Sri Lanka Institute of Information Technology

Ransomware applicable for IOT

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT2007874	Thalawattage T.A.H.S

Date of submission
May 20, 2021

Table of Contents

Abstract

Ransomware applicable for IOT

Thalawattage T.A.H.S

Department of computing, Sri Lanka Institution of Information Technology

The IOT architecture is the process of connecting physical reality and areas to the internet. This digital revolution is making our lives better and enabling us to do tasks that were once unthinkable. The Iot is revolutionizing our way of life and we communicate with technology by bringing it all together on a single network for a variety of uses. Nevertheless, IoT faces many threats in the form of cyber scams, with the likelihood of a Ransomware attack being one of the most severe. Ransomware is a type of malware that prevents access to valuable information and demands payment in return for permission. The ransomware attack is expanding on a daily basis, causing catastrophic consequences like that of the loss of sensitive files, lost productivity, data destruction, consequential damages, and downtime for industries. As a result of the downtime, millions of dollars are lost every day. Organizations will have to update their annual cybersecurity targets as a result and will need to develop a proper resilience and recovery strategy to maintain operations going. However, before moving on with a practical way, it is necessary to synthesize the relevant facts and statistics regarding this critical assault so that researchers and practitioners are aware of it. To close this gap, this paper offers a concise overview of Ransomware's evolution, detection, and mitigation in the light of the Internet of Things. This paper stands out in many ways: first, it goes into more detail about Ransomware's evolution on the Internet of Things. Second, it covers a variety of topics related to Ransomware attacks on IoT, such as different forms of Ransomware, and how to prevent them. Ransomware is still being researched. Existing methods for preventing and mitigating Ransomware attacks in IoT, as well as how to deal with an infected server, whether to pay the ransom and potential emerging Ransomware dissemination patterns in IoT. Finally, to illustrate various study directions, an outline of current research is given. Finally, analysts and experts working on IoT security technologies should find this thorough review useful.

Introduction

The IoT system is a combination of processors, detectors, drivers, applications and other data storage and retrieval elements.[1] Few of the most common benefits of IoT include automation, networking, and knowledge flow with less time and effort.[2] IoT sensors have the ability to coordinate and process data, making them smart machines From the home to major manufacturing and commercial markets, smart devices are already an increasingly significant part of human life.[3] The Internet of Things can made massive ingenuity to our lives by integrating indirect communication between users and smart devices, but it has also made it vulnerable to a number of cyber fraud.[4/6]

Ransomware are among the most dangerous dangers that the Internet of Things has ever seen. The term "Ransomware" is a mixture of the terms "Ransom" and "Ware”. The word "ransomware" defined as a form of malware attack that demands payment in exchange for access to the victim's files. Attacking Ransomware, the attacker tries to cipher data of the target using a powerful encrypting algorithm and asks to pay for a decryption key (typically Bitcoins).[7] Temporary or permanent loss of files, interruption of daily device processes, and financial loss are all possible outcomes of a Ransomware attack.[8] Crypto Ransomware and locker Ransomware are the two most frequent types.[6/9] Attackers encrypt sensitive information in crypto Ransomware from the computer of the victims and ask for a ransom to be deciphered. This restitution is normally required by Bitcoins or some other means that cannot be traced. Crypto Ransomware would not encrypt a victim's whole hard drive; however, it searches for major file extensions that cause the majority of victims. [10/11] Crypto Ransomware employs even symmetrical and asymmetrical data encryption techniques. Any of the latest crypto Ransomware attacks include DirtyDecrypt, TelsaCrypt, Crypt Locker, PadCrypt, and Cryptowall. [12/16] The Locker Ransomware virus encrypts and seals the data on a victim's device. A ransomware assault has been detected in your locker. The victim's information is safe, but access is restricted due to the system's limited computing power. It normally encrypts computers or user interfaces and requests a ransom to unlock them. Locker Ransomware comes in several ways, including DMA Locker, Locky Ransomware, Winlock, TorrentLocker, and CTB-Locker,. [3,17–19]

In 1989, "PC Cyborg," the whole first Windows crypto Ransomware attack, was released. a symmetric key and a combination of setup vectors to encrypt the victim's device data files. [21,22]Ransomware attacks became less frequent in the late 1990s and early 2000s due to a lack of personal computers and limited internet use. [23] Since 2005, ransomware has been a potent cyber-attack, and due to the maturation of the Internet of Things, there has been a huge increase in Ransomware attacks since 2012. The Internet of Things had infiltrated virtually every area of life by 2013, including home and construction automation. [22,24]. According to Figure 1 shows that the cost of ransomware attacks has grown exponentially so far this year.

What happens if a business or person is the target of a ransomware attack, This would only be feasible if a detailed image of Ransomware attacks is provided in the form of a comprehensive survey, especially in the sense of IoT. There is no detailed survey of Ransomware attacks, particularly in the context of the Internet of Things. This report is used to explain how ransomware affected IOT .

Internet of Things (IoT) , Because of the integration of various technology and connectivity solutions, this is a groundbreaking paradigm that has gained a lot of momentum in recent years. 28]. Intelligent computers, actuators, RFID tags and cameras are only a few of the topics that make up the Internet of Things. which engage with one another and cooperate to achieve a shared goal. The IOT is rapidly gaining in importance due to its significant impact on almost every aspect of users' lives and behavior. As seen in Figure 2, both of the above meaning present the same notion of IoT, which is that IoT connects real objects to the internet and is a steadily expanding phenomenon.

