International Journal of Advanced Research and Development
ISSN: 2455-4030
Impact Factor: RJIF 5.24
www.advancedjournal.com
Volume 2; Issue 5; September 2017; Page No. 324-329

Ransomware-worldwide cyber attacker

[1] Dr. Kusum Singal, [2] Pankaj Chhillar
[1] Junior Research Fellow, Dept. of Genetics, MDU Rohtak, Haryana, India
[2] LLM, Dept. of law, MDU Rohtak, Haryana, India

Abstract
Major cyber attacker ransomware has hit the world in may 2017. Two lakh establishments, 150 countries and many organizations has become the victim of this malware. Europe, USA and UK national health services severely got affected. Ransomware is a type of malware that tries to extort a payment from its victim after getting into the computer through anonymous spam attachments. Afterwards, it seeks money from user in order to gain access to your data. For getting decryption key, user has to pay through bitcoins. This paper briefly describes what is this malware, how does this works and ways to prevent such type of cyber attack. This paper also highlights the position of Indian Legal System on ransomware. It briefly discusses the remedies under Indian laws the penetration statics of cybercrime in India and major challenges faced to tackle such crime.

Keywords: Ransomware, Cybercrime, WannaCry, Bitcoins, Cyber attacker, WCry, Wanna Decryptor etc.

Introduction

Cybercrime is the most dynamic form of crime. It has evolved in its nature, sphere of targets and operations. Cybercrime can primarily be categorized into two categories based upon execution the two categories of cybercrime are as follows (I) where a device is used as a tool to execute an attack or a port of an attack (ii) where a device under an attack or a device is under part of attack.

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. A few ransomware may lock the system in a way which is not difficult for a techie to retrieve access, more advanced malware uses a technique called crypto/viral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. During strong crypto viral extortion attack, decryption key is only quagmire to the data under attack– and difficult to trace digital currencies such as Ukash and Bitcoin are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, a recent, and next generation attack, the "Wannacry worm, a ransomware variant, also known as WannaCry, WCry, or Wanna Decryptor, traveled automatically between computers in the morning of May 12, 2017. It was discovered by an independent security researcher. This ransomware variant has spread rapidly over several hours. Open-source reporting indicates requested ransom of. 1781 bitcoins, roughly $300 U.S. Starting from around 2012 the use of ransomware scams has grown internationally in June 2013, security software vendor McAfee released data showing that it had collected more than twice the number of samples of ransomware that quarter than it had in the same quarter of the previous year.

India as a nation has seen itself on constant radar of cyber criminals. It stands on 5thrank in number of attacks launched by cybercriminals after U.S.A, China, Japan and Russia. Over a period of one year 48,000 ransomware attacks were detected in India. A healthy amount i.e. 60% of the attacks detected ware executed on companies. The most hit state by ransomware is West Bengal followed by Maharashtra, Gujarat, Delhi and Orissa. If a list is made of cities where ransomware is detected most in India, Kolkata stands on top followed by Delhi, Bhubaneswar, Pune and Mumbai standing on the 5th strata. The high rate of detection of cybercrime is a serious threat to growing economy like India.

Evolution of Ransomeware

Types of Ransomeware

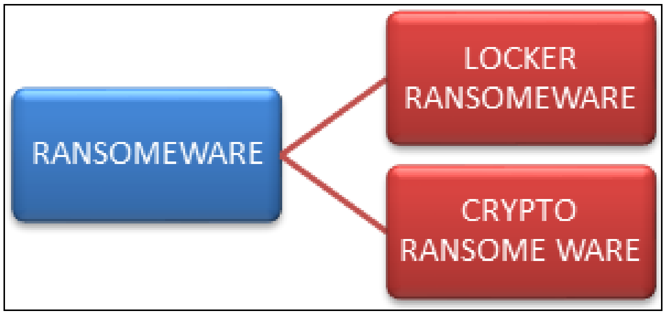


Fig 1

A Ransomeware operated by restriction of access to user into their own content. Such denial or restriction of access can be enforced in several forms. The variation in such enforcement by an attack determines the nature of a ransomeware. Devising a remedy and setting up of a preventive mechanism requires significant study into nature of the ransomeware.

Thus ransomeware are primarily categorized based upon nature of its operation. Any ransomeware can be categorized under two heads i.e (i) Locker Ransomeware, (ii) Crypto ransomeware

1. **Locker Ransomware**

Fig 2

Locker ransomeware is considered to be conventional and crude form of ransomeware. It is also known as computer locker commonly. Then name given to these types of attack is based on the operating mechanism. Attacks from the family of locker ransomeware denies access to the computing machine. It prevents the user from logging into the device which is under attack. The locker ransomeware generally displays the message of attack on boot screen. The displayed message demands specific ransom and has details regarding means for transfer of that ransom.

2. **Crypto Ransomeware**

Fig 3

Crypto Ransomeware is more specific in nature. The targate of crypto ransomeware is not the whole device rater specific files. The attack in this case targets the critically important resources and data stored on users computer in form of files. The files are denied access by mode of encrypting. The encrypted files can only be accessed by a decrypting key only known to the attacker. In crypto ransomware the demand of ransom can be made in several forms. Demand can be extended over email threads or by display of message when the user is trying to open the file. Crypto ransomware is considered to be more advanced than its counterpart. This is also known as data locker.

The above given categorization is not exhaustive a ransomware may further be divided into several categories and subcategories. The basis of categorization can be variation in mode of demand of ransom or the form of demand of ransom. Such categorization is very dynamic and may hold relevance only in specific time frame. The study of such categorization can be curtailed for tracking and incrimination of culprits but it is not important for understanding the concept of ransomware.

History of ransomware

Like another cybercrime ransomware has fairly modern history. The first attack pertaining to ransomware was appeared in the year of 1989 in form of AIDS Trojan. The mode of transmission opted 28 years ago was snail mail and the medium was floppy disk. The potential targets were less due to minute numbers of personal computer users. The most of computer users in year of 1989 were experts of technology which led to failure of Aids Trojan.

Since first appearance of ransomware there has been a constant growth and evolution in this family of cybercrime. Technological growth, Penetration of technology into day today life, relationship of economics and cyber space and role of cyber security in national security has paved path into the growth and evolution of ransomeware. The growth of ransomware has seen a tremendous progress post 2005. Appearance of Trojan attack laid foundation stone and was a turning point into ransomware history. A decade long time i.e.2005 to 2015 is said to have a rich history of modern ransomware.

Study of modern ransomware history

Modern ransomware emerged in the year of 2005. During this period ransomware was primarily tool for money spinning. This development led to breaking of the old age notion that cyber-attack is merely tool for creating nuisance. This association of monetary benefits of the attackers to their activities made them more dedicated and more furious. Cyber attacker invested their energy and developed more efficient ways for execution of ransomware during this time.

If a in-depth study is carried out modern ransomware has the important landmarks namely

(i) Misleading applications, (ii) Fake AV, (iii) Locker (iv) Crypto ransomware

1. **Misleading Applications**: This family of ransomeware appeared in 2005. Such attacks were executed by posing themselves as spyware removal applications or performance enhancement tools. The prominent member of this family is Trozens. These ransomware threatened users by exaggerating the minor issues and demanding small token of 30$ to 90$ as a consideration to resolve such issues. These equally impacted windows as well as os x operating systems.

2. **Fake AV:** Fake ant viruses appeared between the years 2008-2011. At this stage attackers advanced from skin to small application to skin of fully functional anti-virus. The fake antivirus performed dummy scans and showed non existential threats. A fee of 40-100 was demanded as consideration for resolution of such issues by these fake antivirus.
3. **Locker Ransomware**: The next was cited in the year of 2011 that was in form of locker ransomware, this development continued till 2013. The system under such attack denied any access to user. At one point of time the attackers claimed the blocked on the device was under the instruction of law enforcement agencies like F.B.I. etc. The lock screen accused user's involvement into drugs and pornography and extended demand of certain sum for exemption from legal incrimination.
4. **Crypto Ransomware**: Crypto ransomware first emerged in the year of 2013 this development of ransomware is so critical that crypto ransomware are very effective till date. The outbreak of 'WannaCry ransomware' was a major threat round the globe. A typical crypto ransomware on an average demands 300$ from every effected user.

