ABSTRACT

Malware has evolved very fast and has various techniques to deceive antivirus when infect computer. The purpose from attacker or malware maker is installing malware on the victim's device and get full control of the device. As is the threat of full control of the device, the victim will suffer a lot of losses from infomation theft, DDoS attack, abuse of victim computer, email spam, and other related losses. From a variety of possible malware threat that will happen, research must be done to understand the signature of a malware. Malware analysis is needed to perform analysis to malware in terms of impact, category, and characteristics. From the result of the analysis can be concluded how is the classification of malware, malware detection and malware mitigation. By performing malware analyis there is some information about malware API calls. Malware categorization is done using malicious activity data set based on API calls. The more links between malicious activity on a malware, the greater the impact that malware will perform. And conversely, the less links between malicious activity on a malware, the impact will be small. The results of categorization then analyzed using anomaly method. Based on the categorization using anomaly method with the sample of malware, there are 3 malicious activity that do not have any links with the malicious activity, that are IAT Hooking, Bind TCP Port and Capture Network. There are also 2 malicious activities that have only 1 link with the malware samples used. That are Process Hollowing and Drop Files from PE Resource Section.

Keyword : malware, malware analysis, cyber crime, anomaly, malware detection, malware signature, malicious activity.