ABSTRACT

MALWARE ANALYSIS ON NETWORK TRAFFIC USING SECURITYONION

By

AHMAD BAHRI AL-ANWAR

1202150111

Malware is software that is used with the aim of trying to violate computer system security policies related to confidentiality, integrity, or availability. The purpose of malware analysis is usually to provide information needed to respond to network intrusion. The goal is to determine exactly what happened and ensure that all computers and infected files are found. When analyzing suspected malware, the goal is to determine exactly what a particular suspect can do. Therefore, it is necessary to analyze packet capture to find out suspicious malware attacks on computers on the network and find out the anomalies caused by the malware. This research was conducted by testing six PCAP samples that were downloaded randomly, then analyzed using SecurityOnion. The analysis carried out using a static analysis method that focuses on traffic that passes in a network based on anomalies and behaviors of that malware. The results of this analysis are the categorization of malware based on the threats and impacts that are detected. Based on these data the researchers conducted a preventive action analysis of the resulting impacts.

Keyword: Malware, Malware analysis, cyber crime, traffic analysis, Packet capture, Network analyzer, Security Onion