RansomBuster IoT: A Intrusion Detection and Dataset Creation Tool for Ransomware Attacks within IoT Networks

Jackson M. Walker

Christopher Newport University

RansomBuster IoT: A Intrusion Detection and Dataset Creation Tool for Ransomware Attacks within IoT Networks

Jackson M. Walker

Christopher Newport University

COVA CCI Cybersecurity Undergraduate Research

Abstract

The proposed research follows the design-science guidelines(Hevner, 2004). This paper uses these design-science methods for developing the guidelines for the implementation of the proposed architecture, understanding previous research contributions, and evaluating of research. This paper proposes a network artifact for studying ransomware IoT intrusion detection techniques and offers a proposed network architecture to serve as a framework for creating a publicly available dataset for IoT research on ransomware.

Keywords: IoT, Ransomware

Introduction

Internet-of-things (IoT) devices are becoming more utilized and depended upon in all aspects of life(Zanella et al., 2014); however, IoT devices are notorious for lacking basic security mechanisms and being vulnerable to cyber attacks. IoT devices are notorious for being vulnerable to malicious software, eavesdropping, and man-in-the-middle attacks(Meneghello et al., 2019). In 2014 a massive Cyber attack was conducted against the American Department Store Target "*intruders had pushed their malware to a majority of Target's point-of-sale devices, and were actively collecting card records from live customer transactions - Target has said that the breach exposed approximately 40 million debit and credit card accounts between Nov. 27 and Dec. 15, 2013 - Sources close to the investigation said the attackers first broke into the retailer's network - using network credentials stolen from - refrigeration and HVAC systems*(Fiorillo, 2014)." The attackers used the IoT device functionality of the air vents within the building as an access point or *beachhead* for entry into the network.

When launching an attack, hackers knowingly seek out IoT technologies first. This is due to the likelihood of a targeted network not only having a device but additionally having a device with an easily exploitable vulnerability. This risk probability is statistically very high "*70% of IoT products contain security vulnerabilities, and, on average, there are 25 vulnerabilities per device* (Miao, 2020)." This is a frequent trend in IoT security that is especially likely to continue. In years past, ransomware did not typically target IoT devices; however, in recent years, Ransomware attacks in the IoT realm have increased. Currently, there is very little research on ransomware in the IoT context, with many existing works using inaccurate or outdated datasets. The Internet of Things' unique attack surfaces and security concerns make IoT extremely vulnerable to ransomware, and thus, the investment into security solutions has to develop immediately. Machine Learning has become the industry standard for studying malicious software and developing intrusion detection systems(Oz, 2022). This paper proposes a network device for studying ransomware IoT intrusion detection techniques and serves as a framework for creating a publicly available dataset for IoT research on ransomware.

Problem Statement:

The Internet-of-things(IoT) is a growing portal for Ransomware attacks against professional organizations. Ransomware, a type of malware, is currently the biggest security threat faced by organizations today. Ransomware attacks in the IoT realm have increased. Currently, there is very little research on ransomware in the IoT context, with many existing works using inaccurate or outdated datasets. The Internet of Things' unique attack surfaces and security concerns make IoT extremely vulnerable, and thus, the investment into security solutions has to develop immediately. Machine Learning has become the industry standard for studying malicious software and developing intrusion detection systems. This paper proposes a network device for studying ransomware IoT intrusion detection techniques by utilizing port mirroring coupled with a heuristic security analysis approach to detect malicious network activity. This paper also serves as a framework for creating a publicly available dataset for IoT research on ransomware.

Internet of Things: Security Vulnerabilities

The Internet of Things refers to the network of interconnected devices that can process and send data using the internet(Zanella, 2014). IoT is typically classified into either Industry level or Consumer(commercial) devices(Strous, 2020). Consumer-level devices refer to smart home devices like smartwatches, with industry-level devices referring to factory automation systems and healthcare systems. The core security problem associated with IoT resides in the design of these devices.

Due to the nature of their design, it is inherently difficult to implement basic security features since most devices lack the basic system resources required to run many standard security protocols(Meneghello, 2019). Device manufacturers almost always prioritize the low-cost, ease-of-use, and functionality these devices are known for in favor of the personal well-being and data confidentiality and integrity of the consumer (Meneghello, 2019). This has made IoT devices prime targets for malicious actors.

