**NAME : Alexander Miguel D. Pallasigue T289 BSIT-1B**

**What is the event about? What type of cybercrime was identified? How did this differ to other case?**

The WannaCry ransomware attack was a large-scale cyberattack that occurred in May 2017. It targeted computers running Microsoft Windows operating systems by encrypting data and demanding a ransom payment in Bitcoin to unlock it.

This attack was classified as a ransomware attack, a type of malicious software that encrypts a user's files and demands a ransom for their release.

What set WannaCry apart was its rapid spread and the scale of its impact. It leveraged a known vulnerability in Windows, exploiting a flaw in the SMB (Server Message Block) protocol. This allowed it to propagate through networks, infecting over 200,000 computers across 150 countries in a matter of days.

**When did the attack happen? Where the attack was first discovered, and how far did it spread? When it was finally contained? Is the threat ongoing?**

The attack began on May 12, 2017, and it was first discovered in England's National Health Service (NHS). It quickly spread worldwide, affecting various industries and organizations.

The spread of WannaCry was eventually slowed down by a security researcher who accidentally found a "kill switch" in the malware's code. This allowed for a temporary halt in its propagation. However, it remains a potential threat as new variants or similar attacks could emerge in the future.

The attack is believed to have originated from a North Korean hacking group known as Lazarus, which has been associated with state-sponsored cyber warfare activities. They utilized the EternalBlue exploit, which was a hacking tool developed by the U.S. National Security Agency (NSA) that was leaked and subsequently used by cybercriminals.

**What type of attacker(s) was/were involved? How did they perform the attack? Were the perpetrators caught?**

The WannaCry ransomware attack was carried out by a type of attacker known as a cybercriminal. They used a malicious software called WannaCry to infect computers and encrypt their files, demanding a ransom in exchange for decryption. The attack spread through a vulnerability in the Windows operating system, targeting organizations worldwide.

As for whether the perpetrators were caught, some individuals believed to be associated with the attack were identified, but it is unclear if all of them were apprehended. Cybercriminals often operate from different locations and use various techniques to hide their identities, making it challenging to track and apprehend all of them.

**Who, or what entities were affected by the attack? How much damage did it cause?**

Individuals: Many individuals had their personal files encrypted and were faced with ransom demands to regain access to their data.

Businesses and Organizations: Numerous organizations, including hospitals, government agencies, and companies, were affected. The attack disrupted operations, compromised data, and caused financial losses.

Government Agencies: Some government institutions, such as the UK's National Health Service (NHS), were hit hard by WannaCry, leading to canceled appointments and delayed patient care.

The total damage caused by WannaCry is difficult to quantify precisely, but it is estimated to have resulted in billions of dollars in losses worldwide due to ransom payments, recovery costs, and lost productivity. It served as a wake-up call for the need to improve cybersecurity practices and update outdated software to prevent such attacks.

**How did the necessary authorities react to the attack? What countermeasures were used stop/preventthe attack?**

1. \*Law Enforcement Agencies\*: Law enforcement agencies around the world, including the FBI and Europol, launched investigations into the attack to identify and apprehend the individuals or groups responsible for WannaCry.

2. \*Software Patches\*: Microsoft released an emergency security patch for unsupported versions of Windows, including Windows XP and Windows Server 2003, to address the vulnerability exploited by WannaCry. This patch closed the loophole that the ransomware used to spread.

3. \*Network Segmentation\*: Organizations implemented network segmentation to isolate infected systems and prevent the spread of the ransomware within their networks.

4. \*Backup and Recovery\*: Many affected organizations relied on backup and recovery systems to restore their data without paying the ransom. This highlighted the importance of regular data backups.

5. \*Public Awareness\*: Authorities and cybersecurity experts increased public awareness about the importance of regularly updating software, using strong passwords, and being cautious about suspicious emails and attachments.

6. \*Coordination\*: International cooperation and information sharing among cybersecurity organizations and governments were enhanced to track and combat the ransomware's spread.

7. \*Ransom Payment Advisories\*: Law enforcement agencies discouraged victims from paying the ransom, as paying did not guarantee the recovery of data and only encouraged cybercriminals.

While these measures helped mitigate the immediate impact of WannaCry, the incident also served as a catalyst for organizations to reevaluate their cybersecurity strategies and invest in better defenses against ransomware and other cyber threats. It highlighted the need for proactive measures such as regular software updates, employee training, and robust cybersecurity practices.

**In your opinion, what could be done to improve the situation and prevent similar attacks from happening in the future?**

To prevent similar attacks like WannaCry in the future, we need to focus on regular software updates, cybersecurity education, network isolation, robust backup practices, stronger security measures, vulnerability assessments, and international cooperation. These actions, along with legislation and advanced threat detection technologies, collectively strengthen our defenses against ransomware and cyber threats, reducing the likelihood of future attacks.