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. 511-513

Ransomware virus attack

G Bowshi Latha
III – BBA.LL.B (Hons), Saveetha School of Law, Tamil Nadu, India

Abstract
This article discusses about "Ransomware Virus Attack". The Ransomware attack is said to be the attack which is done through online sources and which finally leads to the demanding of money by making some files as hostages. Introductory part of this article says some brief information about Ransomware. The objective of this article is to know, from which year the attack gets started and the ways used by the Virus to spread and attack. The article briefly says about the main target areas for attack of Ransomware attack; kinds of Ransomware attacks and some surveys about the attacks. The article also concluded by giving some safety measures to keep oneself away from online attacks. The information for this article are gather from secondary sources.

Keywords: ransomware, virus, spread, online, introductory

1. Introduction
Technologies like computer, internet, software etc are created only to see developments in world but now a days these advanced technologies are misused in various ways like uploading unwanted informations or other private photos on public websites, hacking others personal data etc,. Among which Ransomware is one of the largest threats faced by people throughout the world. "Ransomware" is the word derived from two words 'Ransom' and 'Software'. It is one of the malicious software. It was designed to extort money from a person in many ways, which may be either holding some of the important files as hostage or may be by locking the whole computer until a ransom is paid. Since mid2000s, it is considered to be one of the most largest threat which may be faced by either PC at home or at work. Let us briefly discuss about some of the informations related to Ransomware like it's target places for attack and it's development from early stage.

2. Target of ransomware
Though the attack of Ransomware is happened all over the world, some areas are fixed as it target places, where the following factors apply,

2.1 Factors for target of Ransomware attacks
- The organisation which carries critical data will be one of the target areas of Ransomware attack
- An emergency sessions where the quick decisions are require are also considered as one the target places of Ransomware attack
- In most of the cases, the data which are targeted to be in attack will be very sensitive like, they may be their personal data which should not be known to others.

2.2 Target places for Ransomware
Educational Institutions: According to the report of Bitsight Insight, educational institutions are in the 1st place to be in target of Ransomware attack. The reason is, they are having number of access to social security; they possess medical records of students; intellectual property; research; faculties, staffs and students financial data will be maintained by them, which will be the main attacking areas in cybercrime. University Collage London remains as the best example, which get attacked by Ransomware.

Government Agencies: According to the report of Bitsight Insight, government agencies are in the 2nd place to be in target of Ransomware attack. The reason is that the services rendered by them are very critical, like police protection which will be very much time sensitive and very critical, so that the hover agencies will be very much willing to pay the ransom to recover their data, so they were in second place of target. To understanding the reason, Texas Police Department will be a very good example, which loses its eight years data who includes body camera video and some in house surveillance video.

Healthcare Organisations: According to the report of Bitsight Insight, healthcare organisations are in the 3rd place to be in target of Ransomware attack. The reason is that the data which are made as hostages will be very important like patients data which is very important in critical situations like life or death situation of patients. Hollywood Presbyterian Medical Centre will be a best example which paid $.17,000 in 2016 to recover its data which get attacked by Ransomware.

Other Target Areas
HR Departments: These departments are targeted to spread Ransomware through mail. It's steps are, the mail will be sent to HR Department which will looks like a mail from a job applicant, so if the HR Professionals open the mail and the attachments from that mail, the Ransomware will attack that computer and will encrypt it, so that they can be forced to pay the Ransom.

Mobile Devices and Macs: Ransomware not only targets PCs but also targets mobiles and Macs. According to Kaspersky Lab Malware Report, which is released in May 2017, 2,18,625 Ransomware files were detected. Security Firm Fortinet discovered that the Ransomware also targets Macs.

3. Kinds Of Ransomware Attack

1989 (AIDS Trojan): AIDS Trojan (or) PS Cyborg is the first attacked Ransomware but at that time, the word Ransomware was not given. It was invented by Joseph L.Popp. It was spread in such way that he sent 20,000 infected disks to the attendees of WHO International AIDS Conference. The disk was labelled as "AIDS Information – introductory Diskettes". The infected disk will show its action after 90 reboots by hiding directories and encrypting the names of the files. The user can regain access only if he pays the demanded amount. Here, the victim should sent $.189 to PC Cyborg Corp. only at post office that is located in Panama. Later the inventor Popp get caught and the files were recovered by decryption. But the work of decrypting files continued for three decades.

2005 (fake programs): In 2005, some programs were arised which were believed to remove spyware but they were fake. These programs fixed critical issues and demanded 50 US Dollars to buy licence.

In the same year 2005, in the Article named "Files Of Ransom", the use of term 'Ransomware' is noticed to be used by the person named Susan Schaibly.

2006 (Archiveus Trojan) – This is said to be the second Ransomware that raised which is very difficult to remove. RSA encryption is used in this Ransomware which encrypted 'My Documents'. To obtaining password for decryption, the victims are forced to a situation to buy some specific websites.

