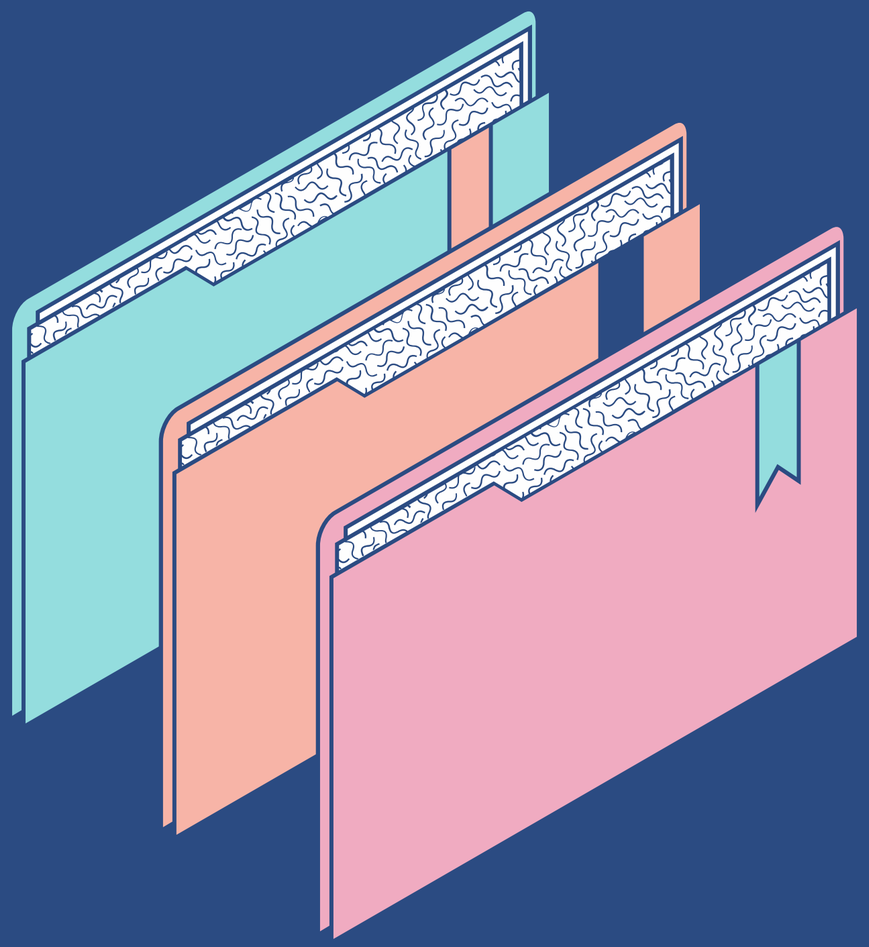
A QUICK INFORMATION GUIDE

Ransomware

A look at the importance of technology in sercurity



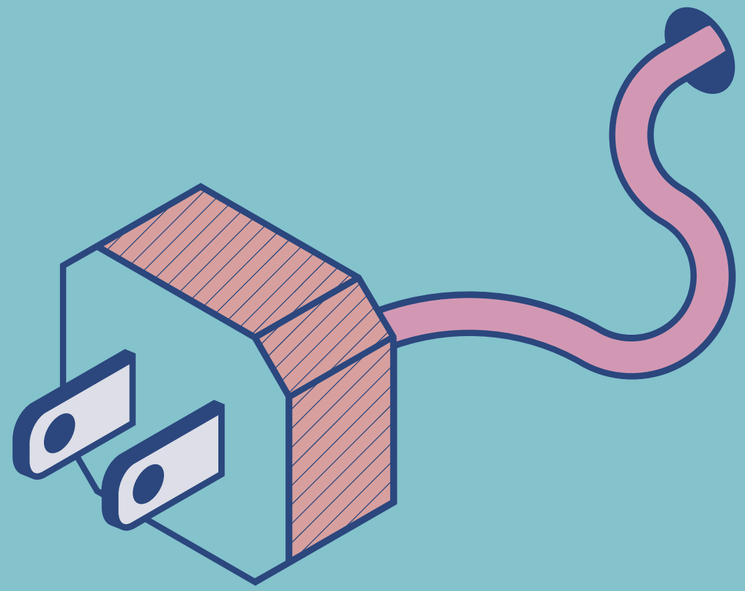
Agenda

KEY TOPICS DISCUSSED IN THIS PRESENTATION

- What is Ransomware
- History of Ransomware
- The era of Ransomware
- The era of CrytoLocker
- How does Ransomware work
- How to prevent Ransomware

