ISCS 4533-003 Malware Analysis

Capstone Assignment

Student:
Dillen Dela Cruz, odv464

Prepared for Malware Analysis
04/17/2024
Professor: Thomas Croy Ervin

Introduction:

The case revolves around Mr. Brown's admission of illicit activities targeting HEB's servers and customer data. In early April 2023, Brown confessed to compromising HEB Server-2 using an SQL Injection attack. He then moved laterally to Server-3, where he discovered and encrypted customer data using an XOR tool with the key "2023". Brown indicated that both the encrypted data and the XOR tool reside in the same directory on Server-3. Additionally, Brown confessed to creating a "countdown" website, demanding monetary payment from HEB executives. Failure to comply would result in the automatic release of remaining customer data to the DarkWeb. The URL of this website is embedded within malware on Server-1, along with Brown's IP address, which was also traced back to the SQL Injection attack logs. On his personal computer, Brown admitted to creating a UPX-packed executable containing a kill-switch password for stopping the data release upon payment. However, he claimed to have forgotten the location of this executable and the PIN required to access it. The case involves tracing the digital footprint left by Brown's actions, including investigating HEB's servers for encrypted data, malware containing the website URL and IP address, and potentially locating the UPX-packed executable on Brown's computer. Additionally, efforts should be made to recover or reset the PIN for accessing the kill-switch password.

--Screenshot of the log on Server-2 showing the IP address & SQL Injection attack (8pts)

