A Primer on Ransomware: Extortion on the Internet

Dr. Vikas Thada
Associate Professor(CSE),
Amity University,Gurgaon,India
Email:vthada@ggn.amity.edu

***Abstract*—**Ransomware is a dangerous piece of malware that in known so as it make system resources hostages by encrypting files and demand for money as ransom. The does not let use user to access to his files. Control to the files and systems can only be possible by paying a ransom. In ransomware the user’s data become hostage to the attacker. The attacker threatens to publish or delete it until a ransom is paid. The paper is a primer on the ransomware and various ransomware attacks covering the definition, actual meaning, how it is spread. It also discusses the complete history from its origin in 1989 to till date covering different types of ransomware that have happened and created havoc in the world. Two examples of modus operandi of ransomware is also covered. The paper also discusses detailed discussion of economic loss along with number of users, organizations, companies, IT industries effected by ransomware. Towards the end mitigation methods from ransomware, bitcoin crypto currency is presented culmination in conclusion.

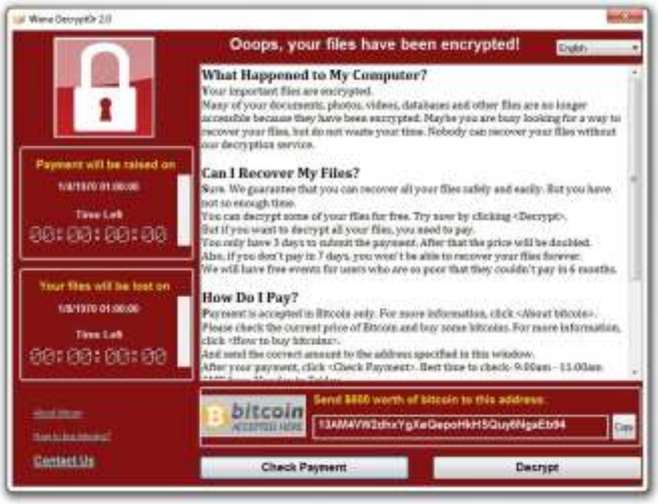
Keywords*- ransom,ransomware,malware,encryption,attack.bitcoin*

*****

I. INTRODUCTION

Ransomware is a dangerous piece of malware that in known so as it make system resources hostages by encrypting files and demand for money as ransom. The does not let use user to access to his files. Control to the files and systems can only be possible by paying a ransom**. The attacker** threatens to publish or delete it until a ransom is paid. **The ransomware** make data hostage onto victim computer’s itself and not letting the user to access any files or the system. This is done either by locking the system's screen or by locking the users' files unless a ransom is paid. All of the user’s files are encrypted/locked and user is not able to view the files. Special categorized families of ransomware popularly known as crypto-ransomware, uses advanced encryption techniques for encrypting file types on infected systems and demand users to pay the ransom in terms of bitcoin through certain online payment methods to get a decryption key for recovering files back[1]. Ransomware is a type of malicious application that steals control of the user's machine or data, then demands a payment from the user to restore normal access to the ransomed content or system. The payment is usually in the form of bitcoin crypto currency. Once the control of the system is gained by some remote attacker any action is possible onto the infected system. Further there is no surety that paying the ransom will return access or not delete the data. The simplest kind of ransomware can easily be cracked by a technically expert person in the related field. The action of the ransomware can easily be reversed. But there are more advanced and complex malware whose action cannot be reversed and victim feels totally helpless. Advanced ransomware employ a technique known as cryptoviral extortion. In this technique the infected machine or system’s files are encrypted using a secret key (as used by the attacker) thus making them inaccessible. The files are only accessible to the system user until a specific amount is not paid to the attacker [1]. To the worst of the situation even the Fill Allocation Table or whole hard disk can be encrypted[4]. Thus, you are being denied of accessing your own files and it is a kind of DOA (Denial of Access) attack. The only way to recover and access your files is using the decryption key which can only be possible once you pay the ransom[2].

