Evolving Threat Agents: Ransomware and their Variants

Toshima Singh Rajput
Affiliated to Barkatullah University
Institute of Technology
112/4B Saket Nagar
Bhopal M.P. (India)

ABSTRACT
This paper studies different kinds of ransomware attacks right from its point of origin to the latest kind of ransomware attacks. As this malware threat has reported a significant increase in the number of report incidents happenings in countries like USA, UK and India. A study of its evolution provides for its first line of defense. So the paper offers an awareness of different kinds of ransomware variants from 1989 to 2017. It also analyses the effects of this malware on Android and Windows platform. After describing these variants it also presents the attack vectors of the Ransomware revolution. The paper also provides guidelines on preventing the losses by avoiding infection.

General Terms
Malware analysis, Malicious software classification.

Keywords
Ransomware, Ransomware evolution, Ransomware classification, Ransomware analysis

1. INTRODUCTION
The rising use of internet for vast information and resources usage, have paved way for the increased amount of threats to vulnerabilities or loopholes in the system. Among the many threats, Ransomware is one of the famous malwares supposed to be one of the topmost threats in the year 2017 and is going to increase in surplus amongst the internet users. Everyday a new victim falls prey to it. For cybercriminals it is profitable, easy money with low risk accessibility. But for business entrepreneurs it is going to be high risk, low profitability and earn great losses for the company.

According to recent reports, a group called as Telebots have launched malware attacks against Ukrainian financial sector using a malicious program called KillDisk. Instead of wiping the data from the system the malware encrypts it and demands a huge ransom to release the data. This attack continued for a month and also aimed at sea transportation sector as well as in Ukraine.

The Symantec, McAfee, Control risks and others have ranked it as one of the topmost threats in the year 2017.Ransomware is a malicious software which block or encrypts the user valuable files and asks for a ransom amount to unblock or decrypt the file. It restricts the user to access their data and forces them to pay for accessing their device data. Some ransomware also does not restrict access, but lures the user to pay some ransom amount through trickery messages.

Modern ransomware can not only impact personal computers but have broadened their horizon by accessing other devices too including IOT. Mobile apps also have many ransomware variants installed in useful apps which when downloaded can harm the smartphones. Android smartphones have become a open and permissive platform which offers their user the flexibility to install apps from any sources thus making their device accessible to the threats. The cloud based services also have become the targets by these ransomware as they become the point of earning money for these cybercriminals. The servers in these organizations act as a central repository of different important documents, files, reports, transaction details and are the major weak points of the business. These ransomware use extortion methods to encrypt these files and lock their data and prompt them to release their data, only if the ransom is paid.

2. KEY CHARACTERISTICS OF RANSOMWARE
These features set it apart from other kinds of malware

- Strong encryption which means that you can't decrypt the files rather you have to use specific decryption tools.
- It has the ability to encrypt files including documents, pictures, audio files, archive and even certificates too.
- It scrambles your files thus making your system vulnerable as you don't know which data was affected.
- It adds different extensions to files like .docx.rsrc.
- It displays a ransom message with the help of an image.
- Bitcoin is an international currency that facilitates peer-to peer payments. This site is used for illegal activities such as in dark web black markets. Its fees are considerably lower and offers recorded transactions. Ransomware uses Bitcoins as a common currency platform.
- Tor is an anonymous and encrypted network accessible through free software widely used by the public and military establishments and is widely popular among cybercriminals. It allows the attackers to hide their location from those conducting network surveillance. It provides RaaS (Ransomware as a Service) platform which can be customized and deployed by attackers. The attackers will download the malware for distribution across a network paying a fee or a percentage of the ransom revenue they are able to generate from their victims.
- It uses complex obfuscation of evasion techniques so that it can go undetected by installed security programs (Antiviruses).
- It escalates the level of infected PCs to botnets so that it can become prone to future attacks.

- It performs data exfiltration thus user credentials are lost when it is infected by Ransomware.
- The ransom note is JavaScript enabled which allows the ransom note to be displayed according to the geographical location of the victim thus in-built localization policy.

