International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. VIII, Issue 9, Sep 2020

http://ijecm.co.uk/

RANSOMWARE OF THINGS: IT'S IMPACT ON ECONOMIC GROWTH AND DIGITAL SOCIETY

Romina MUKA
University of Tirana, Faculty of Economy, Albania
romina.muka@unitir.edu.al

Elira HOXHA
University of Tirana, Faculty of Economy, Albania
elirahoxha@feut.edu.al

Ledia MALEQKA
University of Tirana, Faculty of Economy, Albania
lmaleqka@gmail.com

Kozeta SEVRANI
University of Tirana, Faculty of Economy, Albania
kozeta.sevrani@unitir.edu.al

Abstract

In the recent years, the use of internet and computers has increased, and cyberspace has turned to be the pillar of economic development and digital society, but simultaneously cybersecurity incidents have increased fast in this thriving market. Adding to this the growth of Internet of Things industry, threats from new malware and infections will only increase in the future. One of the most laborious malware categories that has emerged in the last years is ransomware. This paper emphasizes the transition from traditional ransomware threats to new and more complex attacks creating Jackware, which is a type of ransomware designed to attack connected devices (Ransomware of Things), such as Wireless Body Area Networks (WBAN) in e-Health. Thus, the vulnerabilities found in WBAN systems caused from the ransomware, need

to be identified and analyzed. In this paper it is given a brief history of ransomware, its evolution, and some recent statistics and methodologies of ransomware attacks. There are discussed some future trends in terms of Ransomware of Things. Next it is highlighted the importance of security in IoT devices, especially related to e-Health data, from ransomware infection. This paper is an analytical security research on ransomware of things. There are reviewed facts and information already available to make a critical evaluation of the material. It has been used a deductive approach, and there are studied past records and other information sources, with a view to find the origin and development of the phenomenon and to discover trends in the past, in order to understand the present and to anticipate the future of ransomware of things security.
Keywords: Ransomware of Things, Economic Impact, WBAN, IoT, Jackware

INTRODUCTION

In the cyber world, increasingly sophisticated information security threats such as spyware, phishing, worms and other malware are putting in risk confidentiality, integrity, and availability of information. The main purpose of the vast majority of threats is to make money from the victims. Recently, a new form of malware has emerged and has drawn attention among researches and information security specialists. Ransomware is a type of malware for financial gain that denies or limits users from accessing their computer and files. It demands the victims to pay the ransom through certain online payment methods to grant access to their computer, or to get their files in original condition.

There are two basic types of ransomware attacks, Crypto and Locker ransomware. Crypto ransomware applies an algorithm to encrypt the data and files, making it unusable without the decryption key. The other attack is locker ransomware, designed to lock the files and applications, preventing victims from using it (Savage, Coogan, Lau, 2015). Locker ransomwares are having a boom in wearable devices and the Internet of Things (IoT). The next wave of ramsomware is called Jackware, which is seen as a specialized form of ransomware (Cobb, 2016). Jackware is a malicious software that seeks to take control of a device until the user pays up. The IoT ransomware, or ransomware of things (RoT) is fundamentally different from the computer ransomware, but no less dangerous. Millions of connected devices are potentially at risk from this type of ransomware.

Moreover ransomware is being transformed as a service. Ransomware as a service is a variant of ransomware designed to make cybercrime accessible to anyone even with limited cyber knowledge (Salvi, Kerkar, 2016). While ransomware attacks are increasing in

sophistication, that does not mean victims are powerless. There are many steps to be taken to prevent ransomware attacks.

The purpose of this paper is to emphasize how ransomware is evolving and could potentially take over every single device. It will be organized in 4 parts. Section 2 will give a brief overview on related work regarding RoT security analysis, while section 3 will address the techniques of ransomware infections and some recently attacks. Section 4 will discuss the future trend of ransomware, Jackware and the importance of security on Internet of things from this attack. Section 5 will propose a recommendation how to prevent ransomware attacks, and finally concluding with Section 6, where conclusions are drawn for RoT security.

RELATED WORK

Ransomware first appeared in 1989 as AIDS Trojan, and has remained discreet until 2005 when in Russia, the first cases of the attack led to substantial monetary loss (Kaspersky lab, 2016). Kharraz et al. (2015) in their study have observed that the way malicious processes generate requests to access file systems was significantly different from benign processes. In the paper of Kalaimannan et al. (2017) is stated that ransomware is undoubtedly emerging as a serious threat to home users, information security professionals, researchers with the advent of cybersecurity technology and explosion in growth of the Internet of Things. Using infected IoT devices to extort commercial websites by threatening a DDoS attack, or locking IoT devices in order to charge a ransom is something called jackware (ESET,2016).

Attackers demand a ransom to provide instructions on how to decrypt files or drives, but Trend Micro research (2016) showed 1 in 5 companies in the United Kingdom (UK) who paid the ransom after an attack, never recovered the data. Ransomware attacks are usually effective because of the anxiety caused by infection and fear of losing access to files if the victim does not pay the ransom (Hammill, 2017).

Luo and Liao (2007) have stated in their paper that the key to prevent ransomware is to promote the awareness education of corporate employees, management, individual users and small business owners. Another approach to managing ransomware, a socio-technical one, is that of incorporating NIST (National Institute of Standards and Technology) Cybersecurity Framework Core concepts in an eight-dimensional model related to healthcare organization, as proposed by Singh and Sitting (2016).

RANSOMWARE ATTACKS AND TECHNIQUES

The main purpose of ransomware attacks is to extort money from their victims, but they are quite different on how they work technically and operationally. The Ransomware either locks the

computer to prevent normal usage or encrypts the documents and files on it to prevent the access to them. Victims typically get effected by ransomware by opening an infected email attachment, internet traffic redirection to malicious websites, sms messages or drive by downloads. Most commonly, victims are asked to transfer a sum of bitcoins to the cyber attacker anonymous bitcoin address. In terms of their origin, development and malicious consequences, ransomware can be categorized in Scareware, Locker ransomware and Crypto ransomware.

a. **Scareware** is a type of malware that appears as a pop-up window on a computer to trick victims into buying and downloading unwanted software, such as fake antivirus. Ransomware is considered a scareware as it uses social engineering to scare users to pay a fee or ransom. This shock and anxiety continued to victims until they became aware that these applications were more fictional than abolishing. The first attack of this kind was Quickshiel (Securelink Networks, 2005).

b. The next major change for ransomware happened in 2009 (Kalaimannan et al., 2017) when the attack locked the computer and prevented access to the system and files. During the execution of the **locker ransomware**, a message is displayed, which usually states the victim has committed some offense such as viewing or downloading illegal content and the victim needs to pay a fine to regain access. Locker ransomware uses social engineering techniques such as intimidation, confusion, shaming and fear to persuade the victim into paying the ransom. Locker ransomware gains access to the victims machine, upon a click by the user on a malicious link. This attack peaked during 2011 and 2012 and Reveton and FBI Moneypack were some of the variants of this attack that emerged in 2012 (Kalaimannan et al., 2017). However, this form of ransomware faced a severity decline when the public was made aware of the fact that the actual malware was removable.

c. Moreover, ransomware codes have become more sophisticated and shifted from basic programs to well-designed **crypto ransomware**. A crypto ransomware is a type of malware that encrypts users data. Data access is restricted until a ransom is paid to decrypt it (Richet, 2015). The developers of crypto ransomware know that data on computers are very important to users and they may be desperate to get their data back, preferring to pay the ransom to restore access and avoid painful consequences. Its goal is to stay unnoticed until it can find and encrypt all of the files that could be important and valuable to the user. What makes it stand out is the fact that this malware is polymorph, the code changes each time it runs and it is different for each infected host.

