UET-VNU

RANSOMWARE

Student Name: Le Manh Cuong
Student ID: 19021231
Unit Code: INT3307 21
Unit Name: Network safety and Security
Name of lecturer: Dr. Nguyen Dai Tho

Ransomware: Evolution, types, and Preventions

Le Manh Cuong – Student ID:19021231

INT 3307_21- Network safety and Security

VNU University of Engineering and Technology

VNU-UET

Due Date: 10/1/2022

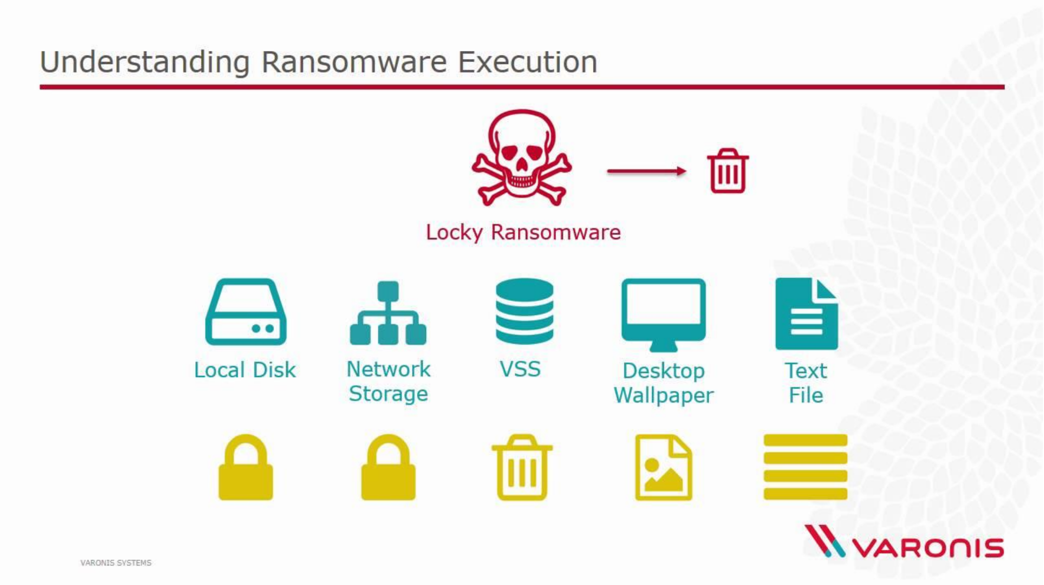
Abstract

Under the influence of covid, the Internet has become closer to people than ever. Therefore, new technologies were born to meet the needs of people's daily lives. Creates a huge opportunity for cybercriminals to make millions of dollars with malware. The most notable is ransomware - a notorious piece of malware that is still growing rapidly. In recent years, ransomware is one of the most notorious malwares that targets end-users, governments, and business organizations. In this article, we present a brief history of ransomware, arguments for and against paying the ransom, how to a ransomware attack, two main types of ransomware, and prevention techniques.

TABLE OF CONTENTS

I. INTRODUCTION: AN OVERVIEW OF RANSOMWARE

Nowadays, the number of internet users is out increasing rapidly. *Specifically, up to now, there are nearly 4.66 billion internet users worldwide with a rate of 59.5%.[1]* With such a large number of users, there are many development opportunities for enemies to attack the network. Therefore, cybercrime is increasing day by day and creating many dangers to users and many problems for network security. One of the scary enemies is a Ransomware attack.



As defined by Wikipedia: *Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. [2]*

Ransomware is a growing form of computer crime that is hitting all types of organizations, including law enforcement. Ransomware is malicious software that once loaded on a victim system encrypts the hard drive and issues a warning that unless a ransom is paid within a short time, all the data will become unrecoverable. The software then tells the victim to typically spend between $250 and $1,000 to the criminal within the allotted period, usually via bitcoin. When the ransom is paid, the criminal will send the victim an alphanumeric sequence to unlock the malware. [3]

At its heart, this form of digital extortion can be broken down into two major types, and then subdivided based on the families they represent. The two major forms of ransomware are those that encrypt, obfuscate, or deny access to files and those that restrict access or lock users out of the systems themselves. These threats are not limited to any particular geography or operating system and can take action on any number of devices. Everything from your Android devices, iOS systems, or Windows systems all is at risk of this type of exploitation via ransomware. Depending on the target, the method of compromise of the device may be different, and the final actions taken would be limited by the device's capability itself, but there are also recognizable patterns that many extortionists follow.[4]

The victims are usually by clicking on some phishing message or downloading some malware that impersonates the ransomware of malicious websites. To then have to pay a ransom in a relatively short time because to prevent the victim from finding alternative decryption methods.

Ransomware remains one of the most profitable tactics for cybercriminals. According to Cybersecurity Ventures, the global cost of ransomware in 2020 is estimated at $20 billion, and the average ransom payment totaling **$1.79 million.**

Below are some 2021 ransomware statistics from CrowdStrike's annual Global Security Attitude Survey:

- the **average ransom payment increased by 63% in 2021** to $1.79 million (USD), compared to $1.10 million (USD) in 2020
- the **average ransom demand from attackers** is $6 million
- 96% of those who paid the initial ransom **also had to pay extortion fees**
- 66% of respondents' organizations **suffered at least one ransomware attack this year**
- 57% of those hit by ransomware **didn't have a comprehensive strategy** in place to coordinate their response [5]

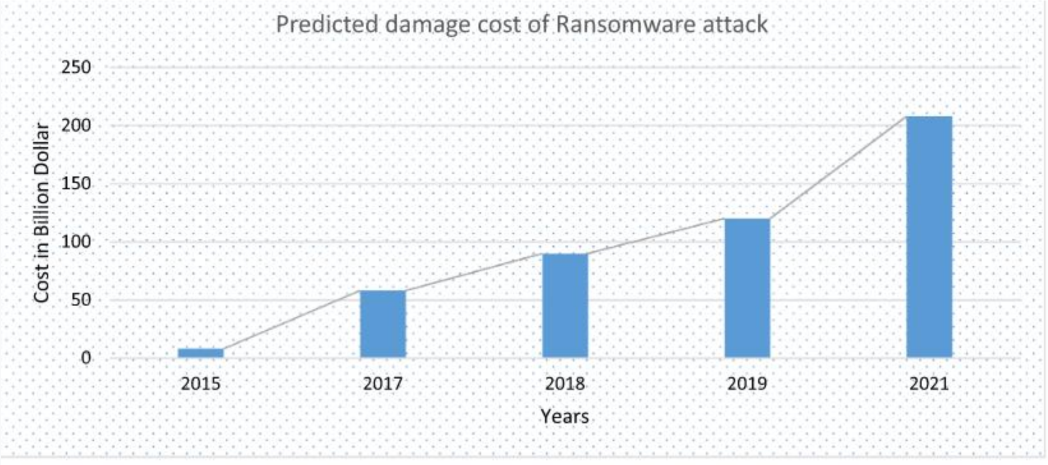


Figure 1: predicted damage cost of a ransomware attack five years ago [4]

Given the high level of danger, sophisticated methods as described above show the need to provide awareness to researchers and academic members about the importance of attack tools, how their operation? What can recovery measures be? In case, if an organization or individual becomes the target of a Ransomware attack? And this is only possible by providing a detailed picture of the ransomware attack tools.

According to my research, many ransomware reports are not detailed and specific. In this article, I will try to synthesize personal opinions or fill in the gaps about ransomware that may not have been mentioned to give you the most detailed and complete picture. about ransomware like the evolution of ransom, ransomware attack, ransom should be paid or not, and prevention techniques.

II. LITERATURE SURVEY

In this section, we provide a detailed overview of the current state of Ransomware attacks. This section consists of 4 subsections and each section provides the user with relevant knowledge to understand the details of the Ransomware attack. Section 2.1 provides the development of Ransomware attacks and why and why cybercriminals use trading virtual currency. Section 2.2 describes how are ransomware attacks and two main types of Ransomware details and some of the ransomware variants. Section 2.3 will evaluate the positive and negative about paying the ransom when attacked by ransomware. This document ends in section 2.4 providing the main challenges of Ransomware attacks along with prevention techniques.

To have an in-depth and comprehensive view of them, I have collected many books, articles published by the Institute of Electrical and Electronics Engineers (IEEE), ScienceDirect, Wikipedia, OReilly, crowdstrike and many data sources searched on google scholar for discussion and analysis. Find out the key limitations along with how we can improve and deliver better solutions for each of them.

1. EVOLUTION OF RANSOMWARE

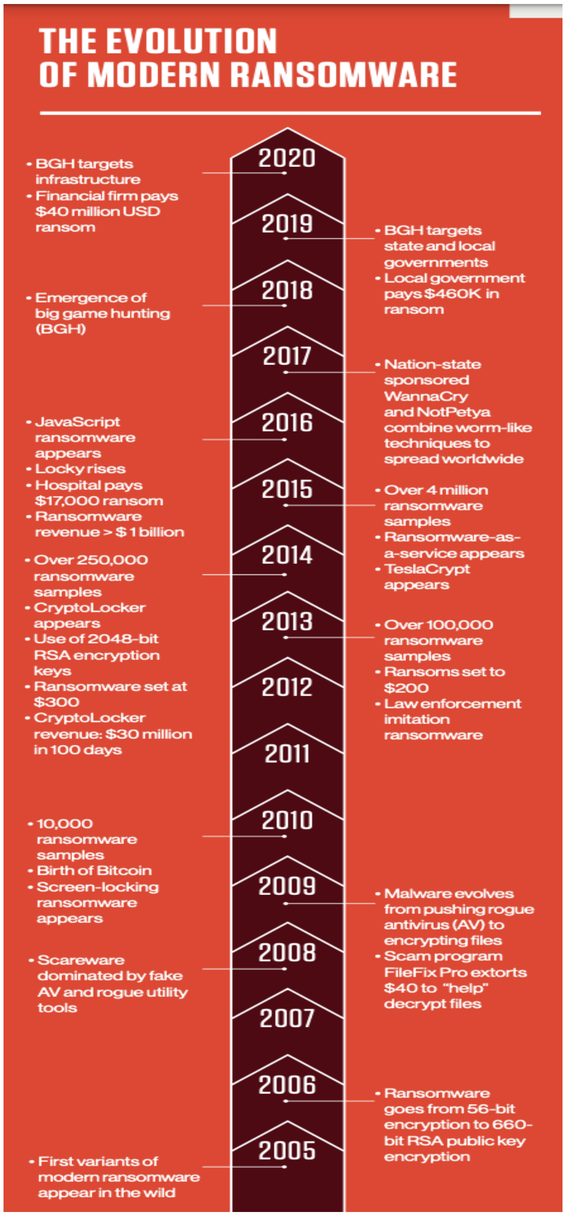

THE EVOLUTION OF MODERN RANSOMWARE
2020
• BGH targets infrastructure
• Financial firm pays $40 million USD ransom
2019
• BGH targets state and local governments
• Local government pays $460K in ransom
2018
• Emergence of big game hunting (BGH)
2017
• Nation-state sponsored WannaCry and NotPetya combine worm-like techniques to spread worldwide
2016
• JavaScript ransomware appears
• Locky rises
• Hospital pays $17,000 ransom
• Ransomware revenue > $1 billion
2015
• Over 4 million ransomware samples
• Ransomware-as-a-service appears
• TeslaCrypt appears
2014
• Over 250,000 ransomware samples
• CryptoLocker appears
• Use of 2048-bit RSA encryption keys
• Ransomware set at $300
• CryptoLocker revenue: $30 million in 100 days
2013
• Over 100,000 ransomware samples
• Ransoms set to $200
• Law enforcement imitation ransomware
2012
2011
2010
• 10,000 ransomware samples
• Birth of Bitcoin
• Screen-locking ransomware appears
2009
• Malware evolves from pushing rogue antivirus (AV) to encrypting files
• Scam program FileFix Pro extorts $40 to "help" decrypt files
2008
• Scareware dominated by fake AV and rogue utility tools
2007
2006
• Ransomware goes from 56-bit encryption to 660-bit RSA public key encryption
2005
• First variants of modern ransomware appear in the wild

Figure 2: evolution of ransomware[7]

Although over the years, we still regularly see ransomware appearing on several cybersecurity sites and in many scientific journals. Ransomware is made with the idea of evaluating the files of the worker by encrypting the files and will interfere with your system when you access the files or use some method so that you cannot execute the file. Do your job with that file and then request to send the money back within a certain period. That implementation method is quite old.

In the late 1980s, criminals were already holding encrypted files hostage in exchange for cash sent via the postal service. One of the first ransomware attacks ever documented was the AIDS trojan (PC Cyborg Virus) that was released via floppy disk in 1989. Victims needed to send $189 to a P.O. box in Panama to restore access to their systems, even though it was a simple virus that utilized symmetric cryptography.[7]

fig 2 will show you the history of ransomware over the years. Specifically, the initial five ransomware when it appeared did not pay much attention and until 2010, with the appearance of bitcoin, ransomware became a lucrative and rapid development. eCrime – a broad category of malicious activity that includes all types of cybercrime attacks, including malware, banking trojans, ransomware, mineware (cryptojacking), and crimeware because not all victims know how to transact with bitcoins[7]. But it is still increasing rapidly, nowadays even high school students in a developing country like Vietnam know bitcoin and even know how to use virtual money. Because of that, we see the tremendous growth of the ransomware crime industry. As for why cybercriminals choose bitcoin, choose the virtual currency for transactions is because: Bitcoin exchanges provided adversaries the means of receiving instant payments while maintaining anonymity, all transacted outside the strictures of traditional financial institutions.

Ransomware could become a billion-dollar cybercrime industry and is growing more destructive and ransomware ransoms are getting bigger.

in my opinion: Ransomware is really growing, we didn't explode in bitcoin, blockchain a few years ago like now. That's because ransomware is growing in popularity and criminals need more transactions.

2. RANSOMWARE ATTACK

In this section, I will answer for you three main questions. Firstly, how does a ransomware attack, secondly the types and turns them into ransomware, thirdly, is ransomware the trend of the times?

A. FIRST, HOW IS THE ATTACK RANSOMWARE?

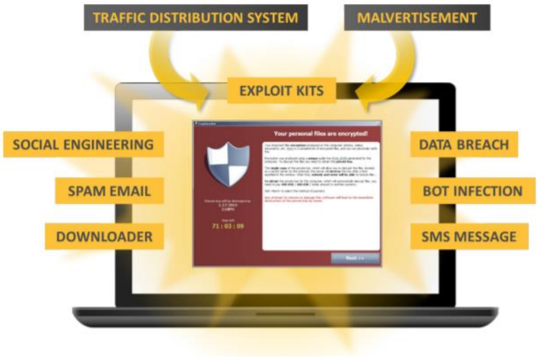


Figure 3: Routes for ransomware to arrive on a computer[8]

Today, ransomware is commonly distributed through highly targeted phishing emails, social engineering schemes, vulnerability attacks, or malicious ad networks. In most cases, the victim will click on a malicious link that introduces the ransomware variant on their device. Once a device or system is infected, the ransomware works immediately to identify and encrypt the victim's files. Once the data has been encrypted, a decryption key is required to unlock the file. To obtain the decryption key, the victim must follow instructions left on the ransom note stating how to pay the attacker - usually in Bitcoin. [8] Threat actors rely on personal and business users becoming so frantic about regaining timely access to data that they will be willing to offer a hefty ransom for the decryption key. required to unlock data.

B. TYPES OF RANSOMWARE

As a research article once said:

“Despite having similar objectives, the approaches taken by each type of ransomware are quite different”

Therefore, to facilitate the evaluation and analysis of the methods of cybercriminals in ransomware, although ransomware has many variants and is difficult to identify ransomware will be divided into 2 main types and some exceptions.

Two main types of ransomware:

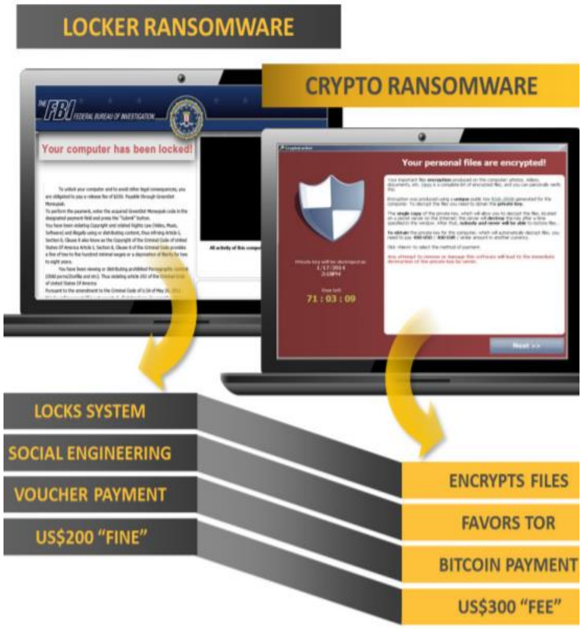


Figure 4: Two main types of ransomware are locker ransomware and crypto-ransomware[8]

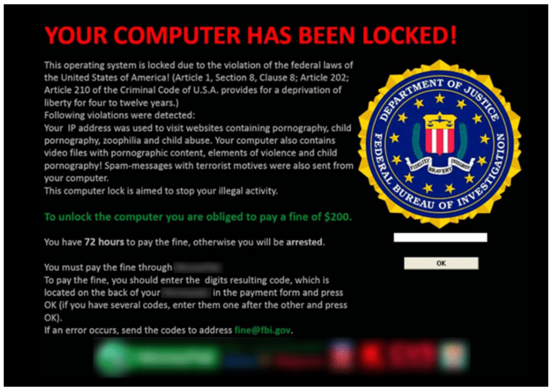
Screen Lockers:

Locker ransomware is designed to deny access to computing resources. This typically takes the form of locking the computer’s or device’s user interface and then asking the user to pay a fee to restore access to it. Locked computers will often be left with limited capabilities, such as only allowing the user to interact with the ransomware and pay the ransom. This means access to the mouse might be disabled and the keyboard functionality might be limited to numeric keys, allowing the victim to only type numbers to indicate the payment code.

The screen locker

Crypto ransomware or encryptors:

This type of ransomware is designed to find and encrypt valuable data stored on the computer, making the data useless unless the user obtains the decryption key*[8]*



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Figure 5: example of locker ransomware

we can see that it only locks the screen and our controls. As a result, nearly all files are recoverable, and ransomware can be deleted to restore the computer to its original state. That is also one of its weaknesses, making it weaker than other ransomware that destroys more data because victims may not be too scared if they know they are attacked by lock ransomware. For that reason, usually, ransomware attacks will often pretend to be a government or a legal agency that sends a penalty request for some reason. It may seem less effective for some individuals, but it is very effective for some cases with limited user interaction because we can't perform some recovery methods, or we can't lose its files because may be fined…

From that, we can see it will be a big potential today when wearable devices and IoT are on the throne.

With crypto ransomware

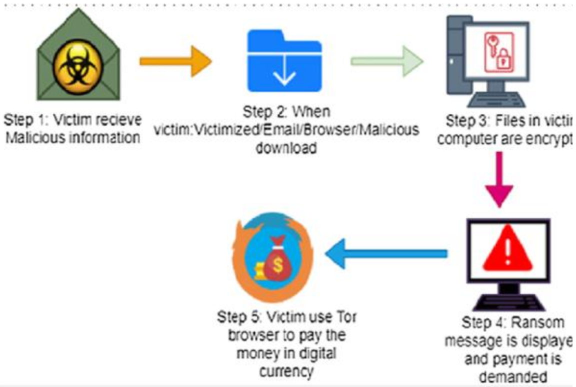
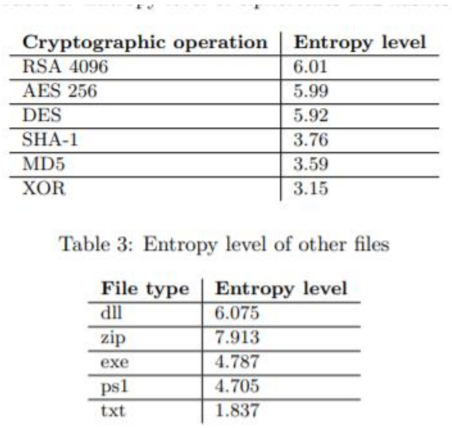

Step 1: Victim recieve Malicious information
Step 2: When victim:Victimized/Email/Browser/Malicious download
Step 3: Files in victi computer are encrypt
Step 4: Ransom message is displaye and payment is demanded
Step 5: Victim use Tor browser to pay the money in digital currency

Figure6 : crypto ransomware: how to attack[3]

we can have a small example. If the victim loses data, such as memories with his lover or confidential company data urgently. They will certainly accept to pay hundreds of dollars for the return.

So why does crypto-only take files that are important to the object, or do it take all the files of the object and then encrypt it? Here, after the computer installs crypto ransomware, it will hide in the computer and search for important data with the victim without the computer knowing it exists. By the time the computer receives the notification, it has finished encrypting the important files it finds. And here the computer will be able to access and use it normally but cannot access and infected files. If you want to access those files, you will have to enter the code it provides. Usually, the cost to get back such files will be much higher than the cost of getting the code from cybercriminals. That's why when

infected Crypto ransomware victims
tend to pay more.



Cryptographic operation	Entropy level
RSA 4096	6.01
AES 256	5.99
DES	5.92
SHA-1	3.76
MD5	3.59
XOR	3.15

Table 3: Entropy level of other files

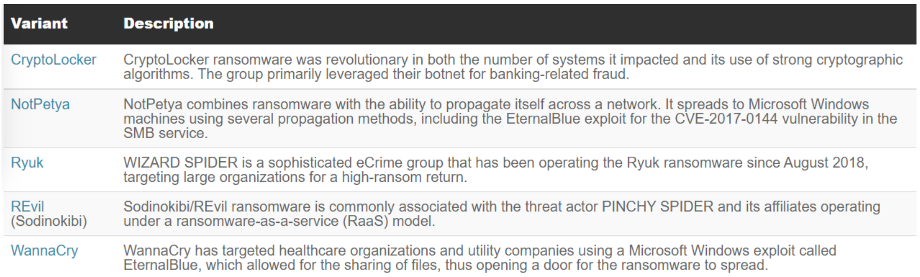
File type	Entropy level
dll	6.075
zip	7.913
exe	4.787
ps1	4.705
txt	1.837

Figure 7 : example entropy the file[11]

The way ransomware identifies files as important is by entropy, a measure of a file that refers to a random unit -Shannon entropy. It is a measure of the randomness of the data in the file on a hierarchy from 1-8, usually text files are low-level. And compressed encrypted files have a high value.[11] So don't think that it will miss your important files, but help you delete junk files because no one will compress junk files again.

From there, we can see that crypto ransomware is more dangerous than lock ransomware, so criminals, tend to be more prone to crypto ransomware.

For example, some variants of ransomware according to research by "Kurt Baker - December 29, 2021" on types of ransomware on crowdstrike:



Variant	Description
CryptoLocker	CryptoLocker ransomware was revolutionary in both the number of systems it impacted and its use of strong cryptographic algorithms. The group primarily leveraged their botnet for banking-related fraud.
NotPetya	NotPetya combines ransomware with the ability to propagate itself across a network. It spreads to Microsoft Windows machines using several propagation methods, including the EternalBlue exploit for the CVE-2017-0144 vulnerability in the SMB service.
Ryuk	WIZARD SPIDER is a sophisticated eCrime group that has been operating the Ryuk ransomware since August 2018, targeting large organizations for a high-ransom return.
REvil (Sodinokibi)	Sodinokibi/REvil ransomware is commonly associated with the threat actor PINCHY SPIDER and its affiliates operating under a ransomware-as-a-service (RaaS) model.
WannaCry	WannaCry has targeted healthcare organizations and utility companies using a Microsoft Windows exploit called EternalBlue, which allowed for the sharing of files, thus opening a door for the ransomware to spread.

Figure 10: example variant of ransomware[7]

Ransomware is evolving as strongly as covid, so it has too many more contagious and more dangerous variants. The trend of ransomware is more destructive to the victim's data (the victim does not pay the ransom, the data will be automatically deleted - cryptolocker, super-infection -WannaCry...). So, ransomware can be understood as the trend of the times when it directly interacts with the victim without having to go through an intermediary like other malware.

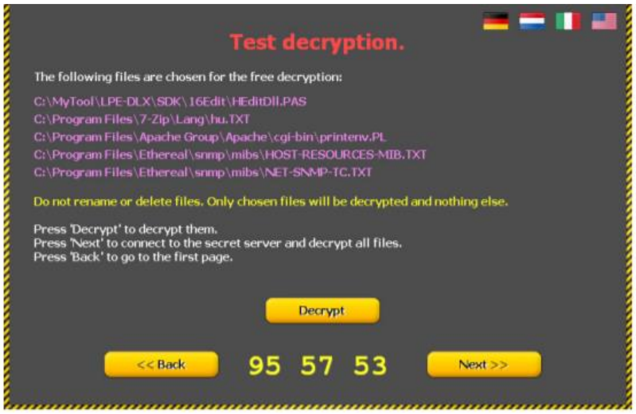
3. RANSOM SHOULD BE PAID OR NOT

This is just a small part of ransomware variants; it can be seen that this ransomware industry is very developed and diverse. So, is paying the ransom right or wrong?

If a business or an individual is attacked by ransomware, should they return the money or not to the individual just need to answer **3 questions**? Is the data value greater than the ransom value? Is the data sure to get back when sending money or not? Also, are paying criminals backing what they're doing?

The FBI does not support paying a ransom in response to a ransomware attack. They argue paying a ransom not only encourages the business model, but also may go into the pockets of terror organizations, money launderers, and rogue nation-states. Moreover, while few organizations publicly admit to paying ransoms, adversaries will publicize that info on the dark web – making it common knowledge for other adversaries looking for a new target. From that, we see that paying the ransom is not recommended [7]

Ransomware criminals seem to have enough business sense to realize that if there is a rumor that they will not provide a decryption code after the ransom is paid; Their business model will fail, and the victim will stop paying. Some ransomware schemes try to build trust by decrypting a few files before paying the ransom. Software to make you believe that scope can send you data We have used many methods such as：



Test decryption.

The following files are chosen for the free decryption:

```
C:\MyTool\LPE-DLX\SDK\16Edit\HEditDll.PAS
C:\Program Files\7-Zip\Lang\hu.TXT
C:\Program Files\Apache Group\Apache\cgi-bin\printenv.PL
C:\Program Files\Ethereal\snmp\mibs\HOST-RESOURCES-MIB.TXT
C:\Program Files\Ethereal\snmp\mibs\NET-SNMP-TC.TXT
```

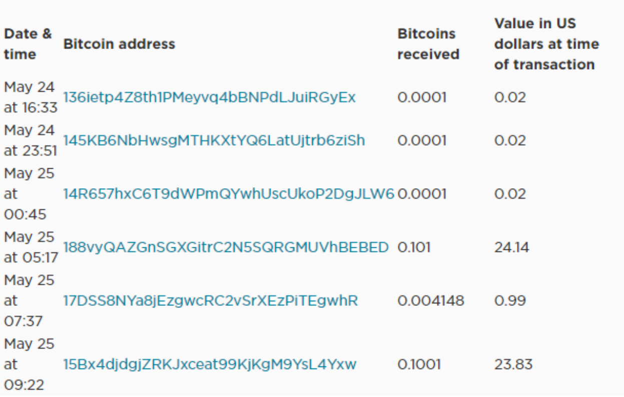
Do not rename or delete files. Only chosen files will be decrypted and nothing else.

Press 'Decrypt' to decrypt them.
Press 'Next' to connect to the secret server and decrypt all files.
Press 'Back' to go to the first page.

Figure 11: CTBLocker offers a “try-before-you-buy” service[8]

Trojan.Cryptlocker.G has the option to decrypt five randomly selected files for free. In other cases, corporate victims can negotiate lower fees. From there, we see that paying the ransom to get the data back has a high probability of success, but you will lose a large amount.

I will give some cases of attacks that can be redeemed by some agencies as noted:



Date & time	Bitcoin address	Bitcoins received	Value in US dollars at time of transaction
May 24 at 16:33	136ietp4Z8th1PMeyvq4bBNPdLJuiRGyEx	0.0001	0.02
May 24 at 23:51	145KB6NbHwsgMTHKXtYQ6LatUjtrb6ziSh	0.0001	0.02
May 25 at 00:45	14R657hxC6T9dWPmQYwhUscUkoP2DgJLW6	0.0001	0.02
May 25 at 05:17	188vyQAZGnSGXGitrC2N5SQRGMUVhBEBED	0.101	24.14
May 25 at 07:37	17DSS8NYa8jEzgwcRC2vSrXEzPiTEgwhR	0.004148	0.99
May 25 at 09:22	15Bx4djdgjZRKJxceat99KjKgM9YsL4Yxw	0.1001	23.83

Figure 12:example of pay for ransomware[8]

Some of the victim's records are important to them. For women can be some sensitive files. For another, it could be some file that stores their important information like memories they don't want to forget or data about a job they're doing. That's why it's common to pay for ransomware. So if the data is really more important than a ransom then you might consider paying the cybercriminals. However, please consider my own opinions:

My opinion: I still like the saying "*it hurts once then hurts many times*"

So not giving the ransom is more reasonable because:

- **you become a bigger goal**
- **criminals will tell each other you pay and will be targeted for other cybercriminals**
- **Criminals probably won't decrypt your data, although the probability is low**
- **your next ransom will be higher**
- **your payment encourages criminals to keep doing what they are doing.**

And if you really defy all you can consider the following pricing system.[13]

4. PREVENTION TECHNIQUES

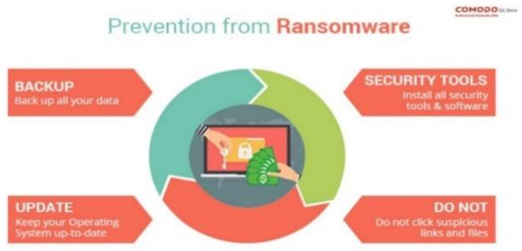

COMODO
Prevention from Ransomware
BACKUP
Back up all your data
SECURITY TOOLS
Install all security tools & software
UPDATE
Keep your Operating System up-to-date
DO NOT
Do not click suspicious links and files

Figure 13: example of prevent ransomware

Herewith the ransomware prevention method, I divide it into two main methods: the first prevention method is for the ransomware to not be able to enter the PC or delete ransomware when it hasn't encrypted any files yet. The second method is that even if the ransomware enters the computer, we are not afraid of losing data. I think method 2 seems better.