3. ANALYSIS OF RANSOMWARE ON WINDOWS AND ANDROID PLATFORMS

The malware data set was collected from the repositories like VirusTotal[12] and AVCeasar[13] and other repositories like Contagiodump[14] and online reports of sandboxes[15]. Based on these samples the ransomware families were identified by comparing their MD5 hash values to the known families of ransomwares identified by antivirus engines. They include the products mostly downloaded from Program repositories like Github or Microsoft websites. The programs are mostly coded in C/C++/Delphi/Python. These families either use fake identification of known agencies like FBI, CSI, and Cyber crime centre. They ask the user to download some browsers and on downloading they induce the following payloads

3.1 Modification of registry entries

These ransomwares modify the registry entries after gaining administrator privileges by modifying its shell entries like some versions of cryptolocker modify the registry like

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "CryptoLocker":<random>.exe

*HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker":*<random>*.exe*

Additionally the configuration data gets stored in

HKCU\SOFTWARE\CryptoLocker or
HKCU\SOFTWARE\CryptoLocker_0388

It also removes the Volume Shadow copies, known as Volume Snapshot services(VSS) files so that user cannot recover their machine through these backups. It then deletes the old registry values and writes “completed=1” value to the malware registry key. It then opens an instruction text file and creates the image from the text file which contains payment information displayed on the desktop wallpaper like Locky changes the desktop background to the bitmap image.

HKCU\Control Panel\Desktop\Wallpaper is set to:
%CSIDL_DESKTOPDIRECTORY%_Locky_recover_instructions.bmp

3.2 Collection of information

Some ransomware families collect information like IMEI number, phone number, call logs, contacts, profile, history bookmarks, SMS, the list of accounts in account service, phone state, GPSlocation of the phone, and IP address. The malware computes the user id and collects information about the infected machine. This user id is generated as a MD5 hash value from the infected machines hard disk. It checks the infected machines version and its type of OS, Affiliate ID and even the language in which the machine operates to display the ransom message.

In Android phone, malware gets installed in the form of APK files in the disguise of a game file and requests the following permissions while downloading

<!-- unlimited Internet access -->

"android.permission.INTERNET"

<!-- network state monitoring -->

"android.permission.ACCESS_NETWORK_STATE"

<!-- read phone state and ID -->

"Android.permission.READ_PHONE_STATE"

<!-- run app when booting the phone -->

"Android.permission.RECEIVE_BOOT_COMPLETED"

<!-- prohibit switching the phone into sleep mode -->

"android.permission.WAKE_LOCK"

<!-- read SD card content -->

"android.permission.WRITE_EXTERNAL_STORAGE"

<!-- write to SD card -->

"android.permission.READ_EXTERNAL_STORAGE"

Two services gets started after the display of immodest messages like ServiceStarter and SDCardServiceStarter and its subcomponents MainService and TorService.

