WannaCry

Easton Jarboe

ODU

CYSE 300

Dr. Kovacic

1/23/24

Microsoft, one of the most influential tech companies around the world, was taken by surprise in the year 2017. WannaCry is a form of malware that took advantage of a bug in Microsoft systems. “As for WannaCry ransomware attack, it exploits the MS17-010 vulnerability to inject the initial binary “launcher.dll” through the Eternalblue exploit and Doublepulsar backdoor (S. -C. Hsiao, 2018).” This Eternalblue exploit led to a catastrophic event of a hacker group taking control of computers in over 150 countries (S. -C. Hsiao, 2018). Eternalblue was developed by the NSA to gather intelligence. Sometime after the NSA made Eternalblue a now infamous hacker group called Shadow Brokers got their hands on it.

Under ordinary circumstances a ransomware attack would only go after businesses that have a lot of money and few resources. However, the Shadow Brokers from Russia had a different idea: they hit the world where it would hurt most. The Shadow Brokers atack places like UK hospitals and Japan’s Honda factories (Q. Chen, 2017). In a sense what the Shadow Brokers did was smart people's lives were on the line so the hospital almost had no choice but to pay. The NSA got wind of the Shadow Brokers obtaining the Eternalblue exploit and they warned Microsoft. There were little to no repercussions for the Shadow Brokers as they are from Russia it was hard for the USA to pursue them.

While Microsoft pushed an update many people neglected to get the update. Their update would have heavily mitigated damages. That is understandable; most people dread updating devices as they can not complete tasks they deem necessary. Not only does this make Microsoft not liable but it helped to save a lot of businesses and mitigate the damages. One of the most glaring issues found is that 63 different Antivirus softwares could not detect Wannacry after the fact (Q. Chen, 17). Not only was Wannacry a fatal blow to businesses it attacked, but also the antivirus companies who neglected to patch their software.

Overall Wannacry is a ransomware for the history books. It not only took down multiple enterprises after Microsoft was warned, but also hospitals too. The underlying lesson learned while researching this case was the NSA has many secret tools that could greatly hurt the public and they are just as if not scarier than the Shadow Brokers. Wannacry was a horrible thing to have happened to the world, but cyber professionals all over the world can learn from this and grow to defend from similar attacks.

References

S. -C. Hsiao and D. -Y. Kao, "The static analysis of WannaCry ransomware," *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon, Korea (South), 2018, pp. 153-158, doi: 10.23919/ICACT.2018.8323680.

Q. Chen and R. A. Bridges, "Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware," *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Cancun, Mexico, 2017, pp. 454-460, doi: 10.1109/ICMLA.2017.0-119.