A Study on Ransomware and its Effect on India and Rest of the World

Naveen Kumar C.G
Research Scholar,
Bharathiar University
Coimbatore, Tamilnadu, India

Dr.Sanjay Pande M.B
Professor and Head of the Department
GMIT, Davanagere,
Karnataka,India

***Abstract*- - Increased growth of internet technology pave the way to every individual and organizations to access the information in touch of fingertip. Almost all the organizations are transacting their day to day activities using internet and they are completely depend upon the internet. Internet is exposed to many type of threats and attacks, it is the responsibility of the stakeholders to secure their information by these attacks. Right now, information security is one of the top priority of the organizations and also the individuals. Cyberattack is an offensive type that targets on information systems, infrastructures, and computer networks etc. by a means of malicious act and destroys or steals the information. This paper is aimed to study the recent attack of ransomware, history of ransomware, its impact on India and rest of the world. This paper also discusses important mechanisms to prevent ransomware**

Keywords—Ransomware; internet; cyberattack; security;

I. INTRODUCTION

Technological advancements since last two decades created plenty of opportunities to eat the fruit of technology to the society. It enables organisations and individuals to adopt the present technologies to map their daily needs. Today organisations including public and private sectors using the internet technology effectively and efficiently to fulfil their day to day activities. All most all organisations providing internet enabled services to its clients. Now the internet became the backbone of organisations. But at the same time, over the year's cyber-attacks and data loss are the two biggest concerns of the organisations.

Recent attack of ransomware flustered the whole world. It raised the caution to the cyber family of the world to secure or protect their information systems from the attack of ransomware. Ransomware is a type of targeted cyber-attack.

II. CYBER ATTACKS

Cyber-attacks are socially or politically motivated attacks carried out primarily through the Internet. It uses malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft, unauthorized web access, fake websites, and other means of stealing personal or institutional information from targets of attacks, causing far-reaching damage. Attacks target the general public or national and corporate organizations [1].

III. TYPES OF CYBER ATTACKS

Cyber-attacks are mainly categorized into four types, they are:

- Targeted attack

Cyber-attacks that are geared at particular organizations, services, and individuals to obtain private, technical, and institutional information, and other intellectual assets for the purpose of vandalism or monetary gain.

- APT (Advanced Persistent Threat)

A kind of targeted attack geared at a particular entity and carried out continuously and persistently using a variety of means in order to gain access to the target. APTs are mainly divided into

(a) Attacks through public servers and public websites on the Internet and

(b) Attacks against users through social engineering of target users into sending malicious programs (typical example is targeted email attack).

- DoS (Denial of Service) attack

A cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

- DDoS (Distributed Denial of Service) attack

An attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

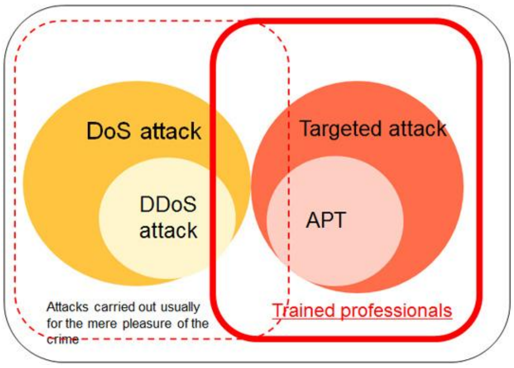

DoS attack
DDoS attack
Targeted attack
APT
Attacks carried out usually for the mere pleasure of the crime
Trained professionals

Fig 1: Types of cyber attacks

IV. RANSOMWARE

Ransomware is a form of malicious software that locks up the files on your computer, encrypts them, and demands that you pay to get your files back. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

V. HISTORY OF RANSOMWARE

Ransomware is one of the largest threat, both in home and at work, too. From humble beginnings, it has become an immense global business that nets millions, sometimes billions, for its creators.

The name ransomware, derived from the two words, ransom and software, is malicious software designed to extort money from a victim, by either holding specific files hostage or by locking the entire computer until a ransom is paid.