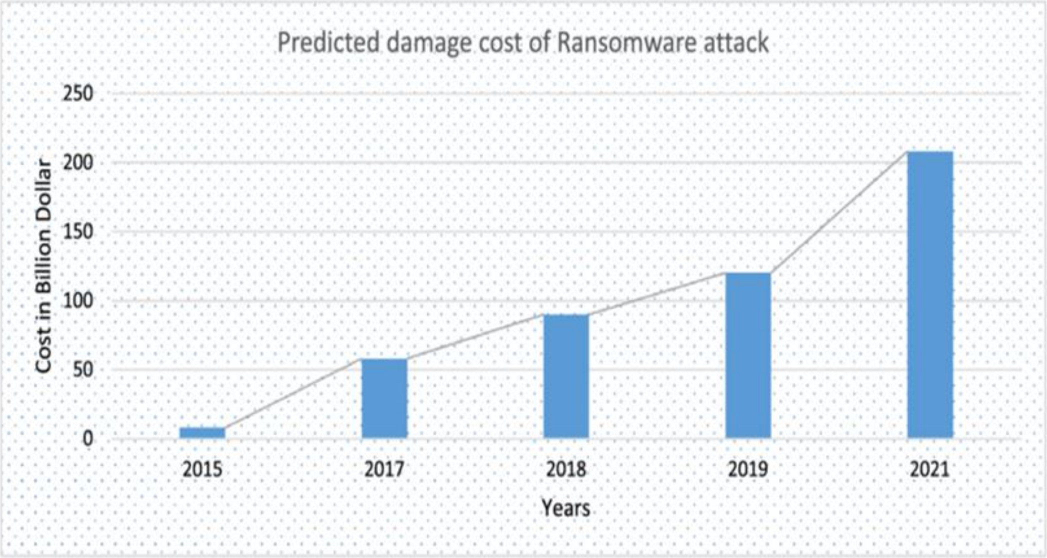


Figure 1: predicted damaged cost of Ransomware.[20]

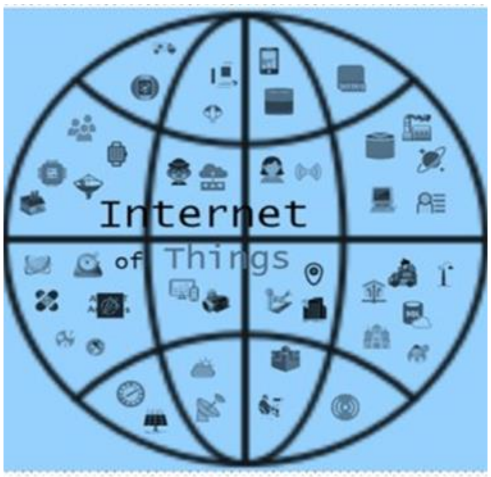


Figure 2: Internet of things.

Ransomware Types,

locked Ransomware and Crypto Ransomware are the two major forms of Ransomware, as we previously mentioned. Both types of Ransomware start with a web connection or an email attachment , and The Ransomware targets the victim's computer by leveraging established operating system vulnerabilities while the user opens the attachment or clicks on the obtained weblink.. Figure 3 depicts the Ransomware threat taxonomy.

The Ransomware targets the victim's computer by leveraging established operating system vulnerabilities while the user opens the attachment or clicks on the obtained weblinkThis method of attack usually uses a 24-bit encryption scheme that is nearly difficult to crack without a key. Exploit packs, in addition to email attachments and web linkages, are used to spread Ransomware.

In the situation of exploit kits, the user is infected by visiting a hacked website rather than downloading the attachment or connecting to the site. The hacker then asks the user for currency, which is usually done in Bitcoins. Bitcoin was used to pay the ransom since it is impossible to track down the suspect. When the victim pays the specified price, the hacker will deliver the unlock key. And when hackers are paid, they do not always give the decryption key, and the data is lost forever. Any new Ransomware attacks exploit operating system flaws and replicate themselves to propagate throughout the network. The workings of a crypto Ransomware attack are describe in [34–37] Figure 4.

The ransomware unlocks and locks the victim's phone when the victim opens the attachment or clicks on the weblink in a Locker Ransomware attack. If the victim pays the money, he won't be able to use the machine again. Until the requested ransom is paid, the victim's computer becomes operational. However, the attacker can refuse to open the victim's computer even after obtaining the demanded ransom. [34,35] Figure 5 depicts the Locker Ransomware attack in action.

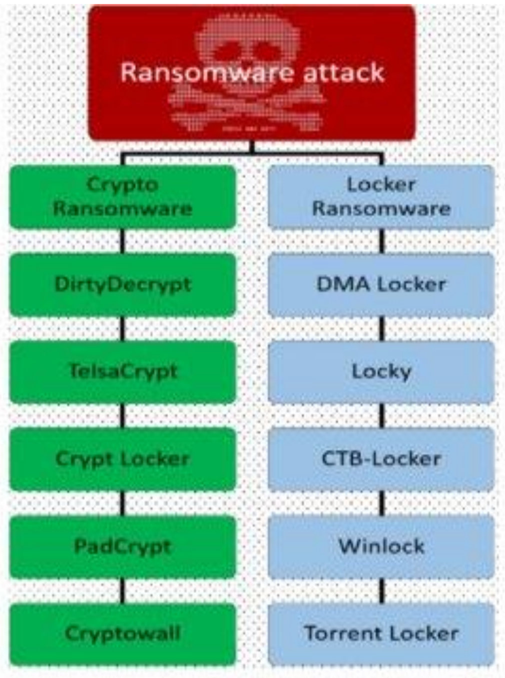


Figure 3: Taxonomy of Ransomware attack.