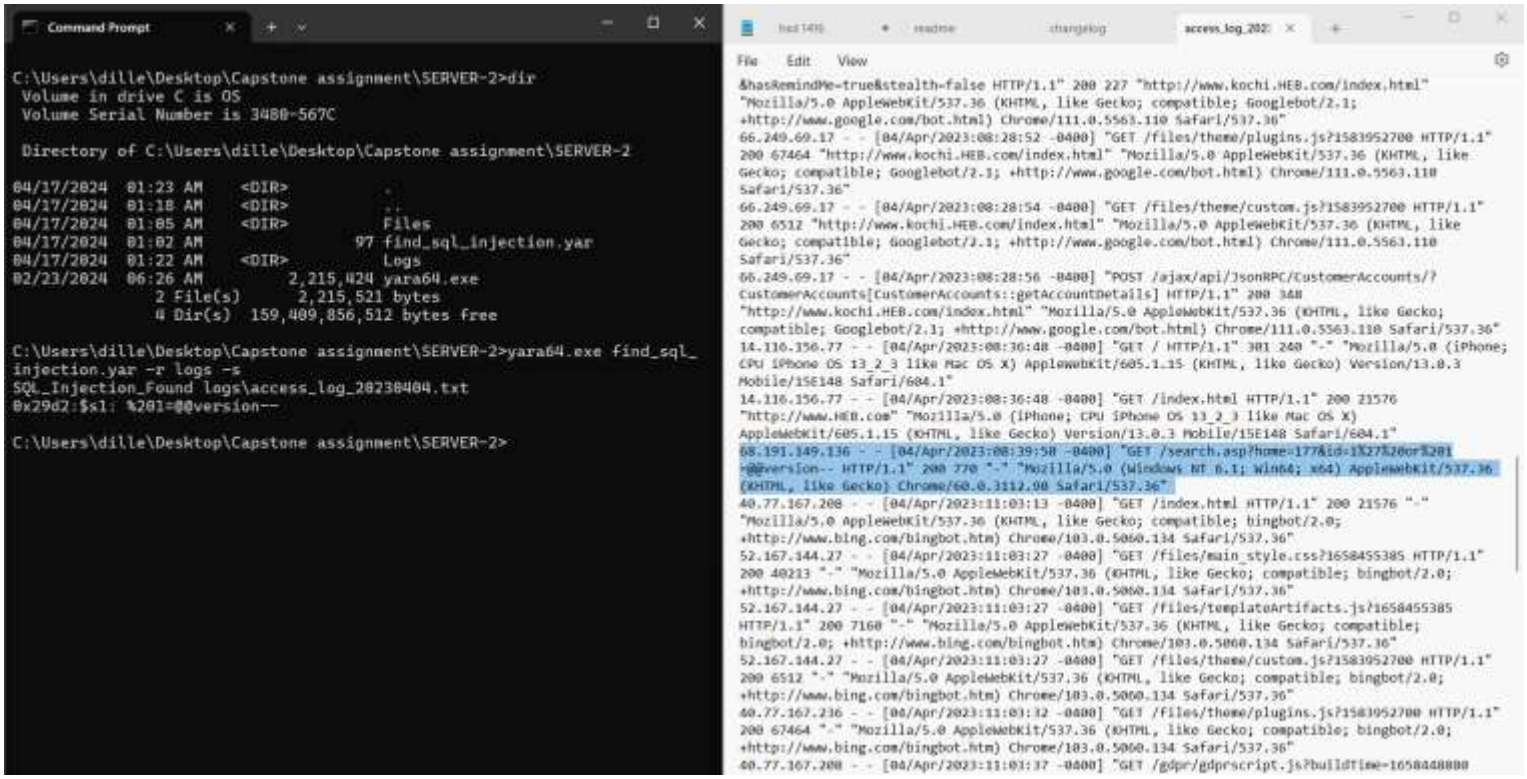

Figure 1: Yara Output

This screenshot captures my use of the yara64 tool along with a YARA rule file to identify both the IP address and the SQL Injection attack. Afterwards, I filtered the specified log file to pinpoint the relevant information needed for further analysis. The IP address associated with the SQL injection is “68.191.149.136”

--Screenshot of how you found the malware on Server-1 with the IP-address embedded (8pts)

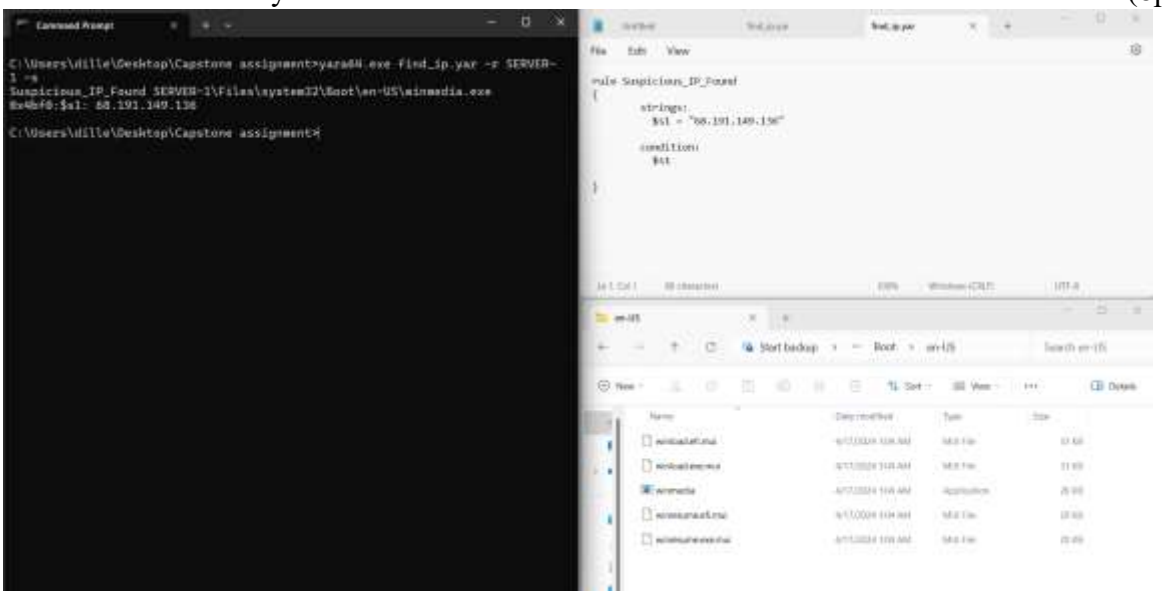

Figure 2: Malware in Server-1

This screenshot captures how I found the malware on Server-1 with the IP-address embedded. First, I created a YARA rule in a text document to target the IP address identified earlier. Then, I used YARA with this rule text file to scan the entire Server-1 directory. As a result, I found the IP address embedded within the "winmedia" file.

