Empirical Analysis and Practical Assessment of Ransomware Attacks to Data in Motion

Raúl Reinosa Simón
Communications Department
Universitat Politècnica de València
Valencia, Spain 46022
Email: rreisim@upv.es

Clara I. Valero
Communications Department
Universitat Politècnica de València
Valencia, Spain 46022
Email: clavalpe@upv.es

José A. Martínez Cadenas
Communications Department
Universitat Politècnica de València
Valencia, Spain 46022
Email: jamarcad@upv.es

Elisa R. Heymann
Computer Sciences Department
University of Wisconsin
Madison, WI 53706-1685 USA
Email: elisa@cs.wisc.edu

Ignacio Lacalle
Communications Department
Universitat Politècnica de València
Valencia, Spain 46022
Email: iglaub@upv.es

Barton P. Miller
Computer Sciences Department
University of Wisconsin
Madison, WI 53706-1685 USA
Email: bart@cs.wisc.edu

Carlos E. Palau
Communications Department
Universitat Politècnica de València
Valencia, Spain 46022
Email: cpalau@dcom.upv.es

2024 IEEE International Conference on Cyber Security and Resilience (CSR) | 979-8-3503-7536-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/CSR61664.2024.10679487

***Abstract*—In recent years, ransomware has established itself as one of the most persistent and devastating threats in cybersecurity. Traditionally, these attacks have focused on data at rest, encrypting files and demanding a ransom for their recovery. However, an alarming trend has emerged: ransomware for attacks to data in motion. This data, which includes information transmitted over networks, is critical to the day-to-day operations of organisations and often receives less protection than stored data. This paper aims to explore and characterise these new ransomware threats for attacks to data in motion. It also aims to test the feasibility of these attacks through the creation and implementation of a laboratory environment, as well as to analyse the potential consequences (based on likelihood and impact assessments) of such attacks if they were to be carried out, providing a comprehensive view of the potential emerging risks and warning of the need to create tools for the prevention, detection and mitigation of these attacks.**

I. Introduction

Over the last five years, ransomware attacks have become significantly more frequent, sophisticated, and costly [1]. The ransomware landscape is continually expanding, with an increasing growth in the number of threat actors carrying out attacks. According to the cybersecurity firm SonicWall, the historical peak of attempted ransomware attacks detected occurred in 2021, with over 623 million incidents [2]. Despite numerous reports and studies, the true extent of ransomware attacks remains largely unknown due to underreporting and the covert nature of these incidents. Organisations and individuals often choose to handle attacks discreetly, either out of fear of reputational damage or to avoid further attacks. Consequently, the full scale and impact of ransomware are difficult to quantify, but the repercussions are undeniably severe [3]. Victims face not only significant financial losses from ransom payments but also potential long-term consequences, such as data breaches, operational disruptions, and erosion of customer trust. This growing menace underscores the urgent need for comprehensive strategies to detect, prevent, and mitigate ransomware threats effectively.

In this landscape, new ransomware variants and groups are emerging, attracted by the potential for high profits and lower barriers to entry. Among these, ransomware attacks that target vulnerabilities in file systems for data in motion are a particularly concerning (so far theoretical) emerging threat [4]. Unlike more common ransomware that encrypts files on a local hard drive, these attacks would exploit weaknesses in the way file systems handle data that is being read from or written to storage. This allows the malware to encrypt or corrupt data as it moves between applications and the file system, making it very difficult to detect.

The plausibility of ransomware attacks on data in motion is due to the fact that modern computing environments increasingly rely on complex file systems and data storage solutions that are continuously accessed and modified. Vulnerabilities in these systems present attractive targets for ransomware. Attackers can exploit these weaknesses to intercept and alter data before it is securely stored, bypassing traditional encryption and security measures.

Detecting ransomware attacks that exploit vulnerabilities in the file system for data in motion is particularly challenging due to their sophisticated and elusive nature. It is not known at this point in time whether such attacks have ever taken place, since these attacks are not yet documented, making

them even harder to identify and understand. Their ability to remain undetected allows them to cause significant damage, including sensitive information leaks and loss of trust among stakeholders. The lack of documentation and research on these specific attack vectors means that traditional detection methods and security measures leave systems vulnerable to potentially devastating consequences.

