2024

NotPetya

THE DESIGNER ATTACK THAT REVOLUTIONIZED CYBER WARFARE

JOSHUA RUSSELL

Joshua Russell
CYSE 280

Introduction

On April 4, 1975, a new computer operating system was born that would change the way users interact with computing devices in the future. Microsoft, created by childhood friends Bill Gates and Paul Allen, originated as an implementation of the BASIC program that would become an interpreter for the first microcomputer produced by Altair. Fast forward to November 20, 1985, and the Windows iteration of the Microsoft program was sent to market as a replacement for MS-DOS (Warren, 2020). With widespread popularity for its ease of use in software development to create compatible applications, Windows has become the gold standard of modern-day operating systems. From individual users to corporations and governments, it is no wonder that Windows has become susceptible to vulnerabilities, threats, and attacks such as NotPetya. NotPetya, a self-replicating worm discovered in 2017, is an attack that affected more than 12,500 computers systems across sixty-five countries. It mimicked ransomware, in which, the worm encrypted everything on a device and requested Bitcoin payment for decryption; however, NotPetya was not ransomware. CIA designated attribution of this attack to the GRU, which is Russia's version of their intelligence and spy agency. With elements of previous attacks and code that compromises existing vulnerabilities, NotPetya had devastating effects. Over time, the NotPetya worm did so much damage, it was considered one the worst cyber-threats in history. This cyberweapon changed the way researchers approached cyber-attacks and their abilities to destroy. This paper seeks to address the reach of the NotPetya worm, and the consequences spread around the world, crippling systems.

Overview

On the heals of its predecessor Petya, NotPetya is a cyberweapon that disguised itself as ransomware, however, it could not be decrypted; it was only meant to destroy. On June 27, 2017, the first occurrences of NotPetya appeared in Ukrainian systems, which was the day before Ukrainian Constitution Day. This is a significant date because prior to Ukraine drawing up their own set of laws and rules, the Ukrainian people lived by the old rules of the former Soviet Union. When deployed, eighty companies were infected, and data systems were held hostage for 300 Bitcoin each. Soon, systems across Europe, including the United Kingdom, Ukraine, and Russia. Within hours, systems in Asia, South America, and the United States were victim to the growing attack that seized systems (Brumfield, 2022). In total, sixty-five countries around the globe were affected by the self-propagating worm. Unlike the typical forms of ransomware, NotPetya did not have the ability to be decrypted even though demands from the attackers stated that it would be. Once inside the system, a series of malicious activities transpire rendering the device completely unusable. The NotPetya worm was particularly dangerous because it utilized zero-day vulnerabilities that existed in Windows 7, 8, and 10 versions. This caused great alarm, as companies such as global shipping giant Mersk, pharmaceutical company Merck, and international food production and distributor Mondelez were held at a standstill with operations. The next section will discuss the three major components of NotPetya and how they operate once inside of a system (Brumfield, 2022).

Methodology

The composition of NotPetya is complex and involves multiple known vulnerabilities in the Windows servers as well as incorporating styles of previous attacks before it. This sophisticated

worm was one of the most dangerous worms in history, and enacted maximum damage to every device that it could. Cleverly disguised as ransomware, this attack infiltrated systems, dynamically replicated itself, and crippled systems beyond repair. Intricate in design, the worm utilized the three powerful and destructive tools, Petya, EternalBlue, and Mimikatz to enter systems and propagate automatically in the network. Each exploit works together to create the perfect storm of events.

Petya was a unique attack that changed the nature of how ransomware works and what it can achieve. It starts with an attacker sending someone a malicious executable file that appears harmless. Once opened, a reboot occurs, and a Windows CHKDSK screen appears. The reboot triggers installation of its own boot loader, which overwrites the affected system's Master Boot Record, then encrypts the master file table of the NTFS file system. Once encrypted, a payment demand screen is displayed requesting Bitcoins (Fruhlinger, 2017). Petya was created by Janus Cybercrime Solutions, a group of hackers with an unknown origin, but believed to be tied to Russia.

EternalBlue was a Windows zero-day exploit that was created in the United States by the National Security Agency (NSA). EternalBlue infects the Windows system and exploits the Server Message Block (SMB) v 1.0 server protocol in Window 7, Windows 2008, Windows XP, and Windows 10 on port 445 (Higgins, 2023). SMB is a file sharing protocol that allows read and write abilities to computers on the same network. Additionally, SMB allows for requests for services to be made on computers residing on the same network. Developed by the NSA's Equation Group, a collective of elite government hackers, EternalBlue exploited the SMB vulnerability and kept it in its secret collection of tools used to infiltrate enemies. Attacker would send out a malicious SMBv1 data packet to a Windows server and inject a malware

payload which would rapidly spread to other systems and devices that were in the network and contained the vulnerable software (Burgess, 2017). EternalBlue was stolen and leaked from the National Security Agency's elite hacking group The Equation Group, then shared online for anyone to use by the hacker collective going by the name of Shadow Brokers. Subsequently Microsoft, unaware of this vulnerability, released a patch to the public to mitigate the threat.

