19054557MScFinalPRojectReport-1.docx

by Muhammad Abdul Latif

Submission date: 27-Aug-2021 04:57PM (UTC+0100)
Submission ID: 159259067
File name: 19054557MScFinalPRojectReport.docx (4.07M)
Word count: 9990
Character count: 55205

University of Hertfordshire
Department of Computer Science

MSc in Computer Science

7COM1039-0509-2020-Advanced Computer Science Masters Project

Date: 27 August 2021

PROJECT TITLE:

Prevention of ransomware attack: strengthening cyber security

Student Name: **Muhammad Abdul Latif**

Student ID: 19054557

Supervisor: **Justin Mifsud**

ABSTRUCT:

Ransomware is regarded as a global cyber pandemic that targets all types of institutions which is a significant threat of cybersecurity. It is one of the major cybercrimes accelerated recently focusing to earn illegal money through encrypting files and victimized people asking money to decrypt that unless they pay ransom to the hackers. Sometimes innocent users or companies pay ransom to gain access of their files and data, however ultimately, they fail to retrieve their files and data. Although Dr. Joseph Popp first developed ransomware in 1989, however, it has revolutionized the cyber world during last three decades as a means of earning illegal money. Paying ransom to retrieve data could not be a permanent solution, rather the best way to avoid losses is the preventive measures. This purpose of this project demonstrates the loop faults by which users can be attacked while using computer systems and how to protect themselves from these disastrous cyber-attacks. In this project, ransomware viruses have created for the research purpose and examined to different Windows and Linux based operating systems to identify the vulnerabilities for being attacked and what are the effective ways they could be secured by updating patches, defenders, and antiviruses. The findings of the study have confirmed that the prevention of ransomware is the key to avoid the individuals, small and enterprise companies, and organisations level in different countries from being continuously attacked by Ransomware. As the types and method of attacks through internet have been updating by the hacker communities the findings in this project can be used as a reference for future research to conduct further study especially for the strengthening cybersecurity.

ACKNOWLEDGEMENTS

The biggest gratefulness and thank is credited to Justin Mifsud, Lecturer at the University of Hertfordshire, and my supervisor of Advanced Computer Science Masters Project, who guided this project in the front end all the way from the topic selection, practical works, report writing to the presentation stage. He has guided me closely phase by phase in every week and has given feedback accordingly.

I also give appreciation to Helen who has taken classes supporting to the construction of this project from the back end. She demonstrated each in every aspect of a MSc project in detailed.

Table of Contents:

Table of Figures and Graphs

Lists of Abbreviations

IoT: Internet of Things

RaaS: Ransomware as a Service

M2M: Machine to Machine

OS: Operating System

IP: Internet Protocol

LAN: Local Area Network

VPN: Virtual Private Network

AES: Advanced Encryption System

RSA: Rivest–Shamir–Adleman

EAP: Extensible Access Protocol

PAP: Password Authentication Protocol

MSCHAP: Microsoft Challenge Handshake Authentication Protocol

WAP: Wireless Application Protocol

AIDS: Aids Info Desk

IT: Information Technology

Chapter-1

Introduction

Information security has become one of the main concerns of this latest world due to the rapid digitalization. Covid-19 pandemic has accelerated online activities globally from individual to the multi-national companies. While data communication and transformation of business operations shifted from manual to automated through connecting internet, cybercriminals took this opportunity to earn illegal money by creating dangerous viruses. They send malwares, access to other systems, encrypt their data and files to commit crimes and even ask ransom in return of that data. This trend is increasing day by day with the latest cybercrime version of ransomware attack in which the victim has nothing to do when being attacked. In some recent cases of ransomware attacks, the victim organizations have paid huge amounts to the attackers, which can be one of the reasons these attacks are getting more popular, instead, what organizations need to focus on is preparation and early mitigation if they want to cut losses to ransomware (Paul Webber, 2020). Ransomware continues to be a major threat to businesses in all sectors, with some areas getting hit particularly hard, especially education and healthcare. In 2020, 1,681 schools were affected in USA by ransomware as well as 560 healthcare facilities (Emsisoft, 2020). Today's cyber criminals are smarter than ever and it's likely that we are yet to see the most advanced attacks (Florian Malecki, 2019). With an estimated global cost of around $6tr (£4.24tr) per year attributed to cybercrime, there can be no denying that digital crime is just as lucrative for criminals as it is destructive to businesses (Morgan, 2017). In 2020, the total number of global ransomware reports increased by 485% year-over-year according to the latest Threat Landscape Report 2020 (Singh, 2021). To understand in depth, to prevent these kinds of attack and to strengthen cybersecurity it demands to do more research on it and need to be analysed in practical and critical point of view.

2. Aim of this Project:

The overall aim of this project is to develop a system that will help individuals, enterprise companies, private and public sector organisations deal with the effects of malware including ransomware. It will provide specific steps to help organisations prevent a malware infection, and actions to take if already infected. The outcome of this project also will reduce the likelihood of becoming infected the spread of ransomware and to strengthen the cybersecurity management system for any organisation in future.

3. Objectives of this project:

Due to the gradually increasing number of ransomware attack globally, the prevention become inevitable. This is a such continuation effort by this project. The overall objective is:

- to explore the main loop faults on internetwork through practical analysis and monitoring by which ransomware-attack is occurred and
- to identify possible preventive measures to strengthening the cyber security.

4. Project Methodology:

This Project has been accomplished into following three gradual phases:

4.1. Planning Stage:

- At first the title has been fixed up with the consultation of supervisor.
- The primary plan of this project has been sorted out after discussing with supervisor,
- Designed the detailed project plan with timeframe by Gantt Chart

From the finding supervisor to giving presentation a detailed plan has been made according to the Gantt Chart. Although this "MSc Project" has been scheduled only 12 weeks, however up to submission it may extend to 14 weeks. In this plan time was allocated more in Literature review and Background Research on the project for similar topic so that research gap can be found, and any new contribution could be made to prevent ransomware attack with the making new strategies through practical work to strengthening the cybersecurity system for an individual to a large enterprise company.

- The total project has been sliced into different parts to complete progressively.
- The experiment part has also been structured through Oracle Virtual Machine.
- Designed the whole plan gradually to carry out the Project report and presentation.

Project Plan (Gantt Chart)

ACTIVITY	WEEKS														PLAN START	PLAN DURATION	ACTUAL START	ACTUAL DURATION	PERCENT COMPLETE
	1	2	3	4	5	6	7	8	9	10	11	12	13	14					
Finding Supervisor															1	5	1	4	100%
Ideas for Project															1	6	1	6	100%
Finalize Project Title															2	4	2	5	100%
Finding Articles of Journals and Literature Review															4	8	4	6	70%
Design Block Diagram															4	3	4	6	25%
Design Gantt Chart															5	4	5	3	20%
Design Flow Chart															5	2	5	5	20%
Practical Analyzing															5	2	5	6	55%
Survey the Hacking Incidents															6	5	6	7	40%
Writing Draft Project															6	1	5	8	50%
Feedback from Supervisor															9	3	9	3	20%
Finalizing the Project Writing															9	6	9	7	25%
Extra Referencing															9	6	9	7	20%
Submission of the Project															9	3	9	1	0%
Preparing Presentation Slide																			0%
Presentation of the Project															9	4	8	5	0%

Figure-1: Detailed Project Plan with time frame

The main tasks need to be completed:

1. Finding the latest Articles from Journals or Books
2. Critically review the literatures

3. Finding the research Gaps
4. Practically Analyzing the Security holes through Kali Linux, Wireshark
5. Analyzing how to encrypt files during Ransomware attack?
6. Critically analyzing the statistics of Global Cyber Attack scenarios
7. Finding out the technical implications after attack
8. What are the measures can be taken to protect end user?
9. Recommendations for preventing Ransomware from NOC to Corporate Level.
10. Writing the Final Project after practical analysis
11. Conclusion
12. Citing proper references

4.2. Data Collection, Installation and Configuration Stage:

- Initial data collection done through reading the books
- Downloaded the latest 50 research articles on Ransomware and cybersecurity.
- Obtained relevant information, statistics, applications, and compilation.
- Downloaded 7 latest Operating Systems Software iso files for Virtual Environment.
- Downloaded and install Oracle Virtual Box.
- Installed 7 Operating Systems on Virtual Box from windows and Linux platform
- Configured of Some OS as non-secured and others with fully updated software and patches.
- Written codes in Microsoft Visual Studio Dot Net for Windows based Operating Systems
- Prepared Executable shell script in python to build ransomware virus for Linux based Operating Systems

4.3 Coding, Scripting and Testing Stage:

- Transferred those viruses through email attachments to the users to attack.
- Tested of the possible cyber-attack and vulnerability without Security features.
- Tested of the possible cyber-attack and vulnerability with updated security features.
- Analyzed of how Antivirus and other security features can protect a PC to be affected by the malwares and dangerous viruses like ransomware?
- Checked security attack on Kali Linux through Wireshark, Metasploit, Nessus, Dmitry
- Evaluating the live attack files and implementing possible solutions by enabling and disabling firewalls, defenders, and antiviruses.
- Configured of possible all shields to protect the PCs and Networks from external ransomware attacks.

4.4. Reporting Stage:

- Prepared draft report and submitted time to time to the Supervisor part by part for further suggestions and modifications.
- Added Harvard Referencing style citations from different books of the different writers
- Included some latest cyber security report statistics and graphs.
- Finalized the report for final submission.

Chapter-2

Background Research Analysis

2.1 Research Question:

What are the most effective strategies to prevent from being attacked by the ransomware?

2.2 Justification of this project

Being attacked in July 2019 as a head of the Information Technology by most of the dangerous virus, ransomware and experienced of encryption of important files, there was an intention to do research on cybersecurity, especially for the prevention of the IT world from ransomware. Although it comes from malware family, but its techniques are different from other malware types. The main target of this category is to encrypt files in AES keys cryptography and demand ransom in the form of cryptocurrency, particularly Bitcoin in return for the hacked data to earn huge illegal money. In other words, Ransomware is a class of self-propagating malware that uses encryption to hold the victims' data ransom (Chen & Bridges, 2017). Target of ransomware can be varied from financial, government, healthcare, corporate companies to end-users as it can be transmitted over the internet. Ransomware can attack through social network, download adverts in the name of benefit, spams through email, take advantage of weak security policy in network and passwords, unauthorized downloads or through open VPN ports or by any other back doors". Payment does not guarantee that encrypted files will be released, and similarly decrypted file doesn't mean that malware is removed from the system (Scaife, Carter, Traynor, & Butler, 2016). The recent cybercrime especially ransomware has turned into a profitable business with an estimated global cost of around $6tr (£4.24tr) per year. It can be no denying that digital crime is just as lucrative for criminals as it is destructive to businesses (Morgan, 2017).

