# Ransomware - Exploring the Electronic form of Extortion

**Samir Thakkar**[1]
[1]Department of Computer Applications
[1]The MS University of Baroda, Vadodara, India.

*Abstract*— Using Internet has become a routine in our day to day life. Availability of Internet on mobile devices has made our life hassle free. From routine activities like paying utility bills to critical activities like banking transactions are all trouble-free and quick to perform now. As more and more people have started using Internet, the number of cyber crimes and cyber attacks has also increased. Attackers are using innovative techniques to target internet users and gain direct or indirect benefit on successful attack. One emerging form of attack which is gaining attention is Ransomware, where attacker gets exclusive access on victim's computer and/or files by installing malicious code and demands to pay money to regain access to computer/files. It is a malware available in various forms and distributed over Internet computers using varieties of infection mechanism. It is the most destructive malware as damage caused by it is mostly severe and unrecoverable. This paper describes various infection mechanisms used by attackers to commit Ransomware attack. The monetization of ransom is also discussed. It is next to impossible to find a safe way out, once we are victim of Ransomware attack. The best strategy is to take preventive measures so that we do not become a victim. This paper also suggests guidelines for safeguarding against such attacks.

***Key words:*** Ransomware, Electronic Extortion, Cyber Threat, Cybercrime, Cyber attack

## I. INTRODUCTION

The Internet provides greater flexibility to its users, especially with the wide spread of high speed broadband connections. By the end of 2014, there will be almost 3 billion Internet users around the world, which is 40% of the world population. It is expected that 44% of the world's households will have Internet access at the end of this year, which is an increase of 3% compared to the year 2013. The mobile broadband subscription has reached to 2.3 billion globally showing growth rate of 20% compared to number of subscriptions in 2013 [1].

The Internet is facilitating business organizations to carry out business activities with great ease and this phenomenon has led organizations to store its critical business information on systems which are always connected to the Internet. Individual users of personal computers are not exceptions. Availability of high speed Internet on mobile devices encourages individuals to keep its private information on mobile devices which might not be having adequate security.

The wide spread Internet is a playground for cyber criminals to conduct their criminal activities by attacking on computer resources in one or another way. A threat report by Symantec Corporation noted that the total number of security breaches in the year 2013 was 62 percent greater than its previous year 2012 with 253 total security breaches [2]. This figure is expected to grow by the end of 2014.

Ransomware is one of the emerging cyber threats which is gaining attention recently. It is a malware that fraudster attempt to install on your computer and uses various lock-out mechanisms to prevent you access to the computer data. It then forces you to pay money to restore functionality of your system. Sometimes the lock out message is displayed to be from local law authorities stating that you have committed a crime like child pornography or unauthorized access to copyrighted information and forces you to pay fine or else you are threatened for imprisonment. Many of the novice users pay in fear of losing valuable information. But it rarely happens that attacker restore functionality of the system.

The attacker locks out information on system in various ways. One of the most common ways is to encrypt all information available on the system using strong encryption algorithms (with larger encryption key) which user can potentially never decrypt. A large number of online criminal gangs using their own ways to plan Ransomware attack and extort money from victims. The extortion amount may vary from few USD to 500 USD or may be more depending on the severity of attack.

It is found to be profitable activity for attackers. Symantec expert studied a specific attack in more detail for a month and found that 2.9 percent of the compromised users paid ransom, permitting the criminals to potentially earn $33, 600 on a single day. It means criminals could have made $394,000 in a month [3]. Thus the number of Ransomware attacks had increased considerably. Ransomware attacks grew by 500 percent in 2013 and turned vicious, a security report said [2]. A recent report by Symantec Corporation stated that overall Ransomware activity remained low since March of this year; however crypto-style Ransomware has been on the rise this year, making up 38% Ransomware activity in September 2014 [4]. Though the Ransomware attacks found to be declining this year, its serious damage cannot be neglected.

## II. KNOWN VARIANTS

This malware uses varieties of innovative ways to infect Internet users. Though security organizations are continuously developing security standards and implementations, the attackers move their feet in the direction of finding a new way out to breach system security. It exhibits a never ending race condition between security organizations and cyber intruders. Some of the known families of Ransomware are explored in this section.

### *A. Cryptolocker:*

Cryptolocker family infects user computers through spear phishing, watering hole attacks and drive-by downloads. Once infected, all the files on user computer start encrypted without users' knowledge. Once all files are encrypted a message is popped up explaining the potential damage and ransom is demanded for the exchange of decryption key.

 


Fig. 1: Cryptolocker Dialog Screen (Source: Invincea Ransomware Whitepaper, 2014)

User has threat of losing valuable information if he/she does not have any backup copies of it. The encryption usually involves much larger length decryption key which is virtually impossible to crack [5]. The ransom is demanded to be paid within certain time duration, usually from 72 to 90 hours in form of virtual currency which might be difficult to trace. The Gameover Zeus botnet which distributed CyptoLocker malware was shut down in the end of May 2014 following multi-national law enforcement by US [6].