Hackers realize that victims are willing to pay to obtain access to their files, specifically ones that hold important, personal content, such as photos, documents or security keys. Additionally, they know that once the ransomware has been developed, the system will remain low maintenance. Because this crime does not involve credit card fraud, which typically requires mules or cloners, making financial transactions is much easier. Whether extorting $300 per user from a small business or $30 million from a multinational enterprise, the level of effort is often similar.

Over the years there have been two distinct varieties of ransomware which remain consistent: crypto and locker based. Crypto-ransomware is ransomware variants that actually encrypt files and folders, hard drives, etc. Whereas locker-ransomware only locks users out of their devices, most often seen with Android based ransomware.

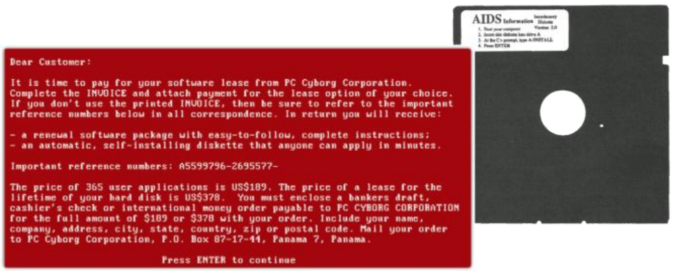
New-age ransomware involves a combination of advanced distribution efforts such as pre-built infrastructures used to easily and widely distribute new strains as well as advanced development techniques such as using crypters to ensure reverse-engineering is extremely difficult.

What's important to note is that ransomware isn't new. In fact, it's nearly 30-years-old. Below is a look at how this threat started and highlights of how it has evolved over time.

1989: THE FIRST OF ITS KIND

1989: The first ransomware virus predates email, even the Internet as we know it, and was distributed on floppy disk by the postal service. It was named the 1989 AIDS Trojan, also known as PS Cyborg. Harvard-trained evolutionary biologist Joseph L. Popp sent 20,000 infected diskettes labeled "AIDS Information – Introductory Diskettes" to attendees of the World Health Organization's international AIDS conference.

But after 90 reboots, the Trojan hide directories and encrypted the names of the files on the customer's computer. To regain access, the user would have to send $189 to PC Cyborg Corp. at a post office box in Panama. Popp was eventually caught and it didn't take long for decryption tools to recover the file names, but this effort set in motion over almost three decades of ransomware attacks.


```
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
```

Fig 2. Trojan AIDS Ransomware

2005-2006: THE RETURN

2005: Fake programs for spyware removal emerged. These software programs claimed to fix critical issues and wanted you to buy a license in the average of 50 U.S. dollars. In actuality, they fixed next to nothing and only exaggerated with the errors they uncovered.

2005: In September 2005, Susan Schaibly wrote an article, "Files for Ransom," for NetworkWorld magazine which contained the first known use of the term "ransomware."

2006: Almost two decades after the first ransomware malware was distributed, another strain was released. But unlike before, this new strain was much more difficult to remove and used RSA encryption for the first time in ransomware history. The Archiveus Trojan encrypted everything in the "My Documents" directory on a system and required users to make purchases from specific websites to obtain the password to decrypt the files.

2008-2009: FAKE ANTIVIRUS APPLICATIONS

2008: Two years after GPcode ransomware was created, GPcode.AK was unleashed and began spreading from PC to PC. Each computer GPcode.AK infected, it would lock or encrypt the victim's files and require the user to pay a ransom or fee to get a code which would unlock their files. The difference between the first GPcode and GPcode.AK was the use of a 1024-bit RSA key used to lock or encrypt the victim's files, making this newer version more of a nuisance and harder to crack.

2008: Bitcoin was introduced in 2008, followed by the release of its open-source software in January 2009. These developments led to an incredible spike in ransomware attacks that have continued to increase ever since.

2009: In 2009 a lot of fake antivirus programs compromised computer systems. They looked and acted almost the same as their legitimate counterparts, but could demand up to 100 U.S. dollars for “fixing” problems on your PC. As a reason for the higher price, these applications provided fake technical support for years on end.