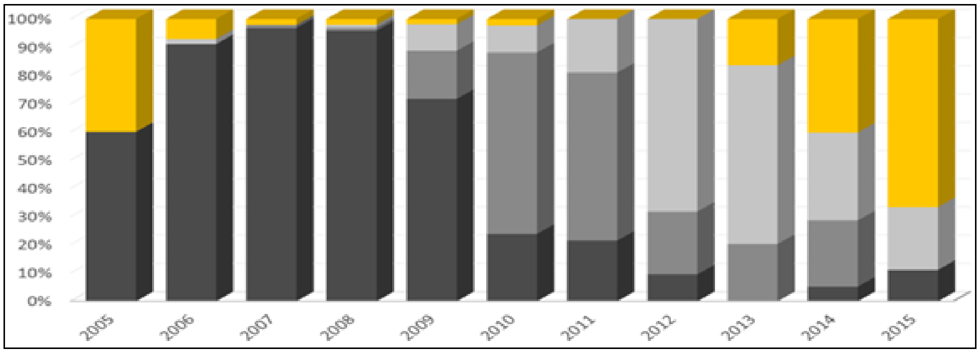
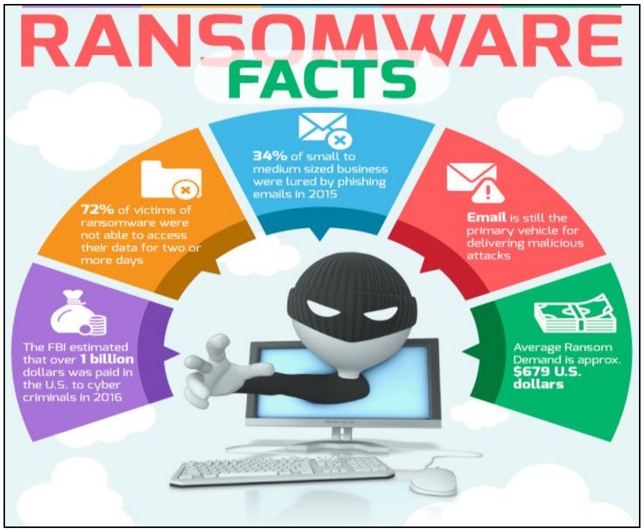


Fig 1: Graphical representation helps showing the pivotal movement ransomware between the years 2005-2015 i.e the era of modern ransomware

The pivotal study suggests that the crypto ransomware poses a significant threat. It contribution in the perils of ransomware is more than one third.

Fact study on targets

An analysis of targets of ransomeware can be made through two perspective i.e. (i) device perceptive target and (user perspective). A device centric study analyses the issues and challenges of ransomeware from the view that which device is under attack it can be a computer or mobile. A user centric study will lay emphasis on issues and challenges faced by a specific category of user be it home users, business users or the public agencies.


RANSOMWARE
FACTS
34% of small to medium sized business were lured by phishing emails in 2015
72% of victims of ransomware were not able to access their data for two or more days
Email is still the primary vehicle for delivering malicious attacks
The FBI estimated that over 1 billion dollars was paid in the U.S. to cyber criminals in 2016
Average Ransom Demand is approx. $679 U.S. dollars

Source: www.ace-data.com/wpcontent

Fig 2: Showing ransomware facts

Top targets for ransomware creators and distributors

Cybercriminals soon realized that companies and organizations were far more profitable than individual users, so they went after the bigger targets: police departments, city councils and even school and the worst even hospitals. To give you some perspective, nearly 70% of infected businesses opted to pay the ransom and recover their files. More than half of these businesses had to pay a ransom worth $10,000 to $40,000 in order to recover their data.But for now, let's find out how online criminals target various types of Internet users. This may help you better understand why things happen as they do right now.

Reasons of target home users

- They don't have data backup.
- They have weak or no cyber security education, which means they'll click on almost anything.
- Lack of online safety awareness makes them prone to manipulation by cyber attackers.
- Lack of baseline cyber protection.
- Don't keep their software up to date.
- Fail to invest in need-to-have cyber security solutions.
- They often rely on luck to keep them safe online.
- Most of the home users still rely exclusively on antivirus to protect them from all threats, which is frequently ineffective in spotting and stopping ransomware.

