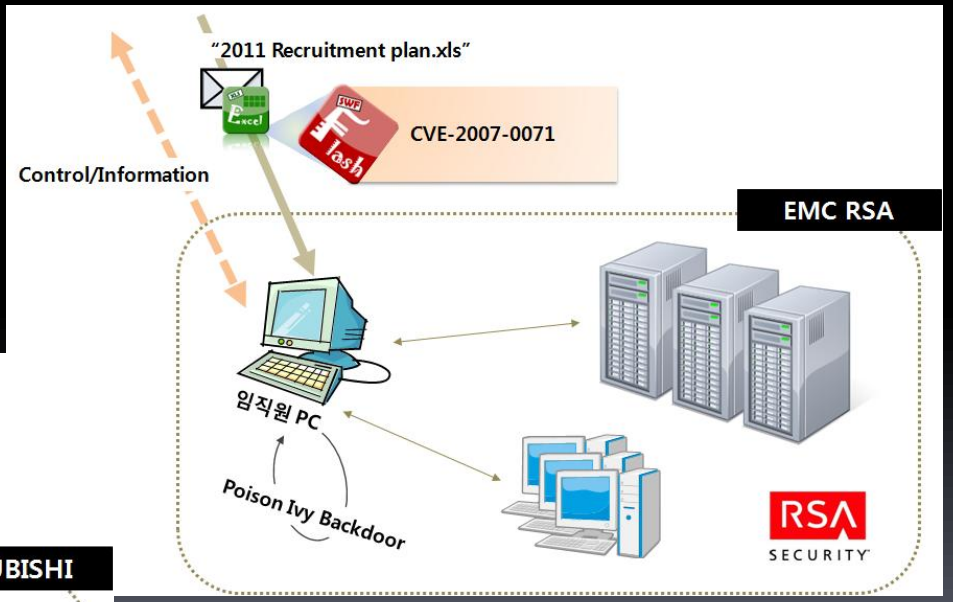
Flash 파일 속 새빨간 거짓말 파헤치기

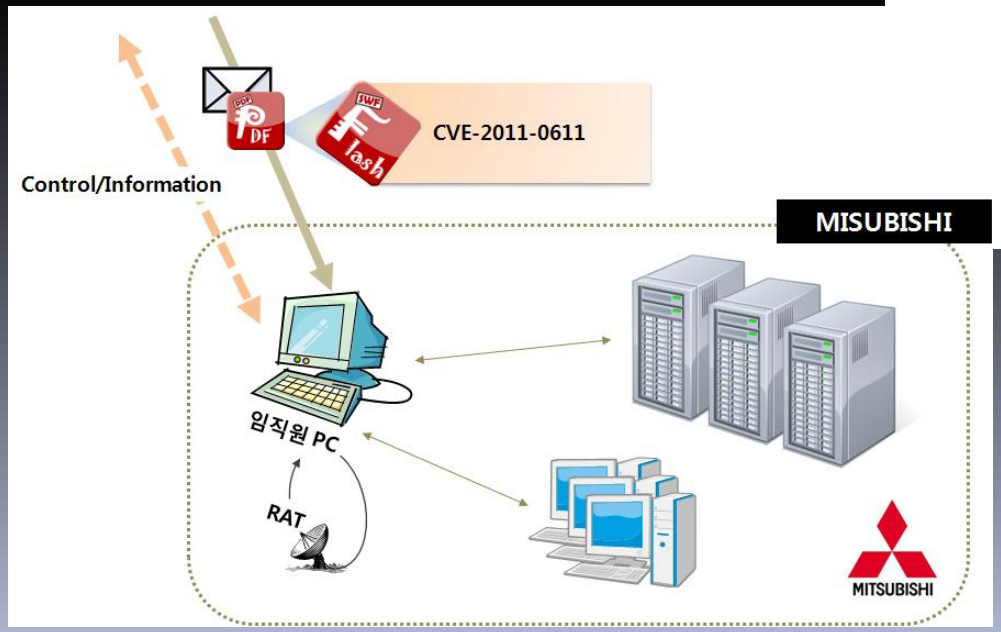