According to the cybersecurity venture report, in 2020, the FBI's Internet Crime Complaint Center received 2,474 ransomware complaints, and those are just the ones that got reported (FBI, 2020). Cybersecurity Ventures expects that businesses will fall victim to a ransomware attack every 11 seconds in 2021, up from every 14 seconds in 2019, and every 40 seconds in 2016 (Singh, 2021).

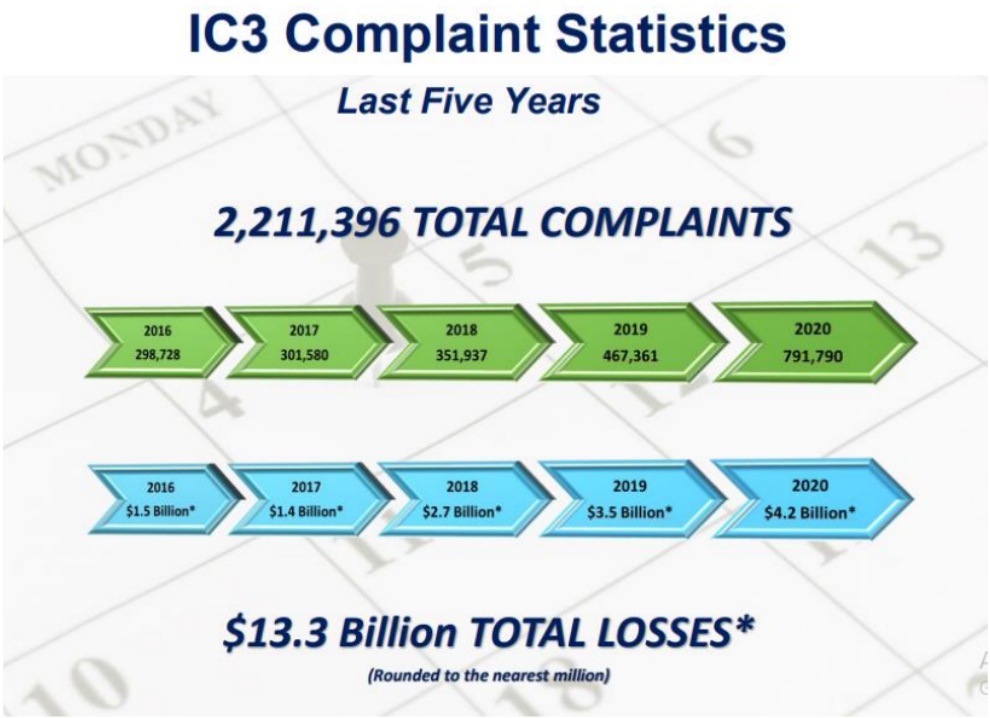


Figure-3: Cybercrime Complaints of last 5 Years to FBI, Source: Internet Crime Report-2020, FBI

The multinational companies that have most money, healthcare system and higher education sectors are the main target of cybercriminals through ransomware viruses. Among the most affected countries, United States, United Kingdom, Japan, Germany, Italy etc. are the highest cases reported in last 6 years. Therefore, as stated by "Cybersecurity Ventures", ransomware is the quickest increasing type of cybercrime. Since, global ransomware wastage expense is

predicted to hit $20 billion in 2021, up from just $325 million in 2015 which, is 57X extra in 2021 (Steve Morgan, 2019).

This project analysed the causes of being attacked by ransomware and the possible ways to prevent it to strengthen cyber security. It will help new researchers by providing them experimented outcome with summaries of previously published research works that will aid them to identify research gaps. The main research question of this study is "What are the most effective strategies to prevent from being attacked by the ransomware?" This question is answered by comparative experiments over several versions of Windows and Linux based Operating systems that how they get attacked and what are the prevention techniques should be taken by the cyber world against the ransomware.

2.3 Definition of Ransomware

Ransomware is a type of malware that makes files on a victim's computer inaccessible and then demands the victim to pay a ransom (usually in the form of bitcoins) in order to regain access to the lost files (L. Kelion, 2013).

Ransomware can be considered as a serious threat when it comes to protection of information assets. The main targets are internet users. Ransomware hijacks user files, causes difficulties and then requests some funds through extortion for decryption purposes (Bhattacharya & Kumar, 2017). Ransomware can be categorized as malware which can affect the vulnerability of the user's system, allowing the system to be accessible individually and eventually encrypts all the files that have been targeted (Gonzalez & Hayajneh, 2018).

2.4 Types and Dimensions of Ransomware

Currently, there are over 50 types of ransomwares exist globally however it can be categorized into three main dimensions. According to Yaqoob et al., (2017), the three basic types of

ransomwares are known as Crypto Ransomware, Locker Ransomware, and Hybrid Ransomware. The Crypto Ransomware represents encrypting files with complex hash algorithm using both symmetric and asymmetric keys and it restricted users from accessing those files without paying ransom to decrypt the files and access it again. WannaCry, Petya is the example of this type of viruses. The Locker Ransomware mainly lock the desktop and its application to access it and it works solely on the core application software and registry level of an Operating System. It starts attack to an OS by sending spams messages with malicious attachment through internet browsers, mails and popups to the target end users. The Winlocker is an example for this type. The third type of ransomware is Hybrid ransomware. This is the most aggressive ransomware as it works Hardware Abstraction Layer (HAL) to lock the device and its functionality and can cause physical damage of the device. The possible target group of hybrid ransomware is the Internet of Things (IoT) devices.

2.4 Development History of Ransomware

Dr. Joseph Popp, who was been declared mentally unfit by the court later, built the first ransomware in 1989. He named it "AIDS (Aids Info Desk) Trojan" and it was the first ever recognized ransomware virus. He mainly created this trojan for Windows based Operating Systems to replace the autoexec.bat file that count the booting number of times of a computer. Once this boot count reaches 90, it would then hide directories and encrypt the names of all the files on the C: drive and make the system unusable. To regain access, the user would have to send $189 to PC Cyborg Corp. at a post office box in Panama. The history began from this event and continues until now with a variety of updated ransomware strains. In 2021, ransomware declared as Ransomware as a Service (RaaS) targeting the customer to use malwares and decrypting solution as a legal service in return of money. Their next aim is the cloud-based database and storage with less secured devices like M2M (Machine to Machine) smartphones and IoT appliances. Although the first-generation ransomware was not successful

as very limited number of people have the access to their personal computers, however, in 1996 Adam L. Young and Moti Yung made an initiative to introduce the first prototype asymmetric ransomware (Aini Khalida Muslim et al., 2019). Unfortunately, this development risked the developers and due to the failure, cyber-attackers worked harder to develop a more malicious ransomware in the form of fake antivirus that can be better executed (Chhillar, 2017). They introduced idea of using public key cryptography for such attacks. This attack was referred to as being "cryptoviral extortion". A cryptotrojan, cryptovirus or cryptoworm hybrid encrypts the victim's files using the public key of the ransomware author and the victim has to pay to obtain the needed session key. This is one of many attacks, both overt and covert in the field known as Cryptovirology (Aini Khalida Muslim et al., 2019).

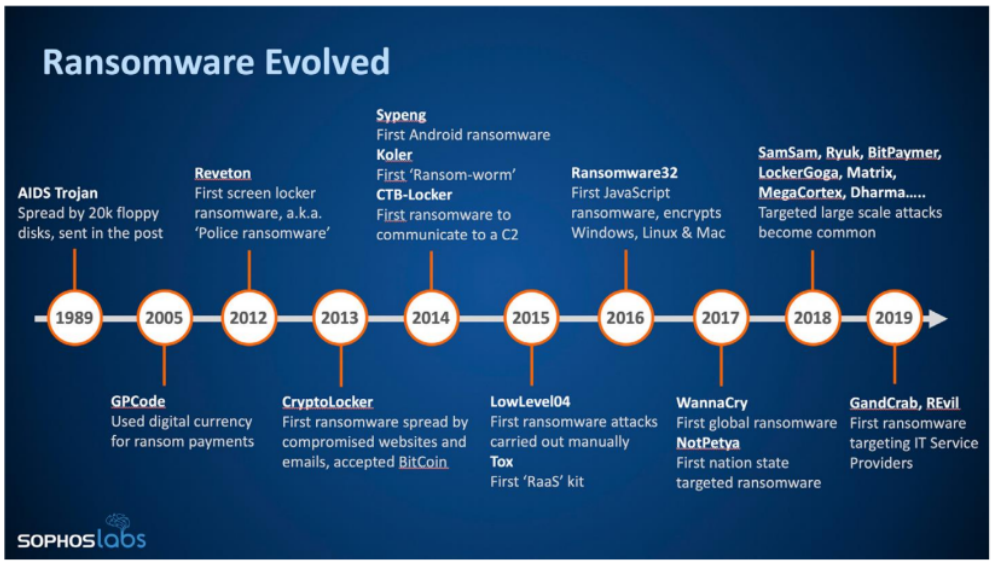
The internet based modern ransomware first appeared in 2015 in the name of GPCode using sophisticated 1024-bit asymmetric RSA key encryption scheme. The modern cybercriminals changed their techniques in that time by sending false attachments in the name of job applications, security updates and patches. The dimension of ransom payment changed from currency to bitcoin and the targets also shifted from personal the corporate companies to earn more money from this illegal cyber business. The most famous piece of ransomware is known as CryptoLocker and it was developed by a hacker named Slavik (Richardson, 2017). During the period of 2015 to 2017 using CryptoLocaker different viruses were developed by the hackers and attacked NHS of UK, Apple and many other giant companies in the world and ransomware became in the limelight of the cyber world.

The common types of modern dangerous ransomware strains that appeared in last 6 years are:

Cerber: This is a recent development of ransomware family. 1n 2020, cybercriminals diverted their concept of virus to a service and named as a Ransomware as a Service (RAAS). It mainly

attacked on cloud-based servers and applications like Office365, Azure, VMware that is the datacenters contained storage of millions of companies and individuals. Thus, online cloud-based servers are faced major challenges in the digital history.

BadRabit: In 2017 a newly variant of ransomware appeared named as BadRabbit. This type of ransomware primarily that was attacked in Russian area through a name of fake update of Adobe Flash player in different webpages. However, when unawre users clicked on that link to update adobe flash player, it redirected to a ransomware page that demands cryptocurrency and on the background the browsers' PC was infected with the encryption of files.



CTB Locker: This ransomware type send attachment to the target user with email in the form of .doc, .docx, .pdf, .ppt, .xlsx etc. with some promotional offers. If user download, can be infected with CTB Locker ransomware and the users' files are become encrypted.

