Vincent Cruz

Capstone Assignment

IS 4533-001

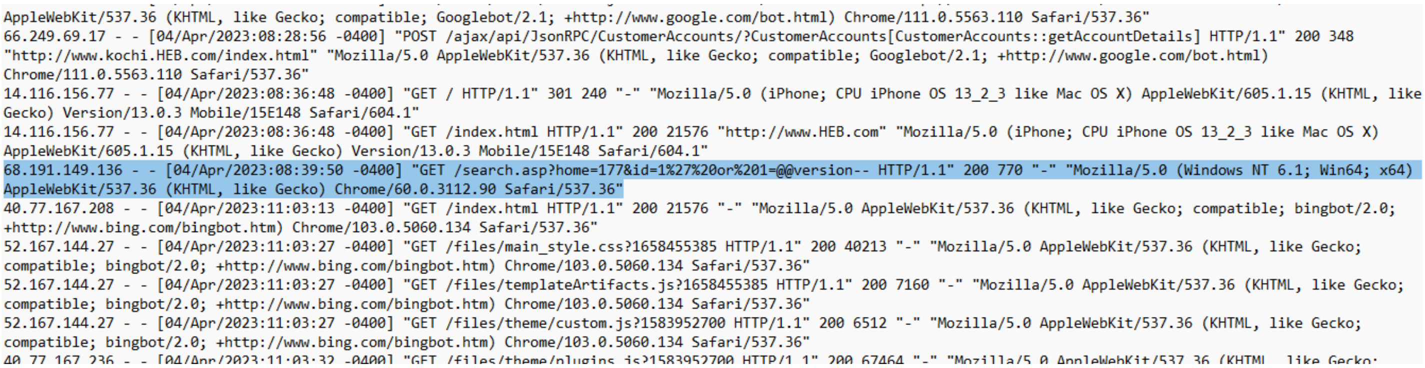
Spring 2023

Case Description

After HEB servers were hacked, the prime suspect is Benjamin R. Brown. After a partial confession, the goal of this project will be to find the evidence of Brown’s malicious activity on HEB’s server 1, 2, and 3 and stop his plan before customer data is released. Brown says he first accessed server 2 via a SQL injection attack, and then encrypted customer data on server 3 using an XOR tool. Brown also says the URL to his countdown website can be found on server 1, and the password can be found in a UPX-packed executable on his computer. The following screenshots will illustrate my usage of multiple forensics tools to investigate the malware and foil Brown’s plan.

