Contribution ID: **21** Type: **Paper**

Crypto-Ransomeware Identification via Behavioural Analysis

Thursday, 14 March 2019 16:48 (15 minutes)

Ransomware is a type of malware attack that uses encryption to make data unavailable for the main purpose of collecting a certain amount of payment. Many victims of this attack who were unable to recover their data from backups have been forced to choose between either losing the data or pay a certain amount demanded by the attacker. This study analyzes ransomware variants based on attack phases and the possibility of identifying ransomware using the network traffic generated prior and after infection. This study, in Windows Operating System environment, considered seven samples of crypto-ransomware for research purposes: Revenge, Crypto-Shield, Crypto-Mix, Cyber, Sage Spora and Locker. Observations from the study reveal five of the ransomwares generated noticeable traffic and analogous file encrypted renaming patterns with time, while Windows Bit defender outrightly choked Spora and Locker. Consequently, understanding this threat and its pattern is an integral part of ensuring a robust secured network in enterprise networks. Hence, the ideas presented in this project can provide insight for additional layers of defense against this deadly attack by ransomware.

KEYWORDS: Malware, Ransomware, Crypto-ransomware, Simulation, Network traffic, Revenge, Crypto-Shield, Crypto-Mix, Cyber, Sage, Server message Block (SMB2).

Primary author: Dr THOMPSON, Aderonke (Federal University of Technology)

Co-authors: Mr ORIJA, Olumide (Computer Science Department, The Federal University of Technology, Akure, Nigeria.); Dr OWOLAFE, Otasowie (Cybersecurity Science Department, The Federal University of Technoloy, Akure, Nigeria.)

Presenter: Mr ORIJA, Olumide (Computer Science Department, The Federal University of Technology, Akure, Nigeria.)

Session Classification: PLENARY SESSION III –Paper Presentations

Track Classification: Applications and Services