RedHidden

E-Mail : redhidden00@gmail.com
Blog : Redhidden.net

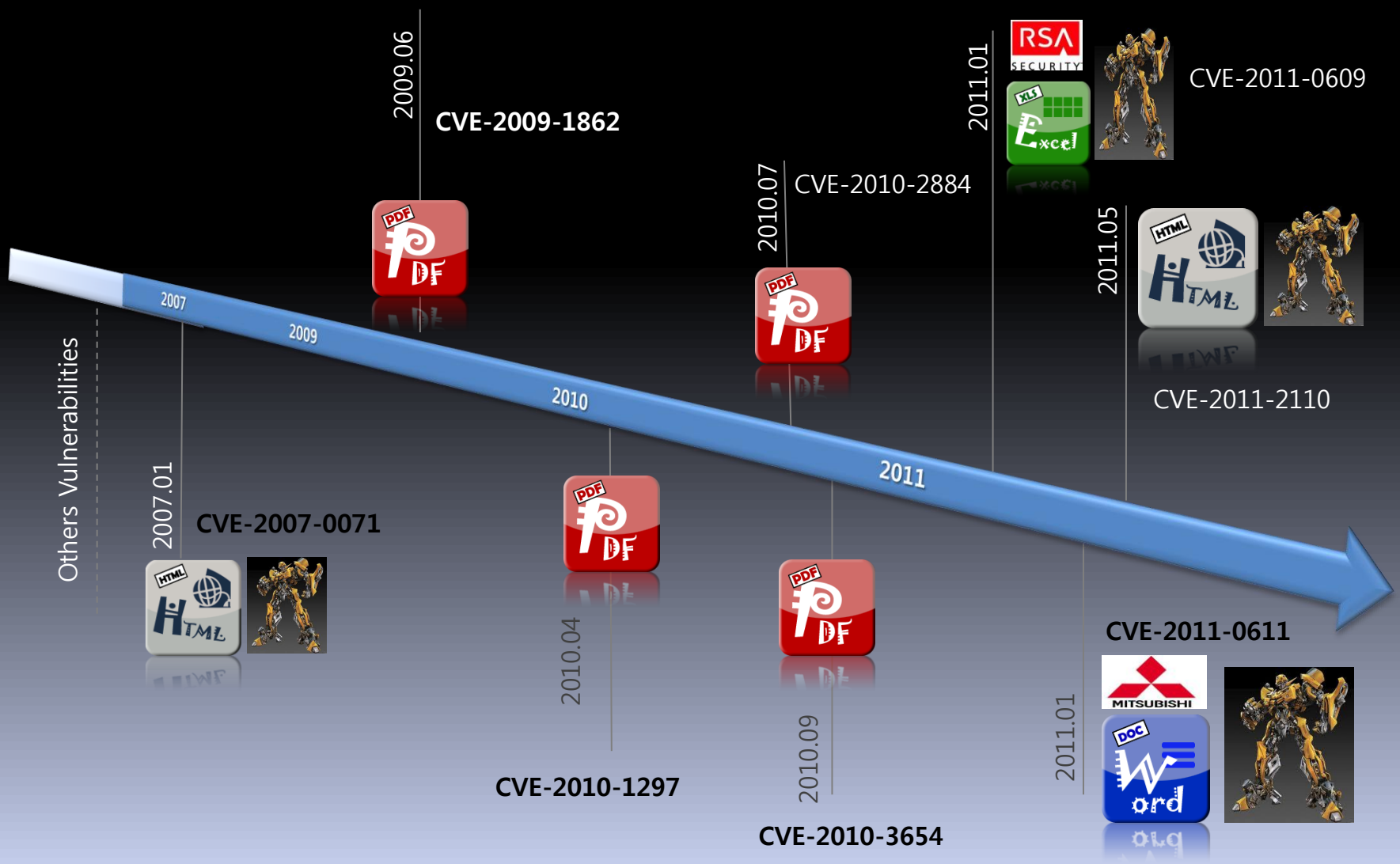
Why ??