--Screenshot of the "countdown" URL found in malware on Server-1 (8pts)

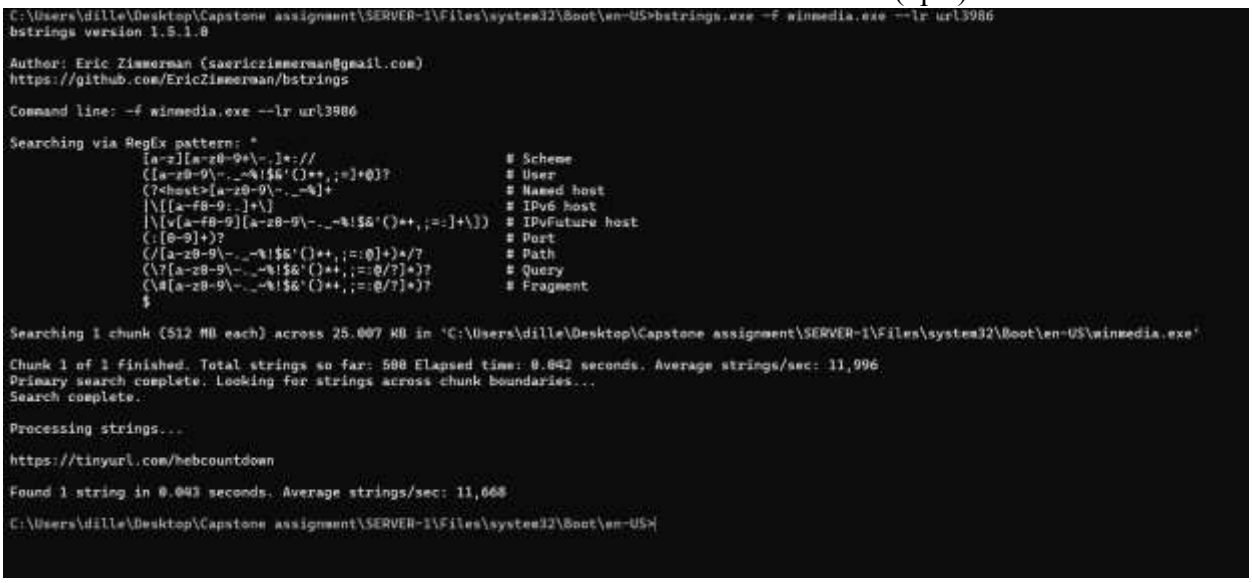

Figure 3: Bstrings Output

I discovered the "countdown" URL in the Server-1 malware by using the bstrings utility. After moving to the malware's directory and placing bstrings there, I executed the tool and used the "url3986" command to search for URLs. The output revealed "https://tinyurl.com/hebcountdown"

--Screenshot of the location of the UPX-packed executable on Brown's computer (8pts)

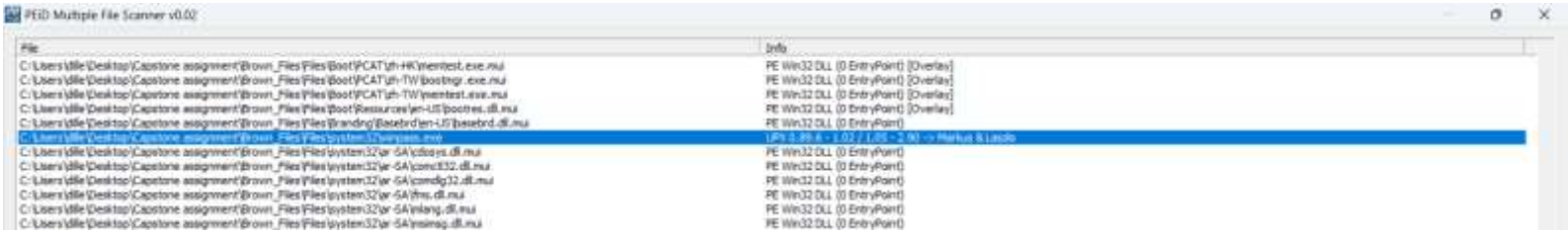

Figure 4: PEiD Output

I located the UPX-packed executable on Brown's computer at "C:\Brown_Files\Files\system32" using the PEiD file scanner. First, I adjusted the scanner settings to run on "recursive subdirectories" and then initiated a "multi scan," directing it to the Brown files. This process revealed the exact location of the UPX-packed executable.