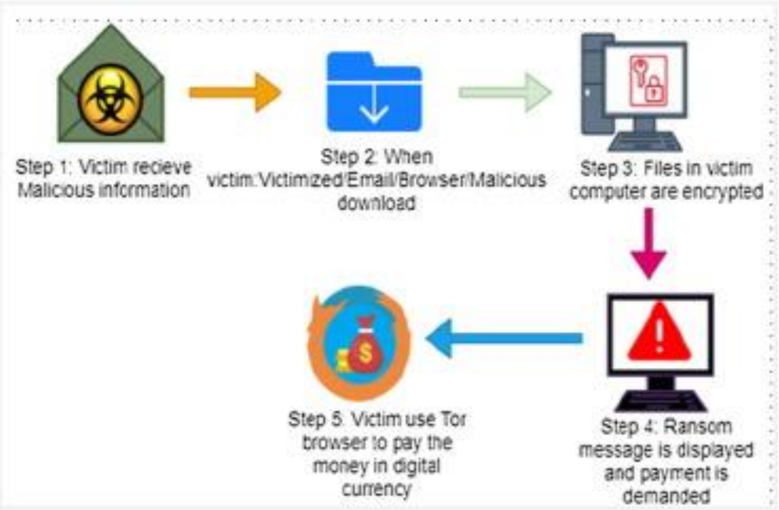

Step 1: Victim recieve Malicious information
Step 2: When victim:Victimized/Email/Browser/Malicious download
Step 3: Files in victim computer are encrypted
Step 4: Ransom message is displayed and payment is demanded
Step 5: Victim use Tor browser to pay the money in digital currency

Figure 4: How crypto Ransomware Work

Evolution

This ransomware has a impositive impact on all aspects of life. However, the exponential development of IoT has brought with it several threats, one of which is the Ransomware threat. As previously stated, ransomware is a form of malware that encrypts or locks the victim's computer data. In order to recover or access his records, the victim must then pay the requested ransom. When the Internet of Things (IoT) expands, so does the threat of ransomware. According to a Symantec survey, Attacks of ransomware increased 113 percent in 2014, with a 4000 percent increase of crypto ransomware [31/32]. Between 2012 and 2015, a Kaspersky report found a five-fold increase in Ransomware attacks[33]. Ransom's rapid growth is no longer limited to individuals; it is now impacting companies as well. [3]The first Ransomware attack, known as Aids Trojan, was introduced in 1989 by a Harvard-trained biologist named Joseph L. Pope. (also known as PC Cyborg). However, since there was insufficient internet access at the time and the concept of the Internet of Things was not yet conceived At an international AIDS conference organized by the World Health Organization, this AIDS Trojan was distributed via floppy disk. This Ransomware encrypts data with a simple encryption method that can be decrypted quickly and easily. [38,39] Despite the fact that ransomware has been around since 1989, it was largely ignored owing to the restricted use of the internet and limited digital currencies until 2005. The concept IoT was proposed in a 2005 study by the International Telecommunication Union to link the world's objects in an intelligent way through technology [40]. As a result, the sophistication of the IoT attack coincided with the maturity of the Ransomware attack. From 2005 to 2021, we'll look at the effects of ransomware attacks.

- **2005:** GPCoder was a malware attack that was released between 2005 and 2008. An email was used as a source to distribute the malware. GPCoder circulated through victim machines after they opened this malicious email, encrypting MS-Office and media data. IoT was still in its infancy at the time, owing to the lack of mobile devices. As a result, the extortion used in the Ransomware attack was remarkably quick and low-tech. This age became remembered as the "age of false antivirus," where unsuspecting computer users were tricked into paying for the removal of a virus that didn't exist [41,42].

- **2006:** Ransom became popular with hackers in 2006. Trojan is a kind of Trojan horse. Cryzip was first released in March of 2006. It copied the data files of the victims into password-protected archived files that could be quickly recovered later. Present Trojan. Cryzip was nothing more than a hacker's effort to try something different. Trojan.archiveus was released the same year, and it was the first ransomware attack to claim a ransom in the form of drugs from real online pharmacies [41,43].

- **2007:** The The first attack in 2007 by Locker Ransomware was aimed against Russia. A pornographical picture was shown on the victim's screen requesting payment by text messages or calling the premium rate number to unlock it. The victim's computer was locked. [22,44].

- **2008:** GPCode is a modern variant of Trojan GPCoder. In the year 2006, AK debuted**.** It encrypts victims' data files with a 1024-bit RSA key and demands $100 to $200 in digital gold currency through the Liberty Reserve system [45]. An centralized digital currency service the liberty Reserve that has been used to allow username, email and birth date address to send money to others. [46,47].

- **2010:** Winlock is a form of Ransomware attack that first emerged in 2010[48]. Winlock disables the computer's I/O interface, making the victim believe it is safe. The Winlock assault Plays a blurred image on the phone of the victim and demands an extra SMS of $10 to receive the unlock code. Ten people were arrested in Moscow in the same year for their involvement in the Winlock attack, and they made more than $16 million from the SMS program. [49].

- **2011- 2012:** Prior to 2011, there were no digital currencies or Internet of Things technology, direct consumer extortion was restricted. The Reveton Ransomware assault, a version of locker Ransomware, was released in 2011–12This was a malware attack in which the browser of the user was locked on a compromised website after one visit only. The The message on Reveton's Victim's machine disappointed the victim because, in response to any major cyber code breaches, it appears from the content of the message that the message is sent by the official body. Victims were told that unless they paid the requested ransom using a bribery payment form, they would face serious criminal charges [50,51].

- 2013: The dirty decrypt ransomware was released in July 2013, and it is part of the crypto Ransomware family. It encrypts eight different types of victim's files and demands payment [52]. This ransomware was usually distributed through exploit kits or using adult-oriented websites. It spread by exploiting malicious JavaScript files that were uploaded to pornographic websites. This attack mostly attacked Windows 2000, NT, XP, Vista, and Windows 2007 versions of the operating system. When dirty decrypt is activated, malicious files are created in different Windows folders [53].

