ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Ransomware - The Evolution of Malwares

Piyush Patil[1]

Student, Dept. of Computer Engineering, SIT, Lonavala, Maharastra ,India [1]

ABSTRACT: Recently, use of personal computers and the internet has exploded and, along with massive growth, cybercriminals have emerged to feed off this flourishing market, targeting innocent users with a wide range of malware . Ransomware is a term used to describe a class of malware that is used to digitally extort victims into

payment of a specific fee**.**Cybercriminals behind ransomware are constantly introducing new methods. With more connected devices around, we can expect to see ransomware appear in new device categories where they were never seen before. Many security professionals don't see the need to know who is behind ransomware or what their motivations are—they just want to know how to stop it. Combating a ransomware threat can be more effective if a security team knows who is behind an attack.

KEYWORDS: Ransomware , Malware , Trojan , RSA , TDS , Bitcoin.

I. INTRODUCTION

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. The modern-day ransomware has evolved considerably since it originated 26 years ago with the appearance of the AIDS Trojan. The AIDS Trojan was released into the unsuspecting world through snail mail using 5¼ floppy
disks in 1989. Though the public was unprepared for this new type of threat all those years ago, the AIDS Trojan failed due to a number of factors. Back then, few people used personal computers, the World Wide Web was just an idea, and the internet was mostly used by experts in the field of science and technology. The availability and strength of encryption technology was also somewhat limited at the time. Along with this, international payments were harder to process than they are today.
In 2005 ,the first wave of modern ransomware started with Trojan.Gpcoder.The top six countries impacted by all types of ransomware in 2016 include the United States, Japan, United Kingdom, Italy, Germany, and Russia. In its earlier years, ransomware typically encrypted particular file types such as DOC, .XLS, .JPG, .ZIP, .PDF, and other commonly used file extensions. To infect a machine, the hackers primarily use the following vectors: phishing emails, unpatched programs, compromised websites, poisoned online advertising and free software downloads. The average ransom amount is US$300.The method of payment requested by most digital extortionists today is cryptocurrency, typically Bitcoin, but this is not the only payment method requested. A number of prepaid voucher services like MoneyPak, Ukash, or PaySafe are also used by criminals.. The favoured payment method for locker ransomware is payment vouchers and for crypto ransomware, it's bitcoins.The cybercriminals behind ransomware do not care who their victims are, as long as they are willing to pay the ransom.
RSA 2048 encryption is used by typical ransomware software to encrypt files. Just to give you an idea of how strong this is, it takes around 6.4 quadrillion years for an average desktop computer to crack an RSA 2048 key. One estimate indicates more than $27 million in ransom payments in just the first few months of the release of the CryptoLocker variant of ransomware in September 2013. CryptoLocker was followed up by the variant CryptoWall, which made $325 million dollars in 18 months, half of that in the United States.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

II. RELATED WORK

Ransomware does much more than encrypt your data and ask for money to unlock it . They have presented in [1] research, that the anatomical study of a ransomware family that recently picked up quite a rage and is called CTB locker, and go on to the hard money it makes per user, and its source C&C server, which lies with the Internet's greatest incognito mode-The Dark Net. Android is currently the most widely used mobile environment. This[2] trend encourages malware writers to develop specific attacks targeting this platform with threats designed to covertly collect data or financially extort victims, the so-called ransomware.In [3] article we show how software-defined networking can be utilized to improve ransomware mitigation. In more detail, we analyze the behavior of popular ransomware - CryptoWall - and, based on this knowledge, propose two real-time mitigation methods.This [4]research investigated methods to implement a honeypot to detect ransomware activity, and selected two options, the File Screening service of the Microsoft File Server Resource Manager feature and EventSentry to manipulate the Windows Security logs. The research developed a staged response to attacks to the system along with thresholds when there were triggered.
There[5] experimental analysis of CryptoDrop stops ransomware from executing with a median loss of only 10 files (out of nearly5,100 available files). There results show that careful analysis of ransomware behaviour can produce an effective detection system that significantly mitigates the amount of victim data loss.

