ENMP 686
Samridha Murali
3/14/2022

Current Event 6

Colonial pipeline is an American oil pipeline that moves around 2.5 million barrels of gasoline, diesel and jet fuel from the US gulf coast to the US east coast market per day [1]. Colonial pipeline was shut down for 5 days, due to ransomware attack in May 2021. An Eastern European hacker group Darkside, which provides ransomware as a service, is responsible for this attack [2][3]. This is the Worst cyber-attack to date on US critical infrastructure [4], since the colonial pipeline is responsible for 45% of East coast's petroleum supply [5] and it affected around 50 million people in South and East America [5]. The exact details about the attack are not known, but realistically, Attackers must have gained access to the network by buying remote access from Initial Access Brokers (IAB) [6].

This attack had impacted severely on massive number of individuals, Businesses and institutions [5]. On May 6, 100GB of data was taken hostage within 2 hours' time [4]. Personal information of around 6,000 individuals who are current or former employees and their families. According to the company, "data included names, contact information, birth date, Social Security, driver's license, military ID and health insurance information". On May 7th, ransomware attack started, company Temporarily halted its pipeline to prevent spread of ransomware and Colonial pipeline paid ransom of 75 bitcoins to get decryption key. On May 9th, President Biden announced a state of emergency in Washington DC and 17 other states [1] and company resumed smaller lateral lines between terminals and delivery points [4]. On May 12th, normal operation of pipeline started again [1].

Since passwords were purchased in this case, changing passwords regularly and frequently will be a solution. Implementing multi factor authentication will increase security. Additionally, since most of the laptops come with fingerprint authentication feature, it can be used as another level of security.

Reference:

1. Digital Shadows (May 10, 2021) https://www.digitalshadows.com/blog-and-research/colonial-pipeline-ransomware-attack/
2. Wikipedia (February 06, 2022) https://en.wikipedia.org/wiki/DarkSide_(hacker_group)
3. FBI National Press Office (May 9, 2021) https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline
4. CNBC (May 10, 2021) https://www.cnbc.com/2021/05/10/largest-us-fuel-pipeline-colonial-still-mostly-shut-impact-and-reopening.html
5. NewsBreak (August 16, 2021) https://www.securityweek.com/colonial-pipeline-confirms-personal-information-impacted-ransomware-attack

6. Dr. Tom Robinson (May 18, 2021) https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin