Modern Applied Science; Vol. 14, No. 3; 2020
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Ransomware Evolution, Growth and Recommendation for Detection

Adel Hamdan Mohammad[1]

[1] Computer Science Department, The world Islamic Sciences and Education University, Amman-Jordan

Correspondence: Adel Hamdan Mohammad, Computer Science Department, The world Islamic Sciences and Education University, Amman-Jordan. E-mail: Adel.hamdan@wise.edu.jo, Adel_hamdan@yahoo.com

Received: January 29, 2020 Accepted: February 23, 2020 Online Published: February 26, 2020

doi:10.5539/mas.v14n3p68 URL: https://doi.org/10.5539/mas.v14n3p68

Abstract

Ransomware is a malicious program that can affect any person or organization. Ransomware is a complicated malicious attack that aims at lock or encrypt user files. Up to this date, there is no individual method, tool, which guarantee to protect against ransomware. Most tools available can detect some types of ransomware but it fails to detect other types of ransomware. In this research author talks about several methods, tools, procedures which can be taken to reduce the possibility of ransomware occurrences. Up to this moment, the main methods used by attacker to infect your machine are malicious emails and malicious links. After analyzing several reports written by some anti-viruses' company such as Kaspersky ,McAfee, and several researches which talks about ransomware, author conclude two points: first point, educating users, following up a strict security policy, procedures and backup strategies are the best methods which can be taken to minimize the possibility of ransomware. second point, future methods to detect ransomware mainly will be based on artificial intelligence.

Keywords: ransomware, malicious software, machine learning

1. Introduction

Ransomware is a specific type of malware that encrypt user data which will restrict individual access to his own files. Ransomware as a name come from two words, ransom and malware. Malware is an abbreviated term for "Malicious Software". Malware is specifically designed to gain access or damage victim machine. Today's malware is created mainly for profit. Malware can be used to stole information such as spyware, advertising such as Ad-ware and sending spam emails such as zombie computer. Ransomware is a very important topic in information technology security. There are a lot of methods which are used and tested to protect against ransomware (Jesper,2017; Matthias,2018). Ransomware is a very dangerous attack, for example, CryptoWall3 damage estimated to be over 320 million Dollar (Cyber Threat Alliance,2018).

Since individual security procedures taken in place are not considerable comparing with organization's security. users are thought to be the most victims of ransomware (KSN Report,2016; Internet security threat report,2019). Knowing that most users are not specialized in information technology and security means that these people didn't take enough procedures to protect themselves. No doubt that targeting big organization which has several defense stages (depth and breadth) such as firewall, anti-viruses and anti-spyware is not as easy as targeting individual who has nothing except built in windows 10 firewall (IBM Ransomware,2016).

Some researchers say that ransomware has two types (Jesper,2017). First type called locker ransomware, which aims at locking the user from accessing the system. Then the attacker asks the victim to pay to unlock the system. Other type of ransomware is crypto ransomware. Crypto ransomware aims at encrypting some or all the files in the victim machine. Then the attacker asks the victim to pay for unencrypting the files.

Ransomware, mainly, spread through different methods such as phishing emails which contain malicious content and attachments, downloading suspected files, visiting infected web site and other methods. Besides that, nowadays ransomware spread through social media, web based instant messages. Attackers with malicious intentions attack people for several decades and for several reasons. When online exploiting is started, several techniques and application such as anti-virus and anti-spyware claim that they can detect any malicious software. Most of these applications can detect malicious software but they ask for money to remove it (Jesper,2017; Hirra Sultan,2018). Ransomware affected all types of operation systems such as windows and Unix based systems. After infecting victim machine attackers ask for money and mainly payment done using bitcoins.

Several reports indicate the impact of ransomware. Semantic reports 405,000 consumers are infected with ransomware between June 2016 and June 2017 (Internet security threat report,2019). Some statistics in 2016 indicate that one company per 40 seconds and one user per 10 seconds are exposed to ransomware attacks (Kaspersky Lab,2016). In 2017, 42% of organizations in the first half of the year are attacked by ransomware (Proofpoint ,2017). In 2019 McAfee report shows that ransomware attacks grew by 118% and new ransomware families are detected (McAfee,2019). In 2015 criminal earned around 24 million from ransomware in the USA (Coveware, 2020).