III. ANATOMY OF RANSOMWARE ATTACK

Ransomware has increased in popularity because it has been successful. In a world of survival of the fittest, it has adapted and changed to meet the growing demands of its creators. By moving from simple trickery and deception to outright extortion, these criminal organizations are playing on our fears and our need to protect our information.

Anatomy of ransomware attack

- Installation - After a Victim’s computer is infected, the ransomware install itself, and keys in the windows Registry are set to start automatically every time your computer boots up.
- Contacting Headquarter - Before ransomware can attack you, it contacts a server operated by the criminal gang that owns it.
- Handshake and Keys - The ransomware client and server identify each other through a carefully arranged “handshake” and two cryptographic keys are generated by the server. One key is kept on your computer, while the second key is stored securely on the criminal’s server.
- Encryption - once the cryptographic keys are established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.
- Extortion - The ransomware displays a screen that indicates a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, $300 to $500, must be paid in untraceable bitcoins or other electronic payments.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

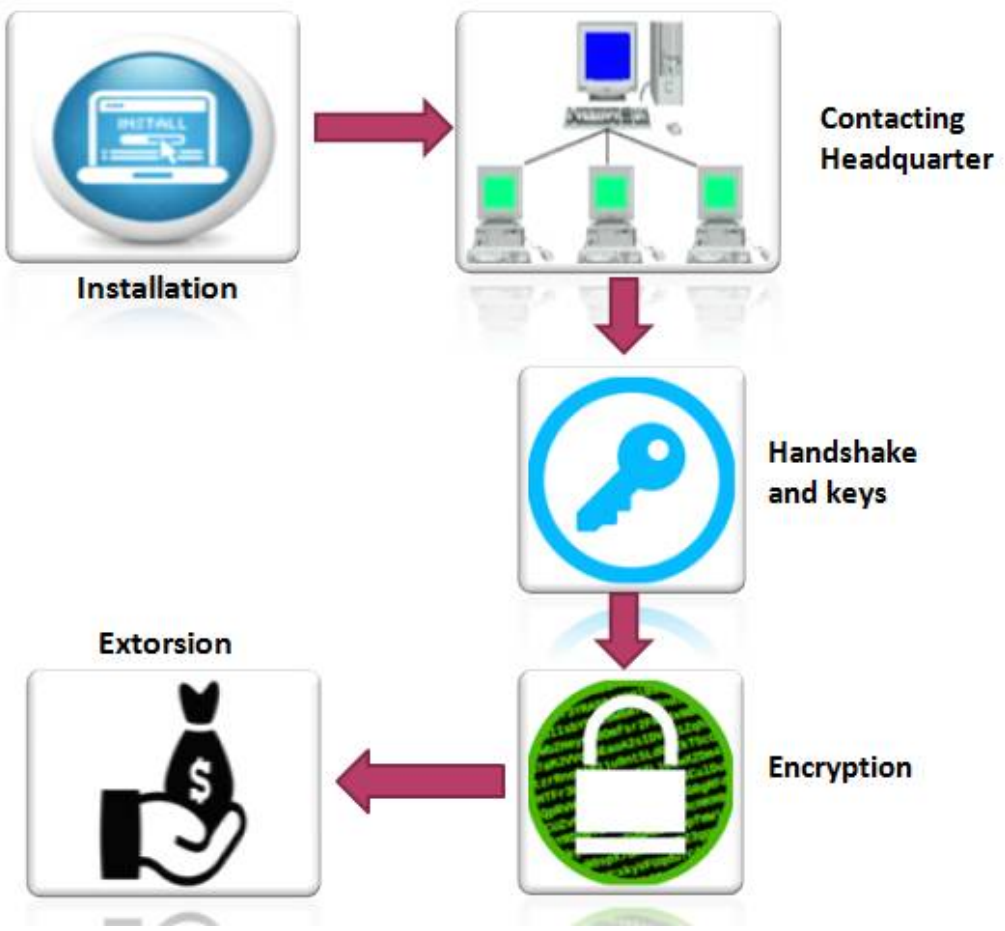

Fig – Anatomy of Ransomware Attack

Kasperspy Lab [13] , in the first quarter of 2016, reported blocking 228 million attacks. Of those blocked attacks, 372,602 involved ransomware, which means that ransomware accounted for only 0.0016% of the attacks.

