart lights are tools that are widely used in household activities. The survey institute even stated that lights are the device that is mostly installed in household activities, up to 65%. So that these smart lights become one of the actors in increasing IoT activity. As the development of IoT increases, the risk of security levels is at risk of harming users, especially wireless networks. Malicious traffic is one of the most serious threats. Because, malicious traffic can send various kinds of illegal activities such as the spread of malware attacks, DOS, and phishing. So that a security system is needed as an effort to overcome cybercrime attacks. Malicious traffic detection focuses on identifying malware intentionally implanted in smart lights.

The purpose of this research is to add to the blacklist of malicious traffic detection on smart lights and add new cybersecurity insights to smart light users. The method used uses port mirroring or SPAN. Port mirroring is a technique of copying traffic by exporting traffic from routers that are connected to each other with smart lights. To connect this, a series of MikroTik *settings are carried out to retrieve the IP number for each device, then an analysis is carried out using the Maltrail application. The devices used are 5 (five) smart lamps with different brands.*

From the results of the design of a malicious traffic detector on smart lamps through the Maltrail application, no malicious traffic was found intentionally planted in these smart lamps. The attack is only found on routers. So it can be concluded that the wireless-based smart light activity system is safe from cybercrime attacks.

Keywords*: IoT, Malicious Traffic, Maltrail, Smart Lights, Port Mirroring.*

[1] Student of Information Technology Jenderal Achmad Yani Yogyakarta University

[2] Lecturer of Jenderal Achmad Yani Yogyakarta University