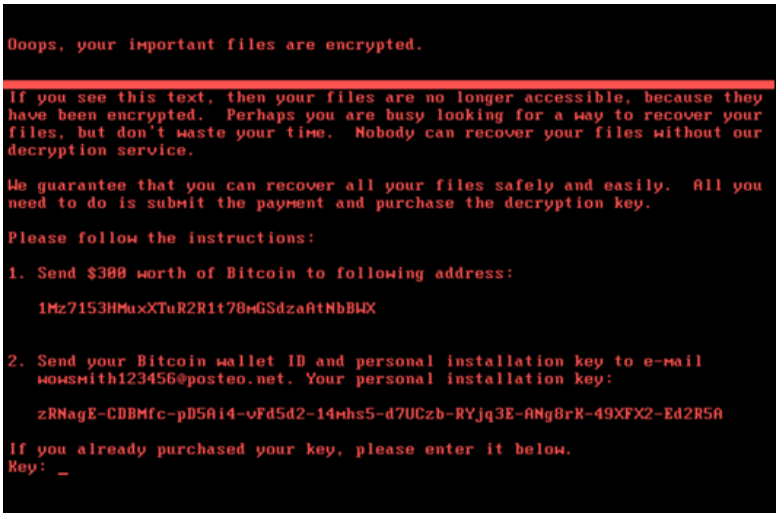
Antonio Shields

December 1, 2022

CS 462 – Blog Term Project

NotPetya Malware Attack



https://www.crowdstrike.com/wp-content/uploads/2017/06/PetrWrap.png

The NotPetya malware attack, according to Greenberg (2018) is the most devastating cyberattack in history. Greenberg probably labeled this attack “the most devastating” because of the estimated $10 billion dollars in damage that it inflicted according to the White House and because of the many networks, companies, and countries this cyber attack was able to infiltrate and successfully disrupt operations in a short period of time.

NotPetya was initially launched on June 27, 2017, which, according to Brumfield (2022), was the eve of Ukraine’s Constitution day holiday. NotPetya was, according to HYPR (2022), a Russian state-sponsored targeted cyber warfare attack that aimed to cripple Ukrainian networks and dissuade other countries from doing business with them. According to Saravanan (2022), the timing of the attack was possibly intentional because most IT employees would not have been at work due to the national holiday.

NotPetya Malware Attack

Although the initial target was Ukraine, the malware effects would soon spread far beyond their borders.

NotPetya's name was given by Kaspersky Labs upon discovery in June 2017. NotPetya was named after the ransomware Petya, which, according to Miller (2021) was ransomware that was created by a group calling itself Janus Cybercrime Solutions in March of 2016. Ransomware is a form of computer virus with the purpose of disabling a computer system useless by encrypting the computer's data to where it is no longer accessible by the user. To regain full access to the encrypted data, the victim is usually offered a decryption solution in exchange for a monetary ransom. According to Cooper (2022), the hackers' goal is to make a monetary gain while staying anonymous, so they will often utilize Bitcoin to extort payments without being traced. In the case of Petya, according to Cooper (2022), Petya lasted from March 2016 until the end of 2016 and was refined three times prior to being shut down by Janus Cybercrime Solutions. Although NotPetya was named after Petya because it displayed similar characteristics to Petya and was assumed originally to be a variant of it, it was soon discovered that NotPetya did not have the same intentions.

How NotPetya conducts its cyberattack is, according to Positive Technologies (2017), it uses TCP ports 135, 139, and 445 to spread using the Server Message Block (SMB) and Windows Management Instrumentation (WMI) services. How NotPetya spreads to other hosts on a network can occur in several different ways: Windows Management Instrumentation (WMI) and PsExec, as well as an exploit of vulnerability MS17-010 (EternalBlue). (Positive Technologies, 2017). EternalBlue, MS17-010, according to Brumfield (2022), was developed by the U.S. National Security Agency (NSA). Newman (2018), also mentioned that EternalBlue was a Microsoft Windows operating system software vulnerability and bug that was intended to be weaponized. According to Newman (2018), the group known as the Shadow Brokers in April 2017, leaked alleged multiple NSA tools to the public, with the EternalBlue exploit being included. Newman (2018), also mentions that the NSA has never officially confirmed that it created

NotPetya Malware Attack

EternalBlue, anything else in the Shadow Brokers releases, or that it was breached, but EternalBlue's origin can be traced back to the NSA through a number of reports, even Microsoft has publicly attributed its existence to the NSA. According to Positive Technologies (2017), WMI is a technology for centralized management and monitoring of Windows-based infrastructure and PsExec is widely used for Windows administration and allows running processes on remote systems. However, WMI and PsExec require local administrator privileges to run, which means that NotPetya can spread only from computers on which users have maximum OS privileges. (Positive Technologies , 2017). The EternalBlue exploit made it possible to gain maximum administrator privileges on any affected systems. (Positive Technologies, 2017). NotPetya also utilized a publicly available tool called Mimikatz that extracts passwords to obtain the credentials of all Windows users in plaintext, including local administrators and domain users. (Positive Technologies, 2017). Utilizing the exploit in tandem with the password extractor allows for NotPetya to spread to multiple computers and networks, even those that were up-to-date on the EternalBlue patch that was released prior to the NotPetya attack according to Greenberg (2018).

