Tyler Kim
Tkj9ep
CS 3710

Forensics

Part 1

Where is the missing server? Rice 003
Who took it? The TA's
Why did he/she/they take it? They wanted Bloomfield's cryptocurrency keys.
Where is it now? aaasuperdupersecurity.com
What else can you tell me about the theft?

- Currency transferred via bitcoin
- Jason B and someone named Amy Washam was involved and showed how to extract crypto currency keys from hard drive
- Jason B's bitcoin wallet address (1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g)
- Taher got bitcoin keys of the hard disk drive
- PyWallet and a data recovery tool was used
- Amy Washam's BTC address (3JZq4atUahhuA9rLhXLMhhTo133J9rF97j)
- Taher snatched Mihir's keycard during OH meeting
- Chase was recording everything

Part 2

Where is the missing server? Rice 003; When logging into the aaasuperdupersecurity.com website, I found a video from a chat message between two parties where the TA's took the server. I looked at the room number and recognized the location.
Who took it?
TA's; I logged into the aaasuperdupersecurity.com website using the credentials found from
Why did he/she/they take it? They wanted Bloomfield's cryptocurrency keys; found in the zipped chatlog about score file.
Where is it now? aaasuperdupersecurity.com; When I viewed the image/video gallery, I found an ups sticker reading that the hard drive was delivered to aaasuperdupersecurity.com. More specifically, it is transported to 3924 Reel Avenue, San Francisco, CA 94115.
What else can you tell me about the theft?

- Currency transferred via bitcoin; found in the chat message when logging into the aaasuperdupersecurity.com
- Jason B's and Amy Washam's involvement; found in the chatlog using the same password for the aaasuperdupersecurity.com and in the contact.txt tmp directory.
- Jason B's bitcoin wallet address (1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g); found in chat log
- Taher got bitcoin keys of the hard disk drive; I used exiftool on the hdd-img.jpg image and found a comment that read it is from Taher's phone.
- Pywallet and data recovery: found in the chatlog
- Amy's bitcoin address (3JZq4atUahhuA9rLhXLMhhTo133J9rF97j): found in the contact.txt which is in her email or the tmp file
- Taher retrieved Bloomfield's keycard during OH; in the Videos folder of the disk

- Chase was recording everything; showed his face in the video where they grabbed the server in Rice 003

Part 3

I really enjoyed the forensics homework. The largest problem I found was that the sleuthkit was slow and hard to deal with, especially with the initial startup of the application and did some googling with that. In addition, running the ingest modules takes an extremely long time so sometimes it felt like wasted time.

I think all the evidence that I have found are properly hidden were not too easy or hard.

One suggestion is to have different passwords for the aaasuperdupersecurity.com website and the other for zip file. Another would be to have the TA's where sunglasses since I think it would look cool.