ABSTRACT

Diskominfo Sumedang is a public service organization that is responsible for data and communications that connects all government institutions such as sub-districts, and offices that are connected to the Diskominfo Sumedang server. The server's job is to server all devices connected to the network, such as monitoring all network activity security, system protection, data, and improving network security quality. Seeing this, the basic needs of Diskominfo Sumedang, we need a system that can detect and block malware that tries to enter the server network at Diskominfo Sumedang.

In this final, a Maltrail (Malware Trail) and Fail2Ban sensor implementation system is designed to detect and prevent malware attacks on Diskominfo Sumedang network server with push notifications, which is another solution to this problem. The software used to detect malware is Maltrail. The way this software works is with sensors that scan all traffic activities on the server network. Then, the software used to block or prevent malware attaks, namely Fail2Ban. The system uses telegram bots as notifications if there is a malware attack on the server.

From the result of malware attacks on the server, there was a decrease in throughput of 56,28%, the results of the implementation of this system were able to detect and block malware traffic on the network, as a result it did not experience a significant decrease in throughput. Then the system detects attacks other than malware, namely scanning ports with a threat level of 2.7%. So that the system is able to minimize the threats of attack and is able to increase the throughput value on the Diskominfo Sumedang network server by looking at comparison of malware traffic before and after the implementation system.

Keywords: *Maltrail, Fail2Ban, Malware, Detection, Prevention.*