Conquering the Threat of Ransomware

Bhagyashree Gawade
University of Central Florida
Department of Computer Science
bhagyashree94@knights.ucf.edu

Jidnyesh Sankhe
University of Central Florida
Department of Computer Science
jsankhe@knights.ucf.edu

***Abstract*— Ransomware has become a threat to most of the Internet users that directly or indirectly encrypts the users data or even locks the access to the browser by holding a decryption key until a ransom is paid by the user. It is the most widespread and devastating hazards that users and other software developers face while using the Web. This may come as a surprise to many of us to know that ransomware prototypes were build in the mid-1990s. [1] Worse still, it is very common to hear about locking of any data and demanding of ransom. Internet Security Threat Report (2016) by Semantic shows 35% grouwth in crypto-style ransomwares during the year 2015 and thus it has classified ransomware as An extremely profitable type of atack. [3] A major chunk of these ransomware attacks are aimed to cause a threat to the users computer by not allowing the user to access the data and also making the user completely vulnerable. This is how it has also turned out to be an effective way of making money from the victims of this threat. Recently, there are two main forms of ransomwares that are most powerful. One is Locker ransomware (Browser locker) that denies access to the device by locking it completely. And the other is Crypto Ransomware (Data locker) that denies access to the files and data stored in the computer. This work is an effort to go into details of the types of Ransomware and their stages by implementing the two most effective ransomware techniques which are Crypto Ransomware, a data locker, and a Browser locking ransomware, Browlock and also implementing techniques to get rid of these ransomware Trojans.**

I. INTRODUCTION

Ransomware as the name suggests is a technique of extorting money from victims for a Ransom to make money. It is a category of malware that can be covertly installed on a computer without letting the user know about it. It can be clearly defined as a malicious software which, when run, disables the funtionallity of a computer in a way that the victim cannot click anywhere else. The ransomware program displays a message demanding for ransom or victims data. The different types of ransomware use files encrypt the entire file system of the computer and refrains the user from accessing the device by using files or browser websites or even emails to trigger the malware.

Many recent surveys say that users come across The Critical alert from microsoft every 10-30 minutes while browsing over the internet. this is usually triggered when the user randomly clicks on any button on a website or link. The figure below shows the alert that pops up. (Fig 1). This malware once executed will be tough to counter. These attackers deploy ransomware for money or other crucial details of the victim. These details include the victims passwords, bank details, credit card details, photos, etc.

One of the example of such ransomware is Maryland Hospital Ransomware attack which took place recently in March 2016. This ransomware, Samsam inflected major information of hospitals database records compelling the hospital to stop external network connection. [2] All these ransomware attacks are implemented using techniques that are well-planed, phases that are effectively monitored and sequentially executed. So, to render a ransomware attack completely unsuccessful, the client must be able to know and block all of the stages involved and thus this gives the victim a chance to mitigate the occurrence of an attack and solving the attack once caused. Hence, in this paper, we have tried exploring the ways to implement Device Locking and Browser Locking to conveniently comprehend how the malware is spread. We have also executed ways to decrypt the encrypted data and solve the browser locking issue like the Critical alert from Microsoft and discuss the possibilities of recovering the data without paying any ransom.

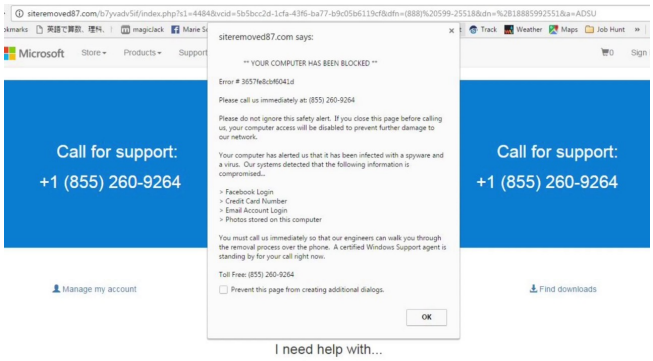

Fig. 1. Critical Alert from Microsoft!

II. OUR CONTRIBUTIONS

In this project, we make the following contribution:

1. Implement an existing technique of Ransomware attack to understand its working:

We start this project, by first implementing two most common types of encrypting Ransomware i.e. Browser lock and Desktop lock attack. The implementation was carried out for educational purpose and we tried to understand how a encryption techniques can be used to create havoc in the life of Internet users. The implementation made us realize how convenient it is to use a existing technique and misuse it. It

also gave us an insight on how to chalk out the prevention techniques based on the working of these attacks.

2. Perform an analysis of encrypting ransomware and its phases:

We read and browsed through various papers and statistics related to Ransomware attacks to get a good statistical understand about how big a threat it poses to Internet users and how mitigating the threat has been tough for various anti virus softwares due to its wide variety and easy deployment. We have also represented the data collected related to attacks with the help of various pie charts and graphs to demonstrate the threat visually.

