WannaCry Ransomware attack on National Health Service(NHS)

Introduction to the case

A Cyberattack tool, which was believed to be developed by US National Security Agency affected the NHS (National Health Service) on a large scale in May 2017, Its effect was seen in more than 150 countries[1] and more than 600 organizations were affected.[6] Mikko Hypponen, of F-Secure, stated that it was the biggest ransomware attack in history [1] The attack caused a complete lockdown of a computer system with a red-lettered message demanding ransom in bitcoins in a particular cryptocurrency wallet.[3] All the staff had no other option than to use pen and paper and their own mobile phones.[2] Hundreds of thousands of computer systems were shut down with all their data encrypted. Major surgeries and doctor's appointments were canceled.[1] The encrypted data on the computers demanded payments of $300-$600 to regain access to the system. Medical care in some areas was brought to a sudden complete halt [2].

Literature Review

A Ransomware called WannaCry is sent to the recipient via Email and users are tricked into opening the attachments in the email which in turn releases the malware into the system.[3] Once the malware is in your system, it locks up and encrypts the files in such a way that it cannot be accessed anymore.[1] It then asks for ransom in the form of cryptocurrency to regain access. WannaCry affected the systems that had not installed Microsoft security update of April 2017 or those using outdated Microsoft Windows without any antivirus software or firewalls on the system.[3] This simple mistake cost NHS around 20 million pounds between 12 May and 19 May and another 72 million pounds in cleanup and upgrades to its IT system and data recovery.[2] NHS estimated that around 19,000 appointments might have been canceled in total.[5]

Experts from many security firms strongly advised all the affected users against the payment of ransom.[3] High revenue to the hackers would make the attack successful and encourage more such attacks. As per the reports, a total of 327 payments were made totaling US $ 130,634.77.[3] Just a day after the attack, Microsoft released security updates for outdated operating systems.[3] The only good news was that researcher Marcus Hutchins found out a kill switch hardcoded in malware which can stop the malware from further spreading.[3]

The Ransom notes were analyzed and predicted that the creators of the WannaCry were fluent in Chinese and had proficient English, the notes were both human written and translated by machine.[3] According to the FBI Cyber Behavioral Analysis center, the computer that was used to create WannaCry had Hangul language fonts installed in their system.[3] Metadata in the language file was also analyzed and was found out that the time zone on the computer that created the worm was set to UTC +09:00, used in Korea.[3] Various cybersecurity companies like Kaspersky Lab and Symantec said that codes were very similar to what was previously used by Lazarus Group based in Korea, who were suspected to have carried out many cyber-attacks in the past.[3] Brad Smith, President of Microsoft and UK National Cyber Security Center and many other cybersecurity organizations reached the same conclusion that the origin of the WannaCry was from North Korea.[3]

NHS was already warned critical alerts about a possible Cyberattack a year before by NHS Digital, but no major actions were taken.[4] The department and the Cabinet sent a written letter to NHS that it was very necessary for them to shift from old software by April 2015.[4] According to NHS Digital all the organizations infected by the WannaCry had the same vulnerability and some simple actions would have protected them from something this big. All the victim organizations had unsupported operating systems without antivirus or firewalls and unpatched operating systems so they were open to any cyber-attack.[4] NHS accepted that it was there fault no to have updated systems or implemented proper firewalls and they weren't prepared for any Cyber-attack.[4] NHS England and NHS improvement asked all the major health groups asking them to ensure that they have operated on all major notices and alerts issued by the NHS digital.[4] This attack could have been easily prevented by taking some simple measures. This mishandling, unpreparedness, and negligence cost NHS millions of dollars and brought medical services to halt.[5] After the attacks, NHS signed a contract with Microsoft to upgrade its computers to Windows 10.[2] NHS invested a lot in upgrading their IT and software and improve their security standards.[3] They also posted 22 lessons learned from the Cyber-attack and learned the importance of cyber-security.[11]