*B. Cryptowall:*

The end of crypto locker malware had a bit relief, but the idea of earning handsome profit through encryption remained lucrative for cyber criminals. Cryptowall is a mimic of CyptoLocker malware, but found to be more destructive in the way it is spreading through various infection mechanisms. The malware uses infection vectors like browser exploit kits, drive-by downloads, sharing malicious links and malicious email attachments. The malware is also spread by sending malicious download link through Cutwail spam botnet. Dell SecureWorks Counter Threat Unit (CTU) has analyzed a family of CyptoWall ransomware from February 2014. They found that activity of the threat had marked growth in the mid of May 2014.

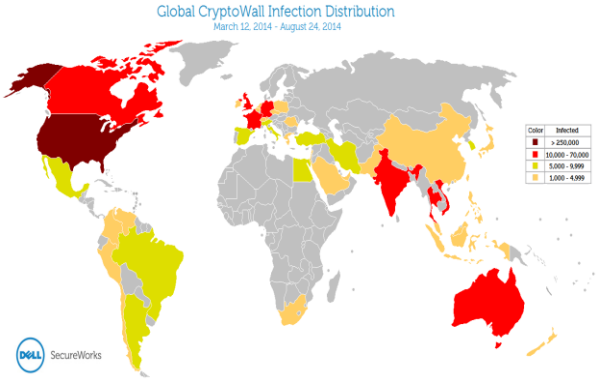


Fig. 2: Global distribution of CryptoWall infections between March 12 (approximate) and August 24, 2014. (Source: Dell SecureWorks)

The above figure shows geographical distribution of infected systems. CTU researcher observed 40.6% infected systems in United States only, due to CryptoWall's frequent distribution through Cutwail spam targeting Englsih-speaking users [7].

*C. Police Ransomware:*

In addition to traditional infection mechanism this malware uses innovative technique of spreading itself through web advertisements being displayed on legitimate websites. Most of the websites uses advertisements as one of the profit earning tools. While visiting such website if user clicks on an advertisement, the URL leads to a website containing exploit kit and the kit gets installed on user system. This variant of the ransomware disallows execution of programs and disables the system. It then shows a message which appears to be from a legitimate local law authorities stating that you have violated copyright law or viewing prohibited pornographic contents which is a cyber criminal activity and makes you liable to pay fine. You are threatened to be arrested if fine is not paid. As this malware is largely distributed through pornographic websites, the individual might be browsing such site and thus giving more weight to the message. The message might be embarrassing to the victim and encourages to get rid of the problem at any cost [3].

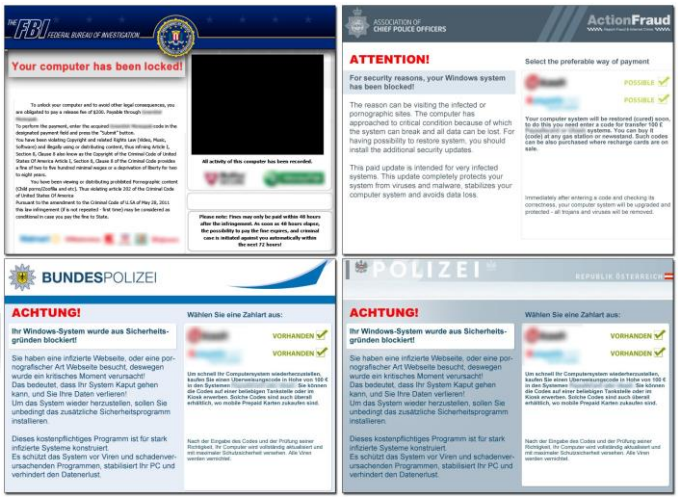


Fig. 3. Location-specific images for USA, UK, Germany, and Austria (Clockwise from top left, Source: Symantec Security Response - Ransomware: A Growing Menace, 2012)

SMS, MBR and RAR Compressed, Password Protected are few traditional variants of this malware [8].

*D. Sms Ransomware:*

It is an earliest variant that locks user computer and shows a message instructing the victim to send a code though a text message to a premium rate SMS number. User gets unlock code in form of a message. In this case, cost of the premium rate SMS is the ransom paid by the user.

*E. MBR Ransomware:*

This variant infects Master Boot Record of the file system and displays messages claiming that all user files are encrypted (which are in fact not encrypted). A ransom is demanded to decrypt the files.

*F. Rar Compressed, Password Protected Ransomware:*

This variant uses a different technique rather than encrypting user files. It compresses all user files into a

 

single password protected file removing from its original locations. A ransom is demanded from user to provide password to extract the files.

## III. MONETIZATION

The attackers make sure that they cannot be traced and that's why they chose payment method of ransom wisely. The threat message on victim's computer flashes a link which direct victim to proceed towards payment of ransom. No exact pattern is found to determine the ransom amount but recent figures vary from $200 to $2000. Different variants use numerous payment methods such as use of pre-paid cards like PaySafeCard, UCash, MoneyPak or cashU. The recent trend is to use accept payment using Bitcoin virtual currency which may be very difficult to trace.