Crypto Locker: This is the version of ransomware that came into limelight in 2013 and earned more than three million dollars as ransom money from the users. In this malware, cybercriminals first used cryptographic keys with 128 bit encryption method with private keys in addition to the public keys that was generated with hash algorithm and almost impossible to unlock without the generator. However, it was also neutralized and closed in 2014.

Crysis: Basically previous ransomwares used single extension to add with the original file names, however this type of ransomware first introduced two extensions with the original file name and was difficult to decrypt. One of the noticeable things was the malware attached with the mail or any webpage were not any .exe file so that email clients and web browsers generally do not doubt about it as a virus.

Crypto Wall: This is one of the dangerous and worst types of the ransomware family because it does not only encrypt files of the victim machine, rather becomes hidden to the system files and watch new files that are left to be encrypted and execute when appeared. Crypto Wall mainly send malware through spam emails to exploit users PC to earn illegal money.

Not Petya: Although the name indicates that it is not a virus or ransomware, however, it was a destructive ransomware version that spread malwares in 2016. The main objective of this type was not to encrypt the files only, but also to destroy the file system structure, so that the internal operating system file standard NTFS or EXT are become crushed and user cannot create any new files.

Petya: Petya is another dangerous virus that comes from ransomware family. It can corrupt MBR (Master Boot Record) and take control of whole system files, boot files, karnel and user files. It also can delete boot files so that the operating system cannot load its files to run the PC. It attacked first in 2017 to Ukraine and targeted mainly to the devices who have not updated patches or security features.

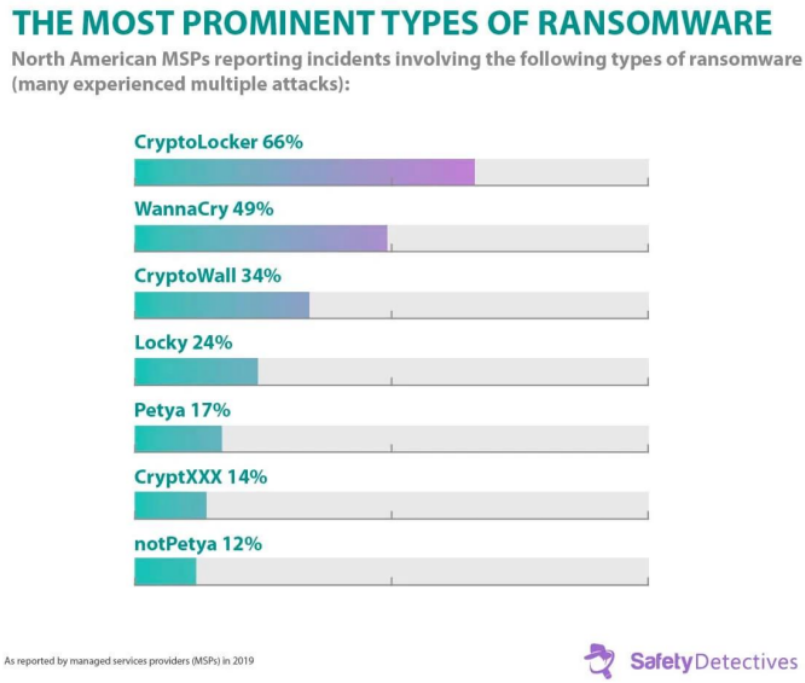
Golden Eye: This is also a recent development in ransomware family that originated from petya coding. The main specialty is that it targeted different organization levels instead of individuals. One of the key developments of this type is, it can accept cryptocurrency payment automatically while user download and become infected. It runs am macro while encrypt the files and can also corrupt MBR to make the system stuck.

Le Chiffre: This type of ransomware first starts in 2015 in USA targeting the business distributors, however later on it attacked many organizations. The approach of spreading malware is different than others. Instead of email attachments or spam, it uploaded many HTTP web pages and provoking users to download free of costs. When user click on it, become hacked and it encrypted all the files with extension of .lechiffre.

Jigsaw: Many variants of ransomware do not delete the user files, rather they encrypt and ask ransom to decrypt it. However, jigsaw is a type which gradually delete the original files if the money was not paid by the victim.

Ke Ranger: It was mainly developed for the Mac Operating systems, although Kaspersky lab discovered it as a ransomware variant, however, it was attached on the one of the software downloading sites of torrent.

Locker Goga: This virus was found in aluminum manufacturing company and one of the very recent that attacked in 2019. It attacked through a non-secured email clients but encrypted all files of that company. Although that company recovered later, however, it paid huge ransom to retrieve their data.



Locky: This ransomware usually spread through emails and encrypt with a strong algorithm using AES keys that was not possible to decrypt without the key maker.

Maze: Maze is also a very recent development of ransomware family that attacked in 2019 and main target was in the health sectors. USA and UK those who preserve users health information, they were the main target points for this type of ransomware variant.

Ryuk: This is the type that spreads silently over the target PC while playing games by the users and appeared as a pop-up window. When users, especially the young one are become very busy to play games, they through a pop-up window and accidentally it was clicked by the player and attacked to the users' files. It is also one of the very recent types that attacked in 2021.

Spider: This type of virus work in background and enter into the computer through Word files so that they do not fee any doubt about this file. Sometimes it comes in the form of bills, invoices, and other promotional offers and become infected.

WannaCry: This is the most dangerous virus that collected more than e million dollars and infected over 200000 PC all over the world. WannaCry mainly found the loop fault in previous versions of Windows, especially, Windows XP and Windows 7, to enter into the network and run a massive operations to encrypt all files and asked ransom money. NHS of UK also was affected by this types of viruses.

2.6 Recent Scenarios of Global Ransomware Attack

In recent years, Europol's annual Internet Organised Crime Threat Assessment report has consistently identified ransomware as a top priority; their latest bulletin states that ransomware remains one of the, if not the, most dominant threats, especially for public and private organizations within as well as outside Europe' (Europol, 2020).

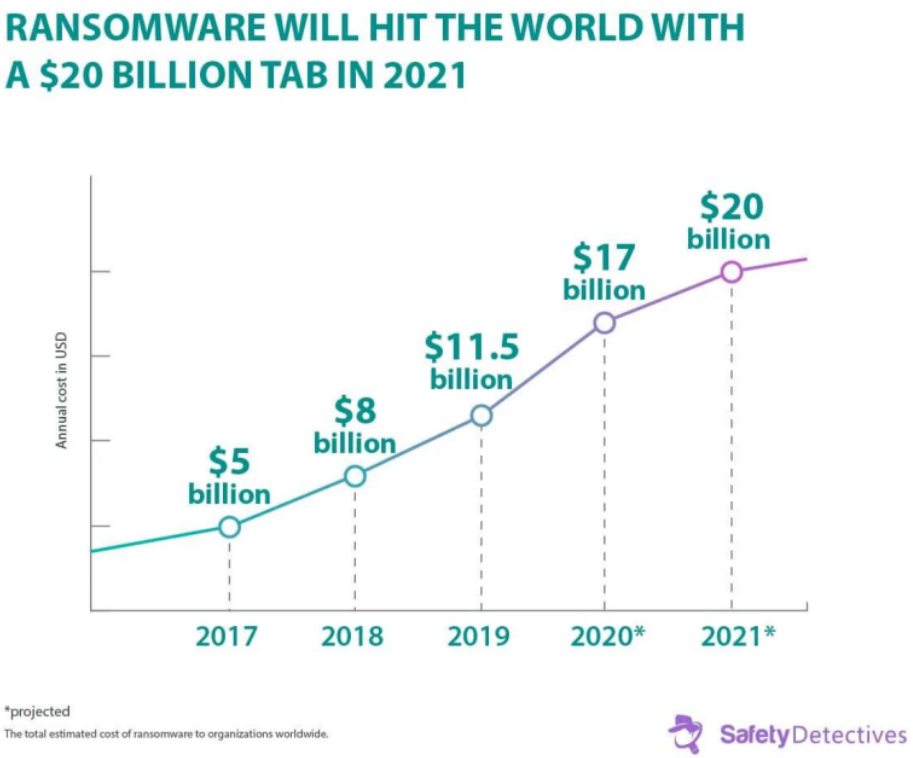
One of the most well-known ransomware types is WannaCry, which caused enormous global damage estimated at several hundred million to four billion dollars. WannaCry attacked more than 200,000 computers in 150 countries (Kristin Masuch et al., 2021).

Perhaps the most memorable cyber-attack in recent history was in May 2017, when the WannaCry attack jolted the public into awareness of just how destructive ransomware can be.2 WannaCry infected over 300,000 Windows computers by encrypting data on the machines and then demanding Bitcoin to unlock the data. It was a particularly destructive attack as it struck a number of high-profile systems, including many in the UK's National Health Service (NHS).

The German Federal Office for Information Security assumes that severe threats are mostly posed by ransomware attacks, which cost 8 billion dollars worldwide in 2017 (Kristin Masuch et al., 2021)

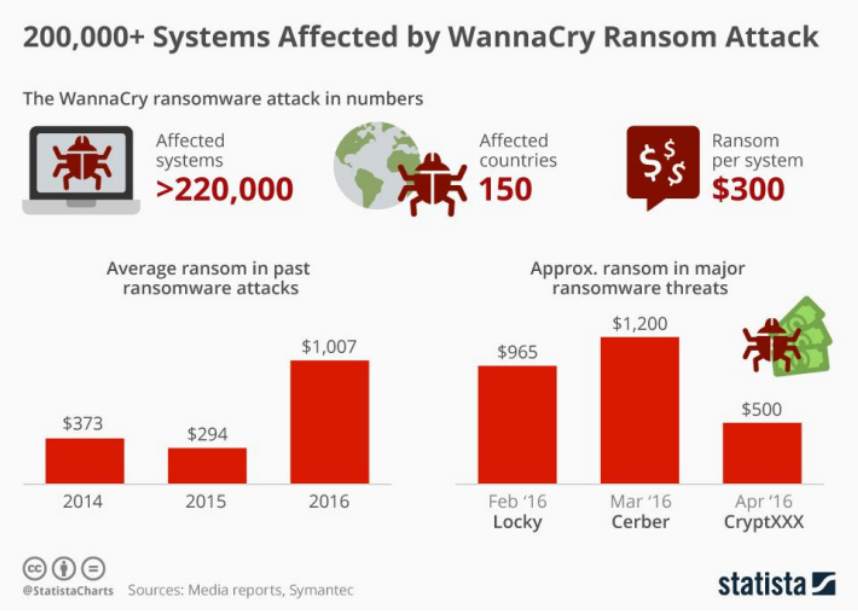
2.6.1 Yearly Attack Statistics

Cyber specialists assume that as the digital underworld expands so quickly especially in the Covid-19 pandemic situation where most of the tasks are performed based on online to include a broader range of cyber-attacks, ransomware increases its harsh financial gain across the globe and it was estimated to grow to $20 billion by the end of 2021. According to the Safety Detectives, a cybersecurity analysis group the financial damage for ransomware attack will hit around 20 billion US dollars.