3.3 Infected files

The files that are infected by cryptolocker have enhanced its set from .doc or.txt to more versions of data files like media files, database objects etc. These file extension are like .3DM, .3DS, .3G2, .3GP, .7Z, .ACCDB, .AES, .AI, .AIF, .APK, .APP, .ARC, .ASC, .ASF, .ASM, .ASP, .ASPX, ASX, .AVI, .BMP, .BRD, .BZ2, .C, .CER, .CFG, .CFM, .CGI, .CGM, .CLASS, .CMD, .CPP, .CRT, .CS, .CSR, .CSS, .CSV, .CUE, .DB, .DBF, .DCH, .DCU, .DDS, .DIF, .DIP, .DJV, .DJVU, .DOC, .DOCB, .DOCM, .DOCX, .DOT, .DOTM, .DOTX, .DTD, .DWG, .DXF, .EML, .EPS, .FDB, .FLA, .FLV, .FRM, .GADGET, .GBK, .GBR, .GED, .GIF, .GPG, .GPX, .GZ, .H, .H, .HTM, .HTML, .HWP, .IBD, .IBOOKS, .IFF, .INDD, .JAR, .JAVA, .JKS, .JPG, .JS, .JSP, .KEY, .KML, .KMZ, .LAY, .LAY6, .LDF, .LUA, .M, .M3U, .M4A, .M4V, .MAX, .MDB, .MDF, .MFD, .MID, .MKV, .MML, .MOV, .MP3, .MP4, .MPA, .MPG, .MS11, .MSI, .MYD, .MYI, .NEF, .NOTE, .OBJ, .ODB, .ODG, .ODP, .ODS, .ODT, .OTG, .OTP, .OTS, .OTT, .P12, .PAGES, .PAQ, .PAS, .PCT, .PDB, .PDF, .PEM, .PHP, .PIF, .PL, .PLUGIN, .PNG, .POT, .POTM, .POTX, .PPAM, .PPS, .PPSM, .PPSX, .PPT, .PPTM, .PPTX, .PRF, .PRIV, .PRIVAT, .PS, PSD, .PSPIMAGE, .PY, .QCOW2, .RA, .RAR, .RAW, .RM, .RSS, .RTF, .SCH, .SDF, .SH, .SITX, .SLDX, .SLK, .SLN, .SQL, .SQLITE, .SQLITE, .SRT, .STC, .STD, .STI, .STW, .SVG, .SWF, .SXC, .SXD, .SXI, .SXM, .SXW, .TAR, .TBK, .TEX, .TGA, .TGZ, .THM, .TIF, .TIFF, .TLB, .TMP, .TXT, .UOP, .UOT, .VB, .VBS, .VCF, .VCXPRO, .VDI, .VMDK, .VMX, .VOB, .WAV, .WKS, .WMA, .WMV, .WPD, .WPS, .WSF, .XCODEPROJ, .XHTML, .XLC, .XLM, .XLR, .XLS, .XLSB, .XLSM, .XLSX, .XLT, .XLTM, .XLTX, .XLW, .XML, .YUV,.ZIP, .ZIPX etc.

3.4 Network

The email attachment when downloaded through a ransomware contains a javascript(.js) which when enabled allows the system to conduct a ping in the background Contacts a domain associated with Tor hidden services and sends the UDP traffic to this malicious IP address hosts. These malware contain hardcoded IP addresses hosts with HTTP over TCP port 80 which establishes a communication

with the command-control servers. These vulnerable ports are identified by Wireshark. These malware then use domain generation algorithm which generate new domain every two days. They are used for reporting infections and exchanging information's.

3.5 Encryption

The encryption used by the first ransomware variants was a symmetric key algorithm. But nowadays the families use the symmetric techniques to encode the file data and asymmetric key to encode the key. The Advanced Encryption Standard (AES) is used for symmetric and Rivest, Shamir, & Aldeman(RSA)/Rivest Cipher 4(RC4) for AES public key encryption algorithm. The first ransomware variants used a symmetric-key algorithm and eventually upgraded to public-keys. Today, more advanced ransomware use a combination of symmetric and public.

4. EVOLUTION OF RANSOMWARE:1989 TO 2017

The first ever Ransomware infection was through a snail mail on a 5 1/4'' floppy disk called as **AIDS Trojan** in the year 1989.Despite the fact that internet were only used by scientists and the idea of encryption technology was weak, as it did not encrypt the data rather filenames were encrypted and the means of payment was difficult to process. The Trojan couldn't do much harm and thus was unsuccessful.

Although the concept gained much significance in the year 2005 and 2006 when a set of misleading applications called as scareware gained momentum. First of its kind was **Quickshiel**[3], developed by Securelink Networks and High falls media, who were sued by Microsoft and Washington Attorney General in 2005. These set of applications used to abstain information from the users by posing as a fake antispyware or antivirus tool. Some of them were **SpySherriff, Performance Optimizer, Registry care, AdwarePunisher and Nortel**. These application used to ask the user pay a ransom amount within the range of USD $30 to USD$90 for cleaning corrupt files or deleting unused registry entries from the computers. The first wave of modern CryptoRansomwares came into existence during this era. The first one was **Trojan.Gpcoder** in the year 2005 which used symmetric encryption algorithm i.e the same key was used for both encryption and decryption. It was also called as **PGPCoder** encrypted common user files with extensions such (.doc, .html, .jpg, .xls and .zip).This Trojan would drop a text file that demanded payment for each directory access with infected files. The payment was in the range of USD $100 to USD$200 or a Liberty Reserve Account.