The ransomware is a type of malware as it clandestinely installs into the user’s system and run’s in the background. The normal malware secretly steals the information from the user’s system, passing it to the attacker. User is not at all aware about this. But in the case of ransomware this thing is not hidden. After locking/encrypting the systems files with its own secret key, it informs the user and demands ransom. An example image is shown for the recently ransomware attack “Wannacry” on 12th May 2007 [1]



What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Fig 1: An example of ransomware[1]

II. HOW DOES IT WORK

When a computer is infected by ransomware through some executable file, the ransomware communicates a central server for getting further instructions or commands which require to activate it. After this the ransomware starts encrypting files on the infected computer with that information. After all the files are encrypted using the secret encryption key, it displays a message to the victim asking for ransom to decrypt the files along with timeline after which ransom may be doubled. The attacker also threatens to destroy the information if it ransom was not paid in stipulated time period usually with a timer attached to ramp up the pressure[3][8].

An example on Windows machine will clarify this:
End user gets a mail that seems to be from some genuine source. The link takes you the user to some legitimate site(seems but not actual). As soon as page gets loaded the malware residing in the server starts communicating with the victim machine. The server's machine look for the vulnerability in the victim's machine and after confirming it sends the ransomware file into the victim system. The ransomware file then spawn some child process of windows system files by hiding the original one. Using the Powershell feature of windows ransomware makes copies of itself and starts encrypting files of specific extension. The different copy of the ransomware files are also stored at specific places in windows (AppData folder, C:\, Start folder) so that logging off and restarting the system will not save you from ransomware. After this the ransomware file sends the encryption key and some device related information to the controlling server and after this a message is displayed on the victim's machine which is actually send by the server as shown in figure 2[3][8].

As another example of ransomware refer figure 4. Similar to the previous discussion here also the working starts through some spam mail or compromised web site followed by the similar process as discussed in the previous paragraph.

III. TYPES OF RANSOMWARE

There are mainly two types of ransomware: Encryptors and Lockers. The third one is a special case of Lockers. Encryptors using advanced encryption algorithm encrypts victims files and demand ransom under strict time period to decrypt the files content. CryptoLocker, Locky, CrytpoWall and latest Wannacry is the example of this type of ransomware. Lockers, actually locks all files in the victim's system without encrypting them and let user no way to use anything on the system. To unlock the files ransom is demanded. Winlocker is an example of this type of ransomware. A special type of Lockers lock the master boot record of hard disk thus disable the normal booting and when MBR ransomware strikes is shows a ransom message on the victim's system. Satana and Petya ransomware are examples of this type of virus[6].

The encryptors also known as crypto ransomware are the most dangerous types of ransomware.

IV. CHARACTERISTICS OF RANSOMWARE[3][6]

i. extremely difficult to decipher the files
ii. It can encrypt almost all kinds of file ie audio, video, image, doc etc
iii. It scramble your file names so you cannot find out exact file names
iv. It changes the extension of your file.
v. It display an image or a message to inform you about encryption and ransom amount
vi. It ask for ransom amount only in bitcoins which is crypto currency. The reason is simple, it is difficult to track this type of currency.
vii. The ransom amount has a strict time limit. If not paid them usually ransom amount is doubled and on
viii. expiration of time limit data may be lost permanently.