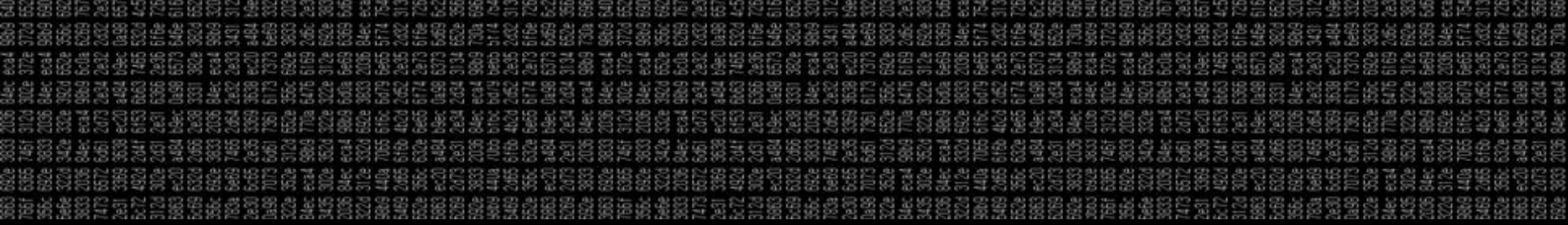
Cases of "APT" attack with Flash





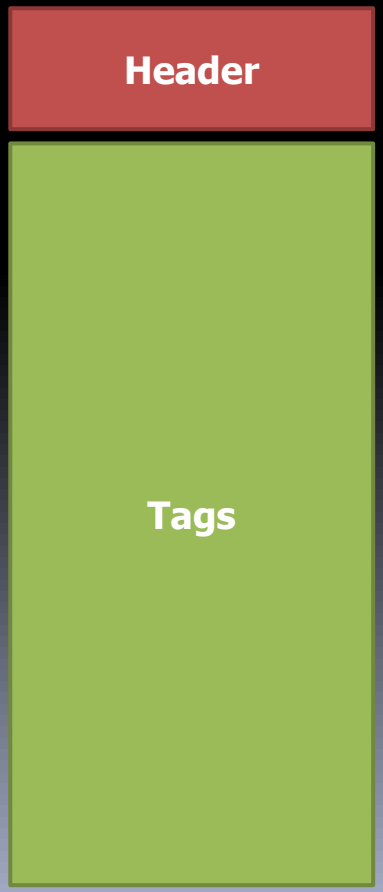
Known Flash Vulnerabilities(History)





What ??

What is FLASH ...



The SWF (pronounced "swiff ") file format delivers vector graphics, text, video, and sound over the Internet, supported by Adobe® Flash® Player software.

- **Network Delivery**
- **Scriptability**

SWF File Format Version 10
ActionScript 3.0 (AS 3.0)
ActionScript Virtual Machine 2 (AVM2)
(Starting with SWF 9, AS 3.0 language + AVM2)

What is FLASH ...

SWF File Header

- Signature (UI8*3) : “FWS”/“CWS”
- Version (UI8)
- FileLength (UI8)
- FrameSize (RECT)
- FrameRate (UI16)
- FrameCount (UI16)

What is FLASH ...

