IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Early Detection and Prediction of Extortion Coverage Attack

Yeola Priti Dipak[1], Deshmukh Sakshi Uttam[2], Shruti[3], Prof. Nikhilesh Mankar[4]
[1,2,3,4]D Y Patil University Ambi, Pune

Abstract- Ransomware attacks have become increasingly prevalent in recent years, posing a significant threat to cybersecurity. This research paper explores the various aspects of ransomware attacks, including their definition, types, techniques, and impacts on individuals and organizations.

Ransomware Cyber insurance, also known as cyber extortion coverage, is typically included with a sublimit under a cyber-liability insurance policy. Ransomware is a type of malware that encrypts the files on a computer, preventing the user from accessing them. It encrypts users' files or steal/delete important information and holds the decryption key until a ransom is paid by the victim, which is mostly in bitcoins due to their untraceable properties.

Keywords – Ransomware Attack, Cybersecurity, Malware, Infection, Encrypt, Decrypt, Cryptowall, Bitcoin, Cryptolocker, WannaCry, Threat.

I. INTRODUCTION

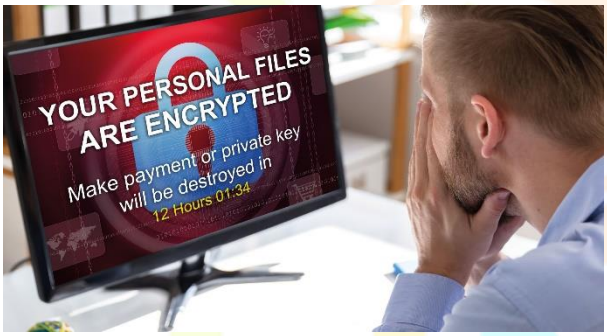
Ransomware, a potent tool in the cybercriminal arsenal, allows them to extort significant sums from victims while causing digital havoc. Protecting networks, servers, personal computers, and devices poses enormous challenges, with the cybersecurity industry estimated at $100 billion. Security solutions for hardware and infrastructure are gaining increased attention in this landscape.

Ransomware is a one type of malicious software (i.e., malware). It is designed to encrypt or limit the access of user data [1]. Ransomware attacks have become more prevalent, brutal and recurrent [16]. The precise initiation details of ransomware attacks remain unclear, but they typically commence with a user being deceived into clicking a link or opening a malicious email attachment. Subsequently, software designed to harm or incapacitate the computer is downloaded, swiftly encrypting all data on the user's machine and potentially spreading over the network to encrypt data on other machines, resulting in the complete inaccessibility of all data [9]. The occurrence of ransomware infection continues to grow in scale, cost, complexity and impact since its initial discovery nearly 30 years ago [2]. As we all know ransomware first appeared more than 30 years ago, its initial impact on the computing community was small with only a few people being affected and recovery from the attack being trivial [3]. Recent attack of ransomware flustered the whole world [4]. The first ransomware relied on encrypting information on the victim's computer to demand payment for the key or software to decrypt the data [5]. The damages caused by a single ransomware variant, CryptoWall3, were estimated to be over $320 million in 2015 [15]. Victim are threatened with permanent loss of access unless they pay a ransom [6]. The payment is often requested in Bitcoin (is a cryptocurrency and a payment system) or other invisible currency. Businesses and individuals worldwide are currently under attack by ransomware [8]. Bitcoin comprises of encryption techniques utilized to regulate the generation of units of currency, whereby fund transfer verification is completed independently of a central bank [14]. Several types of security issues have revealed exploitation and vulnerabilities in cyberspace [7]. For example, the Cryptolocker ransomware alone managed to infect

approximately 250 thousand computers around the world [10]. Android ransomware are disguised as legitimate mechanical man applications [11]. The 2017 WannaCry Ransomware Attack stands out as one of the most severe incidents to date. This form of malicious software, known as WannaCry Ransomware, strategically restricts user access to files or systems, holding them hostage through encryption. To regain access, victims are coerced to pay a ransom in exchange for a decryption key that unlocks the encrypted files or systems. The magnitude of this attack may be challenging to comprehend [12]. To counter the rising threat of ransomware attacks, it is frequently recommended that users establish backups of their essential data. Undoubtedly, implementing a robust data backup strategy reduces the potential expenses associated with falling victim to ransomware and constitutes a crucial aspect of the IT management protocol [13]. Examining notable instances reveals that ransomware attackers often target the systems of professional organizations [17].

II. HISTORY OF RANSOMWARE

Ransomware, originating modestly, has evolved into a significant worldwide enterprise, generating millions, and at times, billions for its originators. The term ransomware, formed by combining ransom and software, denotes malicious software crafted to coerce money from a target, either by seizing particular files or by encrypting the entire computer until a ransom is fulfilled [4].



From 1989 attack of ransomware were started [17]. We have classified the history in two parts:

i. Before Ransomware as a service:

1989- In 1989, the initial ransomware virus, known as the AIDS Trojan or PC Cyborg, was discovered, crafted by Joseph L. Popp, an evolutionary biologist educated at Harvard [16].
2005- The ransomware landscape evolved in 2005 with the emergence of Trojan.Gpcoder, marking the onset of modern crypto ransomware, albeit with initial weaknesses.
2006- As 2006 progressed, ransomware gained momentum, witnessing a surge in attackers.
2007- In 2007, locker ransomware surfaced, notably lacking encryption.
2008- The year 2008 introduced GPcode.AK, a variant of Trojan.Gpcoder utilizing a 1024-bit RSA algorithm for file encryption.
2011- By 2011, Trojan.Winlock, a ransomware worm, mimicked the Windows Product Activation notice, adding complexity for users.
2012- In 2012, a toolkit named Citadel malware facilitated the creation and distribution of Reveton ransomware.
2013- The first iteration of CryptoLocker emerged in September 2013, targeting both companies and individuals through phishing emails.
2014- February 2014 witnessed the release of Crypto Defense, employing Tor and bitcoin for anonymity.
2015- CryptoWall 2.0 entered the market in January 2015, further shaping the ransomware landscape.

ii. After Ransom-as-a-Service:

2016- In January 2016, the cybersecurity community identified Ransom32, a JavaScript-exclusive ransomware-as-a-service (RaaS).
2017- On May 12th, 2017, the WannaCry ransomware caused widespread disruption to hundreds of organizations across at least 150 countries, as reported by Lakhani in 2017.
2018- August 2018 witnessed the initial emergence of the Ryuk ransomware in real-world scenarios, marking its debut outside controlled environments.
2019- In 2019, REvil emerged as a prominent ransomware-as-a-service, earning a reputation as one of the most severe ransomware instances witnessed that year.
2020- In 2020, Cognizant, a tech giant, experienced a major ransomware attack, resulting in a substantial $50 to $70 million in revenue loss, as well as significant expenses for recovery and mitigation. The Maze ransomware infiltrated the company's network in April of that year.
2021- In late December 2021, Shutterfly fell victim to a ransomware attack orchestrated by the Conti ransomware gang, leading to a private data leak page with stolen information. The group demanded a ransom, threatening to disclose the page publicly if not paid. In February 2022, the San Francisco 49ers, a US NFL team, experienced a ransomware attack on its corporate network, with the Black Byte ransomware group identifying them as victims on a dark web leak site.
2022- In February 2022, the San Francisco 49ers, an NFL team in the United States, experienced a ransomware breach on its corporate network. The Black Byte ransomware group disclosed the team as one of its targets on a dark web leak site.

iii. Recent Ransomware:

2023- In 2023, one of the significant ransomware incidents unfolded, targeting Prospect Medical Holdings based in California. The attack, revealed on August 3, initiated with Charter Care Health Partners, Prospect Medical's Rhode Island affiliate, reporting system outages that disrupted both inpatient and outpatient operations.

iv. How it spreads?

