WannaCry, What Went Wrong, and How Cyber Analysts Can Learn From It.

Joshua A. Morton

CYSE 300

Old Dominion University

In May of 2017, thousands of computers all over the world had been infected with a ransomware virus that had shut down hundreds of secure systems and cost over four billion dollars in damages worldwide. The virus was known as WannaCry and even in 2023 is known as one of the most influential security attacks of all time as it infected pivotal systems such as those of universities, governmental offices, and private businesses. One of the more important systems to be attacked by WannaCry was that of the United Kingdom's National Health Service which had been completely shut down. But how did this attack happen, how could it have been avoided, and most importantly what can cybersecurity experts learn from the consequences of the attack?

Firstly, it must be understood what WannaCry was and what security vulnerabilities the ransomware worm exploited to get into sensitive data systems such as the NHS. WannaCry was created as a computer worm meaning that when it is allowed access to a system it will unpack certain programs that lock windows operating systems and force the user to either pay a bitcoin fee or risk having all of their data deleted. WannaCry was so effective because it used the NSA's EternalBlue Windows exploit, which had been stolen and leaked to the public, which used a fault in older windows operating systems to run programs without being detected. The EternalBlue aspect of the worm is what puts a spotlight on security vulnerabilities that many affected organizations had, in that many of the operating systems housing the private data were still using older versions of certain operating systems like Windows 7 and Windows XP that hadn't been patched to prevent the exploit despite microsoft releasing patches and advising companies to apply them. This highlights the fact that companies must invest in upgrading their systems to prevent future attacks as many attacks use vulnerabilities posed by older operating systems and it comes to show that paying a great amount in advance for security will prove better when compared to losing thousands of dollars in data in the future.

WannaCry had a resounding impact on organizations such as the NHS because it was able to force itself onto thousands of computers and systems based on the misuse of one computer. For the NHS, the British healthcare system, WannaCry infected computers containing patient data and appointment schedules leading to the canceling of at least 6,900 appointments that had been vital to patients in waiting. Many affected by the worm also gave into demands and ended up paying the cyber criminals known as Lazarus Group, a supposed North Korean tied hacker group, a total of 51 bitcoin or $130,634 dollars in 2017, and those who didn't give in reported a global total loss of about 4 billion dollars. In Conclusion, Many different factors seem to be at fault in the effectiveness of the WannaCry ransomware attack but the true lesson learned for cybersecurity officials today is that of investing in the updating of systems to prevent outdated system attacks that benefit from unpatched systems and that many organizations in the world must inquire about following certain data recovery frameworks, such as NIST, to prevent the scare of lost data to ransomware.

Works Cited

(2017). *Bolstering the Government's Cybersecurity: Lessons Learned from Wannacry: Joint Hearing before the Subcommittee on Oversight & Subcommittee on Research and Technology, Committee on Science,*

Space, and Technology, House of Representatives, One Hundred Fifteenth Congress, First Session . .

Ehrenfeld, J. M. (2017). WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *Journal of Medical Systems, 41*(7), 1. https://doi.org/10.1007/s10916-017-0752-1

Ghafur, S., Kristensen, S. R., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *Npj Digital Medicine*, *2*(1). https://doi.org/10.1038/s41746-019-0161-6

Mayor, S. (2018). Sixty seconds on . . . the WannaCry cyberattack. *BMJ: British Medical Journal*, *361*. https://www.jstor.org/stable/26960680

Park, J. (2021). THE LAZARUS GROUP: THE CYBERCRIME SYNDICATE FINANCING THE NORTH KOREA STATE. *Harvard International Review, 42*(2), 34-39. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/lazarus-group-cybercrime-syndicate-financing/docview/2581891566/se-2