Readme File for Teachers:  
Case Study on WannaCry Ransomware

**Abstract:**In this case study, students will look into the detail of the WannaCry Ransomware in 2017. Students will learn how the attack take place from the beginning to the end. During the process of case analysis, a list of security topics reflecting different aspects of the breach is introduced. Through guided in-class discussion and hands-on lab assignments, student learning in lecture will be reinforced.

**Target audience:**Undergraduate, Graduate

**Objectives:**

* Describe Ransomware attacks
* Explain zero-day vulnerabilities used in WannaCry ransomware
* List common defense mechanisms against ransomware attacks

**Keywords:**Ransomware, Zero-day vulnerabilities, Malware

**Description:**This case study discusses the widespread cyberattack that exploited vulnerabilities in the Windows SMB protocol to propagate across global networks. Unleashed on May 12, 2017, WannaCry affected over 200,000 machines in 150 countries, encrypting users' files and demanding ransom payments. The ransomware primarily utilized two exploits, EternalBlue and DoublePulsar, developed by the NSA and leaked by the Shadow Brokers. These exploits allowed WannaCry to spread rapidly by enabling remote code execution and malware delivery on unpatched systems. The presentation covers the technical aspects of the attack, including the specific vulnerabilities exploited, and highlights significant impacts on organizations like the NHS, which faced severe operational disruptions and had to divert emergency services.

In addition to outlining the attack's progression and impact, the presentation emphasizes mitigation techniques and the importance of cybersecurity measures. It discusses how a security researcher inadvertently activated a kill switch by registering a domain embedded in the WannaCry code, which helped prevent further infections. This event underscores the critical role of threat intelligence and rapid response in combating ransomware. The presentation concludes with lessons learned, advocating for regular system patching, disabling vulnerable services, and employee training to prevent future ransomware attacks. It also stresses the importance of comprehensive incident response planning and the need for organizations to improve their resilience against such sophisticated cyber threats.

**Cybersecurity topics:**Ransomware, Zero-day vulnerabilities, Malware

**Teaching resources for the case:**A study package with the following materials was developed for the case:  
a) A PowerPoint presentation explaining technical details and lessons learned for the case: used by the instructor to guide the classroom discussion.   
b) A list of discussion questions: It is suggested to ask students to finish the discussion questions before attending the in-class discussion.  
c) A video tutorial introducing the case: For instructors or online students.   
The video can also be used before the in-class discussion. Students will be asked to finish the video before attending the in-class discussion.

**Additional third-party resources for the case:**

* D. Bisson, “WannaCryptor Ransomware Strikes NHS Hospitals, Telefonica, and Others,” The State of Security, 24-May-2017. [Online]. Available: https://www.tripwire.com/state-of-security/latest-security-news/wannacryptor-ransomware-strikes-nhs-hospitals-telefonica-and-others/.
* D. Bisson, “3 NSA Exploits Rewritten to Affect All Windows OSes Since Windows 2000,” The State of Security, 02-Feb-2018. [Online]. Available: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/three-leaked-nsa-exploits-rewritten-affect-windows-oses-since-windows-2000/.
* M. Burgess, “Everything you need to know about EternalBlue – the NSA exploit linked to Petya,” WIRED, 29-Jun-2017. [Online]. Available: http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch.
* K. Collins, “The hackers behind the WannaCry ransomware attack have finally cashed out,” Quartz, 07-Aug-2017. [Online]. Available: https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/.
* A. Singh, “WannaCry Ransomware Analysis: Lateral Movement Propagation,” *Acalvio*, 04-Apr-2018. [Online]. Available: https://www.acalvio.com/wannacry-ransomware-analysis-lateral-movement-propagation/.

**Language:**English

**Date created:**   
May 1, 2023

**Last update:**   
May 1, 2024