Student id:20625630
Name: Viraj chetan Punjani

Assignment-2 (ICB)

WannaCry:

1. In May 2017, WannaCry was a ransomware worm that rapidly spred via computers and links/emails across the world. WannaCry lasted for four days. WannaCry is a type of crypto-ransomware, used by cybercriminals or hackers to extract money for their malicious intent. WannaCry is also known as WannaCrypt. Once WannaCry has entered a computer then it starts to encrypt all essential files and we will not be able to access any files till they provide us the decrypted keys and they will only provide that when we will fulfil their demands by paying the dollars/pounds in cryptocurrency like bitcoin. WannaCry was so devastating because it has taken advantage of unpatched windows vulnerability and they had exploited that properly. Moreover, it was spreading at a vast speed via emails and links. The tools that allowed the development of ransomware are believed to have been developed by NSA(National security agency) U.S.A and later it got exploited by the hacker group called shadow brokers.
   Retrieved from:(CSO INDIA).

2. The main reason for this attack was to steal dollar's from innocent people and to create a panic situation so that they can take good advantage of that and demand for dollars/pounds within/3days of time and if they decline to give them $300 then they will either delete/erase their essential data or they will not send the decrypted keys to the infected PC's. There are many ways ransomware can get into your PC or system. With the help of emails, links and attachments , WannaCry is mostly delivered which tricks the users and by this way malware is released into the computer systems in a technique known as phishing. The main target was hospitals (healthcare

organizations), universities', knocking out banks, public transit systems and computers who were using the Microsoft Windows operating system.
Retrieved from:(CSO INDIA)(TECH REPUBLIC).

3. WannaCry spread through computer Operating Microsoft windows. Exploit kit named as 'Eternal Blue' was developed by NSA (U.S.A) to exploit the SMBv1 vulnerability. WannaCry ransomware attacked 200,000 windows systems by exploiting the SMBv1 vulnerability via the EthernalBlue kit in 2017. To share files to the Windows systems connected to the same network/domain there is a file-sharing protocol named (SMB) A server message block. With the help of SMBv1 vulnerability hackers can take control of an infected system however a patch was released by Microsoft to address the vulnerability but those whose OS was outdated/old and who had not updated the latest security updates have suffered from this outbreak. SMB was using an old system that's why it got vulnerable to hack and the shadow breakers took advantage of these loopholes. Microsoft Windows was vulnerable to zero-day vulnerability and they were exploited by shadow breakers in a vast number of releases of functional exploit tools. However, by exploiting these vulnerabilities it led to remote code execution and full system access.
Retrieved from: (CYWARE.COM).

4. The negative impact where patients appointments got cancelled, surgeries, and emergency admissions to hospitals were cancelled and it got diverted to the other dates. The estimated cybercrime was approx $4 billion in terms of losses all around the world. Not only that it had a huge impact across the infected hospitals. Approx. 13,500 appointments got cancelled during the WannaCry week. This outbreak afflicts over 300,000 +computers who got infected in over 150 countries. After this attack people stopped trusting the NHS hospital. Ambulances were reportedly rerouted leaving people in need of urgent care. Approx. 19,000 appointments were cancelled as a result of this ransomware attack.
Retrieved from:(TECH REPUBLIC)(CSO INDIA).

5. The other ransomware like WannaCry were: Petya, NotPetya, Locky, Crysis, Nemucod, Jaff, Spora, Cerber, Cryptomix, Jigsaw

ransomware, But none of this ransomware had created the impact like WannaCry.
Retrieved from :(TECH REPUBLIC).

References/ SOURCE:

1. CSA INDIA COM:

JOSH FRUHLINGER CSO ,30 AUGUST (2018) 19:22 IST, WHAT IS WANNACRY RANSOMWARE, HOW DOES IT INFECT, AND WHO WAS RESPONSIBLE? 8 TH APRIL RETRIEVED FROM https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

2. TECH REPUBLIC:

Alison DeNisco Rayome, October 31 (2017) 5:43 AM PST, THE TOP 10 WORST ATTACKS 2017, SO FAR, 8TH APRIL RETRIEVED FROM:

https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/

3. CYWARE SOCIAL:

N.D(NOT DECLARED), June 15 (2019), what is SMB vulnerability and how it was exploited to the WannaCry ransomware attack? 8th APRIL RETRIEVED FROM:

https://cyware.com/news/what-is-smb-vulnerability-and-how-it-was-exploited-to-launch-the-wannacry-ransomware-attack-c5a97c48