**Name** : Vaibhav Soni

**Enrolment No.** : IU2141230287

**Branch** : CSE – A

**Sem** : 7

**Subject** : Cyber Security

**Lab – 8**

**Aim :** Case Study on Computer Virus Impact.

* **Introduction**
* In May 2017, a large-scale cyberattack known as the WannaCry ransomware attack hit organizations around the world. This attack targeted organizations worldwide by exploiting vulnerabilities in older versions of Microsoft Windows operating systems. WannaCry is classified as ransomware because it encrypts files on infected computers, locking out users and demanding a ransom payment in Bitcoin for file decryption. If the ransom is not paid, the files remain inaccessible, crippling the infected systems.
* One of the hardest-hit organizations during the WannaCry attack was the National Health Service (NHS) in the United Kingdom. The NHS is the public healthcare provider, and its computer systems are crucial for managing patient records, medical equipment, and hospital operations. The cyberattack caused major disruptions in the NHS, resulting in the cancellation of surgeries, delayed treatments, and widespread operational chaos.



* The WannaCry attack revealed the vulnerabilities in the cybersecurity systems of large organizations like the NHS, many of which were running outdated or unpatched software. The incident highlighted the growing threat of cyberattacks and emphasized the need for stronger cybersecurity measures to protect essential services. The WannaCry attack was a turning point for many organizations, pushing them to rethink their cybersecurity strategies to prevent similar events in the future.
* This case study will explore the operation of the WannaCry virus, its impact on the NHS, the mitigation efforts undertaken by the organization, and the key lessons learned. It aims to provide insights into the consequences of ransomware attacks and the steps organizations can take to strengthen their cybersecurity defenses.
* **Virus Operation**
* The WannaCry ransomware is a type of malware that primarily targets computers running older or unpatched versions of Microsoft Windows. It spreads by exploiting a vulnerability in the Windows operating system known as EternalBlue, which was initially discovered by the United States National Security Agency (NSA). This vulnerability allowed hackers to remotely execute code on a computer without user interaction. EternalBlue was leaked to the public by a hacking group called the Shadow Brokers in April 2017, just a month before the WannaCry attack began.
* Once WannaCry infects a system, it quickly begins encrypting the files on the computer using a strong encryption algorithm, effectively locking the user out of their own data. The ransomware then displays a message demanding a ransom payment of $300 to $600 in Bitcoin in exchange for decrypting the files. The message warns that if the payment is not made within a specified time (usually a few days), the ransom will double, and eventually, the encrypted files will be permanently locked, rendering them inaccessible.
* What makes WannaCry particularly dangerous is its self-propagating capability. After it infects one computer, the ransomware scans the local network for other vulnerable computers and spreads to them automatically without requiring any human action. This is done by exploiting the same EternalBlue vulnerability across multiple systems, which makes it incredibly effective at spreading quickly within large organizations, such as hospitals and businesses, where many computers are interconnected. This rapid spread across networks allowed WannaCry to infect hundreds of thousands of computers in over 150 countries within a matter of hours.
* The virus also included a DoublePulsar backdoor, another tool leaked by the Shadow Brokers, which helps install the ransomware on vulnerable machines. This backdoor allows the malware to install itself on the system even more efficiently, making the infection process faster and more widespread.
* One unusual feature of WannaCry was the inclusion of a kill switch, an unintentional feature coded into the malware by its creators. This kill switch was a hardcoded web domain that the virus attempted to connect to before beginning its encryption process. A cybersecurity researcher accidentally discovered this kill switch while investigating the attack. By registering the domain, the researcher was able to significantly slow the spread of the virus, effectively stopping it from infecting new systems in many regions. However, this did not undo the damage already caused by the virus, as many systems had already been encrypted by the time the kill switch was activated.
* Overall, WannaCry’s operation relied on the combination of exploiting an unpatched security vulnerability, using a self-spreading mechanism to infect other computers, and encrypting files to demand ransom payments. Its rapid spread and the widespread use of outdated software made it one of the most disruptive cyberattacks in recent history. Although the discovery of the kill switch slowed the virus, the damage had already been done, and it highlighted the importance of keeping software up-to-date and having effective cybersecurity defenses in place.
* **Impact on the Organization**