Figure 1 demonstrate how ransomware represent the most familiar type of malicious software used by attacker. ransomware represent 64% of all malicious software (Proofpoint ,2017). One of the most recent research indicates that in Quarter 4 of 2019 the average payment for ransomware reach 84,116, up from 41,179 in quarter 3 of 2019 which means an increased by 104% (Coveware, 2020).

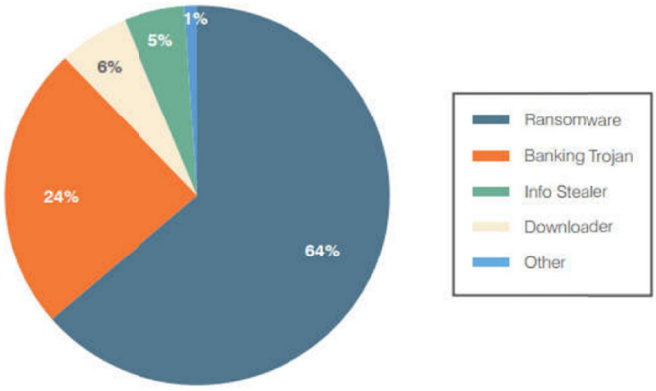

Figure 1. Malicious software types

The main goal of this research is to demonstrate up to date methods and procedures used to fight against ransomware. besides that, this research will demonstrate the speed of the growth and evolution of ransomware. The rest of this research is organized as follows: section two talks about ransomware types. Section three talks about encryption methods used in ransomware. Section four demonstrates up to date related studies that talk about ransomware detection and prevention. Section five talks about up to date recommendation methods used to prevent against ransomware. Finally, section six author demonstrates his conclusion and future work.

2. Ransomware Types

Ransomware has different types. Some researchers say that ransomware has numerous variants with 100 of new forms and patterns every year (Jim Finkle, 2016; J. Wyke,2015; D.Caivano,2017). other researchers talk about two main types of ransomware; others talk about three or more. Author in this research will focus only on crypto ransomware and locker ransomware which considered by several researchers and several companies are the only two main types of ransomware. Figure 2 show predicted growth of damage from ransomware attacks (Morgan,2017.).

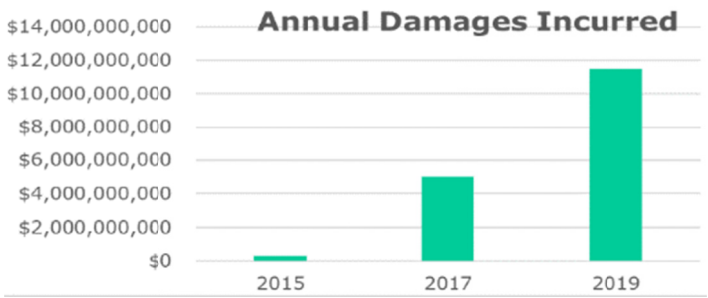

Figure 2. Growth of ransomware damage

Growth of ransomware attack is enormous. Some statistics indicate that ransomware could be the most dangerous attack which could affect individual and organizations. Figure 3 shows the predicted speed of the growth of ransomware attack (Brandon Lee, 2019).

Figure 3. Annual Ransomware Damage

2.1 Crypto Ransomware

Crypto ransomware is a very dangerous type of ransomware which aims at encrypting victim files. After that, attackers ask for money within a specific amount of time to decrypt the files. Payment is done using several methods. Nowadays, payment is mostly done using bitcoins. Some resources indicate that the cost per attack around 300 dollars of bitcoins (Jesper,2017). Crypto ransomware is growing and the number of this type of attack is rising.