-2014: In 2014, The Ransomware crypto family, such as the Cryptowall locker, came into being. When a user opens a spam email or clicks on a malicious connection, The file is instantly downloaded and running TorrentLocker, or Cryptowall. [54]. Another method of attack was from a malicious connection that immediately redirects the user to a TorrentLocker or Cryptowall file download [55]. One of the most significant flaws of both attacks is that they both snatch email contacts from compromised machines and scatter them across the internet [56]. Both attacks are performing malicious code using a hollow method technique the A malicious code injection technique is a hollow method in which malicious code substitutes for a memory operation. When these attacks are successful, the user's device is locked, and a ransom note appears on the screen [57]. CTB-locker, one of the most recent versions of TorrentLocker, first appeared on the scene in December 2014. By the end of 2014, IoT had matured to the point that CTB-Locker could be Spam or malicious links are transmitted. CTB-Locker gets its name from its main benefit: Curve-Tor- Bitcoins. Curves are derived Elliptic curve-based technique of cryptography used to encrypt victim information using this Ransomware attack. Core is The currency of the ransom used to pay the decryption key was obtained from a malicious TOR server which was very difficult to downgrade. [58].

- 2015: IoT's widespread adoption and sophistication have resulted in numerous positive changes and conveniences in human life, especially in the widespread use of smart devices. However, the rapid advancement in technology has aided offenders in devising new methods of attack. In 2015, there were several Ransomware attacks that attacked a variety of people and companies, with hackers earning over 4.5 million dollars because of these attacks [59]. With the release of Cryptowall 3.0 in early 2015, criminals have made it more difficult to track. Cryptowall 3.0 is a virus that is both inexpensive and simple to use, and it spreads quickly. This virus doesn't just encrypt the files; it even hides within the operating system.It even wants to put itself in the launch folder. In the worst-case scenario, it deletes sensitive data, making it more difficult to recover them. [60] TelsaCrypt is a crypto Ransomware family that first emerged in February 2015. TelsaCrypt attacks the victim's game files, among other kinds of files. TelsaCrypt encrypts the files of its victims and demands $500 for decryption, which is doubled if the payment is not made.[61]. Cryptowall 4.0, a new version of the ransomware, was also released in 2015. Cryptowall 4.0 not only encrypts victims' files, but it also switches their names, making it impossible for victims to search their backups.[62] Linux is being attacked by yet another ransomware strain. Encoder, a Ransomware that targets Linux servers and websites, was also discovered in late 2015. It spread by taking advantage of a bug in Magento, an open-source e-commerce program. Linux has locked files. The encoder shows the results.

The file extensions are password-protected. Payment in the form of Bitcoins is requested after the victim file has been infected. However, unlike Cryptowall 3.0, this Ransomware attack does not double the bill. [63]

-2016: Since the most well-known and disruptive cybercrimes affect both individuals and small and medium-sized businesses, 2016 has been dubbed "Ransomware Attacks Year." Locky and mamba were two of the most dangerous Ransomware strains to emerge in 2016. The public transportation infrastructure of San Francisco was one of the most well-publicized mamba attacks in 2016, and it also attacked the Saudi Arabian business network in 2017 [64,65]. Mamba Ransomware doesn't just encrypt a few files; it encrypts the entire hard drive of the user device. It encrypts the whole hard disk and its partitions with the diskcryptor program, which can only be decrypted by a hacker after paying the requested ransom [66]. The Locky Ransomware threat first surfaced in early 2016, and it has remained effective thanks to its massive attack surface, stealth, and costly money extortion methods. Term documents and spam emails are infected with Locky Ransomware, which embeds macros.[67]In 2016, the first SimpleLocker to appear, was the key target of this Ransomware assault, and the most popular operating system for smartphones and tablets at the time, Android. It was the first time a Ransomware attack had been launched against the Android network, encrypting files and rendering them unusable by the victim.[68] Another ransomware threat has been discovered. Cerber is a Ransomware variant that targets victims' computers even though they are not connected to the internet, making it impossible for victims to protect their machines by unplugging them. The survivor of a Cerber attack opens an email with an MS-word text attachment. Cerber encrypts the file until the user downloads it and adjust their suffix to. Cerber.[69]

Petya Ransomware, Discovered in May 2016 for the first time, infects a Windows-based system's boot log, encrypting hard disk files and preventing the device from booting. It spread across several big films, as well as commercials. When the Petya Ransomware infects a device, it requests a $300 ransom in Bitcoins [71]. In mid-2016, another Ransom CryptXXX emerged, The same cyber mob behind Reveton this time. CryptXXX also encrypts files and targets the Windows operating system. As CryptXXX infects a victim, a ransom of around 2.4Bitcoins is requested to obtain the decryption key [72]. As well discovered RAA Ransomware in 2016. This one was composed in Java scripting language and is regarded as a utility. RAA is typically e-mailed or password-protected, making antivirus software harder to detect. Instead of regular people, RAA typically targets enterprises [73]. Satana, a Ransomware attack that targets the boot record and stops the device from booting, first emerged in 2016 [66]. Satana Ransomware hides in a temporary folder with a different name, prompting the user to download the malicious file over and over before the user clicks yes. Satana waits until the device restarts before informing the user that the system is corrupted after installing and running its malicious code.[74] Stampado Ransomware was also discovered in 2016, and it has self-propagating features that affects the entire network. It could encrypt files with over 1200 extensions and claim a ransom payment within 96 hours. The files are erased if the victim does not pay the ransom within a certain period [69,75]. Figure 6 depicts the history of Ransomware attacks from 2005 to 2016, as well as the attack technique.