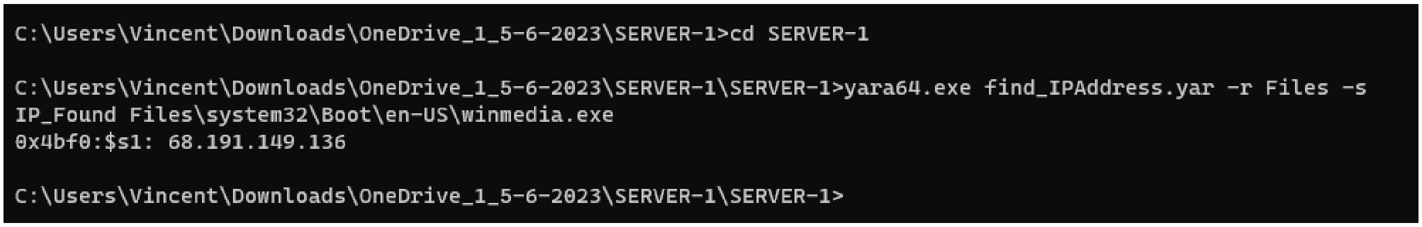
Findings

1. Screenshot showing Brown’s IP address and SQL injection



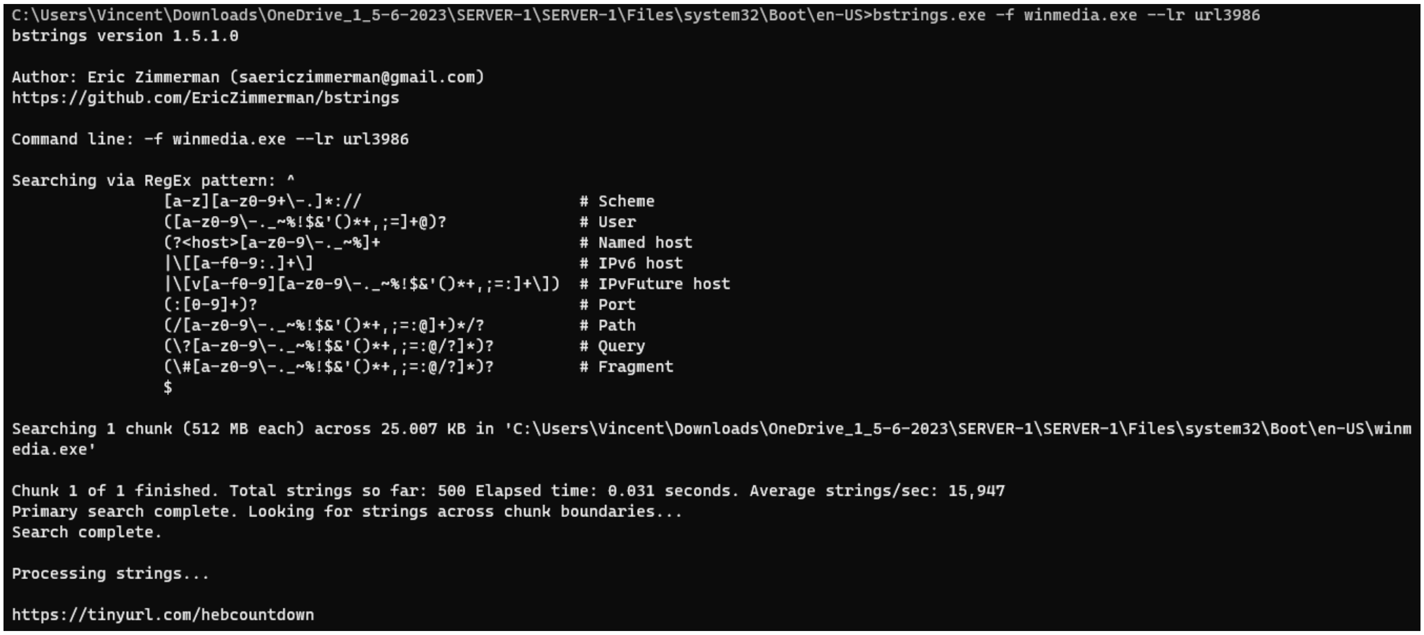
```
AppleWebKit/537.36 (KHTML, like Gecko; compatible; Googlebot/2.1; +http://www.google.com/bot.html) Chrome/111.0.5563.110 Safari/537.36"
66.249.69.17 - - [04/Apr/2023:08:28:56 -0400] "POST /ajax/api/JsonRPC/CustomerAccounts/?CustomerAccounts[CustomerAccounts::getAccountDetails] HTTP/1.1" 200 348
"http://www.kochi.HEB.com/index.html" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Chrome/111.0.5563.110 Safari/537.36"
14.116.156.77 - - [04/Apr/2023:08:36:48 -0400] "GET / HTTP/1.1" 301 240 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1"
14.116.156.77 - - [04/Apr/2023:08:36:48 -0400] "GET /index.html HTTP/1.1" 200 21576 "http://www.HEB.com" "Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1"
68.191.149.136 - - [04/Apr/2023:08:39:50 -0400] "GET /search.asp?home=177&id=1%27%20or%201=@@version-- HTTP/1.1" 200 770 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36"
40.77.167.208 - - [04/Apr/2023:11:03:13 -0400] "GET /index.html HTTP/1.1" 200 21576 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; bingbot/2.0;
+http://www.bing.com/bingbot.htm) Chrome/103.0.5060.134 Safari/537.36"
52.167.144.27 - - [04/Apr/2023:11:03:27 -0400] "GET /files/main_style.css?1658455385 HTTP/1.1" 200 40213 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko;
compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm) Chrome/103.0.5060.134 Safari/537.36"
52.167.144.27 - - [04/Apr/2023:11:03:27 -0400] "GET /files/templateArtifacts.js?1658455385 HTTP/1.1" 200 7160 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko;
compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm) Chrome/103.0.5060.134 Safari/537.36"
52.167.144.27 - - [04/Apr/2023:11:03:27 -0400] "GET /files/theme/custom.js?1583952700 HTTP/1.1" 200 6512 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko;
compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm) Chrome/103.0.5060.134 Safari/537.36"
40.77.167.236 - - [04/Apr/2023:11:03:32 -0400] "GET /files/theme/plugins.js?1583952700 HTTP/1.1" 200 67464 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko;
```

