Crypto Ransomware Attack: How Does It Work, Detection and Prevention Techniques

Group Members (G-5)
Allaa Al-Khalaf – 201404600
Ghareisa Al-Kuwari – 201402464
Alaa Mousa – 201305148

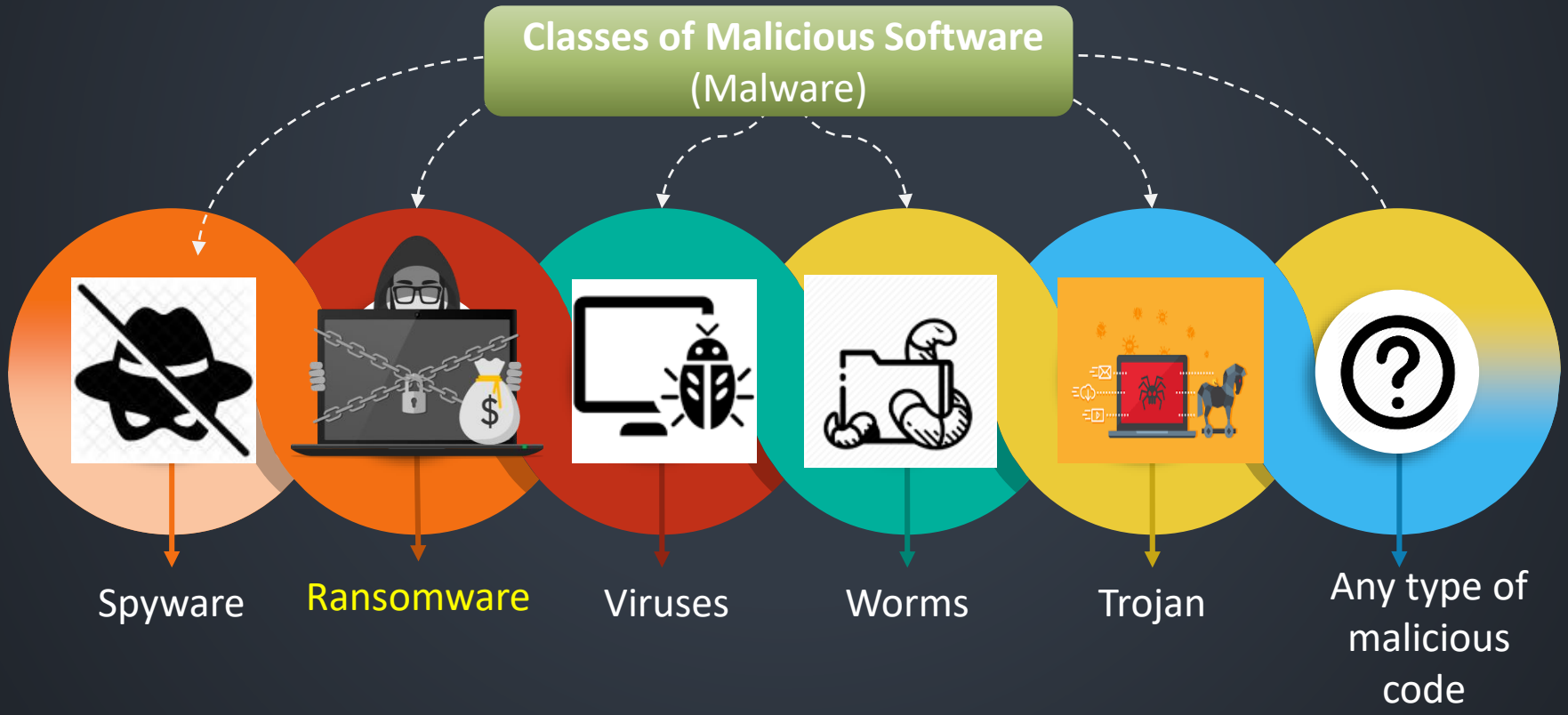
Outline

- What is a ransomware?
- How does it work?
- Detection and prevention mechanisms
- Example: WannaCry
- Demo
- Summary

What is a malware?

Malware

Malware is a malicious software that aims to access or damage a system without the permission of its user.



Malware Types

- **Virus**: piece of software that infects programs
  - replicates and goes on to infect other content
  - easily spread through network environments

- Worm: Uses a network to **self propagate** to other computers
  - Does not need a user intervention
  - Different from a virus because it does not need to attach to any program

- **Trojan Horses** need to be ran or installed onto a computer
  - They appear to be normal download until installed
  - When installed they steal or delete data

- **Spyware** **spies** on the user to see what information it can collect off the user's computer to display pop ads
  - May use memory from programs running in the background of the computer to keep close watch on the user.