The next threat was **Trojan.Cryzip** in March 2006, wherein the attackers used the idea of copying data files into password protected archive files and deleting the original files using the password embedded inside the code of the Trojan. In the same year **Trojan.Archevius** was also deployed with the same feature, except they asked the victim to buy medicine from the provided pharmacy URLs instead of paying the ransom amount by cash.

The next stage of threat evolution was in year 2008 to 2009 when **Fake antivirus** tools were used by cybercriminals to earn money. They used to perform mock scans of the system and give a list of fake threats and security issues in the computer. The users were made to pay USD $40 to USD$100 and some were even made to pay for the multiple year support services. When Fake AV victims started ignoring the AV alerts or started removing the software, cybercriminals moved on to develop further advance ways to earn money.

The era of 2011 and 2012 gave way to new form of threat from the attackers called as Locker Ransomwares, the most well known family called as **Reveton**. In this the cybercriminal disabled the user from accessing their system thus locking up the computer from use. This threat charged around US$150 to US$200 payable through electronic cash vouchers. The first computer locking malware was deployed in the year 2008 called as **Trojan.Ransom.C**. This Trojan spoofed a Windows security centre message locking the computer and asking the user to call a premium rate phone to reactivate the license of the security software.

In this type of threat the victims were exposed to not only fake error messages but also led the attackers introducing real errors and problems in the system. The **Locker ransomware** used social engineering techniques by giving the threat notices as law enforcement notices like FBI notices. The attackers used to give real looking fraudulent threats to the victim, like you have downloaded copyrighted material or watched illegal pornographic videos and have to pay a security amount as payment of fine. Thus there was an increased number of law enforcement ransomware for which the victims had to pay. But these were so real that it had some unforeseen outcomes too among the public.

The era of 2013 saw the family of ransomware move back to data encryption technology called as **Crypto Ransomware**. It did not use the social engineering techniques to lure the victims but fed on the user's lack of knowledge about computer security.

It used to encrypt the files stored on the computer including the data stored on external hard drives. Based on some common actions of the system it gets installed in the system. It searches for specific files in the system and makes a copy of it, encrypts those files and deletes the originals. It then displays extortion messages to the user that his system files are encrypted and offers a payment link to the user. This payment link is the international cyber currency site called as Bitcoin which then make the user believe as legitimate transaction is going on instead of a fake counterfeit transaction thus making him pay for decryption of the files. The decryption key resides in the attackers control server and is retained there until the payment is done.

Many variants of Crypto ransomwares have been evolved working on versions and creating a metamorphosis stage variant. Some of them are Cryptolocker, CryptoWall/CrytoDefense, CTBLocker/Citroni and TorrentLocker, Bitcryptor and coin Vault,TeslaCrypt, Locky,KeRanger

Cryptolocker appeared in September 2013 and showed the new tactics of cybercriminals who used the familiar method of symmetric and asymmetric cryptography and Rivest Shamir Aldeimann algorithm RSA-2048 for key pairs. The data is encrypted with a symmetric key which is then encrypted with a public asymmetric key added to the file. Once all the 70 files of common type have been encrypted the ransomware displays a ransom message for private asymmetric key. It also gives a warning that the symmetric key will be deleted, if the deadline for the payment is not followed. This was propagated through an email sent by Zeus Botnet. This was disabled in the year 2014 when the Zeus Botnet was taken over but still some copy cats have emerged in the history of ransomwares.

Cryptowall first appeared in 2014 and since then many versions have appeared. Its version 2.0 had many propagation channels like email attachments, drive by downloads, exploit kits and malicious pdfs. It also added the use of Onion router (TOR) network for communication to the control server. The version 3.0 uses the privilege escalation techniques and another peer to peer network called as Internet Project (I2P) network which is a superior network because of its dynamics.