Reasons of target businesses

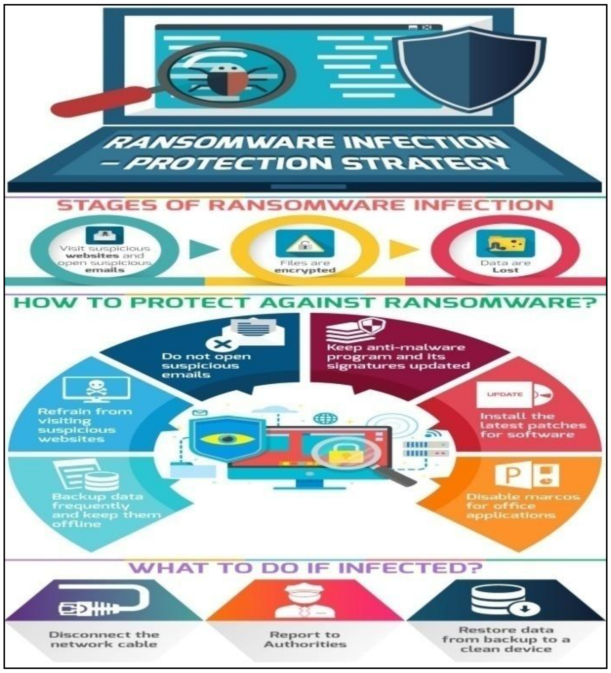
- Large amount of money can be extracted.
- Attackers know that a successful infection can cause major business disruptions, which will increase their chances of getting paid.
- Computer systems in companies are often complex and prone to vulnerabilities that can be exploited through technical means.
- The human factor is still a huge liability which can also be exploited, but through social engineering tactics.
- Ransomware can affect not only computers but also servers and cloud-based file-sharing systems, going deep into a business's core.
- Cyber criminals know that business would rather not report an infection for fear or legal consequences and brand damage.
- Small businesses are often unprepared to deal with advanced cyber attacks and have a relaxed BYOD (bring your own device) policy.

Spread of ransomware threats: - The most common infection methods used by cybercriminals are as follows:-

- Spam email campaigns that contain malicious links or attachments (there are plenty of forms that malware can use for disguise on the web)
- Security exploits in vulnerable software
- Internet traffic redirects to malicious websites;
- Legitimate websites that have malicious code injected in their web pages
- Drive-by downloads
- Maladvertising campaigns
- SMS messages (for mobile device target)
- Botnets
- Self-propagation (spreading from one infected computer to another); WannaCry, for instance, used an exploit kit that scanned a user's PC, looking for a certain vulnerability, and then launched a ransomware attack that targeted it.
- Affiliate schemes in ransomware-as-a-service. Basically, the developer behind the ransomware earns a cut of the profits each time a user pays the ransom.

Methods of protection from ransomware attack

- Recovering files from ransomware is tedious without the attacker's approval, one should avoid to fall under attack at the first place. The best thing you can do is practice good "digital hygiene":
- Don't fall prey to social engineering or phishing, which is where an attacker attempts to have you reveal sensitive information to them. If you receive a suspicious email from your grandma or work colleagues, ask yourself whether it's unusual before you click. If you're not sure, contact the sender via a different medium, such as giving them a phone call, to cross-check.
- Don't install any software, plugging or extensions unless you know they're from a reputable source. If in doubt, ask and only rely on trusted download sources. And certainly don't be tempted to pick up USB sticks found on your pathway.
- Update your software (comprising your operating system, web browser and other installed software) regularly to ensure you are always running the latest versions.
- Backup is must. Important documents need to be treated like valued possessions. Grab a hand full of USB keys and rotate your backups daily or weekly, and don't leave USB keys plugged in having multiple copies means the adversarial effort on holding you for ransom is pretty much worthless.