2. How I found the malware on server 1 with the embedded IP address, using a YARA rule



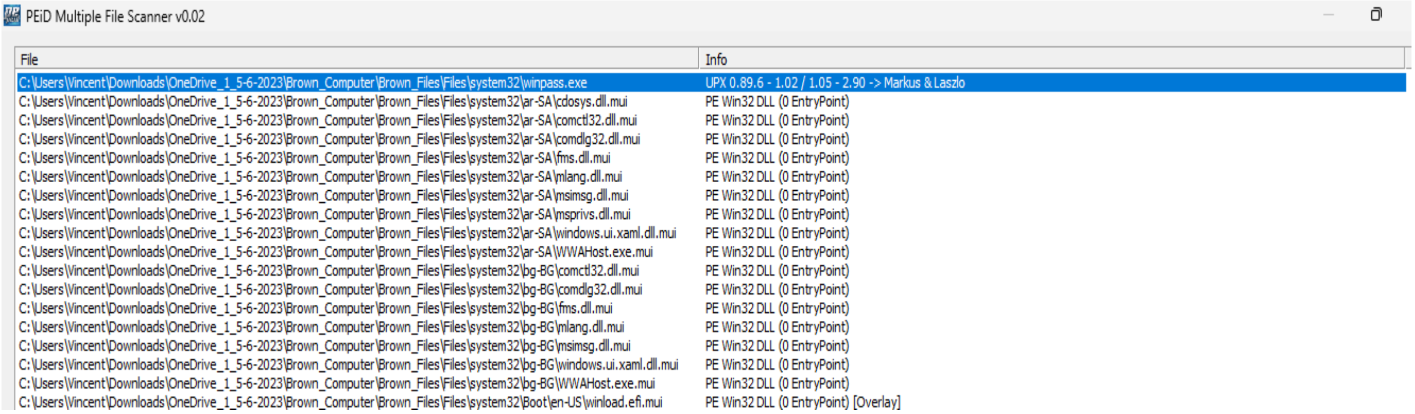
```
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\SERVER-1>cd SERVER-1

C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\SERVER-1\SERVER-1>yara64.exe find_IPAddress.yar -r Files -s
IP_Found Files\system32\Boot\en-US\winmedia.exe
0x4bf0:$s1: 68.191.149.136

C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\SERVER-1\SERVER-1>
```

3. How I found the countdown URL on server 1 using the bstring tool



```
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\SERVER-1\SERVER-1\Files\system32\Boot\en-US>bstrings.exe -f winmedia.exe --lr url3986
bstrings version 1.5.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/bstrings

Command line: -f winmedia.exe --lr url3986

Searching via RegEx pattern: ^
                [a-z][a-z0-9+\-.]*://                                # Scheme
                ([a-z0-9\-._~%!$&'()*+,;=]+@)?                       # User
                (?<host>[a-z0-9\-._~%]+                              # Named host
                |\[[a-f0-9:.]+\]                                     # IPv6 host
                |\[v[a-f0-9][a-z0-9\-._~%!$&'()*+,;=:]+\])           # IPvFuture host
                (:[0-9]+)?                                           # Port
                (/[a-z0-9\-._~%!$&'()*+,;=:@]+)*/?                   # Path
                (\?[a-z0-9\-._~%!$&'()*+,;=:@/?]*)?                  # Query
                (\#[a-z0-9\-._~%!$&'()*+,;=:@/?]*)?                  # Fragment
                $

Searching 1 chunk (512 MB each) across 25.007 KB in 'C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\SERVER-1\SERVER-1\Files\system32\Boot\en-US\winm
edia.exe'

Chunk 1 of 1 finished. Total strings so far: 500 Elapsed time: 0.031 seconds. Average strings/sec: 15,947
Primary search complete. Looking for strings across chunk boundaries...
Search complete.

Processing strings...

https://tinyurl.com/hebcountdown
```