Cryptowall 4 used encryption of filenames along with data to further alleviate the complexity of the encryption process. It uses the explicit mechanisms to evade firewalls and antiviruses installed in the users systems. In June 2015 FBI report posted an alert warning the public of the schemes of Cryptowall resulting in US $18 million losses and identified it as a major threat for the US individuals and businesses.

CTB-Locker is another kind of Cryptolocker that came into existence around the mid 2014s.The ransomware finds their victims through their spam emails or by running malicious websites which deploy exploit kits. The name is derived from the Curve –Tor-Bitcoin locker which uses the elliptic curve cryptography, Tor network for communication and the ransom amount as Bitcoins. Its ransom notes can be displayed in different European languages. It uses polymorphic malware builder to generate malware with a unique hash value for each victim which cannot be detected by antivirus intrusion programs.

TorrentLocker began to appear in 2014 which apart from encrypting files and demanding a ransom in Bitcoins, it used to harvest emails addresses and use them to send spam emails to the victims contact to propagate further. It deletes windows volume shadow copies which are used for restoring older encrypted versions, so that user can pay a ransom amount to recover their files. It is normally set to $500 Bitcoins to be payable to different addresses for each victim.

Ransomware as a Service (RaaS) model was a common platform for cybercriminals which separate technically skilled malware programmers and script kiddies who are more advanced in deploying the malware and exploiting the systems. The whole setup is hidden inside the TOR network wherein a hacker can go to the site hosted on the TOR network and enter a Bitcoin wallet address, choose the ransom amount and the ransom message he wishes to display. Only 70-80% of the ransom is collected by the attacker and rest is used by the developer.

BitCryptor and Coin Vault were the two ransomware variants that infected thousands of machines in NetherLands in the year 2015. Kaspersky, a security firm could decrypt 14000 keys that were needed to decrypt victims files. Thus this security firm created a tool to be downloaded free to recover from the damage done by both of them.

Tesla Crypt appeared in 2015 used to target saved data and files created from games such as Call Of Duty and World of WarCraft. These files were encrypted by the ransomware enabling him to pay $500 Bitcoins. The Cybercriminals released the master decryption key for the ransomware in the year 2016 and thus stopped its propagation. ESET security firm distributed a free tool to recover the damaged files of the victim using the master key.

Locky first appeared in 2016 which used the Microsoft Office attachments to infect systems. When Office attachment is clicked the ransomware prompts the user to enable Office macros. The user enables the macros and he is unaware of the fact that a malware is downloaded in the background during the process. The user files get encrypted and he is prompted with a ransom message set at his desktop wallpaper. This message asks the user to download a Tor Browser and visit a link specified in the Ransom note.

More enhanced versions of Locky infect the users via JavaScript attachments that are run by Windows script host without any need for macros to be enabled. It encrypts the Windows Volume Snapshot services also.

KeRanger appeared in 2016 is the first piece of ransomware to affect the MAC OS. It infects the installer of the BitTorrent client called Transmission. The users system gets infected during the installation of this installer file. This ransomware waits for 3 days and then encrypts 300 file types. It then downloads a text file with a ransom demand of one Bitcoin and with instructions of how to pay. The attacker offers to decrypt one file from the rest for free and gives a pretense that they have a help desk to answer the victim's questions.

Crysis first discovered in 2016 by ESET Security firm, is a copycat of Locky which shadow copies every file including system files .It alleviates the Privilege to admin level thus stealing users login and other credentials. Its main targets are VMWare virtual machines. It uses Remote Desktop Protocol brute force attacks. It not only targets the businesses but reports have shown that it has targeted the Healthcare Service providers too.

Zcrypt follows the unusual method of spreading like a virus infection. It doesn't rely on spam emails and can use USB stick to spread. It creates an *autorun.inf* file that allows it to execute automatically encrypting all important directories and files. It scrambles the file making the recovery impossible.

PowerWare –Powershell hijacker is a ransomware as it targets businesses using MS Word and Powershell scripting interface. After prompting the user to enable macros to a Word attachment it just enables Powershell to download a malicious code.

