DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5858

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A SURVEY ON RANSOMEWARE: EVOLUTION, GROWTH, AND IMPACT

Hirra Sultan
Department of Computer Science & Engineering,
School of Engineering Sciences & Technology,
Jamia Hamdard,
New Delhi, India

Aqeel Khalique
Department of Computer Science & Engineering,
School of Engineering Sciences & Technology,
Jamia Hamdard,
New Delhi, India

Shah Imran Alam
Department of Computer Science & Engineering,
School of Engineering Sciences & Technology,
Jamia Hamdard,
New Delhi, India

Safdar Tanweer
Department of Computer Science & Engineering,
School of Engineering Sciences & Technology,
Jamia Hamdard,
New Delhi, India

Abstract: In Information & Communication Technology (ICT), communication plays a vital role in the current era of technology. Nowadays, ICT is being used by the huge population to communicate for different purposes. For security reason, several security mechanisms are taken as standard in different communication technologies. However, security mechanisms only prevent the attack or sometimes reduce the intensity/loss of the damage incurred by the attack. Several attacks have evolved over last two decades as a result of the inability to reduce the intensity/loss of the damage imposed by these attacks. Among lots of attacks, one such attack became very popular because of its impact, lack of knowledge/awareness to prevent it from occurring and technological advancement of the concept used in it. The attack was evolved from Malware and is now commonly called as Ransomware. It is a malware that can encrypt all data of a user and make it inaccessible to the user unless a ransom amount is paid. The widespread attacks of ransomware across the globe havegiven it popularity including huge amounts of data and financial loss. The ransomware industry generated revenue of USD 5 billion in 2017. In 2018, it is predicted to increase even more. In this paper, we discuss the origin, evolution, and growth of ransomware. The various families of ransomware, their attacks, and prevention from these attacks have been presented. We also discuss various parameters contributing the growth of these attacks in today's technologically advanced world. We conclude with an analysis of several resulting criteria leading towards the creation of the ransomware industry.

Keywords: Information Security, Intrusion Prevention, Security Attacks, Active Attacks, Malware, Ransomware.

1. INTRODUCTION

In computer networks, security breaches can occur when a vulnerability in network or connection is used to damage/sabotage or do some kind of harm to the user. Attacks are mainly of two types, active attacks, and passive attacks. These act either actively, or inactively to steal data, identity or money by using various methods and mechanisms. Examples are snooping, masquerading, replaying, DOS etc. [1] [2] [3].

Malware is an abbreviated term for "Malicious Software". Such software programs are specifically designed to gain access or damage victim's computer. A lot of malware is created today for profit through forced advertising (adware), stealing information (spyware), spreading spam emails or child pornography (zombie computer) or to extort money (ransomware) [4].

Ransomware is a type of malicious software that hinders working of a computer or user access to data and certain programs till a demand is fulfilled[5]. The demand is usually a ransom amount to be paid for access to data[18]. Some malware may merely scare the user into paying the attackers by creating a pop-up on screen, while others may go to the extent of making changes to the boot sector of the operating system and encrypting everything[22]. There has been an increase in ransomware attacks since 2012 [26]. Digital cash/currency provides anonymity to the user and enables hackers to escape prosecution and hence the increase in such attacks[28][30] [32].

In this paper, we have done review study on ransomware. The paper is organized in the following manner. Section 1 starts with an introduction and discusses types of ransomware and working of ransomware in subsections. Section 2 discussesthe history of ransomware and their variants. Section 3 discusses evolution and growth of ransomware. In Section 4, we present preventive measures and in Section 5,we analyze the trends and factors that led to the growth and success of ransomware. In Section 6, we present future work. In Section 7, we conclude the paper. Section 8 lists all the references used for writing this paper.

A. *Types of Ransomware*

There are three main types of ransomware. The severity of attacks varies for each of them. Scareware poses the least security threat. These types of ransomware merely post a pop-up on the screen informing the user that the computer has been locked. A ransom is demanded. If the user checksthe computer, no files or data is encrypted. The message posted is a hoax[6] [7].

The second type of ransomware is locker. This malware locks up the system and asks for a ransom. It denies the user access to certain programs or to the whole computer till ransom is paid. The severity of this ransomware is medium [8][26].

The third type and highly severe ransomware is crypto-ransomware. These malware programs encrypt user data. Hence user is not able to access any of his files till ransom is paid. In certain cases, the ransom amount is doubled after a specific period of time if the ransom is not paid. These tactics improve the chances of the victim falling prey as they dread having to pay double the initial amount[28][29] [32].