This abundance of security vulnerabilities and flaws inherent to IoT technology makes them especially vulnerable to attacks. IoT devices are built to get the most out of their limited hardware and firmware in order to fulfill their basic functionality with little room for anything else. Most IoT devices today either completely lack security mechanisms or can only support very lightweight functions. Like a cheap sports car choosing not to have airbags to keep the price as low as possible; or an expensive race car choosing to ignore features like air conditioning to maximize performance. This is further exacerbated by the fact that 99 out of 100 devices on a network are patched and can defend against a possible threat, but if one cannot, the entire network is compromised. Most notably, IoT devices typically any form of lack intrusion detection systems(IDS) and any means of notifying end-users if malicious activity is detected(Meneghello, 2019). Factors such as device heterogeneity and lack of resources make the attack surface for a typical IoT device extremely unique. This means that in many cases, the evolution of security defense mechanisms that took place with network technology of the past is unable to provide solutions within the IoT context. Specifically, things like intrusion detection systems(IDS), threat mitigation, deep packet inspection, and higher-level encryption are all things that are nearly impossible to be provided by a typical IoT device.

IoT device developers also often lack the necessary skill and expertise to implement these features or design devices with these functionalities in mind from the ground up(Meneghello, 2019). Many device manufacturers specifically hire developers focusing on development, not security. This often leaves security as an afterthought in the development life-cycle of these devices. Since there is a lack of basic/standard security practices with IoT, device developers and manufacturers are not required or obligated to provide security functionality for these devices. This is because the inherent security risks associated with these devices are with the consumer or user of these devices rather than the manufacturer.

In many cases, these exploits or security vulnerabilities are impossible for a device to detect or mitigate independently, often due to a lack of resources. Specifically, things like intrusion detection systems(IDS), threat mitigation, deep packet inspection, and higher-level encryption are all things that are nearly impossible to be provided by a typical IoT device. Industry-level systems have third-party hardware developed by companies like Cisco to serve a similar purpose. To address these concerns, companies will implement security protocols to prevent attacks and design their devices and networks to limit their attack surface. Despite this, it is still extremely difficult to prevent security failures within IoT. The emergence of new technologies, many of which are built on the foundation of wireless, “always online” principles, leads to new life-threatening security vulnerabilities that have not been previously encountered at this magnitude. While the idea of a deadly cyber-attack occurring on a self-driving car or drone is obvious, attacks on needed infrastructures like disaster monitoring technology, missile defense systems, and water treatment facilities are less-so and even more dangerous. During the global

2020 Covid-19 pandemic, attacks against healthcare organizations drastically increased, likely because of the increased reliance on healthcare providers. It was during this time period that a piece of ransomware called Corona began targeting hospitals and encrypting the health records of patients. Also, during this time period, the major US hospital chain Universal Health Services, had computer systems in over 400 locations failing, leaving medical staff to work with "Pen and Paper(Collier, 2020)." In 2017, hackers working for the North Korean government used a ransomware attack called WannaCry that hit "at least 80 medical facilities(Collier, 2020)." against the United Kingdoms National Health System. It should be noted that in this context, the attackers were not targeting the UK National Health System.

Ransomware: Evolution

Ransomware refers to a subset of malicious software(malware) that is designed to restrict access to a system or data until the victim of the attack has paid a specific monetary amount(Oz et al., 2022). The main goal of ransomware is the extortion of money from the victim of an attack. While the malicious software of ransomware as a concept has been around since 1989, the emergence of cryptocurrencies in 2009 has undoubtedly led to the rise in its use and development. Until 2009 the biggest roadblock in the way of ransomware development was the ability for ransom payments to be made in a way that could guarantee anonymity to the attacker(Oz et al., 2022). This, coupled with the decades of experience malicious actors have had to diversify network intrusion and strengthen encryption techniques, has enabled ransomware to be as lucrative as it is. Currently, if an attacker is successful at locking a victim's systems, it is nearly impossible to recover any data without paying a ransom(Oz et al., 2022). These attacks are even further motivated by the fact that it is extremely common for victims of ransomware attacks to pay the attackers. This phenomenon has even caused a rise in

Ransomware-as-a-Service(RaaS), where malicious groups offer either their services or their ransom software to be available as a purchasable service(Oz et al., 2022).