Ransomware attack methods have advanced in techniques and increased in profit in past few years. Affiliate systems and Ransomware as a Service (RaaS) are part of a new cybercriminal

model. Advanced cybercriminals create the malicious code and then offers it for free of charge or a small fee to download and use. Everyone, no matter how limited their programming mastery is, can access these codes and conduct an attack. This incentivizes a higher volume of attacks and higher ransom requests. Ransomware is cheap to purchase and download. It is also easy to spread and people don't need to be information security specialists or have expensive equipment. This means more and more cybercriminals are turning to this type of misconduct. It offers a quicker payout than stealing credit card data or personal information and the most important thing is that, there is a lower risk of being caught due to the anonymity of bitcoin.

Ransomware criminals business model will fail if word gets around, that they do not deliver the decryption code once the ransom is paid. In preventing this, some ransomware schemes try to build trust by decrypting a few files before the ransom is paid (Richardson and North, 2017). The newest versions that emerged in 2017 is the WannaCry ransomware attack that was a worldwide cyberattack, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in Bitcoin. The attack began on Friday, 12 May 2017, and within a day was reported to have infected more than 230,000 computers in over 150 countries (US-CERT, 2017).

RANSOMWARE OF THINGS (RoT)

2016 has been referring as The Year of Ransomware by IT security analysts, but soon it will be known as The Year of Jackware. Initially, ransomware was a problem for the windows users and then it moved to apple and android systems. The growing use of the Internet of Things has redirect ransomware to the IoT as well. Considering the past as well as the future growth of the internet based applications, an additional threat will appear to the connected devices. According to the Institute for Critical Infrastructure Technology (ZDNet, 2017), IoT is especially at risk for malware attacks. The most important reasons why the Internet of Things is at risk for ransomware are the growth of IoT, the evolution of ransomware, and the unawareness of the end users.

Many of the IoT devices in use today are inadequately secured, leaving organizations vulnerable to attacks. This is an immediate issue impacting organizations today. ESET Senior Security Researcher, Stephen Cobb (2016) has predicted the creation of jackware in 2017, a ransomware capable of taking over an internet connected vehicle or other Internet of Things (IoT) devices. According to a report from Hewlett Packard Enterprise (2016), half of interviewed (52 percent) feel external attack as the greatest threat to their IoT systems, and shockingly, 84 percent have already experienced an IoT related breach. The most common breaches were a result of malware (49 percent), spyware (38 percent) and human error (38 percent). The goal of

jackware is not data processing or digital communications, but to lock up a car or other devices until you pay up. The effect of ransomware to IoT may be different from those found on traditional devices. When ransomware hits a computer, it only affects data on that device or network, meanwhile with IoT, it can put physical functions inaccessible. For example, a ransomware that infects a smart thermostat can turn up the heat to full unless a ransom is paid (Fitzpatrick and Griffin, 2016). Smart cars and even smart cities may be the target of ransomware and the impact of ransomware on such utilities can threaten life.

As a result of this new threat landscape, its important for buyers to be more astute in their purchasing choices. Before buying and using a smart device, they should assess the risk of compromising, and evaluate how easy it is to harden the product (e.g., changing default credentials and disabling insecure protocols). They should also have recovery plans in place, so they are prepared in the event their device does become infected. After all, in a world where it is no longer a question of if an attack will happen, but when, being able to rapidly detect and respond to it is the best approach to mitigate its impact. Mobile and IoT applications continue to be released at a rapid pace to meet user demands. If security is not designed into these apps there could be significant negative impacts (Kelley, 2017).

RECOMMENDATIONS

It is always difficult to predict the future development of ransomware. One way to do it, is by estimating the future, based on past models. Nowadays we might have heard about the term of ransomware a lot, but we are not very conscious about it. The ransomware represent a threat for everyone, given the nature that they have and the new ransomware families that are being created. Luo and Liao (2007) have proposed a framework with four steps to prevent ransomware:

- Policy, procedure, regulation
- Access Control and Management
- Exposure Analysis and Report
- Awareness Education and Training

It is important for people to understand how their behavior affect the company, costumers and themselves. In this way they are going to be more cautious in the aspect of information security. According to Nanded (2016), there are some recomandations that should be adopted in order to prevent ransomware infections:

- Take regular backup of files and data.
- Keep security software up to date.

