My Career in Cybersecurity

In 1988, 16 years before I was even born, one of the most famous events in cybersecurity history occurred: Robert Morris distributed the first internet worm to gain widespread mainstream attention from MIT's network (*Morris Worm*), and according to Fortinet, "Although Mr. Morris claimed he did it to explore the size of the cyber space, it soon evolved into a virus that caused between $10 million and $100 million in damage repair costs" (*Top 5*).

In 2023, TeamTNT, a cybercrime group, deployed the silentbob worm that targeted Jupyter deployed on cloud servers. While it is speculated that this was just a test for a larger attack in the future, no new attack has followed (Constantin).

Although these two attacks were 35 years apart, they both display the necessity for cybersecurity, and they prove that we will always need it in the future. As we discussed in class, nothing will ever be one hundred percent secure. It doesn't matter that we have had 35 years to improve security, because in that same time attackers have been able to improve their offensive methods even if they are the same basic concept.

According to Cisco, "Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks" (*What Is Cybersecurity*). However, through my experience at Iowa State, in multiple internship positions, and in class, my definition of cybersecurity has evolved from simply protecting against digital attacks. While that would have been my answer a couple years ago, it seems like every week I have a new one. It would change to "protecting digital information", which is about as generic as it gets, or "protecting digital information from users regardless of malicious intent", or even "using psychology to learn how to think like a clueless user, a genius attacker, and everywhere in between to apply towards engineering a more secure network" like our discussion in class.

In my opinion, the most interesting and most challenging part of cybersecurity are the same thing. Just like I have in my definition, I need to be able to think like a clueless user and a clever attacker, and while some may say a clueless user isn't a threat, sometimes they're even more compromising than the best attacker.

While I was a threat investigation analyst intern over the summer, I was told a story about someone who used to work in the Security Operations Center, but is no longer there and has a button jokingly named after him: One of his last days with the company, he was digging around our ticketing system trying to understand an alarm for who knows what reason when he pushed a button that said disable. According to those who had talked to him after he was no longer with the company, he told management it was an accident when he was trying to keep his job, but he fully admitted he was trying to get out of doing work for the day after he was gone.

I think it's human nature to sometimes wonder what goes on inside someone's head when they do something like this, and luckily, as a cybersecurity major, it will be my job to understand why someone, malicious or not, would press a button labeled disable and why it was accessible to that person in the first place.

During my time at Iowa State, I have had multiple classes that will help me in my cybersecurity career. All the way back in my first semester, we began learning C. We then moved on to Java, which was easier for me since I have been using java since freshman year of high school, but it was still a challenge because the expected application of the language was new to me. Last semester I took "Cyber Security Engineering (CYB E) 230: Cyber Security Fundamentals" which taught me how to set up a very basic network and do the bare minimum to call it secure. This semester I am taking "CYB E 231: Cyber Security Concepts and Tools" which builds off of 230 and teaches us how to perform penetration tests and use other common

EDR tools. I have also learned how to use multiple flavors of Linux (even though they're fundamentally the same I wanted to see which I liked best) and basic JavaScript.

As I previously mentioned, I have had two internships, one over the summer and one over winter break, with a cybersecurity contracting company, and during that time I experienced what it would be like to work on multiple teams: Onboarding, Threat Investigation, and Incident Response. During that time, I got to experience the configuration of firewall sensors, decommissioning of can nodes, working with customers to set up tunnelling and other services before they go live, writing alarms after we begin ingesting data, and handling tickets using a number of EDR tools. I was also tasked with researching and understanding every alarm in our system to create a comprehensive list to provide to prospective customers, so they understand both what we look for and what we protect them from. While I experienced a lot of new things and learned how to properly use many tools, a couple skills I had but grew were my teamwork and communication skills.

In conclusion, cybersecurity remains an evolving study. From Robert Morris's worm in 1988 to TeamTNT's Silentbob worm in 2023, the need for cybersecurity is unmistakable, and as discussed in class, absolute security will be impossible as long as adversaries update their attack methods while we update our defenses. However, intentional attackers are not the only threat. Users with no intention of being malicious are almost a bigger threat as discovered by the company I was an intern for, and while we search for ways to prevent attacks, we must think like both attackers and users to prevent accidents, too. But I got more out of my internship than just a funny but scary story. I got experience with a wide variety of the pieces of cybersecurity, and I got a glimpse into my possible future.

Works Cited

Constantin, Lucian. "Silentbob Worm Attack Targets Multiple Cloud Technologies." *CSO Online*, 13 July 2023, www.csoonline.com/article/646165/worm-attack-silentblob-targets-multiple-cloud-technologies.html.

"Morris Worm." *Wikipedia*, Wikimedia Foundation, 24 Nov. 2023, en.wikipedia.org/wiki/Morris_worm. Accessed 25 Jan. 2024.

"Top 5 Most Notorious Attacks in the History of Cyber Warfare." *Fortinet*, www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare. Accessed 25 Jan. 2024.

"What Is Cybersecurity?" *Cisco*, Cisco, 22 Jan. 2024, www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#:~:text=Cybersecurity%20is%20the%20practice%20of,or%20interrupting%20normal%20business%20processes.