In years past, ransomware did not typically target IoT devices since typical network devices and infrastructure were already vulnerable enough. However, in recent years Ransomware attacks in the IoT realm have increased, likely due to a greater emphasis on security professionals developing ways to defend themselves against families of malware and the increasingly widespread adoption of IoT. This makes way for a "perfect storm" of security vulnerabilities. The abundance of security vulnerabilities and flaws that are inherent to IoT technology makes them especially vulnerable to Malware attacks. Most IoT devices today either completely lack security mechanisms or can only support very lightweight functions. Incidentally, they also typically lack intrusion detection systems and any means of notifying end-users if an intrusion is detected. These factors are exacerbated by IoT heterogeneity, lack of resources, and widespread usage across all avenues of technology. This means that in many cases, the evolution of security defense mechanisms that took place with network technology of the past is unable to provide solutions within the IoT context. Furthermore, IoT is expected to grow and become even more widespread regardless of security threats due to the emergence of technology such as drones, self-driving cars, smart technology, and artificial intelligence. These new technologies not only create new targets for malicious activity but represent a new, more dangerous threat landscape.

Gap in Research:

Currently, little work exists to study ransomware within the IoT realm. This is worrying since most security mechanisms and solutions cannot be adopted due to the unique security problems presented by IoT. The exponential growth of Ransomware attacks and their devastating efficiency has led to many organizations and researchers contributing to studying ransomware and possible solutions. However, very few research articles or conventions currently exist specifically in the IoT context, with many either briefly mentioning IoT or not mentioning it at all. The unique attack surface and security concerns stated previously make IoT extremely vulnerable, and thus, the investment into security solutions has to develop immediately. Ransomware attacks in the IoT realm have increased, likely due to a greater emphasis on security professionals developing ways to defend themselves against families of malware and the increasingly widespread adoption of IoT. This makes way for a "perfect storm" of security vulnerabilities.

Argument

A tool must be created for commercial users of IoT in order to ensure the security of their own devices against Ransomware attacks. This paper proposes an artifact that is designed to collect data from IoT devices operating within an organization's network. The goal behind the device is to utilize **heuristic analysis** to identify potential malicious network traffic and prevent malware from spreading throughout a network using IoT devices. The device will use **port mirroring** to collect data from IoT devices so that it can analyze and serve as a third-party IDS. This paper also proposes a network architecture modeled after a typical organization to function as a sandbox or laboratory setting. This is done to provide the most accurate context for data collection. The artifact is to be implemented with the proposed network architecture to study ransomware attack patterns, packet signatures, and network activity on IoT devices. I argue that my proposed hardware/software-based solution will provide an active and effective framework for studying polymorphic malware, specifically ransomware. I also argue that the proposed framework will serve as an effective starting point for developing a specific solution to find out how effective many of these techniques are at detecting ransomware infecting IoT devices. The effectiveness of the proposed device is then to be tested by using it in the sandbox network environment. A **heuristic** approach utilizes network data collected through device port mirroring in order to determine if malicious activity is occurring. By implementing a system that is able to actively monitor the network for malicious activity, it is possible to stop ransomware infection at the source.

Problem Relevance:

IoT devices are integrated into everyday life and are increasingly mandatory as they provide a wide array of services for users and businesses. "*IoT, IoMT and OT devices combined represent 44% of the total devices in enterprise networks*(R4iot, 2022)." IoT is expected to grow and become even more widespread in usage due to the emergence of technology such as drones, self-driving cars, smart technology, and artificial intelligence. IoT has only just started to become a target of ransomware attacks and is only expected to grow as an even greater target due to the inherent security vulnerabilities of IoT. This is exacerbated by the fact that these new technologies create new targets for malicious activity and represent a new, more dangerous threat landscape widening the attack surface for organizations.

Ransomware represents one of the most rampant and dangerous issues plaguing society in the 21st century. The threat of ransomware has grown exponentially in the last decade, making it the number one cyber threat in the world. Ransomware now threatens every avenue of society that utilizes interconnected systems, including government agencies, businesses, and individuals(Oz et al., 2022). The 2015 Cybersecurity Summit held "*C-Level & Senior Level Executives responsible for protecting their companies' critical infrastructures - and renowned* *information security experts*(2015).” The Assistant Special Agent who oversaw the FBI’s Cyber and Counterintelligence Program, when speaking on ransomware, advised organizations to pay the criminals who launched the attacks. Bonavolonta essentially explained that ransomware was so effective that efforts by the FBI and others to mitigate these threats had failed. Bonavolonta is quoted saying, “*The easiest thing may be to just pay the ransom*(Bisson, 2015).” because certain families of ransomware had become too advanced in their encryption techniques. Unfortunately, that threat has only increased substantially.