SWF TAG

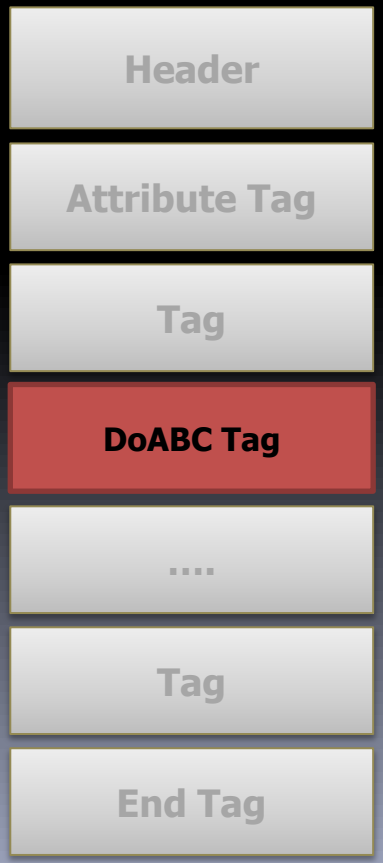
Definition Tag

Control Tag

RECORDHEADER = tag type + length

- Short RECORDHEADER
- Long RECORDHEADER

What is FLASH ...

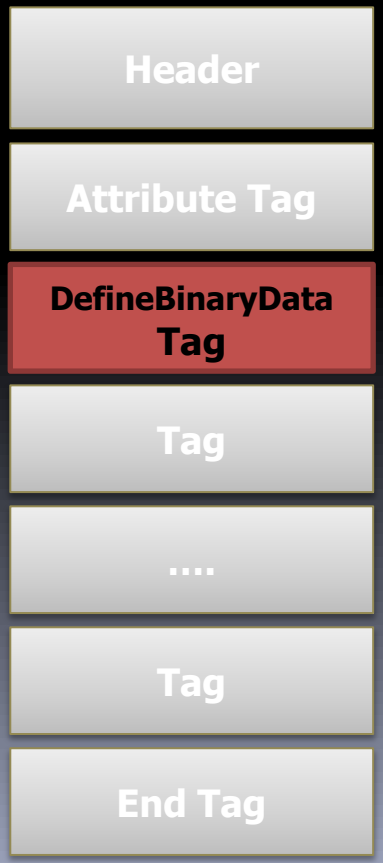


Flash Action Model(9)

DoAction tag (.abc bytecode block)

- RECORDHEADER(type=82)
- Flags (UI32)
- Name (STRING)
- ABCData (Byte[])

What is FLASH ...



Flash Binary Data

DefineBinaryData tag

- SWF 9, definition tag

- RECORDHEADER(type=87)
- Tag(UI16)
- Reserved(UI32)
- Data (BINARY)

How ??

What is “Analysis of Vulnerability” …

“Not a Destination,
it’s a Method for it !!!”

Destination

File based Detection
Network based Detection
Inline-Patch
Others…

4 Points

0x00 ---------- Input ?
0x01 ----- Crash/EIP control ?
0x02 ---------- ShellCode ?
0x03 ---- Malicious Content ?

