Case Identifier: GH-44937

Case Investigator: Dylan McCann

Identity of Submitter: Andrew P. Harris, 1st Congressional District of Maryland

Date of receipt: 12/4/2024

Items for Examination:

- Cellular Device
    - iPhone 14
    - 128GB
    - Model number: B4824
    - OS: 18.1.1.1
- Personal Laptop
    - Lenovo ThinkPad X1 Carbon Gen 12 14”
    - Processor: Intel® Core™ Ultra 5 135U vPro® Processor (E-cores up to 3.60 GHz P-cores up to 4.40 GHz)
    - Operating System: Windows 11 Pro 64
    - Memory
    - 16 GB LPDDR5X-6400MHz (Soldered)
    - Storage: 512 GB SSD M.2 2280 PCIe Gen4 Performance TLC Opal

Findings and Report (Forensic Analysis):

- Cellular Device
    - On today's date I received a search warrant to proceed with forensic analysis on this device through the Washington D.C. U.S. District Courts
    - 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.

Case Identifier: GH-44937

Case Investigator: Dylan McCann

Identity of Submitter: Andrew P. Harris, 1st Congressional District of Maryland

Date of receipt: 12/4/2024

- First step was to remove the sim card from the phone to ensure that it does not connect to the network and overwrite any date, while the SIM card was out it was ran through a SIM card reader that helped me obtain a call logs, text messages, address books, as well as what time and date texts and calls were made.
- While the SIM card reader was extracting data, I turned my attention to the phone and began running a password cracker using a dictionary attack which ran for 3 hours before successfully finishing.
- In that time the SIM card reader finished extracting its data and a text to an abnormal contact labeled “Red Ralph” confirming a lunch date on 2/15/2024
- This was confirmed within the device itself after checking text messages saved on the device
- Because the password was cracked, I then used Oxygen Forensics to begin a full system extraction. Which yielded data and logs off all accessible apps, including emails exchanges with RedHat@gmail.com containing communications about meetings and payments

- Personal Laptop
  - On today's date I received a search warrant to proceed with forensic analysis on this device through the Washington D.C. U.S. District Courts
  - Acquire tools for examination of mobile device:
    - FTK imager
    - Write blocker
    - Autopsy

Case Identifier: GH-44937

Case Investigator: Dylan McCann

Identity of Submitter: Andrew P. Harris, 1st Congressional District of Maryland

Date of receipt: 12/4/2024

- Once the tools were acquired and the search warrant was retrieved, the examination began.
  - First step was to prevent the laptop from connecting to any network and hooking the laptop up to a write blocker to prevent anything from tampering with the data
  - Next was to use FTK imager to create a forensically sound copy of the hard drive to protect the integrity of the original.
  - After taking image, I bypassed the administrator password within the GUI
  - After bypassing the administration password and gaining access to the investigative subjects account, I did an investigation on the accounts and apps that were still logged into and found the same emails that were recovered on the phone.
  - Next, I used Autopsy to recover any deleted files on the system. I found multiple deleted zip files with classified information in them.
  - After checking internet history to see commonly frequented sights, and cross checking it with web logs, I found that multiple of these files were uploaded to a file sharing website.

Conclusion:

- In conclusion to the report, no original media was damaged, manipulated, or changed in anyway
- Hardware that was used to recover files:
  - SIM card reader
  - Write blocker

Case Identifier: GH-44937

Case Investigator: Dylan McCann

Identity of Submitter: Andrew P. Harris, 1st Congressional District of Maryland

Date of receipt: 12/4/2024

- Software that was used to recover files:
    - FTK imager
    - Autopsy
    - Oxygen Forensics Detective (Digital Mobile Forensic Software)
- Evidence includes:
    - Logs of Texts between contact “Red Ralph” and defendant setting up meeting times and locations
    - Email exchanges between defendant and “RedHat@gmail.com” discussing meetings and payment
    - Deleted zip files containing classified material
    - Web logs of the deleted zip files being uploaded onto file sharing sites
- In conclusion, I believe the evidence shows that the defendant did in fact have an outside contact and attempted to share classified information. It would be my assumption given the timeline of events that the defendant was attempting to sell classified information, using file sharing websites as an exchange mechanism and then setting up meeting times to receive a cash payment for the information given.