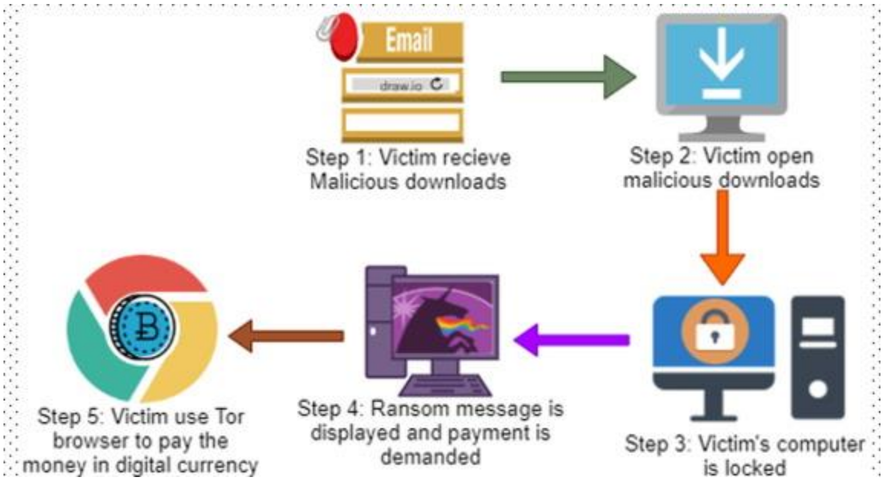

Email
draw.io
Step 1: Victim recieve Malicious downloads
Step 2: Victim open malicious downloads
Step 3: Victim's computer is locked
Step 4: Ransom message is displayed and payment is demanded
Step 5: Victim use Tor browser to pay the money in digital currency

Figure 5: How locker Ransomware Work.

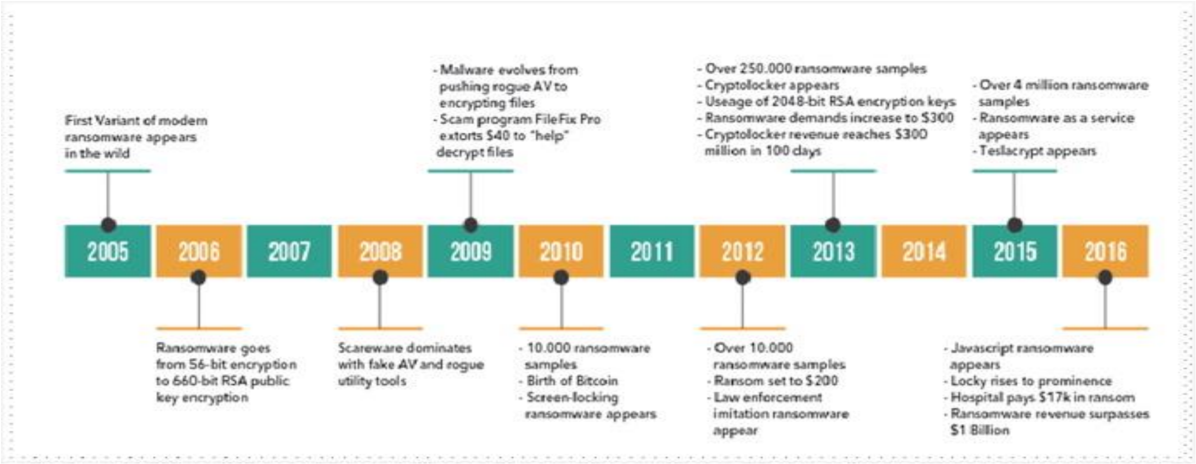
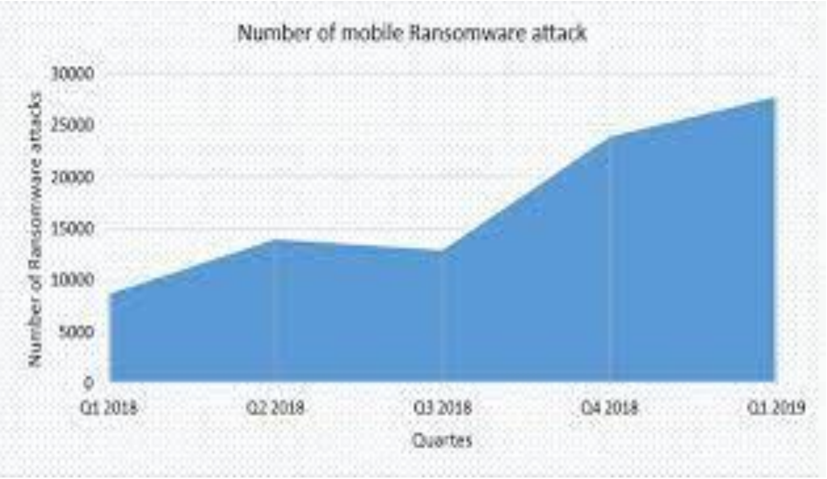

2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
First Variant of modern ransomware appears in the wild
Ransomware goes from 56-bit encryption to 660-bit RSA public key encryption
Scareware dominates with fake AV and rogue utility tools
- Malware evolves from pushing rogue AV to encrypting files
- Scam program FileFix Pro extorts $40 to "help" decrypt files
- 10.000 ransomware samples
- Birth of Bitcoin
- Screen-locking ransomware appears
- Over 10.000 ransomware samples
- Ransom set to $200
- Law enforcement imitation ransomware appear
- Over 250.000 ransomware samples
- Cryptolocker appears
- Useage of 2048-bit RSA encryption keys
- Ransomware demands increase to $300
- Cryptolocker revenue reaches $300 million in 100 days
- Over 4 million ransomware samples
- Ransomware as a service appears
- Teslacrypt appears
- Javascript ransomware appears
- Locky rises to prominence
- Hospital pays $17k in ransom
- Ransomware revenue surpasses $1 Billion

Figure 6: Evolution of Ransomware [70]

Figure 7: Number of mobile Ransomware attack [82]



-2017- 2019: NotPetya, one of the most dangerous Ransomware attacks, first emerged in June 2017 and quickly became the world's second most serious security problem.

This is a tweaked version of the 2016 Petya Ransomware attack. In contrast to Petya, NotPetya encrypts Not just a few files, but the entire system. It reboots the infected computer and modifies the master boot log, rendering it inoperable. Since the master boot record is used to find any file in the system, the system's user is unable to access any file [71,76] . WannaCry, also known as WannaCrypt Ransomware, debuted as a huge attack in May 2017. The distinction between WannaCrypt and past Ransomware attacks was the magnitude of the attacks. WannaCrypt infected over 200,000 machines in over 150 countries around the world [77]. Jaff, Spora, Cryptomix, Jigsaw, Bad Bunny, Breaking Bad, SamSam, and Crysis are some of the other Ransomware attacks that occurred in 2017–2018 [71,78].