B. *Working of Ransomware*

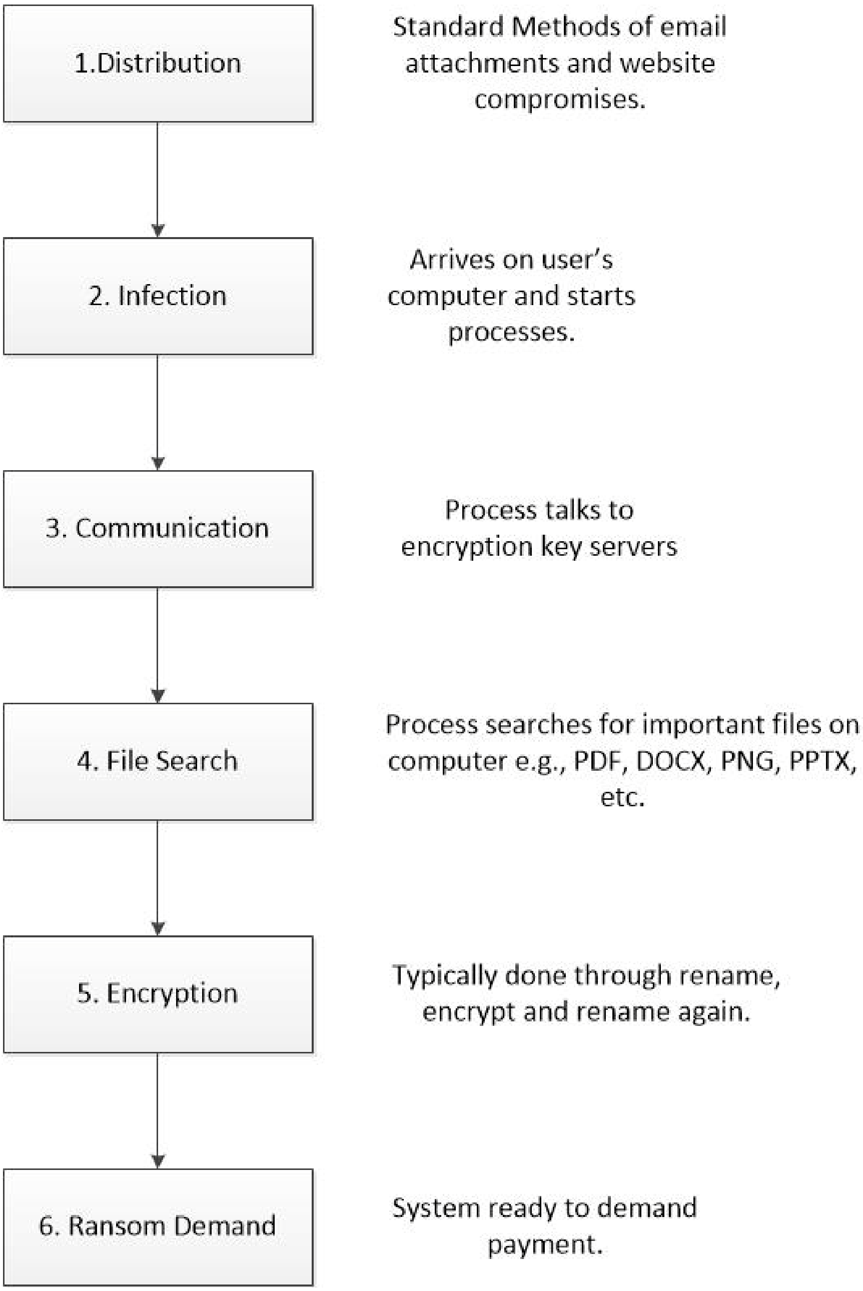

1.Distribution
Standard Methods of email attachments and website compromises.
2. Infection
Arrives on user's computer and starts processes.
3. Communication
Process talks to encryption key servers
4. File Search
Process searches for important files on computer e.g., PDF, DOCX, PNG, PPTX, etc.
5. Encryption
Typically done through rename, encrypt and rename again.
6. Ransom Demand
System ready to demand payment.

Figure 1: Steps involved in successful ransomware execution. [9]

Figure 1 shows the steps of Ransomware attack in execution. There are 6 steps that a ransomware takes to accomplish its goal [5] [6] [25][27][29] [32]. These steps are detailed below:

Step 1: Distribution: For distribution, it uses old tricks of spam emails and phishing, downloads, compromised websites, social engineering, bot infection, SMS message, etc. Since distribution is not easy, they have also started using Pay per Install (PPI) business models. In PPI model, every time ransomware software is installed on host software, the agent gets paid. This is a lucrative offer as cybercriminals don't have to write any code on their own. They only have to capture the market and deliver the software to users. The various techniques used to distribute the software are:

- **Traffic Distribution System (TDS):**

A common method used by such distribution systems is to buy redirected web traffic from a TDS vendor and point it to a website containing the exploit kit. In many cases, the traffic is generated from adult rated websites. If the exploit-kit explores vulnerability in the visiting victim's computer, it leads to drive-by-download of malware.

- **Malvertisement:**

Malicious advertisements (malvertisements) can get posted onto legitimate websites. Clicking on such advertisements causes an immediate infection by ransomware software. Cyber-criminals can use real-time bidding to purchase traffic or ad space to move across borders and target potential victims.

- **Spam Email:**

Spam emails and social engineering are old tools to deliver ransomware to victims' devices. A spam email is sent using botnets to target email ids. They may include malicious attachments that can be downloaded or links to sites that contain exploit kit. The spam emails contain various psychological levers to trick the victim into downloading the malware.

- **Downloaders and Botnets:**

These are another ways of distributing malware across computers. Once they are downloaded, their job is to download malicious software onto the compromised system. Trojan botnets have been known to download ransomware onto computers they have infected.

