The WannaCry Ransomware Attack on the United Kingdom's National Health Service

Understanding the WannaCry Ransomware:

A critical component of the WannaCry ransomware was the EternalBlue exploit. Discussing this exploit's connection to the WannaCry ransomware is essential, as their relationship forms the basis for understanding how a software vulnerability in Microsoft's Windows operating system led to the rise of one of the most infamous ransomware attacks.

The existence of EternalBlue became known when a hacker group called the "Shadow Brokers" leaked multiple software exploits allegedly created by the United States National Security Agency[4]. Among these exploits, EternalBlue quickly caught the attention of adversaries because it uniquely targeted one of the most widely used operating systems, Microsoft's Windows. As described by the Center for Internet Security[3], EternalBlue took advantage of a vulnerability in Windows's Server Message Block version 1 protocol, a network file sharing system facilitating access to files on remote servers. Due to EternalBlue's network-related nature, adversaries could potentially compromise entire networks and all connected devices, leaving the devices vulnerable.

Shifting the focus back to WannaCry, let's uncover its history and pinpoint its usage of the EternalBlue exploit.

Figure 1: WannaCry ransomware note left on victims' devices. It presents a window to the user, instructing the victim to make a payment using Bitcoin, a popular cryptocurrency, in exchange for the decryption of their files.

According to reports from the United States Cybersecurity and Infrastructure Security Agency (CIS), WannaCry was discovered on May 12, 2017, by an independent security researcher[3]. The CIS explains that WannaCry arrives on an infected computer as a self-contained dropper, which installs and executes the ransomware, encrypting files on the victim's hard drive. It then leverages the EternalBlue exploit to scan for and target other vulnerable devices on the local network, attempting to spread and propagate. The ransomware subsequently displays the ransom note in a window named "Wana Decrypt0r 2.0", possibly inspiring the name "WannaCry" due to its cryptographic nature and the emotional impact felt by victims.

The United Kingdom's National Health Service Cyberattack Case Study:

The WannaCry ransomware had devastating effects on the United Kingdom's NHS. According to the United Kingdom's National Audit Office (NAO), this attack unfolded in May of 2017 [2]. The NAO reported that

- The attack led to the cancellation of thousands of appointments and operations, forcing patients to travel further to accident and emergency departments.
- NHS staff got locked out of their devices, delaying their ability to access/update patient information, send test results to general practitioners, and transfer or discharge patients.
- Radiology and pathology-related medical equipment disruptions affected patients who relied on diagnostic imaging (such as MRI scanners) and testing of blood and tissue samples.

However, given all of these disturbances, the NAO states that NHS organizations reported no cases of harm to patients or compromised data.

Figure 2: The NHS releases a statement regarding the WannaCry ransomware attack

- The parties involved:
  - Attackers:
    - Creator(s) of the WannaCry ransomware– the identity of those involved is unclear. However, the U.S. Department of Justice has charged three North Korean military hackers for their alleged involvement[6].
  - Victims:
    - The United Kingdom's NHS
    - Patients
    - Healthcare Workers
    - People connected to the NHS's network.

- The reason for attack:
  - No reports indicate that the WannaCry ransomware specifically targeted the UK's NHS. The self-propagating nature of WannaCry exploited a specific Microsoft Windows vulnerability, which made its way to the NHS network because most devices were running Windows operating systems more than 15 years old and no longer updated or supported by Microsoft[1].
  - Nevertheless, it is clear that the attack's motivations were monetary gain and causing mass destruction, given that it affected over 150 countries, infected more than 200,000 computers, and resulted in estimated total damages of $4 billion dollars[4].
- Timeline of events:
  - **March 2017:** Microsoft released a security update for supported versions of Windows, addressing the same vulnerabilities that WannaCry was exploiting[5].
  - **Unknown:** NHS's failure to patch, update to supported systems, and their reliance on old software leaves them vulnerable to attacks.
  - **May 12, 2017:**
    - WannaCry discovered by an independent researcher→NHS England affected and declares the cyber attack a national major incident→Staff devices and medical equipment locked→A cybersecurity researcher activates a kill-switch to stop WannaCry. Some NHS organizations remained infected, but the kill-switch prevented them from being locked out of their devices and systems.[2]
  - **May 12-19, 2017**: NHS responds in three phases: focusing on securing emergency care pathways, ensuring the stability of primary care services, and initiating a remedial phase[2].
  - **May 13, 2017:** Microsoft releases a security update for all customers, including those using Windows XP, Windows 8, and Windows Server 2003[5].
  - **Aftermath:**
    - Estimated to cost the NHS £92 million after 19,000 appointments were canceled as a result of the attack[4].
    - The Department of Health, NHS England and the National Crime Agency have reported that no NHS organizations paid the ransom[2].
    - The NHS has identified the need to improve the protection of services from future cyber attacks[2]:
      - Develop a response plan setting out what the NHS should do in the event of a cyber attack.
      - Ensure that all parties involved take cyber threats seriously, and understand the direct risks.
    - NHS England and NHS Improvement made parties ensure that they had implemented all 39 CareCERT alerts issued by NHS Digital between March and May 2017 and had taken action to secure local firewalls[2].

Post-Attack Discussion and Analysis:

Through researching the WannaCry ransomware incident, the role of governments in cybersecurity interested me. I believe it's worth discussing the practices of the U.S. NSA in how they created and kept the WannaCry exploit (along with other exploits) a secret, which raises questions about who regulates the actions of governments. Is it ethical to collect exploits for use against other nations or criminals? These questions are complex and require careful consideration, particularly in a world where technology is rooted in everyday life, from healthcare and education to retail. As our world

becomes increasingly tech-dependent, the inevitable vulnerabilities in the digital realm highlight the urgent need for governments to prioritize digital literacy for their citizens. Moving forward, I believe governments should take more action to promote digital literacy and educate citizens about the risks of the digital world. I understand this may be challenging, as people tend to stick to their past beliefs and habits. For instance, in the past, leaving your social security numbers in publicly accessible places like libraries did not pose huge risks[1]. However, we must now protect personally identifiable information because it is necessary for authenticating oneself in the digital world. Unfortunately, many people may wonder why things like a seemingly minor software update is essential. This lack of awareness opens doors to unintended consequences, as noted by the WannaCry attack. It is worth noting that not everyone has the privilege of furthering their digital education. From my experience with family and friends, I have seen older relatives fall victim to phishing scams and malware attempts due to their lack of digital literacy. What I can gain from this case study is that citizens and governments should work together to promote digital literacy through media and regulation. As WannaCry showed, the worm could spread through networks, and anyone could be affected purely by chance.

References

[1] Collier. Nhs ransomware attack spreads worldwide. *CMAJ: Canadian Medical Association Journal*, 189(22):E786–E787, 2017.

[2] U.K. National Audit Office's Comptroller and Auditor General. Investigation: Wannacry cyber-attack and the nhs, 2017. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[3] CIS Center for Internet Security. Eternalblue, 01 2019. https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2019/01/Security-Primer-EternalBlue.pdf.

[4] Kaspersky. What is wannacry ransomware?, 2019. https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry.

[5] Microsoft. Customer guidance for wannacrypt attacks, 05 2017. https://msrc.microsoft.com/blog/2017/05/customer-guidance-for-wannacrypt-attacks/.

[6] U.S. Department of Justice. Three north korean military hackers indicted in wide-ranging scheme to commit cyberattacks and financial crimes across the globe, 07 2022. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

[1] Dr. Lindah Kotut mentioned this in class, and I thought it was interesting.