Jeongyong Yang

CAS CS 357

Professor Goldberg

December 9th, 2022

Final Deliverable Report

As the usage of online applications rises, the need to protect against cyberattacks also rises. In fact, numerous cybersecurity attacks have been reported in the United States within the recent one and a half years.

The most vulnerable attacks are attacks against non-technological worldwide industries. Since technological companies such as Google include high standards for their defense, adversaries usually target companies that lack sophisticated defense. When successful attacks are made on these companies, adversaries can not only cause worldwide impacts by potentially forcing the shutdown of their servers but also impact the customers since they can collect personal information regarding them. Such attacks force companies to pay a significant amount of money to recover their systems and protect users' information from leaking to other locations. In addition, they create distrust among the users on whether they can safely use the industry.

The three most important cybersecurity events that recently occurred are Uber Breach, the T-mobile data breach, and Killnet DDoS attack because they raised important issues regarding cybersecurity in the United States. Considering that the most recent Uber Breach was the third time that Uber became the victim of a cyberattack, it creates a sense of uneasiness among the users of Uber. Although the attack was done to increase the fame of the adversary and did not harm the industry, the stealing of the credentials of an employee is a huge issue since adversaries can conduct numerous actions once they log in as an employee. In addition, it raises the question of whether multi-factor authentication through push alarms

is useful since adversaries can continuously send push notifications to get through the system. The T-mobile data breach is significant because the attack resulted in the stealth of more than forty million customer data, including the social security number and unique phone number identifiers. Theft of personal data is always a significant issue since adversaries are free to share the information with the public, sell it to others, etc. Finally, the Killnet DDos attack raises the issue of cyberattacks from Russia to the United States. Even though President Joe Biden consistently contacted President Vladimir Putin regarding the cyberattack from Russia, there are rumors that Russia intentionally targets industries within the United States.

NCSD should require higher regulation of cyberattacks that occur from hackers outside of the United States and pass a law that prevents companies from paying the adversaries. Considering that some of the attacks on the United States industries such as the JBS and Kaseya ransomware attacks are from hackers outside of the United States (mostly Russia), NCSD needs to cooperate with other countries and reduce the possibility of attacks from overseas even though such a process can involve political issues. Furthermore, the majority of successful cyberattacks require organizations to pay money to adversaries in return for protecting their servers and users. However, if NCSD creates a law that blocks the payment, adversaries will be less inclined to launch cyberattacks on industries, which can minimize attacks on organizations.