In terms of Ransomware attacks, the year 2019 has seen a lot of challenges. In early 2019, a Ransomware attack hit one of Denmark's most well-known hearing aid suppliers, resulting in a loss of about $100 million. In the same year, Pitney Bowes, a major transportation firm headquartered in the United States, was hit by Ransomware. In the United States, there was a surge of ransomware attacks this year, with 90 percent of Fortune 500 firms being affected.

The 360 Security Centre recently discovered a new form of ransomware known as CCryptor. This virus spreads by way of the victim sent fishing emails and a ransomware attack. machine exploiting the CVE-2017–11882 flaw. Using the RSA + AES256 encryption method, this Ransomware attack will encrypt files in 362 different formats. It encrypts user accounts and waits 10 days for the ransomware to be released; if the ransom is not paid within 10 days, all files will be erased.

Figure 7 depicts from the first quarter of 2018 to the first quarter of 2019, the number of smartphone Ransomware attacks increased. This figure was derived from Kaspersky Lab's research, which is a well-known international cybersecurity and antivirus company organization based in Moscow. According to them, Figure 7. There is a constantly increasing number of ransomware attacks. In particular, the increasing use of intelligent IoT devices, notably cellular telephones. This emphasizes the importance of protecting people and organizations from Ransomware attacks, as well as providing analysts and experts with up-to-date information on the Ransomware threat.

-2020- 2021:

It's hard to imagine that Sophos observers were awestruck two years ago when the operators of the ransomware known as SamSam made a $6 million profit. In a 2020 ransomware attack that Sophos referred to, the ransomware operators began talks with a dollar sum that was more than double what the SamSam gang had received in 32 months of service. According to reports, in the aftermath of the COVID-19 pandemic, the year 2020 saw a double ransomware assault attributable to remote working community. The biggest reason for the increase in cyber-attacks was a lack of work from home cyber security measures. Not to mention that another major corporation, Gyrodata, was recently hit by a massive ransomware attack. The cyber threat world has changed in comparison, and cyber criminals are becoming more advanced. They are now running back-to-back cyber-attacks to compromise the data of small and large businesses. Furthermore, numerous ransomware families have now developed advanced methods for stealing confidential data. BFSI (banking, financial services, and insurance), IT, manufacturing, government, and other industry verticals are currently gold mines for cyber criminals looking to steal sensitive data.

Ransomware has emerged as one of the most worrying challenges for companies around the world this year. By gaining unauthorized access to an organization's network, this attack blocks the organization's financial, confidential or sensitive information. Cyber attackers claim a ransom in exchange for keys to data or devices that have been blocked.

These cyber criminals compromise private data by making it public if the demanded ransom is not paid in a timely or timely manner. These threat actors, on the other hand, have been more adept at targeting their victims than in the past. They steal encrypted data and market it for a profit on cybercrime sites at low prices.

Another critical factor to be aware of in terms of ransomware attacks in 2021 is that hackers and cybercriminals are engaged in "big game hunting," as cybersecurity company

CrowdStrike has coined the word figure 8. Instead of, say, adding an attachment to a bunch

of spam emails in the hopes of having somebody to click on it by mistake, cybercriminals now go deep into networks. Those old-school attacks usually yielded modest ransoms, but we're seeing more organized and strategic ransomware deployment these days.

“Attackers are now going after the whole network, not just the big game,” Pace said. “Their first instinct is not to install malware as they use phishing to get someone to click on a connection as an entry point into the enterprise. It's to play a longer game, escalate rights, travel laterally, do some reconnaissance, locate the files, and then go after spreading ransomware across the entire network.

.”

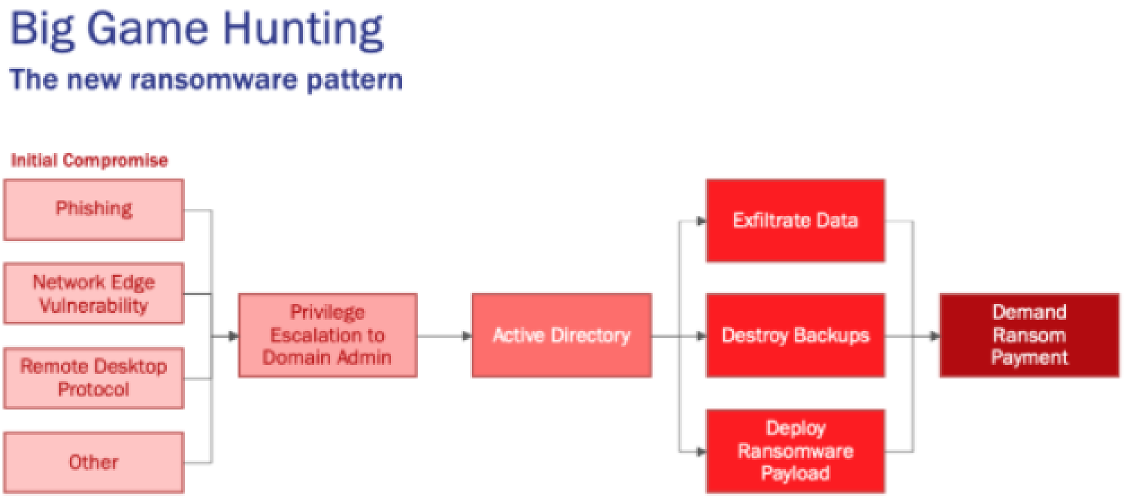


Figure 8: Big game hunting

Future development in the area

Since the Internet of Things is still a relatively recent phenomenon, there aren't many ransomware attacks for IoT in the literature. Below are few examples of ransomware in IoT case studies and possibilities. [83/84]

- **Smart Vehicles**

In recent years, even ordinary commercial vehicles have had some level of internet connectivity. Most automobiles now have operating systems, making them potential IoT devices. As a result, when they are connected to the internet, they are vulnerable to Ransomware attacks. Since the bulk of these units never undergo a manufacturer update, they are vulnerable to network attacks.