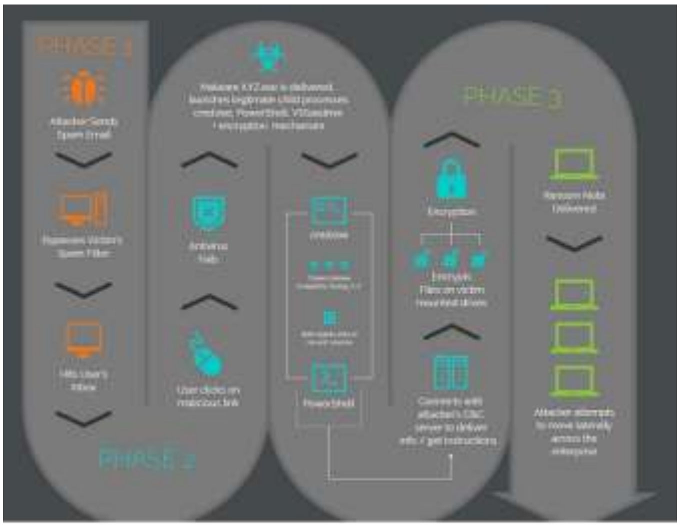
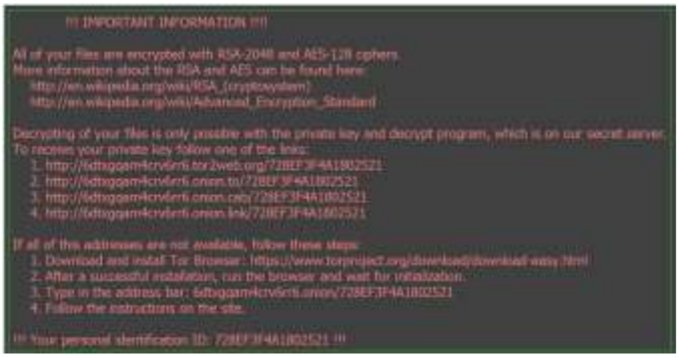

PHASE 1
Attacker Sends Spam Email
Bypasses Victim's Spam Filter
Hits User's Inbox
PHASE 2
User clicks on malicious link
Antivirus fails
Malware XYZ.exe is delivered, launches legitimate child processes, cmd.exe, PowerShell, VSSadmin + encryption mechanism
cmd.exe
PowerShell
PHASE 3
Encryption
Encrypts Files on victim mounted drives
Connects with attacker's C&C server to deliver info / get instructions
Ransom Note Delivered
Attacker attempts to move laterally across the enterprise

Fig 2: Phases of ransomware [8]

ix. Uses a complex set of evasion techniques usually not detected by antivirus software.
x. Often converts infected device into botnets so that joint attacks can be launched into future.
xi. It can spread to other PCs connected to a local network causing much more damage.
xii. It can also steal sensitive data and send it to the controlling server.
xiii. Sometimes includes geographical targeting so that ransom message is easily displayed in victim's native language.

V. EVOLUTION OF RANSOMWARE

The first known ransomware attack was initiated in 1989 by Joseph Popp who distributed infected near about 20,000 floppy disks to some researchers working on AIDS in approximately 90 countries. The malware was activated after the system was started 90 times. The malware displayed a message asking for $189 and $378 to bring back the system to normal state. This ransomware attack since then became famous as the AIDS Trojan, or the PC Cyborg[5].
Until 2000 ransomware attacks were not very common. From the year 2000 attackers started using sort of unbreakable encryption algorithms like AES,RSA. Many other algorithms were also very popular like CryZip, Gpcode,MayArchive,



```
        !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://6dtxgqam4crv6rr6.tor2web.org/728EF3F4A1802521
    2. http://6dtxgqam4crv6rr6.onion.to/728EF3F4A1802521
    3. http://6dtxgqam4crv6rr6.onion.cab/728EF3F4A1802521
    4. http://6dtxgqam4crv6rr6.onion.link/728EF3F4A1802521

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: 6dtxgqam4crv6rr6.onion/728EF3F4A1802521
    4. Follow the instructions on the site.

!!! Your personal identification ID: 728EF3F4A1802521 !!!
```

Fig 3: Early days of ransomware example[4]

Krotten,Archievevus etc. In 2011, a special kind of ransomware worm appeared that was very much identical to the Windows Product Activation notice , making it more difficult for users to decipher genuine notifications from threats[5][6]