- **Social Engineering and Self-Propagation:**

Some ransomware contains the property to spread. Once a device is infected, it not only encrypts and locks the device but also spreads to all the contacts on the device. Socially engineered SMS messages are used to propagate to the devices of contacts and infect them as well.

The issue with self-propagating software is that the author is unaware of the devices being encrypted and asked for ransom. Hence the promise to decrypt the device after the ransom is received is broken. In further attacks, the victim may choose not to pay the ransom as the attacker did not fulfill its promise.

- **Affiliate Schemes:**

Cybercriminals have recognized the potential in ransomware. Hence ransomware-as-a-service has been launched. The vendor provides interested people with tools to create their ransomware along with attractive payment incentives. All they have to do is to spread the ransomware far and wide so that the chances of extracting a ransom increase. The affiliate gets as much as 70% of the ransom paid due to his efforts. Hence it becomes a lucrative offer.

Step 2: Infection:

As the malicious software is downloaded onto victims' computer or arrives by other means, it does the following processes to complete its malicious activities. Since awareness about ransomware has increased, the processes may include sophisticated behaviors:

- Install the software on the computer.
- Generate a unique code that identifies the computer.
- The program is set to run at start-up so that it survives a reboot. This is ensured through service entry, scheduled task, AutoRun key etc.
- Deactivate shadow copies, Windows error recovery, and start-up repair.
- Stop antivirus software, Windows Security Center, Windows Defender, Windows Update Service, error reporting, and BITS.
- Inject into explorer.exe and sychost.exe.
- Retrieve IP address of the computer.

Step 3: Communications:

The ransomware process will start communication with encryption-key servers to retrieve the public-key needed to encrypt the data. The encryption algorithm is mainly RSA, RC4, or similar.

Step 4: File Search:

The ransomware searches for files that have common file extensions (such as JPG, PDF, DOCX, PPTX etc.), which are important to the user. These are the files that the software chooses to encrypt and draw ransom.

Step 5: Encryption:

In this step, the ransomware encrypts the identified files and folders by the encryption key downloaded from the servers. The files are moved, renamed and encrypted. It includes changing the file and folder names, their extensions and then using an encryption algorithm.

Step 6: Ransom Demand:

As encryption is completed, the computer screen is taken over and a ransom demand is made. The victim is left with no choice but to pay the ransom.

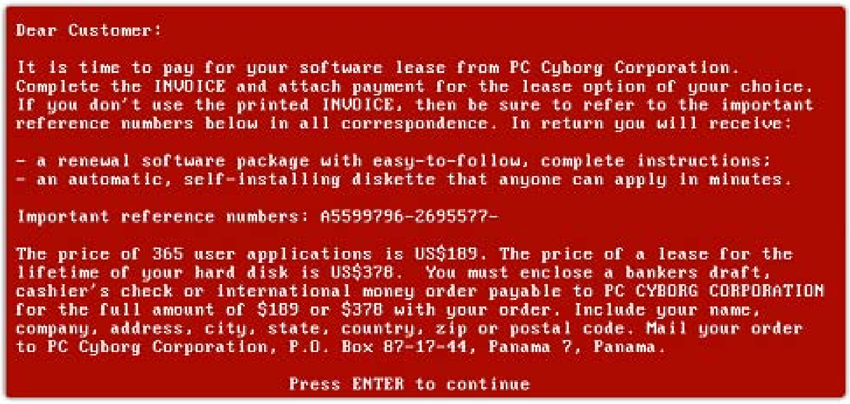
Paying the ransom does not guarantee that a decryption key would be sent, but it does increase the chances of data recovery.Trusting the freely available tools over the internet may not be able to generate the decryption key required to free the data held hostage.

The average time that elapses between download of a malware and a ransom demand is 15 minutes [10].

2. HISTORY OF RANSOMWARE

Ransomware has been around for past 2 decades,although, its use to demand ransom has been recent. Ransomware was first developed in mid-1990. The idea of using asymmetric-key cryptography for attacks was introduced by Adam L. Young and Moti Yung in 1996. In the abstract, Young and Yung said their prototype was meant to show how cryptography could be "used to mount extortion-based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents." Young and Yung presented a proof-of-concept cryptovirus for the Apple Macintosh SE/30 using RSA and TEA asymmetric block ciphers [5] [8][27][30].

The first ransomware attack is attributed to Dr. Joseph Popp, a biologist with Ph.D. from Harvard, in 1989. He distributed ransomware on a floppy disk that was supposed to carry information about AIDS. Upon insertion into a computer, ransomware would install itself, start a counter that would count 90 boot cycles and then create a pop-up demanding ransom. The delay in demand made sure that the source of ransomware was not revealed. But the ransom demand was to be fulfilled by sending money to a post office. This led to tracing of the defaulter. This was called AIDS Trojan Attack [5] [8]. Figure 2 shows the famous screen of AIDS Info Disk Trojan Ransom Splash Page.