▪ <u>Liffícks Analysis of the case</u>

i. ***<u>Ethical Issues in this case:</u>***

- Privacy: Privacy of every system was exploited by encrypting all the user data.
- Security: Computer systems were breached.
- Responsibility: Proper system updates and security patches were not used even after critical warnings.
- Confidentiality: Confidential information was accessed in an inappropriate manner.
- Trust: Trust on an organization was broken.

ii. ***<u>Main participants and actions</u>***

<u>Primary Participants</u>

- Lazarus Groups of hackers (Suspected)
    - Wrote a malicious worm which encrypts the data in a computer system
    - Sent the worm to different organizations to spread via email.
- NHS Digital
    - Gave critical warnings to the organization who were vulnerable to upgrade their system, apply patches and implement firewall.
- NHS and other affected organizations
    - Didn't took security measures even after critical warnings were given to them regarding system upgrade and possible ransomware attack.
    - Lost a lot of money in fixing the issue.
    - Most of their medical service was brought to halt.

<u>Secondary Participants</u>

- Local Consumers
    - people's appointments were canceled and had to suffer in case of a medical emergency.

- Security Organizations
    - Studied the ransomware and found a kill switch which could stop the worm from spreading.

Implied Participants:

- Operating systems providers
    - The operating systems that were vulnerable were out of service and no security updates were provided for them.

iii. ***Reduced List***

- NHS didn't know the importance of Cyber Security and kept on working with the old systems and became the major victim of the attack.
- Lazarus group were the main culprits and were the ones held responsible for the attack.
- NHS Digital knew the probability of any sort of Digital attack on different organizations because of several cases in past years. They knew that old systems with outdated very vulnerable.
- Consumers or Patients of NHS suddenly got all their appointments and surgeries canceled, they were indirectly affected. Hence, they can be eliminated from the scenario
- Security organizations tried to understand and stop the ransomware. They were not affected. Hence, they can be taken out of the list.
- Operating system providers must terminate the use of older operating systems for which no security patches are released. They had a minimal role in this.
- As a result of these assumptions, all participants can be eliminated except:
    - Lazarus NHS
    - Group

iv. ***Legal considerations***

- UK Financial Conduct Authority(FCA) recognizes a cyber-attack to be material if there is a notable loss of data or if someone loses the control of IT systems, affects a lot of customers or results in malicious software taking control of the system. [7]
- FTC Enforcement: An organization's failure to secure its networks from ransomware can cause a lot of harm to consumers or employees.[8] Also according to FTC an organization's failure to maintain, update and patch its system know to be exploited by ransomware could violate Section 5 of FTC act.[8]
- Litigation: In an event of Ransomware Litigation is another potential risk. Affected entities may face lawsuits from their consumers or business partners.[8]
- It is not forbidden to pay ransom under English law, but still, if an organization knows before paying a ransom that the funds would be used for terrorist funding, it would be an offense under Section 17 of Terrorism act 2000.[7]
- Banks and financial institutions must be aware that intentionally encouraging or assisting a crime like this is an offense under section 44-46 of Serious Crime Act 2007.[7]

v. ***Possible Options for participants***

- NHS could have:
    - Taken all the alert seriously and updated their software's, Operating system and installed firewalls and security patches.

  - They could have trained all their employees about the importance of cybersecurity and how to stay protected from any possible cyber-attacks.
  - They could have learned from the previous attack on other organizations and taken it seriously.
- Lazarus Group:
  - Their main motive behind the attack can be to extract money from the victims and create chaos

vi. ***Possible Justification for Actions***

For the NHS:

- Simply kept on working with the older systems and didn't knew about the importance of cyber-security and didn't consider any possibility or threat of cyber-attack.
- They didn't know if updating systems, applying patches, implementing firewalls, would benefit the organization in any way.
- No Employee Awareness

For Lazarus (Suspected):

- Fundraising: They asked for around 300 dollars in Bitcoin per encrypted machine. That would fit the profile of a communist country that is cash strapped, say security experts.

vii. ***Key Statements***

- "all the computers are down. Doctors are told to log everything on paper." [10]
- "…It's very interconnected so if you get an attack in one place it tends to spread."[11]
- "a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice,"[11]
- "Essentially they relied on a domain not being registered and by registering it, we stopped their malware spreading,"[1]
- "has accepted that there are lessons to learn" [11]
- "…. investing over £60m to address key cyber-security weaknesses - and plan to spend a further £150m over the next two years…."[2]
- NHS Improvement published a set of 22 "lessons learned" recommendations following the cyber-attack.[11]

viii. ***Questions Raised***

- NHS didn't understand the importance of having their systems upgraded?
- Was there a need to develop such a malicious application?
- Even after critical warnings, why didn't NHS do the needful?
- Why did the ransomware affect NHS the most?
- Can the effect on NHS be considered as their own fault?
- Why didn't the Operating system provider completely shut down the working of the Operating systems?

ix. ***Analogies employed***

- SimpleLocker ransomware attack on Android in late 2015, It encrypted all the files in an made them inaccessible without the scammer's help. [9]

- NotPetya was an updated version of Wannacry and was active just weeks after the WannaCry attack. [9]
- Another Ransomware that hit in 2017 and 2018 was Ryuk. Organizations that had little tolerance for downtime were there prime target.[9]
- Cryptolocker ransomware in 2013, It spread via attachments in spam messages.[9]

x. ***Code of Ethics Utilized***

Following ACM code of ethics apply:[12]

- 1.1
- 1.2
- 1.3
- 1.6
- 1.7
- 2.7
- 2.8
- 2.9
- 3.1
- 3.4
- 4.1

▪ Three Alternative Proposals

- Optimistic
  - The ransomware attack could have been avoided in the first place if all the employees of NHS were educated about cybersecurity and measures taken to avoid cyber attacks. The ransomware was sent as an attachment in an email which could have easily been avoided if the users had any sort of knowledge about it.
  - If NHS had invested in upgrading its system, security software's or installed security patches the whole scenario would have been avoided.

- Pessimistic
  - WannaCry ransomware affected the systems of NHS, security experts found a Kill Switch that prevented the spread of ransomware which minimized the damage done by a lot.[1] If the Kill Switch wasn't found the damage done on NHS would be very high. They would have to pay a ransom per system, in order to get the access back, that to with no guarantee. If the issues weren't resolved within a couple of days the number of appointments and surgeries canceled would have been tens and hundreds of times the current number, which could have even resulted in a loss of human life.
- Compromise
  - WannaCry affected organizations around the world and caused a lot of chaos. NHS was the most affected and had to spend around 90 million pounds for recovery. The good thing was that they recovered and signed a contract with Microsoft for updated Windows10. They invested a lot in their IT and educated their employees regarding cyber-security after the attack and made their systems hard to penetrate. Getting to know the importance of cybersecurity cost them a lot but that a big lesson learned.

- **Ethical Theory of Conclusion**

The ethical theories that affected the case the most were 1.2, 1.6, 2.7, 3.1.[12] It's a simple rule that no harm must be done to anyone or anyhow either they are protected or not and everyone's privacy must be respected, any sort of attempt to violate anyone's privacy and stalk them is completely unethical. In this case, hackers found a loophole in the systems of many organizations and companies and created ransomware to get into their system for their own personal benefit. Apart from that, it is also the responsibility of an organization to stay protected by constantly updating its systems, applying security patches, using good antivirus software's and spreading awareness among everyone about computer technologies, its power and how much it can make human life easy and consequences if misused.

- **Conclusion**

Many organizations and companies are still not aware of cybersecurity and therefore, they do not give much importance to it. NHS also had the same thought process and they were completely clueless about the hazards of using old outdated and vulnerable systems. Even after being warned they didn't take any action which cost NHS millions of dollars. It was a huge realization for such a big organization who didn't understand the importance of cybersecurity. If the attack would have been more brutal it also could have costed a human life. Therefore, it is very important for every organization to understand the importance of cybersecurity and stay secure.