2011-2012: LOCKER RANSOMWARE

2011: A new type of ransomware emerged in 2011: Rather than encrypt files, Trojan. Winlock displayed a fake Windows Product Activation notice which could only be removed if the victim input an activation key. In order to acquire this key, the user was required to call an international premium rate number.

These early strains of ransomware had one thing in common: they were easily defeated due to the weak encryption and unsophisticated infection methods used. However, cybercriminals would learn from these early failures.

2012: A major ransomware Trojan known as Reveton began to spread throughout Europe. Based on the Citadel Trojan, the piece of ransomware claimed the computer under attack had been used for illegal activities and that in order to unlock the system, the user would be required to pay a fine using a voucher from an anonymous prepaid cash service. In some strains, the computer screen displayed footage from the computer’s webcam to give the illusion that the “criminal” was being recorded. Shortly after this incident, there was a flurry of “police-based” ransomware including Urausy.

Researchers discovered new variants of Reveton in the U.S., claiming to require the payment of a $200 fine to the FBI using a MoneyPak card.

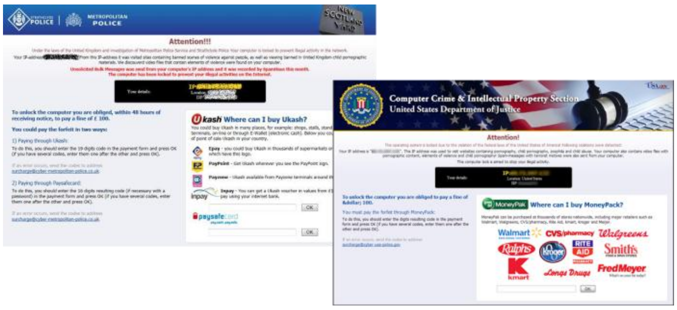

POLICE
METROPOLITAN POLICE
NEW SCOTLAND YARD
Attention!!!
To unlock the computer you are obliged, within 48 hours of receiving notice, to pay a fine of £ 100.
You could pay the forfeit in two ways:
1) Paying through Ukash:
2) Paying through Paysafecard:
Ukash Where can I buy Ukash?
Epay
PayPoint
Payzone
Inpay
paysafecard
OK
Computer Crime & Intellectual Property Section
United States Department of Justice
Attention!
To unlock the computer you are obliged to pay a fine of &dollar; 100.
You must pay the forfeit through MoneyPack:
MoneyPak Where can I buy MoneyPack?
Walmart
CVS/pharmacy
Walgreens
Ralphs
Kroger
RITE AID
Smith's
Kmart
Longs Drugs
FredMeyer
OK

Fig 3: Police Ransomware

2013 AND BEYOND: THE EMERGENCE OF BITCOIN

2013: 2013 saw the birth of Cryptolocker, a crypto-ransomware that was spread via email. Cryptolocker demanded that the victim pay $400 in Bitcoin within 72 hours. This ransomware infected half a million computers, and 1.3 percent of the victims paid the ransom. The attackers netted an estimated $27 million from their victims.

An international collaborative effort called Operation Tovar was formed to crack down on Cryptolocker and another ransomware program, the Gameover Zeus botnet. As a result, Russian hacker Evgeniy Mikhailovich Bogachev was caught and charged as an administrator of both Cryptolocker and Gameover Zeus.

2014: CryptoDefense is released. It uses Tor and bitcoin for anonymity and 2,048-bit encryption. However, because it uses Windows’ built-in encryption APIs, the private key is stored in plain text on the infected computer. Despite this flaw, the hackers still manage to extort at least $34,000 in the first month, according to Symantec.