A ransomware assault on a self-driving vehicle can be unsafe because it has the power to stimulate your steering. For the ransom, the perpetrator may effectively lock the vehicle and claim money, or even lock the steering wheel. Since criminals would be able to grab hold of the vehicle while driving, this will cause serious damage and put the user's life in danger. The assailants might start driving your car away from traffic and into abandoned areas.

This has a negative impact on the economy. Larger linked vehicles transporting goods can be hacked and taken over, resulting in financial losses since the shipment must arrive on schedule. This forces the owner to pay the ransom as soon as possible so any countermeasures will take a long time. The risk of harm is high, and there are several other options for connected vehicles.

- **Smart Homes**

  In developing countries, the number of smart homes is steadily growing. Through the internet, Smart home systems can be operated remotely from any location on the planet. Houses and computers can be locked and unlocked remotely, as well as switched on and off. Nevertheless , these benefits come with a significant disadvantage: hackers would be able to obtain access to and monitor the computers in people's homes. They have the ability to raise our utility rates and even lock our homes, preventing entrance or escape. This provides a massive risk for ransomware because a high ransom could be offered in exchange for the person's permission to leave their home. Repeated attacks are also possible because the perpetrator will likely know his way through the network and will be able to replicate the process, thus constantly requesting ransoms.

- **Medical Equipment**

With the advent of IoT products, the medical sector is undergoing a significant transformation. These instruments are used to diagnose a variety of devices as well as to keep people alive. The machines can be operated remotely over the internet, allowing a doctor or medical official to monitor chronic patients even while they are at home. Doctors can also be able to monitor bedridden patients by controlling oxygen and other supplies.

When hackers get their hands on this code, they can do a lot of harm. however, they take advantage of the ability to infect computers with malware, allowing them to take ownership of the system. This puts the patients' lives in jeopardy because they can give doctors false information while simultaneously weakening their health. Attacks on these life-saving devices, as well as other devices such as MRIs, face a significant danger to the Internet of Things.

Since these machines in hospitals are linked to one another by The infection may spread to other devices through wired or wireless connections. allowing the hackers to take possession of them. As a result, the whole network is hacked, resulting in a multiple-fold increase in the ransom fee. This sets the hospital's processes in jeopardy and gives hackers a leg up.

- **Wearable Devices**

  Since safety features are minimal, there is an increasing variety of portable technology with a simple target. An attack on the machine may result in the loss of any records. Hackers normally claim a small ransom to convince users to pay the fee rather than resetting their computers and destroying their files.

Prevent and Mitigation,

Since each attack is unique, there is no one-size-fits-all approach to defending against them. As a result the whole network must be checked on a daily basis for any traces of ransomware or attacks. Users must also be taught to turn off machines and upgrade the correct firmware offered by the organization on a regular basis. Other protection techniques include scanning the ransomware on a layer-by-layer basis [83, 84]. Despite these safeguards, attackers gain access to the systems. with other bugs, loopholes, or even carelessness on the part of the users If this occurs, the following procedure must be used to undo the damage as soon as possible.

- To uninstall the malware or minimize the potential harm to the IoT network, a team of experts must be enlisted. The machines should be turned off, and the virus should be removed from the network. To ensure the service is not disrupted, an external interface can be attached in place of the affected machine.

- Although not everyone has the financial means or the opportunity to recruit consultants, consumers must have a clear understanding of how to deal with these risks. To prevent these attacks and improve device stability, users must use a dependable protection program.

- Since data is the primary focus of threats, users must periodically back up their data to other servers. This can allow for fast data replacement even though the ransomware deletes it. Users should not need to save money to pay the ransom because their data is encrypted and can be shipped anywhere provided it is securely backed up.

The challenges in IoT protection emerge as a result of the exponential growth and sheer number of interconnected devices. Some of the challenges can arise during ransomware mitigation and prevention [85].

- The majority of the time, Ransomware cannot be defeated by merely turning off the computers because The data has indeed been tampered with, and the consumers have no choice but to accept it.

- Users can also avoid downloading those kinds of files and only do so when absolutely appropriate. System manufacturers can include a list of predefined file types, informing users about the files are required and which are protected.

- Since the network and hardware are extremely heterogeneous, adding uniformity to the architecture has disadvantages. The security protocols must be tailored to the specific types of ransomware. As a result, new threats go undetected before the code is updated to spot them.

Related works,

The writers of [79] suggested an artificial intelligence-based mechanism for detecting ransomware in IoT. To validate the existence of ransomware, the identification approach looks at the battery usage of the computers. The disparity in battery use between legitimate and malicious applications is kept track of. Various machine learning algorithms are used to implement the proposed procedure. The results of each algorithm are recorded using different metrics such as detection rate, precision, and recall. The authors of [80] studied ransomware for two years and found it to be effective. Ransomware attacks are expected to grow in the coming years, according to estimates. The developers have proposed a mitigation method for the Cryptowall ransomware, which is part of the Crypto ransomware family. The proposed approach tracks traffic between Cryptowall's Command and Control (C&C) server and IoT computers. Cryptowall’s conduct is also examined. To detect ransomware attacks, TCP/IP headers from traffic are collected. The research discussed in [81] has shed light on the different IoT communication protocols. In addition, the paper discusses the multiple IoT implementations. Deep learning algorithms for classification have been implemented by the authors. The ransomware was detected using the K Nearest Neighbour (KNN) and Random Forest classifiers. According to the findings, KNN outperforms the other classifiers used in the experiment. [82] proposes a solution for keeping files secure from ransomware. It is recommended that an operating system program be developed that restricts access to the file system. The application is designed to run on cloud servers. Using the Message Digest (MD5) algorithm, the software compresses the files into a single file.

