**Assignment 3**

**Sindhuja Yerramalla (U00839259)**

Title: “A Survey of Ransomware: Attack mechanisms, prevention and mitigation”

Authors: Ahmad Al-Khasawneh, Mahmood Al- Khasawneh and Ayman Al-Fuqaha.

Published in: Journal of Network and Computer Applications, vol. 107, pp.45-76, October 2018.

The paper provides a comprehensive survey of ransomware, including its attack mechanisms, prevention, and mitigation techniques. The authors discuss the history and evolution of ransomware as well as its economic impact on individuals and organizations. The paper also describes the different types of ransomwares, including encrypting ransomware, locker ransomware, and master boot record(MBR) Ransomware. The authors analyze the behavior of these types of ransomwares and explain how they propagate and infect systems.

In addition, the paper presents various prevention and mitigation techniques for ransomware attacks. These techniques include security awareness training for employees, regular backups, network segmentation and the use of anti-malware software. The authors also discuss more advanced mitigation techniques, such as ransomware-specific detection and removal tools, and the use of artificial intelligence and machine learning to detect and prevent ransomware attacks.

The paper concludes that ransomware attacks are a serious threat to individuals and organizations and that a multi layered approach to prevention and mitigation is necessary to effectively combat ransomware. The authors recommend that organizations implement a combination of technical and non-technical measures to protect against ransomware, and that they regularly test their incident response plans to ensure they are effective.

This paper is similar to our project which present a prevention and mitigation technique for ransomware attacks. The difference is in this paper currently most of the ransomware are aware of deception techniques such as decoy files and they have updated their code to encrypt files in the order of most accessed files or most recently used files first. So, by the time they try to modify the decoy file, a lot of original files have already been encrypted and the damage is already done. A few other ransomware variants completely ignore the hidden files. Techniques like using memory dump to retrieve the encrypting key used for encryption will not work if the ransomware uses asymmetric encryption since this method will only give us the public key used for encryption and the files can be decrypted only by the private key which is held by the attacker. But our project is a comprehensive ransomware protection solution which involves detection of ransomware by also taking the C2C server Ip address it communicates with into account, protection of files from ransomware using system hardening and deception techniques in case if our system fails to detect ransomware.

I would like to give 8/10 points for this paper based on the above mentioned comments