ABSTRAK

Nama : Rakha Tri Fadillah

Program Studi : Teknik Informatika

Judul : Analisis *Ransomware* STOP/DJVU Dengan Menggunakan Metode *Static Analysis* dan *Dynamic Analysis*

Situs web phising semakin berbahaya dan menjadi masalah yang serius dibidang keamanan jaringan. Penyerang menggunakan banyak pendekatan untuk menanamkan *Ransomware* ke host target untuk memblok akses korban terhadap data mereka dan memeras korban dengan melakukan pembayaran uang atau sebagai tebusan untuk membuka akses kembali data atau *file* korban. *Ransomware* hadir dalam berbagai bentuk, misalnya mengunci layar pada sebuah perangkat atau perangkat lunak yang berbasis kripto yang mengenkripsi *file* target atau dengan algoritma kriptografi canggih. Salah satu varian *Ransomware* yaitu *STOP* tersebar hampir secara eksklusif melalui keygen dan crack, yang merupakan alat yang mengklaim memungkinkan orang untuk mengaktifkan perangkat lunak berbayar secara gratis. Anak-anak dan siswa yang kekurangan uang biasanya mencari jenis alat ini, yang menempatkan mereka pada risiko yang lebih besar untuk terinfeksi *STOP* dan menyebarkan nya kepada orang lain yang berbagi perangkat dengan mereka. Maka dari itu tujuan dari penulisan ini adalah untuk menganalisa karakteristik *Ransomware* yang sering ditemukan di dunia internet. Adapun metode yang dipakai dalam penulisan ini adalah dengan *Static Analysis* dan *Dynamic Analysis* dengan menggunakan tool Cuckoo Sandbox, Sehingga tidak ada resiko untuk terinfeksi *Ransomware.*

Kata Kunci
Malware, *Ransomware*, Cuckoo Sandbox, *Static Analysis*, *Dynamic Analysis*, STOP/DJVU.

ABSTRACT

Name : Rakha Tri Fadillah

Study Program : Informatics Engineering

Title : STOP / DJVU Ransomware analysis using the Static Analysis and Dynamic Analysis method

Phising website is increasingly dangerous and is a serious problem in network security. The attacker uses many approaches to instilling Ransomware to target host to block the victim's access to their data and extort the victim by making money or as a ransom to open up data access or the victim's file. Ransomware is present in various forms, such as locking the screen on a device or crypto-based software that encrypt the target file or with a sophiscated cryptographic algorithm. One of the Ransomware variants, namely STOP spread almost exclusively through Keygen and Crack, which is a tool that claims to allow people to activate paid software for free. Children and students who lack money are usually looking for this type of tool, which places them at greater risks to infect stop and spread them to others who share devices with them. Therefore the purpose of this study is to analyze the characteristics of Ransomware that are often found in the internet world. The method used in this study is with Static Analysis and Dynamic Analysis by using the Cuckoo Sandbox tool, so there is no risk to be infected with Ransomware.

Keywords
Malware, *Ransomware*, Cuckoo Sandbox, *Static Analysis*, *Dynamic Analysis*, STOP/DJVU.