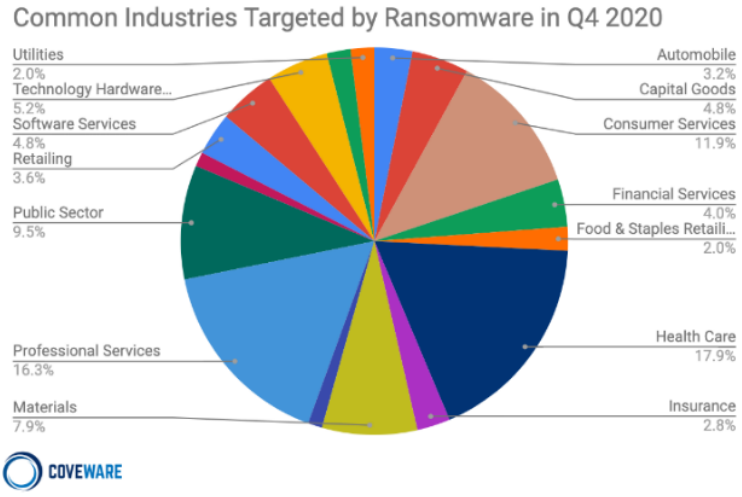


2.6.2 Dramatic rising Trends of Ransomware Attack

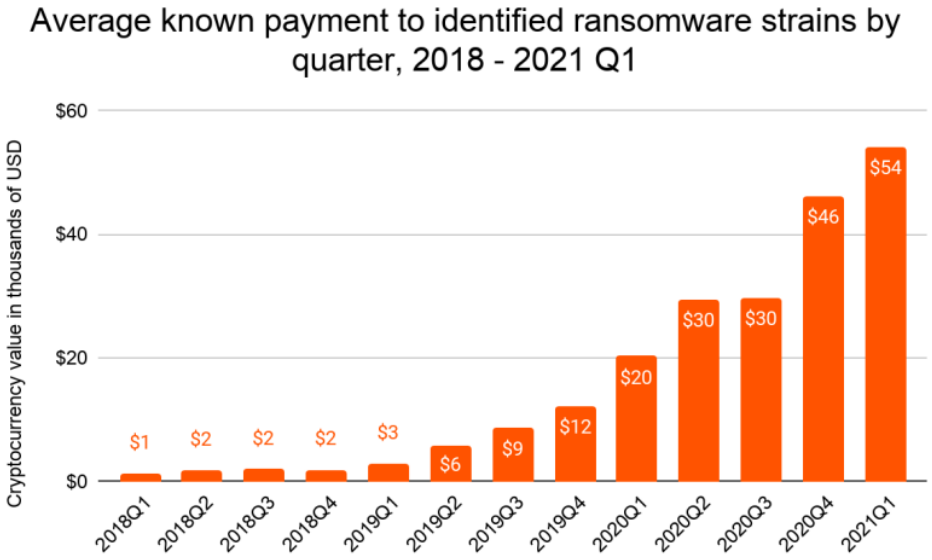
The rising trend of making different ransomware variant has increased dramatically from 2017 when the major attacks were occurred throughout the world. Cybercriminals achieved illegal success on this year and became inspired. For this reason, from 1989 to 2014 the ransomware variant were not more than 20, however from 2017 to 2021 it crossed over 50 due to the earning desire of huge illegal money.

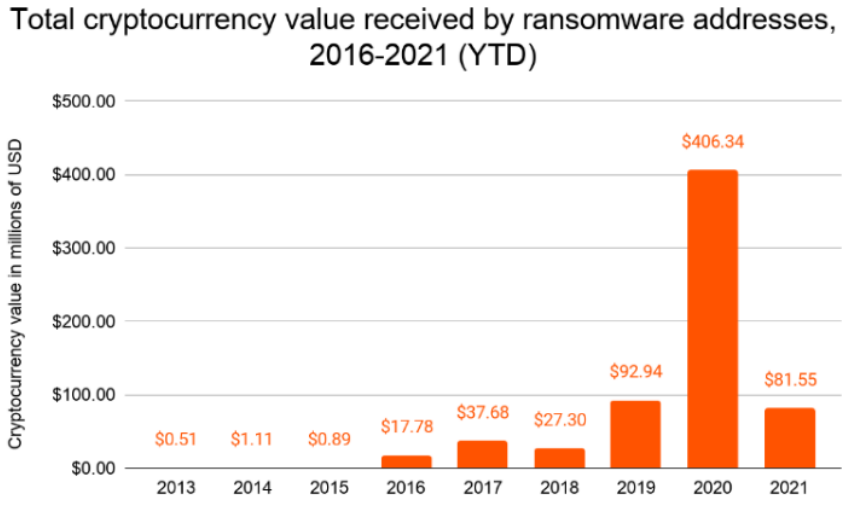


2.6.3 Attack Type and Main Targets



2.6.4 Worldwide Financial Impacts


Average known payment to identified ransomware strains by quarter, 2018 - 2021 Q1
Cryptocurrency value in thousands of USD
$60
$40
$20
$0
$1
$2
$2
$2
$3
$6
$9
$12
$20
$30
$30
$46
$54
2018Q1
2018Q2
2018Q3
2018Q4
2019Q1
2019Q2
2019Q3
2019Q4
2020Q1
2020Q2
2020Q3
2020Q4
2021Q1


Total cryptocurrency value received by ransomware addresses, 2016-2021 (YTD)
Cryptocurrency value in millions of USD
$500.00
$400.00
$300.00
$200.00
$100.00
$0.00
$0.51
$1.11
$0.89
$17.78
$37.68
$27.30
$92.94
$406.34
$81.55
2013
2014
2015
2016
2017
2018
2019
2020
2021

Chapter-3
Design, Test, and Implementation

This project developed a practical situation of demonstration to design a process, build demo ransomware viruses and experimented on virtual environment to implement the hypothesis of this research that reasons for being attacked and the best way to prevent ransomware.

3.1 Installation of Operating Systems on Virtual Environment

To design the whole process the six major Operating Systems from Windows and Linux platform has been installed on Oracle Virtual environment. The main Operating Systems that were tested for ransomware viruses are: Windows XP, Windows 2007, Windows 10, Ubuntu, Debian and Kali Linux.

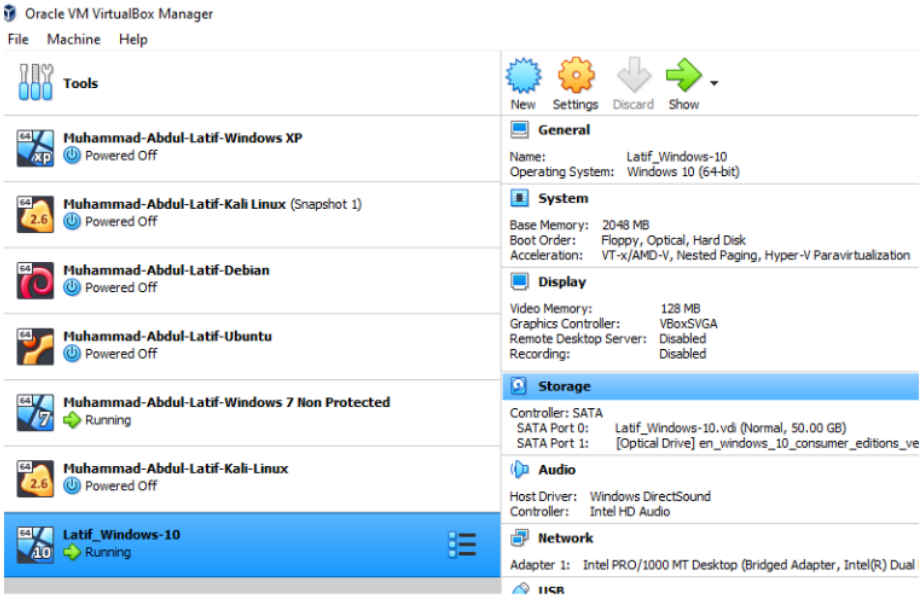


Figure-2: Installation of 7 Virtual Machine on Oracle VM for Testing this Project

3.2 Building the Ransomware Virus

To build a full faced ransomware virus there were some pre-requirements that has been performed sequentially:

Firstly, the Windows based operating systems were required to update. Secondly, DotNet Framework, Visual Studio DotNet, Visual Studio Coder were installed for writing ransomware executable encrypting and decrypting scripts. Python programming language was installed for the Linux based Operating Systems, finally some cryptographic modules and third-party tools were installed to generate RSA 256-bit encrypted public and private keys as well as to send ransom notification through changing the desktop background.

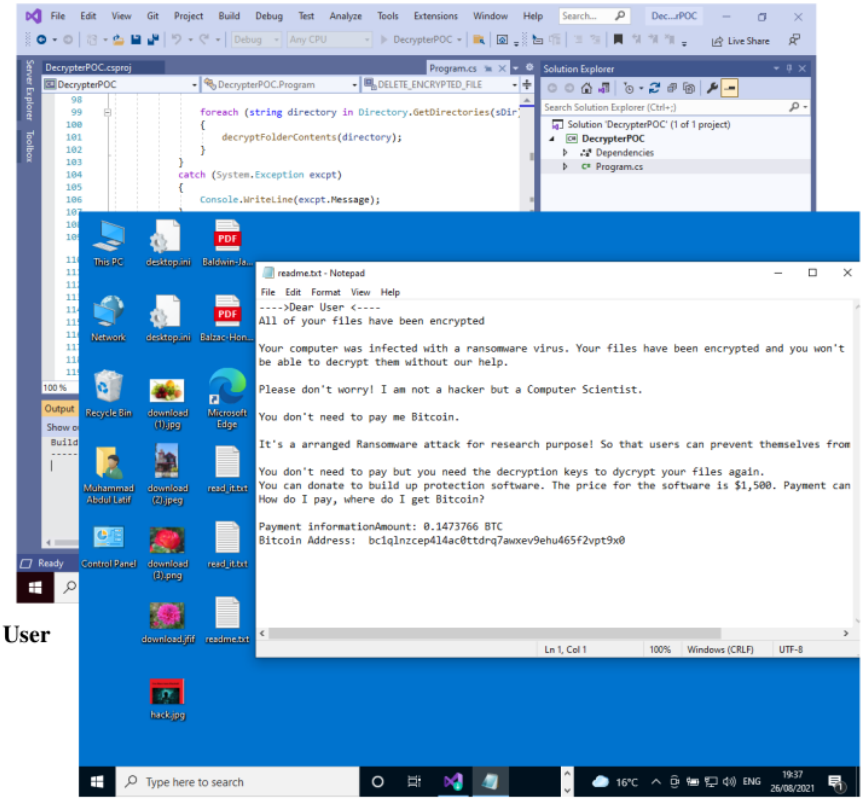
3.3 Insights of the ransomware viruses:

There are several files were created to build a complete ransomware virus. These includes:

1. **Executable Encryptor:** The main encrytor.exe file for Windows based Operating System that consists of main codes to encrypt the user files

2. **Executable Decryptor:** The main decryptor.exe file for Windows based Operating System that consists of main codes to encrypt the user files

3. **User**



Notification File: After encrypting the user files a text file was developed that ransomware virus automatically create this file on the victim machine's desktop to notify that "you are being hacked and your all files have been encrypted". Please contact the specified email and send bitcoin.