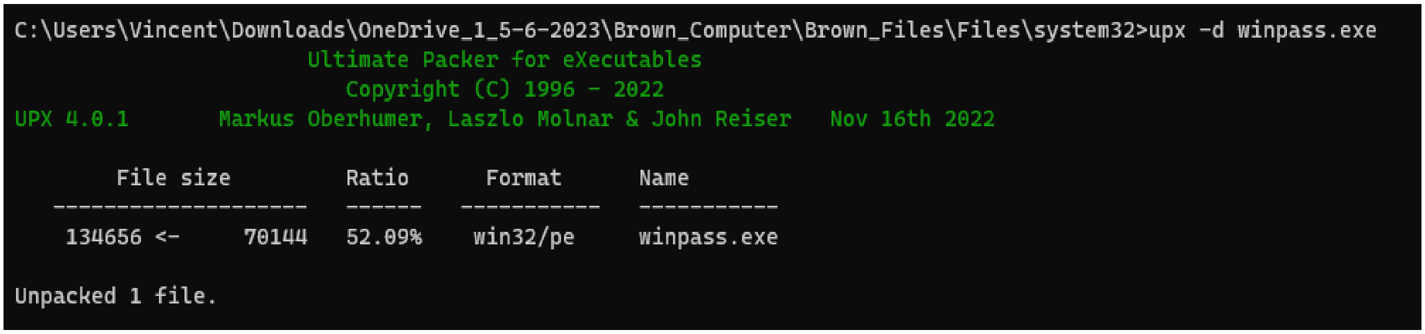
4. Location of the packed executable on Brown’s computer using PEiD to find UPX usage



PEiD Multiple File Scanner v0.02

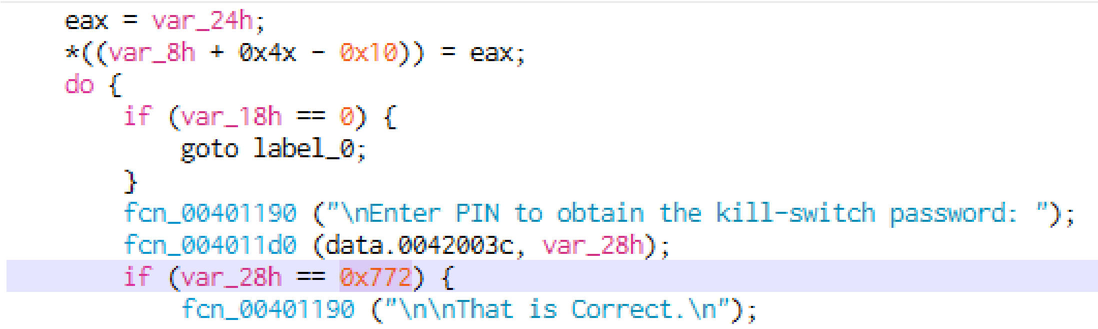
File	Info
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\winpass.exe	UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\ar-SA\cdosys.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\ar-SA\comctl32.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\ar-SA\comdlg32.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\ar-SA\fms.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\ar-SA\mlang.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\ar-SA\msimsg.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\ar-SA\msprivs.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\ar-SA\windows.ui.xaml.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\ar-SA\WWAHost.exe.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\bg-BG\comctl32.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\bg-BG\comdlg32.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\bg-BG\fms.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\bg-BG\mlang.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\bg-BG\msimsg.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\bg-BG\windows.ui.xaml.dll.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\bg-BG\WWAHost.exe.mui	PE Win32 DLL (0 EntryPoint)
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32\Boot\en-US\winload.efi.mui	PE Win32 DLL (0 EntryPoint) [Overlay]

5. Unpacking Brown’s executable using UPX



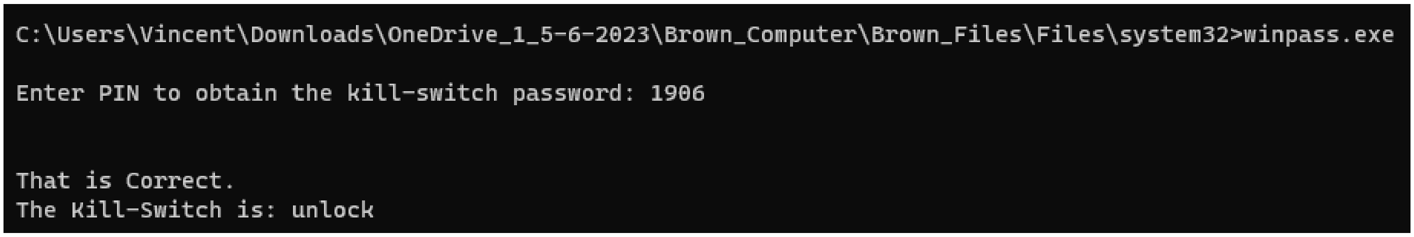
```
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32>upx -d winpass.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2022
UPX 4.0.1       Markus Oberhumer, Laszlo Molnar & John Reiser   Nov 16th 2022

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     134656 <-     70144   52.09%    win32/pe     winpass.exe

Unpacked 1 file.
```