IV. RANSOMWARE TAREGET

Earlier versions of ransomware targeted home computer users almost exclusively. It was very rare to hear about a company being infected with ransomware but now situation had changed.

- HOME USERS

Home users often have sensitive information, files, and documents that are personally valuable stored on the computer, such as college projects, photos, and video game save files. Even though these things are of value to users, home users are still unlikely to have an effective back up strategy in place to successfully recover from events such as a fire or theft, let alone a crypto ransomware attack. A previous survey by Symantec/Norton showed that 25 percent of home users did not do any backups at all. Fifty-five percent backed up some files. In terms of backup frequency, only 25 percent of users backed up files once a week. The rest only made backups once a month

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

or even less frequently than that. This means users are potentially leaving themselves exposed in the event of a ransomware attack.

- BUSINESS
  For many businesses, information and the technology to use it is their life blood, without which the act of Conducting day-to-day business is impossible. The loss of this information could have a dreadful impact on the business. Many companies have backup and disaster recovery plans, but there are still many who do not. Some organization's disaster recovery plans may not extend to cover the individual end users. Even if the businesses had plans, it is quite possible that they might not be tested and may not work as expected when required. These factors make individual business users a feasible target for traditional crypto ransomware. Apart from ransomware impacting individual business users, there have also been cases reported where the company itself had been targeted with file-encrypting ransomware. In a case involving PHP.Ransomcrypt.A, the attackers were believed to have compromised an organization for months, quietly encrypting the database along with all of the incremental backups. At the appropriate time, the attackers made their substantial ransom.

- PUBLIC AGENCIES
  Public agencies such as educational institutes and even law enforcement entities are not excluded from the attention of these cybercriminals and in some cases, they may be specifically targeted. There have been several reports of law enforcement agencies that had been hit with crypto ransomware in the past. In another case, a New Jersey school district, which runs four elementary schools in the Swedesboro-Woolwich area, was hit by cybercriminals who demanded a ransom payment of 500 bitcoins (US$124,000).

Ransomware does not discriminate between Platforms like mobile devices, Computers etc.

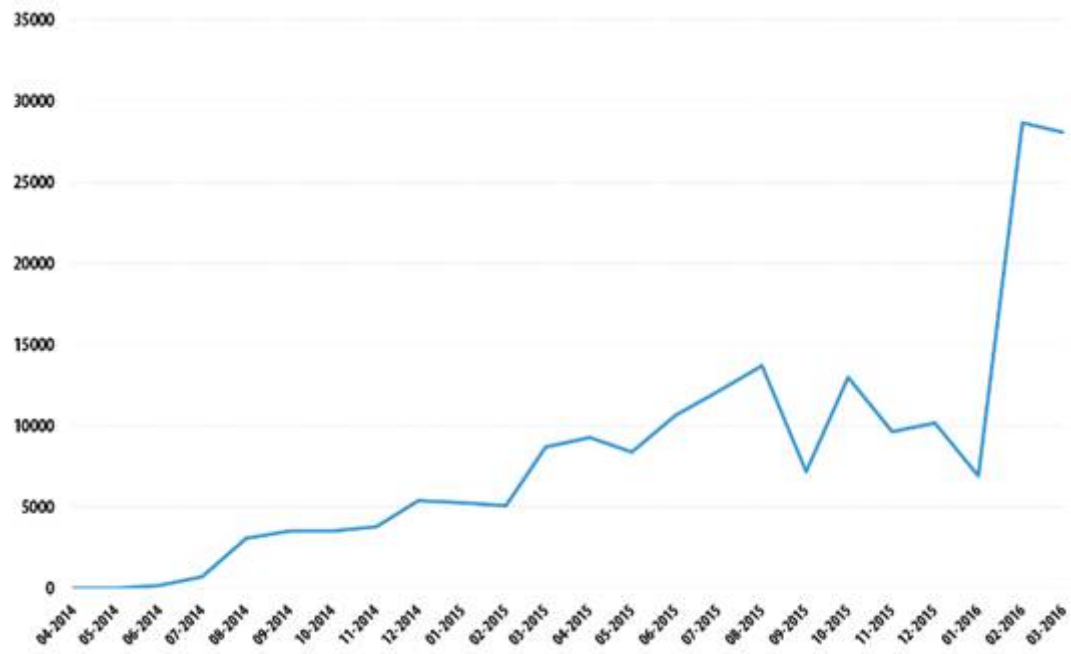

Fig- The number of users encountering mobile ransomware at least once in the period April 2014 to March 2016

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Given the popularity of devices like watches, televisions, refrigerators, and automobiles connected to the Internet, it is only a matter of time before criminals starts targeting those devices.

V. WORKING - HOW IT SPREADS?

Ransomware attackers have been seen to use different techniques or services to get their malware onto a victim's computer.

Malvertisement
A malvertisement (malicious advertisement) is a type of advertisement on the Internet. It is capable of infecting the viewer's computer with malware .Malvertisements are commonly placed on a website in one of these two ways:

1- Legitimate advertisements
2- Popup advertisements

Spam-Email
By definition, email spam is any email that meets the following three criteria:

- Anonymity: The address and identity of the sender are concealed
- Mass Mailing: The email is sent to large groups of people
- Unsolicited: The email is not requested by the recipients

In recent years, the spam emails used to distribute ransomware have favoured the following themes:

• Mail delivery notification
• Energy bills
• Job seeker resume
• Tax returns and invoices
• Police traffic offense notifications

Social Engineering
Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software.

Traffic Distribution System (TDS)
Traffic Direction Systems (TDS) are used as landing pages that direct traffic to malicious content based on a variety of criteria such as operating system, browser version and geographic location. If the exploit kit is successful in exploiting vulnerability in the visiting victims' computer, it can lead to what is commonly referred to as the drive-by-download of malware.

Downloader's & Botnets
A botnet is a number of Internet-connected computers autonomously communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control (C&C) or by passing messages to one another (C&C might be built into the botnet as P2P)
Once the downloader infects a computer, its job is to download secondary malware onto the compromised system.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Fig- Ransomware techniques used by attacker

While most security professionals would argue against paying a ransom, there are some cases where paying the ransom is the best option for the organization.

VI. ANALYSIS

Am I Infected?
It's fairly straightforward to find out if you are affected by a ransomware virus. The symptoms are as follows:
• You suddenly cannot open normal files and get errors such as the file is corrupted or has the wrong extension.
• An alarming message has been set to your desktop background with instructions on how to pay to Unlock your files.
• The program warns you that there is a countdown until the ransom increases or you will not be able to Decrypt your files.
• A window has opened to a ransomware program and you cannot close it.
• You see files in all directories with names such as HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS.HTML.

I'm Infected, Now What?
Once you have determined you have been infected with ransomware, it is imperative to immediately take Action:
1. Disconnect:
Immediately disconnect the infected computer from any network it is on. Turn off any wireless capabilities Such as Wi-Fi or Bluetooth. Unplug any storage devices such as USB or external hard drives.
2. Determine the Scope:
At this point you need to determine exactly how much of your file infrastructure is compromised or encrypted.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Did the first infected machine have access to any of the following?
• Shared or unshared drives or folders
• Network storage of any kind
• External hard drives
• USB memory sticks with valuable files
• Cloud-based storage (DropBox, Google Drive, Microsoft OneDrive/Skydrive etc…)

3. Determine the Strain:
It is important to know exactly which ransomware you are dealing with. Each ransomware will follow a basic Pattern of encrypting your files, then asking for payment before a certain deadline.

4. Evaluate Your Responses:
To put it bluntly, you have 4 options, listed here from best to worst:
1. Restore from a recent backup
2. Decrypt your files using a 3rd party decryptor (this is a very slim chance)
3. Do nothing (lose your data)
4. Negotiate / Pay the ransom

YEARS	RANSOMWARES
2005	Gpcoder
2012	Reveton
2013	Urausy , Kovter , Urausy , Nymaim , Cryptowall ,Browlock
2014	Linkup , Slocker , CTB-Locker/Citron,Onion , Synolocker , TorrentLoker , Zerolocker,Virlock,Convault
2015	Cryptolocker2015,Simplocker,Pacman,Pclock,ThreatFinder, Dumb,Mabouia OSX POC,PowerWorm,DMA-Locker,Hidden Tear,QRX-Locker,Gomasom,ChimeraLocker,TeslaCrypt,BandarChor,CryptVault,Tox ,Troldesh,EncryptorRaas,CryptoApp,LockDroid,LowLevel404,CryptInfinite, Unix.Ransomecrypt,Radamant,VaultCrypt,Radamant, VaultCrypt , XRTN
2016	Ransom32,73v3n,CryptoJocker,Nanolocker,LeChiffew,Magic,Ginx, Locky,Umbrecrypt,Hydracrypt,Vipasana,HiBuddy,JobCryptor,Paycrypt,KeRanger

Fig- This table shows just how many types of encrypting malware researchers have discovered in the past 10 years.

VII. CONCLUSION

Ransomware is fierce, smart and dangerous. The people behind ransomware seem to have a good grasp on a dangerous technology, and they've turned it into a profitable business. Ransomware is still a problem, sure. However, the best

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

weapon against Ransomware or any malware for that matter is education. By learning about the threat, learning how to stop it and spreading the knowledge to friends, family, colleague and even perfect strangers, you are making a dent in the pockets of the cyber-criminal organizations.

REFERENCES

[1] Rhyme Upadhyaya , Aruna Jain,"Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet",29-30 April 2016
[2] Francesco Mercaldo, Vittoria Nardone, Antonella Santone,"Ransomware Inside Out", Availability, Reliability and Security (ARES), 2016 11th International Conference,31 Aug.-2 Sept. 2016
[3] Krzysztof Cabaj; Wojciech Mazurczyk,"Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall", IEEE Network (Volume: 30, Issue: 6, November-December 2016) ,01 December 2016
[4] Chris Moore,"Detecting Ransomware with Honeypot Techniques",Cybersecurity and Cyberforensics Conference (CCC), 2016,2-4 Aug. 2016
[5] Nolen Scaife,Henry Carter,Patrick Traynor,Kevin R. B. Butler,"CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data", Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference,27-30 June 2016
[6] https://www.trendmicro.com/vinfo/us/security/definition/ransomware
[7] https://heimdalsecurity.com/blog/what-is-ransomware-protection/
[8] https://securelist.com/analysis/publications/75183/ksn-report-mobile-ransomware-in-2014-2016/
[9] https://blog.malwarebytes.com/cybercrime/2012/12/ransomware/
[10] https://emailmarketing.comm100.com/email-marketing-ebook/email-spam.aspx
[11] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
[12] https://www.knowbe4.com/ransomware
[13] Alexander Gostev, Roman Unuchek, Maria Garnaeva, Denis Makrushin, and Anton Ivanov, "IT Threat Evolution in Q1 2016," *Securelist*, Kaspersky Lab, May 5, 2016.

BIOGRAPHY

Piyush Patil is a student pursuing graduation in computer science from Sinhgad Institute Of Technology,Lonavala,India
His research interest are IOT,cybersecurity and wireless and network security.