As per the US Computer Emergency Readiness Team (USCERT) within the Department of Homeland Security, ransomware proliferates effortlessly when it confronts software that is either unpatched or outdated. Experts

indicate that WannaCry is disseminated through an internet worm, a type of software that propagates itself by infiltrating other computers on a network, diverging from the typical method of enticing unsuspecting users to open attachments. The cyber-attack is thought to have been executed using tools pilfered from the National Security Agency (NSA) of the United States [4]. Initiating a ransomware attack involves the initial phase of installing components designed for infecting, encrypting, or locking the system. Various methods are employed to deliver malware files to the targeted computer during this stage [5].

Drive-by downloads: In a drive-by download attack, malware is downloaded to a victim's device without their knowledge or consent. It often occurs when a user visits a compromised website that contains hidden malicious code, exploiting vulnerabilities in the user's browser or plugins to initiate the download.

Phishing emails: Attackers send deceptive emails that appear to be from legitimate sources, such as banks, social media platforms, or shipping companies. These emails often contain malicious attachments or links that, when clicked or opened, execute the ransomware on the victim's device.

Exploiting vulnerabilities: Malicious downloads: Attackers may distribute ransomware through malicious downloads from compromised websites, torrent files, or peer-to-peer networks. Users unknowingly download and execute the ransomware by clicking on these infected files.

III. TYPES OF RANSOMWARE

i. Main types of ransomware

1. Encrypting Ransomware: Encrypts the victim's files and demands payment for the decryption key [17]. Examples of typical crypto-ransomware include CryptoWall, CryptoLocker, WannaCry and Locky [5].
2. Locker Ransomware: On the other hand, it locks the victim's screen or device and demands payment to unlock it [17]. Examples of typical locker-ransomware include Winlocker and Reveton [5].

ii. Impacts of Ransomware Attack:

Ransomware attacks can have severe consequences for individuals and organizations, including data loss, financial loss, and reputational damage. In some cases, victims may be unable to recover their data, even after paying the ransom. Moreover, paying the ransom may encourage further attacks and support criminal activities. Decreased operational efficiency stemming from the cessation of essential business systems—resulting in the potential forfeiture of files and data, embodying numerous hours of collective effort.

Ransomware poses a threat not limited to individual users; it can also infiltrate businesses, resulting in adverse outcomes such as [4]

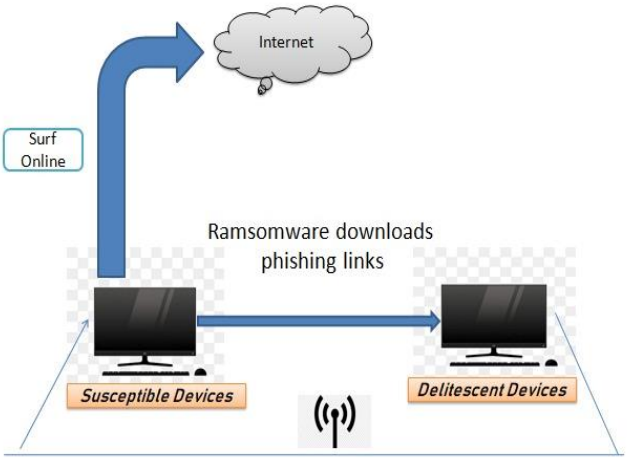
1) The temporary or permanent compromise of sensitive or proprietary data.
2) Disruptions to regular operations, financial losses for system and file restoration.
3) Potential damage to an organization's reputation.

iii. Susceptibility to ransomware:

The classical paradigm is to defend against malware attacks has traditionally been victim-agnostic and reactive, with defenses focusing on identifying the attacks or attackers where (e.g., phishing emails, malicious websites, and files) For example, several studies propose technical, automated solutions to prevent ransomware attacks.

