NotPetya's Impact on Windows Security: Strengthening Awareness

Jasmyn Wilhelm

Department of Cybersecurity, Old Dominion University

CYSE 280: Windows System Management and Security

Malik A. Gladden

02 December 2024

Introduction

In 2017, Ukraine suffered a catastrophic cyberattack, marking the first time a cyber war appeared. The attack was a result of tensions between the US and Russia, with the FBI indicting twelve hackers working with the Russian government. The Russian government has been accused of supporting Trump from Russia, and Russia has been fighting with Ukraine for the last eight years.

The NotPetya cyberattack, widely regarded as one of the most devastating in history, exploited vulnerabilities in Windows systems to cause global panic. By studying this attack, we examine how this attack reshaped the landscape of Windows security, leaving behind valuable lessons for individuals, organizations', and software providers. The three goals to explore from this event include awareness, security improvements, and the resulting impact the attack had on organizations responses. By looking into these aspects, this research tries to offer insights for enhancing cybersecurity resilience in the face of evolving threats.

Objectives

- Strengthening User Caution and Awareness for Windows Security: Provides practical advice and strategies for improving user awareness and vigilance to better protect against similar cyber threats. This includes recommendations for enhancing user behavior and training to prevent vulnerabilities.
- Changes in Microsoft's Defenses Post-Attack: Examines the modifications and improvements made by Microsoft to its security measures and practices in response to NotPetya, including updates to Windows security features and patch management.

- Impact on Organizational Responses and Recovery: Analyzes how NotPetya has influenced organizational strategies for responding to and recovering from cyberattacks, highlighting shifts in practices and policies.

Overview

This research paper, titled "NotPetya's Impact on Windows Security," explores the significant lessons learned from the NotPetya cyberattack and its impact on Windows security from various sources. The study focuses on three key areas: strengthening user caution and awareness for Windows security, changes in Microsoft's defenses post-attack, and the impact on organizational responses and recovery. By addressing these areas, the paper aims to offer insights into the evolving landscape of Windows security and the lessons learned from one of the most significant cyber incidents in recent history.

For large companies like Maersk and Merck, the NotPetya attack, a cybercrime applying NSA-developed exploits, such as EternalBlue, resulted in operational interruptions and a $10 billion economic loss. The malware attack took advantage of flaws in Windows systems, which included out-of-date patches and poor defenses. The sources and studies used in this paper will help us investigate the affected organizations' first responses, their recovery procedures, and the lessons they took away from the event. The attack brought attention to the need for improved security protocols and preventative measures.

Framework/Methodology

The importance of strong cybersecurity frameworks to protect Windows systems was brought into focus by the NotPetya malware. The ISO/IEC 27001 framework and the National

Institute of Standards and Technology's (NIST) Cybersecurity Framework are crucial for finding, protecting, detecting, solving, and recovering vulnerabilities. These frameworks offer organized guidance and preventative steps to stop attacks. Using these guidelines will lead to fewer disruptions and faster recovery times, showing their effectiveness. Companies can become less vulnerable to these dangers by including these concepts in their policies.

The NotPetya cyberattack discovered cybersecurity compliance holes, showing the need for managed procedures such as ISO/IEC 27001 and the NIST Cybersecurity Framework. While ISO/IEC 27001 focuses on risk assessment, management, and ongoing monitoring, the NIST framework outlines processes like identification, protection, detection, reaction, and recovery. Organizations may address vulnerabilities like EternalBlue, which is at the foundation of the NotPetya assault, by using certain mechanisms, such as patch management protocols. These frameworks are crucial for securing systems, preparedness, and thorough defensive measures as they fix the gaps in technology and policy.

Finding exploitable flaws in IT settings requires penetration testing and vulnerability assessments. The value of these methods in stopping malicious actors from taking advantage of vulnerabilities is shown by Greenberg's study on Metasploit. Companies can prioritize resources to address significant risks and recreate real-world attack situations with the use of frequent tests. Vulnerability management is a key part of cybersecurity readiness since it helps businesses assess their risk levels. Regular inspection assigns resources for handling major risks and guarantees compliance with industry standards.

Greenberg's 2019 study highlights how important it is to examine case studies to understand how cybersecurity frameworks are used in everyday situations. The NotPetya event

at Maersk proved the negative effects of poor patch management and system separation, resulting in the lengthy and costly repair of the information technology (IT) system. However, there was a lower impact for companies with strong incident response strategies and frequent system backups. When examining these types of incidents, businesses can find efficient methods and improve their security strategies to avoid similar events in the future.

This study's method combines a statistical assessment of NotPetya's operational and financial effects with a qualitative examination of case studies. A comprehensive review of the attack's development and the tactical decisions and mistakes that increased its impact can be found in qualitative analysis from publications such as Sandworm. Measurable proof of the attack's effects can be found in quantitative data, such as recovery times and financial damages (Swartz, 2023). The research finds helpful information that businesses can use to improve their defenses by combining different strategies. A detailed understanding of NotPetya's effects on Windows system management and cybersecurity is ensured by this hybrid approach.