Encryption of files can be done in several methods such as opening the file, reading its content, encrypting it. Another method is moving the file to another directory where it will be encrypted. Some other methods based on reading the original files and then overwriting it or creating a new file then deleting the original one (Jesper,2017). Examples of crypto ransomware is Crypto-Wall, Crypto-Locker, and WannaCry.

2.2 Locker Ransomware

This type of ransomware preventing users from using their operation systems. Locker ransomware will lock, restrict, and block user access to his own computer resources (Morgan,2017). Locker ransomware could be considered as virus that infects victim machine and locks user files. This lock will prevent users from accessing their data and files allocated on the PC until ransom is done.

3. Encryption Methods Used in Ransomware

Ransomware attackers use several methods for encryption. Attackers mainly used symmetric encryption methods such as RC4 (Rivest Cipher 4), AES (Advanced Encryption Standard). But nowadays attackers prefer hybrid methods of encryption. Today's ransomware attackers send only public key to the infected machine, and the private key in stored in the C&C servers. Symmetric key is used in the encryption in the first stage, then encryption is done in the second stage with RSA (Rivest–Shamir–Adleman) public key. This means that encryption is done first using symmetric method then in the second stage encryption is done using Asymmetric encryption. As a result, files cannot be easily decrypted (Brandon Lee, 2019; Barış Celiktaş,2018; A. Liska,2016).

Strength of ransomware based on the strength of encryption algorithm used. Hybrid methods used in ransomware encryption are done in three phases (Brandon Lee, 2019; Barış Celiktaş,2018; A. Adamov,2017; Vadim Kotov,2014). In phase 1, the ransomware attacker produces asymmetric pair of keys and places these keys inside the ransomware. In the phase 2, encryption is done on victim machine using symmetric key after ransomware is loaded or activated. Besides that, in phase 2, symmetric key which used in encryption is also encrypted by using public key generated by the C&C server. Also, in phase 2, encryption is done, and the symmetric key is deleted so that the original data cannot be easily restored. Finally, in phase 2, a pop-up message is shown with information about how to pay. In phase 3, if payment is done, attacker decrypt the asymmetric ciphertext with the private key and then send the symmetric key to the victim.

Because of the nature of ransomware, it is not an easy task to detect ransomware. Despite that, some researchers talk about several methods and techniques which may help in preventing and detecting ransomware. To take the best steps for ransomware prevention and detection we must know the methods used by ransomware to get inside our organizations and machines. Figure 4 shows most methods used by ransomware (VPN.com,2020). As figure 4 shows, email links, email attachments and web application are the most used applications by ransomware.

Figure 4. Ransomware distribution methods

4. Related Studies

No doubt that ransomware is a new emergent and hot topic. Number of researchers who talk about ransomware is not great. In this section author will talks about up to date researches which talk about ransomware detection and prevention methods.

Jason Thomas (Jason Thomas,2019). In this research author explore different studies talk about ransomware attacks. Also, author discuss several issues about ransomware, at the end of this paper author demonstrates several methods to detect ransomware infection. Author in this research talks about manual method such as looking for file system and storage changes. Also, he talks about using applications and utilities such as anti-ransomware to help in detecting ransomware.

Hirra Sultan (Hirra Sultan,2018). In this research authors talk about the origin, evolution and growth of ransomware. Besides that, authors talk about different families of ransomware and preventing methods. Also, in this paper authors talk about several parameters which can contribute the growth of ransomware attack. At the end of this paper authors talk about awareness of users and how it is very important to reduce the possibility of ransomware attack.

Matthias Held (Matthias Held, 2018). In this thesis author talk about detecting ransomware. Author talks about general method for fighting ransomware. Also, author describes ransomware based on the behavior of the file destruction, extension of encrypted file, operation sequence, name and type of encrypted file. In this thesis author divides ransomware into three different categories: content based, meta-data based, and behavior based.

Gavin Hull (Gavin Hull,2019). In this research authors investigate 18 families of ransomware. Also, in this paper authors talk about creating a model for categorizing ransomware. Based on behavioral characteristics, Authors say that categorizing ransomware can lead to improve ransomware detection. Results in this research validate the importance of backup as a mandatory to reduce the effect of ransomware.