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                          Press ENTER to continue
```

Figure 2: AIDS Info Disk Trojan Ransom Splash Page [14]

This challenge remained for all the hackers who wanted to go forward with ransomware. Hence till 2005, there was no real ransomware threat. In 2005, the introduction of e-gold and Liberty Reserve led to ransomware attacks become a reality. E-gold was world's first digital currency that was backed by hard assets of gold and silver bullion. But the growth did not survive as cyber security could trace the person to whom the ransom was sent.

Crypto-currency such as Bitcoin gave hackers the liberty of anonymity. Since Bitcoin makes users anonymous and transactions cannot be traced back to any user, hence, collecting ransom became easy [5] [8]. Table 1 below shows notable Ransomware in chronological order with the year of their appearance and brief detail about them.

A. Variants of Crypto-Ransomware

Crypto-ransomware has many variants with 100's of new families evolving every year. The most famous are discussed below [11] [21] [28].

CRYPTOWALL: It is a family of file-encryption ransomware that first started operations in early 2014. The encryption used in earlier versions is RSA but in later versions, AES is used and then another unique public key is applied to it. Hence obtaining the key for decryption of files becomes very difficult.

CTB-LOCKER: It is another ransomware that encrypts data on user's hard-drive. When decryption is complete, a demand for ransom is made. It uses elliptical curve cryptography. Its infection rates are quite high, uses Tor, Bitcoin and, multiple languages to fulfill operations.

TORRENTLOCKER: It is a family of file-encryption ransomware that is exclusively distributed by spam email. It is geographically targeted, that is, the initial note and ransom note are in local language. It uses AES algorithmbefore it asks for ransom in Bitcoin. It further expands its reach by gathering email addresses from victim computer.

TESLACRYPT: It is one of the most recent ransomware. It uses AES to encrypt certain files on victim's computer and then asks for a ransom to decrypt them.

CRYPVAULT: This ransomware is written as a simple batch script. It uses RSA-1024 for encrypting files and renames the files by adding extension .vault to it.

Table 1: A chronology of notable Ransomware Development

Year	**Brief Detail of Ransomware**
1999	AIDS Trojan (PC Cyborg) becomes the first known ransomware
2006	GPCode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip, and MayArchieve. First to use RSA encryption algorithms.
2008	GPCode.AK. Utilized 1024-bit RSA keys
2010	WinLock is discovered. Primarily seen is Russia, and would flash porn on a computer screen until the user would make a $10 phone call to a premium-rate phone number.
2011	This unnamed ransomware Trojan that was discovered that would lock up the user's computer, and direct the visitor to a fake list of phone numbers which they would call to reactivate their operating systems.
2012	The Reveton ransomware would let the user know their machine has been utilized to download either copyright material or child pornography and would demand the user to pay a fine. This was a form of scareware.
2013	CryptoLocker, the most notorious ransomware, had increased encryption and was extremely difficult to prevent.
2013	Locker is discovered and would demand a ransom payment of $150 in which the user had 72 hours to pay.
2013	CryptoLocker 2.0 was released and utilized Tor to increase anonymity for payment.
2013	Cryptobit, another ransomware that utilized Tor and would encode the first 1024 bits of every file it affects. It would also install Bitcoin miner on victim's machine to earn more profit.

2014	CTB-Locker (Curve, Bitcoin, Tor), would leverage elliptical curve cryptography, Tor for anonymity and Bitcoin for payment.
2014	CryptoWall, another infamous CryptoLocker clone that was responsible for infecting millions of files worldwide using infected emails.
2014	Cryptoblocker did not encrypt Windows files with file sizes over 100 MB. Utilized AES for encryption.
2014	SynoLocker targeted Synology NAS devices and would encrypt all files.