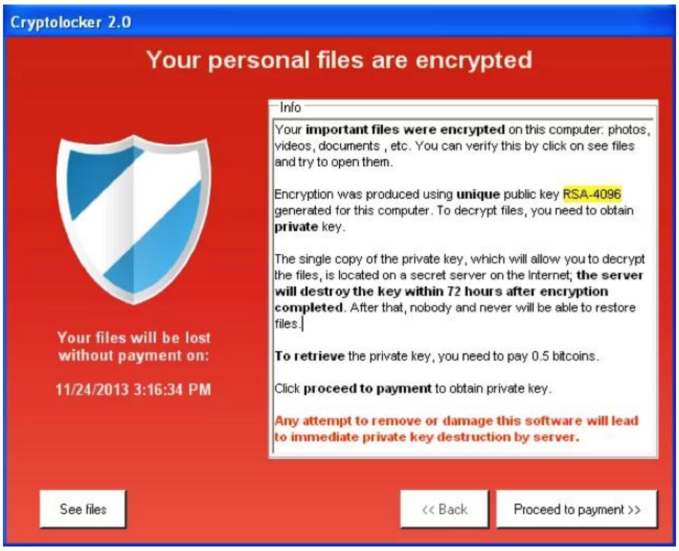
2015: An aggressive Android ransomware strain started to spread across America in September. Security researchers at ESET discovered the first real example of malware capable of resetting the PIN of your phone to permanently lock you out of your own device. Dubbed LockerPin, the ransomware changes the infected device’s lock screen PIN code and leaves victims with a locked mobile screen. LockerPin then demanded $500 to unlock the device.

2016: The first official Mac OSX-based ransomware, KeRanger was discovered in 2016, delivered via a Transmission BitTorrent client for OSX. The ransomware was signed with a MAC development certificate, allowing it to bypass Apple’s GateKeeper security software.

2016: The Jigsaw ransomware became the first of its kind in which the ransom note contained the popular Jigsaw characters from the movie series SAW. It also threatened to delete a file every 60 minutes if the $150 ransom was not paid. Additionally, if a victim attempted to stop the process or restart their machine, it then deleted 1,000 files.

2017: MASSIVE RANSOMWARE ATTACK

On May 12, 2017, various organizations around the world had been affected by a massive ransomware attack. WannaCry infected more than 200,000 networks in 150 countries. The attackers exploited a Windows XP vulnerability used by the NSA for espionage and surveillance.



Your personal files are encrypted

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Fig 4. WannaCry Ransomware

WHAT'S NEXT?

The threat of ransomware continues to evolve, with a new spin on *extortionware*, called *doxware*, that's designed to target and potentially expose sensitive data of ransomware victims. The term "doxware" is a combination of doxing — posting hacked personal information online — and ransomware. Attackers notify victims that their sensitive, confidential or personal files will be released online. If contact lists are also stolen, the perpetrators may threaten to release information to the lists or send them links to the online content.

Doxware and ransomware share some similarities. They both encrypt the victim's files, both include a demand for payment, and both attacks are highly automated. However, in a ransomware attack, files do not have to be removed from the target; encrypting the files is sufficient. A doxware attack is meaningless unless the files are uploaded to the attacker's system. Uploading all of the victim's files is unwieldy, so doxware attacks tend to be more focused, prioritizing files that include trigger words such as confidential, privileged communication, sensitive or private.

VI. HOW IT SPREADS

According to the US Computer Emergency Readiness Team (USCRT), under the Department of Homeland Security, ransomware spreads easily when it encounters unpatched or outdated software. Experts say that WannaCry is spread by an internet worm -- software that spreads copies of itself by hacking into other computers on a network, rather than the usual case of prompting unsuspecting users to open attachments. It is believe that the cyber-attack was carried out with the help of tools stolen from the National Security Agency (NSA) of the United States.

Typically ransomware spread and delivered through social engineering (trickery) and user interaction...opening a malicious email attachments (usually from an unknown or unsolicited source), clicking on a malicious link within an email or on a social networking site. Crypto malware can be disguised as fake PDF files in email attachments which appear to be legitimate correspondence from reputable companies such as banks and other financial institutions, notices with tracking numbers. Attackers will use email addresses and subjects (purchase orders, bills, complaints, and other business communications) that will entice a user to read the email and open the attachment. Another method involves tricking unwitting users into opening Order Confirmation emails by asking them to confirm an online e-commerce order, purchase or package shipment.

Some attackers will use Shortened malicious URLs to mask a malicious link, obfuscating a malicious destination and malicious script (i.e. JavaScript (.js) file) downloader.

Still another technique uses spam emails and social engineering to infect a system by enticing users to open an infected word document with embedded macro viruses and convince them to manually enable macros that allow the malicious code to run.