* The WannaCry ransomware attack had a severe and widespread impact on the National Health Service (NHS) in the United Kingdom, which was one of the most high-profile victims of the attack. The NHS is a large and complex healthcare system that relies heavily on its digital infrastructure for patient care, medical records, scheduling, and the operation of medical equipment. When WannaCry hit the NHS, it caused immediate and widespread disruption to its services.
* One of the most significant impacts was the loss of access to patient data. The ransomware encrypted critical files on infected computers, including patient records, medical histories, and appointment schedules. Many hospitals and clinics across the UK were forced to cancel appointments and surgeries as doctors and nurses could not access important information. More than 19,000 appointments were cancelled, including surgeries, cancer treatments, and outpatient consultations. Some hospitals had to shut down entire departments, and patients were redirected to other facilities, causing delays in treatment that potentially endangered patient safety.
* In addition to disrupting patient care, the ransomware also affected the NHS’s medical equipment. Many devices, such as MRI scanners, blood test machines, and diagnostic tools, are connected to hospital networks and rely on software to function. These devices were rendered unusable by the ransomware, further complicating the NHS’s ability to provide medical services. Without access to these tools, hospitals struggled to diagnose and treat patients effectively, resulting in longer wait times and a backlog of critical medical procedures.
* The financial impact of the WannaCry attack on the NHS was substantial. The direct costs of the attack, including system recovery, canceled appointments, and overtime for IT staff, were estimated to be around £92 million. This figure includes the costs of restoring affected systems, recovering data, and addressing the disruption to patient care. In the long term, the NHS also faced additional costs related to upgrading outdated software and improving its cybersecurity infrastructure. Many of the NHS’s computers were running old versions of the Windows operating system, which had not been updated with the latest security patches, leaving them vulnerable to the EternalBlue exploit used by WannaCry.
* Beyond the financial losses and operational disruptions, the WannaCry attack also had a significant impact on the public’s trust in the NHS’s ability to protect sensitive medical data. While no patient data was stolen or compromised during the attack, the inability to access records raised concerns about the NHS’s preparedness for future cyber threats. Patients and healthcare professionals were left uncertain about the security of the systems they rely on every day. This incident highlighted the critical importance of cybersecurity in the healthcare sector, where the consequences of a cyberattack can directly affect people’s lives.
* The attack also had a ripple effect on the NHS’s employees. Doctors, nurses, and administrative staff had to deal with the consequences of the attack, from rescheduling appointments to manually processing information that would normally be handled digitally. This increased the workload and stress on an already overburdened workforce. The lack of access to digital tools also forced many staff members to revert to paper-based systems, slowing down operations and leading to inefficiencies.
* Overall, the WannaCry attack exposed significant weaknesses in the NHS’s IT infrastructure. The widespread use of outdated software and the lack of timely security updates left the organization vulnerable to a well-known exploit. The disruption caused by the attack not only affected patient care and medical services but also led to significant financial losses and a loss of confidence in the NHS’s ability to defend against future cyberattacks. It became clear that cybersecurity needed to be a higher priority for the NHS and similar large organizations, particularly those handling sensitive and critical data.
* **Mitigation and Response**
* In the immediate aftermath of the WannaCry attack, the National Health Service (NHS) took urgent steps to mitigate the damage and restore its systems. The first critical action was to disconnect infected computers from the network to prevent the ransomware from spreading further. Since WannaCry could propagate across networks by exploiting the EternalBlue vulnerability, isolating affected systems was essential to containing the infection. Although this measure slowed the virus, it also meant that many essential systems were shut down, affecting hospital operations.
* The NHS then collaborated with external cybersecurity experts, including the UK’s National Cyber Security Centre (NCSC), Microsoft, and private cybersecurity firms, to address the root cause of the attack. One of the primary tasks was to apply security patches released by Microsoft in March 2017, which fixed the EternalBlue vulnerability. Unfortunately, many NHS systems had not been updated before the attack, leaving them exposed. NHS IT teams worked around the clock to deploy these patches across affected systems, ensuring that no further infections occurred. However, applying these patches and bringing systems back online took time, prolonging the disruption to healthcare services.