2015	CryptoWall 2.0 used Tor for anonymity and was delivered through multiple attack vectors.
2015	TeslaCrypt and VaultCrypt originally targeted computers that had certain games installed. Newer variants targeted non-gaming machines.
2015	CryptoWall 3.0 shared some of the same characteristics as its predecessors but added additional features such as anti-VM check and was delivered via exploit kits.
2015	CryptoWall 4.0 would encryptnot only data in files but also file names. It would disable any system restore functionality and shadow volume copies.
2015	Chimera was more of a scareware ransomware that not only encrypts files but also threatens the user that they would be published online if the ransom is not paid. Also known as doxing.
2016	Locky is a ransomware that would not only encrypt the user's files but would first scramble the files and then rename file extensions to .locky.
2016	SamSam targets servers instead of end-users. The ransomware exploits vulnerabilities in JBoss application servers and compromises the server to gain shell access. SamSam then proceeds to spread to Windows machines and encrypt their files.

3. EVOLUTION AND GROWTH OF RANSOMWARE

A. Evolution of Ransomware

Ransomware has evolved since 2005 and there are several types of ransomware which are constantly beingdeveloped by attackers. Figure 3 shows the percentage of new familiesof fake AVs, misleading apps, lockers and crypto-ransomware identified between 2005 and 2015 [12]. The figure has a varying number of the families. It can be noted that initially only crypto-ransomware and misleading applications were found. Misleading applications mostlymade use of phishing and other such activities. Crypto-ransomware could not survive in that time due to antivirus applications analyzing and identifying such malware.

By 2009, the misleading applications were replaced by fake antivirus software programs. They would tell the user that some virus has been detected or some problem has occurred. To rectify the same premium version of a paid solution is to be purchased. Threatened for security, victims would pay the same.

The same era saw the rise of lockers. Lockers simply locked the computer screen and asked the victim to make a payment so that the access would be given back. They did not encrypt any data but rendered the computer useless to the victim till the ransom demand was fulfilled.

As lockers, misleading applications and fake antivirus software programs were being identified, crypto-ransomware made a comeback with a stronger encryption algorithm and multiple families. There are so many ransomware families and variants present that it is difficult to study all of them. They all include some minor changes in the code so that detection is not easy.

The constant evolution in the ransomware families is meant to tackle any security features antivirus software programs may embed. Antivirus software programs work by analyzing and making a note of ransomware families and then scanning new downloads for the same code. So the authors of ransomware constantly make changes to the code so it won't be detected and any key, if found for the previous versions, would not work anymore.

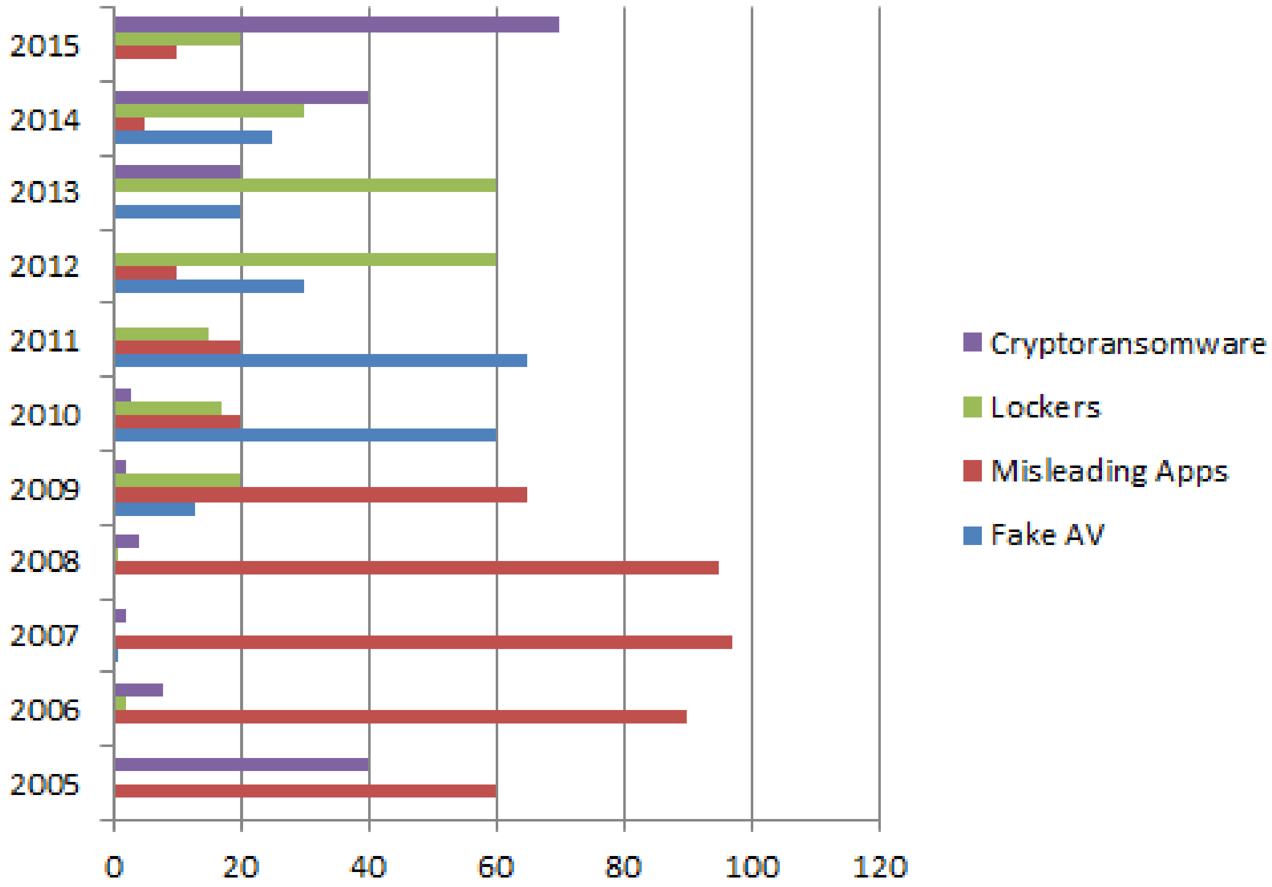


Figure 3: Percentage of new families of fake AVs, misleading apps, lockers and crypto-ransomware identified between 2005 and 2015 [15]

B. Growth of Ransomware

Since the advent of ransomware, the amount demanded in extortion has almost doubled from US$ 294 to US$679 at the end of 2015 to US$1077 in 2016. The amount is further expected to increase as extortion amount is doubled if it is not paid in a specified period and data is deleted after a certain periodlapses. Hence revenues have increased [23] [27] [30] [32].

The number of new ransomware families in the market is steadily increasing with an average of 100 families being discovered in 2015.