Literature review

The research done in this paper is based on the latest findings from a variety of sources, such as IoT security papers, IoT security surveys, and professional Malicious threat reporting organizations. In this paper, I argue that, given the current state of research, ransomware is the most prevalent threat to organizations.

Many have researched ransomware and the security of IoT devices; however, very little research has been done on ransomware infecting IoT devices. The research survey *Internet of Things security: A survey* published in 2017 presents a review of major security concerns in the IoT realm. The survey means to classify IoT devices based on the context of deployment. The survey also proposes a possible solution structure to overcome security issues in the IoT environment. They argue that "we believe that the IoT applications can be secured through adopting a universal IoT security architecture(Alaba, 2017)." Basically, arguing that developing a generic security solution for a wide range of IoT applications that is backward compatible with existing solutions is the safest approach. This survey points out some of the specific challenges and security concerns within the healthcare sector.

The *Internet of Threats* is a research article published in 2019 that mainly focused on Consumer(Commercial) IoT. Gives a brief overview of some of the industry and cultural security challenges unique to IoT devices. This paper describes and classifies the general attack service of IoT devices. Includes a taxonomy of what type of attacks and challenges these devices face within each layer and some general solutions that have been developed to address some of these concerns. Finally, this article describes open research challenges within the realm of cybersecurity. Talks about Zigbee, BLE, 6LoWPAN etc. This paper fails to specifically address the threat of malware against IoT devices.

Newer research publications have begun to address the greater security concerns and lack of research on ransomware within the IoT setting. *A survey on Ransomware: Evolution, Taxonomy, and Defense Solutions* serves as an excellent research survey published in 2022(September) that covers various(137 sources) literature on ransomware between 1989-2020. Gives a detailed overview of the evolution and history of ransomware and notable ransomware families. Provides a holistic analysis of the current trends, characteristics, and taxonomy of ransomware. Includes an extensive overview of ransomware defense research and open research problems. Out of the 132 research articles and conferences referenced in the survey, only five sources include ransomware within the IoT/CPS realm, with four of the five only providing "partial information(Oz, 2022)." Highlights specifically the growing threat of ransomware in the IoT setting, emphasizing the lack of research on the topic.

R*4iot: Next Generation Ransomware* is a professional report generated by Vedere Labs. Motivated by the need for a study of specific IoT-based ransomware. Highlights many of the possible avenues of IoT attacks, providing a demonstration of IoT exploits coupled with ransomware software. Providing a framework and guide for securing organizational networks against ransomware attacks. Specifically focuses on healthcare systems and the technology commonly used in that context. However, despite these new revelations and a slightly greater push into the study of ransomware's effect on networks, one of the biggest research challenges within the IoT realm is the lack of relevant and accurate datasets using real IoT devices and ransomware families. Machine Learning is the most admired technique for detecting ransomware across all technology platforms, with a total of 72% of defense solutions using machine learning to detect ransomware within systems(Oz, 2022). However, past IoT Malware research uses obsolete datasets that don't accurately reflect actual IoT network data or realistic networks. "Since ransomware detection for IoT/CPS environments is not a well-explored field of research, there are only five studies tackling the ransomware detection problem in such environments - For the evaluation of the proposed detection systems, the majority of the studies did not report any data sources. Similarly, most of the studies did not report the number of ransomware families in their datasets(Oz, 2022)."

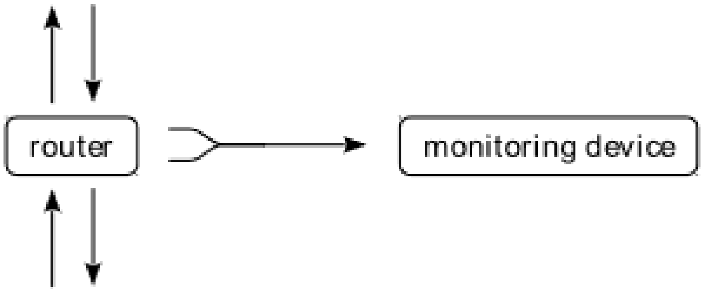
In order to effectively study the use of ransomware in an IoT environment, it is important to conduct studies within a network that accurately represents real IoT protocols and technologies. Due to the constant evolution of ransomware, it is also imperative that the use of real ransomware families is used in any study on ransomware in the IoT context. Studies should also factor in the resource constraints and unique network capabilities presented by IoT devices.

