

Case Identifier: AB12345

Case Investigator: Brandon Creech

Identity of the Submitter: Brandon Creech

Government Official Name: Larry Davidson

Date of Receipt: 02/10/2024

Items for Examination:

- Cellular Device
 - Used for communication via text messages and phone calls between other high ranking U.S. government officials.
 - Contains personal conversations among the government official's friends and family members.
 - Cell Phone: Samsung Galaxy A25 5G, Serial No: ASN39023482
- Personal Laptop Computer
 - Used for communication via emails between other high ranking U.S. government officials.
 - Contains sensitive government information (emails, files, images).
 - Laptop: HP Pavilion 16z-ag000, Serial No: WKP13945167

Findings and Report (Forensic Analysis):

- Cellular Device:
 - On today's date, I retrieved a search warrant through the US District Courts in Washington D.C.
 - Acquire tools for examination of mobile device:
 - SIM Card Reader
 - Oxygen Forensics Detective (Digital Mobile Forensic Software)
 - Once the tools were acquired and the search warrant was retrieved, the examination began.
 - Because the device was still on and locked, the first step I took was employing a brute force technique to infiltrate the password required to access the phone. The software tool Aircrack-ng was used where many passwords different from each other but relevant to the government official eventually led to the phone being unlocked.
 - Using the SIM card reader

Being able to read the SIM card is important to the investigation, as it contains all the contact information stored on the device. However, the SIM card's user data was encrypted, which meant decryption was required to gain access. I used Ciphey to decrypt the SIM card data first, then I connected a SIM card reader to my computer with the SIM card. The data was then available to be extracted on my computer.

- Each phone number and text message were either government officials, friends, or family. However, there were also conversations found that contained highly sensitive government information that proves to be useful as evidence in the investigation. Some of these conversations are allegedly between the targeted U.S. government official and a Russian government official.

Case Identifier: AB12345

Case Investigator: Brandon Creech

Identity of the Submitter: Brandon Creech

Government Official Name: Larry Davidson

Date of Receipt: 02/10/2024

- I took action by using the Oxygen Forensics to extract the user data in the messaging app. This includes all phone numbers, contact lists, and messages between other people on the government official's phone. Some user data was also able to be extracted from cloud platforms on the phone such as Google Drive and iCloud. There was a notable message found amidst the extraction that contains a conversation between the U.S. government official and an alleged Russian government official under the alias "Red Ralph" about an upcoming lunch meeting.
- Documented Message:
 - Phone Number: +7 (922) 555-1543
 - Contact Name: Red Ralph
 - Message: Greetings Mr. Davidson, this is Red Ralph from the Russian government. I wanted to remind you of our upcoming lunch meeting on 02/15/2024. Please bring the necessary equipment that we have discussed. I look forward to making agreements. -Red Ralph

- Personal Computer:
 - On today's date, I began the forensic acquisition/imaging process of the phone by acquiring all digital evidence possible on the device by extracting it from the phone to my computer. This serves as a means of preservation of the evidence so it can not be damaged or lost during the investigation. This is also part of the collection phase of the digital forensics process, which is the first step in the forensic analysis.
- After connecting the original media in the laptop to the hardware write-blocker via USB 3.0 to my examination machine, I began the imaging process.
 - I created a forensic image copy of the storage device on the phone as a basic forensic practice to ensure accuracy to the original data and to articulate the difference between what data was altered by the perpetrator. It was done through physical extraction, where the mobile phone's entire contents were formulated into a bit-by-bit copy similar to a computer hard drive. It also serves as a means of preservation to prevent any tampering.

Case Identifier: AB12345

Case Investigator: Brandon Creech

Identity of the Submitter: Brandon Creech

Date of Receipt: 02/10/2024

- Once the imaging had been completed and was then documented, I used emails as internet evidence, all of which would be relevant to the case. Through investigating the emails of the official, several emails can be uncovered showing a conversation between the official and Red Ralph about meetings and a payment for “consulting services.”

Upcoming Meeting



Mr. Davidson

Upcoming Meeting

Hello Mr. Davidson, I got everything ready. Let me know when you want me to infiltrate the system at Building A.

Red Ralph

Payment



Mr. Davidson

Payment

I'm glad to have had a successful meeting with you. Please send the payment by 12:00pm on Monday

Red Ralph

Meeting



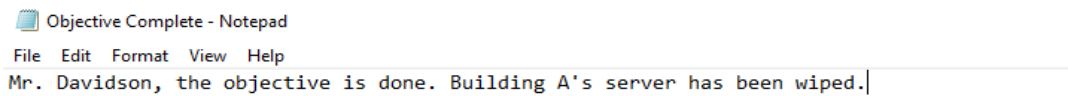
Mr. Davidson

Meeting

I appreciate working with you. Meet me at the parking garage adjacent to the building at 8pm on Tuesday night. The objective will be done within 30 minutes.

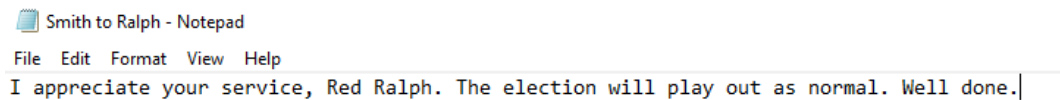
Red Ralph

- Once the email was analyzed and documented, I was also able to view previously deleted zip files that the official attempted to dispose of, including ones that were encrypted. These deleted zip files were of classified material that web logs show was uploaded to a file sharing site. It still remains unclear if anyone downloaded it as a means of transferring the secret information to anyone else.
- File named "Objective Complete."



Objective Complete - Notepad
File Edit Format View Help
Mr. Davidson, the objective is done. Building A's server has been wiped.

- Objective named "Smith to Ralph."



Smith to Ralph - Notepad
File Edit Format View Help
I appreciate your service, Red Ralph. The election will play out as normal. Well done.

Case Identifier: AB12345

Case Investigator: Brandon Creech

Identity of the Submitter: Brandon Creech

Government Official Name: Larry Davidson

Date of Receipt: 02/10/2024

Conclusion:

- In conclusion to the report, no original media was damaged, manipulated, or changed in anyway.
- Hardware that was used to recover files:
 - External Drive Dock
 - Hardware Write Blocker
 - Personal Computer for recovery scans on the storage device
 - Data recovery kit tools such as screwdrivers and spindle tools
- Software that was used to recover files:
 - FTK Imager
 - EnCase Forensic
 - EaseUS Data Recovery
 - Ciphey
- Evidence includes:

- A text confirming a lunch meeting between the official and a Russian official under the alias "Red Ralph."
- An email conversation between the official and Red Ralph regarding meetings and payment about consulting services.
- Several deleted zip files of classified material detailing about the completed objective as specified through web logs.