RANSOMWARE INFECTION – PROTECTION STRATEGY
STAGES OF RANSOMWARE INFECTION
Visit suspicious websites and open suspicious emails
Files are encrypted
Data are Lost
HOW TO PROTECT AGAINST RANSOMWARE?
Do not open suspicious emails
Keep anti-malware program and its signatures updated
Refrain from visiting suspicious websites
UPDATE
Install the latest patches for software
Backup data frequently and keep them offline
Disable marcos for office applications
WHAT TO DO IF INFECTED?
Disconnect the network cable
Report to Authorities
Restore data from backup to a clean device

Source: www.ace-data.com/wpcontent)This image lays down the model activities to be followed for prevention ransomware attack. It also provides the requisite steps which should be taken in case an individual or an institution in under an attack. Understanding the stages of the attack can help both individuals and institutions to take requisite steps. Prevention is considered to be the best form of cure and more of the emphasis should be laid on the proactive means to avoid and prevent attack.

Fig 2: Protection strategy

Law and Ransomware

Ransomware is one of the most widely spread cybercrime in world. The attack of Ransomware is in constant evolution becoming more effective and even difficult to track and formulation of a preventive firewall next to impossible for such a versatile form of malware. Ransomware may cause injury to individuals but it is a serious threat to everyone. An effective judicial system is need of hour to tackle threats arising out of Ransomware. Effective codified laws both on substantive as well as on procedural front should exist and competent investigative mechanism must exist to bring culprits to justice where an attack is executed.

Remedies in Indian Legal System

Indian legal system is state of art design to tackle ransomware attacks. It offers wide spectrum of remedies ranging from The Constitution of India to The Information Technology Act, 2000. Indian Penal Code was enacted in the year of 1860, but still it caters Indian legal system with significantly important provisions to deal with ransomware attack.

Article 21 of The Constitution of India entitles right to life as fundamental rights to Indian citizens. It impliedly grants right of privacy and ensure protection of their sensitive personal data of its citizens. The article puts an onus on state for codification of such laws which are for protection of privacy of sensitive data of citizens.

The Information Technology Act, 2000 is a specialized codification drafted by Indian legislature to deal with the hot topic of cybercrime. The IT Act, 2000 prescribes imprisonment extending up to 3 year and fine. The relevant sections under The I.T. Act, 2000 for crime of ransomware are as follows:

- Tampering with Computer Source documents – Section 65
- Hacking with Computer Systems, Data alteration – Section 66
- Publishing obscene information – Section 67
- Un-Authorized access to protected system – Section 70
- Breach of Confidentiality and Privacy – Section 72
- Publishing false digital signature certificates – Section 73

Indian Penal Code, 1860 is the prime substantive law of Indian judicial system to deal with cyber crime. Though ransomware is a result of changed dynamics of crime still Indian Penal Code is significant for establishing liability of criminal ransomware attack. The relevant sections which implies to crimes pertaining to a ransomware attack are as follows:

- Sending threatening messages by email – Section 503
- Sending defamatory messages by email – Section 499
- Forgery of electronic records – Section 463
- Bogus websites, cyber frauds – Section 420
- Email spoofing – Section 463
- Web-Jacking – Section 383
- E-mail Abuse – Section 500

The structure of Indian legal system stands rigid against mutating monster of crime. Due diligence is shown by law makers in enacting competent and effective laws in order to tackle the widely spread ransomware. Wide spectrum of Indian laws provides reference to each and every domain of this crime.

Procedure to seek justice

Like any other cybercrime ransomware is serious threat to law and order. An individual in order to seek justice in case of commission of crime shall file a complaint against the same. The complaint of any cybercrime can be made to police station which has jurisdiction of area in which the device is located. To tackle the problem CID (Crime investigation department) has opened cyber cell and dedicated cyber police station. A complaint can be made to these police stations as well in order to seek justice. Investigation of any cyber crime is duty of state. Police investigates the complaint on merits of facts available and brings the culprit to justice.

