ABSTRACT

Malware is a software or created to infiltrate or destroy a computer system. Nowadays, the spread of malware is so easy, either through flash, certain advertisements on websites, and other media. Everything is very closely related to crimes such as file theft, credit cards, internet banking and so on. One of the malware that can control the user's computer secretly and remotely is poison ivy malware, known as "Remote Access Trojan" because it can provide complete control through the back door (backdoor). In this level project, the Poison Ivy malware will be analyzed to find out how the Poison ivy malware works. The analysis is carried out by static and dynamic analysis methods where the combination of these methods is a suitable combination to analyze the workings of a malware. Based on this analysis, Poison Ivy Malware works by injecting dll files, namely loadlibrary.dll to control the system on the target computer then adding files and registries to the target computer and when the server connects with the target computer then before connecting the poison ivy malware performs a password matching process if the password matches then the server computer can access the target computer. And poison ivy malware doesn't eat up too many resources on a computer system.

Keywords: Poison ivy, Remote Access Trojan (RAT), Malware.