Mimikatz is a post-exploitation tool that dumps passwords from memory, as well as hashes, PINs, and Kerberos tickets (Porup, 2019). Mimikatz also enables attacks such as pass-the-hash, pass-the-ticket, and building Golden Kerberos tickets, which allow for lateral movements within a network of systems and devices. In 2011, Benjamin Delpy discovered a flaw in the WDigest of Windows authentication and exploited a vulnerability with the single sign-on functionality, which is used to harvest credentials. WDigest loads encrypted passwords into memory and the secret key needed to decrypt them; Mimikatz uses this flaw to gain the user credentials to traverse systems and devices on the network. With these three exploits, NotPetya revolutionized the way nation-states committed cyber-attacks against adversaries.

Results

NotPetya exploits several different methods to spread without human intervention, this is how it works. The original infection vector is a backdoor planted in M.E. Doc, an accounting software package that is used by many companies in Ukraine. Petya portions of the code trigger a reboot of the MBR and encrypt the system. A Windows CHKDSK screen is displayed, the reboot has encrypted the device and locked the user out of the system, and payment of 300 Bitcoin is requested. Then, NotPetya used EternalBlue and other techniques to spread to other computers

by exploiting vulnerable SMB protocols in SMBv1 servers. Next, Mimikatz was used to harvest network administration credentials in the infected machine's memory, and finally use the PsExec and WMIC tools built into Windows to remotely access other computers on the local network and infect them as well (Fruhlinger, 2017). If the company decides they want to pay for the decryption key, it is futile because NotPetya is unable to be decrypted.

The effects of NotPetya had major implications for companies and their devices infected by the worm. NotPetya first took hold of an electrical power company supplying energy to Kyiv, Ukraine. Businesses across the country suffered dire consequences, but it did not stop there. NotPetya then spread across Europe, Asia, and even back to Russia, where it originated from. Hours later, companies in North America and South America fell victim to this quickly spreading cyberweapon. In total, more than $10 billion worth of damage was reported globally (Brumfield, 2022). Before NotPetya, cybersecurity experts and researchers had different ideas of how an attack operated; they were more concerned with theories and complex security problems. With this worm, the Russians took it back to basics. No longer were researchers concerned with the idea of theft or ransom, researchers needed to be concerned with acts of political and geopolitical aggression as modern-day warfare.

Conclusion

In summary, NotPetya was a designer attack created to wreak havoc on vulnerable Windows systems. The attack serves as a stark reminder of the evolving nature of cyber threats and the devastating impact they can have on global infrastructure. The attack leveraged multiple sophisticated tools, including Petya, EternalBlue, and Mimikatz, to infiltrate and propagate

through networks, causing irreversible damage. Its rapid spread and the extensive damage it caused highlight the vulnerabilities in even the most robust systems and the importance of proactive cybersecurity measures. By disabling more than 12,000 computers and spreading to over sixty-five countries, NotPetya was a demonstration of how cyberattacks can be used as tools to engage in geopolitical aggression and commit acts of modern warfare.

Joshua Russell
CYSE 280

Works Cited

Brumfield, C. (2022, June 27). *5 Years After NotPetya: Lessons Learned*. Retrieved from www.csoonline.com: https://www.csoonline.com/article/573049/5-years-after-notpetya-lessons-learned.html

Burgess, M. (2017, June 28). *Everything You Need to Know About EternalBlue – the NSA Exploit Linked to Petya*. Retrieved from www.wired.com: https://www.wired.com/story/what-is-eternal-blue-exploit-vulnerability-patch/

Fruhlinger, J. (2017, October 17). *www.csoonline.com*. Retrieved from Petya Ransomware and NotPetya Malware: What You Need to Know Now: https://www.csoonline.com/article/563255/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

Higgins, M. (2023, April 28). *EternalBlue: What It is and How It Works*. Retrieved from www.nordvpn.com: https://nordvpn.com/blog/what-is-eternalblue/?msockid=3e85129aadab6bfd2e510317ac566a4d

Khandelwal, S. (2017, April 15). *Turns Out Microsoft Has Already Patched Exploits Leaked By Shadow Brokers*. Retrieved from www.thehackernews.com: https://thehackernews.com/2017/04/window-zero-day-patch.html

Porup, J. (2019, March 5). *What is Mimikatz? And How to Defend Against This Password Stealing Tool*. Retrieved from www.csoonline.com: https://www.csoonline.com/article/566987/what-is-mimikatz-and-how-to-defend-against-this-password-stealing-tool.html

Soon, K., & Hurley, S. (2017, June 29). *NotPetya Technical Analysis - A Triple Threat: File Encryption, MFT Encryption, Credential Theft*. Retrieved from www.crowdstrike.com: https://www.crowdstrike.com/en-us/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/

Vavra, S. (2018, January 13). *Russia Behind NotPetya Cyberattack in Ukraine, CIA Concludes*. Retrieved from www.axios.com: https://www.axios.com/2018/01/13/russia-behind-notpetya-cyberattack-in-ukraine-cia-concludes-report-1515853877

Warren, T. (2020, November 20). *Windows Turns 35: a Visual History*. Retrieved from www.theverge.com: https://www.theverge.com/2015/11/19/9759874/microsoft-windows-35-years-old-visual-history