WannaCry Ransomware

Larry Le

Department of Cybersecurity, Old Dominion University

CS 462

Nasreen Arif

November 21, 2024

WannaCry Ransomware

In the paper I will explain in detail what happened during the wannacry ransomware attack. I will be focusing on the vulnerabilities that were present, the actual breach and what events led up to this. Finally I will discuss what we can learn from this previous attack and how this affects today's society.

How It All Started

Back in 2016 a group called shadow brokers was able to get a hold of some of NSA's secret exploits. Their goal was trying to sell the exploits to the highest bidder but after they didn't get the bids or action they thought they deserved, shadow brokers just decided to release all the exploits they collected. According to Matt Burgess, "After the failed Shadow Brokers' auction, the organization's most significant data release came in April 2017. The group published details of hacking tools, alleged to be from the CIA, that are said to allow spying on money transfers. It was said the vulnerabilities published could create problems in the Microsoft Windows version of the SWIFT banking system. The system is used by multiple banks around the world. It was believed the exploits could still be used against Microsoft problems".

How Does It Work

People that didn't take the shadow brokers seriously learned to regret that decision. One of the exploits that was released was called Eternal Blue. According to Sentinel One, " Eternalblue are a family of critical vulnerabilities in Microsoft SMBv1 server used in Windows 7, Windows Server 2008, Windows XP and even Windows 10 running on port 445. Eternalblue itself concerns CVE-2017-0144, a flaw that allows remote attackers to execute arbitrary code on a target system by sending specially

crafted messages to the SMBv1 server". This was very lucitive for the wannacry ransomware. The eternal blue exploit was considered a zero day exploit so if your system had an older Microsoft server message block protocol then they would be at risk of getting infected. What is even scarier is that after being infected they would try and target other hosts on your local network and from there it spreads. Microsoft stated at the time that they had already patched this vulnerability but the thing is not all users are receiving the patch or doing the update. For example I have an Iphone and they do have an option of turning on regular updates during times of not using it. The thing is I actually turn this feature off because of multiple reasons. First of all I actually don't want to log into my phone in the morning and notice an update interfering with things that I am used to. Applications might be moved or the home screen outlook might change and I just don't like that. Secondly, what happens if I actually don't like the new update better than the old one. Companies have sometimes made too many changes thinking that is what we want but in actuality I am used to how things were. In the example for Apple products, new emojis might be added but they don't tell you what emojis they are taken away from, so I like to see how the new update is for other users before I download. Even if Microsoft just recently released a patch for the server message block vulnerability, it doesn't mean that all users want to update or have the ability to update their server.

The Damage

We can guess that using top secret security tools from the National Security Agency should cause massive damage but it actually became one of the biggest ransomware attacks in the history of cyber security. According to Marlese Lessing," The

WannaCry attack occurred in the span of four days; however, the damage proved to be heavy. Infected systems in over 150 countries resulted in a measly $100,000 payout for the attackers — however, the losses in productivity and erased files are predicted to have reached into the billions. Businesses lost hundreds of records, and hospitals reported surgery cancellations due to erased patient files". Ransomware is a type of malicious software that is designed to block access to a computer system or its data by encrypting it until a ransom is paid to the attacker. During these four days many companies were trying to solve and break down the code of the wannacry ransomware attack. It is cyber security 101 to never pay the actual ransome because the odds of getting them to actually decrypt your data is not worth the risk. Most companies should have implemented a backup policy that would be helpful in situations like these, but for the people and organizations that didn't, having someone like Marcus Hutchins was a lifesaver. According to Emma Woollacott, "a kill switch was discovered by British security researcher Marcus Hutchins, who inadvertently stopped the attack by registering a web domain found in the malware's code. Once the ransomware checked the URL and found that it was active, it was shut down – buying precious time and giving organizations breathing room to update their systems".

Key Takeaways

With this becoming one of the biggest ransomware attacks known to man, many key takeaways can be learned from these mistakes. The first key takeaway is that a government entity like the National Security Agency was one of the beginning reasons that this wannacry ransomware domino began to fall. Before 2016, the NSA's public stance on this issue was that they were not hiding exploits and vulnerabilities from the

people. In actuality, because of what the shadow brokers did and released we saw that the NSA actually had hundreds of exploits that us as American citizens and companies like Microsoft and CIsco were not aware of. It is expected that government agencies like the National Security Agency should have the people's needs at the head of their agenda. If the NSA knew about these vulnerabilities before the hack then why didn't they privately consult the companies to bring them awareness to this issue. If they would have come forward with this instead of keeping it a secret for later use then maybe the wannacry ransomware might not have been as devastating as it became. We should continue to question and hold accountable people that are supposed to be serving our best interest. The second key takeaway would be how does this ransomware attack affect today's society. Well the one of the main takeaways was that Microsoft had created a patch about a month before the wannacry ransomware attack even happened. Even so we saw that hundreds of countries and millions worth of business was still affected. At this point we should still stress the importance of up to date systems and good cyber security awareness training. From personal experience this past summer while working in the Fairfax County IT department, one of our main focuses after working on whatever issue the client brought in was to make sure that we updated all their applications and software. In some instances when the computer looks like it hasn't been imaged to the recent image we would also have to reimage the computer. It was a department and county policy which I felt gave us and helped us maintain good cyber security awareness. I know that not all users are that adept in cyber security training but I think the businesses also have to take part of the blame for falling into bad practices. Having good security awareness training and keeping systems

up to date might be the first step, the next key solution that people or businesses might look at should also be what are their backup policies. Just looking at it as a whole ransomware is locking your data and asking you to pay up to unlock it. The issue with this is if you have more than one copy of that data somewhere else then there is no need to even try to get that lost data back. I have a tendency to break or lose my devices very often and I would be devastated if all the stuff of my phone or laptop would be lost with it. So what I do is I set up daily backups to two different cloud services just in case I lose or damage my device and for my laptop I also back up to an external hard drive about once a month as well. I don't see why I am aware enough to make this happen but businesses like to cut these critical corners when it comes to budgeting. I think if your business has the ability to lose enormous amounts of money because of a ransomware attack then having a backup policy that reflects this issue is critical to your business plan.

Conclusion

As we can see, many little mistakes can lead to a world wide dilemma. The initial perpetrators of the wannacry ransomware attack may be the shadow brokers but a lot of that blame can be shared along the way. The NSA for hiding exploits that they think that they can also use down the line. Individual cybersecurity teams for not being better prepared for a ransomware attack and individuals that just are not aware of cyber security best practices. Mistakes like these are critical into what not to do so all we can do now is learn from these mistakes and hopefully be better prepared for the next situation.

References

Burgess, M. (2017, April 18). *Hacking the hackers: Everything you need to know about shadow brokers' attack on the NSA*. Wired. https://www.wired.com/story/nsa-hacking-tools-stolen-hackers/

EternalBlue exploit: What it is and how it works. SentinelOne. (2022, October 27). https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

Lessing, M. (2022, May 4). *Case study: Wannacry ransomware*. SDxCentral. https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-wannacry-ransomware/

Woollacott, E. (2022, May 12). *Marcus Hutchins on halting the WannaCry ransomware attack – "still to this day it feels like it was all a weird dream."* The Daily Swig | Cybersecurity news and views. https://portswigger.net/daily-swig/marcus-hutchins-on-halting-the-wannacry-ransomware-attack-still-to-this-day-it-feels-like-it-was-all-a-weird-dream