What is Ransomware

- Ransomware is spyware or ransomware, it is a common name for a type of malware.
- Malware, whose "effect" is to prevent users from accessing and using their computer system or document files (mainly detected on Windows operating systems)



Variant of Malware

Malware variants of this type often give messages to victims that they have to pay a decent amount of money to the hacker's account if they want to get back their data, personal information or simply gain access to the computer. their character.

History of Ransomware

- The first ransomware was called Trojan AIDS because of its target audience – delegates who attended the World Health Organization AIDS conference in Stockholm in 1989.

- Fortunately, the encryption used by the trojan was weak at the time, so security researchers were able to release a free decryption tool.

The era of Ransomware

1

2006

Start using RSA encryption schemes

Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip and MayArchive

2

2007

The new trend

WinLock is a new type of ransomware that starts a new trend instead of normal file encryption

3

2012

The form impersonating law enforcement agencies

When infected, the computer will be locked and display a page

4

2013

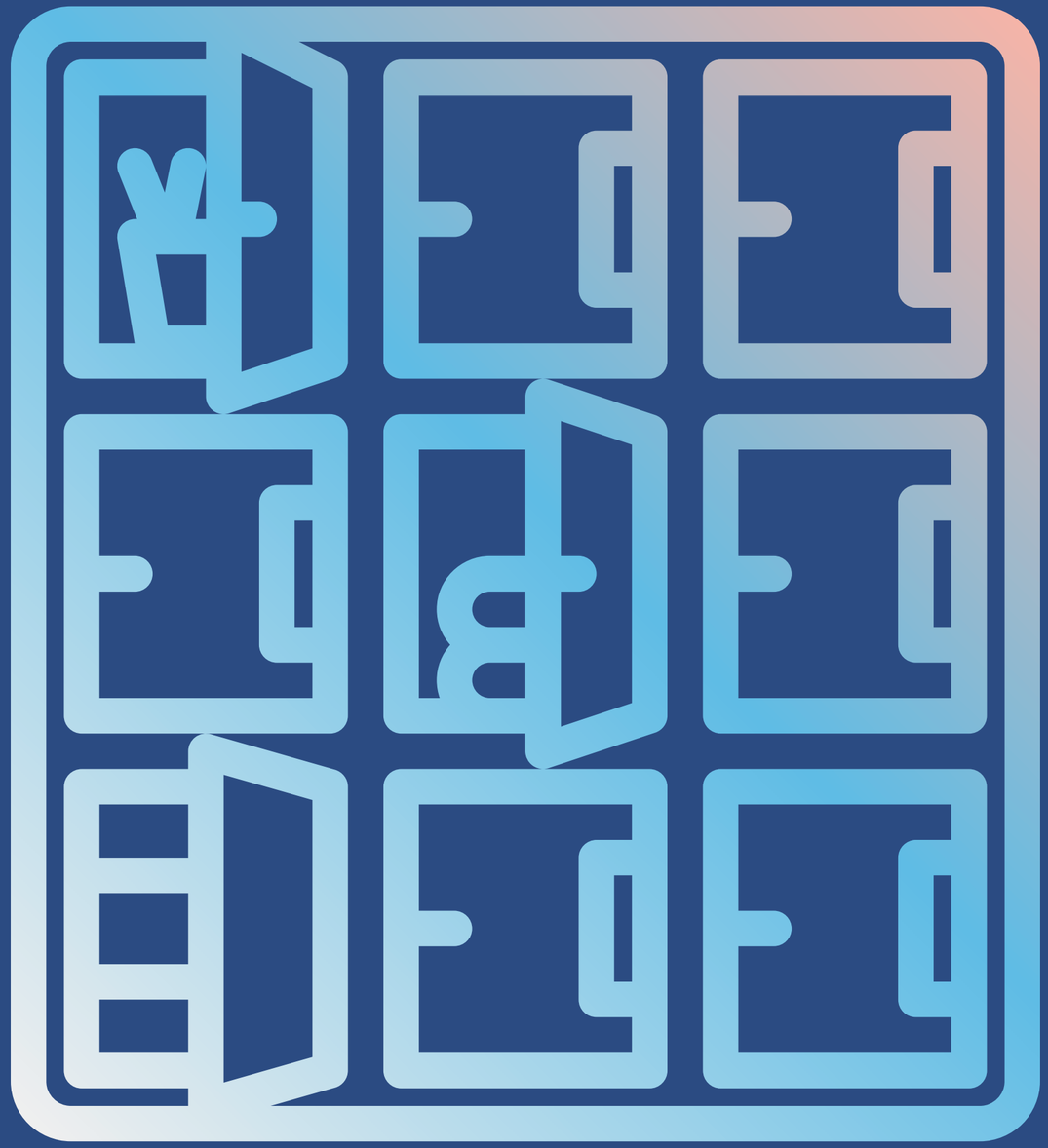
The existence of bitcoin

Choose a robust platform that can help with your objectives.

The era of CrytoLocker

AT THE END OF 2013

TrendMicro has received the first reports on a brand new type of Ransomware



2016

KeRanger

Copies malicious files to the system and runs in the background

This ransomware takes the form of a Trojan that infects an application called Transmission

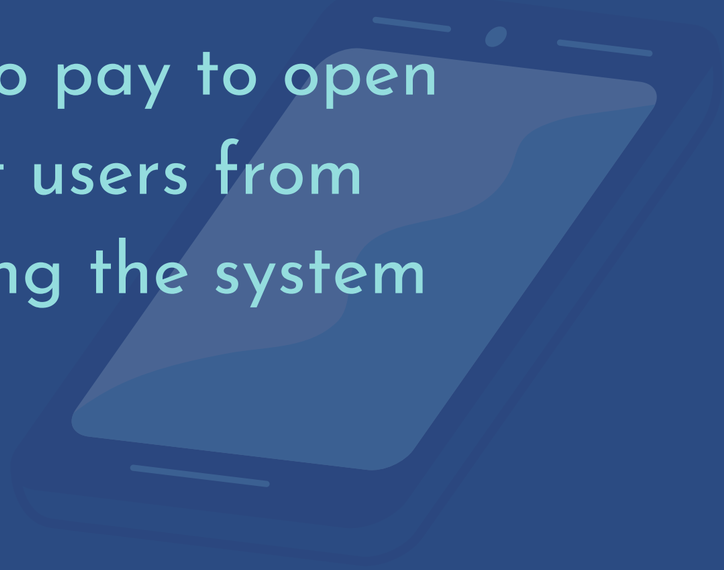
Apple Xprotect

Release updates as soon as ransomware is detected

Ransomware on mobile

2014

- Phone is locked and made to pay to open
- Prevent users from accessing the system



How does Ransomware work

ESSENTIALLY ALL RANSOMWARE PERFORMS THE FUNCTION OF DISPLAYING THREAT MESSAGES AND HAS AN INFECTION MECHANISM.

For scareware

A form of software that gives false threat warnings such as a security upgrade or malicious code in the system

PayLoad

An application designed to lock or restrict the system until payment is made

Steps by Steps

HOW RANSOMWARE FUNCTION

Step 1

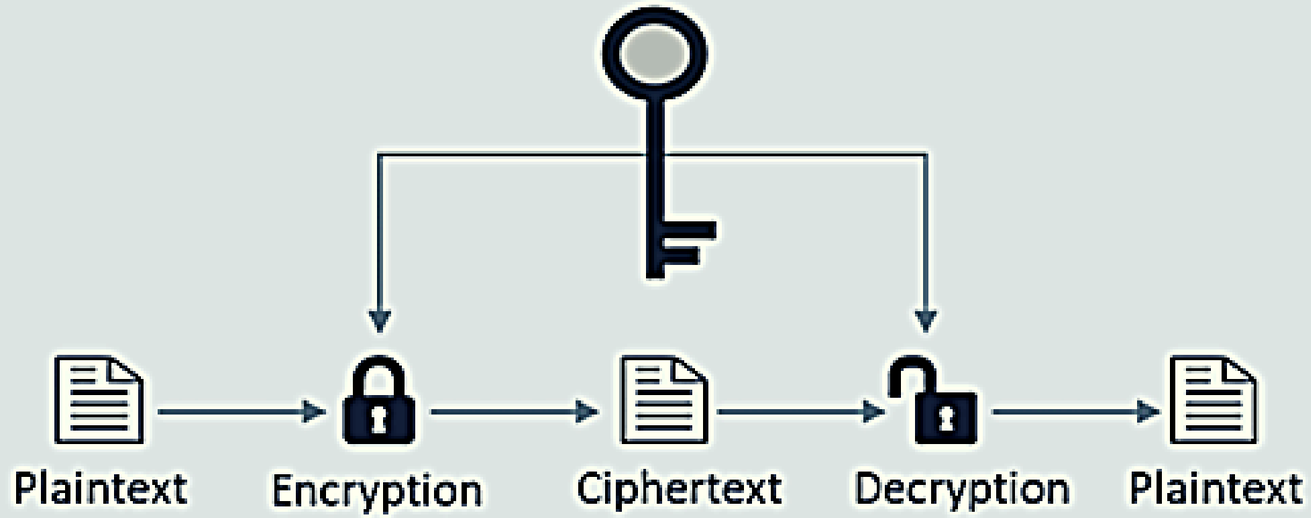
[Attacker → Victim] The attacker generates a key pair and places the corresponding public key in the malware and distributes it to the victim.

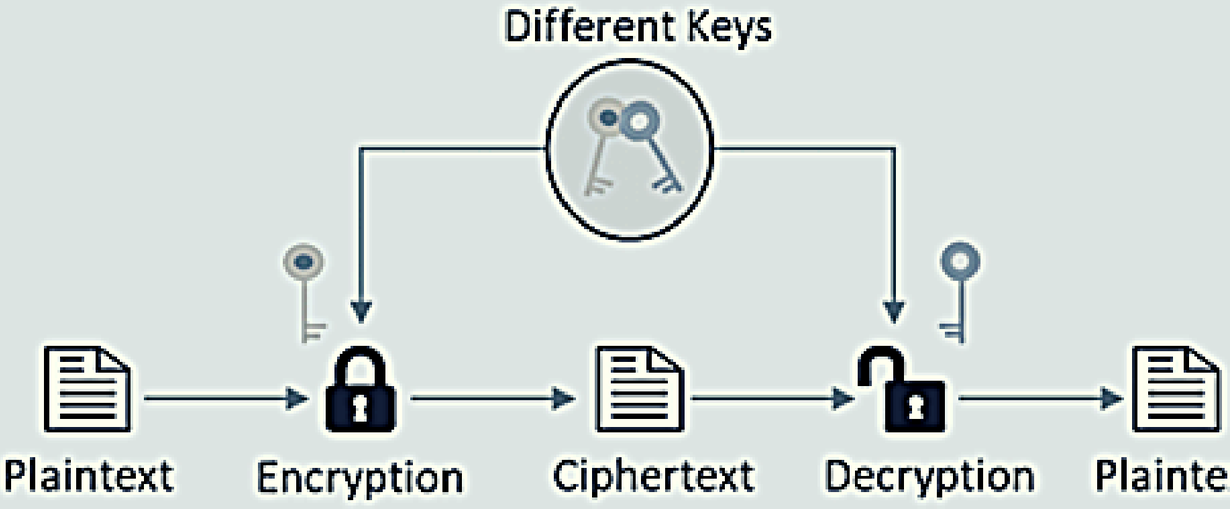
Step 2

[Victim → Attacker] To perform a cryptographic extortion attack, the malware generates a random symmetric key and encrypts the victim's data with this key.

Step 3

[Attacker → Victim] The attacker receives the payment, decrypts the asymmetric cryptography with the attacker's private key, and sends the symmetric key to the victim. The victim decrypts the encrypted data with the required symmetric key.

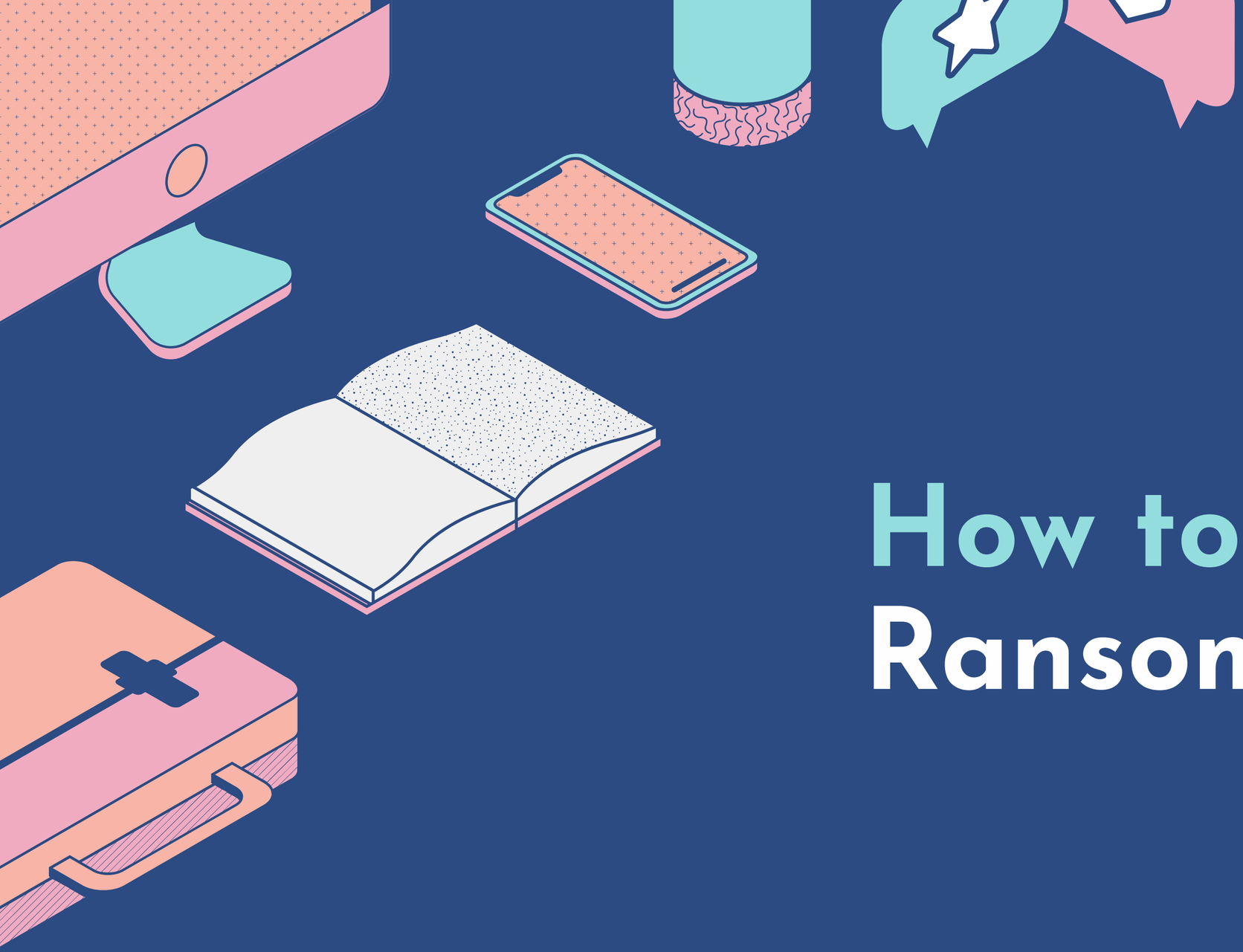




Final Target

IT'S IMPORTANT TO KNOW THE FINAL TARGET

The final purpose of Ransomware is forcing the victim to pay to remove it and decrypt the data



How to prevent Ransomware

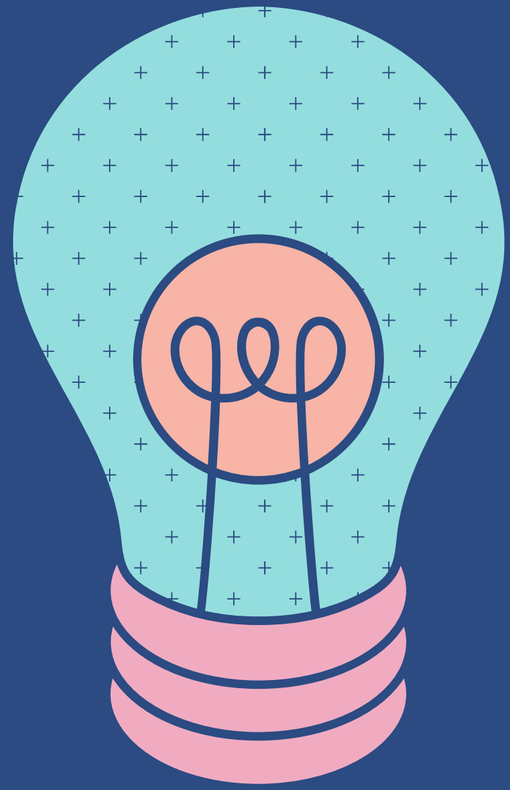
INDIVIDUAL SYSTEMS

PERSONAL USER

ENTERPRISE

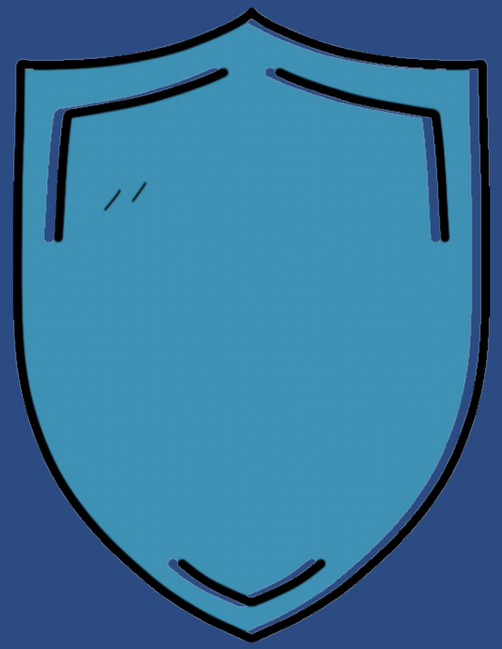
What to do when infected with ransomware?

- NEVER PAY THE RANSOM
- FREE DECODER
- USE SECURITY PRODUCTS



How to prevent ransomware?

- UPDATE OS FREQUENTLY
- NOT INSTALL SOFTWARE
- INSTALL ANTIVIRUS
- BACKUP FILES REGULARLY AND AUTOMATICALLY



SECURITY SCRIPT TO EVADE THE RANSOMWARE

Creat a data backup by use

Creat an anti-virus program to scan and reject the malicious softwares

- GUI (Graphical User Interface - Based) Antivirus
- Hash Scanning
- Real-Time Protection
- Temp Files (Junk File) Remover
- Ram - Booster
- Custom Scanning
- Real - Time Protection ON/OFF Gui - Based Switch

Sources:

https://tek4.vn/ransomware-la-gi-tai-sao-bitcoin-lai-lam-bung-no-cho-su-phat-trien-cua-ransomware

https://www.shift4.com/pdf/Ransomware-USSS-ECTF.pdf

https://giaiphapso.com/lich-su-ransomware-con-duong-phan-mem-doc-hai-xam-chiem-the-gioi/

https://vnpro.vn/thu-vien/ma-doc-ransomware-va-nhung-dieu-can-biet-3590.html

https://quantrimang.com/cong-nghe/ly-thuyet-ransomware-la-gi-118309

https://quantrimang.com/cong-nghe/ly-thuyet-ransomware-phan-2-118311

https://www.kaspersky.com/blog/ransomware-faq/13387/
https://pastebin.com/vdHpV4b0


Q
&
A

THANK YOU