The advent of Ransomware-as-a-service (RaaS) has provided a platform to people who could not develop their own ransomware but are ready to acquire it. These cybercriminals get paid more than the author as they risk being caught in the process. This has also increased the number of cybercriminals. Also, this has attracted a lot of people who want to earn money easily [22]. Ransomware-as-a-service does not work like other services provided by the cloud. Instead, it is merely named so because the author of the ransomware is simply putting up the ransomware to be used by anyone. There is a small upfront payment required for acquiring the ransomware. The person acquiring the ransomware directly shares his profits with the author (20%). This helps him reach multiple markets and demographics without running the risk of being caught. Italso leverages the time available to him as multiple people are now propagating the malware.

Between January 2015 and April 2016, U.S. was the most affected region by ransomware, with 28 percent of global infections. Canada, Australia, India, Japan, Italy, UK, Germany, Netherlands, and Malaysia are the ten most affected countries. Around 43 percent of ransomware victims were employees in organizations [13].

Figure 4 shows Ransomware infections in different countries from January 2015 to April 2016 [23].

Figure 5 shows Ransomware infections by industry from 2015 to 2016 [23].

4. PREVENTIVE MEASURES

Ransomware is an active attack which can be prevented if the user follows and complies with security mechanisms. Figure 6 shows a chart of applicationsthrough which Ransomware entered the organization and infected the system.

In Figure 6, most of the times it was an Email Link (31%) through which the ransomware entered into the organization. Ransomware infection rates are only 71% when it comes to infecting the systems whereas, in 21% chances of attempts, ransomware was targeted to the system, but it does not infect the systems [14].

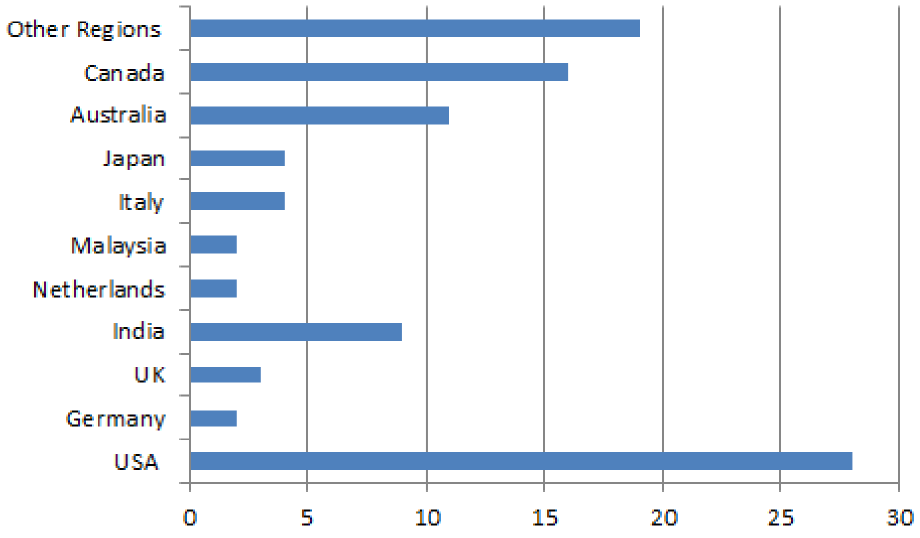


Figure 4: Ransomware infections in different countries from January 2015 to April 2016 [16]

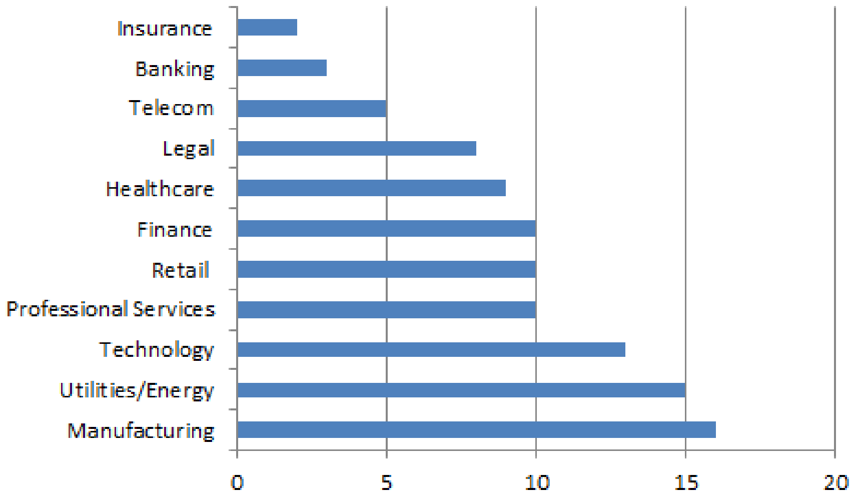


Figure 5: Total Ransomware Infections by Industry 2015-2016 [17]

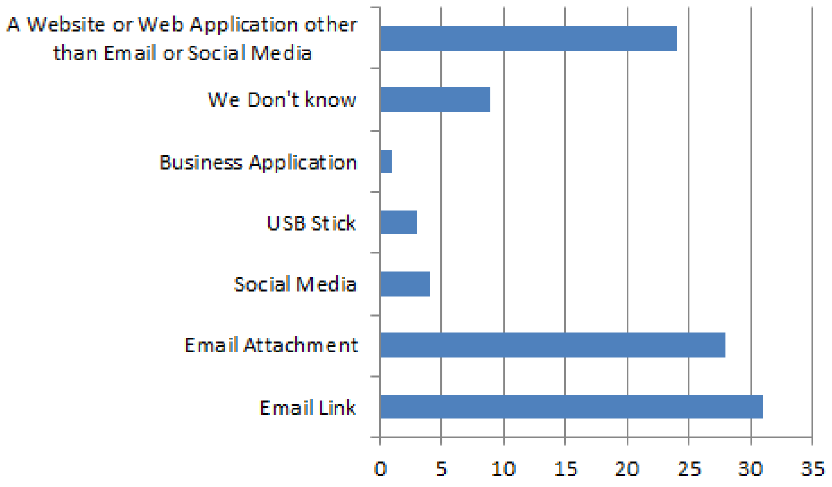


Figure 6: Applications by which Ransomware entered the organization (in Percentage) [19]

One of the most prevalent distribution mechanisms is a spam email. The mechanisms that may be used to ensure ransomware is not spread through emails are:

Attachment Scanning and Filtering: Attachments should be scanned for their content, not merely the provided file extensions. File archives as attachments should also be dropped before email delivery.

Content Filtering: Spam filter threshold should be increased so that messages from suspected bots is dropped or quarantined appropriately.

User Education and Training: Even after applying filters, certain spam may be able to reach the end user. The user should be aware enough not to download unknown attachments or click on such links.

Robust backups should be maintained. The safest and best place to do so is over the cloud. Even if computer is encrypted, all the data can be recovered from cloud [6] [7] [8] [18] [24] [25] [31] [32].

5. ANALYSIS AND DISCUSSION

As per the literature survey that was done in the field, ransomware is identified as a potential misuse of cryptography in early 90's. Still, it could not be used to extort money from people as it was easy to trace the person whom the money was sent. It was only when crypto-currency came into the picture that use of ransomware to earn money could be thoughtof. The rise of ransomware can hence be attributed to the creation of crypto-currency.

The ransomware that was initially circulated was locker and scareware. These malwareprograms did not encrypt any data. They merely locked the screen of the computer and asked the victim to pay the price to regain control. Scareware would pose itself as a security agency which had caught the victim doing some offense (like viewing or downloading pornographic videos) and would ask for an amount as fine so that the charges are dropped. As these malware programs were recognized for what they were doing, fake antivirus software programs stormed the market. They would post bogus messages that some virus had been detected and could only be removed if the victim signs up for paid services.