Thereby, this study aims to characterise and reproduce in a laboratory environment ransomware threat for attacks on data in motion. The paper is organised as follows: Section I introduces the context that justifies the research conducted. Section II describes the context and background of these types of attacks. Section III includes the design and implementation of the scenario architecture. Section IV includes a discussion of the results obtained. Finally, the concluding remarks are presented in Section V.

II. Context and background

This section will focus on the analysis and description of the types of ransomware based on file system attacks on data in motion, the survey of previous related work and the motivation for this article, highlighting the lack of literature and practical implementation of ransomware for data in motion.

A. File system attacks on data in motion

There are two kinds of attacks to data in motion. In the first scenario, data in motion attacks involve encrypting, deleting, or exfiltrating data as it is being written to the file system. To execute this type of attack, the file system code of the operating system must be altered, making it a complex and challenging task. If successful, this attack can create a scenario where data recovery becomes extremely difficult, even with the best backup practices in place. In this type of attack, the file system is modified so that all data written to it is encrypted before storage. The second scenario refers to encrypt the data that is being transmitted over the network. In that case an agent (such as a MitM) intercepts the network traffic sent to a server or to a client, and encrypts it (or part of it) before sending it to the original destination.

In both scenarios, when data is read back, it is decrypted, making the attack invisible until the attacker decides to reveal it. Meanwhile, the existing data in storage is also encrypted using the same key. The attack can be scheduled to activate at a specific time. Once triggered, the encryption/decryption key is deleted from the computer's memory, causing all file reads to return encrypted data. Recovering from this attack is challenging. If the attack was to persist for an extended period of time then the backup best practices would not be effective. Such a scenario is expected to lead to considerable potential data loss.

In this work we focus on the second scenario (encrypting the data that is being transmitted over the network).

B. Previous related works

Ransomware attacks have been a significant concern in recent years, with numerous studies focusing on understanding their mechanisms, impact, and mitigation strategies [5] [6] [7]. In [8] and [9] several ransomware detection and mitigation methods are discussed, highlighting their advantages and disadvantages. Moreover, several recent papers have contributed to the body of knowledge on ransomware attacks, highlighting various aspects of these incidents [10] [11]. In addition, recent studies highlight the rise of Ransomware-as-a-Service (RaaS) platforms [12] [13], which allow cybercriminals with limited technical skills to launch sophisticated attacks. These platforms provide a business model where ransomware developers offer their malware to affiliates in exchange for a share of the ransom payments.

Files are the primary target in ransomware attacks. They can be attacked in various forms, some of which are commonly observed, while others have yet to be reported. In [4] the authors describe a file system attack where the attack takes place on data in motion. Attacks targeting data in motion encompass actions such as encrypting, deleting, or illicitly transferring data while it is actively being saved to the file system. Additional details of these attacks are given in Section II-A.

On the other hand, several studies have examined the role of malware in enabling Man-in-the-Middle (hereinafter MitM) attacks. Some studies [14] [15] [16] identify spoofing as either the initial step or one of the steps in executing a MitM attack. Other research [17] equates spoofing directly with MitM attacks. Meanwhile, in papers [18] [19], the authors describe a spoofing-based MitM attack as a type of spoofing attack that ultimately results in a MitM attack. For these reasons, although there is literature for ransomware attacks to data in motion based leveraging MitM techniques and attack vectors, there is very limited evidence to drive the picture towards practical approaches.

C. Motivation

As mentioned in the Section I, there is not much literature on previous work identifying and analysing ransomware threats based on data in motion. Still, the studies seen have provided valuable insight into the characteristics and behaviours of these types of ransomware. However, despite extensive theoretical literature and descriptive analyses, no current literature has been found that addresses these threats from a practical point of view, demonstrating the viability and impact of these types of attacks through empirical research. This absence in the literature represents a significant gap, as understanding the practical feasibility and real-world impact of ransomware attacks based on data in motion is crucial to developing effective defence strategies. The lack of empirical studies demonstrating how these attacks can be carried out in a realistic environment limits the ability to anticipate and mitigate their effects.