  => causing the program or computer to slow down and become un-fuctional.

What is a ransomware?

Ransomware ?

Ransomware is a type of malware that encrypts files or locks computers, preventing access to them until a ransom is paid.

Types of Ransomware

1- Crypto ransomware encrypt data files on Computer, preventing access to them until a ransom is paid .

2- Locker ransomware locks the computer completely , so the user will not have access to computing resources until a ransom is paid.

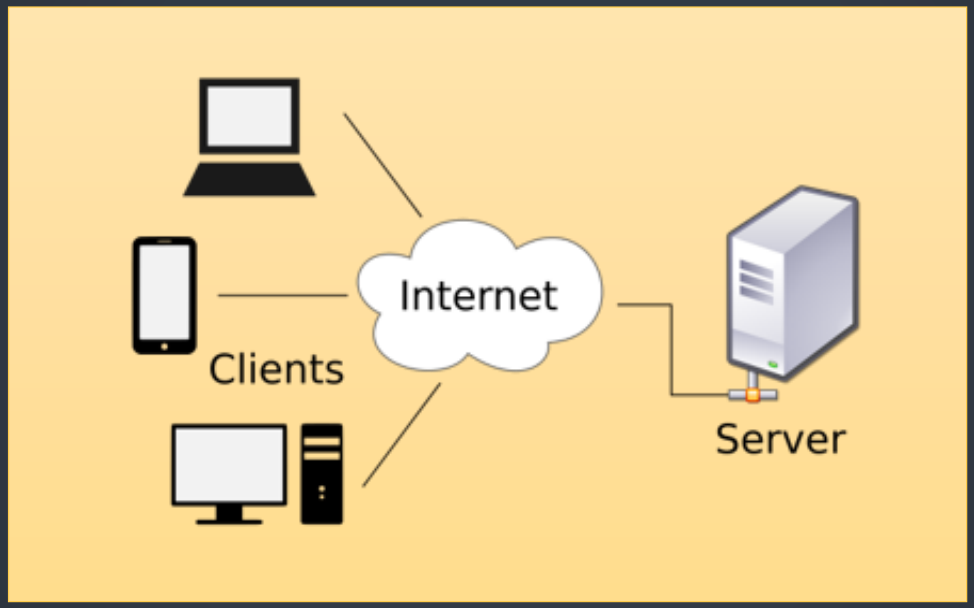
Impact

Loss of access to critical personal or business data / systems

How Does Crypto Ransomware Work

Main Components

1- Malicious software installed on the computer



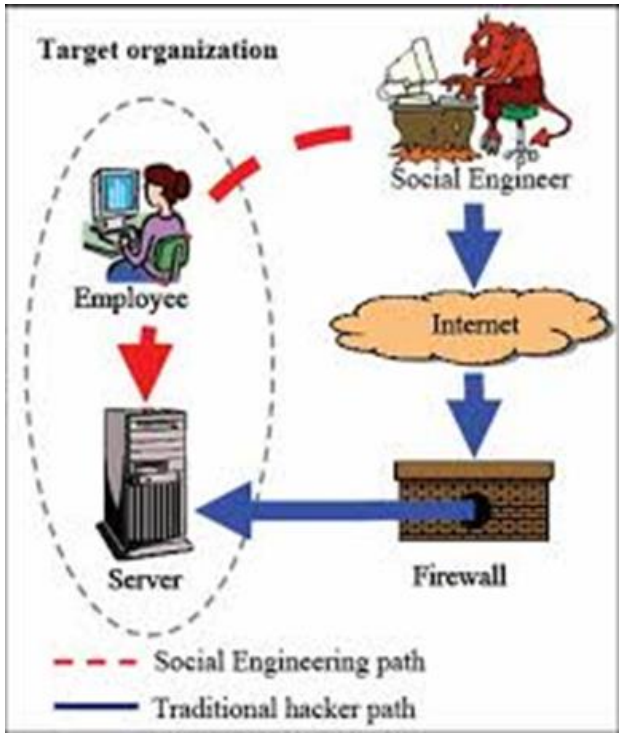
2- Hacker server communicating with the clients and giving orders in a master/slave manner