--Screenshot of successfully unpacking Brown's UPX-packed executable (8pts)

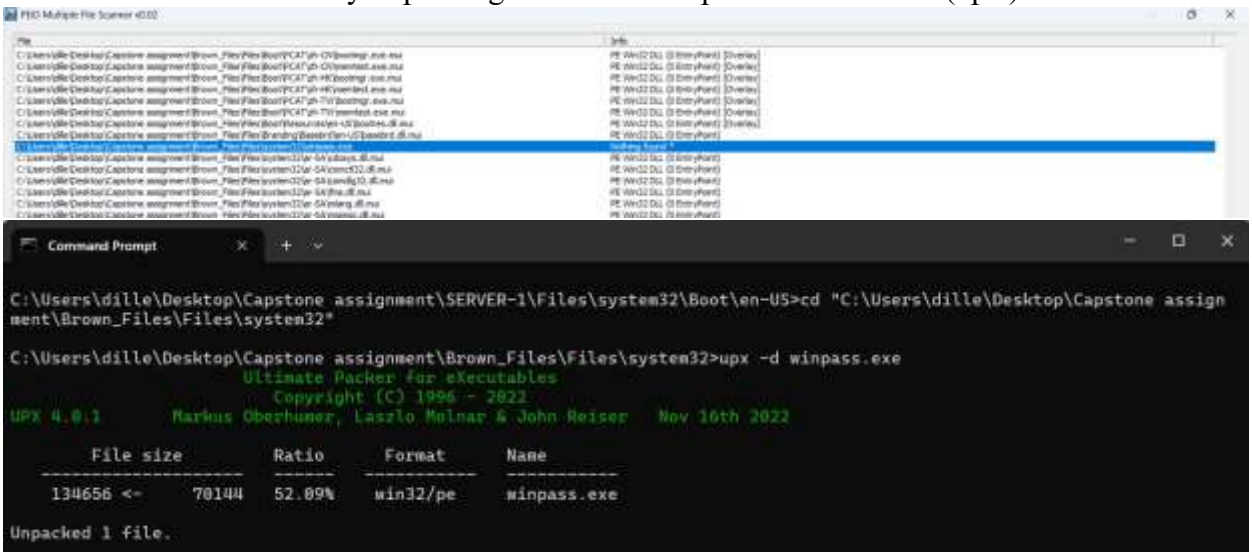

Figure 5: Unpacking using UPX

The screenshot shows that I successfully unpacked the "winpass" executable using the UPX utility and the "-d" option. To do this, I placed the UPX tool in the same directory as the executable. The fact that the PEiD output doesn't show any information in the info section confirms that the unpacking process was a success.

--Screenshot of how you reverse-engineered the PIN from the unpacked executable (8pts)