For this reason, the motivation for this article is threefold. Firstly, we seek to contribute to the scientific community by defining a viable environment that allows such attacks to be carried out in a controlled manner for the sake of prevention and protection. This includes the design and development of

a laboratory test environment that simulates real conditions in which ransomware can attack data in motion. Secondly, we will create a practical scenario as a case study within this test environment, with the aim of empirically demonstrating the dangerousness of these threats. This case study will provide tangible evidence on how and to what extent they can compromise the security of affected systems, enabling a deeper and more practical understanding of the implications of these attacks. Ultimately, this article seeks to warn the community of such emerging threats by encouraging the creation of prevention, detection and mitigation tools.

III. Materials and methods

This section presents the materials and methods used to generate a practical scenario as a case study to illustrate the capabilities of ransomware to attack data in motion. The subsections will detail the theoretical scenario to develop the use case, the setup of a laboratory environment, and finally the implementation and explanation of the data flow and examples of the resulting encryption.

A. Architecture and scenario of the use case

The architecture of the proposed solution is designed to simulate a real environment in which ransomware can take place over data in motion. This architecture includes several key components: physical and network infrastructure, network protocols used and security mechanisms. The physical infrastructure details the agents involved, while the network infrastructure consists of a connection interface between all agents, equipped with operating systems and software commonly used in enterprise environments. The aim of this assembly is to provide an overview of a theoretical scenario and a practical example of the use of ransomware to attack data in motion within a dynamic data environment. The Figure 1 shows the components involved in the use case, where a server hosts several virtual PCs that interact directly with a backup server.

In a basic scenario, some clients send their data to the backup following certain temporal rules, establishing a client-server communication. This configuration is ideal to approach and carry out the attack. For this use case, once the attacker gains access to the internal environment, the attack vector must be technique able to manipulate the network behaviour, across the focused system (to simplify it, the original client-server connection). There are various techniques that could potentially achieve this, but one of the classic ever seen are the MitM attacks. Figure 2 shows a MitM attack using for this use case, when the attacker intercepts the traffic sent between the client and the server, redirecting the traffic through the attacker's machine, allowing to listen and intercept the traffic generated. One prevalent form of MitM attack relies on Address Resolution Protocol (ARP) spoofing. In ARP spoofing, the attacker sends forged ARP message onto the Local Area Network (LAN). These messages associate the attacker's MAC address with the IP address of the legitimate server or client, causing network traffic intended for that IP address to be sent to the attacker's machine instead.

Finally, this case study distinguishes itself from a classic ransomware attack in that it focuses on encrypting the content of the data rather than the files themselves. By intercepting the traffic between the client and the server, the attacker can selectively target sensitive data content (known as payloads) and apply an encryption algorithm to it. Moreover, regardless of whether or not the payload is encrypted at source, the attacker can re-encrypt it before the request reaches its final destination. This means that even if the content is protected during the initial transmission, the attacker can add an additional layer of encryption. When the request reaches the destination, it will be encrypted, which is transparent to the requester who made the initial request. This provides the attacker with another layer of transparency and stealth, especially in situations where there is no thorough review to ensure that transactions have been carried out correctly. When the client receives the data, it is decrypted. Figure 3 shows the flow of encryption and decryption of data in motion.

B. Environment setup

Once the theoretical architecture has been defined in Section III-A, a practical scenario has been laid out within a laboratory environment to test the feasibility and impact of this type of attacks. First, three agents have been defined: client, server and attacker machine. The following Table I lists the main parameters and resources used in this configuration, including the operating system, CPU, RAM and other specifications of each component involved.

TABLE I
Component parameters and resources

Resources	Agents		
	Virtual PC (Client)	Backup server	Attacker machine
Operating System	Windows 10	Ubuntu 22.04	Kali Linux 6.6.9
RAM	64 GiB	8 GiB	8 GiB
CPU	16 CPU(s)	4 CPU(s)	4 CPU(s)
IP	192.168.250.122	192.168.250.146	192.168.250.137
MAC Address	42:26:60: 77:57:A0	F2:85:F4: 20:FA:47	AE:1D:20: 22:7E:35

C. Implementation flow

The most basic scenario involves a client willing to send a file to a backup server. To achieve this goal, an *HTTP* server has been implemented on the server side that accepts *POST* and *GET* requests to send and receive files, respectively. For the testbed implementation, a series of *.JPG* files have been sent and received from the client side to the server.

In parallel, once inside the internal communication network, the attacker executes an ARP Spoofing attack by modifying the client and server ARP tables bidirectionally. This is achieved by overwriting the attacker's own MAC Address in the respective client-server IP cells. This way, the attacker intercepts the traffic between the client and the server and filters it based on the server's IP address (192.168.250.146).

Whenever an *HTTP* request arrives, specifically a *POST* request, the first 1024 bytes of the hexadecimal payload are

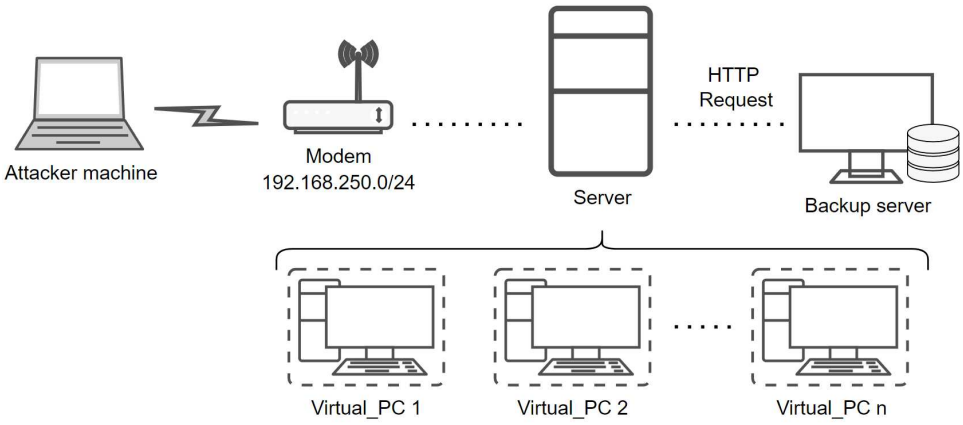

Fig. 1. Hardware technology stack used for deployment

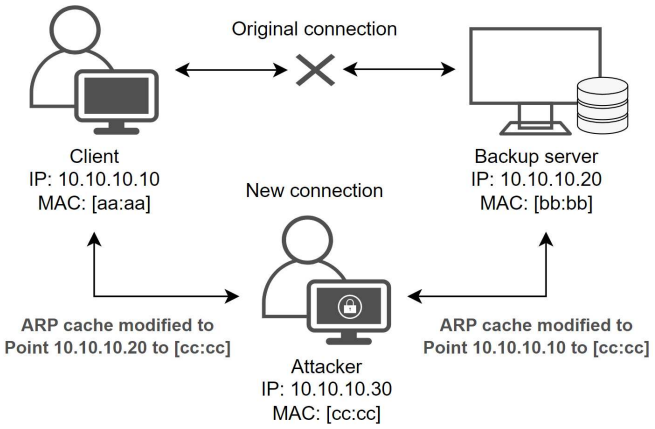

Fig. 2. Example of Man-in-the-middle use case: ARP Spoofing

encrypted using an XOR encryption key. This encryption process targets the content of the file, leaving the *HTTP* headers and other metadata unaffected. As a result, the client receives a successful response, believing the operation is completed correctly. However, as shown in Figure 4, the image stored on the backup system is encrypted. To maintain transparency from the client's perspective, if the client performs a *GET* request to retrieve the file, the attacker re-applies the XOR encryption key on the encrypted payload. Applying the XOR encryption key a second time decrypts the content and restores the original file. This is because XOR encryption, when applied twice with the same key, results in the original message due to the properties of the XOR operation. This mechanism ensures that the encryption and decryption happen seamlessly, making the attack invisible to the client until the attacker decides to reveal it.