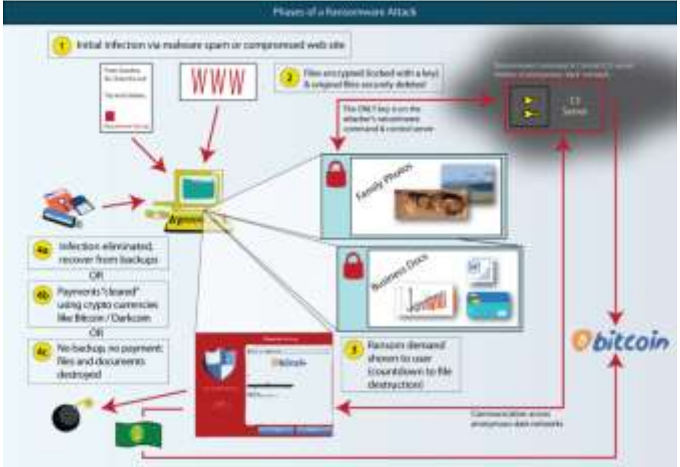
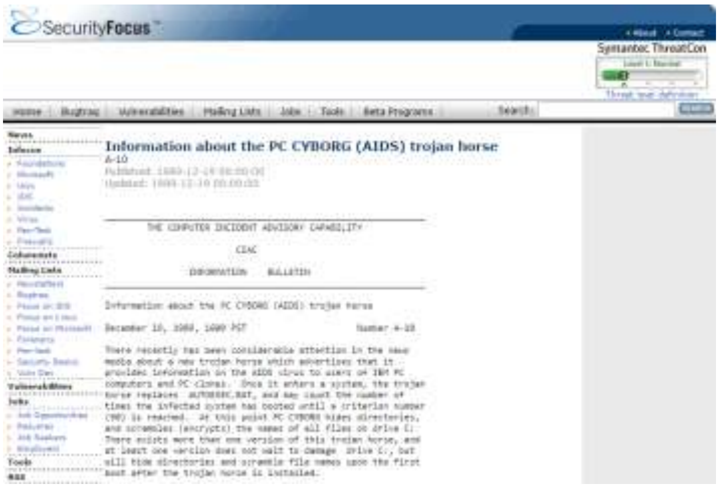

Phases of a Ransomware Attack
1 Initial infection via malware spam or compromised web site
WWW
2 Files encrypted (locked with a key) & original files securely deleted
The ONLY key is on the attacker's ransomware command & control server
C2 Server
Family Photos
Business Docs
4a Infection eliminated, recover from backups
OR
4b Payments "cleared" using crypto currencies like Bitcoin / Darkcoin
OR
4c No backup, no payment: files and documents destroyed
3 Ransom demand shown to user (countdown to file destruction)
Communication across anonymous dark networks
bitcoin

Fig 4: How ransomware starts spreading in system [2]

CryptoLocker was a prominent ransomware variant around 2013, and quite a profitable one at that. Between September and December 2013, CryptoLocker infected more than 250,000 systems. It earned more than $3 million for its creators[6][8]

From April 2014 through early 2016, CryptoWall was among the most commonly used ransomware varieties in the wild, with various forms of the ransomware targeting hundreds of thousands of individuals and businesses. By mid-2015, CryptoWall had extorted over $18 million from victims, prompting the FBI to release an advisory on the threat[8]

In 2015, a ransomware variety known as TeslaCrypt or Alpha Crypt hit 163 victims, netting $76,522 for the attackers behind it. TeslaCrypt demanded ransoms by Bitcoin, or in some cases PayPal or My Cash cards, in amounts ranging from $150 to as much as $1,000[8]



Information about the PC CYBORG (AIDS) trojan horse
A-10
Published: 1989-12-19 00:00:00
Updated: 1989-12-19 00:00:00

```
              THE COMPUTER INCIDENT ADVISORY CAPABILITY

                                CIAC

                      INFORMATION     BULLETIN

Information about the PC CYBORG (AIDS) trojan horse

December 19, 1989, 1600 PST                          Number A-10

There recently has been considerable attention in the news
media about a new trojan horse which advertises that it
provides information on the AIDS virus to users of IBM PC
computers and PC clones.  Once it enters a system, the trojan
horse replaces  AUTOEXEC.BAT, and may count the number of
times the infected system has booted until a criterion number
(90) is reached.  At this point PC CYBORG hides directories,
and scrambles (encrypts) the names of all files on drive C:.
There exists more than one version of this trojan horse, and
at least one version does not wait to damage  drive C:, but
will hide directories and scramble file names upon the first
boot after the trojan horse is installed.
```

Fig 5: First known attack of ransomware[5]

March 2016 also saw the appearance of the Petya ransomware variant. Petya is advanced ransomware that encrypts the victim computer's master file table and replaces the master boot record with a ransom note, rendering the computer unusable unless the ransom is paid. By May it had further evolved to include direct file encryption capabilities as a failsafe. Petya was also among the first ransomware variants to be offered as part of a ransomware-as-a-service operation[6][8].