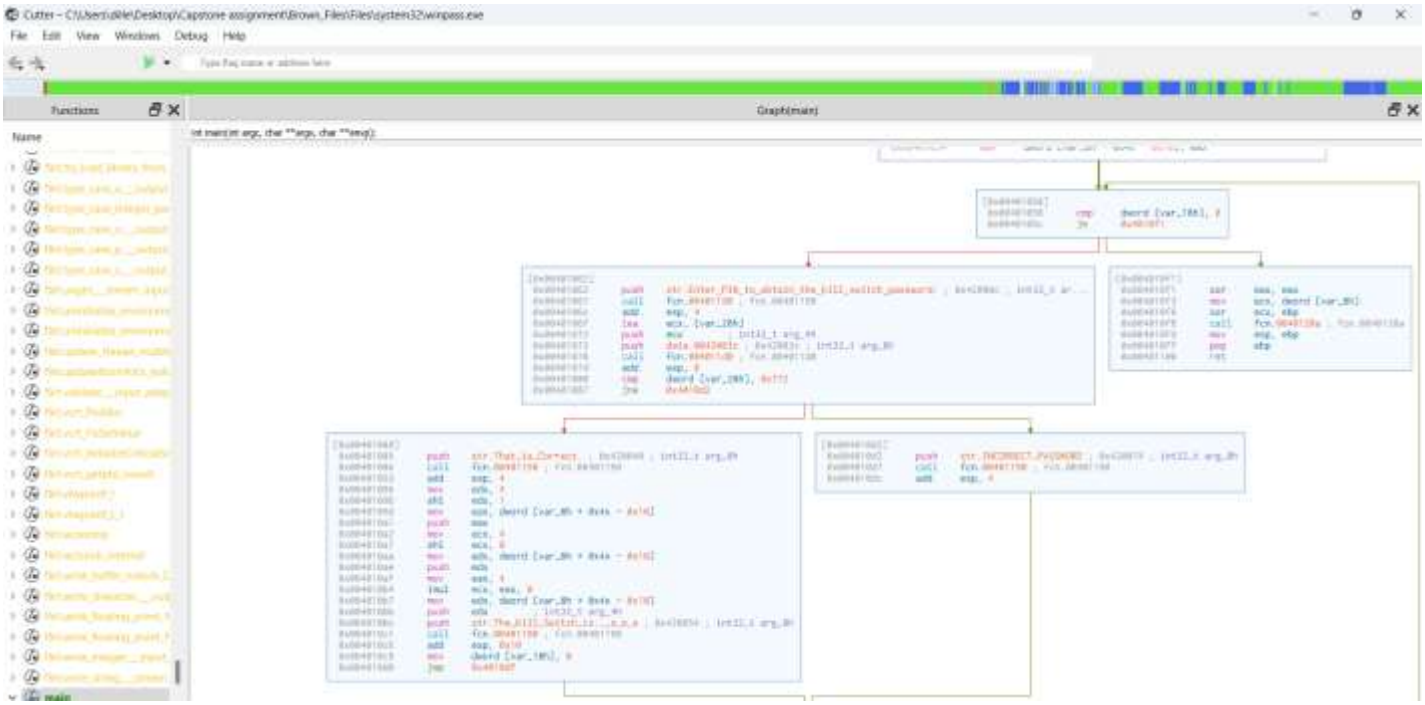

Figure 6: Unpacking using UPX

To uncover the PIN in the unpacked executable, I used the Cutter tool. By examining the main method, I explored the executable's functions. I specifically looked for mentions of "PIN" and found the prompt "Enter Pin to obtain the kill switch password." In this area, I searched for comparisons with "cmp" to identify what the program compares with user input. This analysis revealed that the correct PIN is "0x772" or 1906.

--Screenshot of the kill-switch password after entering the correct PIN from the above executable (8pts)

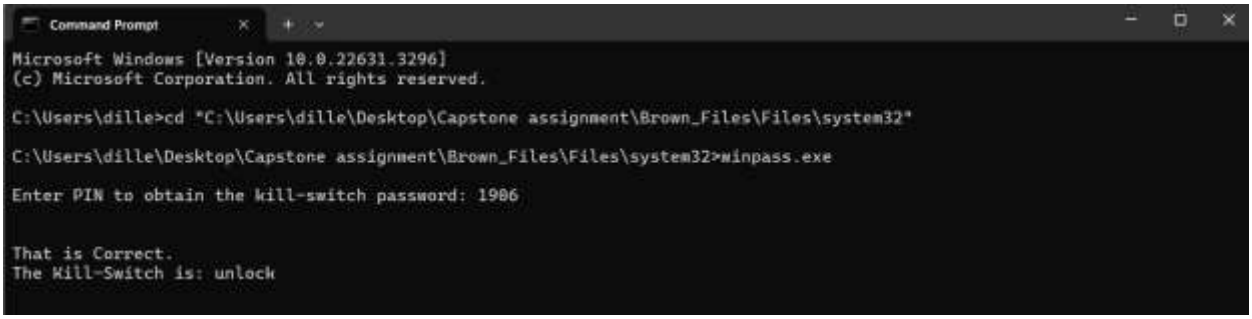

Figure 7: Kill-switch Password

I ran the program via command prompt and entered the PIN obtained from the previous steps, which was 1906. Upon entering it, the kill-switch password was revealed, confirming the correctness of the PIN. The password was shown to be "unlock."

--Screenshot of the directory of the renamed XOR tool & encrypted (XOR) customer data on Server-3 (8pts)