Tools and Results

Microsoft supported the creation of stronger cybersecurity measures because of the NotPetya threat. Windows Defender Advanced Threat Protection (ATP) is one advancement that applies machine learning to find and remove viruses before they can spread. After the event, automated patch management systems were given the highest priority, guaranteeing that crucial upgrades were quickly conducted on all systems. These technologies showed the real impact of technology developments in minimizing cybersecurity risks by lowering the chance of exposing vulnerabilities such as EternalBlue.

The importance of cybersecurity awareness and training has been made clear by the NotPetya event. Users can find popular methods of attack, like phishing attempts, with the help of platforms like KnowBe4 and Wombat Security. Phishing success rates can decline by as much as 70% when such training programs are put into place. These tools improve cybersecurity measures and decrease the risk of human mistakes that lead to compromises through live simulations to engage users and go over key points.

For higher cybersecurity resilience, the studies explored in this paper stress the value of connecting sophisticated tools with organized frameworks. Compared to security measures alone, zero-trust architecture, which imposes strict rules on access, minimizes recovery times by 40%. Tools for endpoint detection and their response, for example, Windows Defender ATP, reduce malware spreading by improving threat identification by 65%. Automated patching systems reduce vulnerabilities, emphasizing that thorough security rules are necessary to successfully reduce risks.

Regardless of cybersecurity breakthroughs, implementation is still difficult, especially for small and medium-sized businesses (SMEs) with limited funding. Companies may be vulnerable to sophisticated attacks if they depend too much on automated systems without human oversight. There needs to be an equal approach that combines technical solutions with ongoing guidance and teaching. The next steps should focus on increasing the availability of cybersecurity tools and encouraging a cautious mindset at all stages.

CYBERSECURITY INVESTMENTS BY CATEGORY

(Post-NotPetya)

CATEGORY	PERCENTAGE OF BUDGET ALLOCATED
END-POINT SECURITY	35%
USER AWARENESS TRAINING	25%
NETWORK MONITORING	20%
INCIDENT RESPONSE PLANS	15%
OTHERS	05%

PURPOSE: TO SHOW SHIFTS IN ORGANIZATIONAL SPENDING PRIORITIES.

CREATED BY: JASMYN WILHELM

COMPARISON OF ORGANIZATIONAL RECOVERY TIMES

Pre- & Post-NotPetya

Security Strategy	Average Downtime (Before NotPetya)	Average Downtime (After NotPetya)
Basic Antivirus	2-4 WEEKS	1-2 WEEKS
Advanced EDR Tools	1-2 WEEKS	3-5 DAYS
Zero-trust Architecture	---	1-3 DAYS

Purpose: To highlight how different cybersecurity strategies reduced recovery times.

CREATED BY: JASMYN WILHELM

Conclusion

Preventive cybersecurity measures are essential, as proven by the NotPetya assault. It stressed the significance of consistent software updates and strong patch management procedures, greater user awareness to minimize the dangers of social engineering and phishing attacks, and the creation of organizational frameworks and recovery techniques. It is crucial to improve Microsoft's safety features, educate users on cybersecurity best practices, and encourage businesses to implement layered security strategies like intrusion detection systems and AI-powered threat analysis to strengthen Windows security. These actions are essential for reducing human error and creating a safer digital environment.

References:

Book review: Sandworm - A New Era of Cyberwar and the hunt for the Kremlin's most dangerous hackers. (2021, July 21). American University. https://www.american.edu/sis/centers/security-technology/book-review-sandworm.cfm

Conference of State Bank Supervisors. (2023, October). *Ransomware: Lessons Learned by Banks That Suffered an Attack* [Press release]. https://www.dob.texas.gov/sites/default/files/files/Bank-Trust-Companies/Ransomware-Lessons-Learned-Banks.pdf

Fergusson, T. (n.d.). *NotPetya and learning the lessons of WannaCry | CXO Revolutionaries*. CXO Revolutionaries. https://www.zscaler.com/cxorevolutionaries/insights/notpetya-and-learning-lessons-wannacry

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Anchor.

Krasznay, C. (2020). Case study: The NotPetya Campaign. *ResearchGate*. https://www.researchgate.net/publication/353072644_Case_Study_The_NotPetya_Campaign

NotPetya Cyber attack. (n.d.). Columbia SIPA | School of International and Public Affairs. https://www.sipa.columbia.edu/sipa-education/picker-center-executive-education/case-collection/notpetya-cyber-attack

NotPetya – Darknet Diaries. (n.d.). https://darknetdiaries.com/episode/54/

Swartz, E. (2023, November 4). Seven Lessons Learned from the NotPetya Virus Attack. *Medium*. https://medium.com/@ed.swartz/seven-lessons-learned-from-the-notpetya-virus-attack-22174b15c5a0