4. **Wallpaper Change:** To change the desktop wallpaper automatically during the ransomware attack there was a customised wallpaper required to be made as a user notification ransomware note.

5. **Extension Selection:** The file types that will be encrypted by the ransomware virus should be mentioned in the code while developing the virus.

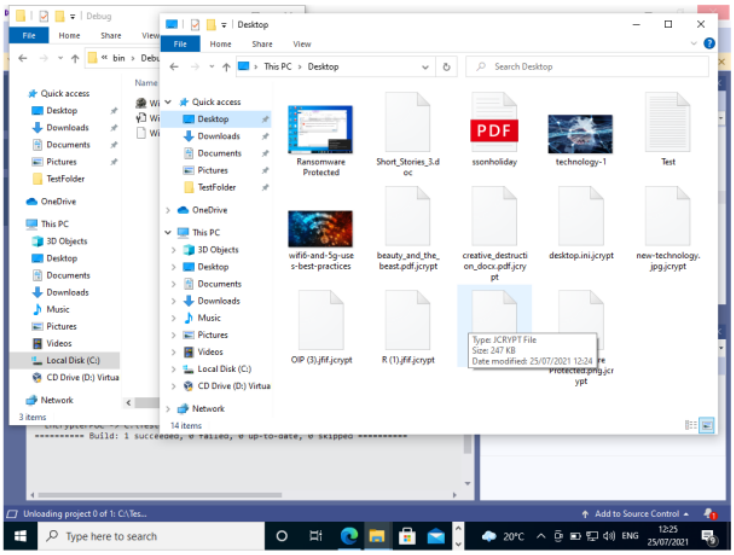
3.4 Practical Testing on Different Operating Systems

3.4.1 Windows Legacy Operating System (Windows XP)

The experiment was tested at first on Windows XP operating System as this is still using at the end user level in some organizations. Although Microsoft has ended the support and update of this operating system long before. The test shows that the ransomware encrypted its files without any encountering challenges from its in-built security features.

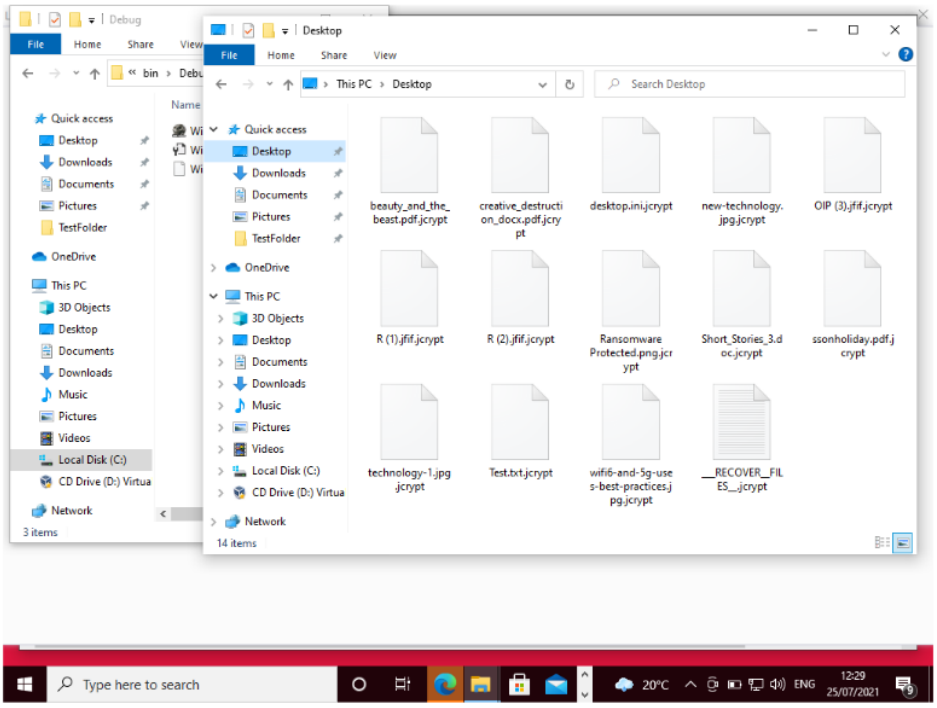
3.4.2 Windows Older Version (Windows 7)

Windows 7 operating system is the main target level for ransomware viruses as it became successful during worldwide massive attack in 2017 through WannaCry family. Windows 7 is still a popular OS for the unexpert users and have been using by many organizations in spite of being outdated declared by Microsoft regarding user support and update. Although Windows Defender primary version is included in this operating system, however, ransomware can disable it while attack.



3.4.3 Windows Latest Operating System (Windows 10)

Microsoft has designed Windows 10 equipped with all kinds of security and endpoint shield features against any viruses including latest dangerous ransomware version. Windows Defender for this version can detect, quarantine, disinfect and automatically delete any kinds of ransomware in the PC, email and web download files while extracted. As a part of this project the experiment was done on Windows-10 with both conditions i.e., by enabling Windows Defender and disabling it. However, if the windows version was not updated its patches and defender was paused, ransomware can attack within few seconds and can make disaster of the important files.



3.4.4 Ubuntu

Although Linux based operating systems are considered as a secured system due to its file structure and security features, however, as most of the webservers are running through Linux based OS, now it became a lucrative target among the cybercriminals for demanding

more ransoms. This project tested ransomware script on Ubuntu through a bash script developed by python programing language to encrypt its files and the test was successful though it notifies its harmfulness.

3.4.5 Debian

Debian distribution of Linux is also mainly used in different server applications and MySQL databases. The ransomware project was tested on Debian through a script file developed by python programing language to encrypt its files as everything in Linux is a file.

3.4.6 Kali Linux

It was well renown that Kali Linux was built by the hackers' community to research on the possible different types of attacks. However, it has been misused by the cybercriminal to develop many viruses through this research platform of Metasploit. Hackers are generally use Kali Linux to develop viruses like ransomware and other malwares. This project also tested such script on this OS to examine and explore the prospective preventive measures form this analysis.

Chapter-4

Test Result Evaluation

To reach in a conclusive position of the main hypothesis of this research project based on the similar parameters on different operating systems practical tests were performed. The constant parameters were if the particular Operating System is updated with patch or not. What are the conditions changed if it enables and disables its built-in security systems? To find out the outcomes ransomware have performed several internal procedures on different operating systems. After the experiments were done on different operating systems the reasons and limitations behind the attack have been explored. This project also analysed and pinpointed the comparative causes and effects of being attacked by the ransomware viruses on both different versions of both windows and Linux based operating systems.

4.1 Attacking procedures of Ransomware

Sometime users notice that their computers are running slow, or the files are not opening rather generating an error message like “unknown file type” and suddenly changed their desktop wallpaper background stating a dangerous message that “your computer is hacked”. This is the initial process when a user can detect that they have been attacked by the ransomware viruses. However, Ransomware usually attacks on a target machine through its different stages as below:

4.1.1 Sending to the Target:

The first and foremost task of cybercriminals is to send the virus to the target machine. Ransomware typically spreads its virus files through spams with attractive names so that users become interested to click it. The phishing emails, or through social engineering efforts is also a common way today as most of the internet users are spending their screen times in social networking applications. It can also be spread through websites or drive-by downloads to infect an endpoint and penetrate the network. However, cybercriminals are

evolving their infection methods constantly and there are countless ways one's technology can become infected. Due to the Covid-19 pandemic situation while people are maintaining social distancing, working from home and preferring to buy and sell through online, the ransomware attack cases increased by 485% in 2020 than previous year according to the latest threat Landscape Report 2020.

4.1.2 Encryption of files

The second stage of the ransomware hackers is to encrypt the files. Some ransomware versions delete the user files, but majority of the distributions generally do not delete the files rather encrypt by using 128/256/1024-bit cypher Asymmetric Advanced Encryption Standard (AES) hash algorithm public or private keys so that users cannot open it without that specific key.

4.1.3 Readme.txt file message

Another mentionable feature unlike other previous malwares or viruses is that ransomware keep a track and inform to their victims that they have been hacked and ask money through cryptocurrency using bitcoin address by creating a file usually named as ReadMe.txt.

4.1.4 Renaming the file extensions

During the encryption process ransomware creator use their own file extension to rename the user files replacing or adding with that specific extension so that users can guise that their files have been encrypted and cannot be open anymore.

4.1.5 Changing the Wallpaper asking money as a ransom

At the last stage of infecting to the target machine is to replace the desktop wallpaper background with a new customized terrible one that clearly reflects about being attacked by the cybercriminals through ransomware.

4.2 Causes for Ransomware Attacks

After experimented practically in this project it was reflected the main reasons for which users or computers are being attacked:

4.2.1 Using Pirated Version of Operating Systems

Original manufactured version of the operating system software is responsible to protect their users from any kinds of attack. However, when users are using non-licensed pirated version of software, they become the target victim that was prove by this experiment.

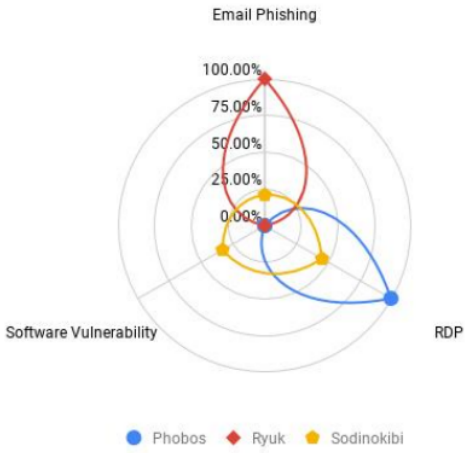
4.2.2 Patches are not updated regularly

While testing one version of windows-7 and 10 was patched and other version was not updated with the latest security patches and found that those versions are not updated patches are more likely to be infected easily by the ransomware attack. Because every operating system updates it's patches time to time by considering with the latest viruses with prospective strong defence systems on it to prevent the users.

4.2.3 Installation of Digitally not signed Applications and Software

Downloading any unauthorized software and installing it without being digitally signed by the operating systems are one of the major causes of the ransomware attack. In this project, a crack activator has been tested and found that this Windows activator has the direct link with the ransomware virus. When users attempt to install and activate this executable file, it automatically redirects to the ransomware encryptor to take over the control of the whole PC. However, there are some warning messages generate by windows that this application

is not digitally signed and a dangerous software that can harm your computer. If users ignore this message and run forcefully, they can be infected by ransomware.



4.2.4 Clicking the dangerous E-mail attachments

As hackers primary attempt to the target users to send the spam or phishing mails in the name of some promoting ways to lure users to click and download the attachments, an unaware user can be affected by this trap easily. Cybercriminals usually send such files naming as “security_updates.exe”, “your_offer.exe”, “claim_your_money.exe” etc.

4.2.5 Network Management system are not secured

As the profitable corporate clients are the main target of cybercriminals, if the Network Management Systems are not configured strongly and monitored continuously, the chance of being attacked has increased in that companies. According to the COVEWARE report in 2020, the big target in this Covid-19 pandemic situation is the Healthcare, Oil and Gas and Higher Education sector (Coveware report 2020). Without configurations of hardware firewalls, network security and sophisticated real-time monitoring systems the giant companies can be a target victim of ransomware.

4.2.6 Sharing Files over the Network through non-secured channel

According to the Gartner report in Q2, 2020, most of the cyber-attack occurred including ransomware due to the Virtual Private Network (VPN) login of the network administrators from their home. Basically, VPN in the corporate office premises is configured with maintaining all possible security risks, however when home users connect to the servers and transfer files with administrative privilege and their home network are not configured based on strong security or firewalls, the whole system are established connection by a non-secured channel and the possible attack was happen.

4.2.7 Using virus affected removable devices

Using removable devices, memory cards are another remarkable risk zone by which users can be infected by the ransomware viruses. The removable hard drive, pen drive, disks that are already contained with malwares or ransomware can spread over whole network nodes in a LAN and can make a disaster for a corporate company by encrypting their important files and lose huge amount of money as well.

4.3 Comparative Vulnerability among different Windows Versions

This project compares the effects of the ransomware in relative vulnerability of different versions of the Windows based operating systems. The experiment result was different based on the versions and security levels.

4.3.1 Weak Security in Legacy Operating Systems (Windows 7, XP)

Windows XP and Windows 7 are considered as the client operating systems. Although Microsoft ended supports and updated of these two versions, however these has still been using in personal as well as corporate end user level. When the encryptor script was run on Windows XP, it does not encounter any hindrance from the system security levels and encrypted all the files. So, using this obsolete version is in high risk for anybody or any organization. On the other hand, Windows 7 version has a limited capacity of Windows Defender and generate error

message if found something harmful but allowed to run if execute with the administrative privileges disabling it. The main attack of WannaCry in 2017 was accessed in worldwide through the Windows 7 versions.

4.3.2 Windows 10 is more secure against any Ransomware attack

Microsoft developed Windows-10 latest versions with the remarkable improvement in security and maintenance features, user access control, device level security, and Windows defender firewalls that can detect any virus file when downloaded or extracted. When a encryptor script was created on windows 10 by using visual studio dotNet, it was been deleted automatically by the Windows defender before executing it. So, it indicates that no virus can enter the Windows 10 updated, and defender enabled version, not even any ransomware. However, when the windows defender was been disabled, the ransomware virus was executed and encrypted the files. Notably, in comparison with windows 7, disabled defender and firewalls on windows-10 are automatically enabled the real-time protection when system restarts.

4.3.3 Windows Defender can protect from Ransomware attack

The latest version of windows defender still can protect from any kinds of malwares and viruses if it became enabled.

4.3.4 PCs with Regular Updated Patches are less vulnerable

It was also tested by this project that PCs with same Operating system those are updated regularly with all patches and security features with automatic updates enabled are less vulnerable to being hacked by any applications or viruses than the unpatched one, especially by the ransomware.

4.3.5 PCs with non-secure file sharing are very easy to be attacked

This project also experimented that, users who transfer files without using encrypted protocol can be infected through this non-secured channel.

4.3.6 Older Versions have no Complex Password Requirements

The previous versions of windows up to windows 7 that have not any complexity requirement of passwords. So, anybody can hack the password easily and can push the virus files to the target computer to run it with the administrative privileges. However, the latest windows versions overcame it and improved a mentionable level.

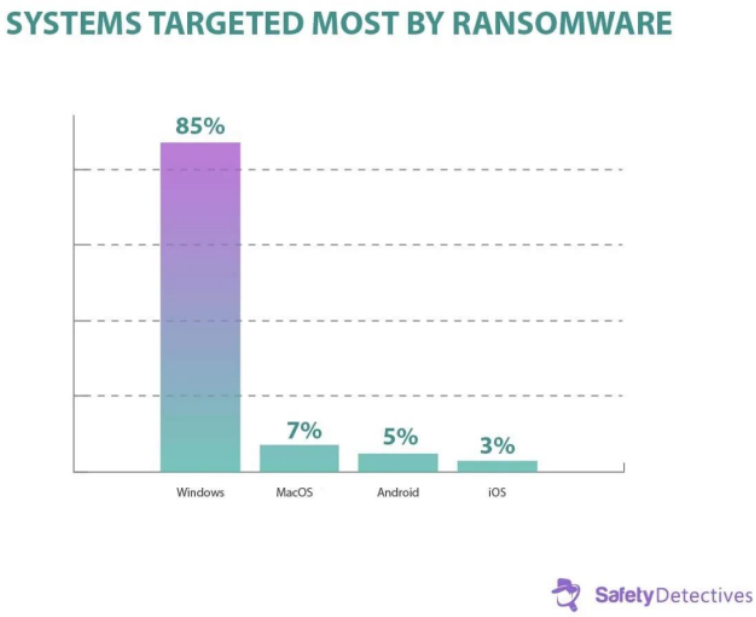
4.3.7 PCs without License Software are more vulnerable

The system which is installed any pirated or crack version of operating system software can be infected by the ransomware at any time, because windows cannot update its patches and security features in that case. Moreover, installing any digitally unsigned application software in any versions of the windows are at high risk to become infected.

4.3.8 Combination of Antivirus with End point Security are more secured

Recently windows 10 introduced a feature that if a system has a licensed antivirus installed in addition to Windows Defender, it makes a secured shield with the combination of both third-party antivirus and windows defender and can prevent PC from any kind of internal and external attacks.

4.6 Comparative Vulnerability among Windows VS Linux/Unix OS



4.6.1 Linux/Unix based systems are less vulnerable than Windows OS

After completion of this real ransomware experiments, it was reflected that Linux based Operating Systems are less vulnerable and more secured than any windows versions. Because it handles user and group level permission for a specific file. Moreover, the system files have only the permission by the "root" user and recently the "root" user is by default become disable unless user switch to a superuser or enable it. The main obstacles for ransomware and other viruses on Linux is that the running ".exe" file is much harder while it is easy in Windows whereas the majority of viruses are made with ".exe" files. The File System Security in Linux is stronger than Windows

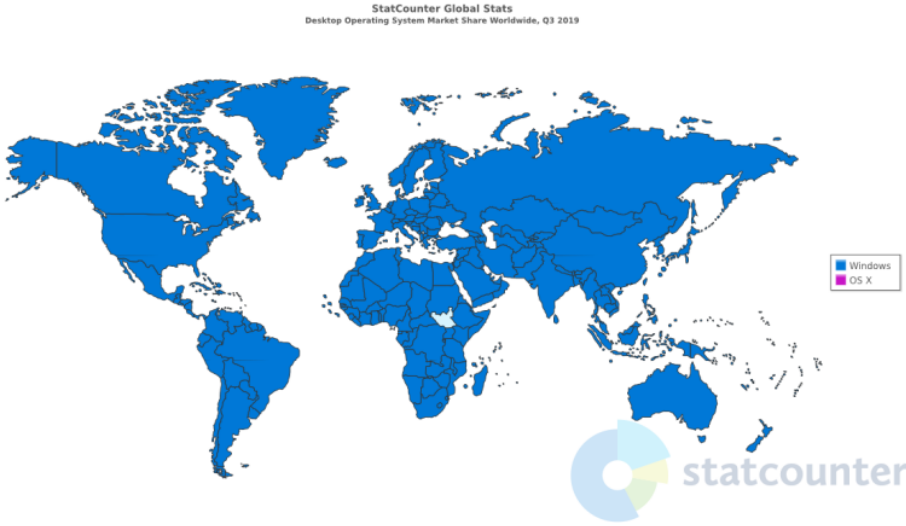
4.6.2 Windows Users are the main target for Ransomware

Initially ransomware was developed for targeting windows-based clients as most of the world's client operating systems are comes from windows OS. According to the Statcounter Globalstats, 72.97% of desktop users are using Windows.

33

Source: https://gs.statcounter.com/os-market-share/desktop/worldwide#quarterly-201903-201903-map

Whereas Linux operating systems are using only 2.38% in July 2021, even in 2019



using Windows percentage was more than 75%. For this reason, the main target of cybercriminals is Windows operating System.

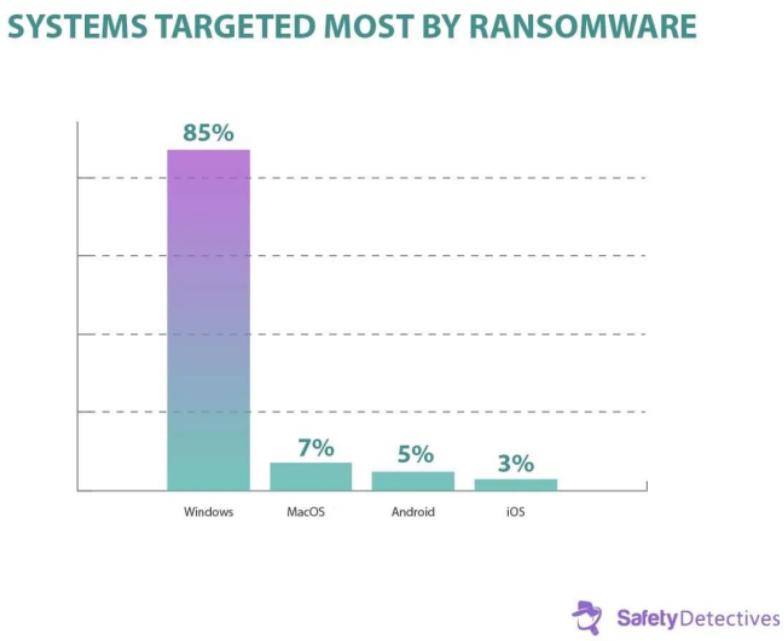


Figure: Different Operating Systems, targeted by the ransomware
Source: SafetyDetectives

4.6.3 Malware, Spam, Trojan cannot encrypt all files in Linux

Generally, it is assumed that, by default, Linux based operating systems are more secure than Windows due to the design, file format and user permission through umask. Another advantage is that viruses cannot encrypt all system files that own by root and after being infected it can be disinfected more easily as everything in Linux is a file.

