Edmark R. Gariando
BSIT 3-1

WannaCry

Summary

- On May 12, 2017, A freelance physicians in hospital of UK experienced the biggest and notorious ransomware in history called "**WannaCry**". The virus affects different organizations computers, especially those who have not been updated or have lower versions and lower security measures. Hackers encrypted their files and displayed a ransom note demanding a $300 worth of Bitcoin before the company can access again or decrypt the files. This ransomware which was encrypting the files was called "**WanaCrypt**", but people quickly started calling it as "**WannaCry**". Many Cyber Security Experts investigated this ransomware on how it started, who it belongs, and how they able to stop this virus.

After several trials of reverse-engineering a program for this virus, they finally managed to stop the spreading of the WannaCry Virus. A statement from the US Department of Justice states that the ransomware virus came from a North Korean programmer and a member of hacking group known as the "Lazarus Group." They concluded that the hacker rented a server for this activity and has a total of 30 email addresses. DOJ asked Google for information about these Gmail accounts, and after tracking it, the email addresses were connected to one person because of the same files and the emails sent between each other's accounts. They also tracked the logs transferred to a Bitcoin Account, but they cannot access more when Bitcoin is transferred to Monero, which is another type of cryptocurrency. Because Monero has extra layer of security features such as the amount of money is stay hidden and generated a one-time address for each transaction.

Reaction/Conclusions

- The ransomware "**WannaCry**" only reminds us to always stay vigilant, and outdated system software can be vulnerable and become a source of any network threats that might affect every individual, organization, or even nation. While "**WannaCry**" is the biggest ransomware in

history, it also served as the biggest lesson that we need to address by emphasizing the importance of system updates and enhancing security protocols against malicious attacks.

We cannot only focus on making countless money, but we also need to focus on how we protect those money. Improving Cyber Security measures can help us mitigate those kinds of risks in the future.