Social engineering has become one of the most prolific tactics for distribution of malware, identity theft and fraud.

Crypto malware can also be delivered via malvertising attacks, exploit kits and drive-by downloads when visiting compromised web sites. An Exploit Kit is a malicious tool with pre-written code used by cyber criminals to exploit vulnerabilities (security holes) in outdated or insecure software applications and then execute malicious code.

Some victims have encountered crypto malware from ransomware malware executables, packaged NW.js application using JavaScript or following a previous infection from one of several botnets such as Zbot (frequently used in the cyber-criminal underground) which downloads and executes the ransomware as a secondary payload from infected websites.

VII. GENERAL IMPACT OF RANSOMWARE

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including [9]

- Temporary or permanent loss of sensitive or proprietary information,
- Disruption to regular operations,
- Financial losses incurred to restore systems and files, and
- Potential harm to an organization's reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

VIII. EFFECT OF RANSOMWARE ON INDIA AND REST OF THE WORLD

Gulshan Rai, the Cyber Security Chief in the PMO said that, there are no major incident in India. As a preventionary mechanism The Indian Computer Emergency Response Team (CERT-In), issued an advisory asking organizations to install updates to Windows systems, “a possible remote exploitation of this vulnerability.” The agency advised that the patch released by Microsoft be applied.

“CERT has checked hundreds of systems since alerted cyber-attack. The attacks seem to be the result of a vulnerability in the Microsoft windows OS.

CERT-In explained that this ransomware called WannaCrypt or WannaCry encrypts the computer’s hard disk drive and then spreads laterally between computers on the same local area network.

According to Kaspersky, only about 5% attacks were reported in India. Quick Heal Technologies Ltd, the maker of antivirus software, has said detected “detected over 48,000 MS-17- 010 Shadow Broker exploit hits responsible for ‘WannaCry ransomware’ outbreak in India”, with West Bengal witnessing the most incidents.

The company said 60% of the ransomware attack attempts by the malicious WannaCry virus were targeted at enterprises, while the rest were on individual customers. Quick Heal received nearly 700 distress calls by customers following the discovery of the attacks which has impacted 150 countries globally.

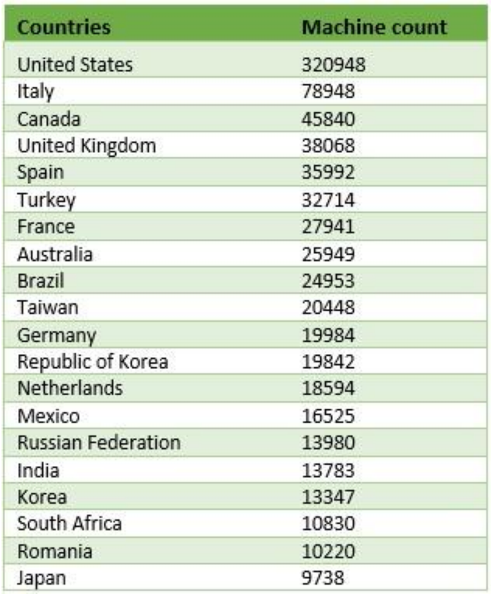
The top five cities impacted by the ransomware attack are Kolkata followed by Delhi, Bhubaneswar, Pune and Mumbai, while the top five states with maximum detections of WannaCry virus are West Bengal, Maharashtra, Gujarat, Delhi NCR, and Odisha.

Quick Heal claimed that it “successfully detected” the ransomware attack and “cleaned the malicious file responsible for file encryption from all the attacked systems.

Indian computer systems have largely escaped a global ransomware attack as the government and companies installed security patches to gain an upper hand against the first wave of an unrivalled global cyber-attack.