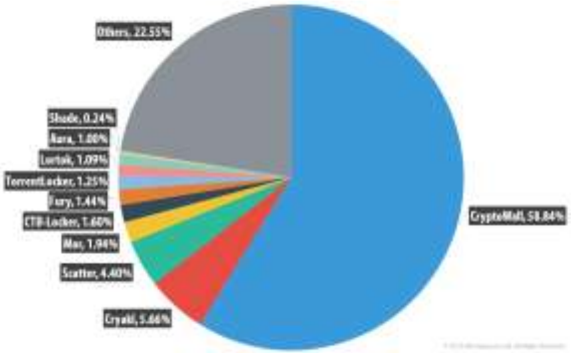


Fig. 6: Attacks by various crypto ransomware in 2014-2015[6]

As per the Kaspersky research lab in May 2016: Teslacrypt (58.4 percent), CTB-Locker (23.5 percent), and Cryptowall (3.4 percent) were the top 3 ransomware families. There was a kind of similarity among all of them as the method used to infect victim's computer was same: spam mail, malicious attachments ,links to infected web pages[7][8]

By mid-2016 Locky had cemented its place as one of the most commonly used ransomware varieties, with PhishMe research reporting that Locky use had outpaced CryptoWall as early as February 2016[8].

As per the report by [6] only a small number of ransomware caused most of the trouble and the same can be categorized into different groups. According to [ ] the groups CryptoWall, Cryakl, Scatter, Mor, CTB-Locker, TorrentLocker, Fury, Lortok, Aura, and Shade were the prominent encryptors victimized approximately 101,568 users all around the world in the period from April 2014 to March 2015.

According to [6] the following groups of crypto ransomware caused 79.21 % of attacks :TeslaCrypt,CTB-Locker, Scatter and Cryakl.

Friday May 12th marked one of the most dangerous and largest ransomware in the history "WannaCry". The WannaCry encrypts the hard disk of computer and propagates to other systems on same network. The ransomware also attacked victims by propagating through attachments to emails. The worm-spreading part of the Wannacry – which is designed to infect other computers — has a special check at the beginning. It tries to connect to a hardcoded website on the Internet and if the connection *FAILS*, it continues with the attack. If the connection WORKS, it exits. Thus, by registering this domain and pointing it to a sinkhole server, a researcher from the U.K. successfully slowed the spread of the worm. Wannacry encrypts the files on infected Windows systems. This ransomware spreads by using a vulnerability in implementations of Server Message Block (SMB) in Windows systems. This exploit is named as ETERNALBLUE[7].

The heavy destruction caused by the WannaCry has made us introspect the limitations and capabilities in preventing and defending such types of ransomware by knowing and understanding their capabilities. It's time to sit down and set the record straight on what we know, what we wish we knew to be one step ahead of the attackers, and what can be done in the near future so avoid these types of really severe attacks.

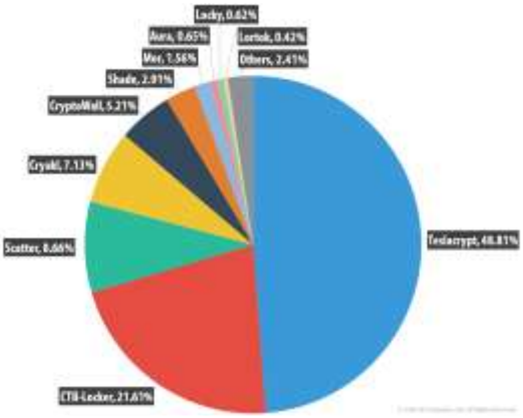


Fig. 7: Attacks by various crypto ransomware in 2015-2016[7]

Comparing the figure 6 and 7 it is observed that victims of ransomware have grown 17.7% from April 2015 to March 2016 all around the world.