Petya attacks the system instead of files. It writes to the Master boot Record causing a full blue screen system crash. When the user reboots the system then he is presented with a danger symbol of skull and cross bones splash screen with a ransom demand and making the system inaccessible for the user.

Cerber is a Ransom as a Service application, not so much active in its country as it is Russian in origin. The system once infected with this application shows fake windows system alerts thus forces the user to reboot before it starts its encryption routine. It uses the method of dropping a text file with a ransom demand. A new variant of the Cerber has the ability to avoid encrypting security software.

RAA is a built-in JavaScript file and is delivered to the victim as a .js file that uses encryption of Crypt-JS. It deletes Windows shadow Copy Service and drops the password stealer to hunt for passwords in the system.

Erebus discovered in September 2016 was distributed through malicious advertisements designed to lure users to an exploit kit server that dropped the ransomware. Once the system is infected the application will drop a text file on the desktop titled ReadMe.html thus threatening the user to delete the encrypted files if the ransom is not paid. It deletes the Windows Volume shadow copy service to avoid recovery of the system.

Netflix with its fast growing consumer subscribers have become a platform for cybercriminal attack. This is typically found on cracked applications site in the form of an executable file Netflix Login Generator v1.1.exe that displays another window with login information paired with a fake password. It then installs the malware in the background. Using AES-256 it encrypts 39 file types and then demands a ransom of 0.18 Bitcoins or US $100.

VirLock was a unique ransomware that not only locks the computer screen but also infects the files. It targets specific files for infection like common documents, executables, archive, audio/video, image and certificate files. It adds an .rsrc extension to the infected files. It repackages these files into an executable file. User could execute the infected files or distribute it to other users. A report has shown that by typing 64 digit zeroes code the application assumes that $250 Bitcoins ransom has been paid.

Charger Android ransomware is a malicious app that carries a ransomware called charger. Once downloaded it carries a ransom demand which locks the mobile device and encrypts the files.

Havoc is another ransomware which attaches *.havocrypt* extension to the infected files. It uses symmetric and asymmetric cryptography to encrypt its files. It demand a ransom of $150 with a 48 hour deadline. If the victim fails to do the payment or deletes the application then the decryption key will not be provided online.

Crypto1coinBlocker is an updated version of earlier ransomware Xorist. Using RSA-2048 cryptography it affects the system files and adds random alpha-numeric numbers which act as the victims Bitcoin wallet address as the filename of the encrypted file. After this, it displays a fake error message informing about compromised data alerting the victim to pay a hefty amount of 5 Bitcoins or US $5000.On clicking OK it asks the user to pay a ransom of $1000.

SerbRansom discovered in the year 2017 threatens its victims by claiming that it will delete a random file every five minutes if the ransom $500 is not paid. It uses simple encryption methods and targets file with extensions .doc,.docx,.ppt, .xls, .pdf, .jpg, .gif, .png files.

LataRebo Locker prevents its victims from using their system by showing a large image splash screen with a ransom note. It corrupts the windows registry entries thus enabling its activation whenever the system reboots. It also disables the task manager preventing the user from terminating processes. Once the correct key ("Rebatsa") is entered, victims are able to access their system. But the program does not terminate itself and remains in the system.

The above mentioned are the ransomware variants discovered since then.[**see Figure 1**]