3. Identify the prevention techniques so as to render the attacks useless:

Implementation of the attacks and reading various related work helped us to chalk out some of the prevention techniques to mitigate the increasing threat of ransomware attacks. We have also tried to compile various guidelines issued by the authorities like the F.B.I. and various anti-virus software companies by using their documentation as reference.

III. Background of Ransomware Attacks

The evolution of Ransomware has an influence from It sector, technology, security and economics. The overall ransomware infection began to climb in the fourth quarter of 2015 and again in first quarter of 2016. [4] The ransomware attacks now use the advanced professional techniques to enhance its effect in all the sectors. The average ransom demands have now reached a rate of $700 from $300. The fig 2 represents overall Ransomware infections in the years 2015 and 2016.

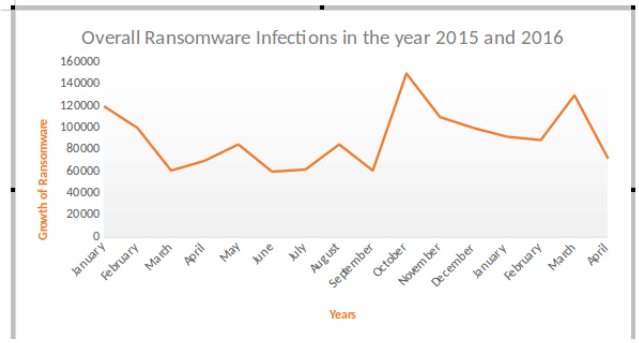

Fig. 2. Overall Ransomware infection between the years 2015 nd 2016.

In Fig 3, we have graphically represented an analysis of the percentage of new categories of deceptive Applications, Locker Ransomware, Fake AVs and Crypto Ransomware acknowledged between the years of 2015 and 2016.

A. Who are the victims of the Ransomware threat?

In Fig 4, we have created a pie chart to make an analysis of victims of ransomware. The figure shows which groups are affected by this threat more often. Consumers are most likely the most vulnerable and easy targets. 56% [4] of all infections between the years of 2015 and 2016 is accounted

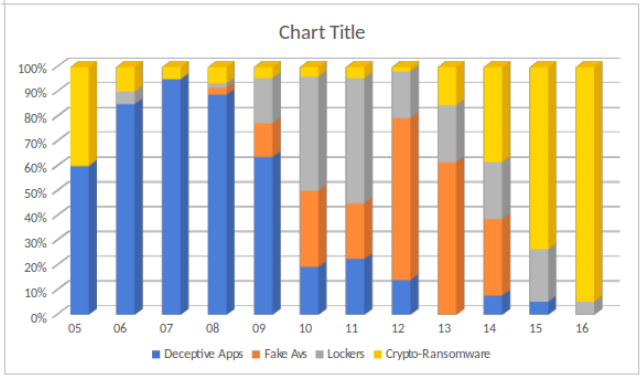

Fig. 3. Analysis of the percentage of new categories of Deceptive Applications, Locker Ransomware, Fake AVs and Crypto Ransomware

by consumers. The other popular group is organizations. The organization contributed almost 44% of the entire infection. Ransomware has slow but a steady effect on organizations. There was increase in the organization infection in the later quarter of 2015. Till then consumers were the most vulnerable group.

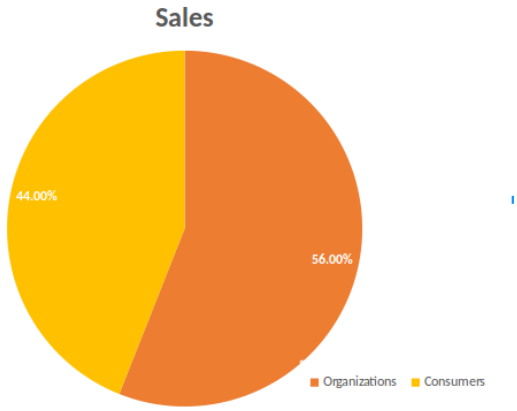

Fig. 4. Pie chart: Categorical distribution of the Victims of ransomware.

IV. Related Work

- In one of the surveys done, the authors present an early-warning detection named CryptoDrop whose function is to alert the user during suspicious file activity. Using a set of behavior indicators, CryptoDrop can halt a process that appears to be tampering with a large amount of the users data. The system can also be parameterized for rapid detection with low false positives, by combining a set of indicators common to ransomware. Their system manages to rapidly detect ransomware with low false positives. The experimental analysis of CryptoDrop stops ransomware from executing with a median loss of only 10 files (out of nearly 5,100 available files). Results show that careful analysis of ransomware behavior can produce an effective detection system that significantly mitigates the amount of victim data loss. [7]
- The ISTR Special Report has an extensive explanation starting from the inception of the CryptoRansomware

attacks to its growth and the factors contributing to the growth. It describes the rise of ransomware attacks and its families, how US continues to be the soft target for attack amongst all the other nations , the most likely organizations to be affected, ways of spreading the attack, various platforms like mobile or windows users, the major and the serious types of attacks like Cerber, CryptXXX and Locky, and it lastly discusses all the prevention techniques for protecting a users valuable data from the attack. This report helped us a lot to gain further insights into the world of Ransomware atttacks and its families along with the growth and trend of the threat. [4]

