Assignment 2

Name: Hayden Cordeiro BECOMPS **RollNo**:05

Case Study on WannaCry,Ransomware 2017

Working of WannaCry

During May 2017, a ransomware worm known as WannaCry infected all computer networks across the globe. Infecting Windows computers, it encrypts files on the PC's hard drive, making them inaccessible to users, and demanding a bitcoin ransom to decrypt them.WannaCry is composed of several components. Droppers, which are self-contained software programs that extract other application components embedded in themselves, are used to infect the infected computer. A data encrypting and decrypting application, encryption keys, and a copy of Tor are among these components. A Hardcoded URL (so-called kill switch) is accessed in the first place; if it cannot, WannaCry tries searching and encrypting numerous popular file formats, such as Microsoft Office documents and MP3s, leaving them inaccessible to users. This is followed by a ransom notice requesting $300 in Bitcoin to decrypt the files. Wormhole WannaCry exploits the implementation of the Server Message Block (SMB) protocol in Windows. By tricking Microsoft's implementation of the SMB protocol into executing arbitrary code, the SMB protocol allows different network nodes to communicate amongst themselves.Rather than reporting the vulnerability to the information security community, the U.S. The National Security Agency developed an exploit called EternalBlue, which exploits this vulnerability. On April 8, 2017, the Shadow Brokers, an anonymous hacking group, released the exploit in an obfuscated form in an apparent Medium post. It was Microsoft itself that discovered the vulnerability in May and had released a patch. However, many systems were still vulnerable, so WannaCry was able to infect computers through EternalBlue.

Preventive measures to prevent WannaCry

Almost two weeks before WannaCry launched, Microsoft Security Bulletin MS17-010 updated the Windows implementation of the SMB protocol to prevent infection via EternalBlue. Even so, in May of 2017, as WannaCry began rapidly spreading, many systems were still unpatched despite the fact that Microsoft had stated the patch was critical.

When unpatched systems are infected, the only option is to restore files from safe backups.

Preventive Measure

1. Keep System up to date
2. Keep Backups
3. Use Spam and Anti-Virus Protection.
4. Be Attentive to Cybersecurity News.

Organisations attacked by WannaCry and how they managed to detect and respond to it.

1. Russian Military

   Russia's Defense Ministry detected and rapidly blocked all the WannaCry ransomware attacks at its information infrastructure, a high-ranking source in the ministry told reporters on Tuesday.As for the ministry's computers connected to the internet, all of them have modern Russian-made protection systems that are constantly updated and allow to combat the current and future cyber threats," the source said.The WannaCry attacks on the ministry's information infrastructure have been timely detected and rapidly blocked," the Russian Defense ministry's source stressed.

2. Andra Pradesh Police

WannaCry ransomware hacker attack has reportedly affected about 25 percent of the computer network of the Andhra Pradesh police department on Saturday. However, senior officials said damage was minimized to 18 standalone systems.However, critical data in almost all police stations was secured and no great damage was done. As a precautionary measure, the department has consulted the National Cyber Security Cell in Delhi, officials said.

When they received an alert they took precautionary measures on the advice of the National Cyber Security Cell.When some systems were found to be encountering problems, they were asked to be unplugged as a precautionary measure.

Loss in terms of finance / reputation / etc ?

More than 350,000 computers were infected by the WannaCry virus in the span of 4 days, causing billions of dollars in damages. The attack was particularly destructive to healthcare organizations, including the National Health Service (NHS) in the U.K., due to their extensive use of outdated and unpatched Windows devices. A major attack rendered critical equipment and systems unusable, forcing emergency rooms to close and lifesaving devices like magnetic resonance imaging (MRI) to halt.

Large manufacturers that used vulnerable versions of Windows were also affected by WannaCry. There were many production outages that were extremely costly.

References:

https://www.researchgate.net/publication/327463247_Wannacry_Ransomware_and_the_Emerging_Threat_to_Corporations
https://www.osti.gov/servlets/purl/1423027