Alexei Hooks

Cyber 440

Professor Moeller

September 15, 2022

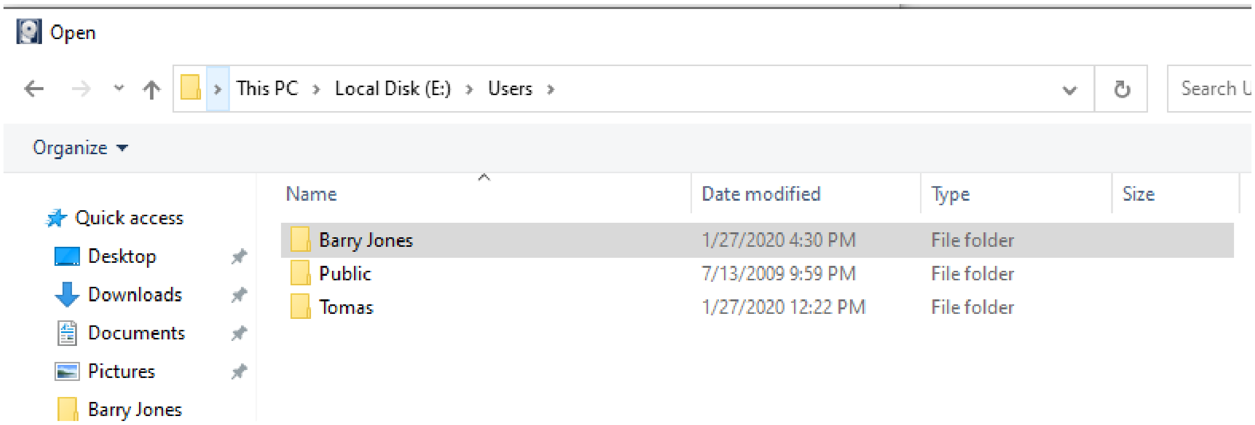
Individual Analytic Lab

Court Message:

My name is Alexei Hooks and I have been entrusted to analyze Barry Jones' personal machine through digital forensics to see if anything out of the usual was found. As I started my investigation into the case, I made sure to keep the MD5 hash the same for the files I was accessing, to ensure the integrity of Mr. Jones' files. As the investigation began, I gained access to the users of the device, Barry and Tomas. With this information I dove deeper into the system and found files within both user's accounts that were caught my eye. I believe Barry was an avid fan of birds and traveling as he had pictures of both in his folders. Barry also believed he lost the ability to access his files from internet explorer. Within Tomas' account were downloads for Tor and Hex Chat which could be linked to a malicious intent. Along with this was a contact for Kate Jones, which read that bank account information had been stolen. I have included my findings and outline of the system below for the court's pleasure, as it helps piece together what the relationships between users may be. I hope that this investigation can help the court in a positive way.

List of Users Who Have used the System:

- Barry Jones
- Tomas



Name	Date modified	Type	Size
Barry Jones	1/27/2020 4:30 PM	File folder	
Public	7/13/2009 9:59 PM	File folder	
Tomas	1/27/2020 12:22 PM	File folder	

File System Hierarchy Diagram:

- Root
    - $Extend
    - $Recycle.Bin
    - Boot
    - Documents and Settings
    - Intel
    - PerfLogs
    - Program Files
    - Program Files (x86)
    - ProgramData
    - Recovery
    - System Volume Information
    - Users

Barry Jones	**Default**	**Public**	**Tomas**
App Data	App Data	App Data	App Data
Application Data	Application Data	Application Data	Application Data
Contacts	Contacts	Contacts	Contacts
Cookies	Cookies	Cookies	Cookies
Desktop	Desktop	Desktop	Desktop
Documents	Documents	Documents	Documents
Downloads	Downloads	Downloads	Downloads
Favorites	Favorites	Favorites	Favorites
Links	Links	Links	Links
Local Settings	Local Settings	Local Settings	Local Settings
Music	Music	Music	Music
My Documents	My Documents	My Documents	My Documents
Net Hood	Net Hood	Net Hood	Net Hood
Pictures	Pictures	Pictures	Pictures
Print Hood	Print Hood	Print Hood	Print Hood
Recent	Recent	Recent	Recent
Saved Games	Saved Games	Saved Games	Saved Games
Searches	Searches	Searches	Searches
Send To	Send To	Send To	Send To
Start Menu	Start Menu	Start Menu	Start Menu
Templates	Templates	Templates	Templates
Videos	Videos	Videos	Videos

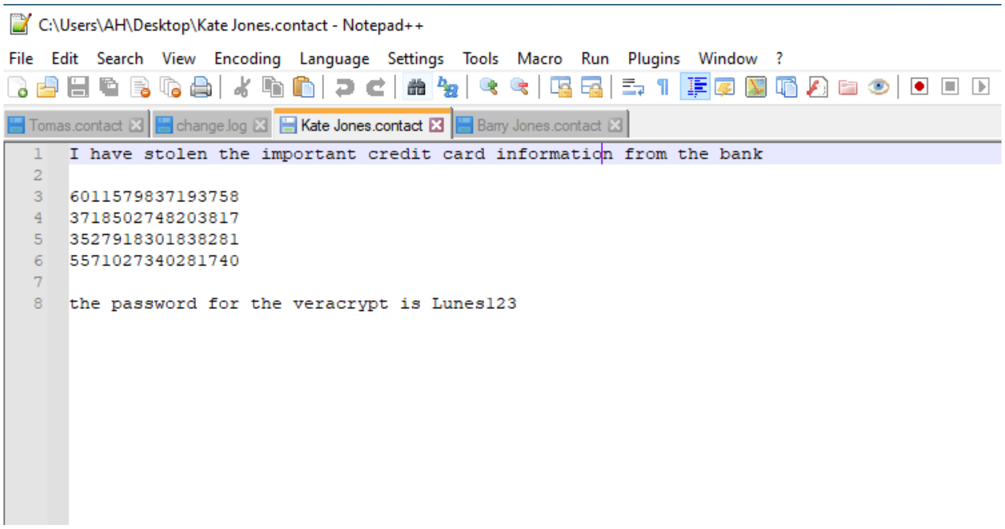
    - Windows

List of Found Data Files:

As I was parsing through the file, I used AccessData FTK Imager 4.5.0.3 to analyze the E01 file. I imaged this case on my local disk (E:). From there, I was able to see the users to the disk, Barry Jones and Tomas. I started with Barry Jones to analyze, as I went to his user information. At first, I went into Barry's Picture folder and found two folders, "hawaiibirds" and "travel" along with a single jpg file named "kate." Within "hawaiibirds," there were images numbered 1-10 of various birds, along with a guide for popular Hawaiian birds called "besthawaiianbirds." The picture labeled "kate" was of a caucasian female with reddish-brown hair. Within the second folder, "travel," there were various images of deserts numbered 001-007. Along with these images was the picture of a caucasian man with brown hair labeled: file name "00001."

Next, I looked into Barry's "Desktop" folder, to see a .txt file labeled "help". I opened this file using Notepad and it read "I have launched internet explorer and my files are gone." Along this there was also a file named "Malware.hidden." Moving down to Barry's "Documents" folder, he had one file called "DecemberLogs."

The last noticeable thing I found on Barry's account was a contact file named "Kate Jones contact," which I opened on Notepad++ to see the message:



C:\Users\AH\Desktop\Kate Jones.contact - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Tomas.contact
change.log
Kate Jones.contact
Barry Jones.contact

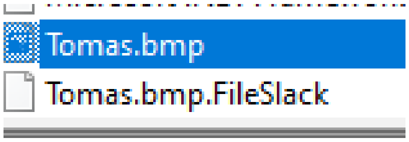
```
I have stolen the important credit card information from the bank

6011579837193758
3718502748203817
3527918301838281
5571027340281740

the password for the veracrypt is Lunes123
```

Nothing else I found looked out of the usual for Barry's account.

Moving onto Tomas' user account, I analyzed his contact folder first which held the application "VeraCryptPortable" (Password mentioned in Kate's contact from Barry's account). Also in the contacts folder was a contact file for "Tomas" which I opened on Notepad++ to discover a data blob. In Thomas' Downloads folder, he had the applications "Hex Chat 2.14.3 x64" and "torbrowser-install-win64-9.0.4_en-US." I found no other items of importance from Tomas' account.

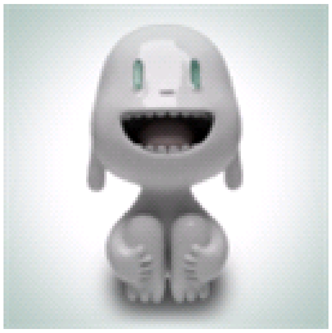
List of Found User Application History:

When looking through the applications for both Barry and Tomas, I have found the internet history while using FTK Imager. These files are in App Data and within each application's data. For Barry I found that he uses Google, Microsoft Windows, and Microsoft Windows Mail. For Tomas, I found that he uses the same apps as Barry but I also found a file in his Temp folder called "Tomas.bmp" which looks as such:



Tomas.bmp

Tomas.bmp.FileSlack



Indicators of Compromise:

When looking through this system, I believe that there is an IOC within it. Remembering the "help" file from Barry's account, I think that he was hacked being that he was not able to access his files via internet explorer. Along with this, the contact for Kate on Tomas' account, that held stolen bank account information could be part of a larger picture. I also believe that having Tor installed on Tomas' account looks suspicious as you don't usually use that browser without knowing how to use computers well enough to cause harm. I plan to keep looking into this system file image to see what else I can find.