- Android being currently the most widely used mobile environment has encouraged malware writers to develop specific attacks targeting this platform with threats designed to covertly collect data or financially extort victims, the so-called ransomware. The authors use formal methods, in particular model checking, to automatically dissect ransomware samples. Starting from manual inspection of few samples, we define a set of rule in order to check whether the behaviours we find are representative of ransomware functionalities. [8]
- Understanding Ransomware and Strategies to Defeat It is a survey made to focus on the birth of ransomware and tries to explore through the phases of ransomware to understand the attacks in detail and develops unique strategies to counter the threat and invarialy defeat it in the long run by making it mpossible to affect the target computers. The strategies were very useful in developing a list of prevention activities in our report. [1]
- Hijacking Your Data, SophosLabs summarizes the entire timeline of Malware. It describes the early variants of Malware such as the SMS ransomware or the win-lockers who try to con the users as law enforcement authorities and try to threaten them of dire consequences if they dont pay up. It then moves on th describe the current methodology of attacks, which is using file encryption techniques to lock user data and to unlock them by giving a key to the user after they have paid for the key. It also discusses the need of a versatile anti virus software that covers the users from various different types of threats. [9]

V. Types of Ransomware Attacks

1. Data Locker (Crypto-Locker Ransomware):

- Crypto-Ransomware is a File encrypting attack that tries to screw victims by holding their files hostage. [7] This Ransomware type varies from other common malware attacks in a way that its consequences are irreversible until they are decrypted via cryptographic keys held by the attackers. Thus, the denies access to the data on the users device and asking the user to pay a fee for the data that is encrypted. Locked data will have very few capabilities like only letting the victim to communicate with the ransomware and pay the ransom. People store a lot of data on the computer as it is convenient to keep it safe and accessible. So, the lives of the people have become professional and digital at the same time. The victims unknowingly face this dilemma without having any prior knowledge of such attack on the data. Thus, there is no backup of the valuable information, details or photos making the user completely exposed to this attack. The user usually does not take the efforts to make a copy of all the data on the device and also setting a backup requires good discipline and it is not so feasible for the users.Compounding these problems, [7] an increasing rate of law enforcement agencies have been victims of this type of ransomware.
- Crypto-Locker aims at these weaknesses of the users and organizations. The inventors of Crypto-Locker have the knowledge of the data stored on the personal computers that is professionally important to the users and traditional clients. This ransomware gets installed and check for important data on the device for encrypting and then keep a key for that data. Later, the victim gets malwares message that tells the user about the encrypted data and asks for a ransom for the decryption key. Fig 5 represents the block diagram of the Data locker process. [5]

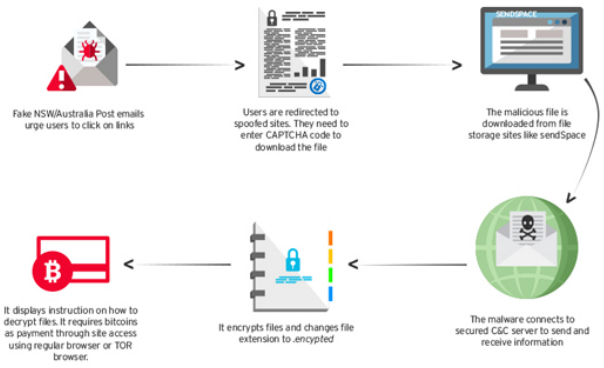

Fig. 5. The block Diagram of a Data-Locker

Fig 6 shows a demo of the demand screen of Data Locker ransomware. It depicts how the hacker asks for ransom in return of the data that is encrypted.

2. Browser Locker (Brow-Lock Ransomware)

- Brow-Lock has different functionality as compared to other Trojans. It does not use binary executable data and block access to any kind of information over the system. This attack has a functionality of infecting users browser when the user navigates to a server hosting Brow-Lock through their web browser. Brow-Lock uses complete client-side internet methodology.
- We have mentioned the Critical Alert from Microsoft in the introduction part with a figure showing the alert. (Fig 1). The users might get annoyed with this type of alert as it pops up every now and then when the users browse the internet. This Malware gets triggered when

Fig. 6. Demand Screen of Data-Locker

the user clicks a malicious link in 1. an email message 2. an instant message 3. on social networking site When the user clicks an email attachment or link on social networking site like Facebook, twitter, shopping sites like ShopHop.com, Shein.com, RoomWe.com, etc. or online movie sites that is malicious or contains virus, an alert window pops up. This is how the malware gets installed on the browser thus locking the browser. The user cannot click anywhere else when the window pops up. Hackers in this way cause harm to the victims browser irrespective of the web browser the victim is using to surf. Also, the ads that are generated depend on the victims search history and choice of websites.