4.6.4 By default, risk websites are not accessible in Linux based Browsers

Linux browsers, by default block all the harmful webpage to be loaded. So, if any webpage contained risk, viruses, harmful contents or ransomware, it automatically blocks and browser will not open that page for user due to the system safety and security. So, this is an advantage in comparison with Windows.

Chapter-5

Prevention of Ransomware

By 2025, at least 75% of IT organizations will face one or more attacks, as free-rein researchers document a dramatic increase in ransomware attacks during 2020, pointing to sevenfold or higher rates of growth (Nik Simpson, Jan 2021). The removal process after being attacked by ransomware is very challenging even if anyone pay the ransom, so, preventive measures are the best way to make secure the digital devices from being attacked. There are many ways to prevent ransomware:

5.1 Identifying Attack Vectors

To prevent systems from ransomware attack, it is essential to identify the attack routes by which hackers usually attempt to enter the system. The main vectors of attack are two types: human attack vectors and machine attack vectors. Common human attack routes are fishing email, sms, social media post link, instant messenger group link and any downloadable weblinks by which hackers trigger human users to click any false attachments or links in the name of security updates or won lottery etc. that contain ransomware executable files inside it and when clicked by users consequently run the ransomware in background and encrypt all files. Similarly, in voicemail they insist users to dial a number that redirect to a ransomware attacking process. The second type of attack vector is a system where hackers scan IP of the target machine, identify network vulnerability and invade automated process attack by machine to machine with very minimum human involvement. This type commonly uses some machine learning techniques and artificial intelligence in the form of drive-by popup webpage, advertising to deliver malware in the form of “Download now” or “Free Download” etc. It also can push ransomware files to any nonsecure ftp server and shared folder to a less secured network. To prevent the systems from ransomware, these routes or vectors must need to be identified and secured.

5.2 Using Licensed Operating System

As customers purchase operating systems from the vendors, these software developer vendors have the primary responsibility to protect their clients. They have been improving their systems gradually based on the global market cyber threads. If clients use original licenced version of the operating system (OEM), it is primarily enough to protect from any kinds of viruses, especially from ransomware. However, if any customer install operating system without activation with the licensed keys, there will be a high risk to become infected at any time.

5.3 Sufficient Backups

Taking offline backup by using external hard drive, tape drive and any other PC that is not connected to the internet and network are the best way to prevent loss of sensitive and important data from individual to the corporate levels. Having online backup through cloud storage can also make the data secured during ransomware attacks. Because the cloud companies configured their network infrastructure and datacenters with proper security for their clients. Although, in recent year there is an increasing trend of sophisticated ransomware attacks are specifically targeting backup data and administrator functions. If the datacenter servers are not configured in a secured with a system of strong authentication and communication between the server and the user, it will be a high risk for the data. However, taking proper regular (full and incremental) backup is one of the ways to prevent data loss in ransomware attack.

5.4 Regular auto update of Security Patches

Every operating system is now very concern about their market reputation in this competitive software arena. For this reason, they are continuously releasing their patches, security updates and improving features to ensure security, integrity, and scalability of their

clients. Regular and auto updating the computers with the latest security patches can protect users from any attack of ransomware and making a strong shield against it by eliminating possible risks and vulnerabilities on it. Outdated operating system software is the main target of hackers to sneak into the system by taking advantage from those weakness of loop faults and holes.

5.5 Enabling Firewalls

Either Linux or Windows configuring and enabling strong firewall is the key to protect systems from any kinds of external attacks. This experiment demonstrated that when firewall policies were disabled, ransomware executed and encrypted files. Inbound, outbound, forwarding and routing firewall need to be configured in layer three level to protect the computers from dangerous ransomware attack.

5.6 Multi factor Authentication

Due to the acceleration of digitalization in every sector from personal email, social networking, online education, e-governance, e-commerce to online banking users are now running their most of the activities through internet. The risk zone for exploiting from these areas have increased tremendously. Therefore, using multi factor authentication technique become imperative to prevent billions of users from being attacked by ransomware and other viruses.

5.7 Network Segmentation

Designing and configuring the network with a logical segmentation in layer three level is also can reduce risk of being attacked by ransomware and to keep safe the network nodes from any kinds of external attack. The network should be segmented into subnets with local private IP instead of public IP because hackers usually target, scan and attack on public

routed IP. If the total network is configured into different subnets and the firewalls applied on the public IP or router, there will be less possibility to be infected by the ransomware viruses.

5.8 Secured network communication

Data transfer within the network through shared folder or file server should be secured channel. If files upload and download perform in encrypted way, nobody can open it or attach any virus script with it. There are many ways to secure the network and file sharing through encrypted protocols like MD5, MS CHAP, MS CHAP-2 etc. Furthermore, some cybersecurity companies such as **Cisco, Palo Alto, Fortinet** etc. have developed strong hardware firewalls that can prevent any kinds of virus attack including ransomware. Such security intelligent applications are Advanced Malware Protection (AMP), Palo Alto Next generation firewalls, Palo Alto Zero Trust Firewalls etc.

5.9 Providing Training for awareness

Users are not aware of the possible vulnerability by which the ransomware can attack to their systems. If a corporate company provide sufficient training to their users about possible risk factors and users do not download any unauthorized software or applications comply with these compliances, their system will be secured from these kinds of disastrous infections. Paul Webber, Senior Director Analyst of Gartner says "Use cyber crisis simulation tools for mock drills and training that provide closer to real-life situations for better preparedness of end users against ransomware. (Paul Webber, 2020)".

5.10 Configuring and Auditing Security Policies

Configuring a well design necessary domain and local level security policy is also another way to protect domain controllers and workstations from possible ransomware attack. Conducting frequent testing exercises of that policies including password policy, system

policy and auditing of that events at regular intervals to check for vulnerabilities, noncompliant systems and misconfigurations are the essential part of being attacked by a serious virus infection.

5.11 Installing Defender or Antivirus

Although there is a rumor that those who develop virus, marketed the antivirus software too by them. However, in this project it was excavated that the built-in security features like Windows Defender, file system ownership and permission in Linux are enough to protect computers from any kinds of virus attack. If users become aware, enable security features it is difficult to become attacked by ransomware. Moreover, installing renown licensed antivirus can add extra strength to defend any kinds of viruses.

Chapter-6

Future Research

There are over 50 variants of ransomware, and the cybercriminals are continuously developing more smarter way to attack users to earn more illegal money. This project only focused on how user become attacked and what are the effective ways to prevent themselves form this dangerous virus. To implement this research questions two executable encryptor and decryptor were developed in Visual Studio Dot Net and python programming language and tested as well. However, recent ransomware attack shows that a simple MS Word invoice from a shop can be a dangerous virus. If user open his invoice of a purchased product, his/her computer may be hacked silently in background and all files could be encrypted. So, this newly developed ransomware can be explored in the future research for the protection of the users.

Chapter-7

Problems faced on the Project

Analyzing security thread is also a big challenge because there is a possibility to being attacked while making ransomware scripts, running these executables files and decrypting it. During the testing phase, although all of the experiments was done in virtual environment, however, transferring virus files was difficult through shared folder as this folder physically located on the real environment. After receiving suggestions from the supervisor, a website has been hosted and configured an FTP server to download ransomware virus files from one virtual machine to another. However, after uploading files through client application software, the less secured hosting company blocked this FTP site for ransomware detection. Later on, there were several attempts to transfer virus files through the Google Mail and failed because it detects as a harmful file. At last, risky virus transfer was accomplished through Google Drive after changing the filetype from .exe to .txt and renamed again after downloading to the target machines.

Chapter-8

Consideration of ethical, legal, professional and social issues:

Although this project has not directly used the other persons as a primary source of analysis, there were no requirements for approval of the ethical and legal issues. After all, making ransomware malware for the research purpose for the welfare of the human beings is meet the compliance and the code of conduct of ethical hacking ***(Council, 2021)*** to identify the limitations by which ransomware can be attacked and to prevent them.

Chapter-9

Conclusion

Ransomware is known as the most popular Cybercrime in the world (Krunal, 2017). It has received considerable news coverage in recent years, in part due to several attacks against high-profile corporate targets. In 2020, Europol's annual Internet Organized Crime Threat Assessment report has consistently identified ransomware as a top priority (Europol, 2020). The dramatic rise of the ransomware attacks makes it more dangerous in recent years. This uprising trend sharply boosted during the Covid-19 global pandemic situation and affects all industries as banking sectors, corporate companies, government agencies, education, healthcare and shopping are mostly operated through online from home. The payments for returning data have also been increased due to the lack of precautionary measures. Cyber criminals are continuously upgrading their capabilities of creating, launching new format of viruses using machine learning, Artificial Intelligence, robotics and other latest technologies and making huge profits from this cybercrime threat to continue in the future. This is the high time to create awareness among the internet users and to protect their digital data and devices. This project, after practical demonstration, analysed different methods of prevention of ransomware. Although no single solution can completely protect an organization from ransomware attacks, however, combinations of these mentioned ways can ensure future security and integrity against any kinds of malware attacks. After visualization of ransomware experiments, it could be concluded here that the best way to protect from the individual home user to the multi-national corporate companies is to use licensed version of Operating System software with regular updated patches and security features. If the billions of users become safe and secure from these kinds of dangerous ransomware malware, this project will be a one-step forward to the milestone of building a highly skilled and technologically advanced global society.

Chapter-10

References

Works Cited

Aini Khalida Muslim et al. (2019). A Study of Ransomware Attacks: Evolution and Prevention. *JOURNAL OF SOCIAL TRANSFORMATION AND REGIONAL DEVELOPMENT VOL.1 NO. 1 (2019)*, 18-25.

Chhillar, P. (2017). Ransomware-Worldwide Cyber Attacker. 324–329.

Council, E. (2021). *Code of Ethics*. https://www.eccouncil.org/code-of-ethics/.

Emsisoft. (2020). *The state of ransomware in the usreport-2020*. USA: Emsisoft, a security solutions provider.