These virtual currencies can be exchanged to buy goods and services online. The main problem with such payment vouchers is that there is no record kept if the voucher moves from one hand to another hand. A transaction is recorded only when voucher is spent, which is obviously an activity not done by an attacker. The attacker sell voucher and it keeps changing hands until it is sold to an end customer. Another market for exchange of these vouchers is underground sites which act as black market of exchanging virtual currencies. These markets accept virtual currencies from cyber criminals at 40 to 50 percent of its value and resell them as discounted voucher to end users at 90% of its nominal value. Though an attacker loses considerable percentage of ransom earned but still left with a quite handsome amount. The transactions performed in such markets are usually untraceable [9].

In a recent analysis of CTU researchers of Dell SecureWorks from the observation of known Cryptowall payment servers states that total 939 bitcoins were paid as ransom from March 2014 to August 2014. At the BTC exchange rate as of August 2014 (1 BTC = $520), threat attackers have earned more than $488,000 as ransoms [7].

## IV. MOBILE DEVICES – A NEW TARGET

It is expected that number of mobile subscriptions will reach to 6,915 million till the end of 2014 worldwide. Mobile broadband subscription is going to reach to penetration of 32% in 2014, compare to 26.7% in 2013 [1]. Tremendous hike in the usage of mobile devices and mobile Internet have attracted Ransomware players to target this devices. As soon as the mobile devices are increasing their capabilities with respect to Internet connectivity and processing power, cyber attacks on these devices are increasing too. According to Norton report, a global survey of end users showed that 38 percent of mobile users had already experienced mobile cybercrime. 52 percent of the mobile phone users are storing sensitive information on their mobile devices, putting their data on risk [2].

A cloud based Internet security solutions organization had noticed debut of Ransomware on Android. The first version of Ransomware appeared in May 2014, takes over phone on launching applications and states that you are watching child pornography and liable to pay fine to unlock the phone. A month later Cryptolocker version of Android appeared which encrypts files on SD card and demands ransom to decrypt them [10].

It is expected that the Ransomware threat for mobile devices is going to increase and become wide spread. It is likely that the malware may successfully pass itself to all the contacts available within phone address book or may use any other attack vector present in mobile device.

## V. MITIGATING STRATEGIES

The following preventive measures can be taken to protect from ransomware campaigns.

- Do not open spam mails or mails from unknown senders.
- Do not click on links within emails if you are not sure what it is about.
- Never download attachments within unknown emails.
- Use antivirus software and update it regularly.
- Backup your data on multiple devices regularly. We may increase backup frequency to ensure that the most recent data is protected.
- Disconnect Internet connection when not in use.
- Avoid clicking on greedy advertisements on websites.
- Be cautious as Government or low enforcement agencies never use electronic payment systems like MoneyPak, UCash or any such payment options to collect fine.
- Make sure that the web browser software is updated and never install any unknown plugins.
- Browse and download software only from trusted websites.
- If you experience a ransomware attack, report it immediately to local law enforcement agency.

Recently a patent for a security device has been filed which may help to get protection against ransomware attacks. The patent suggested a device that can be plugged into USB port of the system and can be activated by a button place on the device to remove ransomware malware from the system when under attack [11].

## VI. CONCLUSION

One of the major concerns is lack of awareness of such attacks among computer users. Upon police ransomware attacks it is most likely that a novice user pay ransom right away rather being exposed as a porn surfer.

Clearly, ransomware is emerging as a most efficient profit making technique for cyber attackers. Attackers are planning numerous ways to spread ransomware to as much systems as possible increasing potential earnings. Though number of attacks in the current year has decreased but they are likely to increase as technology evolves. A concrete solution to remove ransomware effect from the system is required to be devised.

## REFERENCES

[1] "ICT Statistics" *International Telecommunication Union*.http://www.itu.int/en/ITU-

 

D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls (accessed November 2014).
[2] Symantec Corporation. "Internet Security Threat Report." Annual Security Report, 2014.
[3] O'Gorman, Gavin, and Geoff McDonald. *Ransomware: A Growing Menace*. Symantech Security Response, Symantec Corporation, 2014.
[4] Symantec Corporation. "Symantec Intelligence Report." 2014.
[5] "Ransomware: Malware that kidnaps your data to extort money from you." *Whitepaper*. Invincea, Inc., Jun 2010.
[6] Office of Public Affairs. "Justice News." *The United States Department of Justice*. Jun 2014. http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware (accessed November 2014).
[7] Dell SecureWorks Counter Threat Unit™ Threat Intelligence. "CryptoWall Ransomware." *Dell SecureWorks*. http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/ (accessed October 2014).
[8] Ajjan, Anand. "Ransomware: Next Generation Fake Antivirus." *A SophosLabs technical paper*. Sophos Ltd., February 2013.
[9] Sancho, David. *Police Ransomware Update*. Research Paper, Trend Micro Incorporated, 2012.
[10] CYREN. "Internet Threats Trend Report." Second Quarterly Report, 2014.
[11] Denis, Bogdanov. Method for Neutralizing PC Blocking Malware Using Seperate Device for an Antimalware Procedure Activated By User. United States Patent US2014/0325654 A1. October 2014.

 