How Does It Work

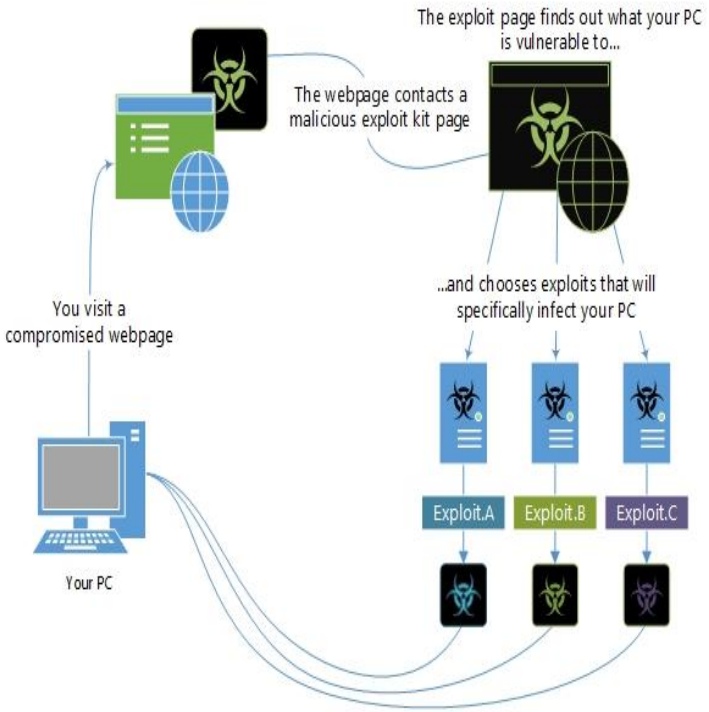
Crypto ransomware goes through 5 stages

Stage-1: Installation

Delivered as files



Delivered by exploit kits

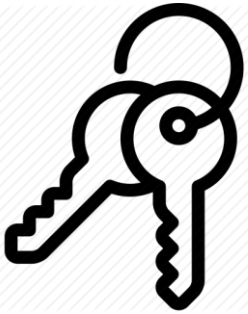


Stage-2: Contact Server & Handshake

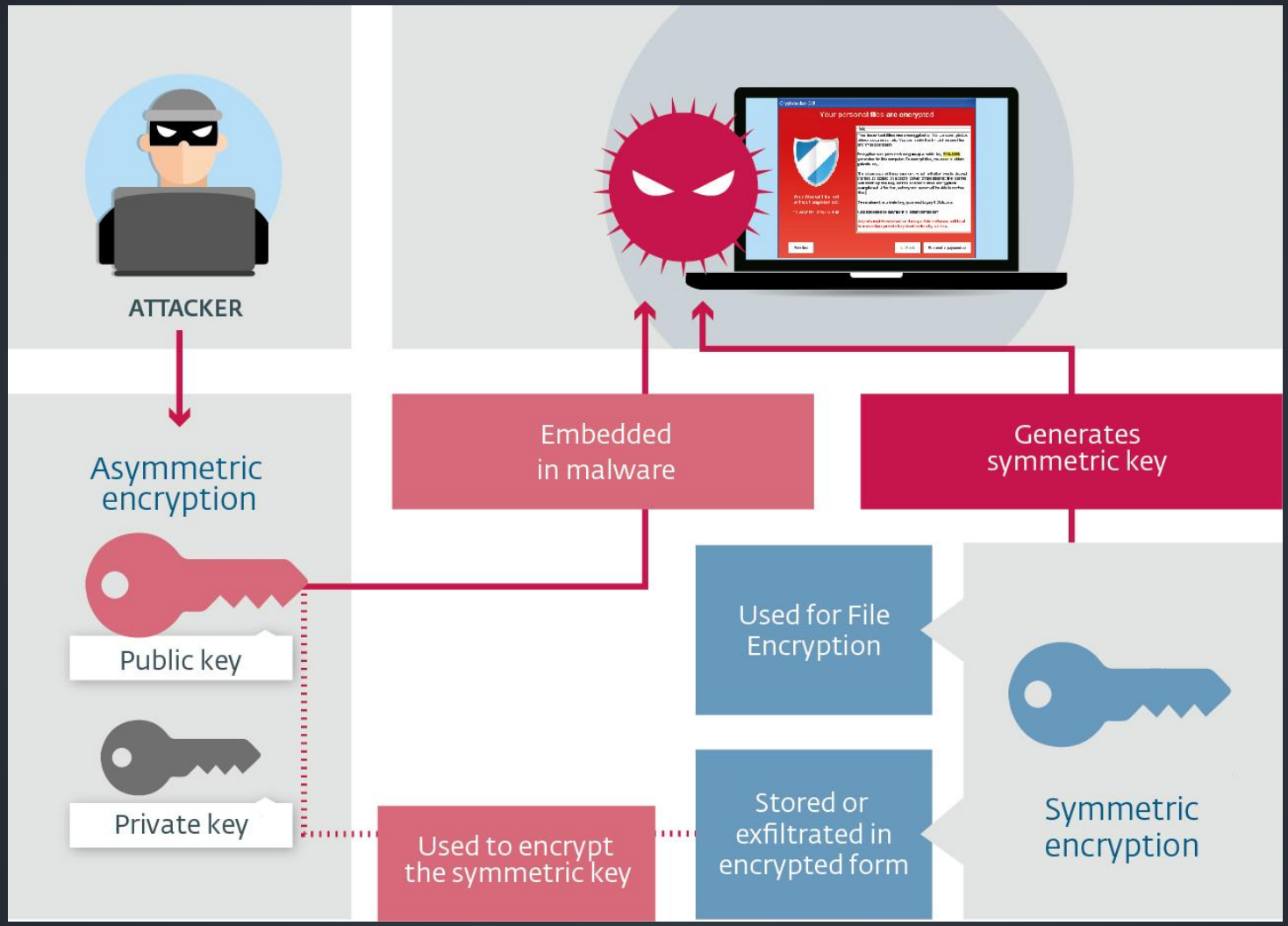
Ransomware server and client identify each other by handshake.