Methodology

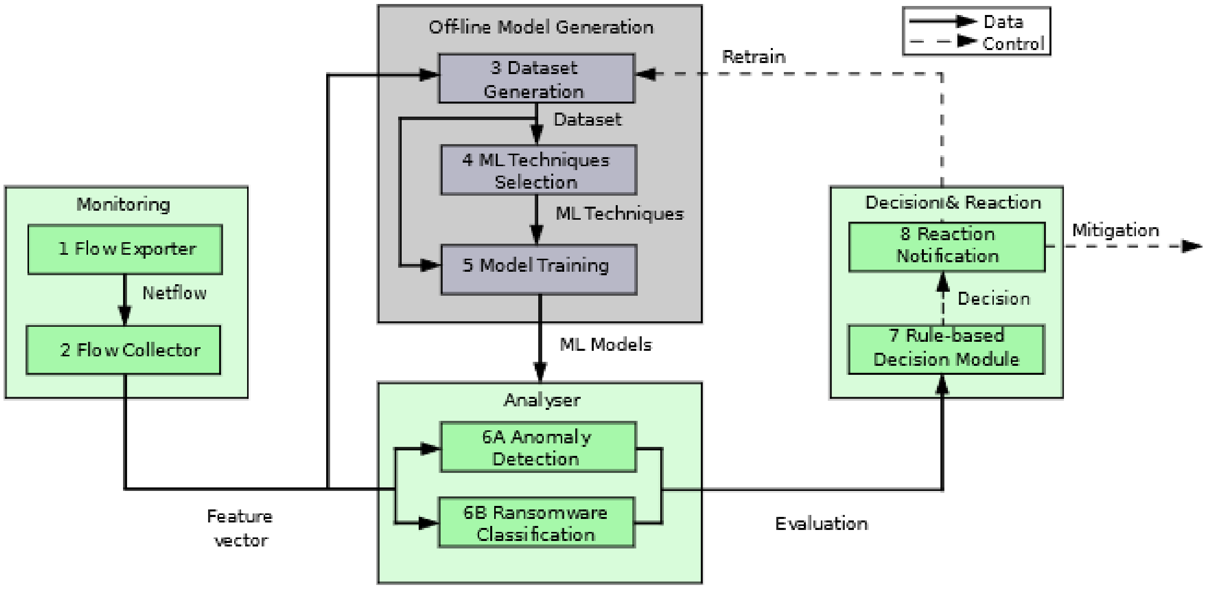
In order to use the proposed architecture, it is important to collect relevant data from the network. IoT devices have very specific network functions and traffic. The objective of the proposed device is to be able to collect data from IoT devices within the network and utilize that data to differentiate between normal network functions and malicious network activity. Using a heuristic approach, network administrators would define a relative scope of network functionality that a particular IoT device within the network is capable of performing. The proposed device works by collecting data from the network and utilizing said data to perform network operations. The network administrator would then be able to develop a system for differentiating between normal network activity and malicious activity.

Proposed Artifact:

I propose a physical network device that utilizes **port-mirroring** to collect data on network traffic. **Port mirroring** is a technique usually implemented within organizational networks in which a network device collects data on the traffic passing through specific ports(Svoboda, 2015). A device within a network will have a separate port where all traffic is mirrored to a duplicate port that is able to be used for network observation(Svoboda, 2015). Figure-2 represents a model of how port-mirroring works.



(Figure 2. J. Svoboda, I. Ghafir and V. Prenosil. (2015). Network Monitoring Approaches: An Overview, International Journal of Advances in Computer Networks and Its Security, Vol. 5, No 2.)



(Figure 2. Design of the proposed solution to detect, classify and mitigate ransomware in ICE Maimó et al, 2019)

Proposed Network:

The proposed network will be modeled after the network used in the research paper *Intelligent and Dynamic Ransomware Spread Detection and Mitigation in IntegratedClinical Environments*. I will use a Honeypot device designed to mimic actual IoT devices used in industry settings that will serve as the device that a ransomware attack is targeting. The proposed device utilizes port-mirroring techniques to collect data on ransomware software from the Honeypot device.