- Browser Hackers and also Microsoft critical alert are widely observed as unwanted malwares that have the capability to lock the browser by distributing ads and fake AVs through the malware. [6] However, these viruses wont affect the data from the device. This malware causes the browser to slowdown and takes help of most of the computer resources to produce fake ads in enormous quantities.
- Fig 7 depicts the window of a system Virus Warning, [3] it can be referred to as a cross-platform ransomware as it will be executed on any other platform that will provide the web browser supporting JavaScript, HTML and CSS features on it. As shown in the fig 7, the window asks to either a call a anumber to know more about the threat, which is fraud number and will extract details about the users phone number and other details. It also shows the possible network damages from potential threats and the data exposed to risk like credit card details, e-mail passwords and other account information, Facebook, Skype, ATM and other chat logs and private photos in order to threaten the user.

VI. Experimental Setup and Implementation

1. Experimental Setup for Data-Locker

- Software: Visual Studio 2017

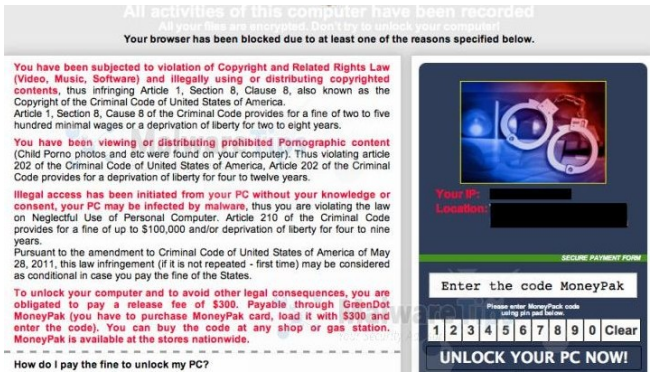

Fig. 7. Demand Screen of Brow-Locker

- Programming Language: VB.Net and C
- Operating System: Windows

2. Experimental Setup for Browser-Locker

- Programming Language: HTML, JavaScript and CSS
- Operating System: Windows and Linux

A. Implementation of Data-Locker Ransomware

Encrypting ransomware works by obfuscating the contents of user files, often through the use of strong encryption algorithms. Victims have little recourse other than paying the attacker to reverse this process. Some attackers even enforce strict deadlines and host elaborate customer service sites to encourage victims to pay.[7] We tried to implement a similar CryptoLocker using Secure Hashing algorithm(SHA-512). The SHA-512 algorithm belongs to the SHA-2 family of algorithms. The algorithm has a maximum message digest of 512 bits. The windows desktop application is built in Visual Studios and the language used is vb.net. The encryption algorithm used is SHA-512 which belong to the SHA-2 family and it encrypts the data of the specified folder path and encrypts all the files in the folder by computing their hash functions and converting their file types into .anon files. The files require a key to start decryption and is given to the user only when they have paid a ransom to the hacker.

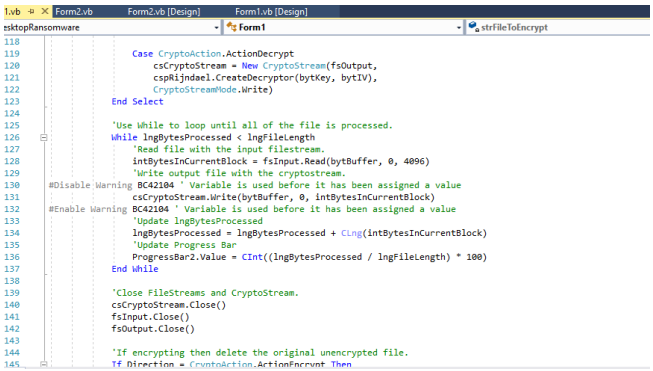

Fig. 8. Snippet for implementation of Data-Locker using Visual Studio

B. Implementation of Brow-Lock Ransomware

Brow-Lock is created using client-side web technology. We have created a fake website using JavaScript, HTML

and CSS. The website is a online Movie Hub which contains links to other Youtube channels and also asks for a ”Login”. This ”Login” Button trigers the malware by poping up a ”Microsoft alert window”. This alert window asking for ransom contains HTML code and JavaScript for the alert message. The page contains JaaScript code that defines the two functions: alertpopup() and confirmpopup(). The Ransomware is redirected to a malicious server, through an ad or buttons on a website, the server will fingerprint the victim's running windows, It will also send the ransomware designed for the Windows system. In case of victims using Linux, Mac OS X, it sends Brow-Lock. Fig 9 shows a snippet of the source code from Brow-Lock showing the Website design and the ”Microsoft Alert Window”.

```
</head>
<script language="javascript" type="text/javascript">
var bflat = new audio();
bflat.src = "micro.mp3";
document.getElementById(bflat);
function alertpopup()
                {
                alert("Critical Alert from Microsoft \n\n There is a .net frame work file missing due to some harmfull virus\n\n
Please contact microsoft technicians to rectify the issue.\n Please do not open Google Crome for your security issue. to avoid data
corruption on your registery of your operating system.Please contact microsoft tecnician at\n\n Tollfree Helpline at 1-844-522-7825\n
\n YOUR COMPUTER HAS BEEN BLOCKED AND ALERTED US THAT IT HAS BEEN IFECTED WITH A VIRUS OR SPYWARE. THE FOLLOWING INFORMATION HAS BEEN
STOLEN \n>Facebook login\n\n . Credit Crad Details \n >Email account Login\N >Photos stored on this computer\n\n .PLEASE DO NOT SHUT
DOWN OR RESARTT YOUR COMPUTER. DOING THAT WAY MAY LEAD TO DATA LOSS AND FAILURE OF OPERATING SYSYTEM, HENCE NON BOOTABLE SITUATION
RESULTING COMPLETE DATA LOSS. CONTACT DMINISTRATION DEPARTMENT TO RESOLVE THE ISSUE ON TOLL FREE- 1-844-522-782");

            bflat.Play();
            }
function confirmpopup()
                {
                var c=confirm("Do you wish to continue")
                if(c==true)
                alert("You pressed ok button")
                else
                alert("You pressed CANCEL button")
                }
</script>

<body bgcolor=#737373 text=#FFFFFF background="/home/jidnyeshps/Documents/malware/new/movies.jpg">
<div class="topnav">
  <a class="active" href="#home">Trailers</a>
  <a href="#news">Movies</a>
  <a href="#contact">Songs</a>
  <a href="#about">About</a>
</div>

<div style="padding-left:16px">

</div>
<center>
<img src="/home/jidnyeshps/Documents/malware/new/movlebackround.jpg">
<b><h1 style="color:white;" style="font-family:courier;" style="font-size:400%;"> Watch Movies Online</b></h1>
<strong><p style="color:red;" style="font-family:courier;" style="font-size:300%;">Welcome to the online Movie Hub</p></strong>
<a href="http://www.comingsoon.net/trailers">Click Here to watch the movie trailers online.</a>
</center>

<center>
                <form>
                    <p style="color=gold;" style="font-family:courier;" style="font-size:200%;">Login to Watch Movies Online</
p>

                    <audio id="bflat"> </audio>

                    <input type="button" value="Login" onclick="alertpopup()">
                    <input type="button" value="confirm" onclick="confirmpopup()">
```

Fig. 9. Source code from Brow-Lock showing the Website design and the ”Microsoft Alert Window”

VII. Results

- Results after implementing Data-Locker Ransomware

1. The target folder contains files to be encrypted by the Data-Locker Ransomware. We have attached a folder named ”Happy” which contains a list of Text files. Although the Data-Locker can encrypt any types and extensions of files. Fig. 10 shows the files.

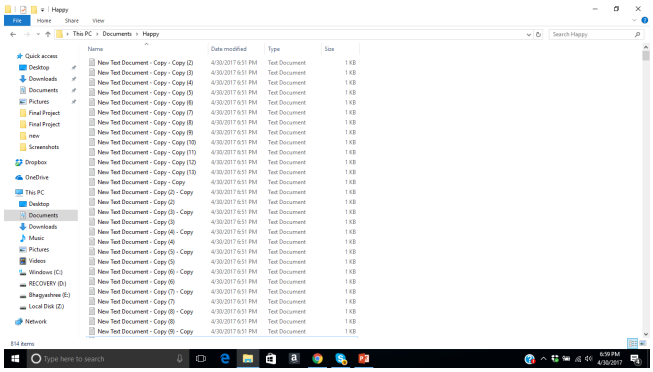

Fig. 10. Folder Containing all files to be encrypted

2. We have implemented a Windows Application using Visual Studio 2017 to encrypt the files from a computer. The Encryption is done using the algorithm SHA-512. Fig. 11 shows the files getting encrypted along with the list of encrypted files.

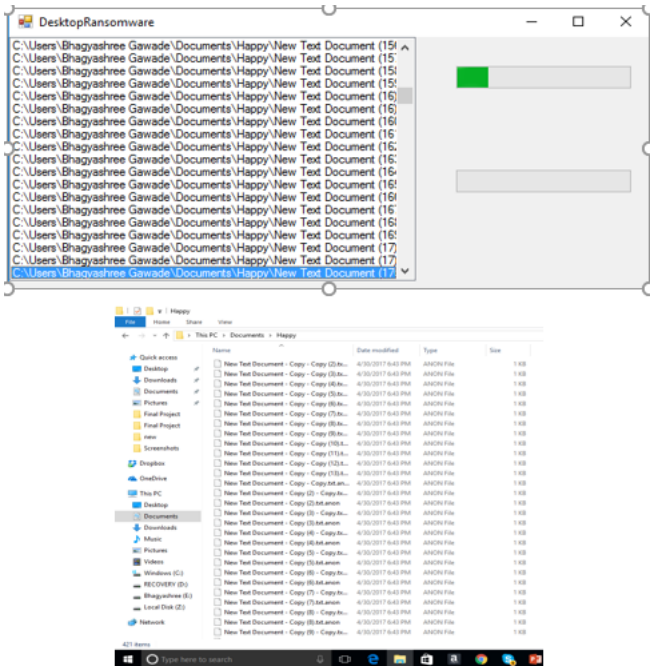

Fig. 11. Files getting Encrypted and the changes that took place in the ”Happy” folder”

3. When the victim tries to access his files, a Message box comes up stating that his files are locked and he has to pay a ransom to get the decryption key. Fig 12. shows the Message box.

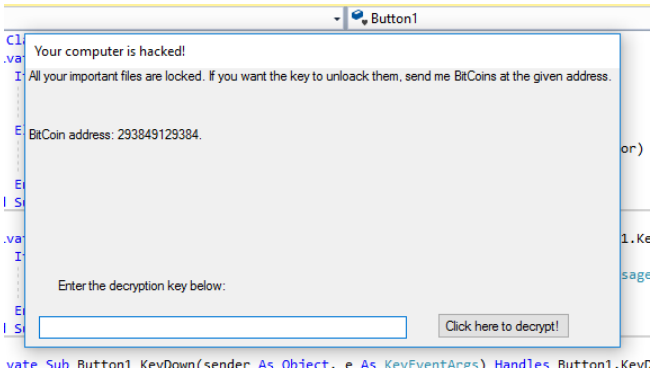

Fig. 12. ”Message box asking for decrytion key”

4. Various user attempts to get rid of the messsage box by either inputting a random encrytion key or using Windows shortcut keys of ALT+F4 to close the message box fail. Fig 13 and Fig 14. shows the attempts going fail.

5. Fig 15 shows that after giving up and paying a ransom to the hackers, the victim gets a decryption key (in our project, the decryption key is: Thanks for the money!) and he can

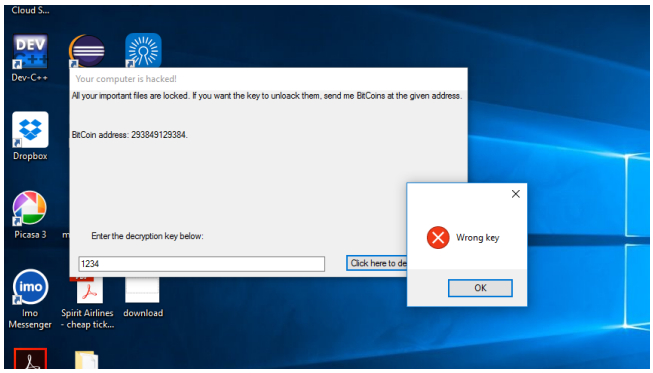

Fig. 13. "Victim trying to input a random decryption key"

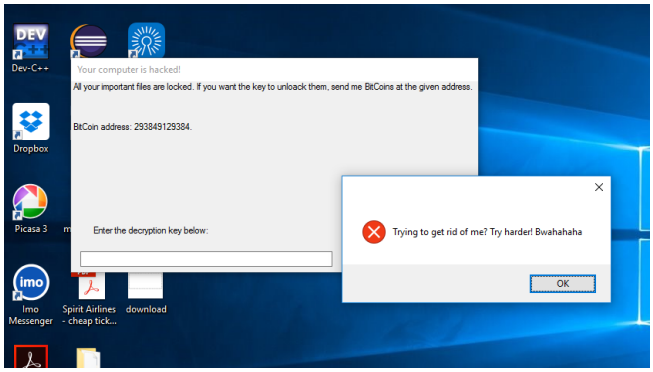

Fig. 14. "Victim trying to close the Message box."

now enter this key to decrypt his files. The fig 16. shows the decrypted file list.

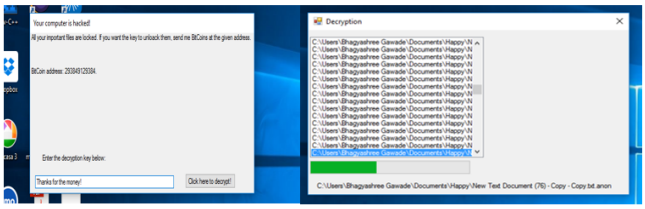

Fig. 15. "The correct decryption key is entered."

- Results after implementing Brow-Lock Ransomware.

1. Fig. 17 shows the Movie-Hub website created using Java-Script, HTML and CSS. This is a website that contains a YouTube link to the movie trailers and a link to another site. It asks to click on the Login button to watch movies online.

2. Fig. 18 shows the "The Critical Alert from Microsoft" alert window that pops up on clicking on "Login" button. Fig. 19 shows the dialogue box that pops up on clicking the "Confirm" button.

VIII. Profits Gained by Attackers from Ransomware Attacks

- ransomware has become a great help to professional criminals who wish to expand into distributon of ransomware. The ransom that is asked for the the decryption keys or System;s access ranges from $200 USD to $700 USD. Around 68,000 unique IP addresses were identified connecting the CC Server (Comand and Control Server) over a period of one month of activity, from Setember to October. [12]
- Cybercrooks have started retailing ransomware programs for mokaing money. Karmen Ransomware is being sold on Dark Web forums from Russian-peaking cyber-criminal DevBitox for $175.[13]
- Hackers are targeting healthcare institutions with ransomware malware due of their poor cyber-security posture, reliance on legacy IT systems, third-party services and the need to access information as soon as possible in order to deliver great patient care. [14]

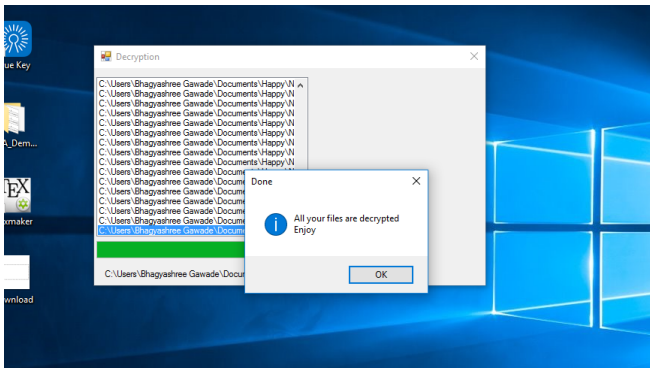

Fig. 16. "Decryption process starts and after completion the window pops up showing that decryption is complete."

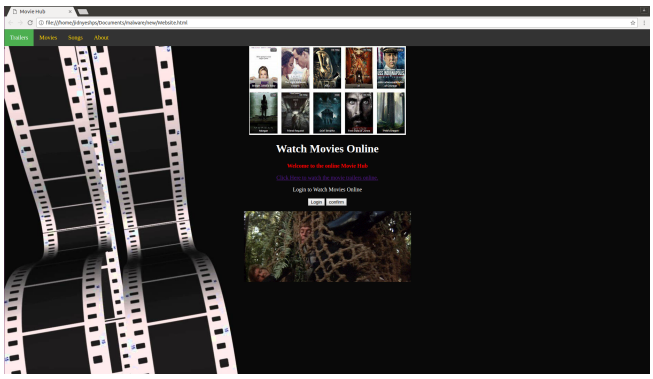

Fig. 17. "Website"

IX. Prevention Techniques

Some of the ways to protect your networks from Ransomware threat:

- Educate yourself Attackers often enter the organization by tricking a user to disclose a password or click on a virus-laden email attachment. Remind employees to never click unsolicited links or open unsolicited attachments in emails. To improve workforce awareness, the internal security team may test the training of an organizations workforce with simulated phishing email.
- 2. Proactive Prevention is the Best Defense Infections can be devastating to an individual or organization, and

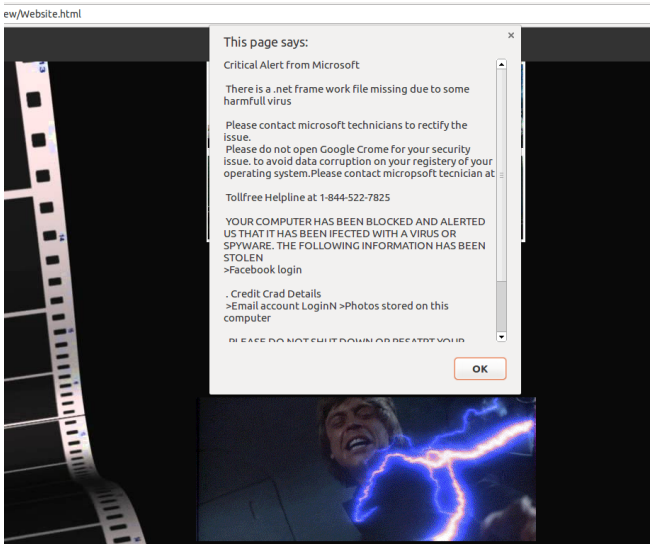

Fig. 18. ”Critical Alert from Microsoft! Alert window.”

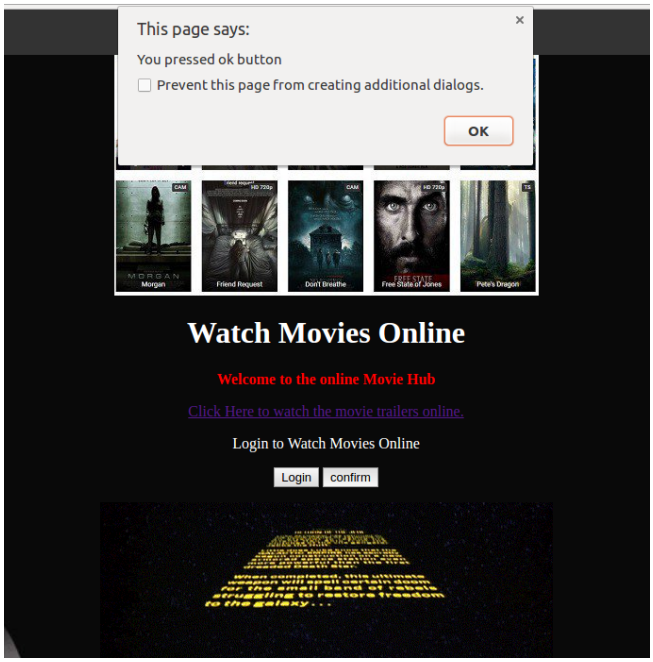

Fig. 19. ”Dialogue Box”

recovery may be a difficult process requiring the services of a reputable data recovery specialist. Preventive Measures:

- Implement an awareness and training program
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Disable macro scripts from office files transmitted via email
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application white-listing, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.

Business Continuity Considerations:

- Back up data regularly.
- Conduct an annual penetration test and vulnerability assessment.
- ecure your backups. Ensure backups are not connected permanently to the computers and networks they are backing up.[10]

A. *Steps to Remove the Ransomware*

Some ransomware viruses are relatively easy to remove, while others are hard. The browser lock ransomware which has been implemented in this project are commonly known as the Scareware browser attack and are the easiest one to remove. The can be easily removed by closing their task on the Task managers of the desktop computers. The harder ones encrypt either the Master File Table in Windows, or individual files, or the whole hard drive. We have also implemented one such ransomware which encrypts the target folder. The possible solution to such attack is running the recovery mode on the computer.

- Following steps can be imitated to try and remove the encryption.
  1. If your PC boots to the Windows login screen, hold the Shift key, click the power icon, and select Restart.
  2. It should reboot to the recovery screens.
  3. SelectTroubleshoot¿Advanced Options¿System Restore.

  The above technique might work on ransomware affecting the windows operating system. If System Restore doesnt help and you still cant get into Windows to remove the ransomware, try running a virus scanner from a bootable disc or USB drive. However, untangling and identifying more than a few files could be a huge task. However, if your ransomware encrypts each file with its own unique key, likeRokku, then you will probably not get your files back. This is why offline and possible off-site backups are essential for protecting valuable data. [11]

X. CONCLUSION

Ransomware continues to adversely affect unwary victims due to its use of encryption techniques. Affected users often have little alternative other than to pay the ransom,

fueling a vibrant economy for attackers who can employ new variants with ease. In this paper, we have first tried to list down all the different types of ransomware and how largely they have affected internet users along with its brief history. We have then implemented two commonly found Ransomware attacks to understand their working and analyze the preventive measure. We have decribed the current trend of Ransomware graphically to make an analysis. Based on our implementation and analysis, we tried to list down all the preventive measure one could exercise to ensure safe internet usage and data privacy. Through this project, we also aim to help researchers identify the countering measure of the ransomware attack once it has been instantiated and the users data is at risk. While attempting to recover a file which is locked due to the attack, a anti ransomware software should be able to recover them at minimal damage, this requires more research and the future scope of this study is finding a software that an help remove any type of ransomware with minimal damage to the files and data.

REFERENCES

[1] obert Leong, Director of Product Management, McAfee Labs, Contributors: Christiaan Beek, Cedric Cochin, Nicola Cowie, Craig Schmuga: Understanding Ransomware and Strategies to Defeat It.

[2] Justin David PinedaRodger Louis ArtetaAdrian Tobias and Shogo Roxy Serra, Examining the Ransomwares Anatomy: From Proliferation to Mitigation, School of Computing and Information Technologies (SoCIT)

[3] Kevin Savage, Peter Coogan, Hon Lau, The evolution of ransomware, veersion 1.0-August 6, 2015.

[4] Dick OBrien, Editor John-Paul Power, Assistant Editor Scott Wallace, Graphics Design, Ransomware and Businesses 2016, an ISTR Special Report.

[5] Trend Micro, CTB-Locker Ransomware Includes Freemium Feature, Extends Deadline, January 21, 2015.

[6] Maria K , Microsoft Critical Alert Pop-up Scam Removal, https://howtoremove.guide/microsoft-critical-alert-pop-up-scam-removal/

[7] Nolen Scaife, Henry Carter, Patrick Traynor,Kevin R.B. Butler, CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data, 2016 IEEE 36th International Conference on Distributed Computing Systems, 2016.

[8] Francesco Mercaldo ; Vittoria Nardone ; Antonella Santone, Ransomware Inside Out

[9] Richard Wang, Anand Ajjan, Ransomware: Hijacking Your Data, SophosLabs

[10] The guardian, How to protect your network from Ransomware, F.B.I

[11] How can I remove a bibitemc12ransomware infection?'.

[12] Geoff McDonald - Threat Analysis Engineer, Gavin OGorman - Sr Threat Intelligence Analyst, Ransomware: A Growing Menace.

[13] John Leyden, Profit with just one infection! Crook sells ransomware for $175.

[14] By Sead Fadilpai, betanews, https://betanews.com/2016/09/20/ransomware-lucrative-attacker-profit/