6. Reverse engineering the PIN using Cutter, 0x772 = 1906



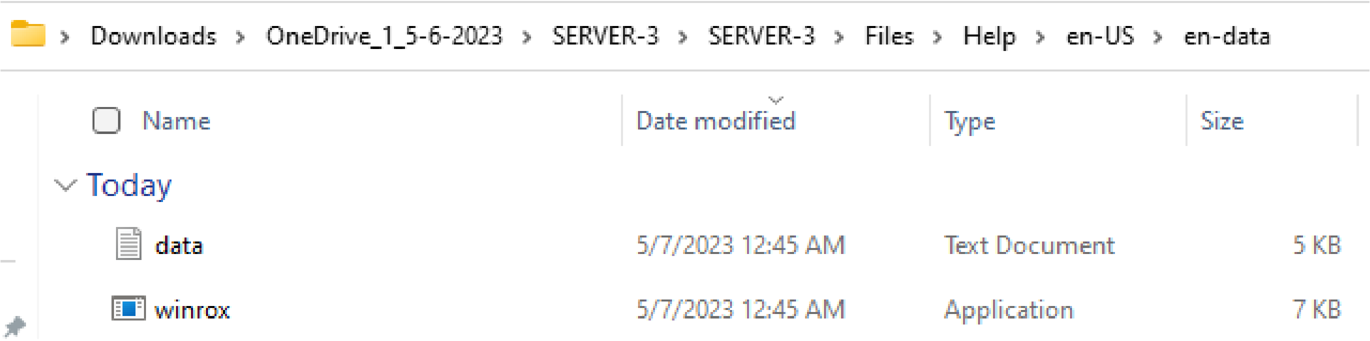
```
eax = var_24h;
*((var_8h + 0x4x - 0x10)) = eax;
do {
    if (var_18h == 0) {
        goto label_0;
    }
    fcn_00401190 ("\nEnter PIN to obtain the kill-switch password: ");
    fcn_004011d0 (data.0042003c, var_28h);
    if (var_28h == 0x772) {
        fcn_00401190 ("\n\nThat is Correct.\n");
```

7. Retrieving the kill switch by entering the password into the executable.



```
C:\Users\Vincent\Downloads\OneDrive_1_5-6-2023\Brown_Computer\Brown_Files\Files\system32>winpass.exe

Enter PIN to obtain the kill-switch password: 1906


That is Correct.
The Kill-Switch is: unlock
```

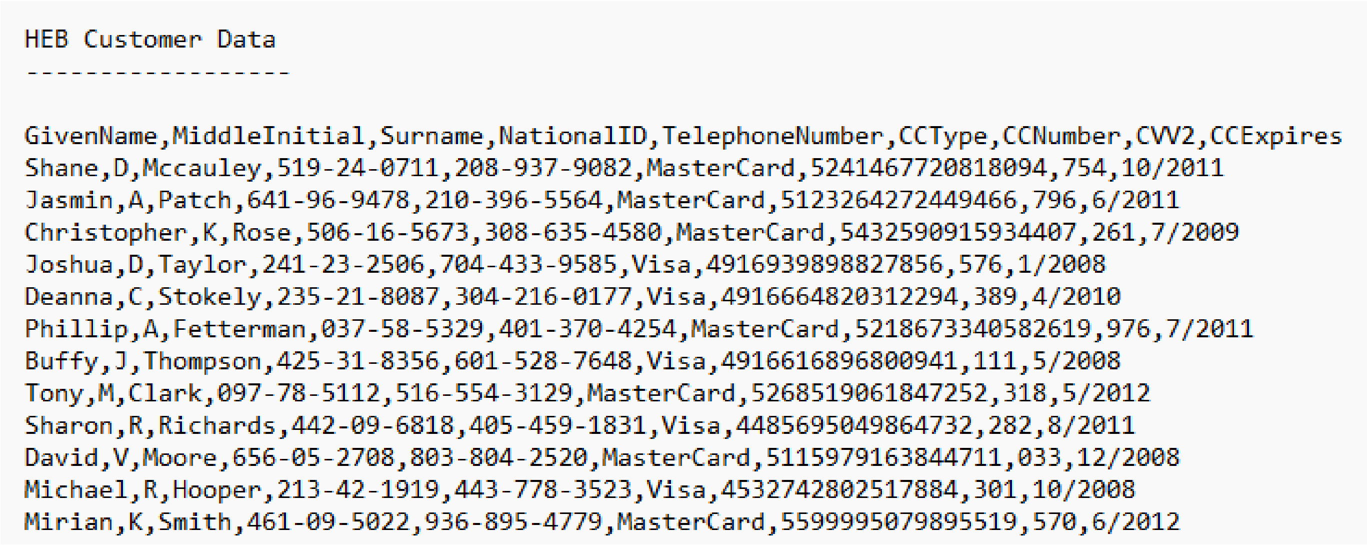
8. Path of renamed XOR tool and customer data, found using hashmyfiles and comparing the original XOR tool MD5 to the MD5 hashes in server 3 files.



