Cybersecurity Breach Analysis: The WannaCry Ransomware Attack (2017)

Rebecca Hight

Old Dominion University

CYSE 300

September 8, 2024

Cybersecurity Breach Analysis: The WannaCry Ransomware Attack (2017)

One of the most renowned cybersecurity breaches that occurred recently was the WannaCry ransomware attack in 2017. It came at scale and at pace, impacting critical infrastructure and key service sectors in 150 countries. More than 200,000 computers were affected, and many organizations in the fields of healthcare manufacturing and governmental sections were put to a halt (Mohurle and Patil, 2017). The base of the event was a weakness in Microsoft Windows operating systems, more specifically, CVE-2017-0144 within SMB, which provided opportunities to execute code remotely on unpatched systems. Even though a patch was released for this vulnerability in March 2017, WannaCry attacked numerous organizations that had not updated their systems. Many systems were left exposed due to delayed patching and overall carelessness in ensuring the latest security releases are installed, showing that even when security updates are issued, they may remain unknown to large organizations.

The cybercriminals behind WannaCry employed sophisticated methods, leveraging the EternalBlue exploit, which was reportedly developed by the U.S. National Security Agency (NSA) but leaked by the hacker group Shadow Brokers. Upon entering a system, WannaCry encrypted vital files and sought ransom in Bitcoin to provide decryption codes. The worm component of the malware allowed it to propagate itself from one compromised system to others on its own. This made the attack not only proactive but also highly contagious to systems with similar weaknesses. The spread of ransomware in numerous regions within a short span was made possible by outdated systems and insufficient security measures, thus exposing how cyber-attacks thrive due to the lack of internal change (Hsiao and Kao, 2018). This made the effects of the attack even worse due to the fact that no particular sector was spared in the attack.

The effects of WannaCry were wide-ranging and catastrophic. This attack impacted the U.K. healthcare sector most severely, with the National Health Service (NHS) losing tens of thousands of appointments and surgeries and steering emergency patients away from hospitals due to unusable systems. Sometimes, the records could not be accessed by the healthcare professionals, implying that there were severe delays in treatments. In the global context, the disruptions were similar across industries. Production lines in manufacturing plants were affected, and governments all over the world reported delays in the delivery of public services. The economic cost of the attack reached the level of billions of dollars in total, considering the total amounts involved in reimbursements and ransoms, as well as lost working days and recovery operations. In addition to the financial repercussions, organizations that were targeted by the attack suffered reputational losses as the breach highlighted their inability to protect their systems from threats (Akbanov et al., 2019).

Reflecting on the WannaCry attack, it is possible to state that most of the negative outcomes might have been prevented or their impact lessened with proper cybersecurity measures. Among these practices, the most significant is the timely release of security patches. Microsoft had released the update for SMB vulnerabilities months prior to the attack, but most organizations had not applied it or had done it at a very slow rate. This highlights the need for the cultivation of a culture of cybersecurity, which means swift patching of systems and applying updates. Moreover, organizations could have prevented the ransomware from affecting everyone in the organization through the use of advanced threat detection technologies, including IDS and IPS, to alert before the ransomware spread within organizational systems (Hsiao and Kao, 2018). Network segmentation, which is a process of partitioning an organization's network so it can be easily isolated in case of an attack, would also limit the spread of malware to other systems. In

addition, regular and segregated copies of the data that are vital for the uninterrupted functioning of the organization might have prevented the entities from restoring their systems within the timeframe and without paying the ransom.

In conclusion, the WannaCry ransomware attack is a good example of why organizations need to pay close attention to their cybersecurity. It targeted certain weaknesses, some of which are well-documented and could have been avoided if only the vulnerabilities that are well-known had been addressed using security fixes. It was WannaCry that shed light on the global consequences of inadequate, or even non-existent, safety precautions. This case is a clear example of why organizations need to design better security measures to prevent such risks in the future. The key takeaway from the WannaCry attack is clear. The protection of cyberspace requires greater consideration within every organization. There is a risk of losing potential customers' money and the organizations's reputation, and the absence of proper security measures does not only drain organizations' cash but even paralyzes their operations. Such risks can never be totally eliminated, however, organizations require improving their security levels in a continuous and efficient manner while at the same time keeping an eye on possible risks.

References

Akbanov, M., Vassilakis, V.G. and Logothetis, M.D., 2019. WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *Journal of Telecommunications and Information Technology*, (1), pp.113-124.

Hsiao, S.C. and Kao, D.Y., 2018, February. The static analysis of WannaCry ransomware. In *2018 20th international conference on advanced communication technology (ICACT)* (pp. 153-158). IEEE.

Mohurle, S. and Patil, M., 2017. A brief study of wannacry threat: Ransomware attack 2017. *International journal of advanced research in computer science*, *8*(5), pp.1938-1940.