Over 75,000 users in around 99 countries were infected by the ransomware WannaCry. Further they were demanded ransom in bitcoin cryptocurrncey using 20 different languages. In the course of a weekend the WannaCry ransomware spread to over 200,000 computers in 150 countries, crippling operations at hospitals, telecom providers, utility companies, and other businesses around the globe. The WannaCry ransomware demanded $300 per computer to be paid in bitcoin. Several companies in Spain, Britain, USA, Russia, and India became victim of the WannaCry. The attackers of WannaCry gave their victims a 7 day deadline from the day their computers got infected [17][18][19].

Towards the end a brief summary of all famous ransomware is tabularized.

Table 1: Summary of various ransomware[8]

Name	Origin	Brief Description
Archiveus Trojan	2006	Contents of MyDocuments were encrypted and victims were forced to get recovery password from an online pharmacy store.
GPcode	2006	spreaded via an email attachment intending to be a job application, used a 660-bit RSA public key.
CryptoLocker	September 2013	Spreaded using an email and on clicking renames all files and folders on network drives
Locker	December 2013	Locked user files using AES encryption; demanded $150 to get the key
CryptoLocker 2.0	December 2013	Used 2048 bit encryption and written using C#. The latest variant is not detected by anti-virus or firewall.
CryptorBit	December 2013	Corrupted the first 1024 bytes of any data file it finds. Bitcoin again used for a ransom payment.
CTB-Locker (Curve-Tor-Bitcoin Locker)	March 2014	First infections were mainly in Russia

CryptoWall	April 2014	Spreaded through malicious ads linking to sites that were CryptoWall infected and encrypted their drives. More than 600,000 systems were infected and 5.25 billion files being encrypted. A ransom of around $1,101,900 was paid.
Cryptoblocker	July 2014	Encrypted files of size <100MB using AES encryption.
SynoLocker	August 2014	Main victim were Synology NAS devices encrypted files one by one. Bitcoins was as ransom;Tor was used for anonymity.
OphionLocker	December 2014	Encryption method was ECC; victim has to pay within 3 days else private key will be deleted.
Pclock	January 2015	Files in a user's profile are encrypted.Volume shadow copies are deleted and disabled. Time period of 3 days and ransom was 1 bitcoin 72-hour
CryptoWall 2.0	January 2015	Infected method was email and malicious pdf files. Encrypted user's data and ransom was asked in bitcoin for decryption key.
TeslaCrypt	February 2015	Infection through popular video game files like Call of Duty, MineCraft, etc.
VaultCrypt	February 2015	Infection method was batch files and GnuPG software
CryptoWall 3.0	March 2015	I2P network communication;AES CBC 256 bit algorithm; Anonymity using Tor browser and $500 as ransom
CryptoWall 4.0	September 2015	Re-encrypts filenames of the encrypted files, making it more difficult to decipher
LowLevel04/ Onion Trojan-Ransom	October 2015	Encrypts files using AES encryption but the key itself is encrypted using RSA. Spreaded using Remote Desktop or Terminal Services
Chimera	November 2015	Spreaded using phishing or email campaigns . The hackers will publish the encrypted files on the Internet if the victim doesn't pay!
Emper	Jan 2016	Infected when user visits malicious sites; Demands 13 bitcoins as ransom
Locky	Feb 2016	Deletes shadow copies of files to make local backups useless, main targets were healthcare facilities.
Petya	March 2016	Infection mechanism through cloud storage services like Dropbox; overwrites MBR of infected system.
Waltrix	April 2016	Wide distributed via angler exploit kit
Bucbi	May 2016	Arrives via brute force Remote Desktop Protocol.
Crypshed	June 2016	Wide distributed via angler exploit kit
CryBee	July 2016	Uses disposable email addresses to maintain anonymity
Sharkraas	August 2016	Creates customized ransomware
Milicry	September 2016	Packages and sends gathered information as .PNG files
Comline	October 2016	First ransomware that uses command line to execute
Telecrypt	November 2016	Uses telegram channels to communicate with C & C server
Goldeneye	December 2016	Infected through MS office files; pretends to reboot system to perform disk check; $500 as ransom.
Wannacry	May 2017	Exploited vulnerability in the SMB Server; biggest ransomware attack to date.