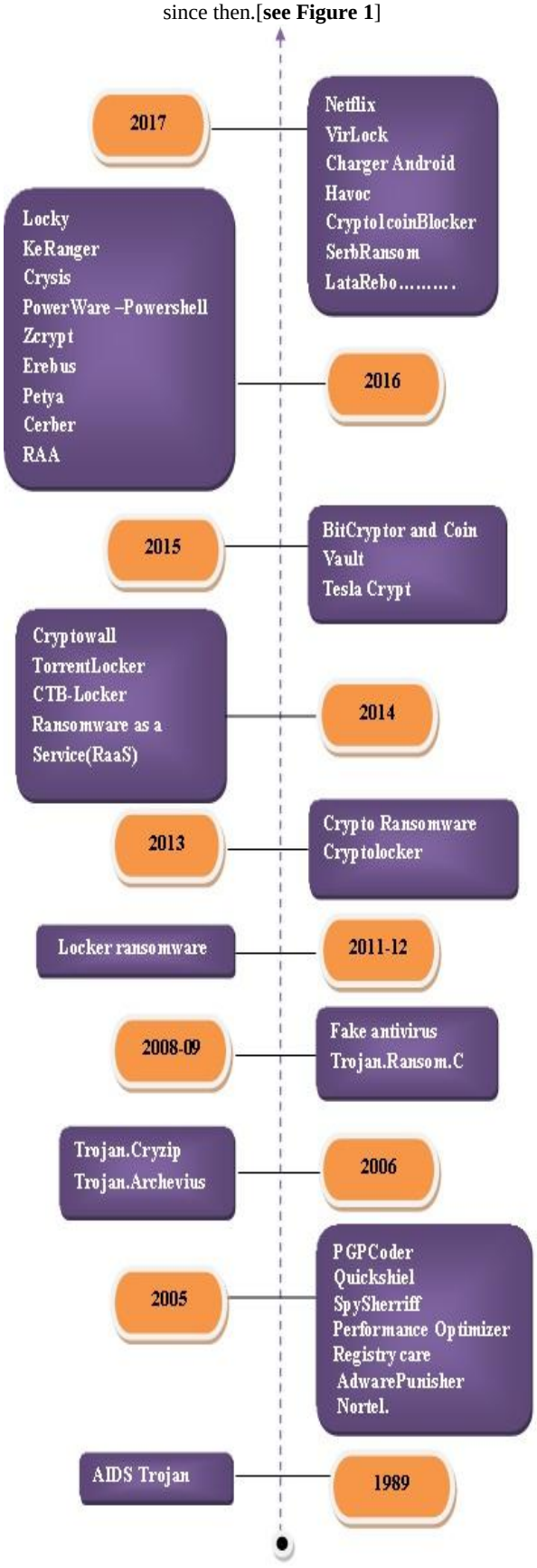

Figure 1. Evolution of different variants of Ransomware

5. ATTACK VECTORS

5.1 Home users

They are the specific targets for the ransomwares as majority of users have little knowledge about these kinds of applications. They lack the online safety awareness which makes them prone to the attackers. They don't keep their software's up-to-date and often believe in luck to keep them safe online. The financial accounts, social media sites or email accounts are popular targets and easy to monetize. The severity of the damage depends upon the kind of data that can get stolen.

They are the primary targets as they contain valuable files like document, personal photos, projects and any loss to these files make them vulnerable to accept the ransom amount and under peer pressure they are forced to pay the amount. They also lack any technical assistance which makes them prone to these kinds of threats. Even if they take backups the crypto ransomwares can delete local backups too thus making recovery impossible.

5.2 Businesses

Information and technology is the life and blood of many businesses. Many critical data of daily transaction are stored in these systems. Imagine one day of work without the IT systems functioning would create havoc in the organization. These critical data are in the form of business proposals, plans, reports, source code etc. Crypto Ransomware variants can not only lock the data stored in the computers but also access the external hard drives and other removable disks and encrypt the files there.

Ransomware affects not only computers but also cloud based file sharing services. Many employees are vulnerable to social engineering tactics due to lack of awareness. Businesses wouldn't even report of such attacks due to fear of legal or reputation related outcomes.

5.3 Public institutions

Public institutions such as government agencies manage huge databases of personal and confidential information which become the target for these cybercriminals. Lack of proper cyber defenses, outdated software's and infrastructure just create security holes for exploit attacks. According to latest report UK business are effected by a bluff ransomware attacks and are paying an average of £13,412.29.Over half of large UK businesses shared that information with police and Cyber Security organizations such as National Cyber security centre.

