COMPARATIVE ANALYSIS OF CONTEMPORARY RANSOMWARE

A PROJECT REPORT

Submitted by

Avantika Krishnan (20BCY10028)
Arundhati Menon (20BCY10031)
Aditi Kurutala (20BCY10006)

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE and ENGINEERING
(SPECIALIZATION IN CYBER SECURITY AND DIGITAL FORENSICS)

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

VIT BHOPAL UNIVERSITY

KOTHRIKALAN, SEHORE
MADHYA PRADESH - 466114

DECEMBER 2021

VIT BHOPAL UNIVERSITY, KOTHRIKALAN, SEHORE
MADHYA PRADESH – 466114

BONAFIDE CERTIFICATE

Certified that this project report titled COMPARATIVE ANALYSIS OF CONTEMPORARY RANSOMWARE is the bonafide work of AVANTIKA KRISHNAN (20BCY10028), ARUNDHATI MENON (20BCY10031), ADITI KURUTALA (20CBY10006) who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

PROGRAM CHAIR	**PROJECT GUIDE**
Dr. R. Rakesh, Assistant Professor	Mr. Suryakanta Panda, Assistant Professor
School of Computer Science and Engineering	School of Computer Science and Engineering
VIT BHOPAL UNIVERSITY	VIT BHOPAL UNIVERSITY

The Project Exhibition I Examination is held on _______________

ACKNOWLEDGEMENT

First and foremost, I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to Dr. S. Poonkuntran, Head of the Department, School of Computer Science and Engineering for much of his valuable support encouragement in carrying out this work.

I would like to thank my internal guide Mr. Suryakanta Panda, for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School of Computer Science and Engineering, who extended directly or indirectly all support.

Last, but not least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

i. LIST OF ABBREVIATIONS

ABREVIATION	EXPLANATION
RSA	Rivest-Shamir-Adleman
RC4	Rivest Cipher 4
CVE	Common Vulnerabilities and Exposure
MBR	Master Boot Record
RAAS	Ransomware as a Service
C2C	Command and Control
API	Application Programming Interface
VM	Virtual Machine
GB	Gigabyte
SMS	Short Message Service
CTU	Counter Threat Unti
XRP	Cryptocurrency token of Ripple
BTC	Bitcoin
ITU	International Telecommunication Union
AI	Artificial Intelligence
AIRaD	AI-based Ransomware Detection
USB	Universal Serial Bus
RISC	Reduced Instruction Set Computer
DNA	Deoxyribonucleic acid
DLL	Dynamic Link Libraries
CPU	Central Processing Unti
FP	Frequent Pattern
DCR	Represents the DLL chain ratio
FCR	Represents a function call chain ratio
ACR	Represents the assembly chain ratio
MPCR	Represents the ransomware profiling chain ratio
MNC	Multinational corporation
AIDS	Aids Info Disk
FBI	Federal Bureau of Investigation
RDP	Remote Desktop Protocol
US	United States
EU	European
SIEM	Security information and event management
UKG	Ultimate Kronos Group
HR	Human Resources

ii. LIST OF FIGURES AND GRAPHS

iii. LIST OF TABLES

iv. ABSTRACT

The past decade has seen an exponential rise in large-scale Ransomware attacks on various organizations and multinational companies. The purpose of such attacks varied from financial gains through malicious methods to affecting the company's asset value by locking out or selling the company's consumer database, thus compromising sensitive information. Among the countless ransomware attacks occurring globally, each ransomware differs from its predecessor and due to this constant shift being observed in attack patterns in computer systems across the world, as cyber security students, our team decided to elucidate the repercussions and aftermath of this change on global computer security.

This research paper aims to recognize the parameters which differentiate one Ransomware from another. Based on the discussed parameters, we establish a comparison between modern Ransomware attacks through surveys and analysis of existent research papers and data released by the victim organization. The results of a survey conducted by the team regarding the general awareness of people on most recent and impactful ransomware attacks over the past decade will also be presented as a highlight of this project paper. We shall also shed light upon the mode of distribution of recent Ransomware attacks and compare it with a previous large-scale attack through case studies.

TABLE OF CONTENTS

CHAPTER-1:

PROJECT DESCRIPTION AND OUTLINE

1.1 INTRODUCTION

Ransomware is a malware that restricts access by encrypting files in an attempt to extort money or ransom, usually in the form of cryptocurrency. This cyber threat is an increasingly rising global issue. Constant modifications and advancements make older platforms susceptible to Ransomware attacks. This is why Cybersecurity researchers are constantly testing and modifying various systems. For instance, from the month of June to November 2017, Windows 7 devices were 3.4 times more vulnerable to encounter ransomware, compared to Windows 10 devices.

1.1.1 What does Ransomware do?

Most types of Ransomwares encrypt files using encryption algorithms like RSA, or RC4, which are very hard to break. Some Ransomware like Cerber and Locky search and encrypt target files. When encryption is complete, the malware leaves a ransom note, which will include instructions on how to pay it. Advanced ransomwares like Spora, WannaCry and NotPetya include other capabilities, like spreading to other computers via network shares or exploit.

Older ransomware like Reveton doesn't encrypt files but instead locks the screens. They do this by displaying an image on the screen and then disabling Task Manager. The files are safe but become inaccessible. The image will contain a message from law enforcement that the computer was involved in illegal cybercriminal activities and that a fine needs to be paid. For this reason, Reveton has also known as Police Trojan or Police ransomware.

1.1.2 How does a Ransomware infection occur?

The following vectors can play a role in Ransomware infection -:

1. Downloader Trojans carried via email messages. They attempt to install Ransomware.

2. Exploit kits use vulnerabilities in web browsers and other software to install Ransomware. Usually, they are hosted by Websites.
3. Recent ransomware has worm-like capabilities. It enables them to spread to other computers in the network. For example, Spora releases ransomware copies in network shares. To infect other computers WannaCrypt exploits the Server Message Block (SMB) vulnerability CVE-2017-0144, also called EternalBlue. A Petya variant has the ability to exploit the same vulnerability along with CVE-2017-0145, also called EternalRomance, and uses stolen credentials to move laterally across affected networks.

1.1.3 How big is the ransomware problem?

Ransomware has become a lucrative source for cybercriminals. These attacks are not necessarily launched by individuals. It could be planned by a group of skilled people. An even major threat is ransomware-as-a-service (RaaS). RaaS is a cybercriminal business model, where malware creators can sell their ransomware to any buyer, who then operates the ransomware attacks. The business model also defines profit sharing between all the parties involved.

Ransomware is constantly evolving. It has progressed and become a large-scale cyber threat. Thousands of variants are being produced from older versions which are damaging. Analysis of this rise will help us be informed and tackle obstacles thrown our way.

1.2 MOTIVATION FOR THE WORK

Recent times have seen a surgical expansion in the number of ransomware attacks globally, raising multiple issues concerning the security of one’s confidential information in the digital world. Financial gains, disrupting crucial public or private services, or destabilizing a firms' network are few of the major intentions of malicious hacker groups who infect computer systems with dynamic and alternating variants of ransomware and cause panic and chaos all over the world.

As computer engineering students pursuing cyber security as a specialization, it is crucial to understand the basis and premises under which a particular cyber-attack on a system or network of systems is carried out and to prevent large-scale disruptive attacks on pivotal organizations. In order to fulfill this assignment and perform necessary duties towards our goal of a secure computer network, we must be aware of the past and present of the problem in order to shield ourselves and proper arrangements for the future.

1.3 ABOUT PROJECT

In this survey we have reviewed several research papers based on ransomware and related works. Through this research-based report, we aim to review the damage caused by ransomware attacks over the years with the help of graphs and reliable statistics in order to highlight the difference between contemporary attacks on systems and the variants preceding them based upon some common grounds which will be referred to as parameters. Through a series of thought-provoking questions, we shall highlight the general awareness of the public on ransomware and the methods individuals or organizations must adopt to prevent large-scale ransomware from affecting and damaging sensitive information.

1.4 PROPOSED WORK

Seeing the exponential rise in the number of ransomware attacks on numerous organizations, both large-scale and small-scale, our team conducted a comparative survey analysis by reviewing the biggest ransomware attacks and distinguishing between contemporary ransomware and their predecessors, and discuss upon the impact these attacks had on the target information.

We shall also shed light on the causes of the problem along with discussing the solutions we can adopt in order to secure our systems from contemporary ransomware attacks.

1.5 OBJECTIVE OF WORK

This project will review the damage caused by ransomware attacks, compare and analyze large-scale malicious cyber-attacks from over the past decade with contemporary ransomware, and how the affected organizations dealt with the circumstances.

1.6 ORGANIZATION OF WORK

The project is divided into various components among which are a collective review of authentic and riveting research papers from the past decade on ransomware and its impacts over different sectors and organizations along with a general awareness survey conducted by the team members to captivate the audience and help them enhance their awareness around ransomware. Comparative analysis-based case studies were also researched upon and mentioned in the paper which describe how and on what parameters contemporary ransomware differ from their predecessor.

Chapter 1 deals with the project introduction and how the ransomware has risen to be the most fearsome of all cyber-attacks to occur globally, what it does to system files, what infection vector is followed by a particular ransomware attack and how it infects and spreads across the computer are all elaborated throughout the chapter.

Chapter 2 provides detailed insight and reviews recent research papers released on ransomware and establishes its findings through graphs, flowcharts and figures created by the team members.

Chapter 3 aims to clearly establish the points or parameters which form the foundation of our comparative analysis of contemporary ransomware. The distinction of these parameters has been illustrated through tables prepared by the members along with preparing a helpful guide on the timeline to remove ransomware and its remnants from the system.

Chapter 4 highlights the technical implementations of our report through case studies and comparative case studies completed with tables of distinction between two ransomwares based on the parameters discussed in chapter 3.

Chapter 5 spotlights the results of a general survey conducted by the team members on the awareness of the public on the growing problems and threats of ransomware. The results were collected through a Google form created by the team members and were accumulated in the form of pie charts.

Chapter 6 draws conclusion to the report by summarizing the crucial points covered in the report and provides precautionary measures to help undo the after-effects of a ransomware attack or prevent it from occurring completely.

1.7 SUMMARY

This project report will highlight an elaborative study of contemporary ransomware variants and establish a distinction between modern ransomware and its previous variants through surveys, graphs, recent statistics, and comparative in-depth analysis and explanation in a real-world context.

CHAPTER-2:

RELATED WORK INVESTIGATION

2.1 INTRODUCTION

Under this section we reviewed existing papers on ransomware that will provide us with an insight into our own topic. We analyzed various papers belonging to a variety of categories related to ransomware. Detailed investigation was done on a particular ransomware called WannaCry, research on solving challenges currently faced was analyzed and even simple definitions of ransomware and its evolution were looked into.

This study will help us gain knowledge about how much ransomware has changed, and make us realize the threat it poses on our future. Industries all around the world right now are under the radar for a ransomware attack. One strike is all it needs to bring down an organization to its knees. Which is why constant research, awareness and consciousness is required.

2.2 LITERATURE REVIEW

The study by Jinal P. Tailor Et al. [1] elaborates on the different prevention methods to adopt while a ransomware attack occurs and conducts a comprehensive survey on the detailed methods of monitoring ransomware and damage control for affected system and files. He describes ransomware as a malicious code that encrypts data to lock us out of our system. To make our system accessible and save our data, the ransom will be required to be paid, usually as Bitcoin. Common methods of spreading ransomware -

1. Phishing emails
2. Malicious Websites
3. Drive-by Downloads

Ransomware has become more bothersome as they sometimes threaten to expose sensitive information. Industries around the world are right now facing this issue.

Once ransomware infects a computer it communicates with the Command-and-Control server. These servers might be directly controlled by malware writers or themselves have been compromised. The victim's information is sent to the server, and the computer receives an encryption key. While the malware deletes backup folders and shadow volume copies, which help in restoring data in the system, the variant looks for data to encrypt. After the entire encryption procedure, a ransom note will be displayed.

A brief idea about the history of ransomware has been presented via the **Fig 2.2.1**

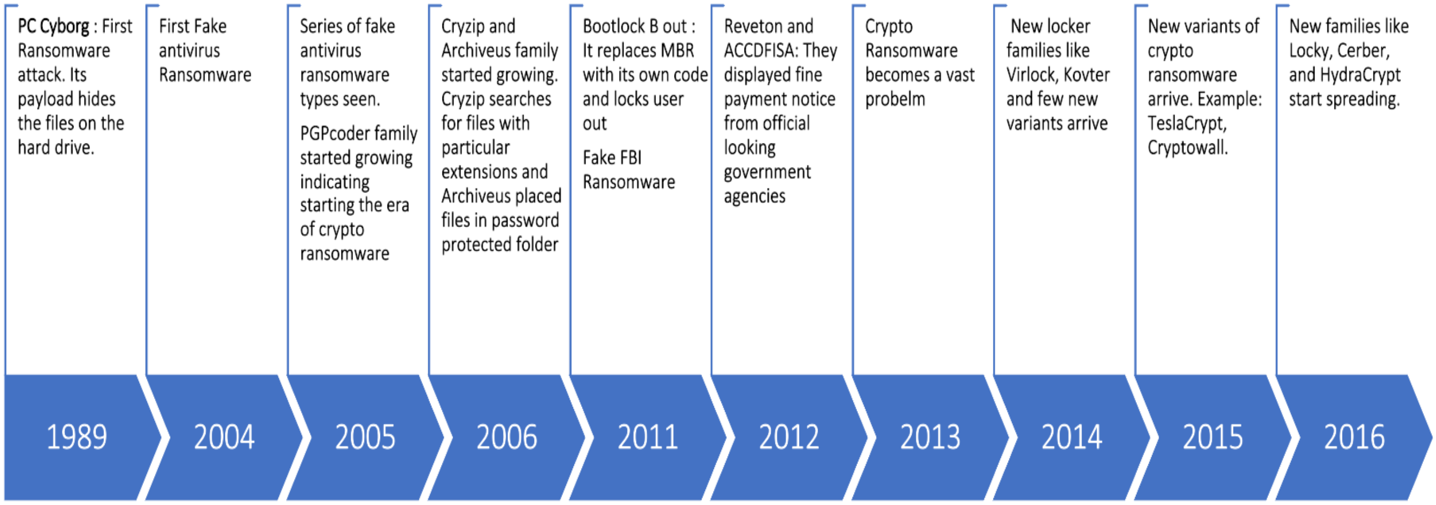

PC Cyborg : First Ransomware attack. Its payload hides the files on the hard drive.
1989
First Fake antivirus Ransomware
2004
Series of fake antivirus ransomware types seen.
PGPcoder family started growing indicating starting the era of crypto ransomware
2005
Cryzip and Archiveus family started growing. Cryzip searches for files with particular extensions and Archiveus placed files in password protected folder
2006
Bootlock B out : It replaces MBR with its own code and locks user out
Fake FBI Ransomware
2011
Reveton and ACCDFISA: They displayed fine payment notice from official looking government agencies
2012
Crypto Ransomware becomes a vast probelm
2013
New locker families like Virlock, Kovter and few new variants arrive
2014
New variants of crypto ransomware arrive. Example: TeslaCrypt, Cryptowall.
2015
New families like Locky, Cerber, and HydraCrypt start spreading.
2016

Fig 2.2.1 Ransomware Evolution *(Source: Created using Smart Art)*

This paper provided us with useful insights into research papers on Ransomware attack. A few of the research paper have been mentioned in the **Table 2.2.1**

S.no	Title	Overview	Positive Aspects	Limitations
1.	Experimental Analysis of ransomware on windows and Android platforms and volution Characterization	It shows the Life Cycle and analysis of windows- based Ransomware and presents its evolution.	Using PEid tool ransomware was detected by monitoring abnormal file behavior.	To prevent loss of data, incremental online and offline backups is required.
2.	The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platforms	It discusses Ransomware prevention technique on Android platform, using a technique proposed, designed using three module - Configuration, Monitoring, Processing	The proposed can monitor file events of when the ransomware accesses and copies files	It does not need to install an application such as exiting prevention and reduce damage caused by unknown ransomware attacks.
3.	Protecting Your Networks from Ransomware	Methods like Remote Desktop and Software Restriction Policies are used. The main approach is to determine whether a mobile application can lock us out and encrypt data	Ransomware targets home users, business, and government networks and can lead to temporary or permanent loss of sensitive or corrective information.	The prevention measures are to set anti-virus and anti-malware programs to conduct regular scans.
4.	Unknown Malware Detection Using Network Traffic Classification	It presents an end-to-end supervised based system to detect malware by analyzing network traffic.	The proposed method analyzes DNS, HTTP, and SSL, protocols and combines different network classifications methods in different resolutions of network	Evaluated the effect of the environments on the performance

Table 2.2.1 Overview of Research papers *(Source: Created using SmartArt)*

This paper discusses some useful ways to detect and protect ourselves from ransomware. These tips can be useful for everyone and even protect us from becoming victims of ransomware.

Detection of ransomware

- Keep an eye on file extensions.
- Keep checking upon an increase in file renames.
- Create a sacrificial network share.
- Using anti-ransomware agents

Prevention of ransomware

- Backing up files regularly
- Not to carelessly open any unsolicited attachments
- Stay logged in as administrator only as long as needed.
- Avoid browsing as an administrator.
- A firewall should be turned on and updated.
- Regular antivirus scans should be performed.

The 2018 paper by A.K. Maurya Et al. [2] presents few facts about ransomware with its working and suggestion to save computers from attack. It features safety guidelines from ransomware that will be helpful to researchers as well as society to save data in near future. The review discusses ways of working and tricks to save our data during the attack. The study shows the light on various kind of infection performed by a ransomware including data infection and infected machine. The paper provides a sight on various target types of the ransomware. This paper tries to demonstrate few ransomware attacks case studies to show the problem created by various ransomware as an example. After an attack, what a victim should do after infection is also discussed at the end of the paper.

INFECTION BY RANSOMWARE

In this paper, the author lists 4 options a user has after his/her device is infected with ransomware:

- Pay the ransom
- Restore from backup
- Lose the files
- Brute force the key

It is also cited that to brute force, the key would require factoring 617-digit numbers, which would take about 6.4 quadrillion years on a standard desktop computer

TARGETS FOR RANSOMWARE

This paper classifies the targets for ransomware into two sections:

1. User-wise:
   - i. The Average User
   - ii. Businesses
   - iii. Emergency Services
   - iv. Financial Institutions
2. System-wise:
   - i. Personal Computers
   - ii. Mobile Devices
   - iii. Servers

SAFETY METHOD

The paper presented few suggestions to deal with ransomware to use before and after infection as:

Step 1: Back Up

Step 2: Avoid all spam and unknown links.

Step 3: Patch and Block

Step 4: Drop-and-Roll

Additional suggestions based on few case studies were derived as follows:

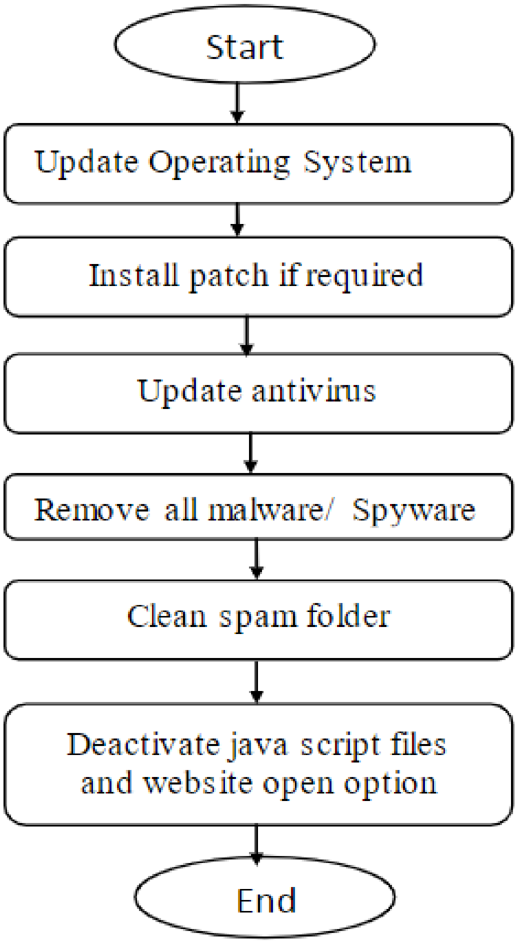

Start
Update Operating System
Install patch if required
Update antivirus
Remove all malware/ Spyware
Clean spam folder
Deactivate java script files and website open option
End

Fig 2.2.2 Flowchart to deal with ransomware

1.To save a system from ransomware attack first step to update the operating system, sometimes it requires the patches thus installation of patches is next step.

2.Do not use Operating System that is not supporting.

3.Tasks of step 1 are meaningless if the system does not have any updated antivirus, so it is a suggestion that system must have a good quality antivirus.

4.Cleaning of spam folder must be the next step after a removal of all malware/spyware.

5.Javascript files and website open option is risky so deactivate it at the end of all precautions.

Ransomware attacks are carried out on various platforms with each attack evading safety maneuvers taken by the victim operating system. The 2018 research paper by N. Hampton Et al. [3] present an analysis of 14 strains of ransomware that infect Windows platforms and do a comparison of Windows Application Programming Interface (API) calls made through ransomware processes with baselines of normal operating system behavior. The study identifies and reports salient features of ransomware as referred through the frequencies of API calls.

In this work, the authors have successfully identified Windows API calls that differ significantly in their usage between normal non-malicious operations and ransomware activities. The goal of this research was to investigate API calls that could allude toward ransomware infection.