VI. WAYS TO MITIGATE

Ransomware is a type of attack on cyber security. To mitigate this there are a few steps that general computer users and companies alike should follow to lessen their risk of be prey at ransomware significantly. There are number of best practices that come under the realm of cyber security like regular backing up of data, updating software (especially antivirus and internet security programs) regularly, and staying on top of the common tactics used to spread ransomware. Keeping these types of activities regularly will definitely help in averting off ransomware infections[4]

Even though the discussed best practices are not hidden and known to everyone, most of the users do not follow them and even some companies keep the backup only within their network, which can also be vulnerable to ransomware attack[4]

Effective ransomware defense totally rely on educating every user on internet and companies to follow advanced techniques of protection and following the best practices. Users and enterprises should devote time in learning best options for automated data backups and software updates, educating themselves about the ransomware distribution tactics – such as phishing attacks, drive-by downloads, and spoofed websites – should be a top priority for anyone using an internet-connected device today[5][6]

The best practices for ransomware prevention can be

summarized as:

Ransomware Prevention:

- Avoid opening unverified emails or clicking links embedded in them.
- Back up important files using the 3-2-1 rule—create 3 backup copies on 2 different media with 1 backup in a separate location.
- Regularly update software, programs, and applications to protect against the latest vulnerabilities.

VII. BITCOIN THE CRYPTO CURRENCY

Bitcoin is a type of currency that can be used secretly by the people for buying anything be it services or goods on the internet. Bitcoin can also be used for exchanging money individually or in a group. The main idea behind bitcoin is non-involvement of banks, any government, credit card issuers or any other third parties. Once the system files and resources become hostage to the attacker, the money asked as ransom is always in the form of bitcoin to get control back of the system[10][11]

The reason behind using bitcoin by the users of the dark web and ransomware attacker is that the identity of the user is completely anonymous. The coins are created by users who 'mine' them by lending computing power to verify other users' transactions. The fee for using their resources is given in terms of bitcoin. The coins also can be bought and sold on exchanges with U.S. dollars and other currencies. As on writing this one bitcoin is equal to $2744.77. Going into bit deeper if you really want to know what bitcoin is then bitcoins are basically lines of computer code that are digitally signed each time they travel from one owner to the next. It can be termed as cash but only as digital. It's just a exchange of money between two persons with no inclusion of bank. The reason behind this is that no bank or government issues bitcoin[12[13]

A. WORKING OF BITCOIN

From a simple user point of view bitcoin is nothing more than a mobile app or computer program. It provides a personal Bitcoin wallet to each individual user. Use of bitcoin wallet let user to send and receive bitcoins. This is how Bitcoin works for most users.

The term “block chain” is used for public ledger in the Bitcoin network which is shared among its users. This ledger has an entry for every transaction that was carried out using bitcoin by any user in the network. The validity of the transaction can easily be verified by user's computer. To verify the authenticity of each transaction digital signatures are used which make use of signing message digest using the private key of the user. Use of digital signature let users to have full control over sending bitcoins from their own Bitcoin addresses. As discussed in the introductory paragraph for processing transactions computing power of specialized hardware of any user can be used and in exchange bitcoins can be earned as reward point. This is often called "mining".

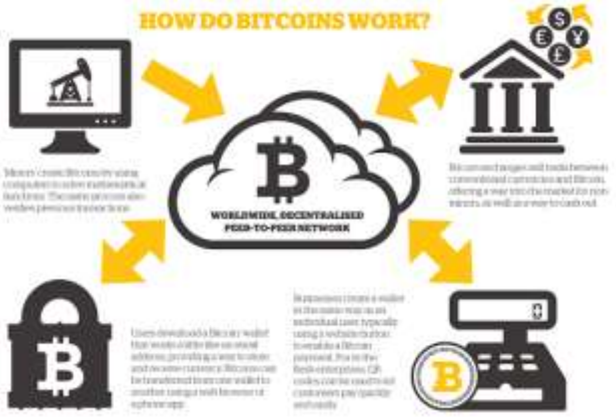


Fig 9: Working of Bitcoin[11]