Here are some recommendations on how to minimize the losses by avoiding infection:

1. Regularly backup your data and recovery plan for all of your critical information. Perform and test regular backups to minimize system losses. Network connection backups can also be affected by ransomware so they should be isolated from the network. Use an external hard drive for your backups. Unplug the drive after its finished copying files.
2. Application white listing means listing specified programs and blocking unknown programs from use. Allow specified programs to run and block all other programs, if it is considered suspicious.
3. Keep your software and antivirus up-to-date as vulnerable application programs and operating systems are the targets for attacks. This reduces the number of exploit attacks. Use latest patches for installation in the devices.
4. Give least privilege to the user to install and run software applications.
5. Avoid enabling across from email attachments, thus enterprises or organizations should block email messages with attachments from unknown sources.
6. Do not follow unsolicited email links.
7. If infected by ransomware then do not pay the ransom because even if the ransom were paid there is no surety to regain access of your data. It can also increase the likelihood of more extortion attempts.
8. Remove the infected system from the network.
9. Ransomware has the ability to attack local files first, so it's better to create a sacrificial network share which can slow down the system by diverting its attention to large number of random files to cipher.
10. Regularly track for filename with unknown extensions.
11. Keep a track of unusually large documents from email downloads.
12. Over the years companies like Emsisoft, Symantec and Malwarebytes are making anti-ransomware softwares and have a repository of different types of ransomware protection software to decrypt files which are cipher encrypted. It's better to use these in case of infections.

6. CONCLUSION

In this paper, I performed a study about the different types of Ransomware families as we focused on their evolution and characteristics. Result of this analysis shows that a large number of Ransomware families exhibit similar characteristics. Section 3 deals with how ransomware affects their registry entries, Files and even the network. We have seen that particular set of Registry keys are modified and in case of proper monitoring of Registry sets and file system activities can provide protection against these Ransomware. Ransomware attacks happen through malicious advertisements, spam emails, drive by downloads caused by visiting the websites which are rigged with these exploit links. They also spread through botnets. A detailed study of Android manifest files with services mentioned in the paper can provide the information whether the Android phone is infected or not. With the increasing number of ransomware variants as you can find through the above article it's better to be prepared and be aware that simple antivirus programs can not suffice the user from being the victims of these exploit attacks. I have studied through a large number of android and windows platform attacks to draw the conclusion that these kind of attacks are not only going to infect the iPhone, Android and Windows platforms but are posing a major threat to Linux and MacOS systems.

Vulnerability testing and security loopholes have to be identified and people have to be aware of these kinds of exploit mechanisms. The rise in the number of attacks has made this one of the greatest threats in the coming years. It's better to be aware and be prepared. The study reveals that attacks happen in program repositories too so it's better to be careful while downloading large files from these repositories. The analysis of files using a sandbox from these repositories and iPhone data for ransomware infection will be the future research work.

7. REFERENCES

[1] Common types of ransomware accessible at http://www.vinransomware.com/types-of-ransomware

[2] Ransomware attackers are going old school with social engineering accessible at www.continuum.cisco.com

[3] Influences on ransomwares evolution and predictions for the future challenges by Ezhil Kalaimannan, Sharon K. John, Theresa DuBose and Anthony Pinto

[4] The evolution of ransomware by Kevin Savage, Peter Coogan, Hon Lau accessible at www.symantec.com

[5] Types of Ransomware accessible at http://mobile.esucurityplanet.com/malware/types-of-ransomware

[6] Ransomware Recap :January 14-29 2017 accessible at www.trendmicro.com

[7] Ransomware Recap :January 30-February 15, 2017 accessible at www.trendmicro.com

[8] Ransomware and recent variants accessible at www.us-cert.gov.in

[9] Ransomware Dos and don'ts: Protecting Critical data accessible at www.symantec.com

[10] Bluff Ransomware attacks Bamboozle British Businesses accessible at www.citrix.com

[11] 5 Methods for detecting Ransomware activity at www.netfort.com/blog/methods-for-detecting-ransomware-activity

[12] https://www.virustotal.com

[13] https://avcaesar.malware.lu

[14] http://contagiodump.blogspot.in/2010/11/links-and-resources-for-malware-samples.html

[15] https://www.hybrid-analysis.com