INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2024-2025 – 1st Period

Digital Forensics Report Lab3

Group number:	35	Name	IST Number
Student 1:		Rodrigo Leal Saraiva Ganância	103809
Student 2:		Pedro Miguel de Melo Ribeiro	102663
Student 3:		Diogo José Almeida Rodrigues	102848

1 Acquired artifacts

Name	Type	SHA-256 Value
BankStatement	pdf	6bcaa146616cff67eb5acf9ac6a2e84e503236e86a398d9784316a76e5a5d502
report	pdf	0e9aef94d7876a996be9f2fac6644e7d2258016f5409897e045501d7dfaa0625
MKU documentation	pdf	75a554633a3d0a98faed4b5b1cc2e52d166fd44ee2804deb808a8f889f6ca3a5
rafael	eml	2e55a4810f3d82762d8097d9bd48487e5eaa41ace53a95eb34fa85d8748d20f4
blueprint	png	eda61b735509d596f43631bb867471ed586e841b6d85f011380cef3b3bd2009f
diary	txt	a733b817952b31665f965a2fa7717a00116b60b5268b0fe7f409782fc28b22a2

2 Report of all findings

Phishing (trace 3):

When Exporting Objects with Text filter as “search” we can find google searches from Miguel Estrela’s IP for terms like “phishing email examples” and “hook security phishing email quiz”. We can also find a ChatGPT conversation when using “chatgpt” as a filter. Miguel requests ChatGPT’s assistance in drafting a phishing email to Rafael Calhau, impersonating Ricardo Prado and asking him to "update drivers”. From this exchange he got a template, which was later found in Rafael Calhau’s mailbox. Calhau responded to this email, which contained a phishing link designed to install malware on his computer, indicating that he would proceed with the requested driver update.

Emails:

In the "Export Objects" section of Wireshark, a search for Outlook objects reveals several JSON files containing references to Rafael's email history. Among these are emails Rafael sent to Virgolino and Adelino Rebelo de Sousa, the Mayor of Oeiras. In his message to Virgolino, Rafael instructs him to execute MKUltra commands on restaurants in Oeiras. In another email, he confesses to Adelino that he received a commission from these same restaurants. Additionally, a reply email was found regarding a driver update, which was in response to the phishing attempt mentioned earlier in this report, found to be the work of Miguel Estrela.

ARP, SSH (trace 3):

Upon filtering for "arp" in the Display Filter, multiple ARP requests originating from Miguel Estrela's IP address range (194.210.60.0 to 194.210.63.255) were identified. These requests indicate the use of an ARP scanning tool to collect network information, specifically targeting the discovery of IP and MAC addresses, including that of Rafael's device.

Following this scan, Miguel attempted to connect to Rafael's computer, initially without success. Miguel, then, performed a search on "How to establish a connection using an SSH port", after which he successfully established an SSH connection to Rafael's PC.

Malware (trace 3):

When exporting objects with the content type "application/zip," we located a folder titled "driver-update", associated with the phishing incident. Inside this folder was an executable file that triggers a Python script concealed within a ".malware" subdirectory. The script is programmed to send encrypted HTTP requests containing commands to extract files from the targeted device. These requests are directed to a specified IP and port—Miguel Estrela's IP and port 1337, in this case—which prompted us to search for HTTP communications with Miguel's IP.

Applying the text filter "194.210.61.136:1337" (Miguel's IP), we identified encrypted message exchanges between Miguel and Rafael. The encryption in these messages matched the functions and the password embedded within the Python malware script. Using this information, we created a decryption script (decoder.py) to decode the content of these messages.

Upon decryption, we found a series of commands originating from Miguel's IP, such as "download <filename>", followed by either the corresponding file data or a "file not found" error message from Rafael's IP. The most critical file transfers follow:

- **blueprint.png:**

  command: "download blueprint.png" , response: blueprint.png data

  We couldn't reassemble the whole image, due to packet loss, therefore only half the data was captured. This image is the ISTSat-1 blueprint artifact found in the pen drive.

- **logs.txt:**

  command: "download logs.txt" , response: logs.txt data

  This file is the MKUltra API logs regarding its usage on Oeiras' restaurants. This is also the artifact found in the pen drive and João Musk's PC.

- **diary.txt:**

  command: "download diary.txt", response: diary.txt data

  This file is Rafael Calhau's diary, which contains critical information on the integration of the MKUltra project with ISTSat-1. In the diary, Rafael admits to incorporating MKUltra technology into ISTSat-1, implicating both himself and Virgolino in the project. He further notes that Adelino, the Mayor of Oeiras, is

aware of and informed about the project's details. Following repeated experimentation on animals, Rafael expresses growing suspicions that Virgolino and Adelino may be collaborating to extend MKUltra's capabilities to enable control over human subjects.