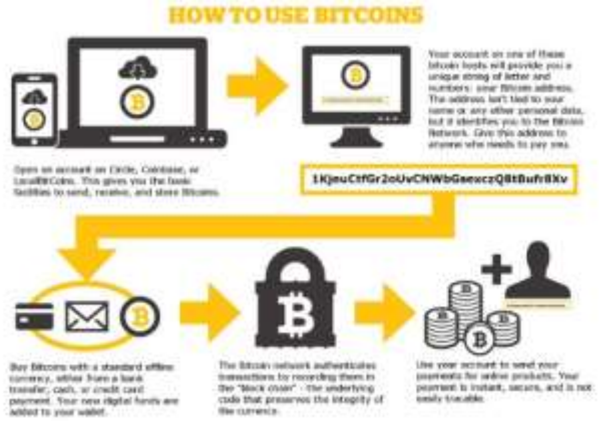

HOW TO USE BITCOINS
Open an account on Circle, Coinbase, or LocalBitCoins. This gives you the basic facilities to send, receive, and store Bitcoins.
Your account on one of these bitcoin tools will provide you a unique string of letter and numbers: your Bitcoin address. The address isn't tied to your name or any other personal data, but it identifies you to the Bitcoin Network. Give this address to anyone who needs to pay you.
1KjeuCtfGr2oUvCNWbGaexczQ8tBufr8Xv
Buy Bitcoins with a standard offline currency, either from a bank transfer, cash, or credit card payment. Your new digital funds are added to your wallet.
The Bitcoin network authenticates transactions by recording them in the "block chain" - the underlying code that preserves the integrity of the currency.
Use your account to send your payments for online products. Your payment is instant, secure, and is not easily traceable.

Fig 10: Transaction using bitcoin[11]

VIII. CONCLUSION

In this paper a complete survey of ransomware, its types, history, working, evolution, economic loss and effected users and organization is discussed. The paper has covered enough topics related to ransomware right from its evolution to the present day. The research paper wanted to convey a through coverage of ransomware covering all its related terminology, spreading methods, methods of prevention, concept of bitcoin and future of ransomware and it has succeeded in it.

ACKNOWLEDGMENT

The author would like to thanks Google search engine and various researcher, academicians, security specialist whose research papers, articles have helped me in preparing this manuscript. I also thank my colleagues and family members for their constant encouragement and untiringly support.

REFERENCES

[1] http://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html
[2] http://www.infosectoday.com/Articles/Ransomware/Evolution-of-Ransomware.htm#.WSWLPVFEldh
[3] https://heimdalsecurity.com/blog/what-is-ransomware-protection/
[4] https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
[5] http://www.securityfocus.com/advisories/700
[6] https://securelist.com/analysis/publications/75145/pc-ransomware-in-2014-2016/
[7] https://securelist.com/blog/research/78411/wannacry-faq-what-you-need-to-know-today/
[8] http://www.informationsecuritybuzz.com/articles/a-brief-history-of-ransomware/
[9] https://www.trendmicro.com/vinfo/us/security/definition/ransomware
[10] http://economictimes.indiatimes.com/wealth/spend/what-is-bitcoin-a-look-at-the-digital-currency/articleshow/58694578.cms
[11] https://www.quora.com/What-is-Bitcoin-and-how-does-it-work-Is-it-legal-Whos-behind-it
[12] https://en.wikipedia.org/wiki/Bitcoin
[13] http://metro.co.uk/2017/05/15/what-is-bitcoin-how-do-i-buy-it-and-why-do-ransomware-criminals-want-them-6638325/
[14] https://bitcoin.org/en/faq#what-is-bitcoin
[15] https://blog.knowbe4.com/new-knowbe4-survey-ransomware-infections-double-in-two-years
[16] http://blog.goldeneaglecoin.com/what-is-bitcoin-mining/
[17] https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/
[18] http://www.wired.co.uk/article/wannacry-ransomware-virus-patch
[19] https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware.