Ransomware

Orel Rahum

June 2020

1 Introduction

Since the 50s, the world has seen the merits and the wonders of the Internet. Internet users generate about 2.5 quintillion bytes of data each day.(and every each day its grow-up) It is easy to see that as the size of the information that goes through the internet is greater, the need to prevent attacks over the Internet increases with it. one kind of malware that use the importance of the internet called ransomware.

ransomware is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. there are two type of ransomwares, one

Basically, there are two types of ransomwares: locky and crypto. Locky ransomware locks the entire system from access by its user, but it is usually easy to resolve. However, crypto ransomware uses encryption technology to lock selected files from user access; this is much more difficult to resolve and the damage caused may be irreversible. Crypto ransomware is also the more popular type employed by cybercriminals. A third type of ransomware called scareware has been mentioned in the literature [3]. This ransomware does not actually damage the victim's computer but only scares the victim into

It is a relatively new malware but has generated much interest from cybercriminals because of its successful attack and direct financial interest. Ransomware objective is to block its victim from accessing their own resources by locking the OS or encrypting targeted files that seem valuable to the victim, such as images, spreadsheets and presentations. [2]. Basically, there are two types of ransomwares: locky and crypto. Locky ransomware locks the entire system from access by its user, but it is usually easy to resolve. However, crypto ransomware uses encryption technology to lock selected files from user access; this is much more difficult to resolve and the damage caused may be irreversible. Crypto ransomware is also the more popular type employed by cybercriminals. A third type of ransomware called scareware has been mentioned in the literature [3]. This ransomware does not actually damage the victim's computer but only scares the victim into

2 Related work

In this section we review existing work, we noticed that we can divide the used techniques for detect ransomware to 3 categories- some of the studies based on the network level (traffic), some of the studies based on the system level(size), and some of them based on both levels.
in the article"*Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics"* article they used SDN-based solutions, they used characteristics of the network communication between the infected host and proxy server. "Machine Learning-Based Detection of Ransomware Using SDN" used network traffic signature to classify various types and identify ransomware using their adaption of random forest algorithm.

in the article "*Detecting Ransomware using Support Vector Machines*" The researchers suggested a solution using SVMs. The solution is SVM-based scheme deeply inspects the sequences of API calls, and our vector representations include the number of q-grams in the execution logs. By doing this, unknown ransomware is effectively detected in keeping with a smaller probability of malicious programs being undetected,

in the article *"Detecting Ransomware with Honeypot techniques"*, suggest honeypot as a solution, honeypot is a network-attached system set up as a decoy to lure cyberattackers and to detect, deflect or study hacking attempts in order to gain unauthorized access to information systems.

In the article "*Ransomware, Threat and Detection Techniques: A Review*" The researchers Introduce several identification methods:

• Machine learning (ML) involves learning the patterns in data to create a model. This model can then predict the outcome when fed with new data.

• Honeypot involves setting up decoy files for the ransomware to attack. Once these files are accessed, the ransomware can be identified.

• Statistic can be used to analyze ransomware to better understand their important characteristics.

In the article *"PayBreak : Defense Against Cryptographic Ransomware"* The researchers suggested a solution using " PayBreak". PayBreak is a novel protection mechanism that defeats, the threat of crypto-based ransomware. PayBreak implements a key escrow mechanism that stores session keys in a key vault. Keys in the vault are encrypted with the user's public key and thus, only the user's private key can unlock the vault. As opposed to government-mandated key escrow systems, PayBreak ensures that only the legitimate user has access to the keys held in escrow