More relevant to our work are user studies that identify the vulnerable population and the behaviors that predispose users to malware infections. These cover a wide range of contexts and sub-segments of the population and are typically administered to small, non-representative sample sizes. As a result, it has been difficult to draw conclusions with respect

to the general importance of demographic, situational, and behavioral factors on risk of victimization. Ngo et al. apply the general theory of crime and routine activities to assess the effects of individual and situational factors on seven types of cybercrime victimization-among them, a computer virus.



Dealing with a ransomware attack can be a stressful and challenging situation. Here are some thoughts and steps to consider when facing a ransomware attack:

Stay calm and assess the situation: It's important to remain composed and not panic. Take a moment to understand the extent of the attack and gather information about the affected systems, data, and potential vulnerabilities.

Disconnect affected systems from the network: Isolate the infected systems immediately to prevent further spread of the ransomware within your network. Disconnecting them from the network can help contain the attack and protect other systems.

Notify appropriate personnel: Inform your organization's IT department, network administrators, or any other designated security personnel about the attack. They can provide guidance and support in dealing with the situation.

Preserve evidence: Document and preserve any evidence related to the attack. This may include screenshots, logs, or any other information that can aid in the investigation and mitigation process. This evidence may also be useful for law enforcement agencies if they get involved.

Contact law enforcement: Depending on the severity and impact of the attack, it may be necessary to involve local law enforcement or cybercrime units. They have the expertise and resources to assist in dealing with the ransomware attack and potentially track down the perpetrators.

Engage with cybersecurity experts: Consider reaching out to cybersecurity professionals or incident response teams who specialize in dealing with ransomware attacks. They can provide technical assistance, guidance, and help in the recovery process.

Evaluate the ransom demand: Assess the feasibility and potential risks of paying the ransom. It's generally not recommended to pay, as it encourages future attacks and there's no guarantee that you'll regain access to your data. Consult with cybersecurity experts and legal advisors before making any decisions.

Implement security improvements: Once the immediate threat has been addressed, take steps to enhance your organization's security posture. This may involve patching vulnerabilities, updating security software, educating employees on cybersecurity best practices, and conducting security audits.

Learn from the experience: Conduct a post-incident analysis to identify weaknesses in your security infrastructure and response procedures. Use the lessons learned to improve your organization's overall security posture and develop a robust incident response plan for future incidents.

IV. SAFETY METHODS

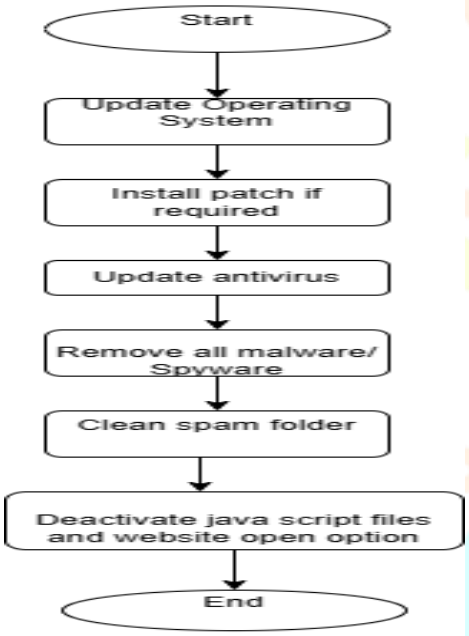
Mitigating ransomware attacks necessitates a blend of sound security protocols and preemptive actions. PH Rughani, who conducted practical tests on an Android phone, revealed that mobile devices are susceptible to ransomware attacks similarly to other machines [17]. Instances include altering the PIN numbers of phones and demanding payment for access [16]. Taking proactive measures is crucial in safeguarding against ransomware attacks; these include consistently updating your antivirus software, activating pop-up blockers, regularly updating all your software, ensuring the smart screen is enabled in Internet Explorer to identify phishing and malware websites, and exercising caution when encountering suspicious email attachments. Remember, prevention is more effective than dealing with the aftermath [4]. To thwart ransomware infections and address them if they occur, implement preventive strategies.

Step 1: Make backups plan- Ensure your files are backed up regularly, maintaining a current off-site backup that is encrypted to ensure exclusive restoration access [8].