Analyzing figure 3, it can be seen that crypto-ransomware came very late into the scenario. Initially, crypto-ransomware was usedbut then it was dropped against the easier options of locker and scareware. As awareness grew, lockers, scareware, and fake applications could not be used. The revival of crypto-ransomware was inevitable. The huge number of families of crypto-ransomware also evolved to ensure key cannot be found. If the key to any previous version of family is found, that would not affect the attack on any another victim. This evolution can also be seen in Table 1. The continuous evolution meant that there are so many variants of ransomware present that a single decryption tool cannot work everywhere. Even if a variant has been found and decrypted, it will not affect the ransomware market as many other variants are present and many others can be created.

From figure 4, it is evident that the highest attacks have been observed in the US. This is directly implied by the widespread use of IoT devices. Thisis also implied by the DDoS attack (occurred on 26th October 2016) on the DNS server in the US which rendered services of many websites affected. Since all IoT devices are connected to the internet and all of them are not equipped with high-security features, it is easy to tap them in an attack. Other developed countries have a high occurrence of ransomware due to the same reason. The reason that amongst all the developed nations, India also features as one of the most impacted countries is the lack of awareness about ransomware. Also, the security is not adequate. Hence the systems are easy to target.

From figure 5, it can be seen that the industries that are mostly targeted are the ones with high requirement of the data (manufacturing, healthcare, security), high loss of energy (this might be done to damage a city or an area; energy/technology sector), or the intent of denial of services (professional services, IT, finance). The attackers also choose the industry as per the payment they expect. Every industry has a different capacity to pay. Some attacks might simply be executed to impact the economy and working of an area.

It has been predicted that the ransomware industry would grow further in 2018. This can be attributed to the fact that majority of the IoT devices in use are still insecure. They are either too simple to be secured using complex passwords or there is no scope for having a password or any other security mechanism in place. Another major reason is the lack of knowledge. People do not know how to protect themselves from ransomware attacks. Also, there are no solutions available that could detect and stop a ransomware attack. This leaves users pretty vulnerable to the risks of the internet.

6. FUTURE WORK

In this paper, we review about Ransomware and their types. Ransomware is an active attack. Apart from security mechanisms, prevention and awareness may result in stopping the execution of the ransomware. In future, we focus on developing a security mechanism which prevents the ransomware attacks [20] [26] [30].

7. CONCLUSION

In the current scenario of security in computer networks, vulnerabilities are being discovered and exploited every day. Attacks are happening everyday resulting in compromising of privacy and integrity of data. Among such attacks, a variant of attack is the use of malicious software. Though malicious software programs are of many types, they are together categorized as ransomware as they demand a ransom from the victim. Many variants of ransomware are available in the market, with varying strengths. To add to the booming business of ransomware, "ransomware-as-a-service" (RaaS) was further introduced. Cybercriminals are using RaaS to reach new targets and in turn, earn huge profits. Although other kinds of malicious attacks can be detected and stopped, there is still no means to stop or detect a ransomware attack. Only some prevention can be taken so that computers are not infected. In such conditions, awareness of users is of utmost importance as social engineering is also employed. Some researchers have tried to develop anti-ransomware software programs but their acceptance and usefulness is yet to be seen.

REFERENCES

1. W. Stallings, “Cryptography and network security: principles and practices”,Fifth Edition, 2011, Prentice Hall, pp. 13-22, 257-287.
2. B. Forouzan, “Cryptography and network security”,4th Edition, Tata McGraw Hills, 2007, pp. 931-960.
