Combating Ransomware: A Review of CNA's Ransom Payout

Zoë Medina

Professor Hoffman

CYBR-501 Intro Cyber Concepts and Tools

Shiley-Marcos School of Engineering (SMSE), University of San Diego

Combating Ransomware: A Review of CNA's Ransom Payout

Abstract

In 2021, CNA experienced a ransomware attack that ended in a payout of 40 million dollars. The attack was a result of an uninformed employee unknowingly trusting a fake browser update on a legitimate website that housed malware. The hacking group infiltrated their systems and copied over thousands of sensitive data on CNA employees before holding their systems for ransom. Despite FBI warnings about giving into ransom demands, CNA paid the hackers and got their systems back. However, this sparked a governmental investigation into why so many companies give in to the demands of hackers and how it can be prevented to discourage copycats.

Background

On March 21st of 2021, CNA's systems were held for a ransom amount of 40 million dollars, making it one of the highest ransom payouts to date. CNA is one of the United States' biggest insurance companies, responsible for insuring businesses that experience cyber attacks. On March 5th, an employee of CNA was at their workstation when they were greeted with a browser update popup. Unbeknownst to them, this was actually malware disguised as a fake update on a legitimate website. Once the hacker group gained access to this workstation, they were able to escalate their privilege within the system and move laterally to establish footholds on other devices within the network. The group was able to remain within the network for 15 days undetected using legitimate credentials and gather reconnaissance on the company's IT structure. On the night of the 20th and leading into the morning of the 21st, the hacking group launched their attack. First, they disabled all monitoring and security tools within the system so as to not raise alarms. Then, they began deleting all the system back ups and deploying their

ransomware on the servers. Reports after the incident have stated that the group managed to also affect remote devices connected via the VPN. By the end of the attack, the group had copied all unstructured data across three of CNA's virtual servers into their own cloud server. Following the incident, CNA got the FBI and police involved to investigate. The investigators reported that over 75,000 of the employee's personal identification and social security numbers had been retrieved during the attack. After four months, CNA disclosed to those affected that their information had been stolen and offered them two years of free monitoring. The attack also resulted in crucial CNA systems, such as their corporate email and web server, going offline.

A week after the ransom attack occurred, CNA decided to pay the ransom amount of 40 million dollars. According to Business Insider, "the FBI advises against paying a ransom and says doing so could instead encourage more hacks" (Chang, 2021). Despite these warnings, CNA paid the ransom quite quickly before a majority of the investigation had been completed. This malware has since been called "Phoenix CryptoLocker" and shares some similarities with the "Hades" malware, whose origins were traced back to a Russian hacker group known as Evil Corp. Because of these similarities, it has been speculated that "Phoenix" was created by the same hacker group. After the events involving "Hades", Evil Corp was put on a list of groups to which companies were prohibited to pay ransom. In a statement to Bleeping Computer, CNA stated "the threat actor group, Phoenix, responsible for this attack, is not a sanctioned entity and no US government agency has confirmed a relationship between the group that attacked CNA and any sanctioned entity" (Gatlan, 2021) and therefore no charges have been pursued for the payment. The FBI confirmed that the data stolen had not been viewed or shared outside of the cloud server.

During a US committee meeting to investigate how to minimize the effects of ransomware, it found that companies in the private sector faced logistical challenges when it came to reporting incidents. The committee stated “some companies lacked clear initial points of contact with the federal government” (Simpson, 2021), meaning many reports would receive slow response times. Coupling this with the pressure that hacker groups put on companies to respond to their demands within a certain amount of time, it was no surprise that so many companies were paying the ransom demands. However, the FBI continues to advocate against giving into demands due to the lack of accountability on the hacker’s end. There is no guarantee that the hackers will release the systems once the money is received or that the integrity of the systems will still be intact. Instead, the FBI and US government have required companies to bolster their cyber security defenses and meet a certain standard for their systems in order to reduce vulnerabilities. Furthermore, companies must put more time into educating employees in basic cyber security techniques, such as not clicking random links or downloading.

Conclusion

In conclusion, the attack against CNA was a reminder that the biggest threat companies face is an uninformed employee. For hackers, humans are the most easily exploitable with the use of social conditioning. Therefore, it is important that companies take the initiative to educate employees on how to be aware of malicious activity and report it. The incident at CNA and other ransom attacks in that year provided a push to investigate why so many companies pay the hacker’s demands. The government also created higher fines for companies that do pay ransom to certain hacker groups since paying them only motivates these groups to attempt more ransom attacks. While these steps would not stop cyber attacks entirely, companies are less likely to face heavy consequences if they follow the security standards laid out for them.

References

Chang, B. (2021, May 22). One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack. Retrieved January 16, 2023, from https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5

Gatlan, S. (2021, July 22). Ransomware gang breached CNA's network via fake browser update. Retrieved January 16, 2023, from https://www.bleepingcomputer.com/news/security/ransomware-gang-breached-cna-s-network-via-fake-browser-update/

Simpson, A. (2021, November 29). Memo cites lessons from ransomware payments by CNA, JBS and Colonial Pipeline. Retrieved January 16, 2023, from https://www.insurancejournal.com/news/national/2021/11/29/643569.htm