Downloads › OneDrive_1_5-6-2023 › SERVER-3 › SERVER-3 › Files › Help › en-US › en-data

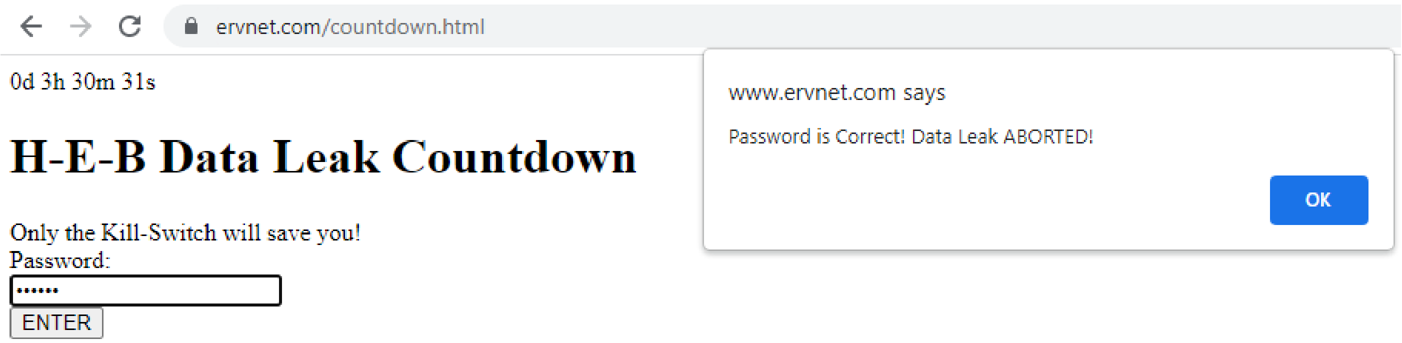
Name	Date modified	Type	Size
Today			
data	5/7/2023 12:45 AM	Text Document	5 KB
winrox	5/7/2023 12:45 AM	Application	7 KB

9. Screenshot of some of the decrypted HEB customer data



```
HEB Customer Data
------------------

GivenName,MiddleInitial,Surname,NationalID,TelephoneNumber,CCType,CCNumber,CVV2,CCExpires
Shane,D,Mccauley,519-24-0711,208-937-9082,MasterCard,5241467720818094,754,10/2011
Jasmin,A,Patch,641-96-9478,210-396-5564,MasterCard,5123264272449466,796,6/2011
Christopher,K,Rose,506-16-5673,308-635-4580,MasterCard,5432590915934407,261,7/2009
Joshua,D,Taylor,241-23-2506,704-433-9585,Visa,4916939898827856,576,1/2008
Deanna,C,Stokely,235-21-8087,304-216-0177,Visa,4916664820312294,389,4/2010
Phillip,A,Fetterman,037-58-5329,401-370-4254,MasterCard,5218673340582619,976,7/2011
Buffy,J,Thompson,425-31-8356,601-528-7648,Visa,4916616896800941,111,5/2008
Tony,M,Clark,097-78-5112,516-554-3129,MasterCard,5268519061847252,318,5/2012
Sharon,R,Richards,442-09-6818,405-459-1831,Visa,4485695049864732,282,8/2011
David,V,Moore,656-05-2708,803-804-2520,MasterCard,5115979163844711,033,12/2008
Michael,R,Hooper,213-42-1919,443-778-3523,Visa,4532742802517884,301,10/2008
Mirian,K,Smith,461-09-5022,936-895-4779,MasterCard,5599995079895519,570,6/2012
```

10. Successfully entering the kill switch password! Woohoo!



ervnet.com/countdown.html

0d 3h 30m 31s

H-E-B Data Leak Countdown

Only the Kill-Switch will save you!
Password:
••••••

www.ervnet.com says

Password is Correct! Data Leak ABORTED!