The paper observes and finds that several versions of ransomware releases revealed that they were mostly copy-paste code from previous versions. Therefore, many of the limitations of one version were carried over to the next. In addition, several ransomware variants operated in unconventional ways. For instance, the Reveton ransomware, released in 2015, was found to merely lock the operation system's boot process without encrypting user data. Consequently, the ransomware activity was limited to disruption of operations and recovering user data without having to pay the ransom amount, was found to be easily achievable.

Another observed characteristic of recent ransomware traits is the ransomware procedural requirement to contact a centralized Command-and-Control (C2C) Server, once the victims' machine is infected, prior to encrypting the data. The C2C Server typically holds the cryptographic key required to decrypt the victim's data which has been held for ransom.

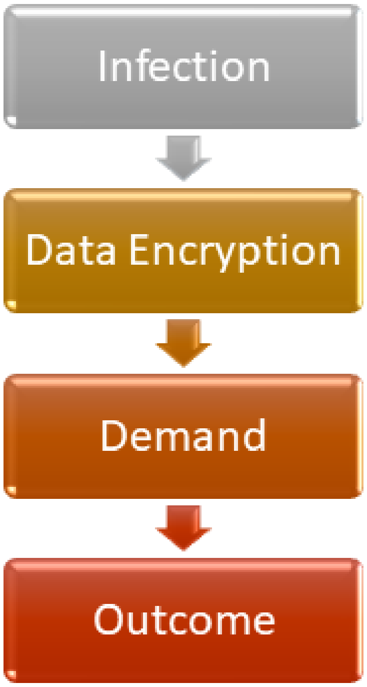


Figure 2.2.3 Stages of a ransomware-based attack

(Source: Created using Smart Art)

The paper states that ransomware activity must by nature follow specific patterns of behavior. These patterns include:

1. File identification process
2. Encryption of files
3. Network command and control communications
4. Use of anonymous networks

METHOD, SET UP AND PROCESS

Selection: Ransomware strains from recently circulated and well publicized ransomware variants from various online resources.

1. Analysis: Ransomware strains were analyzed based on their individual behavior patterns. Ransomware and normal (non-malicious) baseline operations were tested in successive experiments on a standardized Virtual Machine (VM).
2. Configuration: For each experimental test, we reset the VM to the same initial configuration, loaded a target test case, started the VM, logged Process Monitor events for a fixed duration of 10 minutes, and then halted the machine, and finally we exported the logged data and saved it for analysis.

File type	**Count of files in shared (network) folder**
jpg and png image files	1337
ppt (and pptx)	2
pdf	55
doc (and docx)	34
xls (and xlsx)	17
mp3/mp4 (audio and video media)	20
other filetypes	27
directory and subdirectory entries (maxdepth = 5)	31

Table 2.2.2 Shared folders (network) file counts

The total disk space was 25 GB with 13.5 GB used space.

A 32-bit Windows 8 Virtual Machine in a Virtual Box was created. This Test VM was provided with a firewalled Internet connection through an intermediate VPN router and firewall.

3. Automation: All ransomware tests were fully automated with the experimental tests execution and data collection scripted through a combination of BASH scripts, batch files and PowerShell scripts to ensure uniformity over each experimental test.

Automation element/method	Automated on Host or Guest	Description
Create PowerShell experiment execution control file	Host	Create a control file for use by Windows PowerShell on boot up –specifies the experiment to run, working directory and various other conditions
VirtualBox automation	Host	Use of BASH script and VirtualBox Manage commands to start/stop and reset VM snapshots
PowerShell scripts	Guest	Read the control file from a shared read-only resource to identify experiment's executable and run conditions
Shared filesystem	Host	BASH script to reset shared filesystem resources
Timed hard shutdown	Host	Hard shutdown of the guest VM and restart into data extraction mode
Data extraction	Guest and Host	Restart and launch ProcMonto recover boot time data. Save files and then move extracted files to a safe location for future analysis

Table 2.2.3 Technology and elements used for automation of texting

RESULT AND ANALYSIS

Of the 1262 calls to external functions across all experiments, 244 were present in ransomware which were further reduced to 209 calls by combining similar calls of ANSI and Unicode variants

The interesting calls identified included:

1. 8 API calls - only in ransomware at a significant level.
2. 4 API calls -in both ransomware and normal operations

The API call was statistically significant and more common in ransomware samples than in normal baseline operations.

3. 6 API calls - in both ransomware and baseline normal operation

The ransomware frequency count exceeded the baseline mean by more than three standard deviations (3σ).

Windows API Call	**Count of ransomware samples used**	**Count of baseline samples used**	**Usage differs between ransomware and baseline (Fisher exact P-value)**
InternetOpen	6	0	0.006
CryptDeriveKey	5	0	0.017
CryptDecodeObject	4	0	0.042
CryptGenKey	4	0	0.042
CryptImportPublicKeyInfo	4	0	0.042
GetUserName	4	0	0.042
NdrClientCall	4	0	0.042
socket	4	0	0.042
tailMerge_CRYPTSP_dll*	9	1	0.002
CoCreateInstance	8	1	0.005
SHWindowsPolicy	8	1	0.005

GetFileType	10	4	0.027

Table 2.2.4 Call to Windows APIs without considering call frequency – ransomware vs normal baseline operations

Windows API Call	**Call Count of ransomware samples using high ($\bar{x}$+3σ) frequency calls rates**	**Count of baseline samples using high ($\bar{x}$+3σ) frequency call rates**	**Significance (Fisher exact)**
CryptAcquireContext	7	0	0.002
CloseHandle	6	0	0.006
FindNextFile	6	0	0.006
SetFilePointer	6	1	0.035
GetFileSize	4	0	0.042
SetFileAttributes	4	0	0.042

Table 2.2.5 Calls to Windows APIs where ransomware call frequency exceeds baseline mean call frequency by more than 3 standard deviations.

The fisher-exact test of independence showed a remarkably elevated level of certainty that the baseline versus ransomware samples differed through a systematic process, namely, that the presence of ransomware in the system and not in baseline tests was not merely coincidental.

Based on the results reported in this paper, the authors provide a fundamental platform for researchers to examine methods of ransomware detection based on behavioural analysis and/or entropy-based analysis, for future research.

The research paper by Samir Thakkar [4] explored the depths of how ransomware works and how the attackers exploit the attack vector and pattern of ransomware to exploit vulnerabilities of an individual's or organization's digital network for financial gains. It describes various infection mechanisms used by attackers to commit ransomware attacks and provides an insight on the monetization pattern of such attacks and why they can be difficult to trace. A few general guidelines have also been highlighted for safeguarding against ransomware attacks.

The research paper was published in the year of 2014 and hence the statistics mentioned in the paper are now old and inexact. Hence, to clear this discrepancy in the accuracy if this report, the team decided to include the details of the statistics presented in the research paper and compare them with present statistics in order to put forward a refined interpretation of the paper.

The paper mentions the growth in the number of internet users globally through statistics and percentages. By the end of 2014, it was projected that 40% of the world population will become avid internet users which would increase to 44% by the end of 2016.

The statistics as of now show the increase in internet usage at a booming 51.4% in the year 2019. The year-wise trend of increase in the usage of internet worldwide is represented through **Figure 2.2.4**.

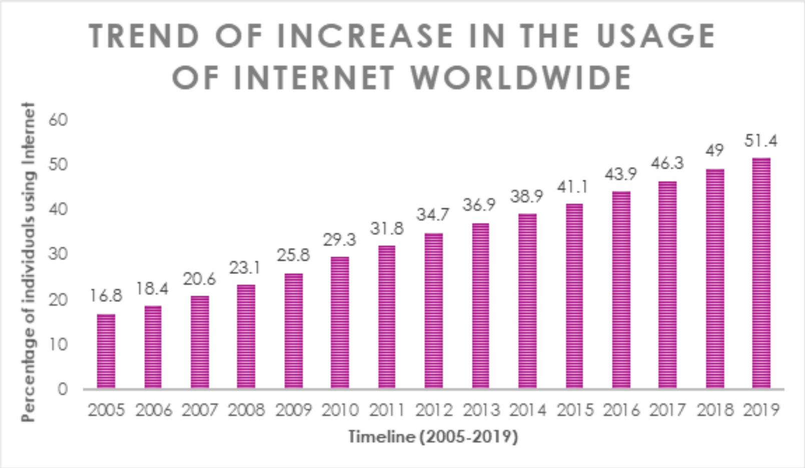


Fig 2.2.4 Increase in usage of internet worldwide *[Source: Created using SmartArt Microsoft Word 2019]*

According to a report by Symantec Corporation [2014] the cyber security breaches in 2013 were 62% more than that in the year 2012. Ransomware attacks grew by 500% in 2013.

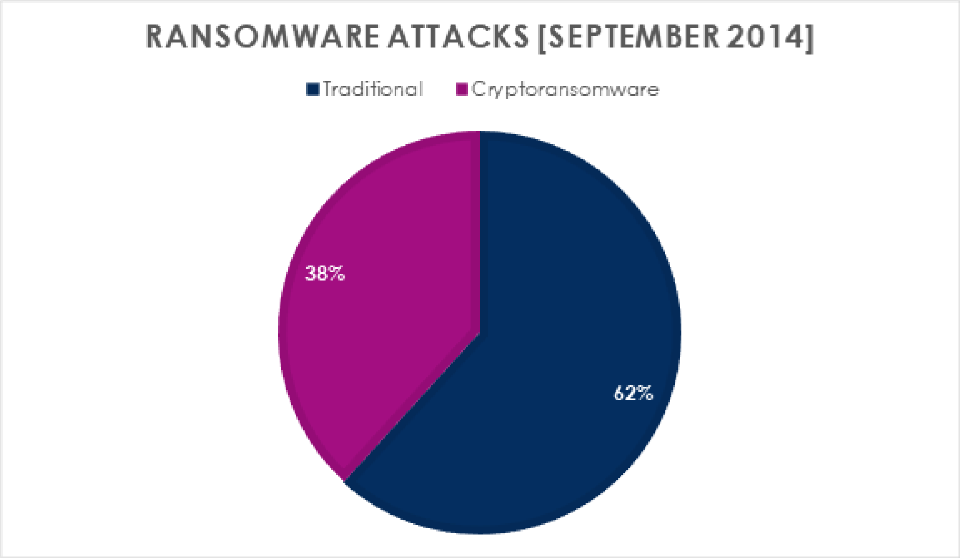


Fig 2.2.5 Type of Ransomware Attacks in September 2014 *[Source: Created using SmartArt Microsoft Word 2019]*

Figure 2.2.5 represents the types of attacks that occurred in the month of September of the year 2014.

Recent volume of the Internet Security Threat Report [ISTR-Volume 24] released by Symantec in February 2019, there was a drop observed in the number of ransomware attacks on individuals for the first time since 2013. A tip in the balance was also recorded as the attackers now targeted enterprises and organizations instead of individuals. This dramatic observation was made in the survey of the year 2017.

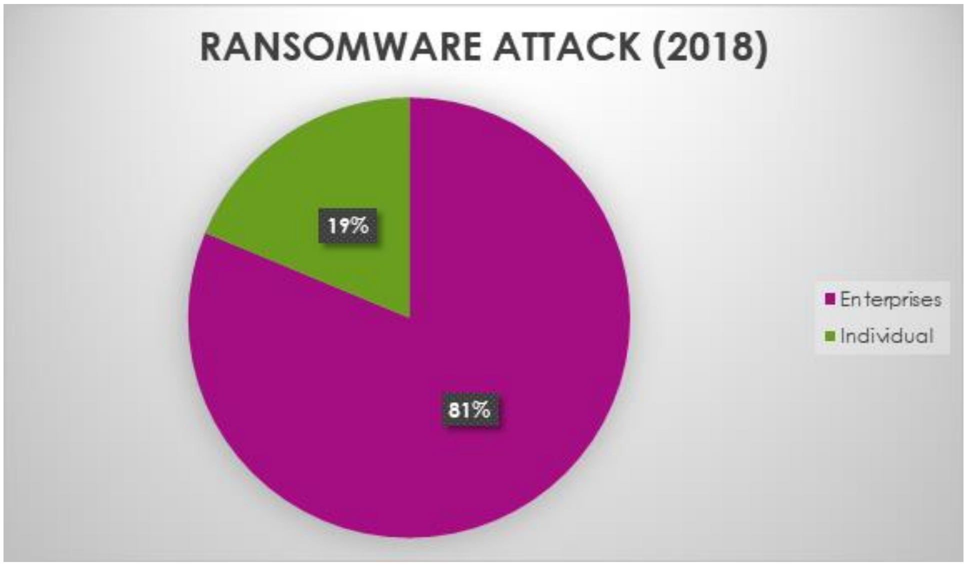


Fig 2.2.6 Categorization of victims of ransomware attacks in 2018 (*Source: Created using SmartArt Microsoft Word 2019)*

Figure 2.2.6 shows the acceleration of the above-mentioned shift in target in the year 2018 which accounted for 81% of all ransomware attacks. The report speculated that the reason behind this dramatic shift was due to the decline in exploit kit activity and the simultaneous introduction of a new distribution path. In 2018, the major attack path used were malicious email and attachments to distribute ransomware across computer networks.

The paper was distributed into 4 core sections which summarized the whole research.

- Known variants
- Monetization
- Mobile Devices – A New Target
- Mitigating Strategies

KNOWN VARIANTS

This theme describes the known families of ransomware and the paper draws conclusive differences between the discussed families of ransomware in terms of functionality and the amount of damage dealt to the affected system.

Figure 2.2.7 shows us the basic division of variants of ransomware mentioned in the paper.

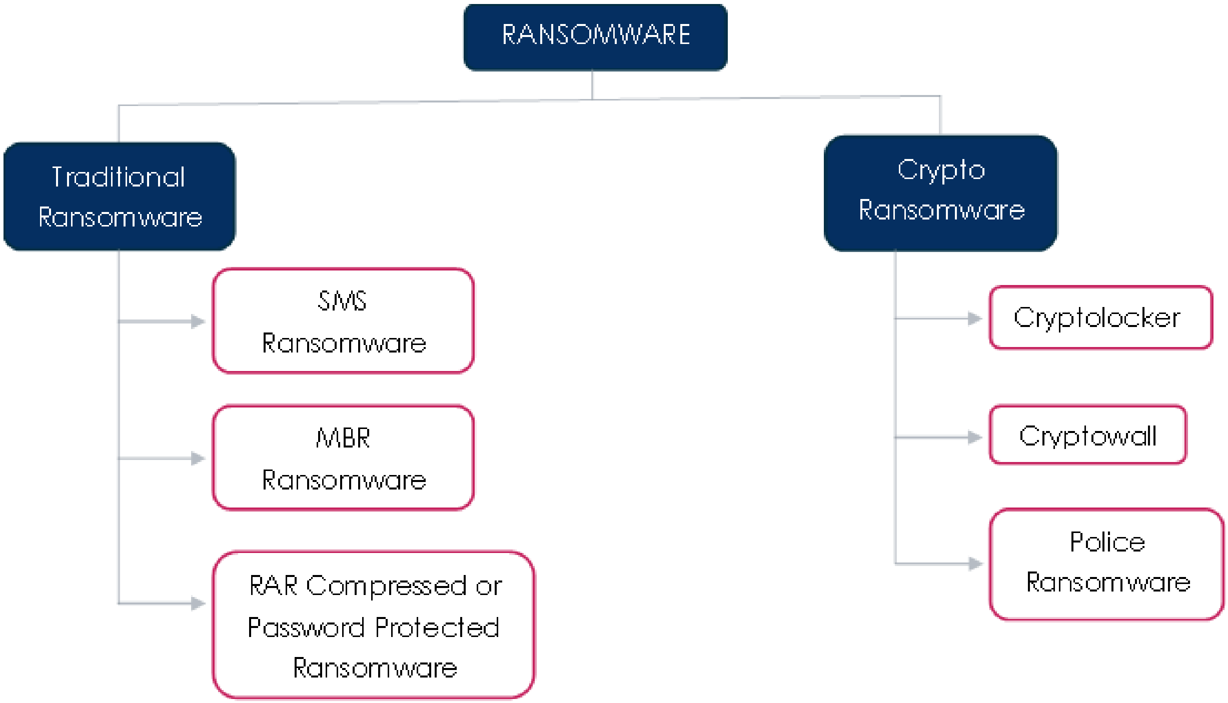


Fig 2.2.7 Types of ransomwares *[Source: Created using SmartArt Microsoft Word 2019]*

Traditional Ransomware

Traditional ransomware includes previous, simple versions of ransomware which blocks the users access to basic computer functions. The recovery of files and data is relatively easy and thus, the distribution of this ransomware is comparatively less than its crypto - styled variants.

SMS RANSOMWARE

- This ransomware is the earliest variant.
- The working of this ransomware is given step-by-step clearly in figure 2.2.8.

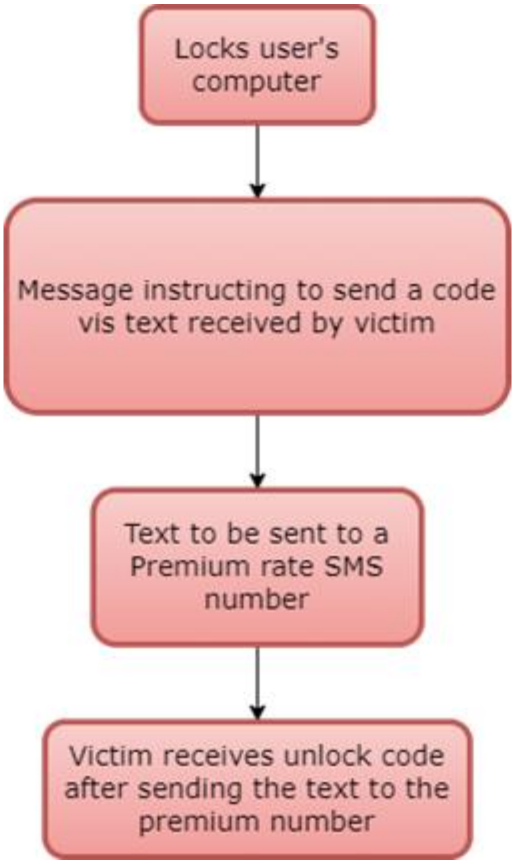

Locks user's computer
Message instructing to send a code vis text received by victim
Text to be sent to a Premium rate SMS number
Victim receives unlock code after sending the text to the premium number

Fig 2.2.8 Working of SMS ransomware *(Source: created on https://app.diagrams.net/)*

- Here the cost of the Premium rate SMS is the ransom.

MBR RANSOMWARE

- Infects the Master Boot Record of file system.
- A master boot record (often shortened as MBR) is a kind of boot sector stored on a hard disk drive or other storage device that contains the necessary computer code to start the boot process.
- Falsely claims to encrypt data files.
- Ransom is demanded to decrypt files.

RAR COMPRESSED or PASSWORD PROTECTED RANSOMWARE

- The basic functionality of this ransomware is completely different from any of its predecessors.

- Instead of encrypting files of the user, RAR compressor ransomware compresses all target files into one password protected file.
- The compressed files are removed from their original locations and can only be accessed through the password protected folder.
- Ransom is demanded in exchange of the password.

Crypto Ransomware

The aim of crypto ransomware is to encrypt your important data, such as documents, pictures and videos, but not to interfere with basic computer functions. This spreads panic because users can see their files but cannot access them.

CRYPTOLOCKER

- Method of Deliverance:
- Spear Phishing
- Watering hole attacks
- Drive-by downloads
- The working of this ransomware is given step-by-step in **Figure 2.2.9**.

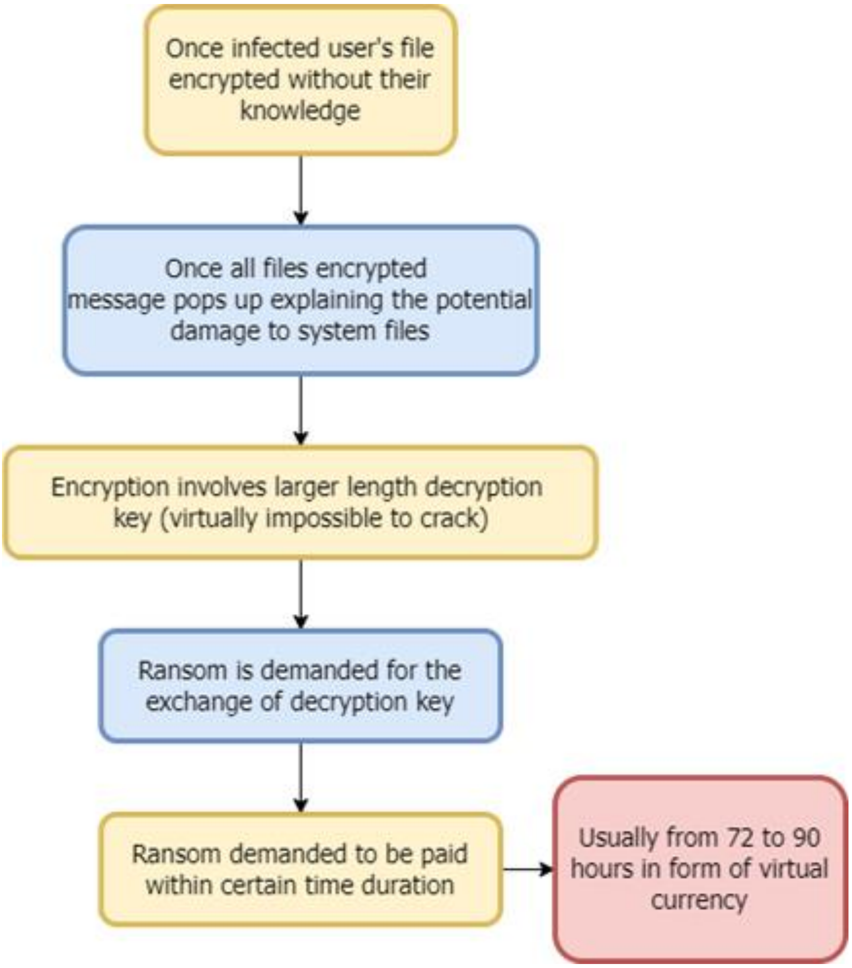

Once infected user's file encrypted without their knowledge
Once all files encrypted message pops up explaining the potential damage to system files
Encryption involves larger length decryption key (virtually impossible to crack)
Ransom is demanded for the exchange of decryption key
Ransom demanded to be paid within certain time duration
Usually from 72 to 90 hours in form of virtual currency

Fig 2.2.9 Working of Cryptolocker ransomware *(Source: created on https://app.diagrams.net/)*

- This ransomware was first distributed globally by the Gameover Zeus botnet which was shut down in May 2014 and the impacted regions were highlighted in **Figure 2.2.10**.

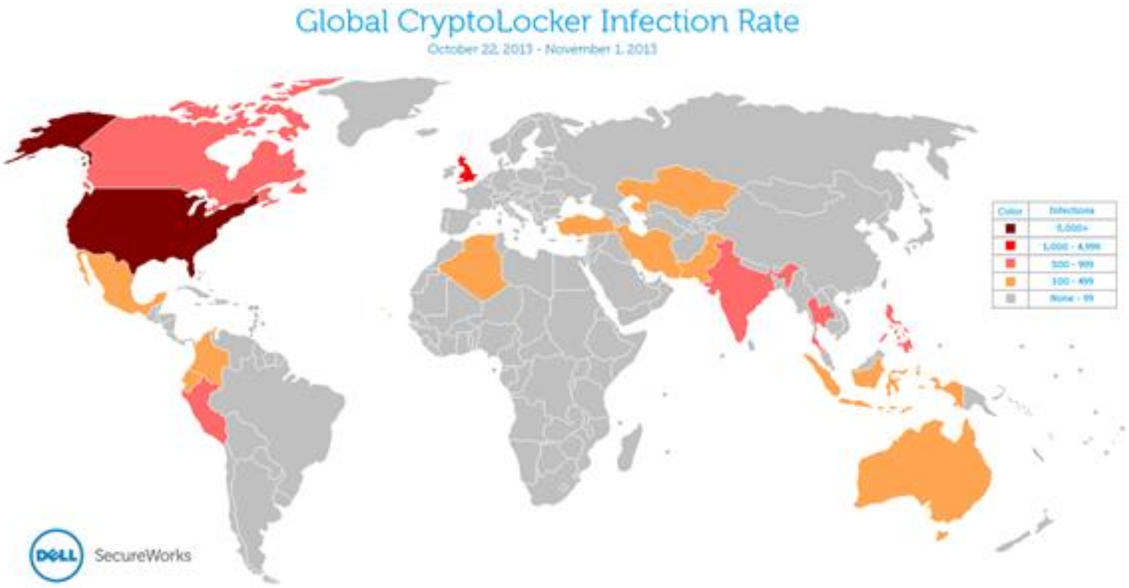


Fig 2.2.10 Global infection rate of Cryptolocker ransomware

CRYPTOWALL

- A mimic of the Cryptolocker ransomware but substantially more destructive.
- Follows infection vector to spread across systems
- Method of Deliverance:
- Browser-exploit kit
- Drive-by downloads
- ❖ Malicious e-mail
- ❖ Cyrptowall follows various infection mechanisms.
- ❖ Was distributed through a malicious download link spread by Cutwail Spam botnet.

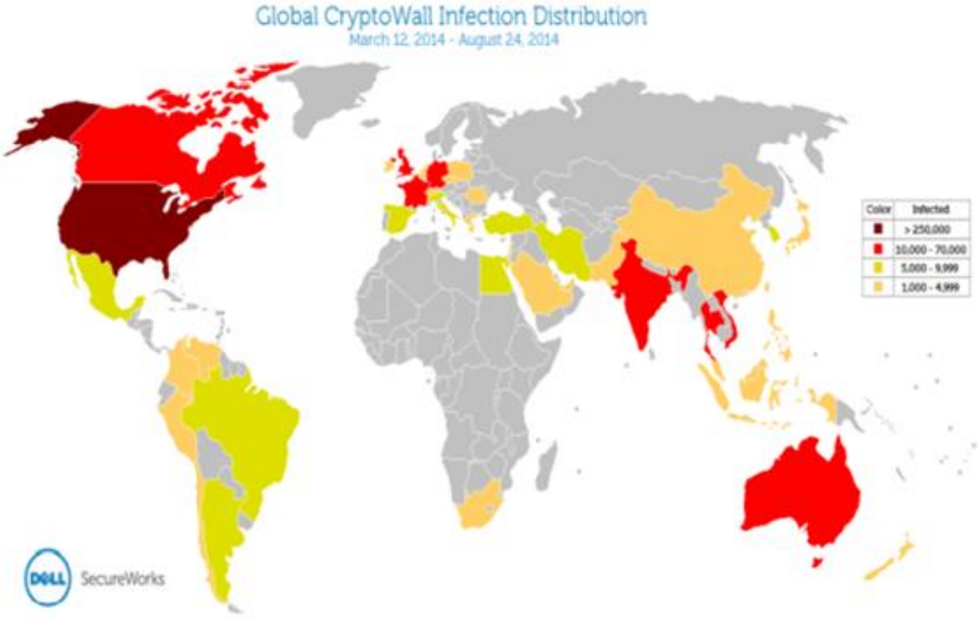


Fig 2.2.11 Infection distribution of Cryptowall ransomware

- **Figure 2.2.11** shows the distribution of the Cryptowall ransomware globally. It was observed that the activity of Cryptowall grew around mid-May 2014. [Report by Dell SecureWorks Counter Threat Unit {CTU} (February 2014 – May 2014)].
- CTU researcher observed 40.6% infected systems in United States.

POLICE RANSOMWARE

- This ransomware has a unique mode deliverance as it spreads itself through web advertisements shown on legitimate websites.
- The flow of attack of police ransomware is illustrated below in **Figure 2.2.12**

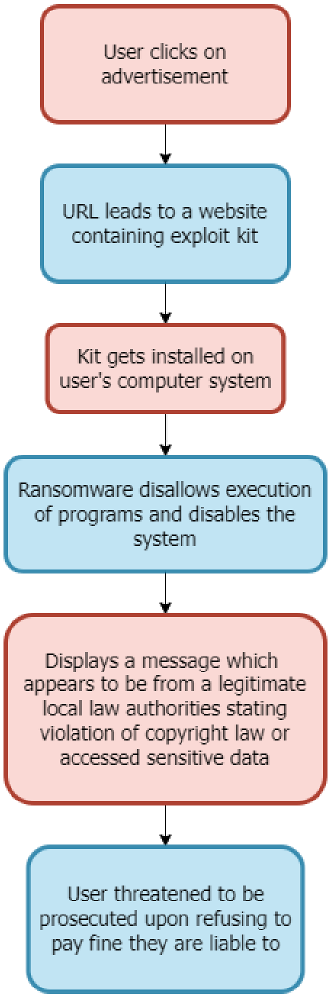

User clicks on advertisement
URL leads to a website containing exploit kit
Kit gets installed on user's computer system
Ransomware disallows execution of programs and disables the system
Displays a message which appears to be from a legitimate local law authorities stating violation of copyright law or accessed sensitive data
User threatened to be prosecuted upon refusing to pay fine they are liable to

Fig 2.2.12 Working of Police ransomware *(Source: created on https://app.diagrams.net/)*

MONETIZATION

This section was quite unique to the paper as it discusses, in elaborate details, the process followed by various attackers to receive financial gains from ransomware attacks along with highlighting the measures taken by the attackers to hide the money trail of the ransom.

Different variants of ransomware adopt different payment methods for the payment of ransom. Some utilize pre-paid cards like PaySafeCard, UCash, MoneyPak or cashU while others demand payment in form of virtual currencies like Bitcoin, Litecoin, XRP (cryptocurrency token of Ripple).

Paper highlights the reason behind the untraceable nature of virtual currencies.

Observation of the Cryptowall payment servers made by the researchers of the Dell SecureWorks Counter Threat unit revealed that a total of 939 bitcoins were paid as ransom between march 2014 and August 2014.

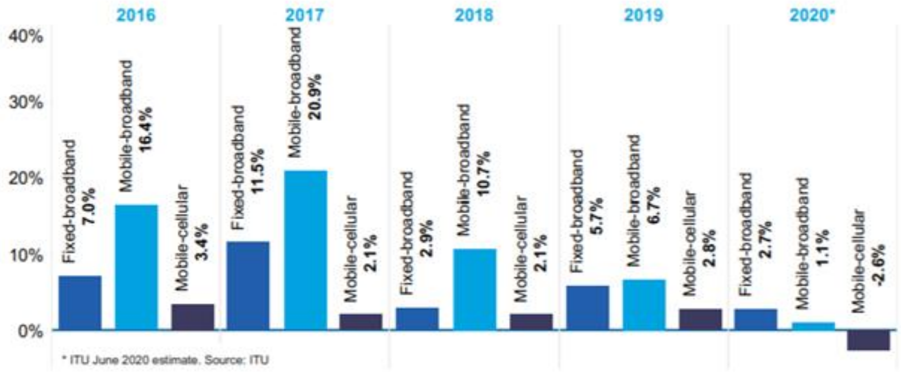
According to the Bitcoin (BTC) Exchange Rate, in August 2014, the value if 1 BTC was equivalent to $520, thus attackers earned more than $488,000 as ransom in 2014.

MOBILE DEVICES – A NEW TARGET

This section of the paper elaborates the findings of different reports regarding the growth in the number of attacks on mobile devices by presenting relevant statistics and data.

According to the statistics mention in the paper "Ransomware-Exploring the Electronic form of Extortion", the mobile broadband subscription was 26.7% for the year 2013 and was expected to reach 32% by the end of 2014 [6,915 million individual subscriptions].

Recent figures released in a report by the International Telecommunication Union [ITU] called Measuring Digital Development: Facts and Figures (2020), revealed the following developments.



* ITU June 2020 estimate. Source: ITU

Fig 2.2.13 Annual growth of mobile subscriptions [2016-2020]

Figure 2.2.13 taken from the report Facts and Figures (2020), is the result of a global survey conducted on 100 inhabitants and displays the annual growth of mobile subscriptions during the time period of 4 years (2016 to 2020).

The graph reveals a steady growth in the number of mobile broadband subscriptions up until 2017 and then a decline from 2018 to 2020 as more people moved in to faster and affordable optic fiber connections and fixed broadband connections.

The research paper also mentions the findings of the Norton report (2014) which states that in a global survey conducted for end users, results showed that 38 percent of mobile users had already experienced mobile cybercrime **[Figure 2.2.14].** 52 percent of the mobile phone users are storing sensitive information on their mobile devices, putting their data on risk.

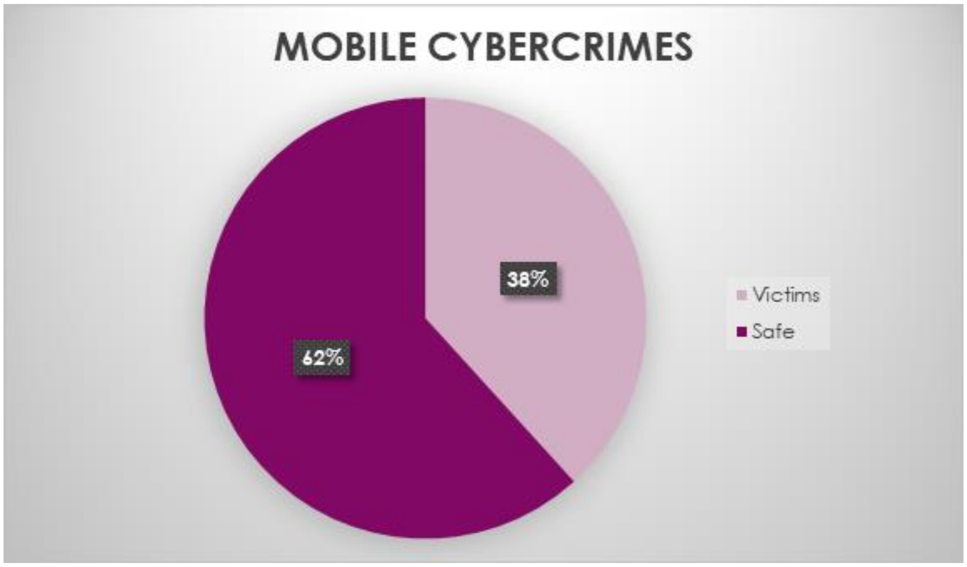


Fig 2.2.14 Victims of Mobile cybercrimes [2014] *[Source: Created using SmartArt Microsoft Word 2019]*

Crypto ransomware is a menacing variant which applies the concept of cryptology to encrypt user files which can have severe effects on confidential information. The paper by Subhash Poudyal [5] gives us an insight into Crypto-Ransomware, a form of malware that has affected various industries. Attackers are developing and modifying Ransomware variants constantly. Preventive and detection measures are continuously proved ineffective. Latest research on Ransomware with AI techniques ignores behavioral analysis and correlation mapping.

An approach to solve the recent challenges using an AI-powered hybrid algorithm and deep inspection approach for multi-level profiling of crypto-ransomware has been discussed. Experimenting with crypto-ransomware samples, the highest accuracy of 99.72% was achieved. It proved that multi-level profiling is better at detecting ransomware samples. A prototype called AIRaD(AI-based Ransomware Detection) was designed to visualize the proper implementation.

The paper elaborates upon the current status of Ransomware and discussed the spread of the ransomware-as-a-service model. Spread via phishing emails, victims often fall prey to social engineering attacks. According to a survey done by Sophos, 45% of ransomware attacks are via malicious links or attachments in emails, and 21% are from a remote attack on the server. The remaining are via misconfigured systems and USB devices.

The current COVID-19 pandemic has also played a role in the spread of Ransomware. Innocent victims are lured to click on Malware infected links and advertisements disguised as medical information and help. Many recent Ransomware attacks have occurred by exploiting vulnerabilities of a system. Ransomware such as Ryuk, SamSam, and Satan uses this technique.
The current anti-ransomware tools fail to detect zero-day ransomware attacks. Also, malware with obfuscated code is often bypassed. To overcome these limitations, the prototype AIRaD, which uses hybrid analysis has been discussed.

Various research papers were investigated where static, dynamic, and hybrid techniques of ransomware detection was discussed-

- Ransomware prevention using performance counters is known as RAPPER. It utilizes neural networks and Fast Fourier Transformation. Hardware performance counters are used as event traces. A popular tool in Linux called Perf is used to monitor the behavior.
- Using deep learning techniques to learn ransomware patterns on a semi-supervised framework. Implemented on an isolated environment using a Cuckoo sandbox, the run time varied from four to nine minutes. This approach was less efficient and robust as it ignored samples that could not be run on the given experimental settings and misses the obfuscated nature of Ransomware.

- Analysis of API called and amount of system resources used is done to determine if the sample is Ransomware or not. The results are sent to various machine learning models. This method helps analysts quickly check if the current sample is ransomware.
- Preventive measure for smartphone crypto-ransomware using dynamic analysis and hash-based techniques. Using entropy values, user data is analyzed to make decisions. The entropy and structure of data are observed to neutralize the ransomware. This approach has high accuracy but low resilience to obfuscate the behavior of Ransomware.
- A block cipher algorithm is used to prevent ransomware infection using an Alf and Vegard's RISC processor microcontroller. This approach uses static analysis and shows high accuracy.
- A deep inspection method using API call sequence and support vector machines showed a 97.48% accuracy. This model showed improved detection performance.
- Inspection of Ransomware behavior using a Window system, by analyzing the frequency of usage of API and normal binaries can identify Ransomware without the need to compare code signature.
- Use of Intel PIN tool to produce windows API call sequences. The accuracy reported is very high. Although, the test tun rime extends to five minutes which malware writers often fool
- A two-staged ransomware detection model was proposed. It uses the Windows API call sequence pattern to construct a Markov model. To train the remaining data, the Random Forest machine learning model was adopted.
- Assigning alphabets to API functions and applying DNA sequence alignment algorithm. It will help in pulling out malicious processes. Sequence analysis is better as malware writers insert dummy functions to cheat the frequency analysis. Analysis showed a 99.8% accuracy but could not handle obfuscated Ransomware
- Use of DNA sequencing using Naive Bayes, Decision stump, and AdaBoost algorithms. It is generated for selected features making use of DNA sequence design constraints. With the highest accuracy of 87.9%, the approach cannot handle obfuscated binaries.
- An approach using Ransomwall tool which combines static and dynamic analysis. This method claims to be capable of detecting zero-day Ransomware.

HYBRID REVERSE ENGINEERING AT MULTIPLE LEVELS

Details of Advanced reverse engineering plays an important role in multiple-level implementation. The following discusses the details about the methods-:

A. Hybrid Reverse Engineering

Reverse Engineering is a process of recreating things using an opposite of the function used to create them. To identify the malware code, Reverse Engineering is required. Malware writers use various ways to bypass defenders. Though some anti-ransomware claims to overcome these problems, it is a lot more difficult than anticipated. This is why a hybrid approach is adopted.

Some tools used for hybris reverse engineering -:

- Dynamic Binary Instrumentation- There is two types of instrumentation, code and Binary. Since the code of the malware is not available, we use only Binary. In this paper's approach, they use the PIN tool for Dynamic Binary Instrumentation, helping them keep track of every instruction.
- Cuckoo Sandbox- It is an advanced open-source automated malware analysis tool. It uses the virtualization technique to run malware samples.
- Ghidra - It is a reverse engineering framework. Allows us to observe binaries on various platforms and gives us a more accurate analysis of Ransomware samples.

FEATURE EXTRACTION AT MULTIPLE LEVELS

The output we get from hybrid reverse engineering is fed to the feature extraction component which consists of the following three levels-:

- DLL Level - These are Dynamic link libraries that can perform actions on file systems, such as manipulation, navigation, creation, and communication. They can be loaded into memory and removed when required, letting us use memory efficiently. DLL extractor parses through the output and gives us all DLLs, called by various functions.
- Function call Level - It is a code that helps identify a function unique to a malware behavior. Function call extractor parses through the output and makes a list of all function calls being used by the program.

- Assembly level - Dynamic binary instrumentation tool PIN is used to get the assembly instructions being used by the program. Assembly instruction is also called machine code, can be directly executed using the CPU. Every function call is carried out by a set of such instructions.

USE OF MACHINE LEARNING

Machine Learning increases the accuracy for detecting Ransomware. It makes use of various supervised and unsupervised classifiers to train, test, and validate. If a Binary is classified as ransomware then it is deleted, if not then it is marked as Benign. Frequency analysis and association rule mining are Data mining techniques used to find hidden features and patterns. It helps us differentiate a given family sample from others. The prototype of this paper uses an FP-growth algorithm. It is more efficient as it requires only two database scans. It is array-based and uses depth-first search. Ransomware detection sequences are created from FP-Growth association rules, which are generated when a list of DLLs, functions calls, and assembly instructions are fed to the algorithm.

AI-BASED RANSOMWARE DETECTION FRAMEWORK

After the discussion upon machine learning and hybrid reverse engineering technique, we need to take a look at Behavioral Chaining which is another core component.

A. Behavioral Chaining

It is a sequence of components that achieves a purpose. It is a collection of functionality chains belonging to different levels. Reverse engineering is used to build behavioral profiles.

1) RELATIONSHIP BETWEEN BEHAVIOR CHAIN
AND ASSOCIATION RULES

Association rules are explained using a behavioral chain. On one hand association rule defines patterns while the Behavioral chain classifies them.

2) CHAIN VALIDATOR

Chain validator helps in the validation of behavioral chains. A novel approach is used to calculate the Ransomware profiling chain ratio.

DCR = No. of DLL chains seen/ Total no. of DLL chains

FCR = No. of functional chain seen/ Total no. of functional chains

ACR = No. of assembly chains seen/ Total no. of assembly chains

MPCR = DCR+ FCR + ACR / Total number of levels

Chain level analysis is important to create unique Ransomware signatures. The analysis is based on static and Dynamic analysis, function call trace, assembly codes, and disassembled code blocks. This paper provides us with a brief explanation of all the different Chains. The basic functions of each chain are given below as diagrams from **Fig 2.2.15 to Fig 2.2.17** *(Source: Created using Smart Art)-:*

-

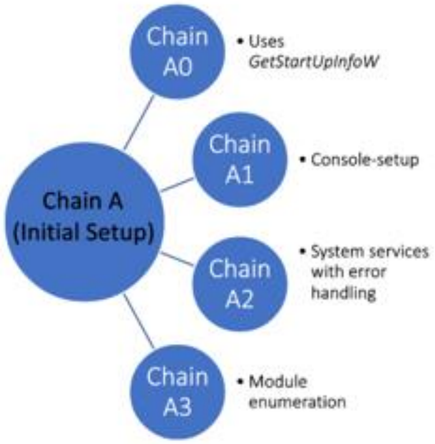


Fig 2.2.15 CHAIN A

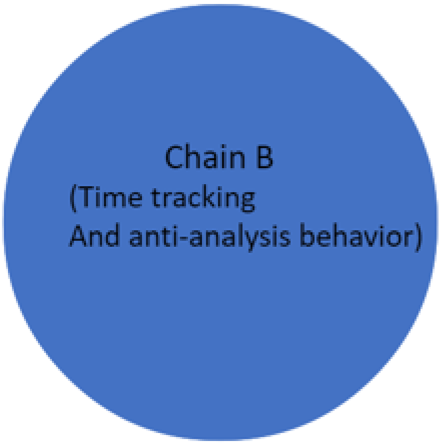


Fig 2.2.16 CHAIN B

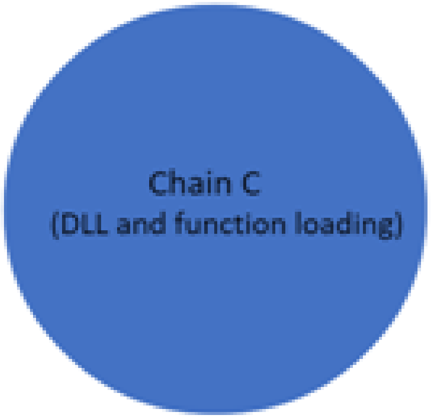


Fig 2.2.17 CHAIN C

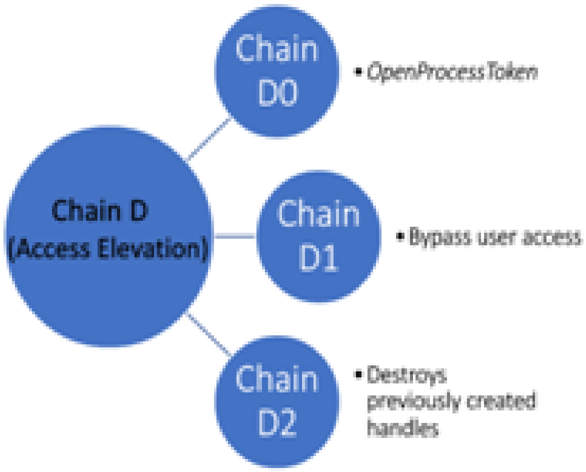

Chain D0
• OpenProcessToken
Chain D (Access Elevation)
Chain D1
• Bypass user access
Chain D2
• Destroys previously created handles

Fig 2.2.18 CHAIN D

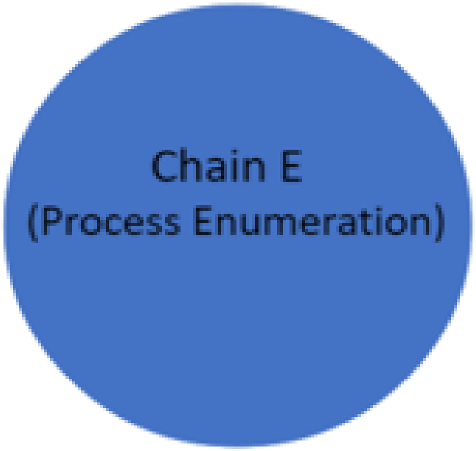


Fig 2.2.19 CHAIN E

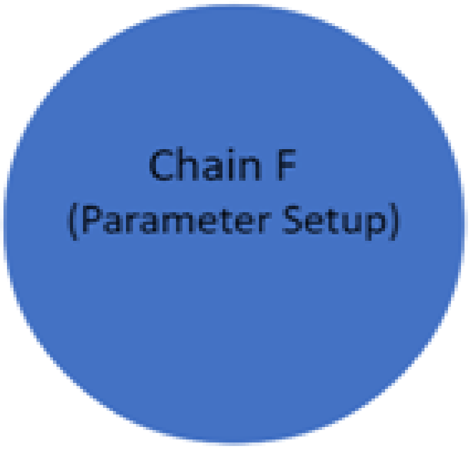


Fig 2.2.20 CHAIN F

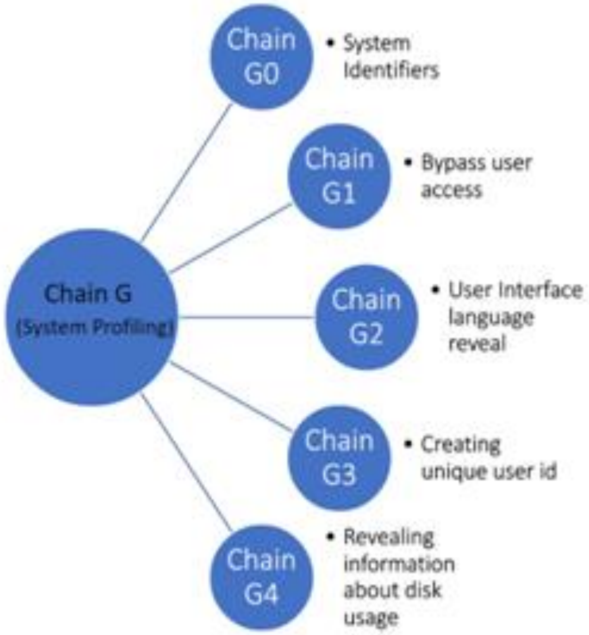


Fig 2.2.21 CHAIN G

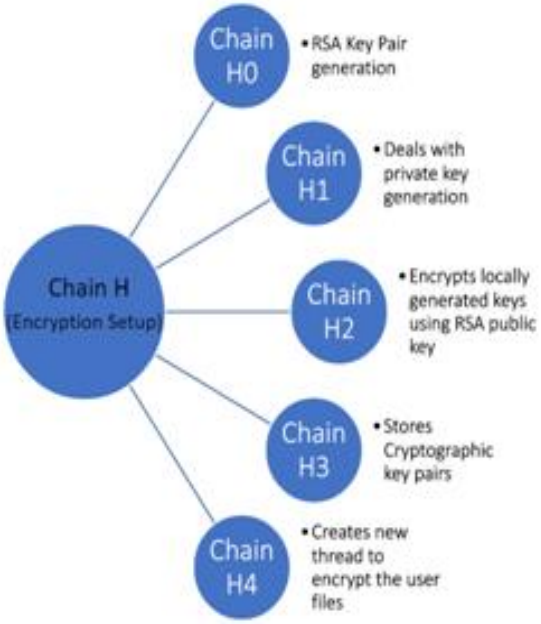

Chain H
(Encryption Setup)
Chain H0
• RSA Key Pair generation
Chain H1
• Deals with private key generation
Chain H2
• Encrypts locally generated keys using RSA public key
Chain H3
• Stores Cryptographic key pairs
Chain H4
• Creates new thread to encrypt the user files

Fig 2.2.22 CHAIN H

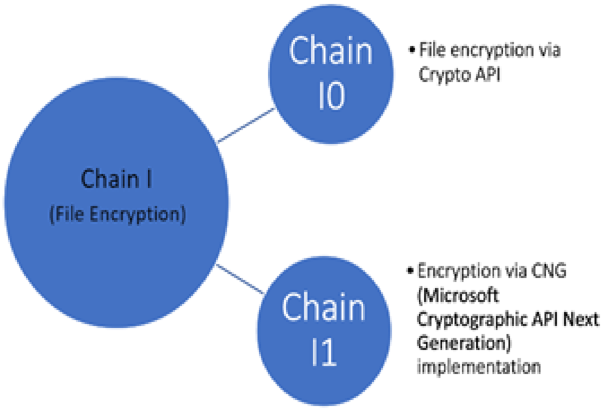

Chain I
(File Encryption)
Chain I0
• File encryption via Crypto API
Chain I1
• Encryption via CNG (Microsoft Cryptographic API Next Generation) implementation

Fig 2.2.23 CHAIN I

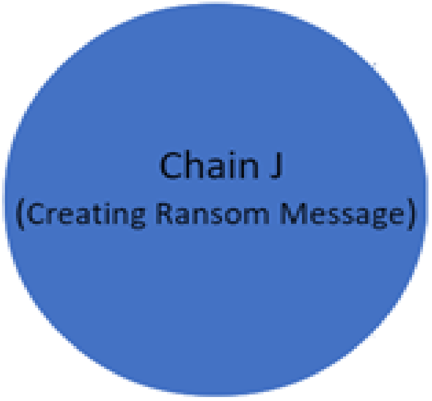


Fig 2.2.24 CHAIN J

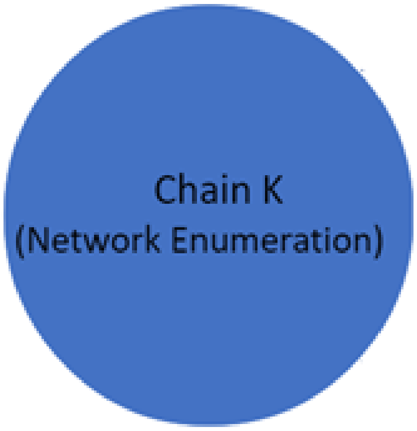


Fig 2.2.25 CHAIN K

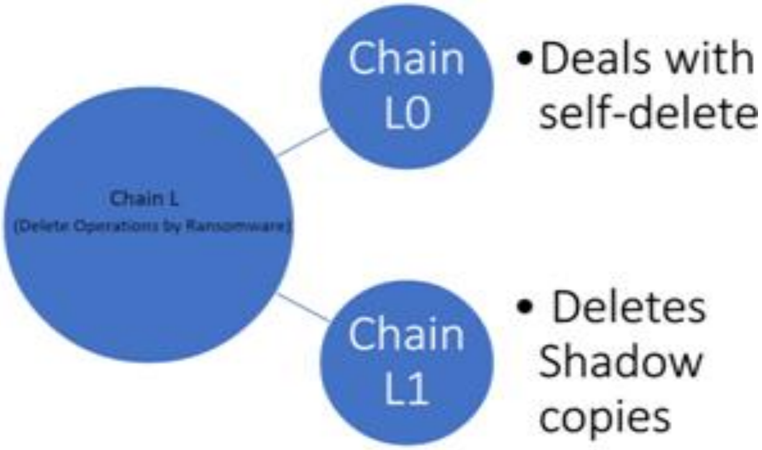


Fig 2.2.26 CHAIN L

Fig 2.2.27 CHAIN M

DATASET AND EXPERIMENTS

1) Dataset used - Using VirusTotal 2600 Malware samples, of which 550 crypto Ransomware were collected over six months of the year 2019. Labeling was done with the help of the detection category provided by Malwarebytes, Kaspersky, and Microsoft. 540 benign applications were collected from Windows OS and Open-Source Applications.

2)Experimental Protocol and evaluation measures - Python, bash script, and machine learning libraries were used. Six virtualized environments using i7 processors were set up to test Malware same.

Prototype AIRaD

The paper shows us an interesting discussion of a prototype that uses multilevel detection. Most approaches have low-level accuracy for capturing Ransomware showing obfuscated behavior but this prototype shows us otherwise. The association amongst DLL, function call, and assembly components helps us recognize Ransomware behavior and create a unique signature.

Over the years the exponential rise in the number of ransomware attacks on computer systems globally, each more complex and vicious in nature than its predecessor, has tipped the balance of computer security for the near future. The research paper by Savita Mohurle Et al. [6] briefly describes the most devastating ransomware attack of the whole decade (2010-2020), WannaCry, which tipped the balance of information security giving rise to multiple steps of protection to be taken by MNCs and tech giants for the proper safeguarding of user data.

Global digitization has made access to any amount of information easier and affordable for the world population along with playing its part in reducing, previously internet based, global criminal activities by a tenfold. However, this digitization has also endangered the security of personal and confidential information of an individual. Ransomware is one such attack that renders the system and the user helpless by encrypting data and important on the computer until and unless the demands of the attacker is fulfilled.

HISTORY OF RANSOMWARE

Ransomware has recently reached the peak of its attacks however it has been in existence for more than 30 years, with each new variant challenging tech industries and security analysts to deploy effective safety maneuvers for protection of data.

AIDS TROJAN- The First Ransomware Attack

PC Cyborg or AIDS Trojan was the first ever ransomware to be launched in December 1989 by an evolutionary biologist, Dr. Joseph L. Popp to 20,000 individuals and medical institutions.

Method of Deliverance

The unorthodox distribution method of the AIDS Trojan has been highlighted through **Figure 2.2.28**:

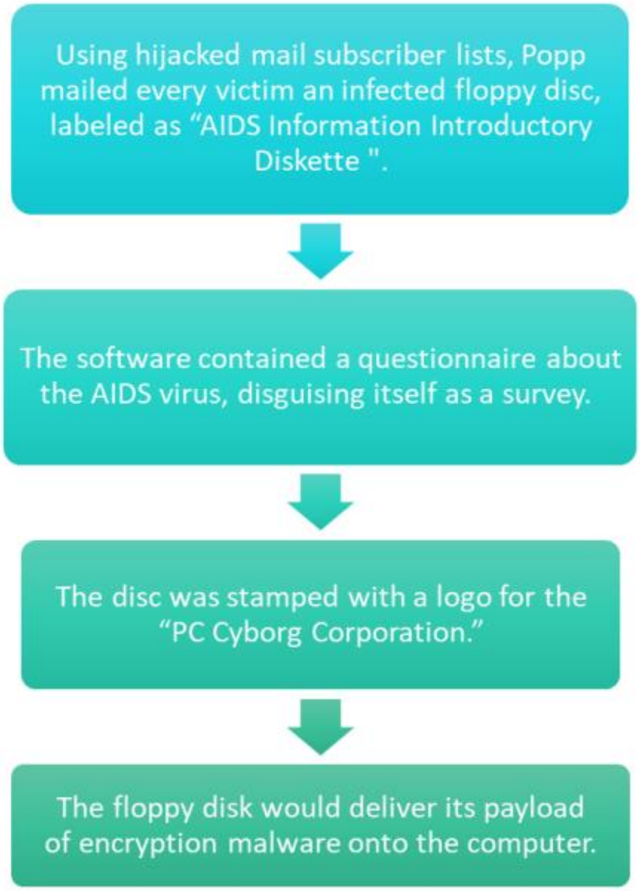

Using hijacked mail subscriber lists, Popp mailed every victim an infected floppy disc, labeled as "AIDS Information Introductory Diskette ".
The software contained a questionnaire about the AIDS virus, disguising itself as a survey.
The disc was stamped with a logo for the "PC Cyborg Corporation."
The floppy disk would deliver its payload of encryption malware onto the computer.

Fig 2.2.28 Working of AIDS Trojan ransomware *[Source: Created using SmartArt Microsoft Word 2019]*

In order to have their files decrypted, the victims were to send $189 to a P.O. box in Panama. While the malware itself was weak, and easily removable through a decryption software, the attack set the stage of over 30 years of ransomware and virus attacks, and highlighted the need for data security measures.

24 years following to the AIDS trojan attacks, a new variant of ransomware [Cryptolocker] wreaked havoc and chaos globally as it was for the first time the world witnessed the use of cryptological concepts for the purpose of encrypting user files and block the path of their access to their personal information.

Figure 2.2.29 shows the chronological order of the occurrence of each ransomware along with specifying which type of operating system was affected by a specific ransomware.

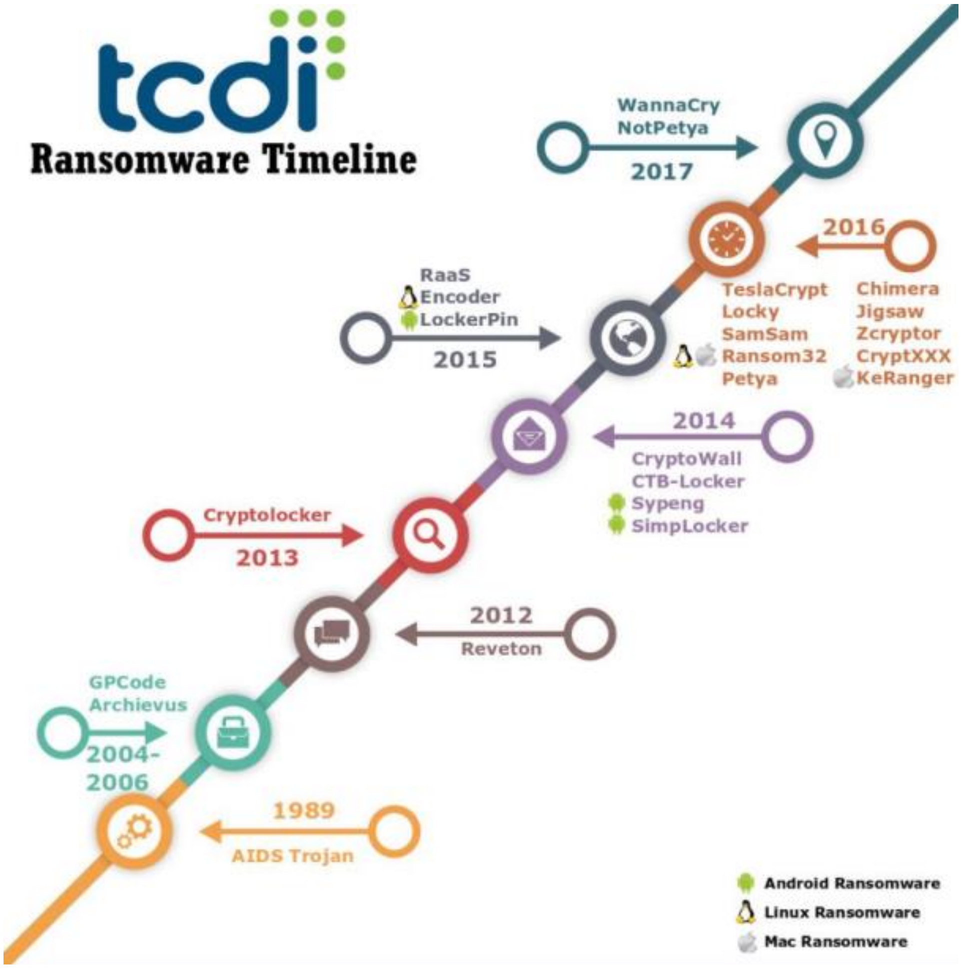


Fig 2.2.29 Ransomware timeline

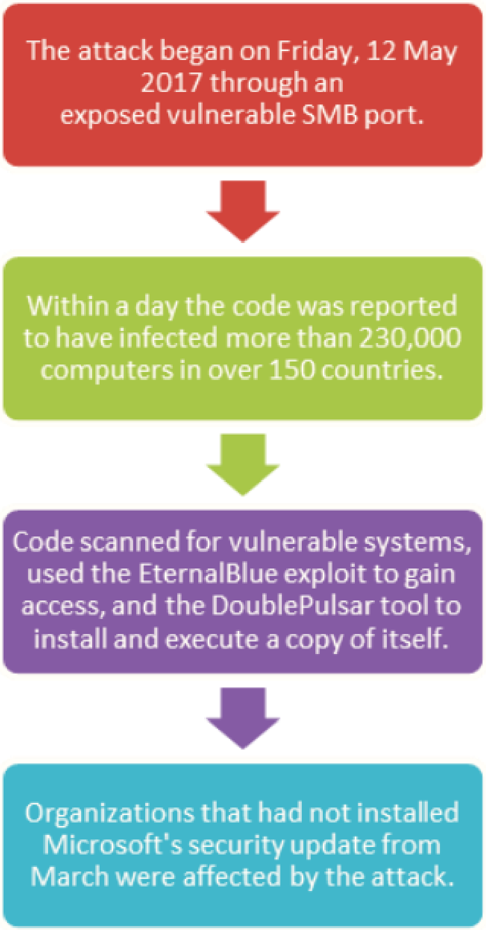
Among all the past ransomware attacks, the WannaCry ransomware attack [2017] caused the most devastating damage to computer systems all over the world.

WannaCry Ransomware: An Immense Attack on Cybersecurity

WannaCry ransomware was a massive cyber-attack carried on computer systems all over the world in the month of May 2017.

WannaCry (also known as WannaCrypt), was a ransomware Cryptoworm that targeted computers running the Microsoft Windows operating system. It encrypted data on the system and demanded ransom payments in Bitcoin cryptocurrency in exchange for the decryption key. The code for this hazardous Cryptoworm was stolen and leaked by a malicious hacker group called the Shadow Brokers.

The entire timeline and progression of the attack is described by **Figure 2.2.30**



The attack began on Friday, 12 May 2017 through an exposed vulnerable SMB port.

Within a day the code was reported to have infected more than 230,000 computers in over 150 countries.

Code scanned for vulnerable systems, used the EternalBlue exploit to gain access, and the DoublePulsar tool to install and execute a copy of itself.

Organizations that had not installed Microsoft's security update from March were affected by the attack.

Fig 2.2.30 Working of WannaCry ransomware *[Source: Created using SmartArt Microsoft Word 2019]*

The ransomware campaign was unparalleled in scale according to Europol, which estimated that around 200,000 computers were infected across 150 countries. According to Kaspersky Lab, the four most affected countries were Russia, Ukraine, India and Taiwan.

The paper specifically mentions the severe impact of WannaCry on computer systems in India. According to eScan antivirus reports 2017, India was one of the worst affected by cyber-attack.

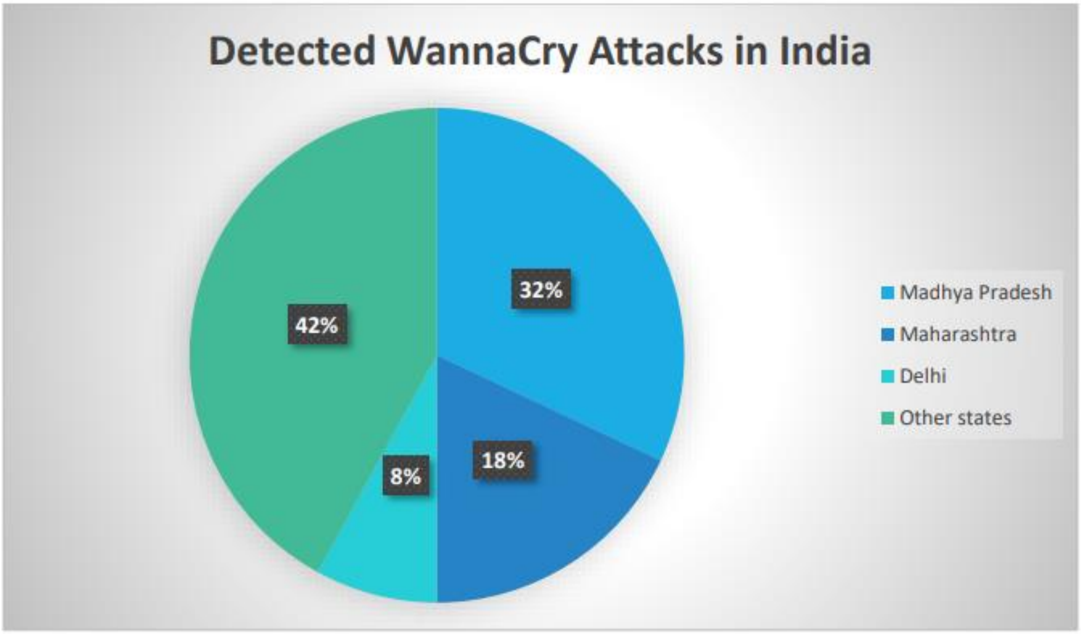


Fig 2.2.31 Reported WannaCry attacks in India *[Source: Created using SmartArt Microsoft Word 2019]*

Figure 2.2.31 shows the affected regions based on the detected and reported WannaCry attacks in India. Fascinatingly, Madhya Pradesh was the worst affected region in the country with around 32.63% of total ransomware attacks detected within country.

Madhya Pradesh was followed by Maharashtra at 18.84% and Delhi at third position with 8.76% share of the total detected attacks on the country.

The paper concludes with the preventive measures one must follow if they ever are under a ransomware attack and clearly establishes a brief and discreet explanation behind the workings of the WannaCry ransomware and its gigantic impact on the security of computer networks.

Ransomware has continued to evolve at a faster pace throughout the past decade and has recently seen a sharp shift in terms of targets of hacker groups and the method of deliverance. The research by Ronny Richardson Et al. [7] gave a clever and in-depth analytical point of view on the recent developments and the changes in ransomware which were observed and mentioned in numerous surveys conducted over the past decade.

Ransomware single-handedly is liable for loss of millions of dollars annually and is rapidly increasing both in terms of damage and number of incidents reported globally. Evidently, with the passage of time, newer versions of ransomware with the ability to avoid or conceal their presence from antivirus software and other intrusion detection systems were constantly observed.

The report was divided into 3 main components or sub-topics which were thoroughly read and analysed by the team members. These sub-topics are:

- Growth and Shifting Targets
- COVID-19 and Ransomware
- Ransomware Prevention

GROWTH AND SHIFTING TARGETS

The paper elaborated the shift in targets and growth rate of contemporary ransomware and highlighted the effects this change has brought upon the victims of these attacks.

The growth rate of insurance claims related to ransomware increased exponentially, exceeding 100% according to the data presented forward by the results of the survey and the statistical data of Motta (2020), Kauflin (2019) and FORBES (2019).

The paper mentions that the new strains of ransomware have a similar “frequent and severe” ideology behind their working. This suggests that the hackers or group behind the attack tend to strike a group of networks frequently and leave a long-lasting, severe impact on the affected systems.

A rise in the average financial demands of the attackers were also detected. According to the Motta report 2020, in the earlier strains of ransomware such as the SamSam and the Dharma ransomware, the average demands were less than $10,000. However, it was observed that for the newer strains of ransomware like BitPayer, Ryuk, and Sodinokobi, the demands exceed $100,000.

In reference to the Internet Crime report published by the Federal Bureau of Investigation (FBI) for the year 2018-2019, the research paper mentions a 37% annual increase in the number of reported cases for ransomware was observed. A 147% annual increase in ransomware associated losses was also recorded and the data was published.

With the increase in the number of organizations which were victims of large-scale ransomware attacks, a shrink in the number of individual systems being attacked by the same strain of ransomware was detected. The evident reason behind minimal damage to individual system is that customers and individuals are not willing to pay more than $1000 in order to retrieve their data however, large organizations and MNCs are much more willing to pay more as they are at a risk of their reputation and at an even severe risk to lose sensitive data of their consumers or have it sold on the dark net.

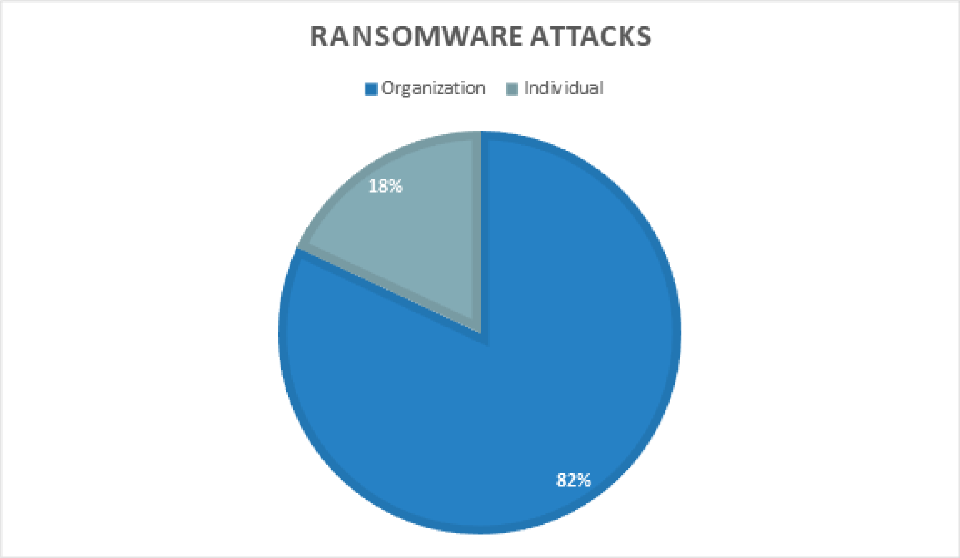


Fig 2.2.32 Victims of ransomware attacks [2018-2019] (*Source: Created using SmartArt Microsoft Word 2019)*

Figure 2.2.32 shows the record of the organizational attacks which accounted for 82% of all ransomware attacks during the year 2018-2019.

This was also an indication regarding how the landscape of attack vector followed by new strains of ransomware in order to micro-target large organizations and extort financial gains from the victims.

COVID-19 AND RANSOMWARE

During the pandemic the major cause of concern regarding ransomware was its circulation by the process of phishing. According to the researchers at Proofpoint a major increase in ransomware distribution through malicious email masked as COVID-19 related mails. Hundreds and thousands of such harmful emails were and still are being sent out daily.

The paper mentions and elaborates upon the published report of INTERPOL on the incidents related to ransomware. The report highlights the quantity of content circulated across various platforms over a period of 4 months [January 2020 – April 2020]. Within the report there is a clear mention of 48,000 malicious URLs, 737 malware related incidents and 907,000 spam messages which were reported all in accordance to COVID-19.

The largest attack that was carried out on multiple health institutions and hospitals was by a new ransomware strain called AVADDON which according to the June 2020 report of Palmer, involved the distribution of over 1,000,000 phishing emails within a single week, mainly targeting major US organizations.

RANSOMWARE PREVENTION

The research paper concluded on a positive note by elaborating on the 5 important points to remember in order to prevent major damage being caused to the computer system under the attack of a ransomware.

1. Most of the ransomware attacks are a target of opportunity hence one must try and make their organization less prone to being attacked. According to the Motta report 2020, the two most common attack vectors are phishing and remote network access points out of which Microsoft Remote Desktop Protocol (RDP) is the most common pathway. Limiting or completely avoiding the use of RDP can minimize the risk of a remote ransomware attack on the system by a tenfold.
2. Being vigilant and observant about what links and emails are being visited or downloaded across the computer network of the organization is also crucial in order to prevent large-scale

attacks. The average time between infection and activation is 30 days with a range of 30 minutes to one year (Motta, 2020). In many cases, this gives vigilant organizations time to recover from a ransomware attack before its payload is triggered.

3. Elimination of remote access and limiting administrative access can also prove to be successful in defending the network from malicious attacks and compromise of data. Using multi-factor authentication, and maintaining basic hygiene, like regular patching are also important (Motta, 2020).
4. It is also quite essential to have good reliable backups of sensitive data. Offline backups (sometimes called a cold site backup) are important since this prevents the ransomware from encrypting the backup (Motta, 2020).
5. In the extreme case of compromised data, it is advised to seek professional, experienced, third-party expert to manage negotiating with the ransomware group to come up with a viable solution and possibly completely retrieve all lost data.
6. Be cautious as Government or law enforcement agencies never use electronic payment systems like MoneyPak, UCash or any such payment options to collect fine.

CHAPTER-3:
DESIGN METHODOLOGY AND ITS NOVELTY

3.1 Parameters

Analysis of ransomware can be strenuous. There are various features and details that need to be taken into account and older versions of ransomware keep coming back with new modifications. The various variants, constant advancements, and technological developments make it hard to compare and analyze. To make our work easier, we divided some aspects of ransomware and investigated under those parameters. This helped us gain a comparative understanding of the changes faced in the world of ransomware.

3.1.1 Method of Deliverance:

It is critical to understand how ransomware gets delivered by attackers. It is a parameter that will help us protect ourselves better and reduce the risk of an attack.

Fake advertisements and phishing emails are the leading techniques used to deliver a ransomware attack. Some other common ways are -:

Drive-By Download - It refers to the malicious programs that get installed into the victim's system without their consent

RDP – Remote Desktop Protocol is a software that can give access to desktop or application on a remote host. This access is used as a backdoor to infect a system with ransomware.

Exploit kits - It is an all-in-one tool which includes a collection of exploits. Cybercriminals with mediocre knowledge can easily use it for attacks.

The following **Table 3.1** shows a general categorization of ransomware based on our research of the current Parameter: -

Phishing	Drive-By attack	Vulnerabilities
Cerber	Bad Rabbit	Petya
Ryuk	CryptoWall	WannaCry
Maze		
Jigsaw		
MISCHA		
Cryptolocker		
CryptoWall		

Table 3.1 Categorization of ransomware based method of deliverance

With the development of technology, attackers started exploiting the vulnerabilities of a system. For example, in an organization a target computer can be hacked and the ransomware can be spread by exploiting vulnerabilities, such as unpatched security, eventually affecting their entire system and bringing down the company. In 2014, CryptoWall exploited Java Vulnerability. The ransomware spread via emails. In 2017 we saw the WannaCry ransomware at work. It could spread itself within corporate networks without user interaction by exploiting known vulnerabilities in Microsoft Windows.

Hence, ransomware has evolved in such a way that it can spread without user interaction and it is the responsibility of the authorities to work on its system vulnerabilities.

3.1.2 Attack Vector

Ransomware can be classified into active or passive types. Here active and passive defines the involvement of the user's actions, which plays a role in ransomware infection spread. When a ransomware attack happens due to clicking on an unknown link found on websites or emails, we can define it as active. Phishing emails is the leading Active method used for ransomware attack. If the system is compromised, without the user playing any role but solely due to the vulnerabilities present, we can define it as passive. For example, the Petya ransomware spreads to other Windows-based endpoints and servers that are vulnerable to MS17-010. It is an SMB vulnerability that everyone was instructed to patch during WannaCry.

The following **Table 3.2** broadly classifies a few ransomwares as Active or Passive based on our research:-

Active	**Passive**
Ryuk	WannaCry
Cerber	Petya
CryptoWall	
Maze	

Table 3.2 Categorization based on Active or Passive nature

3.1.3 Impact on affected data:

All ransomware types have almost the same effects on data. They encrypt the data and lock us out of our system. The victim then has to pay a certain amount to obtain the key, which will unlock their system.

Cybersecurity experts advise us against paying the ransom. Since many a time, the attackers disappear without giving us the key. It only funds them for future attacks.

There are ransomware types from which data recovery is possible. For example, in Bad Rabbit ransomware, two defects were found. It did not delete the Shadow volume copies after encryption. Along with that, the malware did not delete the generated password from the memory until the computer was rebooted, by the victim. Extraction of decryption passwords from the dispci.exe file was possible if the system was not rebooted after a ransomware attack. Hence, data can be recovered to some extent.

In the more recent ransomware types, the chances of recovery of data are very bleak. For example, in Cerber ransomware recovery of data is very hard since it uses RSA encryption which is very hard to crack. You can try to pay the ransom and hope they send you the decryption key, but many people don't receive it.

Since attackers are constantly modifying and working on different ransomware, saving data is becoming more and more difficult. Constant research in this field is slowly becoming a top priority.

3.1.4 Types of Ransomwares:

There are many kinds of ransomware affecting the system in different ways, but the purpose is the same. To make our data inaccessible until Ransom is paid. Some of the types are -:

1. **Crypto-Ransomware:** They encrypt the files of a system, making them inaccessible without a key. They are the most common variant.
2. **Lockers:** They completely lock us out of our system. A lock screen displays the ransom demand. Sometimes a timer is shown to increase urgency.
3. **Scareware:** It is fake software that claims to have detected a virus or other issue in our computer. Clicking on it will direct us to pay to resolve the problem. Some types lock us our system while some don't damage anything and flood the screen with pop-up alerts.
4. **Doxware:** It threatens to distribute sensitive information online. To prevent the data from reaching the wrong hands or being publicly distributed, most people panic and pay the ransom. One variation of this type is police-themed ransomware which claims to be law enforcement and warns that illegal online activity has been detected, but imprisonment can be avoided by paying a fine.
5. **RaaS (Ransomware as a Service):** Refers to contract hackers. They host malware anonymously, take care of the distribution, payment collection, and restore access. In return, the attacker will get a part of the loot.

If we compare the advancements of ransomware, we will see that the lines which differentiated between the different types have started to blur. In 2013 Crypto-Locker was discovered. It belonged to both a locker and crypto variant. In 2016 Petya was discovered. Along with encrypting files, it also overwrote the master boot record. This enables it to encrypt the master file table and lock victims out of their hard drives quickly. Hence, with time the ransomwares coming into existence has started belonging to more than one category, making them more dangerous.

3.1.5 Timeline to remove Ransomware:

Anyone can become a victim of a ransomware attack. Due to constant modifications, it is hard to protect ourselves all the time. There has been an emergence of technology use due to the Pandemic, making us more vulnerable to cyber threats.

Some basic steps should be followed, as per protocol, in case of a ransomware infection.

1. Isolation: We need to prevent the infection from spreading. This is done by pinpointing the center of infection and disconnecting it from all networks. It is a very crucial first step to be followed by an organization.
2. Identification: We need to collect evidence to identify the variant we are dealing with.
3. Report: The appropriate authorities need to be informed.
4. Determine Your Options: We have several ways to deal with the infection. We need to determine which approach is best for us.
5. Restore and Refresh: Use safe backups and program and software sources to restore your computer or outfit a new platform.
6. Plan to Prevent Recurrence: After Recovering from an attack, it is important to understand why it happened in the first place. It will help in protecting ourselves from future attacks.

In a well-managed recovery effort, the general time frame of removal is one to two weeks. Although, there are many variables to consider. While removing a ransomware attack, everything cannot always go as planned. Sometimes the authorities themselves might be unable to resolve the problem quickly, or the isolation could not be completed in time, or the variant found was a new one. The more advancements in ransomware strains, the more complicated the removal process becomes.

CHAPTER-4:
TECHNICAL IMPLEMENTATION & ANALYSIS

4.1 Introduction

Case studies gives us a range of perspective, giving us an opportunity to gain deeper understanding into our topic. The in-depth investigation and analysis of these real-world occurrences provide a deeper insight on the need for awareness surrounding ransomware and how we can prevent a vicious scale attack on computer systems to ensure uncompromised user privacy and data security.

4.2 Case Study

Under this section of the research paper the team elaborates on the recent case studies which impacted organizations and individuals due to its dangerous and infectious nature resulting in compromised security of essential data and services.

4.2.1 Case Study 1 - Health Care Organization Attack

Details of the Cyberattack

The attack happened on the weekend and all the computers that were either not shut down or in hibernation were infected. The center was made aware of the attack on Monday morning when a staff member indicated they were unable to log into the system. There was an electronic ransomware message on the desktop and in every folder stating that the files were encrypted and stating the terms of the ransom. The center immediately disconnected from the Internet. Investigations indicated that access was gained through a decommissioned Windows 2003 terminal server that was supposed to be off (line) but was still on and connected to the network. Additionally, there was a firewall policy to enable a remote desktop protocol (RDP) connection on the server over the Internet without a virtual private network (VPN) connection. The remote desktop protocol is a network communications protocol designed for remote management and for remote access to virtual desktops, applications, and an RDP terminal server. The cyber attacker(s) gained access to the entire network through the Windows 2003 server, sent themselves an administrator password, and proceeded to encrypt all the servers. This then propagated to computers that were left on or in hibernation. Backups that were accessible on the network were also encrypted. The center was using the Nightingale on Demand electronic medical record (EMR) software, which was accessed securely over the Internet, therefore no client medical data was affected. Furthermore, the center had moved to Office 365, a cloud-based application set, so no Office files (including emails) stored in the cloud were affected. Only local organizational and financial files were encrypted by the ransomware. Fortunately, six years prior, the center outsourced Information Technology vendor had recommended the creation of a regular automatic backup. This was designed to run on a segregated virtual local area network or VLAN. A VLAN is a group of devices on one or more local area networks (LANs) that are configured to communicate as if they were attached to the same wire, when in fact they are not. This backup had been successfully running for the past six years and proved to be invaluable. After verifying that the files were intact, the center used the backup copy to restore their systems.

Insurance

The center did not reach out to their insurance company because they were able to do a full system restore. They did report the incident to the community police and informed their board of what data was lost, the overall costs, and suggestions for mitigation.

Cost

Costs were associated primarily with staff time including staff working directly on the restore and the tremendous amount of clean-up work that had to be done.

Timeline

Day 1

After work some staff left their computers on, others put them into hibernation and some shut down their computers.

Day 2, Day 3

Unprotected Windows 2003 server was attacked and used to gain access to the rest of the network; all computers either in hibernation or that were left on were encrypted.

Day 4

Users found the network unavailable. Ransom note was found on computers. Work to investigate and restore began immediately; unfortunately, backups that were on network access storage (NAS) devices were encrypted. A backup process installed on a segregated virtual server was found to be untouched. Restoration and rebuilding activities began.

Day 5

Some users were given access to the EMR to continue serving clients

Day 6

Back to full operational status.

CURRENT

Preventative measures to address the weakness in security exposed by the incident.

4.2.2 Case Study 2 - Colonial Pipeline Ransomware Attack

Details of the Cyberattack

The Colonial Pipeline hack is the largest publicly disclosed cyber-attack against critical infrastructure in the U.S. The attack involved multiple stages against Colonial Pipeline IT systems. The pipeline's operational technology systems that actually move oil were not directly compromised during the attack. The attack began when a hacker group identified as DarkSide accessed the Colonial Pipeline network. The attackers stole 100 gigabytes of data within a two-hour window. Following the data theft, the attackers infected the Colonial Pipeline IT network with ransomware that affected many computer systems, including billing and accounting. Colonial Pipeline shut down the pipeline to prevent the ransomware from spreading. Security investigation firm Mandiant was then brought in to investigate the attack. The FBI, Cybersecurity and Infrastructure Security Agency, U.S. Department of Energy, and Department of Homeland Security were also notified of the incident. Colonial Pipeline paid DarkSide hackers to get the decryption key, enabling the company's IT staff to regain control of its systems. Colonial Pipeline restarted pipeline operations on May 12.

Cost

The shutdown affected consumers and airlines along the East Coast. The hack was deemed a national security threat, as the pipeline moves oil from refineries to industry markets. This caused President Joe Biden to declare a state of emergency. The organization also paid 75 bitcoins, out of which it recovered 64 bitcoins.

Timeline

May 6, 2021

Initial intrusion and data theft.

May 7, 2021

Ransomware attack begins.

Colonial Pipeline becomes aware of the breach.

Security firm Mandiant called in to investigate and respond to attack.

Law enforcement and federal government authorities notified of the attack.

Pipeline taken offline to reduce risk of exposure to the operational network.

Colonial Pipeline pays ransom of 75 bitcoin ($4.4 million)

May 9, 2021

Emergency declaration by President Joe Biden.

May 12, 2021

Pipeline restarted as normal operations resumed.

June 7, 2021

Department of Justice recovers 63.7 bitcoin (approximately $2.3 million) from the attackers.

June 8, 2021

Congressional hearing on the attack.

4.3 Comparative Case Studies

4.3.1 CASE STUDY 1: RYUK Vs HERMES

Ransomware attacks are changing constantly thus making them unpredictable and almost impossible to eradicate completely. This ever- changing nature of ransomwares prove to be dangerous. In many situations, the ransomware evolves from one form to another changing the entire scenario and attack pattern. However, they carry some similar characteristics with their predecessors.

The example of this phenomena is observed in the case of Ryuk and Hermes ransomware.

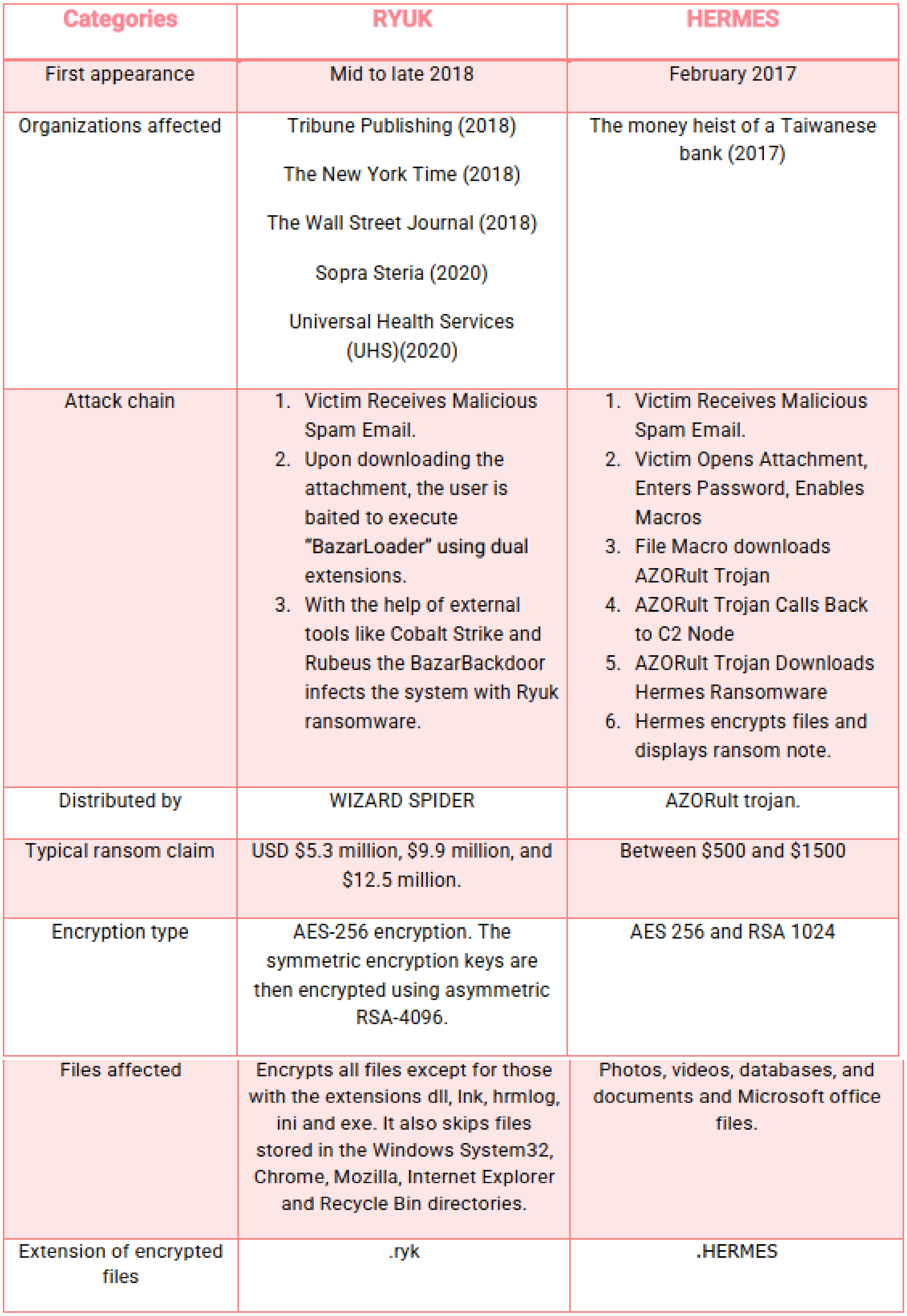
Ryuk ransomware is a cyber threat that has been targeting organizations, specifically hospitals, businesses, and government institutions since 2018. Hermes is a ransomware family that was first detected in February 2017. The Hermes Ransomware carries out a typical ransomware attack, which involves encrypting the victims' files to demand the payment of a ransom.

Hermes employs social engineering to spread malware spam related to fake job applications while Ryuk uses third party tools to encrypt the files.

However, code comparison analysis of Ryuk ransomware and Hermes ransomware showed that both are generally equal, giving credence to the theory that the developer of Ryuk has access to the Hermes source code.

Upon conducting a comparative analysis, we observed certain differences between Ryuk ransomware and the Hermes ransomware.

These differences are listed in the form of a comparative **Table 4.1**:



Categories	RYUK	HERMES
First appearance	Mid to late 2018	February 2017
Organizations affected	Tribune Publishing (2018) The New York Time (2018) The Wall Street Journal (2018) Sopra Steria (2020) Universal Health Services (UHS)(2020)	The money heist of a Taiwanese bank (2017)
Attack chain	1. Victim Receives Malicious Spam Email. 2. Upon downloading the attachment, the user is baited to execute "BazarLoader" using dual extensions. 3. With the help of external tools like Cobalt Strike and Rubeus the BazarBackdoor infects the system with Ryuk ransomware.	1. Victim Receives Malicious Spam Email. 2. Victim Opens Attachment, Enters Password, Enables Macros 3. File Macro downloads AZORult Trojan 4. AZORult Trojan Calls Back to C2 Node 5. AZORult Trojan Downloads Hermes Ransomware 6. Hermes encrypts files and displays ransom note.
Distributed by	WIZARD SPIDER	AZORult trojan.
Typical ransom claim	USD $5.3 million, $9.9 million, and $12.5 million.	Between $500 and $1500
Encryption type	AES-256 encryption. The symmetric encryption keys are then encrypted using asymmetric RSA-4096.	AES 256 and RSA 1024
Files affected	Encrypts all files except for those with the extensions dll, lnk, hrmlog, ini and exe. It also skips files stored in the Windows System32, Chrome, Mozilla, Internet Explorer and Recycle Bin directories.	Photos, videos, databases, and documents and Microsoft office files.
Extension of encrypted files	.ryk	.HERMES

Table 4.1 Comparative analysis of Ryuk and Hermes

Table 4.1 is a clear indication of how the Hermes ransomware evolved and what parameters were worked upon by hackers in order to make Ryuk the most feared ransomware of all time.

4.3.2 CASE STUDY 2: Nefilim and RansomEXX

In this case study we compare Nefilim and RansomEXX, which were very active in 2020 in ransomware landscape and has been behind several high-profile attacks during that year. The Nefilim malware uses AES-128 encryption to lock files and their blackmail payments are made via email. After encryption, it drops the ransomware note named 'NEFILIM-DECRYPT.txt'. All files are encrypted with the extension of (. NEFILIM). The comparison is done based on the following listed parameters.

Timeline

1.Nefilim

Neifilim ransomware infection was executed over 58 days. The gap between first Cobalt Strike and the host-based reconnaissance and antivirus discovery was 22 days. Within 2 days after the ransomware binary was compiled, the infection occurred. Figure 4.3.1 shows the timeline of the Nefilim ransomware attack.

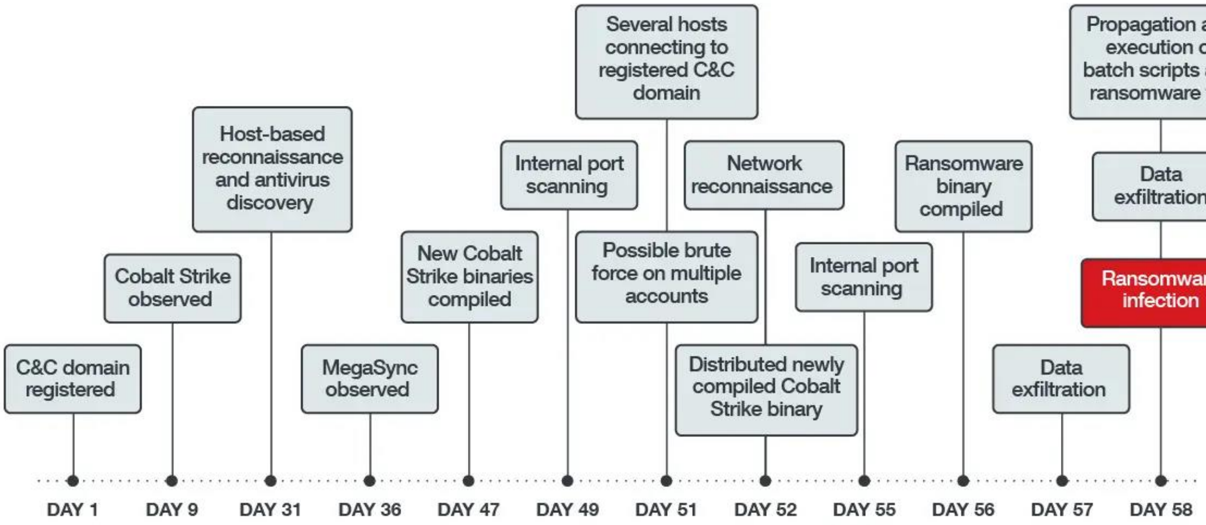

Several hosts connecting to registered C&C domain
Propagation and execution of batch scripts and ransomware file
Host-based reconnaissance and antivirus discovery
Internal port scanning
Network reconnaissance
Ransomware binary compiled
Data exfiltration
Cobalt Strike observed
New Cobalt Strike binaries compiled
Possible brute force on multiple accounts
Internal port scanning
Ransomware infection
C&C domain registered
MegaSync observed
Distributed newly compiled Cobalt Strike binary
Data exfiltration
DAY 1
DAY 9
DAY 31
DAY 36
DAY 47
DAY 49
DAY 51
DAY 52
DAY 55
DAY 56
DAY 57
DAY 58

Figure 4.3.1 Attack timeline of Nefilim ransomware *(Source: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22)*

2.RansomEXX

The ransomware RansomEXX first affected the US Government body in May. After 2 months, it was again used against a technical company based in Japan in August. Thereafter, it was used multiple times in different organizations in UD, Canada, and Brazil till November. Figure 4.3.2 shows the timeline of the RansomEXX attack.

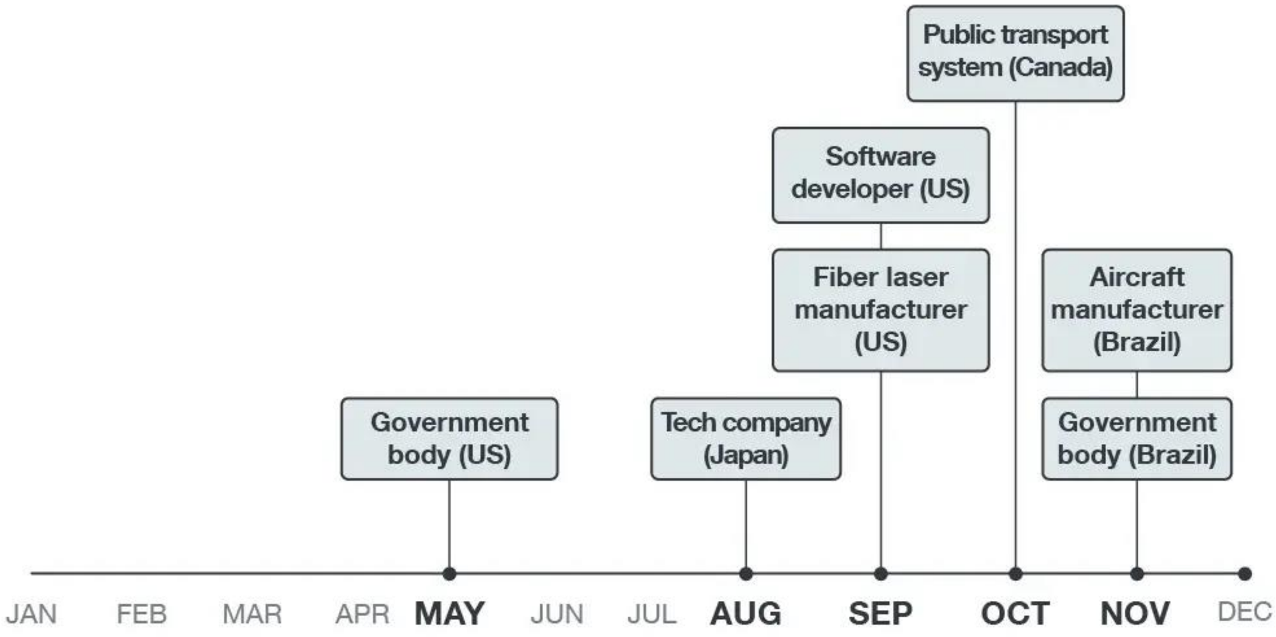
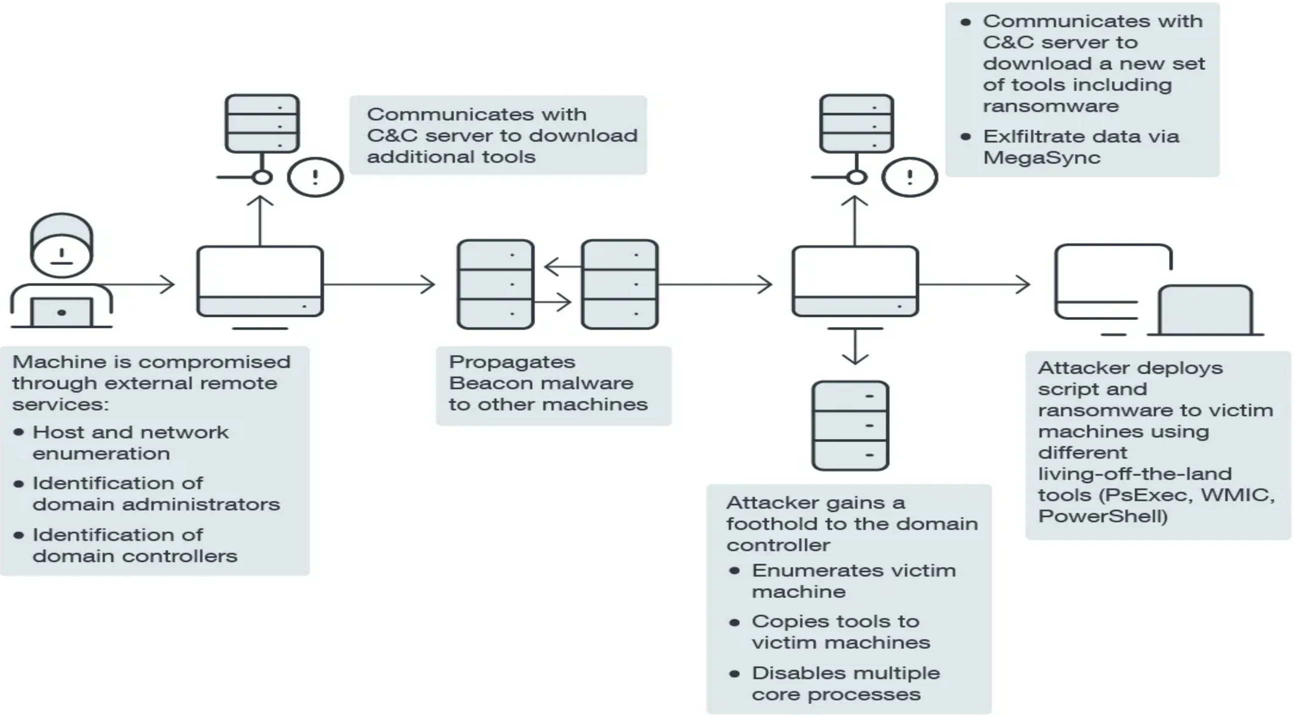


Figure 4.3.2 Attack timeline of RansomEXX ransomware *(Source: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22)*

Infection Chain

1. Nefilim

Because this attack involves staying longer in the network, it needs to stay hidden for as long as they can. To do this, the threat actors mostly used legitimate utilities (taskkill.exe, net.exe, sc.exe, wmic.exe, etc.) that already existed in the environment. Figure 4.3.3 shows the infection chain through which Nefilim was executed.



Communicates with C&C server to download additional tools
Communicates with C&C server to download a new set of tools including ransomware
Exlfiltrate data via MegaSync
Machine is compromised through external remote services:
Host and network enumeration
Identification of domain administrators
Identification of domain controllers
Propagates Beacon malware to other machines
Attacker gains a foothold to the domain controller
Enumerates victim machine
Copies tools to victim machines
Disables multiple core processes
Attacker deploys script and ransomware to victim machines using different living-off-the-land tools (PsExec, WMIC, PowerShell)

Figure 4.3.3 Infection chain of Nefilim

(Source: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22)

2. RansomEXX

From initially infecting Windows servers, its developers have created a newer variant capable of infecting Linux servers. One indication of how RansomEXX targets its victims lies in the samples from each attack, which contained the hardcoded name of the victim. Figure 4.3.4 shows the infection chain through which RansomEXX was executed.

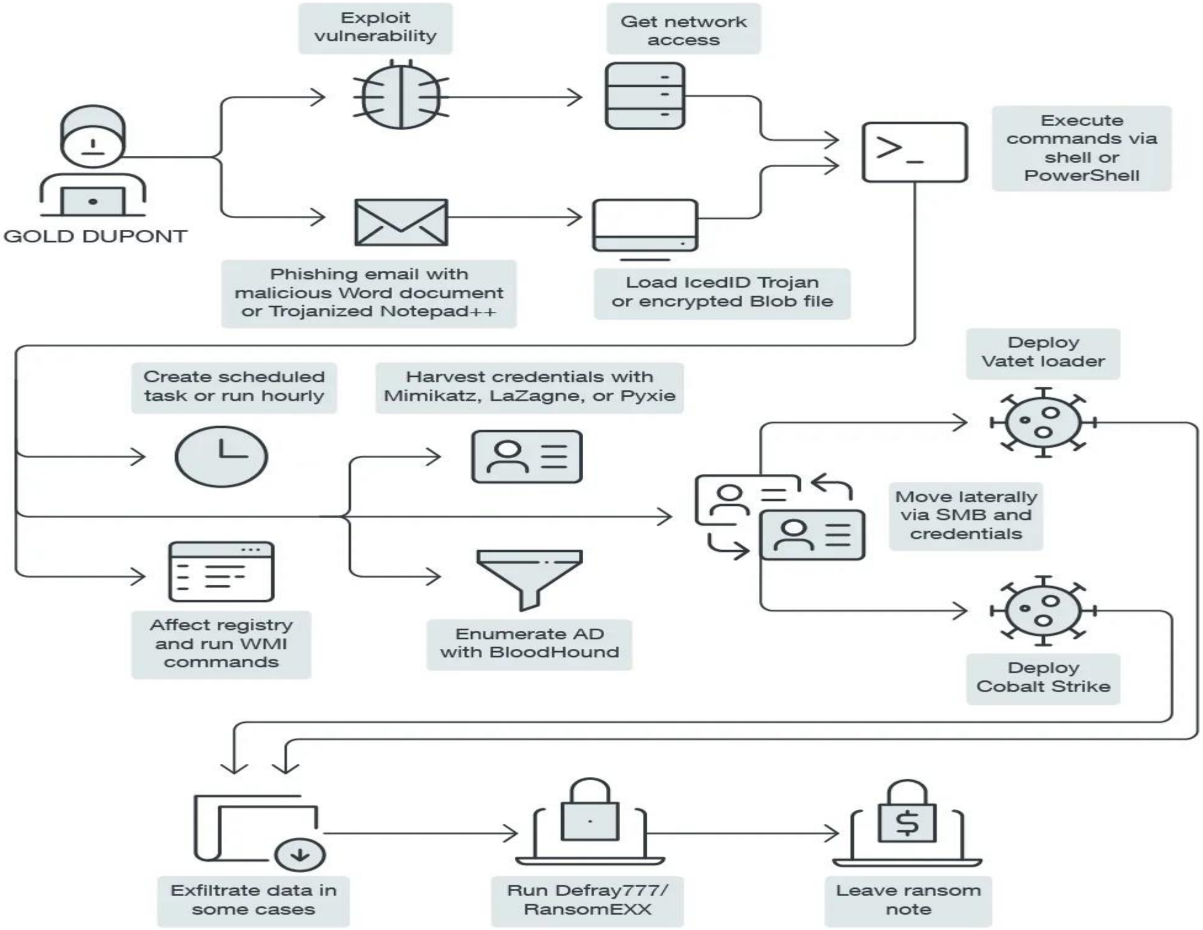

GOLD DUPONT
Exploit vulnerability
Get network access
Execute commands via shell or PowerShell
Phishing email with malicious Word document or Trojanized Notepad++
Load IcedID Trojan or encrypted Blob file
Deploy Vatet loader
Create scheduled task or run hourly
Harvest credentials with Mimikatz, LaZagne, or Pyxie
Move laterally via SMB and credentials
Affect registry and run WMI commands
Enumerate AD with BloodHound
Deploy Cobalt Strike
Exfiltrate data in some cases
Run Defray777/ RansomEXX
Leave ransom note

Figure 4.3.4 Infection chain of RansomEXX

(Source: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22)

Tactics and Techniques (Various Parameters)

The Table 4.2 shows the various tactics and techniques used by Nefilim and RansomEXX to affect their target device.

TACTICS AND TECHNIQUES USED	NEFILIM	RANSOMEXX
INITIAL ACCESS	T1133 – External Remote Services T1078 – Valid Accounts	T1133 – External Remote Services T1566 - Phishing
EXECUTION	T1509 – Command and Scripting Interpreter T1047 – Windows Management Instrumentation	T1509 – Command and Scripting Interpreter T1053 – Scheduled Task/Job T1047 – Windows Management Instrumentation
PERSISTENCE	T1078 – Valid Accounts	T1543 – Create or Modify System Process T1133- External Remote Services T1053 – Scheduled Task/Job
PRIVILEGE ESCALATION	T1078 – Valid Accounts	T1543 – Create or Modify System Process T1053 – Scheduled Task/Job
CREDENTIAL ACCESS	T1003 – 0S Credential Dumping T1110 – Brute Force	T1003 – 0S Credential Dumping
LATERAL MOVEMENT	T1021 – Remote Services T1570 – Lateral Services	T1021 – Remote Services
COLLECTION	T1005 – Data from Local System T1039 – Data from Network Shared Drive T1560 – Archive Collected Data	T1005 – Data from Local System T1074 – Data Staged
EXFILTRATION	T1048 – Exfiltration Over Alternative Protocol	T1041 – Exfiltration over C2 Channel T1567 – Exfiltration Over Web Service
IMPACT	T1486 – Data Encrypted for Impact T1489 – Service stop	T1486 – Data Encrypted for Impact

Table 4.2 Comparative Analysis of Tactics and techniques used by Nefilim and Ransomexx

CHAPTER-5
PROJECT OUTCOME AND APPLICABILITY

5.1 OUTLINE

This section encompasses the achievements of the team in collecting and grouping relevant data surrounding the project, so as to establish the required applicability of this research. This was done by conducting a through and detailed survey with a sample of 40 respondents along with extensively analyzing the survey’s results to draw necessary and pertinent inferences.

5.2 SURVEY

Surveys help us analyze the general public opinion, understand their awareness of a particular subject, and attract their attention towards the details and specifications of a topic. It is an inexpensive and flexible method to spread information and gain insights into opinions and preferences. More importantly, it is a valuable tool, used to gather data. Through our project, we wanted to understand and compare Contemporary Ransomware. While analyzing various research papers we came across a common idea and heeded warnings, stating that Ransomware is an increasing and unpredictable complication. We wanted to see if the general public were familiar with this growing threat. Hence, we conducted a survey to investigate how much people are aware of ransomware and its destructive nature. The following are the results of the survey: -

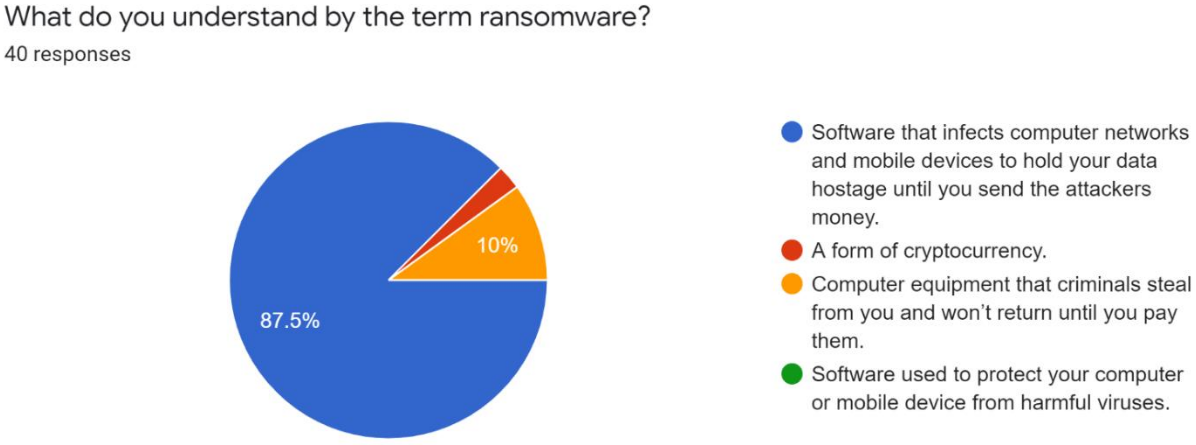


Figure 5.2.1 What do you understand by the term ransomware?

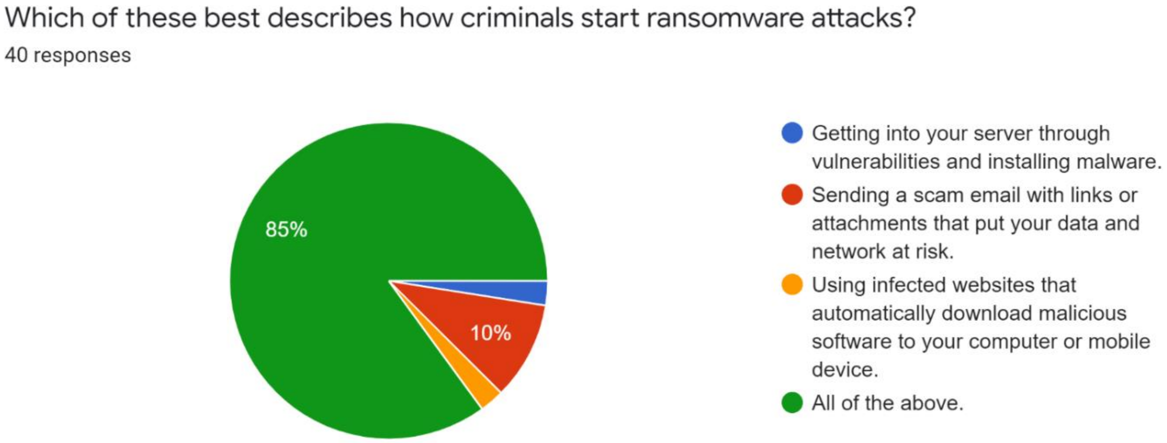
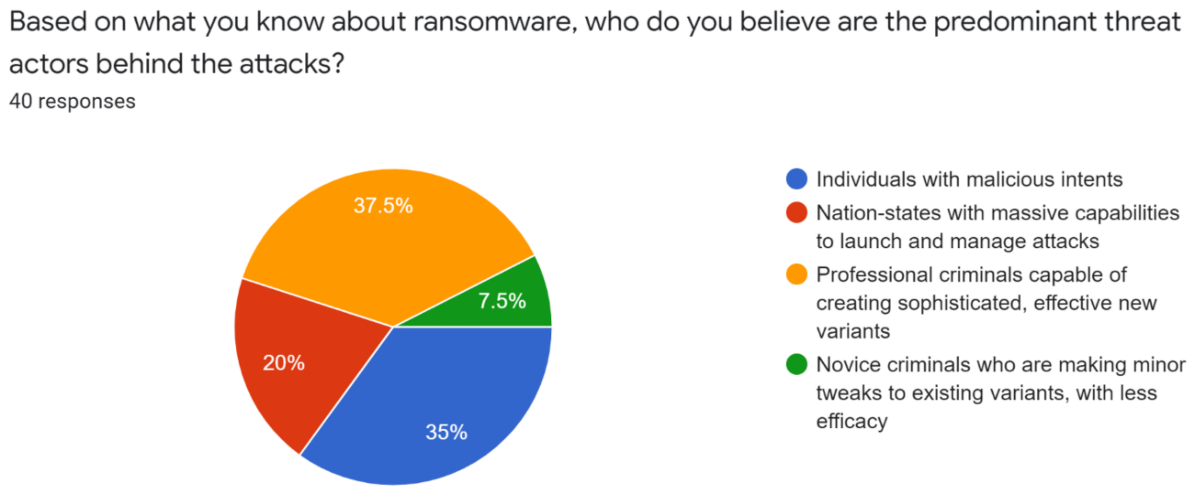


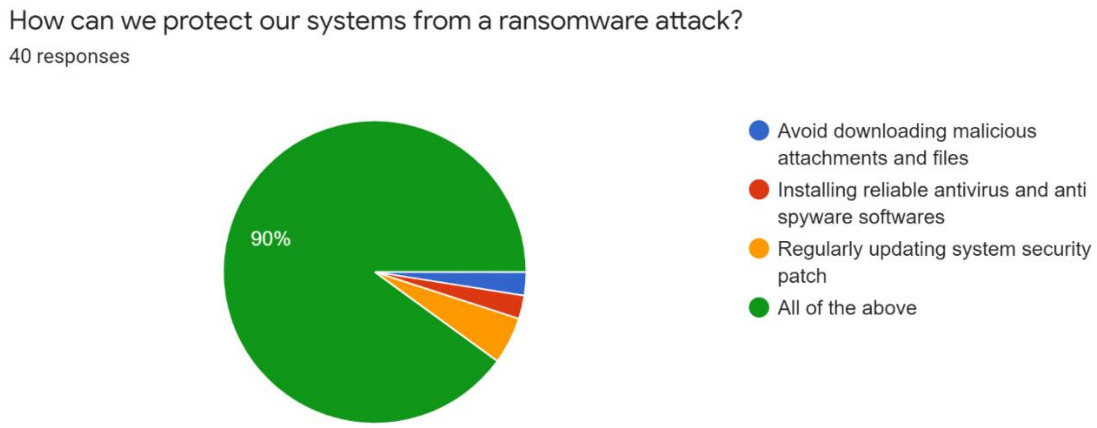
Figure 5.2.2 Which of these best describes how criminals start ransomware attacks



Based on what you know about ransomware, who do you believe are the predominant threat actors behind the attacks?

40 responses

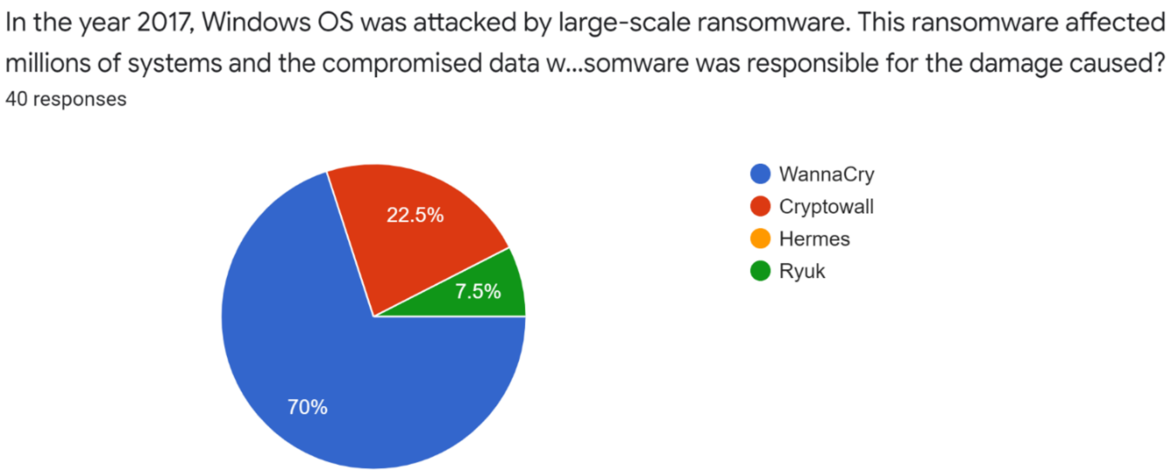
Figure 5.2.3 Who do you believe are the predominant threat actors behind the attacks?



How can we protect our systems from a ransomware attack?

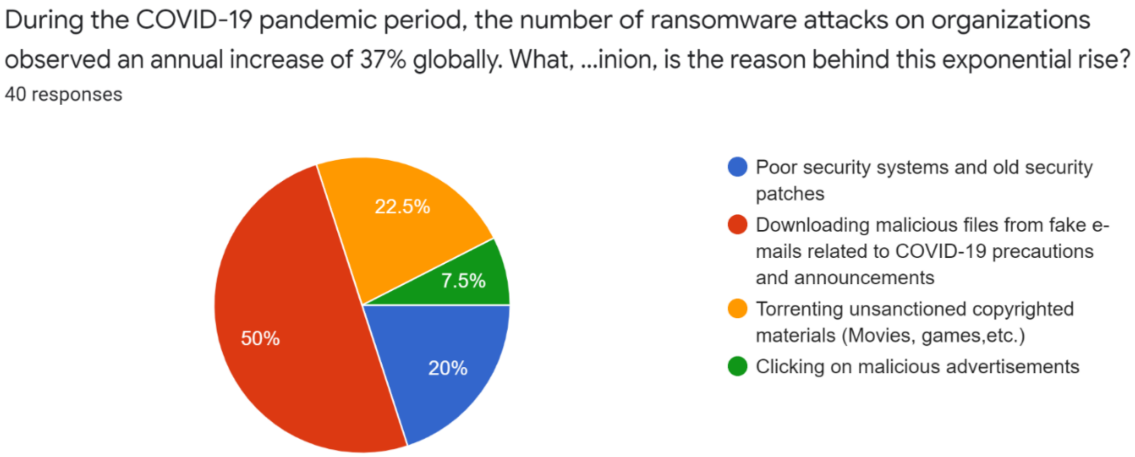
40 responses

Figure 5.2.4 How can we protect our systems from a ransomware attack?


In the year 2017, Windows OS was attacked by large-scale ransomware. This ransomware affected millions of systems and the compromised data w...somware was responsible for the damage caused?

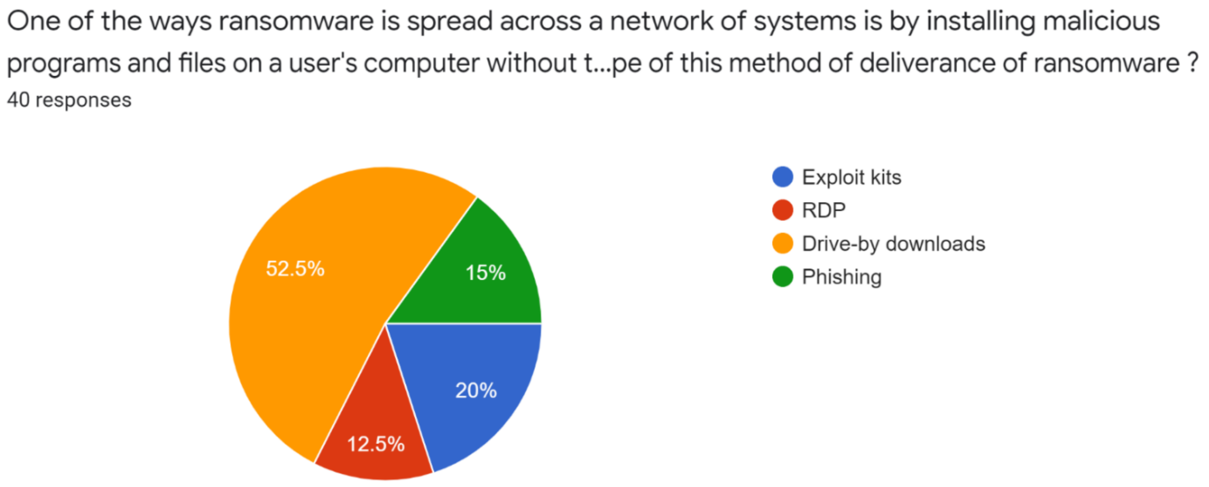
40 responses

Figure 5.2.5 Who caused Windows OS ransomware attack caused by?


During the COVID-19 pandemic period, the number of ransomware attacks on organizations observed an annual increase of 37% globally. What, ...inion, is the reason behind this exponential rise?

40 responses

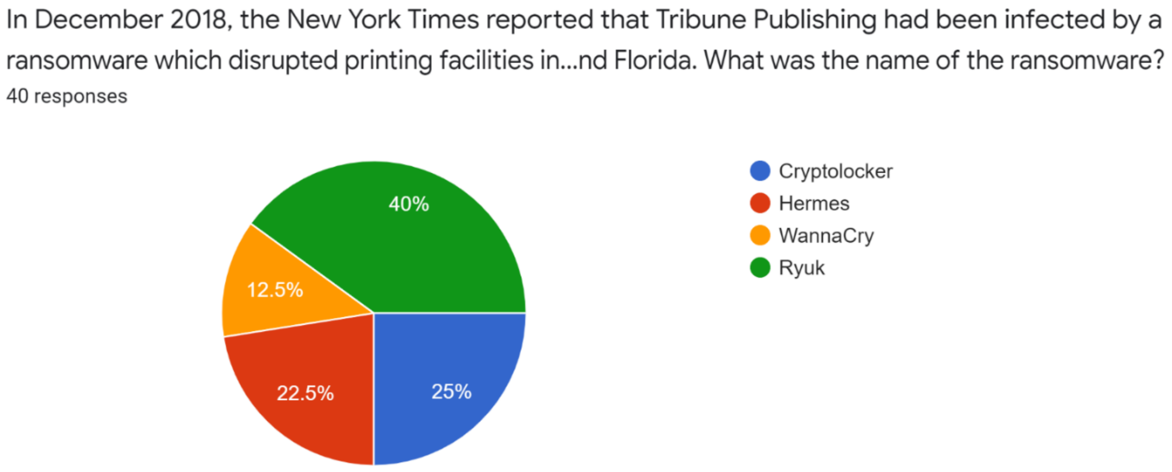
Figure 5.2.6 COVID-19



One of the ways ransomware is spread across a network of systems is by installing malicious programs and files on a user's computer without t...pe of this method of deliverance of ransomware ?

40 responses

Figure 5.2.7



In December 2018, the New York Times reported that Tribune Publishing had been infected by a ransomware which disrupted printing facilities in...nd Florida. What was the name of the ransomware?

40 responses

Figure 5.2.8 Who caused New York Times ransomware attack?

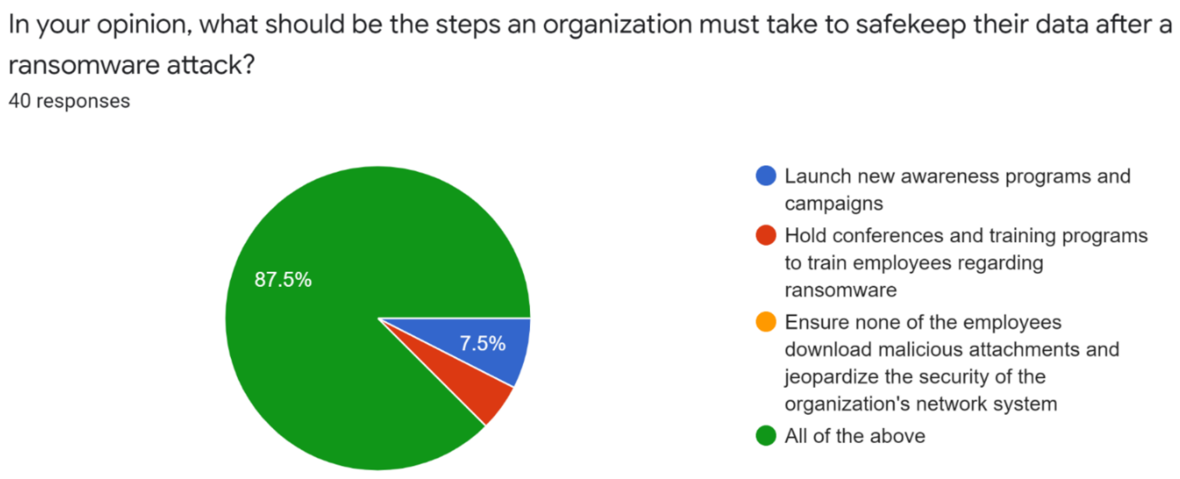


Figure 5.2.9 Steps taken to safekeep

Upon analyzing the results, we observed that most people knew about the basics of ransomware, such as the definition of the general term, how one might become a victim and some preventive measures that can be used, but on the other hand people did not know about the current major attacks faced by organizations. For example, when asked about the Ransomware attack reported by the New York Times in 2018, only 40% knew about the correct answer, which was Ryuk. As for the WannaCry attack on Windows OS in the year 2017, 70% people knew about it.

Keeping the Covid-19 in mind we wanted to know what in the public's opinion was the main reason for the rise of ransomware. 50% of the people thought that it was due to downloading malicious files from emails related to Covid-19 precautions and announcements. The other 50% thought that it was due to poor security systems, renting unsanctioned copyrighted materials, or clicking on malicious advertisements.

Their views on the main threat actor were quite diverse. Upon being asked what in their opinion are the predominant threat actors behind the attacks, 37.5% people thought that it was skillful professionals, 35% of people believed it to be Individuals with malicious intents, 20% thought it was Nation-states with massive capabilities and 7.5% believed that it was Novice criminals who make minor tweaks to existent variants, with less efficacy.

Common feedback which we got while conducting the survey was that people found it difficult to answer a lot of the questions and made them think deeply upon this topic. In conclusion, the general public need to have more knowledge about Ransomwares and know about its increasing strength in this era of technology.

CHAPTER-6

CONCLUSIONS AND RECOMMENDATION

6.1 OUTLINE

In this project report, we have explored the A-Z of Ransomware; from the definition of ransomware to its application in the ransomware-as-a-service (RaaS) industry, acting as a lucrative business model for the cybercriminals and the nightmare for the various business and service organizations.

This paper approaches the study of ransomware in a comparative model, to understand the evolution of ransomware from various parameters, not limited to but including its diverse variants, method of deliverance, the attack vector, impact it had on affected data and timeline to remove the ransomware.

The paper includes literature reviews of the recent (contemporary) research done around ransomware, thereby acting as a cumulative resource for further studies or reference.

The paper also features 4 case studies of real-world ransomware attack, comparing the affect it had based on the selected parameters. It concludes with a minor survey on the awareness of ransomware and the opinions on this rising industry by the general public.

6.2 LIMITATIONS AND CONSTRAINTS IN THE RESEARCH

Any report based on data and facts is eventually constrained on the data available. In the field of Cyber Security, various variables occur that often do not provide the complete picture of the event and hence may lead to distorted facts and thereby we must rely on various assumptions in the statistics and trust the data provided by the organizations and the nation states.