NetPetya was initially able to start its infiltration, according to Greenberg (2018), through a piece of accounting software called M.E. Doc, which is compared to the Turbotax or Quicken that is used in the United States. M.E. Doc is used by many Ukrainians and installed on many computers throughout the country. M.E. Doc is owned by Linkos Group, which is a small family-run Ukrainian software business. (Greenberg, 2018). According to Greenberg (2018), the Russian military hackers were able to hijack the Linkos Group's update servers and created a hidden back door sometime prior to the launch of NetPetya. Then at the opportune time prior to June 27, 2017, the back door was utilized, an update was pushed to the software users and the NotPetya cyber attack began.

According to Greenberg (2018), When Netpetya was initiated, it was set to spread automatically, rapidly and indiscriminately. When NotPetya first reached and infected a computer according to Saravanan (2022), a threatening message appeared on the screen and said that all the files on the device were

encrypted and demanded $300 in bitcoin as ransom, which subsequently claimed that if the ransom was paid to wowsmith123456@posteo.net, which was shut down by posteo upon discovery, a decryption key would be given to restore the computer back to normal. This similarity is why NotPetya is often compared to the Petya ransomware and why it is often referred to as ransomware itself. The reason why NotPetya differs from Petya is that the ransom demand in exchange for a decryption key was a guise. According to Saravanan (2022), NotPetya was actually modified wiper malware, which was designed to make the system inaccessible once infected.

According to Cooper (2022), about 80 percent of all NotPetya attacks hit computers in Ukraine. However, because of the rapid spread of NotPetya when it moved through networks, it spread to other businesses outside of Ukraine. According to HYPR (2022), some of the most notable businesses affected were: Pharmaceutical giant Merck, which lost $870 million, Mondelēz, the parent company of Cadbury Chocolate lost $188 million, Fedex's European subsidiary TNT Express lost $400 million, and UK global shipping giant Maersk lost between $250 million to $300 million. Most of these businesses did not have proper, timely, and encrypted backup systems in place to restore from and had their operations come to a standstill until solutions were discovered. Maersk for example, according to Greenberg (2018), was able to recover its data because one office in Ghana, Africa, suffered a blackout prior to NotPetya being launched and stayed offline and disconnected. This allowed Maersk to recover its systems prior to the attack and get operations back online.

This malware attack shows the importance of making sure that good cyber hygiene is practiced individually and corporately. Ensure to thoroughly vet emails and do not open attachments from unknown sources to avoid phishing attacks, keep all computers and devices constantly updated with the latest patches and software. If all computers were updated with the patch that was released prior to the launch, there would not have been that vulnerability to exploit and would possibly have had a better

outcome. Most importantly, ensure that you backup all data, keep the backups updated for any changes or modifications, and keep it encrypted to ensure unauthorized tampering.

References:

Brumfield, C. (2022, June 27). 5 years after notpetya: Lessons learned. CSO Online. Retrieved December 1, 2022, from https://www.csoonline.com/article/3664930/5-years-after-notpetya-lessons-learned.html

Cooper, S. (2022, November 11). What is Notpetya Ransomware & How to protect against it. Comparitech. Retrieved December 1, 2022, from https://www.comparitech.com/net-admin/notpetya-ransomware/

Greenberg, A. (2018, August 22). The untold story of notpetya, the most devastating cyberattack in history. Wired. Retrieved December 1, 2022, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

HYPR. (2022). What is NotPetya? 5 Fast Facts. Security encyclopedia. Retrieved December 1, 2022, from https://www.hypr.com/security-encyclopedia/notpetya

Miller, C. (2021, October 7). Throwback attack: Petya, the Red Skull of Ransomware. Industrial Cybersecurity Pulse. Retrieved December 1, 2022, from https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-petya-the-red-skull-of-ransomware/

Newman, L. H. (2018, March 7). The leaked NSA Spy Tool that hacked the world. Wired. Retrieved December 1, 2022, from https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

NotPetya Malware Attack

Positive Technologies. (2017, June 28). Everything you wanted to know about Notpetya but were afraid to ask. Positive Technologies - vulnerability assessment, compliance management and threat analysis solutions. Retrieved December 1, 2022, from https://www.ptsecurity.com/ww-en/about/news/everything-you-wanted-to-know-about-notpetya-but-were-afraid-to-ask/

Saravanan, A. (2022, November 29). NotPetya - Not your average ransomware. ManageEngine Log360. Retrieved December 1, 2022, from https://www.manageengine.com/log-management/cyber-security/notpetya-ransomware.html