Jesper Christensen (Jesper,2017). In this thesis a tool to detect and minimize ransomware effect is created. This tool contains different methods of detection for ransomware. Experiments in this thesis are conducted using virtual machines. Also, 65 different types of ransomware are used. Experiments shows that tool crated is 77% active in all cases.

Barış Celiktaş (Barış Celiktaş,2018). In this thesis author talks about different methods to detect ransomware such as signature-based, anomaly-based. Using signature-based ransomware detected by signature information. In anomaly based several rules are set to determine whether the software is harmful or not. Results of this thesis indicated that using only signature-based methods will fail to detect and prevent ransomware. Author design a tool to detect abnormality and then provide an early warning to the user.

5. Recommendation for Ransomware Detection and Prevention

Knowing that the potential cost of ransomware cost is high, a normal question is whether it is possible to identify or detect a ransomware before infection. If users or organization can predict or identify ransomware it is possible to prevent from ransomware. Author in this section will talk about only windows machines. Beside general note to protect against any malicious attach such as update your operating system regularly, run schedule scan, in this section author will demonstrate up to date notes and recommendation for ransomware detection and preventing.

5.1 Monitoring File Activity and Event Tracing

Detecting ransomware can be done by monitoring file system activity. The System Service Descriptor Table (SSDT) is a table that contain information about the service tables which used by operating system for dispatching system calls. By filtering out process name and id, it could be possible to identify suspicious requests. One importance thing to mention here is that, if a log of the SSDT calls is done, it is possible to remove ransomware spread. This is done by shut down all related process (Jesper,2016 Matthias,2018; Brandon Lee, 2019). CyberPoint (Ben Lelonek & Nate Rogers,2016) research team conduct a research in 2016 and present that ransomware can be detected by Event Tracing in windows operating systems. Their approach was based on analyzing the event generated by files such as read, write and change in size. They developed an algorithm to do this task. One major drawback of this algorithm is high number of false positive. Method of detection based on looking at changes in file size when compared to the original size. But the encrypted file size is depending on encryption method and in initial vector used. CyberPoint research team says that their method can detect, almost, every ransomware.

5.2 Honeypots

Honeypots is a decoy network system used to attract attackers and then to detect them. The idea of honeypots is place files on the network with the intention of trap the attacker. If the attacker access files of honeypot, the system will react and know that there is an intruder. This type of detection is more helpful for organization than individual. For many people detecting ransomware by honeypot may sound strange but it is a valid security measure.

5.3 Educate Users

Most cyber security attack, including ransomware, conducted on careless employees. Some employees may share password with family and friends, other may write it on a piece of paper on his office, and most employees use easy and predictable password. Author believes that many cyber-attacks can be prevented by educating and training user on security policy. In addition, users have a critical role in cybersecurity. Using security guidelines is very important in all organization. All organization must follow up a clear security strategy to protect against malicious software. For example, developing a security policy, training new employees, create a security-conscious culture, and monitoring the effectiveness of security policy.

5.4 Using Antiviruses

Antiviruses are most common techniques used to protect against malicious software. Several companies developed several anti-virus programs. Anti-virus programs work using several techniques such as heuristic detection method and signature-based detection (Jesper,2017). Every anti-virus has an its own database. When a file is examined, it is analyzed, and it is signature is compared to signature database. Some anti-virus analyzes the code itself in the heuristic module. Unfortunately, the problems of malicious program and ransomware are not completely solved with any anti-virus programs. Detecting ransomware using anti-virus are based on analysis of the ransomware behavior. Most anti-virus can detect ransomware, but it cannot stop it once it is taking control of your system. The answer for if antiviruses can stop ransomware? is yes and no, antiviruses can prevent many types of ransomware, but it cannot stop ransomware once it is taken control.

5.5 Machine Learning Methods

Machine learning is a branch of artificial intelligence. Machine learning methods used in several applications such as pattern recognition, text classification, decision making and spam detection (Adel Hamdan,2011; Raed Abu-Zitar,2011; Adel Hamdan,2016). Absolutely, detection of ransomware using machine learning methods can be done.

