Ransomware Worm WannaCry

Micah L Wieburg

School Of Computer Information Sciences

University of the Cumberlands

MSCE-534: Principles of Cybersecurity

Dr. Eric Harmon

September 24 2023

Fall 2023

Ransomware Worm WannaCry

The WannaCry ransomware is regarded as one of the most financially damaging and impactful examples of ransomware. Primarily, this is due to the number of machines that became infected by the ransomware and the financial costs associated with its spread. The primary targets of the WannaCry ransomware included large sectors and aided in establishing a new trend that involved holding critical infrastructure systems for ransom. Due to the worm component of WannaCry, it was able to spread rapidly during the infection phase and reach the level of devastation that left several systems unusable. Moreover, this outbreak led to new defensive techniques and questions surrounding known vulnerabilities and the impact they can have when exploited.

Hutchins and SMB

Hutchins identified the connection between the WannaCry ransomware and the SMB port by utilizing a virtual environment to analyze it and discovered that the behavior matched a previously known SMB exploit. Hutchins (2017) stated that the WannaCry sample code running in the virtual environment began connecting to IP addresses on port 445, which is used by SMB, and was able to recall a recent ShadowBroker leak of National Security Agency (NSA) exploits that listed an SMB exploit. This knowledge of the SMB exploit formulated the strategy for Hutchins to stop the ransomware from spreading further. Consequently, this incident serves as a viable example of the importance of learning known vulnerabilities.

Hutchins Recommendations for WannaCry outbreak

Hutchins provided many recommendations that tended to fall into the standard procedures he would perform for stopping the spread of malware. According to Hutchins (2017), the first step

was to register the unregistered domain that the ransomware was querying and to sinkhole the traffic, second to reverse engineer the ransomware code to find vulnerabilities that would allow him and his cohorts to hijack the ransomware and third to patch any software that needs to be patched to prevent newer versions of the malware from taking advantage of the same exploit. These recommendations predict that remaining current on software patches can play a vital role in thwarting exploits of known vulnerabilities and fostering a more secure system. Therefore, remaining knowledgeable of any identified vulnerabilities is critical for security professionals.

Awareness of identified vulnerabilities

Remaining aware of identified vulnerabilities is critical for security professionals as these vulnerabilities can be devastating for organizations, leading to financial losses and even the loss of human life if an exploit of the vulnerability is performed in a specific scenario. Lightbody et al. (2023) highlight an onboard software vulnerability of the Jeep SUV discovered by a team from IBM, which showed that exploiting the vulnerability would give attackers remote control of the vehicle's speed and steering, ultimately leading to the vehicle driving off the road and potentially causing fatal accidents. This example supports the criticality of security professionals remaining knowledgeable of known vulnerabilities to prevent their impact. Additionally, understanding attempted breaches or attacks is vital for security professionals.

Studying attempted breaches

Studying attempted breaches allows a security professional to gain insight into hackers' thought processes and tactics to launch their attacks. Lee & Wogan (2018) presented a survey of 126 companies operating in the maritime sector and discovered that 47 percent of the large companies had

acknowledged an attempted breach of their system compared to just 3 percent of small companies in the maritime sector. These survey findings predict that hackers are targeting larger systems in the maritime sector, making it beneficial for security professionals to be aware of this trend. Nevertheless, it is also beneficial to study successful breaches.

Studying successful breaches

By studying successful breaches, security professionals can better understand the actions performed by hackers and formulate countermeasures against them. According to Shu et al. (2017), perpetrators of the 2013 target breach were able to capture sensitive information due to a lack of segmentation between normal network portions and sensitive assets. The discovery of the network fallacies of this data breach creates a valuable learning point for professionals to create more secure systems in the future. Moreover, the learning opportunities associated with studying successful breach attempts are crucial for developing improved security procedures.

Conclusion

The relevancy of the age of the breach or attempted breach is established by the benefits and examples highlighted in the literature. Studying attempts and successes of breaches provides an avenue for security professionals to remain knowledgeable and innovative in their countermeasure attempts. Remaining knowledgeable on identified vulnerabilities gives professionals a foundation to draw from when investigating breaches and ransomware attacks. The actions performed by Hutchins during the WannaCry ransomware attack are a supporting example, as knowledge of the SMB vulnerability aided in creating the path to solving the attack.

References

Hutchins, M. (2017). How to accidentally stop a global cyber attacks – malwaretech. Retrieved September 19, 2023, from https://malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

Lee, A. R., & Wogan, H. P. (2018). All at sea: the modern seascape of cybersecurity threats of the maritime industry. *OCEANS 2018 MTS/IEEE Charleston*, 1–8. https://doi.org/10.1109/OCEANS.2018.8604554

Lightbody, D., Ngo, D.-M., Temko, A., Murphy, C. C., & Popovici, E. (2023). Attacks on iot: side-channel power acquisition framework for intrusion detection. *Future Internet*, *15*(5), 187. https://doi.org/10.3390/fi15050187

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the target: an analysis of target data breach and lessons learned. https://doi.org/10.48550/arXiv.1701.04940