The numerous examples/cases when and how the data differs have been discussed further.

A case study from Recorded Future, noted the difference between the actual dates of ransomware attack and their response times along with the public disclosure dates of the event in Germany that occurred in 2021.

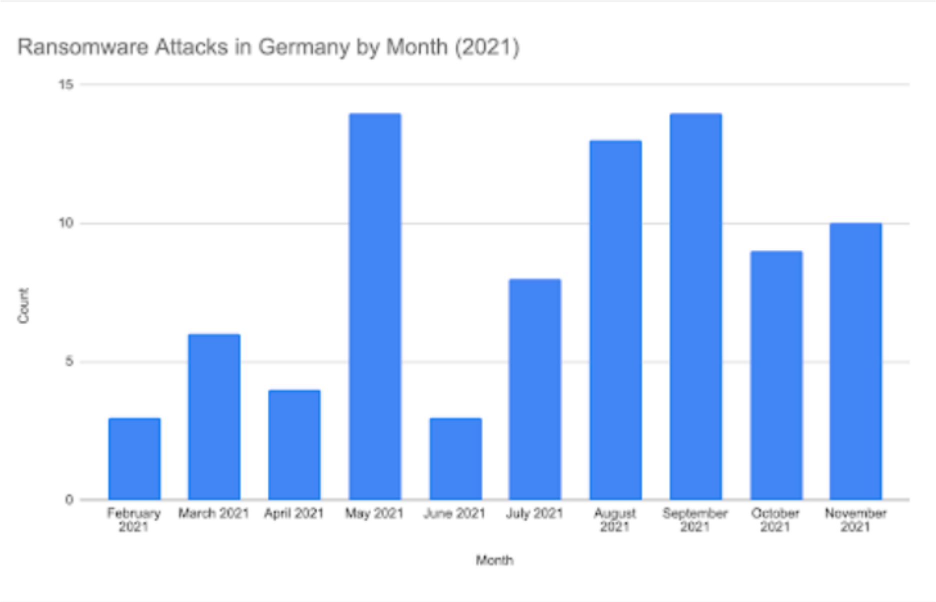


Figure 6.2.1: Comparison of ransomware attacks posted to extortion sites, compared to when the attacks occurred

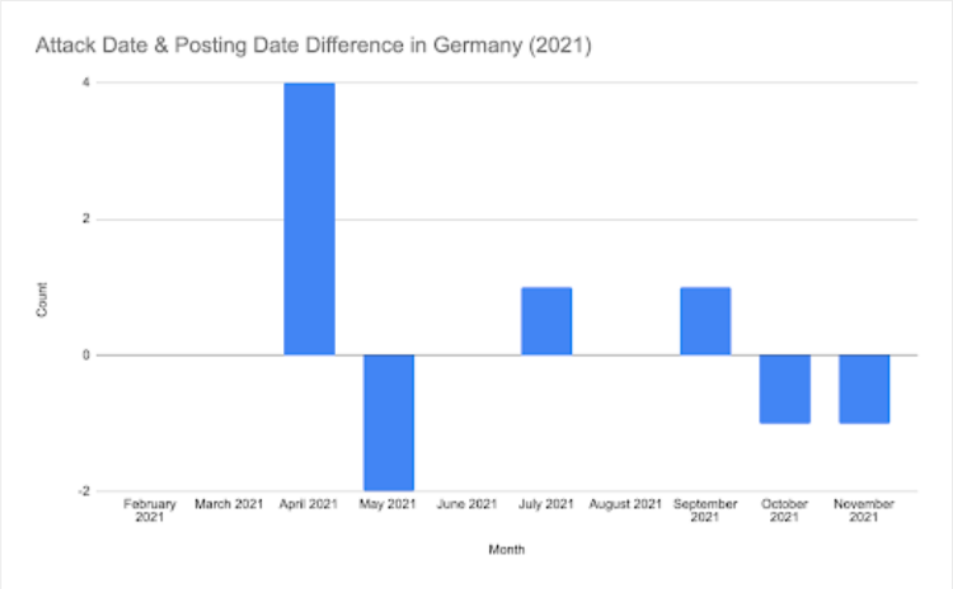


Figure 6.2.2: Showing the difference between when attacks are reported and when they happen

The occurrence of the attacks differs by the geographical location. Like, we observe that in the first half of the year publicly reported ransomware attacks were only around 42% and the second half constituted 58% of the thereby noting an increase in the occurrence of the attacks towards the latter half. While there were 242 publicly reported ransomware attacks in France through the end of November, according to Rieß-Marchive; looking at the breakdown by half year, 63% of the attacks occurred in the first half of 2021 and 37% in the second half.

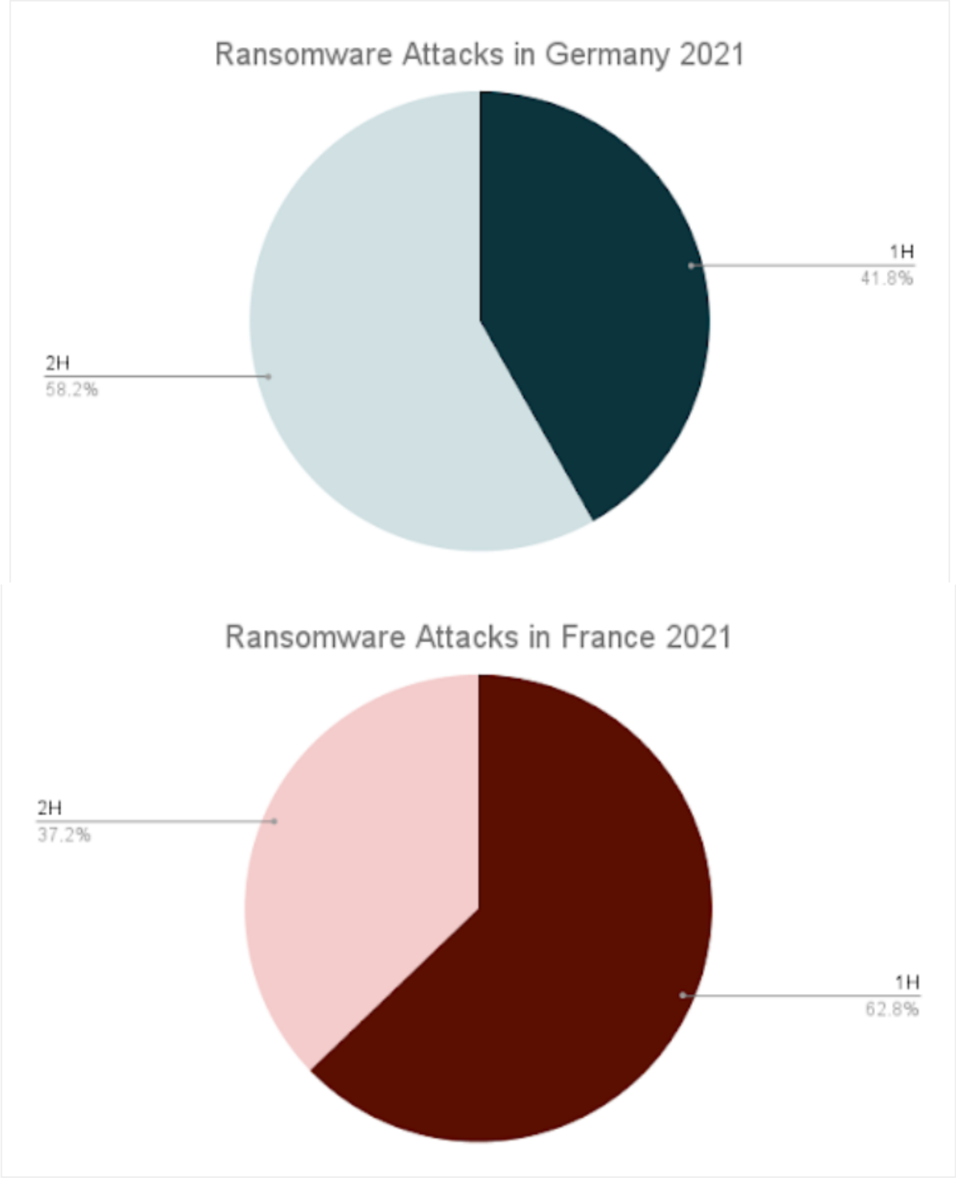


Figure 6.2.3: Comparison between publicly reported ransomware attacks in Germany and France (Source: Recorded Future)

This statistic may also be affected due to non-disclosure of the attacks by the affected organizations. As Figure 6.2.4 demonstrates, there is a huge gap between what is being publicly and privately reported. Ransomware attacks may be continuing their increase, but fewer of them are being publicly reported. Ransomware groups know these attacks generate a lot of attention and they may not want the type of negative attention that comes from these attacks so they are focusing their efforts on sectors that don’t draw criticism.

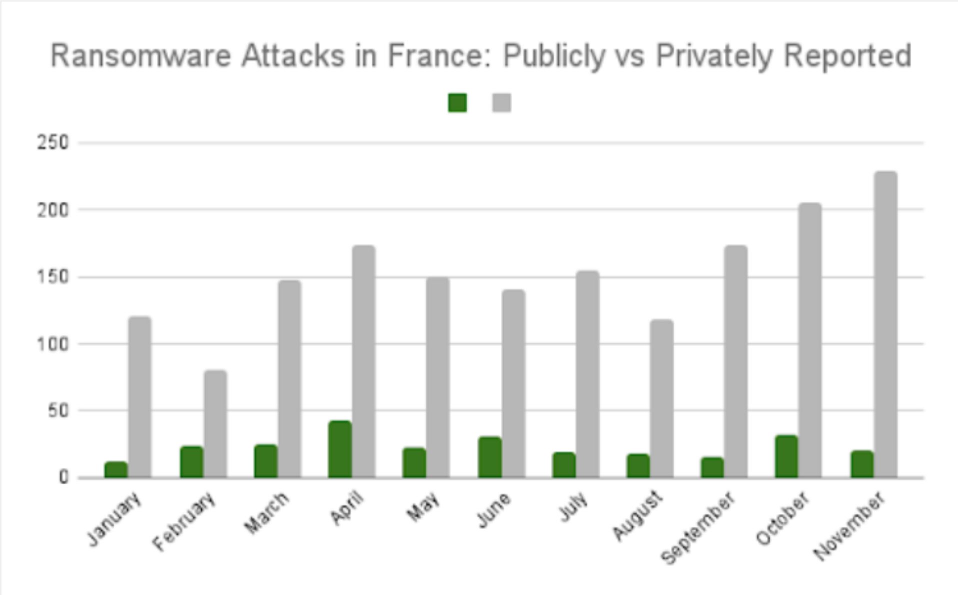


Figure 6.2.4: Ransomware attacks in France, publicly reported versus privately reported in 2021 (Source: Recorded Future)

6.3 FUTURE ENHANCEMENTS

This project report is currently limited to the data available till 22nd December, 2021. As the world becomes more aware of the ransomware attacks and its direct implications on the daily life of the people is felt, nation states would have to develop stringent security policies and laws and organizations would have to publicly disclose their confrontations with such situations to tackle these issues.

For example, 2021 has seen unprecedented global law enforcement action taken against ransomware groups. The 30-nation ransomware task force led by the United States appears to be seeing early success with almost weekly announcements against ransomware groups.

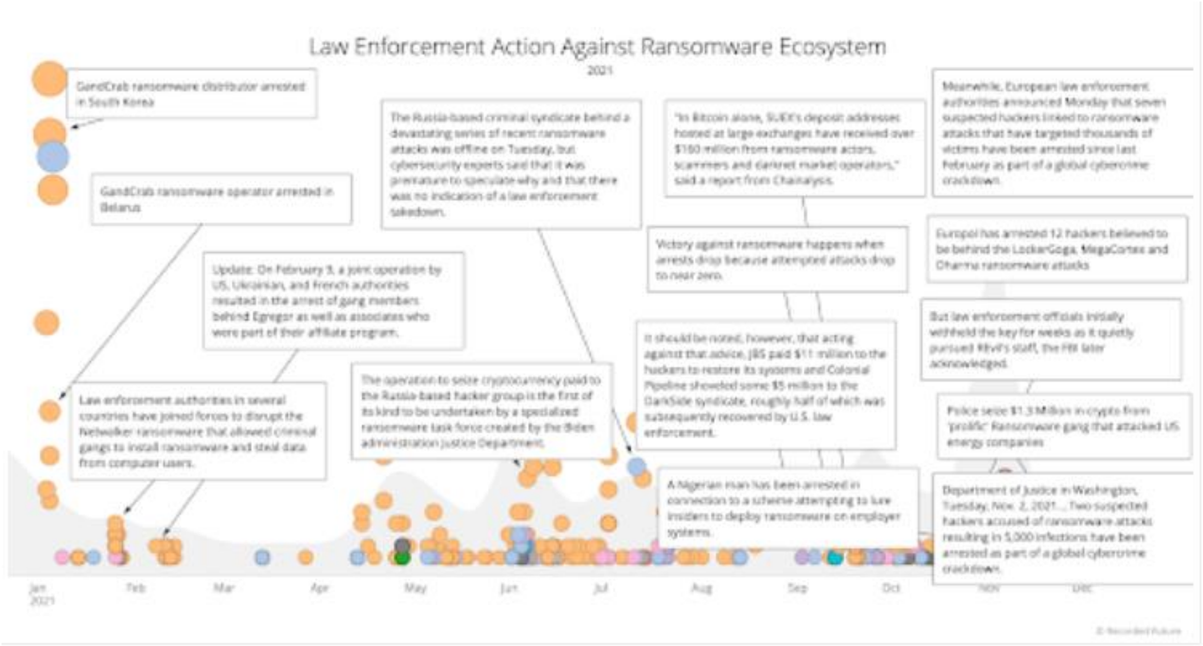


Figure 6.3.1: Some of the law enforcement action taken against ransomware groups in 2021 (Source: Recorded Future)

The 30-nation ransomware task force led by the United States came into effect when ministers and representatives of the participating governments met virtually on 13-14 October 2021 to discuss a consolidated approach to the increasing cyber threat posed by ransomware attacks. It is noteworthy that the representatives agreed to use diplomacy to tackle challenges presented by ransomware. Among the nations that signed the joint statement are the US, EU (and some individual EU member states, e.g., France, Germany, Netherlands, Italy, Estonia), the UK, Australia, Japan, Singapore, Canada, Israel, Brazil, South Africa, and Nigeria.

The key steps set out in the joint statement include:

- Improving network resilience to prevent and respond to ransomware incidents.
- Addressing the abuse of financial mechanisms to launder ransom payments or conduct other activities that make ransomware profitable.
- Disrupting the ransomware ecosystem via timely and consistent collaboration (both domestic and international) of law enforcement to investigate and prosecute ransomware crimes

6.4 INFERENCE

After studying so much about ransomware and reviewing papers on it, we have learnt that newer solutions and proper SIEM to tackle ransomware attacks are required. Cyber Security researchers continuously need to monitor software and system infrastructure along with patching vulnerabilities. Everyday new vulnerabilities are found and these need to be patched quickly to avoid severe consequences. In the end of year 2021, he revelation of the Log4Shell vulnerability has, for some organizations, been augmented by a ransomware attack on Ultimate Kronos Group (UKG), one of the biggest HR and workforce management solutions providers in the US. Many organizations use Kronos for organizing workers' schedules, tracking vacations, processing payroll and bonuses, etc. Such attacks are not only costly economically but also is a breach of privacy of the users as their confidential data gets compromised in the hands of cyber criminals.

To conclude with this paper, listed below are some of the preventive measures to avoid ransomware attacks:

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

If ransomware attacks need to decrease overall, it is not just possible by increasing law enforcement. There is anecdotal evidence that cyber insurance companies are requiring that policyholders have more stringent cybersecurity protections in place before they will renew a policy and, according to a source, companies are spending 12% more on cybersecurity this year which is only expected to rise in coming years. The combination of law enforcement activity, more effective cybersecurity spending, and better controls put in place by cyber insurance companies may contribute to the decline.

This data is very comprehensive, but it is a trend that bears watching and something we will continue to monitor and update.

REFERENCES

1. Jinal P. Tailor and Ashish D. Patel, *"A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control"* 2017, 4 (6S), 2321–2705 IJRSI link A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control (rsisinternational.org)

2. A.K. Maurya, N. Kumar, Dr. Alka and Prof. R. A. Khan, *"Ransomware: Evolution, Target and Safety Measures"* 2018, 6(1), 2347-2693, International Journal of Computer Sciences and Engineering link https://www.researchgate.net/profile/Neeraj-Kumar-179/publication/325777408_Ransomware_Evolution_Target_and_Safety_Measures/links/5bc5bfdea6fdcc03c789073c/Ransomware-Evolution-Target-and-Safety-Measures.pdf

3. N. Hampton, Z. Baig, and S. Zeadally, ''*Ransomware behavioural analysis on Windows platforms*,'' J. Inf. Secur. Appl., vol. 40, Jun. 2018 link https://www.sciencedirect.com/science/article/abs/pii/S2214212617306506#keys0001

4. Samir Thakkar, *"Ransomware-Exploring the Electronic form of Extortion"* 2014, 2(10), 2321-0613 IJSRD link https://www.researchgate.net/profile/SamirThakkar/publication/308802806_Ransomware__Exploring_the_Electronic_form_of_Extortion/links/581ae2f908aed2439386d642/Ransomware-Exploring-the-Electronic-form-of-Extortion.pdf

5. Subhash Poudyal and Dipankar Dasgupta "*Analysis of Crypto-Ransomware Using ML-Based Multi-Level Profiling"* 2021, 10.1109, ACCESS.2021.3109260, IEEE link IEEE Xplore Full-Text PDF:

6. Savita Mohurle and Manisha Patil, *"A brief study of WannaCry Threat: Ransomware Attack 2017"*, 2017, 8(5), 0976-5697, International Journal of Advanced Research in Computer Science link https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

7. Ronny Richardson, Max M. North and David Garofalo, *"Ransomware: The Landscape Is Shifting --A Concise Report"*, 2021, 17(1), 5-8,86 link http://www.americanscholarspress.us/journals/IMR/pdf/IMR-1-2021/V17n121-art1.pdf

8. Joseph Johnson, *"Global Internet Access Rate [2005-2019]"*, 2021, https://www.statista.com/statistics/209096/share-of-internet-users-in-the-total-world-population-since-2006/

9. Symantec Corporation, *"Internet Security Threat Report [ISTR]"*, 2019, 24, https://docs.broadcom.com/doc/istr-24-2019-en
10. https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types
11. https://en.wikipedia.org/wiki/Ransomware#History
12. https://www.paloaltonetworks.com/cyberpedia/ransomware-common-attack-methods
13. https://app.diagrams.net/
14. https://www.lifewire.com/what-is-a-master-boot-record-mbr-2625936

15. https://content.secureworks.com/-/media/Images/Insights/Resources/Threat%20Analysis/010%20cryptowall%20ransomware/cryptowall_ransomware_05.ashx?h=252&w=500&hash=E4A8C37E4E26AD3CF269B3C499729F0400A33A0B&la=en&modified=20210602184150
16. https://content.secureworks.com/-/media/Images/Insights/Resources/Threat%20Analysis/000%20cryptolocker%20ransomware/img014.ashx?la=en&modified=20160216143258&hash=E59B62CC568ED01C2D8A351608BD7505
17. International Telecommunication Union [ITU], *“Measuring Digital Development: Facts and Figures”*, 2020, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf
18. https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf
19. https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/
20. https://www.tcdi.com/ransomware-timeline/
21. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
22. https://en.wikipedia.org/wiki/Ransomware
23. https://www.proofpoint.com/us/threat-reference/ransomware
24. https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html
25. https://www.crowdstrike.com/resources/infographics/ransomware-during-covid-19/
26. https://www.trendmicro.com/en_in/what-is/ransomware/ryuk-ransomware.html#ryuk-attack-tm-anchor
27. https://forms.gle/ftRz1Z9BLaeEKkUb7
28. Top 5 ways ransomware is delivered and deployed - Infosec Resources (infosecinstitute.com)
29. What is Ransomware? - How is Ransomware Delivered?- Tessian
30. Common Types of Ransomware Strains & How to protect systems (datto.com)
31. Bad Rabbit - Ransomware | Qualys Security Blog
32. https://www.sitelock.com/blog/what-is-cerber-ransomware/
33. https://www.varonis.com/blog/cryptowall/
34. https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/petya.html
35. How to remove MISCHA Ransomware - virus removal steps (updated) (pcrisk.com)
36. Jigsaw (ransomware) - Wikipedia
37. Ransomware WannaCry: All you need to know | Kaspersky
38. (14) How To Recover Data Encrypted By Ryuk Ransomware? | LinkedIn
39. What is Maze Ransomware - Definition and explanation | Kaspersky
40. Most Common Types of Ransomware | CrowdStrike
41. Complete Guide to Ransomware: How to Recover and Prevent an Attack (backblaze.com)
42. Ransomware | KnowBe4
43. https://www.jdsupra.com/legalnews/representatives-of-over-30-nations-to-1481874/
44. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

45. https://www.recordedfuture.com/are-ransomware-attacks-slowing-down/?utm_medium=email&_hsmi=198040784&_hsenc=p2ANqtz-_Z1ic1W2ev6jNa3ux5WU6Wm6NEHuYutOw3W2Upl6B4Ifs9Ayl_Dy9XYm_1caqmRH5gyS9A3D7ZN3FdxN5ftwGxFfkph2s7wkQTKMwKf_d0LP60fZU&utm_content=198040784&utm_source=hs_email
46. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22