3. B. Schneier, “Applied cryptography: protocols, algorithms and source code in C”, second edition, 1996, John Wiley and Sons, pp. 1-10.
4. [Online] “What is malware and how can we prevent it”, Norton Security Center, https://in.norton.com/internetsecurity-malware.html [Last accessed 2018/04/18].
5. “Understanding ransomware and ways to defeat it, White Paper”, McAfee Labs, 2017.
6. “Ransomware white paper”, October 2016. SWGfl.
7. “Ransomware white paper”, 26th July 2016, CERT.be.
8. “Ransomware holding your data hostage”, White Paper, 12thAugust 2016, Deloitte.
9. A. Ivanov, D. Emm, F. Sinitsyn, S.Pontiroli “The ransomware revolution”, 2016, Kaspersky Security Bulletin.
10. “How ransomware works”, White paper, May 2016, LogRythm.
11. J. Wyke, A. Ajjan, “The current state of ransomware”, December 2015, SophosLabs Technical Paper.
12. K.Savage, P.Coogon, H.Lau,“Security response: The evolution of ransomware”, White Paper, 6th August 2015, Symantec.
13. A special report “Ransomware and businesses 2016”,2016, Symantec.
14. [Online] “PHP ransomware attacks blogs, websites, content managers and more…”https://nakedsecurity.sophos.com/2016/03/02/php-ransomware-attacks-blogs-websites-content-managers-and-more/ [last accessed 2018/04/16].
15. K. Richards, “Recent ransomware attacks: data shows 50% growth in 2016”, 2016, SecuritySearch.
16. J. Crowe, “Ransomware growth by the numbers: ransomware statistics 2017”, June 2017, Barkley.
17. J. Crowe, “Ransomware by the numbers: must-know ransomware statistics 2016”, August 2016, Barkley.
18. “White paper: ransomware. The virus plumes new depths.”9th August 2017, Ethical IT.
19. “Understanding the depth of theglobal ransomware problem”, August 2016, Osterman Research Survey Report.
20. N. Scaife, H. Carter, P. Traynor, K. Butler, “CryptoLock (and Drop it): stopping ransomware attacks on user data”, 2016, IEEE 36th International Conference on Distributed Computing Systems, pp. 303-312.
21. “Five things you need to know about CryptoLocker”, White Paper, Zscaler, 2017.
22. G. O’ Gorman, G. McDonald, “Ransomware: a growing menace”, White Paper, 8th November 2012, Symantec.
23. “Ransomware and businesses 2016”, White Paper, August 2016, Symantec.
24. S. Mehmood, “Enterprise survival guide for ransomware attacks”, White Paper, 30thApril 2016, SANS Institute Reading Room.
25. “Ransomware and phishing: how to avoid falling victim to these threats”, White Paper,19th January 2017, Barracuda.
26. R. S. Sajjan, V. R. Ghorpade, “Ransomware attacks: radical menace for cloud computing”, 2017, International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),pp. 1640-1646.
27. C. L.Gande, R. G. Gutierrez, “Give us this day our daily ransomware”, 2017, IEEE 37th Central America and Panama Convention (CONCAPAN XXXVll). pp. 1-6.
28. D.Caivano, G.Canfora, A.Cocomazzi, A.Pirozzi, C. A.Visaggio, “Ransomware at X-Rays”, 2017, IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 348-353.
29. Q. Chen, R. A. Bridges, “Automated behavioral analysis of malware: A case study of WannaCryransomware”, 2017,16th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 454-460.
30. H. Kim, D. Yoo, J. Kang, Y.Yeom “Dynamic ransomware protection using deterministic random bit generator”, 2017, IEEE Conference on Application, Information and Network Security (AINS), pp. 64-68.
31. B. Kenyon, J.McCafferty, “Ransomware recovery”, vol.: 58, Issue: 4, Dec. 2016, ITNOW, pp. 32-33.
32. D. Gonzalez, T.Hayajneh, “Detection and prevention of crypto-ransomware”,2017,IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pp. 472-478.
33. [Online] “Ransomware to hit cloud computing in 2018, predicts MIT” https://www.computerweekly.com/news/450432488/Ransomware-to-hit-cloud-computing-in-2018-predicts-MIT [last accessed 2018/04/16]
34. [Online] “Global ransomware damage costs predicted to exceed $ 5 Billion in 2017” https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/ [last accessed 2018/04/16]
35. [Online] “DDoS attack that disrupted internet was the largest of its kind in history, experts say” https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [last accessed 2018/04/16]
36. [Online] “Got ransomware? What are your options?” https://nakedsecurity.sophos.com/2016/03/03/got-ransomware-what-are-your-options/ [last accessed 2018/04/16]