* Data restoration was another critical aspect of the NHS’s response. WannaCry encrypted files, making them inaccessible, but the NHS had backup systems in place for patient records and other critical data. These backups were used to restore the encrypted files on many systems. However, this process was slow, as it required significant manual effort to ensure that all data was properly restored and systems were functioning correctly. In some cases, data restoration was prioritized for the most critical departments, such as emergency care, to minimize the impact on patient services.
* In the aftermath of the attack, the NHS implemented several long-term security measures. These included upgrading outdated systems and investing in more modern and secure IT infrastructure. The WannaCry attack exposed the risks of relying on legacy systems, so the NHS began phasing out older versions of Windows and improving its patch management processes. Regular updates and security audits were introduced to prevent future vulnerabilities from going unpatched.
* The NHS also revised its incident response plan to improve its readiness for future cyberattacks. This included better staff training on recognizing phishing attempts and other common attack vectors, which are often the first point of entry for ransomware. Additionally, the organization strengthened its disaster recovery procedures to ensure that data could be restored more quickly in the event of another cyber incident.
* Although the NHS managed to recover from the WannaCry attack, the response was criticized for being reactive rather than proactive. Many argued that the organization could have avoided much of the damage if it had applied security patches earlier and upgraded outdated systems. Nevertheless, the lessons learned from the attack led to significant improvements in the NHS’s cybersecurity defenses, making it better equipped to handle future threats.
* **Lessons Learned and Future Implications**
* The WannaCry attack provided several important lessons for the NHS and the broader cybersecurity community. One of the most critical takeaways was the need for regular software updates and patch management. The attack exploited a known vulnerability for which Microsoft had already released a patch two months earlier. However, because many NHS systems were outdated and unpatched, they remained vulnerable. This emphasized the importance of promptly applying security updates to all systems, especially those critical to operations like healthcare.
* Another key lesson was the value of having robust backup systems. While the NHS did have backups of important data, the process of restoring encrypted files was slow and labor-intensive, which extended the disruption of services. This highlighted the need for faster, more efficient data recovery systems and practices, ensuring that in the event of future attacks, organizations can restore essential data quickly and minimize downtime.
* The attack also underscored the importance of proactive cybersecurity measures. The NHS’s reliance on outdated technology and lack of sufficient cybersecurity infrastructure made it an easy target for the WannaCry ransomware. In response, the organization learned that upgrading systems regularly and investing in modern IT infrastructure are critical to preventing such attacks. Moreover, having a comprehensive incident response plan in place could have mitigated the impact of the attack. This includes training staff to recognize threats like phishing and ransomware and preparing IT teams for rapid containment and recovery.
* Looking forward, the WannaCry attack has broader implications for the global healthcare sector and other industries dependent on secure IT systems. It serves as a stark reminder that cybersecurity is no longer optional but an essential part of protecting sensitive data and maintaining operational continuity. The attack prompted many organizations, including the NHS, to increase their investment in cybersecurity defenses, adopt regular security audits, and prioritize disaster recovery planning to ensure readiness for future threats.
* **Conclusion**
* The WannaCry ransomware attack was one of the largest cyberattacks in history, and the NHS was one of its most notable victims. The virus caused massive disruptions, exposing weaknesses in how organizations manage cybersecurity. However, by responding effectively and learning from the experience, the NHS was able to recover and take steps to improve its security in the future.
* This case study serves as an important lesson for all organizations about the real-world risks of cyber threats and the critical need for strong cybersecurity practices.
* **References**

1. National Audit Office - Investigation into WannaCry Cyber Attack and the NHS

<https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>

1. NHS England - The WannaCry ransomware attack was a worldwide cyber-attack which took place in May 2017. The cyber-attack targeted PCs running Windows.

<https://www.england.nhs.uk/long-read/case-study-wannacry-attack/>

1. Acronis – How and why it happened?

<https://www.acronis.com/en-sg/blog/posts/nhs-cyber-attack/>

1. Wikipedia – description and defensive response

<https://en.wikipedia.org/wiki/WannaCry_ransomware_attack>

1. Avast - When did the NHS attack take place?

<https://www.avast.com/business/resources/what-is-hospital-ransomware>