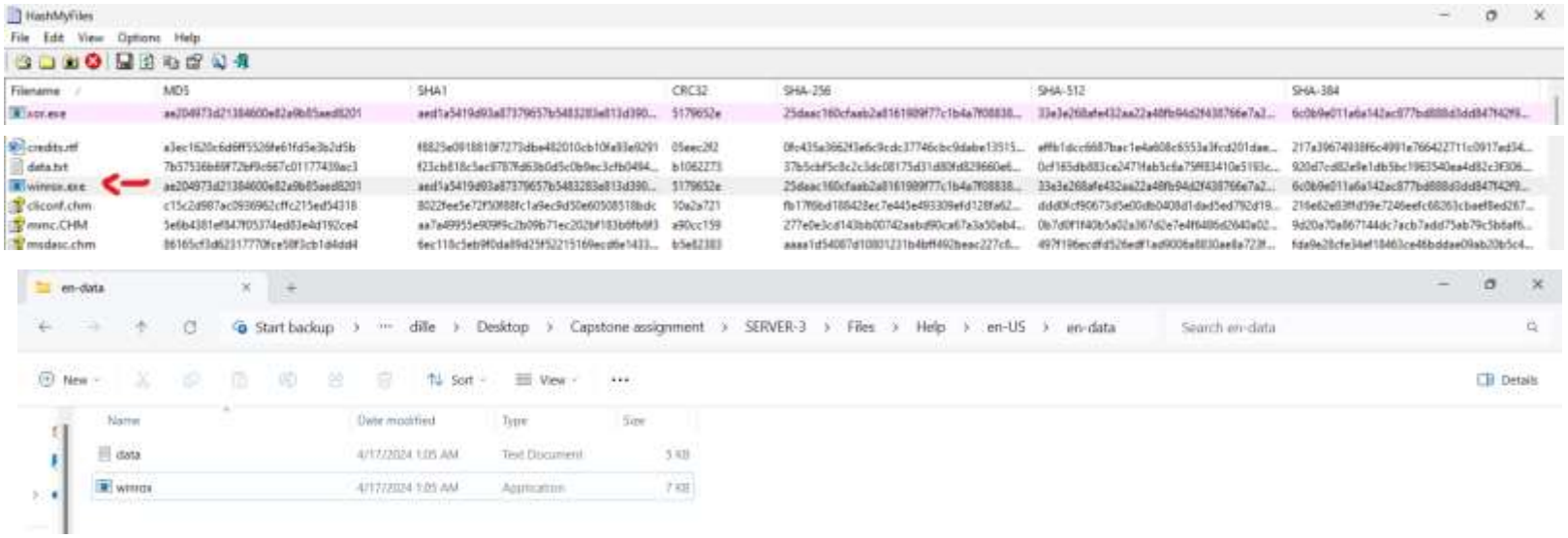

Figure 8: Kill-switch Password

To achieve this, I completed several steps. First, recognizing that the renamed XOR tool shares the same hash value as the XOR tool in Brown's files, I utilized the HashMyFiles tool to hash the XOR tool. Next, I hashed all files in the Server-3 directory. Finally, I utilized the find tool in HashMyFiles to identify matching hashes, which directed me to "winrox.exe." Afterwards, I conducted a search in the Server-3 directory for "winrox.exe," leading me to the directory containing the encrypted data and the renamed XOR tool (winrox.exe).

--Screenshot of a snippet of the decrypted (XOR) customer data (8pts)