Discord messages (traces 1, 2, 3):

By exporting objects in Wireshark with the text filter set to "discord", logs of conversations between Miguel Estrela and Diogo Caseiro, under the filename "messages", were discovered in all three traces. In these messages Miguel expresses his suspicion that Rafael Calhau and Virgolino Gonçalves are involved in dubious activities. He shares with Diogo a copy of the Deco Report, which details the significant growth of restaurants in Oeiras—an item Miguel found during personal research after overhearing a suspicious conversation between Rafael and Virgolino that made him suspicious about the satellite. Miguel tells Diogo that he plans to investigate further by accessing their computers for potential evidence. Later, Miguel reports back to Diogo, confirming that he uncovered incriminating information linked to MKUltra and the ISTSat-1 satellite. Miguel mentions his intent to send the findings to João Musk, following a Diogo's recommendation, emphasizing that the information was too important to keep to himself.

API documentation, bank statement:

Through an analysis of FTP exchanges in Wireshark, we observed a sequence of login attempts by João, who tried to authenticate as Virgolino using the passwords "lsiurhgilsuh," "juriodlgjd," and finally "ubuntu." On the final attempt, João successfully established a connection and proceeded to search for and transfer files. He accessed both the API documentation and a bank statement belonging to Virgolino. Additionally, João retrieved a file named "rafael.eml", which contained the previously mentioned message from Rafael Calhau instructing Virgolino to direct MKUltra commands at restaurants in Oeiras.

3 Analysis of relevant findings

3.1 Do you find any evidence of transfers involving the five hidden documents in the analyzed network traces? What can you determine about the source of these documents?

We found evidence of the five hidden documents in these network traces: DECO's report, Virgolino's bank statement, MKUltra API documentation, MKUltra API logs and ISTSat-1 blueprint.

DECO's report was gathered by Miguel Estrela when researching about the topic online in trace 1, according to the discord messages sent by Miguel to Diogo.

The MKUltra documentation and Virgolino's bank statement were transferred from Virgolino's computer via FTP by Miguel Estrela in trace 2. Miguel attempted to log in using the password "ubuntu", succeeding only after two initial incorrect attempts.

The transfers of the blueprint and logs are found in trace 3. These were directly transferred from Rafael Calhau's IP to Miguel Estrela's IP through HTTP requests involving the malware script.

3.2 What can you deduce about the identity of the person(s) responsible for transferring the documents?

The responsibility for transferring the documents falls on Miguel Estrela, as he admits to being wary of both Virgolino and Rafael, and mentions accessing their computers during a conversation with Diogo Caseiro.

" [...] I managed to access Virgolino's computer and found some shady things. [...] I'll try to see if I can get something from Rafael as well",

All evidence regarding phishing google searches and Chat GPT requests from Miguel Estrela indicate that he created the malware and sent the email to Rafael in order to remotely steal his files. The network IP to where the

malware was sending HTTP requests was also Miguel's IP which confirms he was receiving requests and sending commands to Rafael's PC.

It was also validated that Rafael transferred the API documentation and bank statement from Virgolino's computer via FTP. After two attempts, Rafael successfully guessed Virgolino's password, "ubuntu", and completed the transfers from his own IP address.

3.3 Can you establish a timeline of key events that explains how the data exfiltration occurred and how the documents ultimately ended up in João Musk's possession?

The timeline of key events is attached to this folder and it explains the order of events throughout the Ariane-6 case. After Miguel gathered substantial evidence related to MKUltra and ISTSat-1, he was uncertain about how to proceed independently. Diogo then advised Miguel to send all materials to João Musk, whom he believed to be trustworthy and capable of managing the situation. Eventually, Miguel must have sent the anonymous email to João and left the pen drive with all documents from the Ariane-6 case that he had gathered.

3.4 Based on all the evidence gathered in this investigation, what can you infer regarding the conspiracy hypothesis that initiated this inquiry? Did you find any additional evidence supporting it? If so, who might be the actors involved, and what steps would you recommend for the next phase of the investigation?

The initial conspiracy hypothesis suggested the existence of an ongoing crime involving the satellite. Our investigation has confirmed this theory through the analysis of evidence related to the five artifacts retrieved by Miguel Estrela. Additionally, we uncovered further evidence, including Rafael's diary, emails, and Miguel's Discord messages. These documents collectively support the integration of MKUltra in the satellite operation, establishing that both Rafael and Virgolino are orchestrating this scheme.

Our investigation has identified additional key players beyond Miguel, Virgolino, and Rafael, notably Adelino Rebelo de Sousa. Rafael's diary indicates that Adelino is aware of the MKUltra testing and expresses interest in its capabilities, particularly in using it to manipulate elections. This aligns with Rafael's emails to Adelino, in which they discuss a "master plan" they are developing together. Furthermore, these emails reveal their involvement in receiving commissions from the restaurants involved in the brainwashing conspiracy.

To advance this investigation, seizing Virgolino's and Rafael's equipment for detailed forensic analysis is essential. Additionally, a comprehensive inquiry into Adelino's involvement, including the specifics of his "master plan", is necessary. The restaurants suspected of paying commissions to Rafael Calhau should also be inspected to determine their knowledge of MKUltra's applications in Oeiras. Lastly, interviewing Diogo Caseiro could be valuable for confirming key events and providing further insights.