- Always be cautious by avoiding downloading email attachments from untrusted sources and clicking on links from email.
- Use reputed antimalware/antivirus and Scan systems regularly.
- Use strong firewall.
- Enable popup blocker.
- Train and educate employees.

CONCLUDING REMARKS

This paper presents a comprehensive overview of origin, evolution and malicious effects of ransomware. Ransomware is emerging as a serious threat to both information security professionals and researchers, as the encryption methods combined with social engineering are reaching the limits of modern cryptography. It has become a profitable business for cyber-criminals and for other people too, with the evolution to ransomware as a service. It is affecting the economic growth and the digital society.

As mentioned by Hernandez-Castro et al., (2020) ransomware is likely to become more costly to society because of the increase of the ransom demands. It is difficult to determine the optimal ransom for attacks, but as shown by a Symantec report (O'Brien, 2017) the average ransom demand during 2016 increased dramatically from $294 (in 2015) to $1,077. Then in 2017 it decreased to $544 which although it is less than the year before it is a considerable value (85 percent up from 2015). This ransom demand might not look a lot even to small businesses, but big organizations should keep in mind that this value is for only one device. When the ransomware affects hundreds of devices the total amount is far more substantial and it doesn't stop there. It can also result in reputational damage caused by the significant disruption of the attack, which give rise to lost productivity, unfulfilled deadlines and cleanup costs. Moreover, as a result of these kind of breaches or attacks often many small businesses go bankrupt.

Anyway it is difficult to estimate the total cost of these and other attacks especially because many data breaches can go undetected, often not reported, or their final cost is unknown. According to the evidences reported by CEA (2018) it turns out that the damage to the US economy from cyberattacks in 2016 was $57.1 billion, representing 0.31% of that year's GDP. Of course part of this, is related to ransomware attacks that can have a big economic impact especially when the attack deviate from the original target to economically related firms and magnifying thereby the damage to the economy. It is also reported that cyberattacks in businesses related to infrastructure sectors may cause large negative spillover effects to the wider economy.

Also, there are discussed some future trends of ransomware. The growth of the wearable market like Wireless Body Area Networks (WBANs), IoT and several other technological trends has allowed cybercriminals to target new areas with malicious software. So, the mayor concern for all is the attention to security. This is a challenging task and we all have a role to play in it. It is not enough anymore to consider the normal use cases while creating new software or products. Security improvements and taking malicious scenarios in consideration should be now the major challenge for product designers.

All the basic security practices should be considered such as avoiding clicking links or attachments that may be of malicious origin and patching exploitable software vulnerabilities. We need to take precaution steps for preparing and eventually minimizing the danger from these ransomware attacks. The most important issue is the awareness education of corporate employees, managers as well as individual users and small business owners for security. The future will lead to studies focused on the behavior of the home and organizational users, considering the effect of the ransomware on them. The studies themselves will offer the chance of designing more efficient security solutions that are able to resist against ransomware of things.

REFERENCES

Chase, J. (2013). The evolution of the internet of things. Texas Instruments, 1, 1-7.

Cobb, S. (2017). RoT: Ransomware of Things.

Fitzpatrick, D., and Griffin, D. (2016). Cyber-extortion losses skyrocket, says FBI. CNNMoney, (15 April 2016). Available at http://money. cnn. com/2016/04/15/technology/ransomware-cyber-security.

Hammill, A. (2017). The rise and wrath of ransomware and what it means for society (Doctoral dissertation, Utica College).

Hampton, N. and Baig, Z.A., (2015). Ransomware: Emergence of the cyber-extortion menace.

Hernandez-Castro J., Cartwright A., Cartwright E. (2020). An economic analysis of ransomware and its welfare consequences. R. Soc. open sci. 7: 190023. http://dx.doi.org/10.1098/rsos.190023.