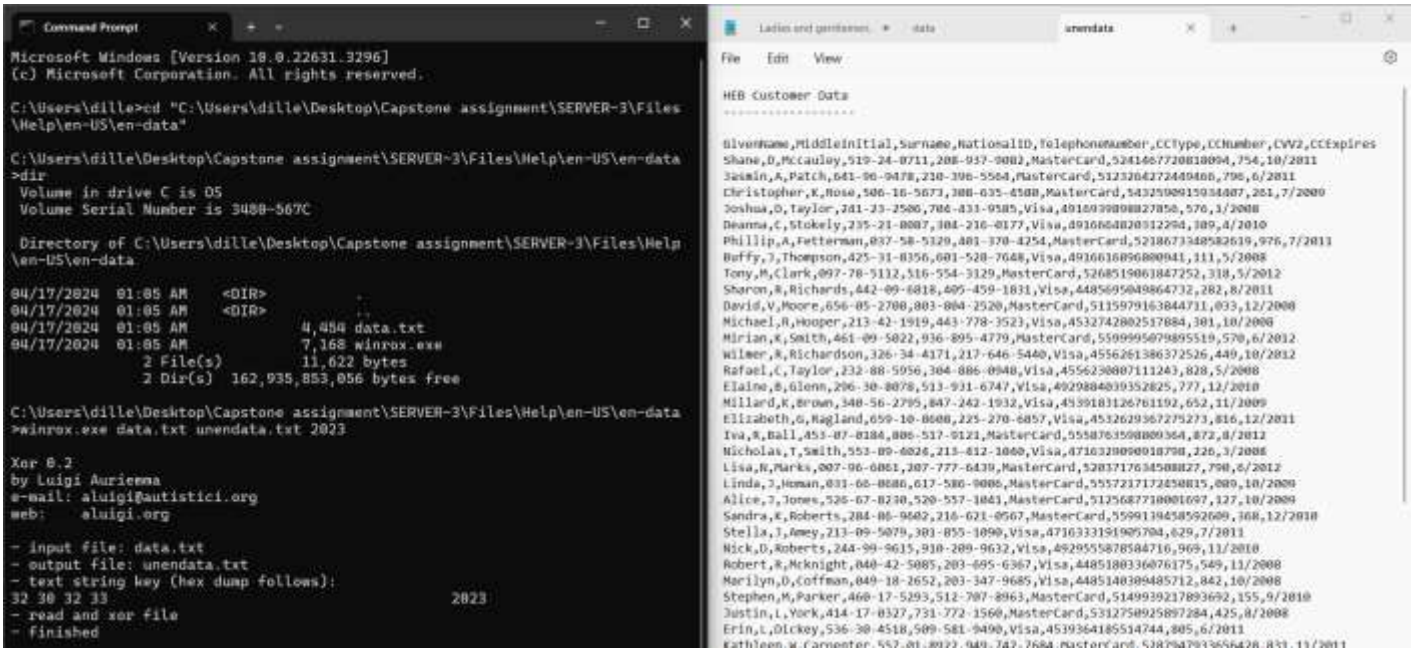

Figure 9: XOR Tool

In the screenshot, I decrypted the data to reveal customer information. I used the XOR tool, which was renamed and located in the "en-data" directory. By running the tool, I extracted the decrypted data into a new document, using the key 2023 provided to me.

--Screenshot of successfully entering the kill-switch password on the "countdown" website (8pts)

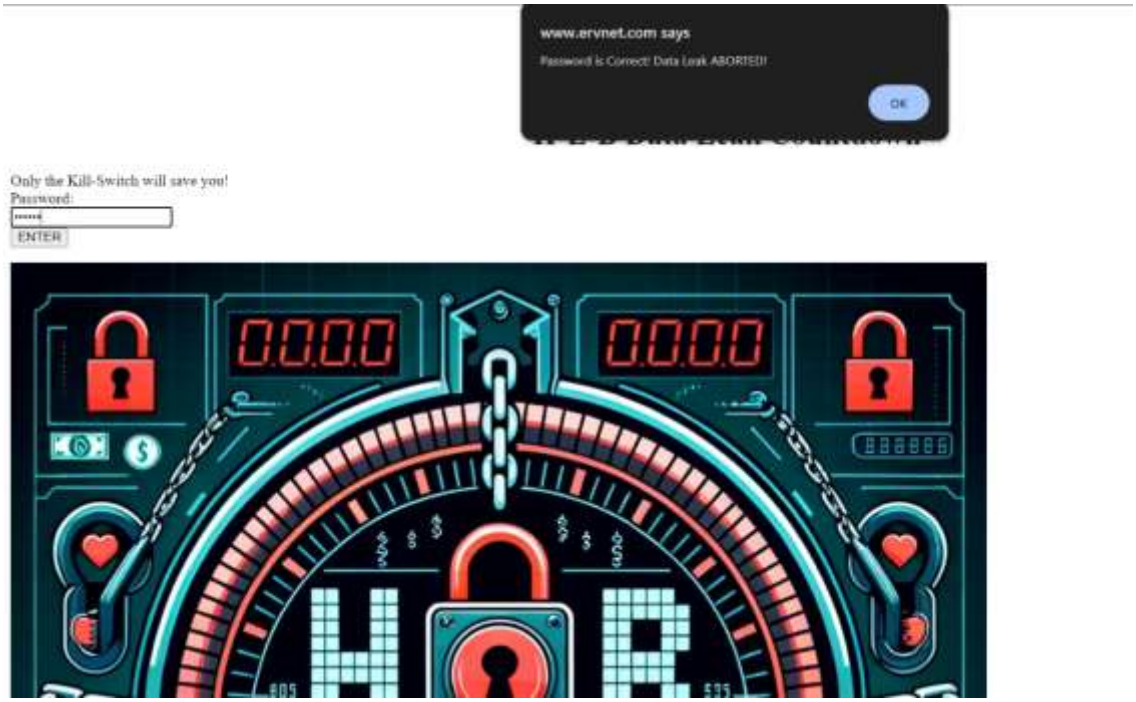

Figure 10: "countdown" website

In the screenshot, I successfully prevented the data leak using the password discovered in the previous steps, which was "unlock." I accessed the URL obtained from the bstring output of the malware on Server-1. Upon reaching the webpage, I encountered a user input box where I entered the password to halt the data leak from occurring. The password was correct, and a box appeared at the top confirming my actions.