Once the attack concludes or the connection is closed, the final step involves erasing all data on the local PCs if the attacker has access. The backup servers retain only the encrypted data. Consequently, during the backup process, the stored data remains ciphered. This type of ransomware affects data integrity, as it will be impossible to decrypt the files without the decryption key. After the attack, the attacker may contact the victims, demanding a ransom in exchange for the script containing the decryption key, which is necessary to decrypt all the affected data on the server.

IV. Discussion and Results

This section will analyse and assess the consequences of ransomware attacks based on data in motion. To achieve this, it will calculate the likelihood and the impact it can have on organisations. According to the NIST document [20], it is crucial to perform continuous consequence assessments to identify and mitigate cybersecurity threats.

A. Likelihood calculation of ransomware attacks to data in motion

Even when ransomware attacks are rigorously tested in laboratory environments, accurately gauging their real-world viability requires meticulous evaluation of numerous technical and logistical factors. To determine the likelihood of occurrence, three guiding factors have been taken into account:

- **Motivation and threat source capability:** Incentives or reasons for threat actors to attack an organisation and what resources, skills or ideals attackers have to carry out a successful attack.
- **Nature of vulnerability:** This factor takes into account the ease of exploitation, the severity of the impact of the attack and how exposed the vulnerability is (level of accessibility).
- **Existence and effectiveness of current controls:** For this factor, the existence of controls or procedures to prevent the threat and their level of maturity have been taken into account.

In addition, Table II shows the probabilities for the calculation of the likelihood of occurrence.

Taking these three concepts into account, the assessment is that the probability of the threat occurring is **medium**. The source of the threat shows high motivation and capability, due to the importance of the transmitted data, implying a significant potential to carry out an attack. The identified scenario is

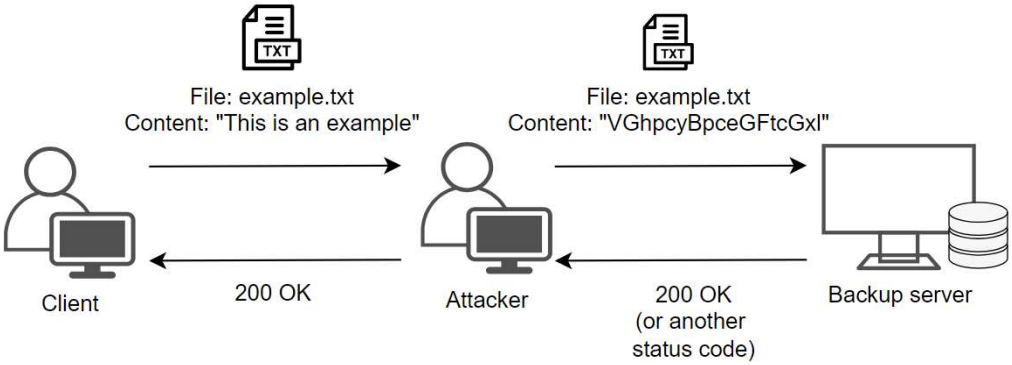

Fig. 3. File encryption and decryption data flow: Traffic is encrypted in motion and the client receives a successful response to its request

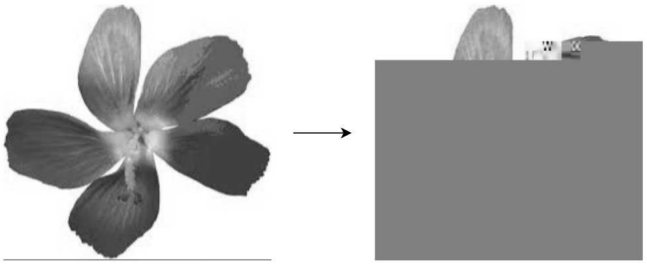

Fig. 4. Example of file encryption on moving data: The original payload is replaced by the encrypted code

TABLE II
LIKELIHOOD LEVEL ASSESSMENT

Likelihood level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

relatively difficult to occur, due to several factors, among them: (i) the attacker must have gained access to the network, (ii) the attacker must be able to intercept communications to and from the server and (iii) must be able to apply ARP Spoofing techniques or derivatives to generate the MitM, these factors make it difficult to execute the attack, although it could have a considerable impact if it were to be carried out. Finally, although there are security controls in place regarding MitM detection, there are no known specific controls to detect and mitigate this type of attack, which increases the likelihood of success if this attack were to be carried out.