Kalaimannan, E., John, S.K., DuBose, T. and Pinto, A., 2017. Influences on ransomwares evolution and predictions for the future challenges. Journal of Cyber Security Technology, 1(1), pp.23-31

Kavya, D. (2017). Ransomware of Things (RoT). Fuzzy Systems, 9(2), pp.29-32.

Kenyon, B. and McCafferty, J. (2016). Ransomware Recovery. ITNOW, 58(4), pp.32-33.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015, July). Cutting the gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 3-24). Springer, Cham.

Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. Information Systems Security, 16(4), 195-202.

Luo, X. and Liao, Q. (2009). Ransomware: A new cyber hijacking threat to enterprises. In Hand-book of research on information security and assurance (pp. 1-6). IGI Global.

O'Brien, D. (2017). Ransomware 2017: An ISTR Special Report. Internet Security Threat Report ISTR, July 2017.

Packard, H. (2018). The Internet of Things. Today and Tomorrow.

Pathak, P.B. and Nanded, Y.M. (2016). A dangerous trend of cybercrime: Ransomware growing challenge. International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 5(2).

Richardson, R. and North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. In International Management Review, 13(1), p.10.

Richet, J. L. (2016). Extortion on the internet: the rise of crypto-ransomware. Harvard.

Salvi, M. H. U., & Kerkar, M. R. V. (2016). Ransomware: A cyber extortion. Asian journal for convergence in technology (ajct), 2.

Savage, K., Coogan, P., & Lau, H. (2015). The evolution of ransomware. Symantec, Mountain View.

Sittig, D.F. and Singh, H. (2016). A socio-technical approach to preventing, mitigating, and re-covering from ransomware attacks. Applied Clinical Informatics, 7(2), p.624.

The Council of Economic Advisers – CEA. (2018). The Cost of Malicious Cyber Activity to the U.S. Economy, February 2018. Thompson Hine LLP. Privacy & Cybersecurity Update.

PhD Candidate Romina Muka holds a bachelor's degree in Business Informatics and a Master of Science in Information Systems in Economy from University of Tirana (UT), Albania. She is also a lecturer at UT since 2015. Romina has been a guest lecturer in several international universities in Europe, and has been the contact person of different projects funded by Erasmus+, Interreg IPA BCC, Ministry of Science and Education in Albania, and Industry. Her research interests include security of WBANs in IoT and optimal deployment of sensors and controllers for the operation of the smart distribution grid.

Dr. Elira Hoxha graduated in 2008 from the University of Tirana, Faculty of Natural Sciences, with a 5-year degree in Computer Science and later in 2011 with a Master Degree in Advanced Informatics from the same University. Experienced in web development and computer programming. Currently working as a lecturer at University of Tirana, Faculty of Economy, Department of Statistics and Applied Informatics. Responsible for teaching Database Systems, Software Engineering and Artificial Intelligence. Since June 2014, holds a PhD diploma in Information Systems, with a thesis in the field of Semantic Web Services.

M.Sc. Ledia Maleqka is a Business Analyst with almost three years of experience. She is also an assistant lecturer at the Faculty of Economy, University of Tirana. Ledia holds a Master of Science Degree in Information Security and a Bachelor Degree in Business Informatics. She is currently focused in gaining deep and comprehensive knowledge related to the field of Business Analysis.

Prof. Dr. Kozeta Sevrani has graduated the Faculty of Natural Science in 1984. She is a Professor of Computer Science and Management Information Systems at the Faculty of Economy, University of Tirana, Albania. Her research interests include: information security; data science; digital divide; issues and solutions in building information infrastructure, e-business, e-learning, e-government/e-business and e-services in developing countries, particularly in Albania. She is in the Editorial Board of several international journals and does an extended work in consulting private companies and government agencies in Albania. Also, she has presented her work in numerous national and international conferences. Her work has been published in several journals and she has co-authored four one monograph and four books. Professor Sevrani has been awarded many important prizes among them "The Academic of the Year" from the ICT Award Albania in 2014. She is currently the head of Statistics Council of Albania and Head of Commission for promoting academic titles in University of Tirana.