A. NOT BE ABLE TO ENTER THE PC OR DELETE RANSOMWARE

Figure 3: you can see that the method of a ransomware attack. And Have key sources of ransomware:

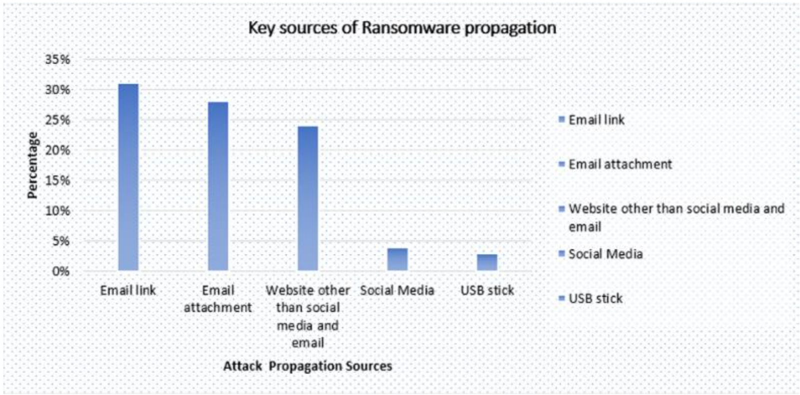
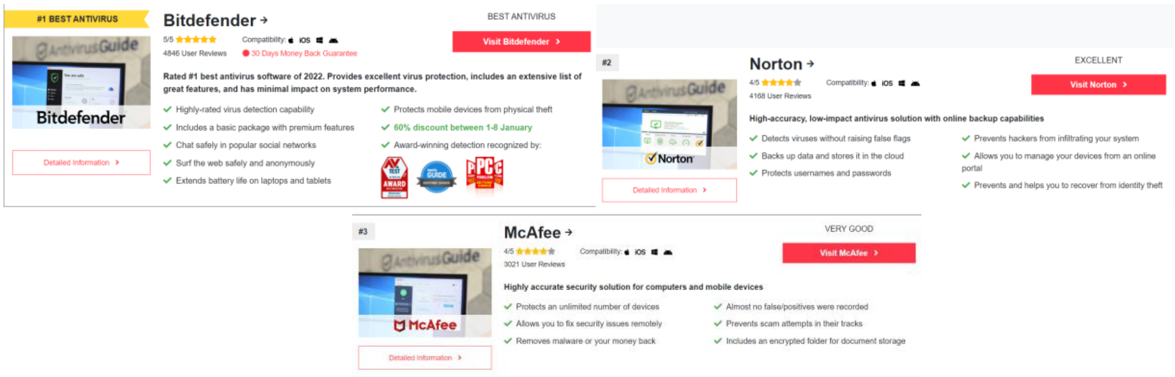


Figure14: Key sources of Ransomware propagation [8]

So, we have methods:

- Do not use free Wi-Fi networks, USB, social MEDIA, origin is not clear.
- Limit clicking on strange links, unknown email addresses.
- Change the default password on all access points.

It sounds easy, but it is impossible to always do all three of the above correctly, so you should try to install some software that can prevent ransomware such as:



#1 BEST ANTIVIRUS

Bitdefender →

5/5 ★★★★★ Compatibility: iOS
4846 User Reviews
● 30 Days Money Back Guarantee

BEST ANTIVIRUS

Visit Bitdefender ›

Rated #1 best antivirus software of 2022. Provides excellent virus protection, includes an extensive list of great features, and has minimal impact on system performance.

✓ Highly-rated virus detection capability
✓ Includes a basic package with premium features
✓ Chat safely in popular social networks
✓ Surf the web safely and anonymously
✓ Extends battery life on laptops and tablets
✓ Protects mobile devices from physical theft
✓ 60% discount between 1-8 January
✓ Award-winning detection recognized by:

Detailed Information ›

#2

Norton →

4/5 ★★★★ Compatibility: iOS
4168 User Reviews

EXCELLENT

Visit Norton ›

High-accuracy, low-impact antivirus solution with online backup capabilities

✓ Detects viruses without raising false flags
✓ Backs up data and stores it in the cloud
✓ Protects usernames and passwords
✓ Prevents hackers from infiltrating your system
✓ Allows you to manage your devices from an online portal
✓ Prevents and helps you to recover from identity theft

Detailed Information ›

#3

McAfee →

4/5 ★★★★ Compatibility: iOS
3021 User Reviews

VERY GOOD

Visit McAfee ›

Highly accurate security solution for computers and mobile devices

✓ Protects an unlimited number of devices
✓ Allows you to fix security issues remotely
✓ Removes malware or your money back
✓ Almost no false/positives were recorded
✓ Prevents scam attempts in their tracks
✓ Includes an encrypted folder for document storage

Detailed Information ›

Figure best anti-ransomware in 2021[9]

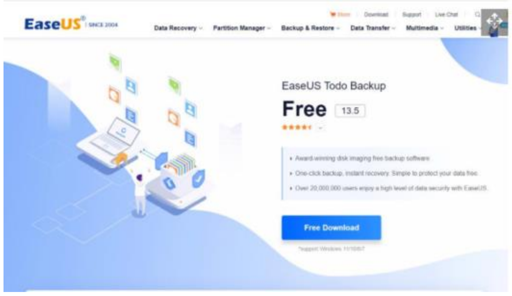
It has a lot of advantages that you can easily see however "Nothing is absolute" is very true. Although both software is very good, there are still shortcomings such as Unlimited VPN access requires a separate subscription (Bitdefender), Online backup strictly for Windows (Norton), Missed some modified ransomware samples(mfcafe)…fee.

Because of that, if you are an individual user, it is more reasonable to use the data-saving way.

B. DATA SAVING

You can often or use USB or some other manual tool to save the data. But with this method, it is not as good as installing software like Bitdefender. Because manual storage can cause damage and loss, it may not be possible to store new data in time. So, the best way today is to use software that can backup data and update regularly such as:

- **EaseUS**: A perfect balance of automatic protection and manual control



EaseUS Todo Backup

Free 13.5

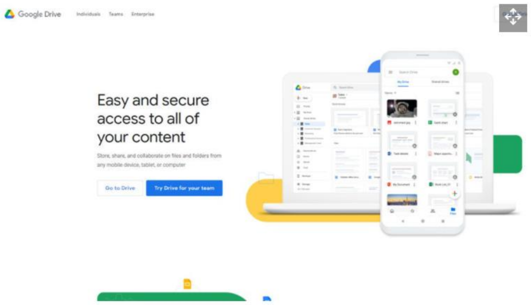
- Award-winning disk imaging free backup software
- One-click backup, instant recovery. Simple to protect your data free.
- Over 20,000,000 users enjoy a high level of data security with EaseUS.

*Support Windows 11/10/8/7

EaseUS Todo Backup Free has lots of bases covered: backing up individual files and folders, whole drives or partitions, or creating a full system backup. There's also a 'smart' option that automatically backs up files in commonly used locations, and you have the option of using cloud storage.

Backups can then be scheduled, running as incremental, differential, or full backups as required [10]

- **Google drive**: A new backup tool that uses Google Drive to store your files



Easy and secure access to all of your content

Store, share, and collaborate on files and folders from any mobile device, tablet, or computer

Google Drive isn't a traditional backup tool by any means, it is cloud-based and just what you can back up will depend on how much online Google storage you have available.
You're given a limited amount of space for free, and there are various ways to boost it without having to part with any money, but in reality, Google Drive is going to be useful for backing up individual directories – not your whole system.

For backing up key files and folders, however, it's superb. You can easily specify any number of folders for the software to monitor, and any changes, additions, or deletions are implemented near-instantaneously.

As the name suggests, the software can be used to synchronize files between computers, and they are accessible on any device via the Google Drive web app. An excellent, if slightly limited, backup tool. [10]

You may be thinking, why not come up with a way to delete ransomware instead of being defensive. But I can assure you that deleting ransomware is not a simple matter because in ransomware there is a strong encryption algorithm that rarely makes a mistake by cybercriminals. So decoding is extremely time-consuming. So, try to "*prevention is better than cure*". However, in my personal opinion, there should be a system to identify the malicious code of each website, email… everything that we visit to give warnings, and determine where the ransomware exists.

III.CONCLUSIONS

In conclusion, by going into the length of history can confirm the outstanding development of ransomware and can determine how ransomware has traded so far. It could be a wake-up call for us to better understand ransomware.

Next, I showed how ransomware attacks your computer from which to introduce 2 main types of ransomwares: lock ransomware and crypto ransomware. The way that crypto ransomware uses entropy to encrypt and filter your files to find important files, more dangerous ransomware, new variants of ransomware that have appeared in recent years. its danger. Then we took the step to confirm one issue: "is it good or wrong to pay the ransom".

With that ransom payment, I clarified 3 main questions and came up with my best friend's argument on this issue that the ransom should not be sent.

In order not to lose the ransom, I have come up with 2 main types of solutions when ransomware hits: defend or wipe it or let it destroy my files to get it back. And from there, make my own arguments about defense methods and come up with a plan that I think will be more reasonable: remove ransomware hosting addresses.

IV.REFERENCES

[1] -list of countries by number of Internet users.https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users

[2] ‘ransomware’. https://en.wikipedia.org/wiki/Ransomware

[3]”ransomware” www.sciencedirect.com/topics/computer-science/ransomware .Ira Winkler, Araceli Treu Gomes, in Advanced Persistent Security, 2017

[4]” introduction of ransomware” https://www.oreilly.com/library/view/ransomware/9781491967874/ch01.html . oreilly-Ransomware by Allan Liska, Timothy Gallo

[5] “Ransomware Statistics”https://www.crowdstrike.com/cybersecurity-101/ransomware/ (Kurt Baker - December 29, 2021)

[7]” history” https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/ Kurt Baker - June 21, 2021

[6] “Ransomware: Recent advances, analysis, challenges and future research directions” – CraigBeaman AshleyBarkworth ToluwalopeDavidAkande SaqibHakak MuhammadKhurramKhanLallieetal. 24 September 2021.

[8]”security response -evolution of ransomware” Kevin Savage, Peter Coogan, Hon Lau Version 1.0 – August 6, 2015

[9] The Best Anti-Ransomware Software Of 2022

[10] *https://www.techradar.com/best/best-free-backup-software*

[11] https://quantrimang.com/ly-thuyet-ransomware-la-gi-118309#mcetoc_1cugtarkm8

[12]” Ransomware: Evolution, Mitigation and Prevention” Ronny Richardson, Max M. North 1-1-2017

[13]” The 5Ws and 1H of Ransomware” Microsoft Defender Security Research Team May 18, 2016