[2008–2009 is said to the period when fake antivirus applications are used to encrypt files to demand the ransom]

2008 (GP Code.AK) – GP Code Ransomware is said to be created in 2008. Later, GP Code.AK. is released which differs from GP Code by the use of 1024- bit RSA key, which is very harder to crack. GP Code.AK is used to spread from PC to PC, which worked by infecting or locking or encrypting files in PC. To unlock these files victims are forced to a situation to pay a Ransom so that they could be able to get Code to unlock their files.

2009 (fake antivirus programs) – In 2009, some fake antivirus programs are released, which actually looks like a legitimate program and after getting downloaded it creates some problems in PC. By creating such problems, it demands 100 US Dollars to fix the problems.

[2011 – 2012 is said to the period when Locker Ransomware are used to lock files to demand the ransom]

2011 (Trojan Winlock) – Trojan-Winlock was introduced in 2011 which won't encrypt any files but will display a fake window product activation notice. The activation key will be with the victim for which the user should call the international premium rate number.

2012 (Reveton) – In 2012, the major Ransomware Trojan was introduced which was also named as Reveton. This Ransomware spreads mainly in Europe, in which the computer will be claimed for attack which will be used for illegal activities. The only way to get rid of this is to unlock the computer for which the user should pay some Ransoms using prepaid cash service.

[2013 – 2017 is said to be the period of the emergence of Bitcoin]

2013 (Cryptolocker) – Birth of Cryptolocker took place in the year of 2013 which was spreaded through e-mail. The Ransomware which infected computer would demand $.400 in Bitcoin which should be paid within 72 hours. According to a survey, nearly half million computers were got infected by this Ransomware and the victims who paid Ransom were estimated to be 1.3%. The attachers netted an estimated $.27 million from their victim.

[An operation was planned to crack down two Ransomware programs namely Cryptolocker and Gameover Zeus Botnet. The operation was named as 'Operation Tovar'. In this operation, a Russian hacker was get caught named Evgenily Mikhailovich Bogachev who is said to be the administrator of both the Ransomwares - Cryptolocker and Gameover Zeus Botnet]

2014 (Crypto defense) – During the Ransomware attack in 2014, the hackers were estimated to extort at least of $.34,000 in the first month of their attack.

2015 (Dubbed Locker PIN) – In 2015, Ransomware attack of 'Dubbed locker PIN' was araised. During September, it got spread in America. Once the device get attacked, the system will get locked with displaying lock screen, so only if the PIN Code is entered the system can be unlocked. To get the PIN Code, the hacker will offer $.500 as the Ransom.

2016 (Ke Ranger) – Ke Ranger Ransomware was arised in 2016 which is said to be the first MacOSX based Ransomware q. It is delivered through transmission BitTorrent client for OSX.

2016 (Jigsaw Ransomware) – The Ransomware named Jigsaw Ransomware contained Jigsaw characters which is taken from the movie series named SAW. This Ransomware threatened the victims by deleting some important files in affected PC or Mac or Mobile for every 60 minutes, if the ransom is not paid. They demanded the Ransom of $ 150. If the victim tried to restart the window then 1000 files were get deleted.

2017 (WannaCry) – WannaCry is said to be the massive Ransomware attack which took place in May 12,2017. More than 2,00,000 networks in 150 countries were identified to get infected by this Ransomware. It worked by exploiting a Windows XP vulnerability which is used by NSA for espionage and surveillance.

4. Survey of ransom ware attack

Approximately $ 300 had said to be demanded per user for small businesses and $ 30 million had said to be demanded by hackers for multinational enterprises.

4.1 Internet Crime Complaint Centre Report (IC3)

- More than 7600 Ransomware attacks were said to take place between 2005 and March 2016
- Over 6000 data were got breached in Ransomware attacks
- In 2015, nearly 2,453 Ransomware complaints were received by IC3 which amount to costs about $ 1.6 million.

4.2 Tom's IT Pro Report

- Nearly 7,18,000 corporate users were said to be get affected by Crypto Ransomware, between April 2015 and March 2016
- Previously, between April 2014 and March 2015, 1,31,000 attacks were noticed.
- So, Ransomware attack between April 2015 and March 2016 is said be six times increased when compared with attack between April 2014 and March 2015.

5. Conclusion

Misusing of others personal or official data by evil intentioned hackers cannot be washed out completely by can reduced by protecting ones own data. Protecting own data can be done by the following ways like by regularly checking privacy of their accounts, by frequently resetting passwords, by preventing opening of foreign unknown data, by regularly backing up data, by keeping softwares up to date, by staying on common tactics which are used to spread Ransomware. So, misusers cannot be get stopped by anyone but self-prevention can protect one from misusers.

6. References

1. https://spideroak.com/ransomware/timeline
2. https://www.csoonline.com/article/3086077/data-breach/11-ways-to-fight-off-ransomware.html
3. https://www.csoonline.com/article/3208111/security/who-is-a-target-for-ransomware-attacks.html
4. https://digitalguardian.com/blog/ransomware-protection-attacks