B. Impact calculation of ransomware attacks to data in motion

Similarly, assessing the impact of ransomware attacks from a cybersecurity perspective is paramount to understanding the potential ramifications and designing effective mitigation strategies. The specifications in Table III have been taken into account to measure the magnitude of the impact if the attack were to be executed.

TABLE III
IMPACT LEVEL ASSESSMENT

Impact level	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organisation's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organisation's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organisation's mission, reputation, or interest.

Considering these concepts, it is concluded that the impact estimate is **high**. This conclusion is based on several factors: (i) If the attack is successful, critical assets stored in backup systems would be compromised, leading to the loss of essential system recovery files. (ii) Additionally, the attacker may exfiltrate files and subsequently demand a monetary ransom for their return. Therefore, as is common with ransomware attacks, the potential impact is highly critical, posing a significant threat to the organisation's operations and financial stability.

C. Determination of actual consequences

Once the likelihood and impact calculations have been defined (in Sections IV-A and IV-B, respectively), the actual consequences can be determined by drawing up a matrix of consequence levels and consequence scale. Table IV shows the consequence level matrix and consequence scale.

Based on the above results, a possible **current consequence of 50** is determined. This implies that corrective actions are needed and a plan should be developed to incorporate these actions within a reasonable period of time, according to NIST document [20] recommendations.

TABLE IV
LIKELIHOOD/IMPACT MATRIX CONSEQUENCE SCALE

Threat Likelihood	**Impact**		
	Low (10)	**Medium (50)**	**High (100)**
High (1.0)	**Low** 10 x 1.0 = 10	**Medium** 50 x 1.0 = 50	**High** 100 x 1.0 = 100
Medium (0.5)	**Low** 10 x 0.5 = 5	**Medium** 50 x 0.5 = 25	**High** 100 x 0.5 = 50
Low (0.1)	**Low** 10 x 0.1 = 1	**Medium** 50 x 0.1 = 5	**High** 100 x 0.1 = 10

V. CONCLUSIONS AND FUTURE WORK

Ransomware attacks to data in motion are, up to now, difficult to detect, undoubtedly dangerous and a potential threat factor for organisations. This work has offered the first approach to understand their viability, impact and capacity to compromise the security and integrity of files (data) transferred through the network. Concretely, such interventions occurring in transit (before reaching the ends of the communication line) are likely to happen in the form of MitM attacks. There, an illegitimate attacker may cater sophisticated ciphering techniques upon files so that those become irretrievable unless paying a ransom.

The depicted simulation of such a scenario should allow the community to realise their feasibility, and should foster further research on advanced methods to work against them. In this regard, authors will continue investigation on potential prevention, detection and mitigation strategies, aiming at diminish the impact of this potential threat.

In addition, the authors plan to extend the replication scenario to incorporate more complex parameters and larger infrastructures, which could provide insight into the methods of these attacks and facilitate the development of countermeasures. This approach opens up research avenues focused on creating a robust testbed capable of simulating attacks on data in motion. This testbed would also allow training AI algorithms to classify network traffic and detect ransomware attacks through MiTM interventions, thus providing a resilient and adaptive security solution. The envisioned environment aims to be mature, reproducible and well-documented, incorporating features that support scalability and comprehensive study, as well as including the source code used to build the testbed and detection algorithms.

ACKNOWLEDGEMENT

This work has been developed under the framework of the NGISARGASSO-2024-CALL2-3-GUARDIAN project. The project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101092887.

