The *NotPetya* Cybersecurity Attack & Breach

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity, Professor Dr. Joseph Kovacic

September 7, 2025

Short Research Paper #1 Instructions:

Perform research on a significant cybersecurity breach within the past ten (10) years. Use the ODU library and/or appropriate Internet resources to perform content discovery. After you have completed reading through the research materials, write a 1–3-page paper discussing the specific cybersecurity breach. The paper needs to address the following:

- What were the cybersecurity vulnerabilities?
- What threat(s) exploited the vulnerabilities?
- What were the repercussions of the incident?
- What cybersecurity measures could have been taken to mitigate the consequences or prevent the incident?

The *NotPetya* Cybersecurity Attack & Breach

Ransomware is a type of malware that blocks access to critical data and then demands a cryptocurrency payment in exchange for the decryption key to access the inaccessible data (Aidan et al., 2017). Most ransomware is called Crypto Ransomware (e.g., Petya): its primary goal is to collect money from unsuspecting and unprepared victims (Kara et al., 2022; McDonald et al., 2022). For Windows operating systems, the malware encrypts the Master File Table (MFT), making all files inaccessible, and then demands a ransom for the decryption key. Without the decryption keys, it is nearly impossible for victims to recover their encrypted data without costing them an incredible amount of time and money to restore systems to their original states. However, there is another type called Locker Ransomware (e.g., NotPetya). Its primary goal is to eradicate data by encrypting all of it, then deleting the decryption keys and making the encryption process "irreversible" (Kara et al., 2022; McDonald et al., 2022). It is a pseudo form of "wiping" or "destroying" data, similar to a Denial-of-Service Attack. Typically, state actors of nations employ the Locker Ransomware approach to sow chaos and disarray among their enemies, disrupting entire economies and incurring millions of dollars in damages and restoration costs for victim nations. In the case of the 2017 NotPetya attack, this is what happened between Russia, Ukraine, and eventually the world (Rhysider, 2019).

NotPetya Attack — Tuesday, June 27th, 2017

The NotPetya Locker ransomware infection began when attackers sent spam and phishing emails to potential targets. Once the targets opened those emails and clicked on the included malicious links and URLs, the attackers were able to infiltrate and commandeer the update server for a popular Ukrainian accounting software program (McDonald et al., 2022). After their initial infiltration, the attackers created a backdoor to the accounting software and pushed updates to all

users via the update server. By exploiting that vulnerability using the tool called Mimikatz and the EternalBlue exploit, the attackers used a worm to spread the NotPetya Locker ransomware from the initial targets to other machines on the victims' networks.

NotPetya ransomware works first by modifying and encrypting the Master Boot Record (MBR) of a Windows operating system (OS), not just the MFT (Aidan et al., 2017; McDonald et al., 2022). It then performs a full-disk encryption, making recovery impossible. Once finished, the ransomware forces the system to crash and reboot itself. Upon restarting, the modified MBR will prevent the Windows OS from booting correctly, and an ASCII message will display, soliciting a ransom payable in Bitcoin in exchange for the decryption key. However, unlike its predecessor, the Petya Crypto ransomware, the attackers' ransom email server was quickly shut down, removing the ability to recover the decryption keys, even if a ransom was paid. Without the decryption keys and access to the servers, the domain controllers operating the Windows Server were unable to render their services to employees and customers (McDonald et al., 2022).

What Tools and Cybersecurity Vulnerabilities did the Hackers Use?

The NotPetya cyberattack consisted of several components: the tool called Mimikatz, and the EternalBlue exploit, and a malicious worm that contained ransomware. First, Mimikatz is an open-source tool to scan computer systems and networks for vulnerabilities in Microsoft's Authentication protocols: it attempts to gain access to login credentials stored in the memory (sometimes in plaintext) by extracting the usernames and passwords or even their hashes or tokens to gain unauthorized access to the target's computer and network (Rhysider, 2019).

Second, the EternalBlue exploit was a vulnerability that targeted the Microsoft Windows Server Message Block (SMB) protocol, enabling computers to share data. The exploit provides attackers the ability to execute arbitrary code without the need for authentication, thereby

bypassing any/all login credentials to gain direct access to workstations and networks. If the Mimikatz tool cannot find or access any login credentials at the front-end of the cyberattack, then the cybercriminals would use the EternalBlue exploit to bypass any and/or all required authentication to gain access to systems to spread the ransomware. Afterward, the cybercriminals will reinitiate Mimikatz to extract all of their victims' login credentials, sending the information to them for later use. Lastly, the malicious worm used in the attack was a self-replicating program that could spread and infect computer networks without requiring further user intervention or consent after the initial infiltration of the NotPetya attack. It carried and installed the Locker Ransomware to run on the infected networks and machines.

Although Microsoft had provided a patch for the EternalBlue exploit and vulnerability in months prior to help resolve similar exploits spawned from the recent 2017 WannaCry attack, many companies, including the Said Ukrainian accounting software company, did not promptly patch their systems (McDonald et al., 2022). Once an unsuspected target clicked/downloaded the malicious file in the phishing emails, the attackers would use the Windows MS17-10 vulnerability and the remote access feature of Windows Management Instrumentation (WMI) to spread within the network to infect other neighboring computer systems. The ransomware writes its code to the MBR and initiates a system reload. While rebooting, the computer displays a "repairing file system" screen to the user, giving the impression that the system is naturally fixing itself after the unexpected system crash; however, the NotPetya ransomware is encrypting the Master Boot Record in the background, and then the entire hard drive. Lastly, if the system shuts down for any reason during the encryption process, the encryption process will resume from where it left off once the system is powered back on.

Repercussions of the NotPetya Cyberattack

Authorities later discovered that Russia sponsored the NotPetya cyberattack. Russia's primary goal was to physically occupy and grab more Ukrainian land using Russian troops, a climax of bloody history, tensions, and attacks since World War II between the two nations. The NotPetya cyberattack initially targeted Ukraine by completely shutting down and rendering Ukraine's cyber infrastructure unusable and useless. Ukrainian organizations from all different shapes, sizes, and industries were negatively impacted and experienced full-day nationwide system shutdowns, with employees and customers completely locked out of their accounts. Victims include post offices, hospitals, utility companies, and many financial institutions (i.e., Oschadbank). However, the ransomware also preyed upon and attacked multinational companies affiliated with and connected to Ukrainian-based companies' networks. By the end of 2017, companies like Merck & Co. and FedEx lost millions, if not billions, in U.S. dollars when filing insurance claims (Rhysider, 2019; McDonald et al., 2022). In conclusion, the malicious virus impacted numerous organizations and industries across the global economy, including finance, logistics and transportation, medical services, manufacturing, and the governments of various nations.

Final Recommendations & Cybersecurity Mitigation Actions

In general, and particularly the NotPetya attack, there are several proactive measures people can take to prevent or help mitigate the consequences of a successful ransomware cyberattack (Aidan et al., 2017; Kara et al., 2022; Sandbu, 2022; Lochstampfor, 2025b). First, IT administrators and household users must update and patch their Windows OS promptly. Second, people should create a routine of regularly backing up their critical data. In fact, it is best to schedule these routine backups during non-working hours and onto separate or offline devices, thereby reinforcing network segmentation and adhering to the 3-2-1 backup strategy.

Third, people should annually review how ransomware attacks target potential victims by researching reliable authority sources and learn how to spot potential ransomware threats. That includes avoiding opening attachments, URL links, or downloading files from unsolicited or unknown sources that you, as the user, do not or cannot validate as a credible source. Additionally, maintaining updated Anti-Virus software (AV) is crucial. Lastly, enabling automated patches for operating systems and web browsers to avoid untimely delays or users/IT administrators forgetting to do so manually.

References

Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2017). Comprehensive Survey on Petya Ransomware Attack. In *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)* (pp. 122-125). IEEE. https://ieeexplore.ieee.org/document/8520323/

Jack, Rhysider (Host). (2019, October 8). NotPetya (No. 54) [Audio podcast episode]. In DarkNet Diaries. https://darknetdiaries.com/episode/54

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for Windows based ransomware attacks. Expert Systems With Applications, 190, 116198. https://www.sciencedirect.com/science/article/pii/S0957417421015141

Lochstampfor, C., Jr. (2025a, May 26). Darknet diaries: The NotPetya attack (Unpublished manuscript). Department of Cybersecurity, Old Dominion University, CYSE 280 - Windows Systems Management and Security, Professor Malik A. Gladden. https://sites.wp.odu.edu/locky/2025/05/29/darknet-diaries-notpetya-attack/

Lochstampfor, C., Jr. (2025b, July 31). Ransomware mitigation strategies for Windows systems: Securing servers and endpoints (Unpublished manuscript). Department of Cybersecurity, Old Dominion University, CYSE 280 - Windows Systems Management and Security. https://sites.wp.odu.edu/locky/cyse-280/

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). Ransomware: Analysing the impact on Windows Active Directory domain services. Sensors, 22(3), 953. https://www.researchgate.net/publication/358119298_Ransomware_Analysing_the_Impact_on_Windows_Active_Directory_Domain_Services

Sandbu, M. (2022). Windows ransomware detection and protection. Packt Publishing.