Programming Homework: Forensics
Yannie Wu
ylw4sj

Part 1

- Where is the missing server?

159 Hill Haven Drive, Charlottesville VA, 22904.

- Who took it?

4 students and a 5th recording the crime.

- Why did he/she/they take it?

The server contained bitcoin keys.

- Where is it now?

The server was sent by UPS to 123 Locust View Drive, San Francisco CA, 94115, which is the address of a hard drive recovery service.

- What else can you tell me about the theft?

The server was stolen by students who stole Professor Bloomfield's UVA ID in order to get access to the server. A student named Natasha contacted someone named Jason to get advice about recovering the data and led them to the website aaasuperdupersecurity.com. The server was then mailed by UPS to a hard drive recovery service so that they could get the bitcoin keys stored on the server in order to access Professor Bloomfield's wallet. The UPS label was sent by an anonymous person that they talked to over chat on aaasuperdupersecurity.com with the username "lisa." They will pay the BTC to Kathy Jackson (KathyKJackson@einrot.com) at the address 3JZq4atUahhuA9rLhXLMhhTo133J9rF97j to be laundered and also pay Jason at the address *1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g* who will handle Lisa's payment.

Part 2

First, I created a new case/host using autopsy, then uploaded an image disk. I typed "file ylw4sj.mg" into my terminal to learn that the image file was for a volume partition and that the file system type was ext4.

Next, I went to Image Details on autopsy and saw that the disk was last written to on April 25, 2023 (2023-04-25 23:59:54). Using this info, I created a timeline so that I could view the activity from April 25th.

I found a few suspicious files by looking at the last entries that occurred on April 25th: ups-label.png, hdd-img.jpg, the_steal_a0c877ba.mp4, and contact.txt.

To investigate, I went to File Analysis and viewed each file. I was able to quickly find the files because the timeline included the directory path of each file.

1/home/student/Downloads/ups-label.png
This image is a UPS label from a Charlottesville address (presumably where the student lives) to a hard drive recovery service in San Francisco.

1/home.student.Pictures.hdd-img.jpg
From this image, I deduced the students wanted the server because it contained bitcoin keys that could open a valuable wallet, especially because HODL stands for “hold on for dear life.”

1/home/student/Video/the_steal_a0c877ba.mp4
https://andromeda.cs.virginia.edu/ics/videos/the_steal_a0c877ba.mp4.php
This video shows a student stealing Professor Bloomfield’s UVA ID after a meeting.

```
Contents Of File: /1/tmp/contact.txt


The cryptocurrency contact is:
Kathy Jackson at KathyKJackson@einrot.com.
Once you pay the BTC to that address (3JZq4atUahhuA9rLhXLMhhTo133J9rF97j),
it will be laudered as per our agreement.
```

contact.txt
This is the contact of a crypto launder, which I figure is who the student will use to clean the stolen bitcoin.

/1/home/student/.mozilla/firefox/common/.cache/mozilla/firefox/f54e1s71.default/thumbnails/cc83d6a1968d841411dc9090dba7c599.png
The student accessed a website called AAA Super Duper Security, Inc

/1/home/student/bin/login-info
Website: aaasuperdupersecurity.com
password: Mf86ca
username: lisa

http://aaasuperdupersecurity.com/private/videos/the-score.mp4
This video shows the students stealing the server and was found by logging into aaasuperdupersecurity.com using the credentials above.

```
Contents Of File: /1/home/student/.bash_history


firefox &
ls
cd Pictures
eog *
cd ~/Documents
unzip -P Mf86ca chatlog.zip
cat chatlog-about-score.txt
cat /dev/zero > chatlog-about-score.txt
rm chatlog-about-score.txt
rm -f chatlog.zip
logout
```

1/home/student/.bash_history
The commands show that the student opened Firefox, opened images in the Pictures directory, then went to the Documents directory and unzipped a password protected file called chatlog.zip. Then, he overwrote chatlog-about-score.txt with the contents of dev/zero/ and removed both the .zip and .txt file.

Using photorec ylw4sj.img, I selected the file type as .zip and recovered chatlog.zip and used the password Mf86ca to recover the chat log file below:

Nattasha: Hey Jason, do you have any experience with extracting cryptocurrency keys from a hard drive?

Jason B: Yeah, I've done it a few times. Why do you ask?

Natasha: Well, I have an "acquired" hard drive that I think has some Bitcoin keys on it. I want to try to recover them, but I'm not sure where to start.

Jason B: Got it. Well, the first thing you'll need to do is make sure you have the right tools. You'll need a data recovery software that can search for lost or deleted files.

Natasha: Okay, that makes sense. Any recommendations?

Jason B: I've used two different ones, which I can email you about, both are good options. Once you have the software, you can scan the hard drive for any Bitcoin-related files or folders.

Natasha: And then what?

Jason B: After you've found the files, you'll need to extract the private keys from them. This can be a bit tricky, but there are some tools available that can help.

Natasha: Like what?

Jason B: Well, one popular tool is called PyWallet. It's a Python script that can extract private keys from a Bitcoin wallet file. You'll need to know the password for the wallet file, though.

Natasha: Okay, I'll keep that in mind. Is there anything else I should know?

Jason B: Just be careful when you're working with the hard drive. If you accidentally overwrite or delete any data, you could lose your chance to recover the keys. And of course, always make sure to keep your passwords and keys secure!

Natasha: That's all a lot of work.

Jason B: There are various services that will do all this for you. Try aaasuperdupersecurity.com -- they provide these types of services. My contact there is 'Trust Me' (I'm sure that's fake), who logs in with the username 'lisa'. Apparently this person uses the same password for everything -- crazy, right?

Natasha: Thanks for the advice, Jason. I appreciate it.

Jason B: No problem, happy to help! Good luck with the recovery. If you do recover any, my Bitcoin wallet address is 1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g. You can send my fee there. I'll handle sending the payment to lisa.

Looking at the deleted files, the majority are Linux headers. The student may have deleted these at random to prevent herself from being identified, or these could've been deleted as a byproduct of other actions taken by the thief to cover his tracks. The space the deleted files were in were reallocated to new header files that are identical, meaning the student deleted and reinstalled the header files for some reason.

Part 3

- What did you think of it? We are looking for an honest answer here, not a sycophantic one.

I thought it was a fun activity to do, but I wish there was more guidance in what exactly we had to find, such as how many pieces of evidence there were or maybe a trail of clues.

- Was there anything that we screwed up on? Specifically, was there a particular piece of evidence in which we did not properly hide something? Or did we give something away?

No.

- Give one (or more!) suggestions for additional content to hide, or where to hide it, or improvements to the story.

Include a wishlist.txt file that shows what the student wants to buy once they get the bitcoin.