Europol. (2020). *Europol. Internet Organised Crime Threat Assessment*.

FBI. (2020). *Internet Crime Report 2020*. USA: FBI and Cybersecurity Venture.

Florian Malecki, S. (2019). *Best practices for preventing and recovering from a ransomware attack*. UK: Computer Fraud & Security.

Kristin Masuch et al. (2021). The Impact of Threat and Efficacy on Information Security Behavior: Applying an Extended Parallel Process Model to the Fear of Ransomware. *Proceedings of the 54th Hawaii International Conference on System Sciences | 2021*, (p. 6700). Hawaii.

Krunal, G. (2017). Survey on Ransomware: A New Era of Cyber Attack. *International Journal of Computer Applications, 168(3)*, 975–8887. Retrieved from https://pdfs.semanticscholar.org/71df/288033380d3023f09d49b7b55a77677d27a2.pdf

Morgan, S. (2017, Oct 16). 'Cybercrime Damages $6 Trillion By 2021'. *Cebersecurity Ventures*. Retrieved 2019, from https://cyber securityventures.com/hackerpocalypse-cybercrime-report-2016/

Nik Simpson, R. B. (Jan 2021). Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware. *Gartner, ID G00733304*.

Paul Webber, S. D. (2020). *How Security and Risk Leaders Can Prepare for Reduced Budgets*. Gartner, Senior Director Analyst, Gartner. Gartner Report. Retrieved from https://www.gartner.com/smarterwithgartner/how-security-and-risk-leaders-can-prepare-for-reduced-budgets/

Richardson, R. &. (2017). Ransomware : Evolution , Mitigation and Prevention. *Informing Science & Information Technology*, 10–21.

Singh, A. (2021). *Ransomware: How to Prevent or Recover From an Attack*. USA: Backblaze.

Steve Morgan, E.-i.-C. (2019, Feb 6). 2019/2020 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. *Cybersecurity Almanac*.

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., &Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications, 24(3), 10-16.

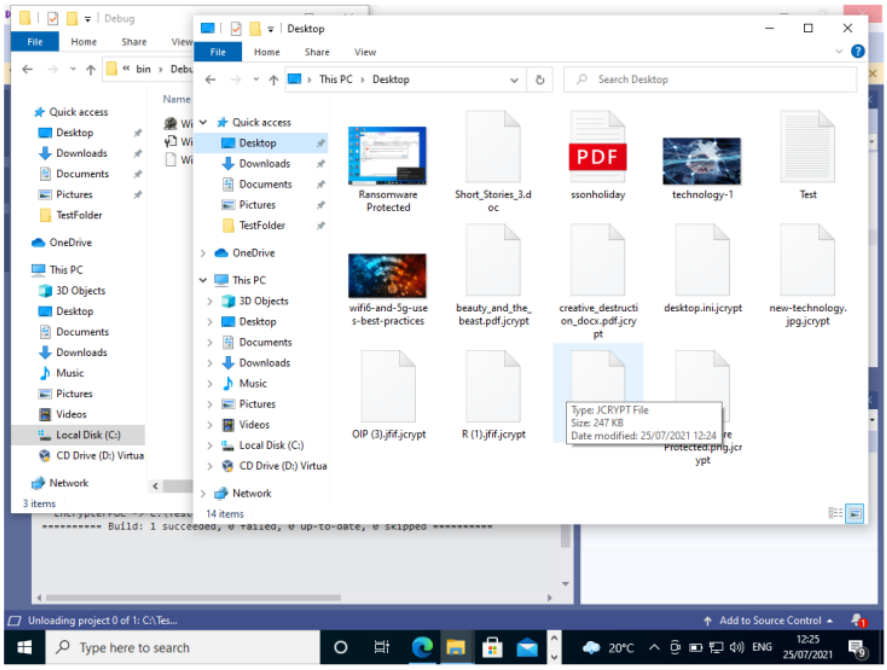
Zhanhui, L., Azlina, N., & Rahman, A. (2017). A Review on Ransomware Trend of Attacks and Prevention, 12(16), 6201–6210.

Sophos. The State of Ransomware 2020: Results of an independent survey across 26 countries, 2020. https://www.sophos.com/en-us/medialibrary/ Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Richet, J. L. (2016). Extortion on the internet: the rise of crypto-ransomware. Harvard.

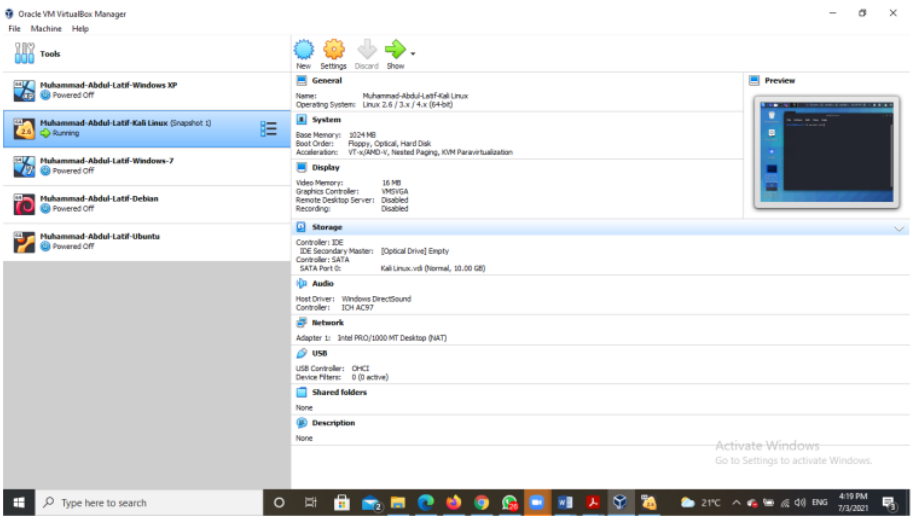
Chapter-11

Appendices:

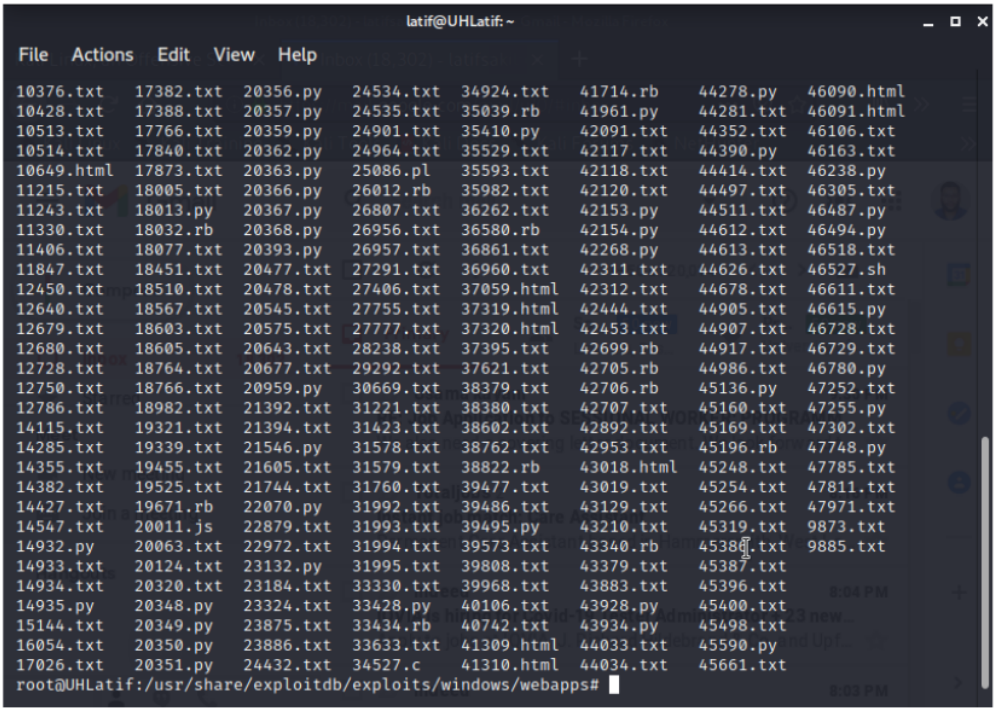


Appendices-1: APplications

Appendices-2: Experiment on Virtual Environment



Appendices-3: Analyzing Security Thread



19054557MScFinalPRojectReport-1.docx

ORIGINALITY REPORT

16%	15%	4%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	publisher.uthm.edu.my Internet Source	3%
2	www.backblaze.com Internet Source	2%
3	coek.info Internet Source	2%
4	global.oup.com Internet Source	1%
5	www.asianssr.org Internet Source	1%
6	www.gartner.com Internet Source	1%
7	scholarspace.manoa.hawaii.edu Internet Source	1%
8	www.ijcaonline.org Internet Source	1%
9	Submitted to University of Hertfordshire Student Paper	<1%

10	Submitted to University of Bolton Student Paper	<1%
11	Rhythima Shinde, Pieter Van der Veeken, Stijn Van Schooten, Jan van den Berg. "Ransomware: Studying transfer and mitigation", 2016 International Conference on Computing, Analytics and Security Trends (CAST), 2016 Publication	<1%
12	Submitted to Bournemouth University Student Paper	<1%
13	academic.oup.com Internet Source	<1%
14	Submitted to University of Sunderland Student Paper	<1%
15	Submitted to Campbellsville University Student Paper	<1%
16	www.eyetrodigital.com Internet Source	<1%
17	core.ac.uk Internet Source	<1%
18	Submitted to Macquarie University Student Paper	<1%
19	Submitted to Mesa State College Student Paper	<1%

20	Submitted to Bridgepoint Education Student Paper	<1 %
21	Submitted to University of New Haven Student Paper	<1 %
22	Submitted to University of Petroleum and Energy Studies Student Paper	<1 %
23	www.usenix.org Internet Source	<1 %
24	Submitted to Flinders University Student Paper	<1 %
25	Submitted to University of Portsmouth Student Paper	<1 %
26	William Panek. "MCSA Windows Server 2016 Complete Study Guide", Wiley, 2018 Publication	<1 %
27	Submitted to Northcentral Student Paper	<1 %
28	hdl.handle.net Internet Source	<1 %
29	Submitted to American Public University System Student Paper	<1 %
30	Gerda Bortsova, Cristina González-Gonzalo, Suzanne C. Wetstein, Florian Dubost et al.	<1 %

"Adversarial attack vulnerability of medical image analysis systems: Unexplored factors", Medical Image Analysis, 2021
Publication

31	docplayer.net Internet Source	<1%
32	www.yumpu.com Internet Source	<1%
33	www.uni-due.de Internet Source	<1%
34	www.knowbe4.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		