According to Jaimin Modi (Jaimin Modi,2014) network traffic can be divided into three categories which are connection based, encryption based, and certificate based. Based on analyzing these characteristics Jaimin explore a model for detecting ransomware.

Machine learning can be used and adapted to solve any problem. The challenge is how to use machine learning, and what is the suitable algorithms to hire. Detecting ransomware is a challenge which needs a method and tools for monitoring network and files activity. Author thinks that machine learning methods which based on learning by example, common patterns can be adapted and used for ransomware detection. By analyzing normal behaviors of ransomware creating a tool to predict ransomware is highly possible.

Subash Poudyal (Subash Poudya,2018) develop a reverse engineering framework for ransomware detection. This framework is based on acting multi-level analysis such as row binaries, assembly codes, libraries and function

call. Experiments results for ransomware detection varied between 76% and 97%. Authors in this research use eight machine learning classifiers.

6. Conclusion and Future work

In this work author talks about one the main threats which can affect all users and organizations. No doubt that ransomware is a very complicated malicious programs which may affect your device. in this research several studies about ransomware and ransomware protection are mentioned. Nowadays. Users and organizations use several methods, tools, and procedures to minimize the probability of ransomware attacks. According to several antiviruses' companies and according to up to date researcher who are talking about ransomware detection, there is no anti-virus, method, and tool guarantee to detect ransomware. Most of methods used to fight against ransomware success in detecting some types of ransomware and fails for detecting other types. most of researchers and companies demonstrate that there is no single method or tool guarantee to protect against ransomware. So, author conclude that, up to this moment, the best thing you can do to protect against ransomware is to consider a good backup strategy. Besides that, author think that because of the nature of ransomware, developing any active method to protect against ransomware mainly will be an artificial intelligent method. So, author future work will be adapting a machine learning method to detect ransomware.

References

A. Adamov. (2017). The state of ransomware. *Trends and mitigation techniques, 2017 IEEE East-West Design & Test Symposium, 00*, 1-8. https://doi.org/10.1109/EWDTS.2017.8110056

Adel Hamdan, & Raed Abu-Zitar. (2011). Spam Detection Using Assisted Artificial Immune System. *International Journal of Pattern Recognition and Artificial Intelligence, 25*(8), 1275-1295. https://doi.org/10.1142/S0218001411009123

Adel Hamdan, Tariq Alwada'n, & Omar Al-Momani. (2016). Arabic Text Categorization Using Support vector machine, Naïve Bayes and Neural Network, *GSTF Journal of Computing, 5*(1), 108-115. https://doi.org/10.7603/s40601-016-0016-9

A. Liska, & T. Gallo. (2016). *Ransomware: Defending Against Digital Extortion*, O'Reilly Media, Inc.

Barış Celiktaş. (2018). The ransomware detection and prevention tool design by using signature and anomaly-based detection methods, Istanbul technical university, Master Thesis, May 2018.

Ben Lelonek, & Nate Rogers. (2016). Make ETW Great Again. http://ruxcon.org.au/assets/2016/slides/ETW_16_RUXCON_NJR_no_notes.pdf. (Accessed Jan 1,2020).

Brandon Lee. (2019). *What is Ransomware?* The Major Cybersecurity Threat Explained, https://spinbackup.com/blog/what-is-ransomware-the-major-cybersecurity-threat-explained/. (Accessed Jan 1,2020).

Coveware. (2020). *Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate*. https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate. (Accessed Dec 1,2019). https://doi.org/10.1016/S1361-3723(20)30015-4

Cyber Threat Alliance. (2018). *Lucrative ransomware attacks: Analysis of the cryptowall version 3 threat*. Technical report, 2015. https://www.cyberthreatalliance.org/wp-content/uploads/2018/02/cryptowall-report.pdf. (Accessed Jan 1,2020).