WannaCry was a devastating incident in the history of cybercrime, but it was just a teaser of what can the world expect in the future if proper actions are not taken. It is very difficult to find, investigate and arrest the people who commit cybercrimes. It's now time that we must learn from our past mistakes and do everything possible to prevent any such attacks. In order to tackle cyber-crime, the world and each governing body of every country must know its seriousness and how devastating it can be. The world needs a common worldwide governing body to fight against cyber-crime like Interpol or WHO.

- **References:**

[1] Graham, Chris. (20 May 2017), Cyber attack: Ransomware Explained [online]. Available at https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/ [Accessed 6 Nov 2019]

[2] Field, Matthew. (11 Oct 2018), WannaCry cyber attack cost the NHS 92m pounds as 19000 appointments cancelled. Available at https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ [Accessed 6 Nov 2019]

[3] WannaCry ransomware attack, Wikipedia: The Free Encyclopedia. Available at https://en.wikipedia.org/wiki/WannaCry_ransomware_attack [Accessed 6 Nov 2019]

[4] nao.org.uk. (27 Oct 2017), Investigation: WannaCry cyber attack and the NHS, ISBN: 9781786041470. Available at https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/ [Accessed 7 Nov]

[5] Higgins, Patrick. (7 Nov 2018), THE WANNACRY CYBER ATTACK: A CASE ANALYSIS, Corporate Social Responsibility. Available at https://www.corporateresponsibilitynetwork.com/wannacry-cyber-attack/ [Accessed 6 Nov 2019]

[6] Ghafur, S. Kristensen, S. Honeyford, K. Martin, Darzi, A & Aylin, P. (2 Oct 2019), A retrospective impact analysis of the WannaCry cyberattack on the NHS. Available at https://www.nature.com/articles/s41746-019-0161-6 [Accessed 7 Nov 2019]

[7] Brown, Mayer. (Aug 2018), Cyber attacks: legal and regulatory considerations arising in their wake. Available at https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2017/08/cyber-attacks-legal-and-regulatory-considerations/files/cyber-attacks-legal-and-regulatory-considerations/fileattachment/cyber-attacks-legal-and-regulatory-considerations.pdf [Accessed 8 Nov 2019]

[8] Kurth, Hunton Andrews. (16 May 2017), Global Ransomware Attacks Raise Key Legal Considerations. Available at https://www.huntonprivacyblog.com/2017/05/16/global-ransomware-attacks-raise-key-legal-considerations/ [Accessed 8 Nov 2019]

[9] Fruhlinger, Josh. (5 April 2019), The 6 Biggest ransomware attacks of last 5 years. Available at https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html [Accessed 8 Nov 2019]

[10] Murray, Sean. (12 May 2017), This was an international attack: NHS plunged into chaos in large-scale cyber hack. Available at https://www.thejournal.ie/nhs-cyber-attack-3386944-May2017/ [Accessed 10 Nov 2019]

[11] BBC. (17 April 2018), NHS could have prevented WannaCry ransomware attack. Available at https://www.bbc.com/news/health-43795001 & https://www.bbc.com/news/technology-41753022 [Accessed 10 Nov 2019]

[12] ACM Code of Ethics and Professional Conduct. (22 June 2018). Available at https://www.acm.org/code-of-ethics

- **<u>Bibliography</u>**

- Cyber Security Policy. (Oct 2018), Securing cyber resilience in health and care: Progress update. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf
- Johnson, Sarah. (16 Nov 2018), More NHS cyber-attacks ‘inevitable’, warn experts. Available at https://www.theguardian.com/society/2018/nov/16/more-nhs-cyber-attacks-inevitable-warn-experts
- Griffin, Andrew. (16 May 2017), NHS Cyber Attack. Available at: https://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-hack-north-korea-who-behind-hospitals-hackers-lazarus-a7738026.html