Challenges before Indian legal system

Ransomware is a tedious cyber crime to deal. It comes under the cyber crime category. It has various complications and put forward various challenges to Indian legal system. This generis of crime has serious problems with ascertaining jurisdiction. Competent investigative agencies need special specializations with subject of Information Technology. Extra territorial jurisdiction calls for complex extradition process which varies from country to country and is widely dependent on interpersonal relationship of those countries which not only delays the judicial process rather at times it leads to scenarios where culprit is out of bounds. Major challenges of legal system are as follows:

- Exponential growth in cybercrime. In the year of 2012, 2876 cases were registered under provisions of Information Technology Act, 2000 whereas the no of cases registered in the year of 2013 are 4356.
- Lack of specialized knowledge among investigative agencies.
- Extra territorial jurisdiction of attackers.
- Penetration of technical knowledge among masses.
- Legal awareness among masses about their rights in cyber space.

Conclusion

Ransomware is unprecedented threat not only to the private players rather it possess threat to governments and state machineries. Extraterritorial operations and execution is fundamental limitation faced by law enforcement bodies in bringing culprits to justice. Although the government has ambitious plans with emphasis on ‘Digital India’ and cashless transaction, to these flurry of ransomware is a serious hurdle. E-governance, cyber connectivity and boom in E-commerce has serious monitory interest of individuals and institutions attached to them. At such crucial moment the scope and meaning of security in cyberspace is yet to be expounded. Ransomware has made leading IT professionals and law enforcement helpless. A collective effort is called for with government, private players and other stakeholders working on same page. Security policy and assurance with early detection and prevention is need of the hour to curb ransomware. Coordination mechanism should be established on international level with structural inspiration from Interpol, such mechanism should check and restrict any flourishing attack. Special mutual extradition laws shall be practiced by all states in order to expedite the procedure of criminal justice system. Strong national policy on cyber security should be enacted. Last but the most important widely penetrating awareness programs must be undertaken by government and it professionals.

References

1. Hiran Nath V, Babu M. Mehtre, Static Malware Analysis Using Machine Learning Methods, International Conference on Security in Computer Networks and Distributed Systems, 2014.
2. http://www.vinransomware.com/types-of-ransomware, Types of ransomeware.
3. https://heimdalsecurity.com/blog/what-is-ransomware-protection.
4. https://heimdalsecurity.com/blog/what-is-ransomware-protection.
5. Indian Legal System: Problems and Challenges / http://www.publishyourarticles.net/knowledge-hub/essay/indian-legal-system-problems-and-challenges-essay/1636.
6. Indian Penal Code, 1860.
7. Information Technology Act, 2000.
8. Kharraz A, Robertson W, Balzarotti D, Bilge L, Kirda E. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: Almgren M, Gulisano V., Maggi F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA. Lecture Notes in Computer Science, Springer, Cham, 2015, 9148.
9. Legal action Against Ransomware Attack / https://blog.ipleaders.in.
10. Livemint An Analysis of Ransomware, http://www.livemint.com/Industry/ -ransomware-attack-attempts-seen-in-India-Quick-Heal.html.
11. Mattias Weckstén, Jan Frick, Andreas Sjöström, Eric Järpe. A novel method for recovery from Crypto Ransomware infections.
12. N.C.R.B. Crime data portal 2012 / https://data.gov.in/resources/cases-registered-under-it-act-cyber-crime-during, 2012.
13. N.C.R.B. Crime data portal 2013 / https://data.gov.in/resources/cases-registered-under-it-act-cyber-crime-during, 2013
14. Nikolai Hampton, Zubair Baig A. Ransomware: Emergence of the cyber-extortion menace, The Proceedings of [the] 13th Australian Information Security Management Conference, held from the Edith Cowan University Joondalup Campus, Perth, Western Australia, 2015, 47-56.
15. Nikolai Hampton**,** EdithCowan University.
16. Paul Rubens, Common Types Of Ransomeware (E-Security Planet).
17. Protection strategy http://www.ace-data.com/ransomware-infection-protection-strategy.
18. Ransomware cyber-attack sweeps globe, India's largest container port in Mumbai hit, India Today/ http://indiatoday.intoday.in/story/petya-ransomware-major-global-cyber-attack-wannacry-jawaharlal-nehru-port-trust/1/988915.html.
19. Zubair A. Baig Security Research Institute, Edith Cowan University.