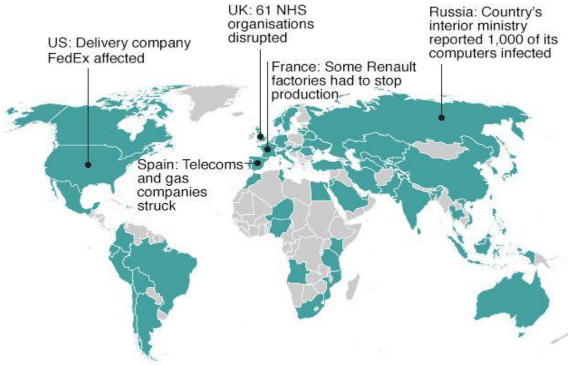
A global cyberattack unleashed that more than 200,000 computers across more than 150 countries were affected by the "ransomware," called "WannaCry,"

Microsoft recently published a data mentioning how many machines (users) were affected by ransomware attacks across the world. It was found that the United States was on the top of ransomware attacks; followed by Italy and Canada. Here are the top 20 countries which are majorly affected by ransomware attacks.



Countries	Machine count
United States	320948
Italy	78948
Canada	45840
United Kingdom	38068
Spain	35992
Turkey	32714
France	27941
Australia	25949
Brazil	24953
Taiwan	20448
Germany	19984
Republic of Korea	19842
Netherlands	18594
Mexico	16525
Russian Federation	13980
India	13783
Korea	13347
South Africa	10830
Romania	10220
Japan	9738

Countries hit in initial hours of cyber-attack


US: Delivery company FedEx affected
UK: 61 NHS organisations disrupted
France: Some Renault factories had to stop production
Russia: Country's interior ministry reported 1,000 of its computers infected
Spain: Telecoms and gas companies struck

*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Norway, where incidents have been reported since

IX. HOW TO PREVENT RANSOMWARE

The best way to protect the computer is to create regular backups of files. The malware only affects files that exist in the computer. If the machine is infected by ransomware, reset the machine using backup and reinstall the software and restore all the files from the backup.

According to Microsoft’s Malware Protection Centre, other precautions include regularly updating your anti-virus program; enabling pop-up blockers; updating all software periodically; ensure the smart screen (in Internet Explorer) is turned on, which helps identify reported phishing and malware websites; avoid opening attachments that may appear suspicious. As the popular saying “Prevention is better than Cure”. Here are a few steps you can take to tackle or deal with ransomware attacks:

- Windows users advised to keep their Windows Operating System up-to-date. It is advisable upgrade to windows 10
- Always back-up your important data in an external hard-drive.
- Enable file history or system protection.

- Beware of phishing emails, spam, and check the email before clicking the malicious attachment.
- Disable the loading of macros in Office programs.
- Disable your Remote Desktop feature whenever possible.
- Use two-factor authentication.
- Use a safe and password-protected internet connection.
- Avoid browsing websites that are often the breeding grounds for malware such as illegal download sites, porn sites and gambling sites.
- Install, use, and regularly update an antivirus solution
- Make use of some good anti-ransomware software
- Don’t pay the ransom. As tempting as it may seem, it won’t guarantee that you will get your files back and it simply helps to fund criminals.

X. CONCLUSION

The nature of internet is vulnerable to threats. Hence cyber security must be the top priority of the organizations. Organizations should implement necessary security policies to avoid security breaches. The recent attack of ransomware, a malware program which flustered the whole world. It is the need of the hour to take precautionary mechanisms to avoid ransomware attacks further.

XI. REFERENCES

[1] http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html

[2] https://spideroak.com/ransomware/timeline

[3] The History Of Ransomware: Where It Started And Where It’s Going by Ladan Nikravan Hayes

[4] http://www.complete-it.co.uk/a-brief-history-of-ransomware/

[5] http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html

[6] https://medium.com/threat-intel/ransomware-history-3165f10ab5a5

[7] https://www.datto.com/uk/blog/the-history-of-ransomware

[8] http://www.thehindu.com/sci-tech/technology/internet/cert-in-alert-on-ransomware-attack/article18448177.ece

[9] https://security.berkeley.edu/faq/ransomware/what-possible-impact-ransomware

[10] http://www.bbc.com/news/technology-39920141

[11] http://www.thewindowsclub.com/ransomware-attacks-definition-faq

[12] www.wikepedia.com

[13] www.csoonline.com

[14] http://www.informationsecuritybuzz.com/articles/a-brief-history-of-ransomware/