# Case Study: WannaCry Ransomware Cyber Attack

The WannaCry ransomware cyber attack was a significant global incident that occurred in May 2017. It was a form of malicious software (malware) that targeted computers running the Microsoft Windows operating system. The attack affected hundreds of thousands of computers in over 150 countries, causing widespread disruption and financial losses.

Here are some key details about the WannaCry ransomware cyber attack:

**1. Spread and Infection:** WannaCry spread rapidly through a worm-like mechanism, exploiting a vulnerability in the Windows operating system called EternalBlue. This vulnerability was originally discovered by the National Security Agency (NSA) but was later leaked by a group called "Shadow Brokers." WannaCry took advantage of this vulnerability to infect computers connected to the internet without adequate security patches.

**2. Encryption and Ransom:** Once a computer was infected, WannaCry encrypted files on the system, making them inaccessible to the user. The ransomware then displayed a message demanding a ransom payment in Bitcoin in exchange for a decryption key. The amount initially requested was around $300 worth of Bitcoin.

**3. Global Impact:** The WannaCry attack had a significant impact on various sectors worldwide, including healthcare, telecommunications, logistics, and government organizations. It notably affected the UK's National Health Service (NHS), causing disruptions in patient care and postponement of non-emergency medical procedures.

**4. Kill Switch and Mitigation:** A cybersecurity researcher accidentally discovered a "kill switch" domain embedded within the WannaCry code. When the malware attempted to connect to this domain and failed, it would stop spreading. By registering the domain, the researcher unintentionally slowed down the attack. However, this did not fully stop the ransomware's impact on already infected systems.

**5. Attribution and North Korean Connection:** The United States and the United Kingdom attributed the WannaCry attack to the North Korean government. The attribution was based on various technical indicators and similarities with previous cyber attacks linked to North Korea. The attack was believed to have been carried out by a group known as Lazarus Group.

**6. Lessons and Security Measures:** The WannaCry attack highlighted the importance of regular software updates and security patches to protect against known vulnerabilities. It also emphasized the need for robust backup systems, network segmentation, and strong cybersecurity practices to mitigate the risks of ransomware attacks.

Since the WannaCry attack, there have been efforts to improve cybersecurity measures, collaboration between governments and private organizations, and increased awareness of the potential threats posed by ransomware and other cyber attacks.

**The WannaCry ransomware cyber attack can be examined under the OSI (Open Systems Interconnection) model to understand the various layers of the attack and how they were affected. The OSI model is a conceptual framework that describes the different functions of a network communication system, divided into seven layers. Let's examine the WannaCry attack in the context of the OSI model:**

**1. Physical Layer:**

The Physical layer deals with the actual transmission of data over the network medium. The WannaCry attack did not directly impact the Physical layer as it targeted vulnerabilities in higher layers of the OSI model. However, the attack spread over networks, which relied on the Physical layer for transmission.

**2. Data Link Layer:**

The Data Link layer is responsible for data framing and error detection at the link level. The WannaCry attack did not specifically target this layer, but it utilized various methods to propagate across networks, including exploiting vulnerabilities in the SMB (Server Message Block) protocol, which operates at this layer.

**3. Network Layer:**

The Network layer handles logical addressing, routing, and the fragmentation and reassembly of packets. The WannaCry attack exploited vulnerabilities in the Windows operating system's implementation of the SMB protocol (such as EternalBlue) to spread rapidly across networks. By exploiting this flaw, the malware bypassed network security measures and allowed lateral movement.

**4. Transport Layer:**

The Transport layer ensures reliable data transmission by establishing end-to-end connections, segmenting data, and providing error recovery. The WannaCry attack did not specifically target the Transport layer, but it utilized network connections established at this layer to propagate and communicate with command and control servers.

**5. Session Layer:**

The Session layer establishes, manages, and terminates connections between applications. The WannaCry attack did not directly impact the Session layer, but it used established network connections to communicate with its command and control infrastructure, initiating the encryption process and issuing ransom demands.

**6. Presentation Layer:**

The Presentation layer deals with data formatting, encryption, and compression. The WannaCry attack did not focus on this layer as its primary objective was to encrypt files on infected systems and demand ransom. However, the encryption of files by the malware

can be considered a form of data encryption at the Presentation layer.

**7. Application Layer:**

The Application layer represents the layer at which users interact with the network through applications and services. The WannaCry attack primarily targeted the Application layer by exploiting vulnerabilities in the Windows operating system, particularly the SMB protocol used for file and printer sharing. It encrypted files on infected systems, making them inaccessible until a ransom was paid.

In summary, the WannaCry ransomware attack predominantly targeted vulnerabilities at the Network and Application layers of the OSI model. Exploiting weaknesses in the Windows SMB protocol and other vulnerabilities, the attack rapidly spread across networks, encrypting files at the Presentation layer and demanding ransom from affected users.