REFERENCES

[1] S. Kamil, H. S. A. S. Norul, A. Firdaus, and O. L. Usman, "The rise of ransomware: A review of attacks, detection techniques, and future challenges," in *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*. IEEE, 2022, pp. 1–7.

[2] SonicWall, "2023 sonicwall cyber threat report," SonicWall, Tech. Rep., 2023, accessed: 2024-05-29. [Online]. Available: https://www.sonicwall.com/medialibrary/en/infographic/2023-cyber-threat-report-infographic.pdf

[3] F. B. of Investigation, "2023 sonicwall cyber threat report," Federal Bureau of Investigation, Tech. Rep., 2023, accessed: 2024-05-29. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2023IC3ElderFraudReport.pdf

[4] B. P. Miller and E. R. Heymann, "Trusted ci webinar: The technical landscape of ransomware: Threat models and defense models," *Trusted CI Webinar*, 2023.

[5] S. Mohurle and M. Patil, "A brief study of wannacry threat: Ransomware attack 2017," *International journal of advanced research in computer science*, vol. 8, no. 5, pp. 1938–1940, 2017.

[6] R. Brewer, "Ransomware attacks: detection, prevention and cure," *Network security*, vol. 2016, no. 9, pp. 5–9, 2016.

[7] N. Scaife, H. Carter, P. Traynor, and K. R. Butler, "Cryptolock (and drop it): stopping ransomware attacks on user data," in *2016 IEEE 36th international conference on distributed computing systems (ICDCS)*. IEEE, 2016, pp. 303–312.

[8] H. Alshaikh, N. Ramadan, and H. Ahmed, "Ransomware prevention and mitigation techniques," *Int J Comput Appl*, vol. 177, no. 40, pp. 31–39, 2020.

[9] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Computers & security*, vol. 111, p. 102490, 2021.

[10] L. Yuryna Connolly, D. S. Wall, M. Lang, and B. Oddson, "An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability," *Journal of Cybersecurity*, vol. 6, no. 1, p. tyaa023, 2020.

[11] J. A. Herrera Silva, L. I. Barona López, Á. L. Valdivieso Caraguay, and M. Hernández-Álvarez, "A survey on situational awareness of ransomware attacks—detection and prevention parameters," *Remote Sensing*, vol. 11, no. 10, p. 1168, 2019.

[12] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The ransomware-as-a-service economy within the darknet," *Computers & Security*, vol. 92, p. 101762, 2020.

[13] A. A. M. A. Alwashali, N. A. Abd Rahman, and N. Ismail, "A survey of ransomware as a service (raas) and methods to mitigate the attack," in *2021 14th International Conference on Developments in eSystems Engineering (DeSE)*. IEEE, 2021, pp. 92–96.

[14] V. Ramachandran and S. Nandi, "Detecting arp spoofing: An active technique," in *Information Systems Security: First International Conference, ICISS 2005, Kolkata, India, December 19-21, 2005. Proceedings 1*. Springer, 2005, pp. 239–250.

[15] M. Carnut and J. Gondim, "Arp spoofing detection on switched ethernet networks: A feasibility study," in *Proceedings of the 5th Simposio Seguranca em Informatica*, 2003.

[16] X. Yu, X. Chen, and F. Xu, "Recovering and protecting against dns cache poisoning attacks," in *2011 International Conference of Information Technology, Computer Engineering and Management Sciences*, vol. 2. IEEE, 2011, pp. 120–123.

[17] R. Philip, "Securing wireless networks from arp cache poisoning," Master's thesis, San Jose State UniversitySan Jose State University, 2007.

[18] S. Y. Nam, S. Jurayev, S.-S. Kim, K. Choi, and G. S. Choi, "Mitigating arp poisoning-based man-in-the-middle attacks in wired or wireless lan," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, pp. 1–17, 2012.

[19] S. Y. Nam, S. Djuraev, and M. Park, "Collaborative approach to mitigating arp poisoning-based man-in-the-middle attacks," *Computer Networks*, vol. 57, no. 18, pp. 3866–3884, 2013.

[20] R. Ross, "Guide for conducting risk assessments," 2012-09-17 2012.