Step 2: Avoid email links and attachments if unknown- To not open unknown attachments and emails. It recommends blocking executable and zip file attachments [17].

Step 3: Patching software - All the browsers, OS and security system should be always kept patched and up-to-date including third-party plug-ins, like Java and Flash. [17].

Step 4: Drop-and-Roll- The infected system should be disconnected to the network, turn off all the Wi-Fi and Bluetooth, and remove any external drives, USBs or devices. [17].



Flowchart

V. FUTURE SCOPE

Ransomware remains a significant global menace, notorious for swiftly targeting numerous users. Employing widespread phishing campaigns, it encrypts crucial files and documents. This study provides key insights into ransomware, its operational methods, and recommendations for safeguarding computers. The safety protocols outlined serve as valuable guidance for both researchers and society in preserving data integrity in the foreseeable future [17]. Ransomware in cybersecurity remains concerning, with attackers constantly evolving tactics. Expect increased targeting of critical infrastructure, sophisticated social engineering, and possibly the use of emerging technologies for more effective attacks. Staying vigilant, regularly updating security measures, and educating users are crucial in mitigating these threats. There are many types of network varieties they can offer so many services and numerous of which are cloud based consequently [14]. In recent years, there has been a surge in the prevalence of ransomware attacks orchestrated by cybercriminals. This malicious software seeks payment in exchange for restoring access to stolen functionality, personal information, or data that has been restricted, employing tactics like online payment services or cryptocurrency extortion from victims

VI. REFERENCES

[1] Received February 5, 2022, accepted April 14, 2022, date of publication April 20, 2022, date of current version May 2, 2022.
Ransomware Attack as Hardware Trojan: A Feasibility and Demonstration Study.
[2] Differential Area Analysis for Ransomware Attack Detection within Mixed File Datasets.
Simon R. Davies, Richard Macfarlane" and William J. Buchanan"
[3] Evaluation of Live Forensic Techniques in Ransomware Attack Mitigation.
Simon R. Davies, Richard Macfarlane" and William J. Buchanan"
[4] Special Issue-2017
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181 NCICCNDA-2017 Conference Proceedings
A Study on Ransomware and its Effect on India and Rest of the World
[5] A note on different types of ransomware attacks
Mihail Anghel, Andrei Racautanu, email: racautanu.andrei.nicolae@info.uaic.ro Computer Science Faculty, "Al. L. Cuza" University, Iasi, Romania
[6] Economics of Ransomware Attacks
Terrence August*, Duy Dao!, Marius Florin Niculescu
May 2019
[7] Ransomware and phishing cyberattacks: analyzing the public's perception of these attacks in Sweden
Ali Hoseini
[8] International Journal of Research and Scientific Innovation (IIRSI) | Volume IV, Issue VIS, June 2017 | ISSN 2321-2705
A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control
[9] A Socio-technical Approach to Pre-venting, Mitigating, and Recovering from Ransomware Attacks
[10] Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks
Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda
[11] International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021
Ipact Factor-5.354
e-ISSN: 2582-5208
SURVEY ON RANSOMWARE ATTACK

www.irjmets.com
Gaikwad Rutuja*1, Prof. Rathod U. V*2
[12] Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info
A brief study of Wannacry Threat: Ransomware Attack 2017
[13] Ph.D. Thesis Proposal
Techniques and Solutions for Addressing Ransomware Attacks
[14] INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 6, ISSUE 06, JUNE 2017 ISSN 2277-8616
307
IJSTR©2017
www.ijstr.org
Ransomware - Threats, Vulnerabilities And Recommendations
Nadeem Shah, Mohammed Farik
[15] "I was told to buy a software or lose my computer. I ignored it": A study of ransomware
[16] Ransomware Attacks: Critical Analysis, Threats, and Prevention methods
Asibi Imaji
Fort Hays State University
[17] Ransomware Evolution, Target and Safety Measures
Article INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND ENGINEERING July 2018