CE1.4 Assignment

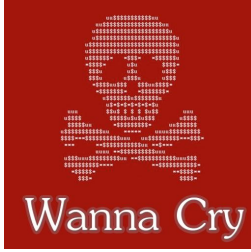
2017 - WannaCry ransomware attack

LIM WEI YANG

MINGZI YANG

LIM WEI JIE

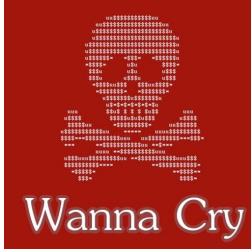
What happen?



Synopsis

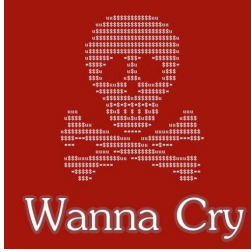
- What is WannaCry? WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017.
- After infecting a Windows computer, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.

What is the effect?



- Ransomware cryptoworm is created to target on computers running Microsoft OS
- Data and files were encrypted and hackers demanded for Bitcoin
- This ransomware is a network worm where it includes a transport code to spread itself onto any connected PCs on a network running Windows OS
- They have used the tool Eternal Blue to exploit and gain access and using a back end application DoublePulsar which grants hacker access to the PCs and load malware onto the system.

The Solution (How they solve the problem?)

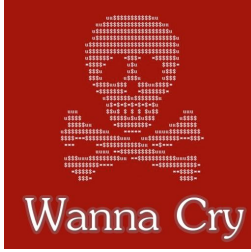


- The WannaCry ransomware attack was **not "solved"** as it was mitigated and its impact was reduced.
- The attack was one of the largest and most widespread ransomware incidents in history, affecting over 150 countries and targeting computers running Microsoft Windows operating systems.

Kill Switch Discovery

- A security researcher named Marcus Hutchins, also known as "MalwareTech," accidentally discovered a "kill switch" in the malware's code.
- He noticed that the ransomware was trying to contact a specific domain, and when that domain was registered, it acted as a "sinkhole," effectively halting the spread of WannaCry.
- This discovery greatly slowed down the infection rate.

How to prevent?



- Keep software and systems updated with the latest security patches
- Utilise firewalls and intrusion detection/prevention systems to detect suspicious activities and alert administrators of potential threats
- Backup data regularly and stored securely
    - data recovery in case of ransomware attack
- Install reliable and up-to-date antivirus and anti-malware software
- Educate users on phishing awareness