Jasmyn Wilhelm 03 October 2024

CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Homework 6

Short Answer Questions (short answers should generally be at least three to four sentences in length. However, it is important to be as concise as possible when responding.) or you may choose to **Upload a Two-Minute Audio or Video recording** to answer the following questions.

Listen to “Episode #25: Alberto of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/25/

Based on the podcast, answer the following questions.

Jasmyn Wilhelm 03 October 2024

1. **What led to the police investigation of Alberto Hill?**

Uruguay's police are investigating Alberto Hill as a suspect in a 2017 medical records breach. The breach involved a ransom email sent to several medical providers. The providers, with local law enforcement's help, discovered an IP address associated with the email sender, leading police to Hill's apartment in Montevideo.

2. **How did Alberto gain access to the medical provider's database, and what did he do afterward?**

By using the login and password "admin" to connect in to the medical provider's website, Alberto was able to access the database. Alberto notified the Uruguayan Computer Emergency Readiness via email about the vulnerability he had discovered. When he found and reported the vulnerability on the medical provider's website, he says he did nothing with it.

3. **What was the hacker's demand in the 2017 medical records breach?**

The hacker first demanded payment of fifteen bitcoins to keep the medical records, obtained during the data breach, private. For each day the ransom is not paid, the hacker has threatened to raise the amount by five bitcoins. It's uncertain if the medical professionals impacted by the cyberattack paid the ransom or not.

4. **What evidence did the police find in Alberto's home, and how did it contribute to their suspicions?**

In Alberto's home, authorities found numerous electronics and large amounts of cash in different currencies. Additionally, they discovered malware, viruses, and hacking tools on all of Alberto's machines, which raises the question of how an innocent person might have the need for such software. This discovery made others wonder if Alberto's things were secure.

5. **How did the authorities link the extortion email to Alberto, and what was his defense?**

Because of his hacking expertise and evidence from a police raid, authorities were able to connect Alberto to an extortion email. To stop the authorities from raiding his mother's and girlfriend's houses, Alberto created a fake admission of the crime. The court found Alberto guilty due to his email sent to CERT, claiming he was the only one who knew and acknowledged the online vulnerability, making him the responsible party for the crime.

Jasmyn Wilhelm 03 October 2024

Resources

Alberto – Darknet Diaries. (n.d.). https://darknetdiaries.com/episode/25/