ABSTRACT

Redline Stealer is a malware variant discovered in early Marach 2020 by proofpoint analyst. Redline is famous for its ability to bypass the antivirus scan. Redline Stealer was created by hacker with the purpose to steal vitim's information such as login data, password and credit card information from the browser application that used in infected computer. This research uses static and dynamic method to analyze redline stealer. The process of static analysis is carried out by observing the malware's sample file, while dynamic analysis is carried out by monitoring malware's activity when the malware is running on the system. The result of the analysis is show that Redline Stealer is uses the obfuscation feature, based on .net, can run only when there is internet connection, stealing sensitive information especially in browser application. The malware runs the vbc.exe process and sends the stolen information via vbc.exe to the malware's server with the IP address 37.220.87.47. The treatment for a computer that has been infected with Redline Stealer malware is by blocking IP address 37.220.87.47, stop the vbc.exe process in the task manager and delete the malware and vbc.exe file.

***Key Word**: Malware Analysis, Obfuscation, Redline Stealer*