D. Caivano, G. Canfora, A. Cocomazzi, A. Pirozzi, & C. A. Visaggio. (2017). Ransomware at X-Rays, IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 348-353. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.58

Gavin Hull, Henna John, & Budi Arief. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science, 8*(2). https://doi.org/10.1186/s40163-019-0097-9.

Hirra Sultan, Aqeel Khalique, Shah Imran Alam, Safdar Tanweer. (2018). A survey on ransomware: evolution, growth, and impact. *International Journal of Advanced Research in Computer Science, 9*(2).

Internet security threat report, 2019, Symantec, vol. 22. Technical report, Symantec, 2019. https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf. (Accessed Jan 1,2020).

IBM Ransomware. (2016). *IBM Study: Businesses More likely to Pay Ransomware than Consumers*. https://www-03.ibm.com/press/us/en/pressrelease/51230.wss. (Accessed Jan 1,2020).

Jaimin Modi. (2014). Detecting Ransomware in Encrypted Network Traffic Using Machine Learning, A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Applied Science in the Department of Electrical and Computer Engineering, B.Eng., Gujarat Technological University, 2014.

Jason Thomas. (2019). Enterprise Cybersecurity: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques. *Computer and Information Science, 12*(3), 2019. https://doi.org/10.5539/cis.v12n3p72

Jesper B. S. Christensen. (2017). Ransomware detection and mitigation tool, Technical University of Denmark, Department of Applied Mathematics and Computer Science, Master Thesis , 2017.

Jim Finkle. (2016). Ransomware: Extortionist hackers borrow customer service tactics | Reuters. URL https://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0X917X. (Accessed Dec 1,2019).

J. Wyke, & A. Ajjan. (2015). The current state of ransomware, December 2015, SophosLabs Technical Paper.

Kaspersky Lab. (2016). Kaspersky Security Bulletin, Story of The Year: The Ransomware Revolution, Report. https://media.kaspersky.com/en/business-security/kaspersky-story-of-the-year-ransomware-revolution.pdf. (Accessed Jan 1,2020).

KSN report. (2016). Ransomware in 2014-2016. Technical report, Kaspersky Lab, 2016 https://media.kasperskycontenthub.com/wpcontent/uploads/sites/43/2018/03/07190822/KSN_Report_Ransomware_2014-2016_final_ENG.pdf. (Accessed Jan 2,2020).

Matthias Held. (2018). Detecting Ransomware, University Konstanz, Faculty of Sciences Department of Computer and Information Science, Master Thesis ,2018.

McAfee. (2019). McAfee Labs Threat Report. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf. (Accessed Dec 1,2019).

Morgan, S. (2017). Cybersecurity Business Report. Retrieved from CSO:https://www.csoonline.com/article/3237674/ransomware/ransomware-damage-costs-predicted-to-hit-115b-by-2019.
https://www.researchgate.net/publication/334683080_Enterprise_Cybersecurity_Investigating_and_Detecting_Ransomware_Infections_Using_Digital_Forensic_Techniques. (Accessed Dec 1,2019).

Proofpoint. (2017). 2017 Q3 Threat Report. https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q317-threat-report_1.pdf. (Accessed January 1,2020).

Raed Abu-Zitar, & Adel Hamdan. (2011). Application of Genetic Optimized Artificial Immune System and Neural Networks in Spam Detection, *Applied Soft Computing, 11*(4), 3827-3845. https://doi.org/10.1016/j.asoc.2011.02.021

Subash Poudyal, Kul Prasad Subedi, & Dipankar Dasgupta. (2018). A Framework for Analyzing Ransomware using Machine Learning, 2018 IEEE Symposium Series on Computational Intelligence (SSCI). https://doi.org/10.1109/SSCI.2018.8628743

Vadim Kotov, & Mantej Singh Rajpal. (2014). In-Depth Analysis of the Most Popular Malware Families, Bromium, Understanding Crypto-Ransomware Report.

VPN.com, Malware, Adware, Spyware, and Ransomware: What Do These Terms Mean, https://www.vpn.com/guides/malware-adware-spyware-and-ransomware-what-do-all-these-terms-mean. (Accessed Jan 1,2020).