Conclusion

This digital advancement is making our lives simpler and helping us to achieve goals that were previously unattainable. In bridging this gap quickly and conveniently the Internet of Things (IoT) plays a crucial role. In a website that is combined with a number of daily applications, The Internet of Things (IoT) is changing our way of living and how we interact with technology. However, it is important to handle them in a safe and responsible way and to maintain new applications. This are susceptible to a variety of security risks, particularly ransomware, in which unauthorized users / hackers may limit data or access and make it difficult to recover it safely.

According to the literature, ransomware attacks are expected to increase fivefold by 2025, costing more than $16 trillion in ransom payments. Furthermore, this research reveals that a ransomware attack occurs every 11 seconds around the world. Furthermore, this study centered on existing IoT-related ransomware attacks, mitigating strategies, and proposed ransomware prevention methods. After a ransomware attack, prevention becomes faster than recovery. Finally, this report delves further into different facets of ransomware, such as its ransom payment rules evolution, prevention methods, data volume, taxonomy, and infection year by year.

1. References

[1] Azmoodeh A et al. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. J Ambient Intell Hum Comput 2017:1–12.

[2] Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus Horiz 2015;58(4):431–40.

[3] Zahra A, Shah MA. IoT based ransomware growth rate evaluation and detection using command and control blacklisting. IEEE.

[4] Koopman, M., Preventing Ransomware on the Internet of Things. 2017.

[5] Sharma, P., S. Zawar, and S.B. Patil. Ransomware Analysis: Internet of Things (Iot) Security Issues, Challenges and Open Problems Inthe Context of Worldwide Scenario of Security of Systems and Malware Attacks. in International conference on recent Innovation in Engineering and Management. 2016.

[6] Yaqoob I et al. !!

[65] Alelyani S, Kumar H. Overview of Cyberattack on Saudi Organizations. J Info Security Cybercrimes Resear (JISCR) 2018:1(1).

[66] Mehnaz, S., A. Mudgerikar, and E. Bertino. RWGuard: A Real-Time Detection System Against Cryptographic Ransomware. in International Symposium on Research in Attacks, Intrusions, and Defenses. 2018. Springer.

[67] Homayoun S et al. Know abnormal, find evil: Frequent pattern mining for ransomware threat hunting and intelligence. IEEE Trans Emerging Top Comput 2017.

[68] Mercaldo F, Nardone V, Santone A. Ransomware inside out. IEEE; 2016.

[69] Ganorkar SS, Kandasamy K. Understanding and defending crypto-ransomware. ARPN J Eng Appl Sci 2017;12(12):3920–5.

[70] Matthias Gruber, Evolution of Ransomware, Detecon Switzerland, Accessed on December 2019.

[71] Fayi, S.Y.A., What Petya/NotPetya ransomware is and what its remidiations are, in Information Technology-New Generations. 2018, Springer. p. 93-100.

[72] Paquet-Clouston, M., B. Haslhofer, and B. Dupont, Ransomware payments in the bitcoin ecosystem. arXiv preprint arXiv:1804.04080, 2018.

[73] Aziz SM. Ransomware in High-Risk Environments. Information Technology Capstone Research Project Reports. 2016;1.

[74] Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science 2019;8(1):2.

[75] Kawaguchi Y, Yamada A, Ozawa S, AI, Web-Contents Analyzer for Monitoring Underground Marketplace. Springer; 2017.

[76] Scaife N, Traynor P, Butler K. Making sense of the ransomware mess (and planning a sensible path forward). IEEE Potentials 2017;36(6):28–31.

[77] Furnell S, Emm D. The ABC of ransomware protection. Computer Fraud & Security 2017;2017(10):5–11.

[78] Bajpai, P., A.K. Sood, and R. Enbody. A key-management-based taxonomy for ransomware. in 2018 APWG Symposium on Electronic Crime Research (eCrime). 2018. IEEE

[79] A. Zahra and M. A. Shah, "IoT based ransomware growth rate evaluation and detection using command and control blacklisting," ICAC 2017 - 2017 23rd IEEE Int. Conf. Autom. Comput. Addressing Glob. Challenges through Autom. Comput., no. September, pp. 7–8, 2017.

[80] A. Dash, "Ransomware Auto-Detection In IoT Devices Using Machine Learning," no. December, pp. 0–10, 2018.

[81] M. Baykara and B. Sekin, "A novel approach to ransomware: Designing a safe zone system," 6th Int. Symp. Digit.
Forensic Secur. ISDFS 2018 - Proceeding, vol. 2018-Janua, no. March, pp. 1–5, 2018.

[82] C. Science, C. Science, C. Science, "Naive Bayesian Classifier And Pca For Web Link Spam," vol. 1, no. 1, 2014.

[83] Castilho SD, Godoy EP, Castilho TWL, Salmen AF. Proposed model to implement high-level Information Security in Internet of Things. In: 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC) [Internet]. IEEE; 2017. p. 165–70. Available from: http://ieeexplore.ieee.org/document/7946425/

[84] Stewart CE, Vasu AM, Keller E. Communityguard: A crowdsourced home cyber-security system. In: Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization - SDN-NFVSec '17 [Internet]. New York, New York, USA: ACM Press; 2017. p. 1–6 Available from: http://dl.acm.org/citation.cfm?doid=3040992.304099

[85] Solangi ZA, Solangi YA, Chandio S, bt. S. Abd. Aziz M, bin Hamzah MS, Shah A. The future of data privacy and security concerns in Internet of Things. In: 2018 IEEE

International Conference on Innovative Research and Development (ICIRD) [Internet]. IEEE; 2018. p. 1–4. Available from: https://ieeexplore.ieee.org/document/8376320/