Design Evaluation:

In order for Ransomware attacks to be prevented, the malicious software must be detected in the infection phase. I believe that the proposed artifact is capable of providing a foundation for detecting ransomware in IoT networks. The device can also be further built upon in order to conduct further anomaly detection and behavioral analysis of ransomware in IoT networks. In order to most accurately judge the effectiveness of the proposed device and network architecture, I will set up the laboratory network to be as close to a real-world network as possible. The proposed architecture would mimic that of a standard organizational setting. The best way to study ransomware and ransomware IDS is by using machine learning. Most IoT research that studies ransomware uses obsolete or outdated datasets. The data collected in the proposed study can be used to deduce how the specific IoT devices' Operating systems are affected by ransomware and how the target devices' traffic and other network data are affected by ransomware. The collected data is then used to update the algorithm to detect ransomware on the proposed device and tested to see its accuracy and efficiency.

Conclusion

Ransomware is currently the biggest security threat faced by organizations today. The Internet-of-things is a growing portal for Ransomware attacks against professional organizations. The Internet of Things' unique attack surfaces and security concerns make IoT extremely vulnerable, and thus, the investment into security solutions has to develop immediately. Machine Learning has become the industry standard for studying malicious software and developing intrusion detection systems. However, due to the lack of datasets available, the creation of new datasets utilizing real IoT data and ransomware families is necessary. The research contributions of this paper are the following. This paper proposes a novel network device for studying ransomware IoT intrusion detection techniques by utilizing port mirroring coupled with a heuristic security analysis approach to detect malicious network activity. This paper also serves as a framework for creating a publicly available dataset for IoT research on ransomware.

References

A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. (2014). Internet of Things for smart cities, IEEE Internet Things J. Vol. 1, no 1, pp. 22-32.

F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices, IEEE Internet Things J., vol. 6, no. 5, pp. 8182–8201.

T. Fiorillo. (2014). Target Hackers Broke in via HVAC Company, *Krebs on Security*, 5 Feb, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

A. Hevner, S. March, J. Park, and S. Ram. (2004). Design Science in Information Systems Research, Management Information Systems Quarterly. Vol. 28, No. 1, pp. 75-105.

H. Oz, A. Aris, A. Levi and A. Uluagac. (2022). A survey on Ransomware: Evolution, Taxonomy, and Defense Solutions, ACM Computing Surveys, Vol. 54, No. 11s, Article 238, https://doi.org/10.1145/3514229.

R4iot: When ransomware meets internet of things. BrightTALK. (2022, June 1). Retrieved December 14, 2022, from https://www.forescout.com/blog/r4iot-when-ransomware-meets-the-internet-of-things/.

J. Svoboda, I. Ghafir and V. Prenosil. (2015). Network Monitoring Approaches: An Overview, International Journal of Advances in Computer Networks and Its Security, Vol. 5, No 2.

L. Strous, S. Solms and A. Zúquete. (2020). Security and privacy of the Internet of Things, Computers & Security. Vol. 102, no. 102148, pp. 1-3.

K. Collier. (September 2020). Major hospital system hit with cyberattack, potentially largest in U.S. history, NBC News, https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254.

F. Alaba, M. Othman, I. Hashem, F. Alotaibi. (April 2017). Internet of Things security: A survey, *Journal of Network and Computer Applications.* Vol. 88, pp. 10-28.

Cyber Security Summit. (2015). New York City Cyber Security Summit, The Official Cyber Security Summit, https://cybersecuritysummit.com/2015-new-york-city/.

D. Bisson. (Oct., 2015), Ransomware Victims Should 'Just Pay the Ransom,' Says the FBI, Tripwire, Integrity Management, https://www.tripwire.com/state-of-security/ransomware-victims-should-just-pay-the-ransom-says-the-fbi.

Fernández Maimó, L., Huertas Celdrán, A., Perales Gómez, Á., García Clemente, F., Weimer, J., & Lee, I. (2019). Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments. Sensors, 19(5), 1114. MDPI AG. Retrieved from http://dx.doi.org/10.3390/s19051114