Stage-3: Generate Keys

The server or the client generate the keys that are going to be used for encryption step.



Stage 4: Encryption

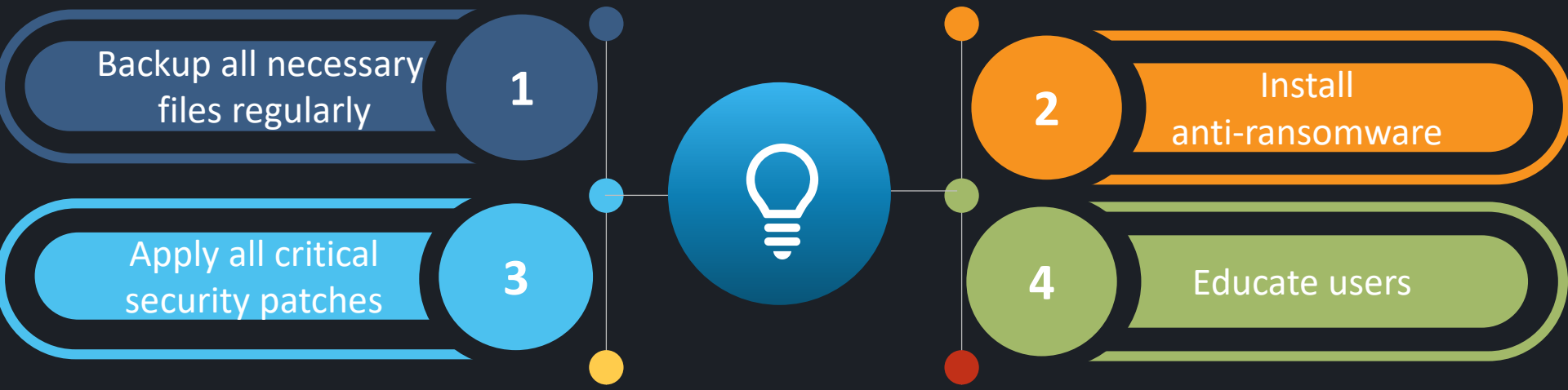


After paying the ransom the **symmetric key gets decrypted by the attacker's private key**. Then it is used to decrypt the files.

Stage-5: Extortion

Finally, a screen is displayed to the users informing them about time limit to pay up before destroying the decryption key by the criminals.

Staying Safe



Example: WannaCry

Self-propagating worm module

Ransom module deals with asking and making sure ransom is paid

Spreading Method: Worm module scans for open TCP port 445 on IP addresses in same network, or a random IP address. Then, exploits 2 vulnerabilities to spread.

Encryption: Every file encrypted using different AES key, which is itself encrypted using 2048-bit RSA.

Weaknesses: Kill Switch feature, and Bitcoin payment implementation.

Summary

- There are two types of ransomware:
  - Crypto ransomware => locks files
  - Locker ransomware => locks computer
- Crypto ransomware goes through 5 steps: installation, contact server, establish keys, encryption and extortion
- Crypto ransomware has a negative impact if the encrypted files contain critical data
- One can stay safe by installing some anti ransomware, having a backup for all important files and applying all the critical security patches
- WannaCry is a famous crypto ransomware but has weaknesses