Containers of Flash

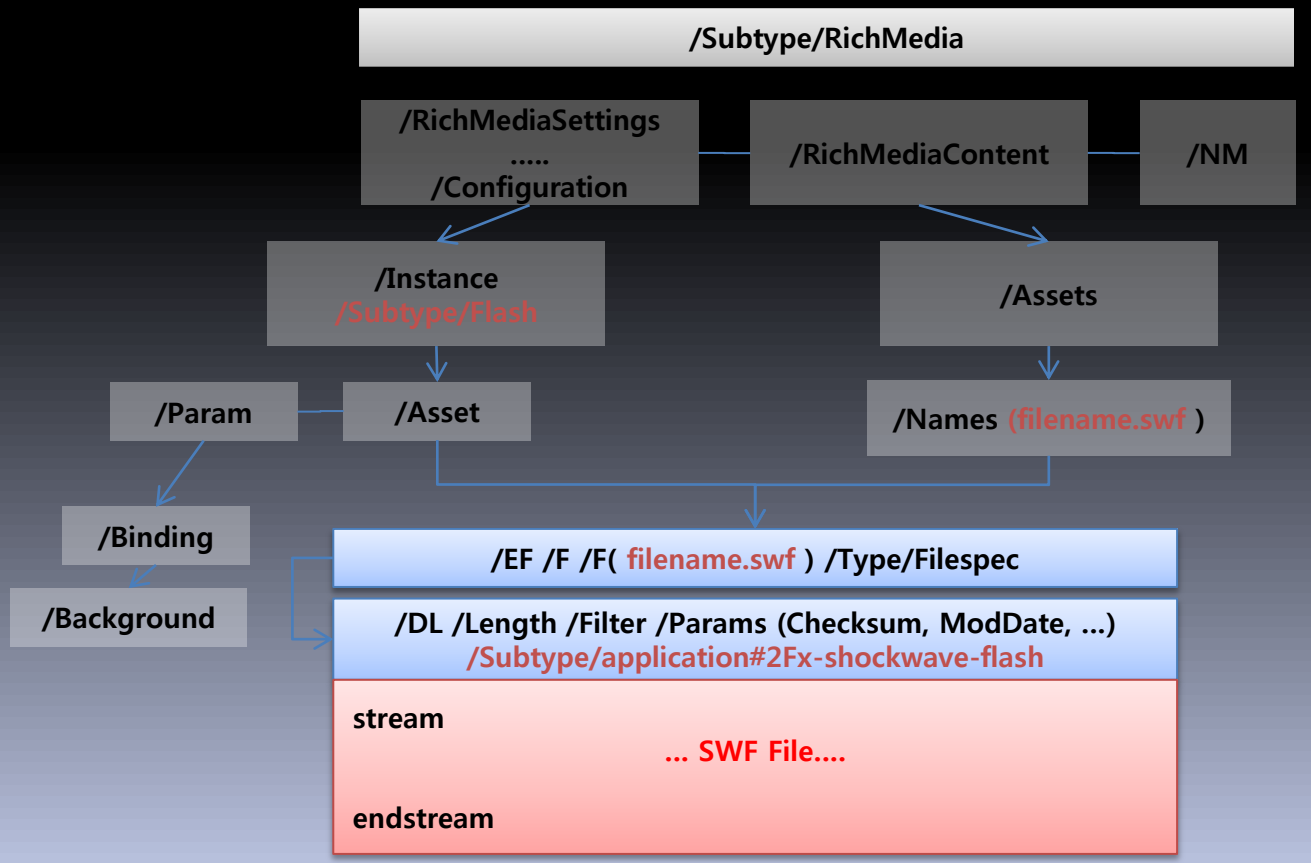
- Easy to Fake
- Low Security Policy
- Large Space

Flash in HTML


```
1  <html>
2  <body>
3  <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" codeba
4  width="668" height="100"  id="mymoviename">
5  <param name="movie"  value="security_     .swf" />
6  <param name="quality" value="high" />
7  <param name="bgcolor" value="#ffffff" />
8  <embed src="security_asec.swf" quality="high" bgcolor="#ffffff" wid
9  </embed>
10 </object>
11 </body>
12 </html>
```

Flash in PDF

The rich media annotation means that Flash applications, video, audio, and other multimedia can be attached to a PDF document. (*ExtensionLevel 3*)



Flash In Word/Excel

File name: D:₩임지₩문서1.doc

- 문서1.doc
  - Summary Info
  - Document Summary Info
  - Data
  - 1Table
  - ┌CompObj
  - WordDocument
  - Macros
  - ObjectPool
    - _1374519309
      - OCXDATA
      - ┗ObjInfo
      - ┗OCXNAME
      - Contents
      - OCXPROPS
    - _1374519310
      - OCXDATA
      - ┗ObjInfo
      - ┗OCXNAME
      - Contents
      - OCXPROPS
  - MsoDataStore
    - ÄÝÙÙHËG1ÙEÒCAÀÍ1M2Q
      - Item
      - Properties

General | Stream Data

Display mode: Hexadecimal Insert mode: Overwrite

```
00000000: 67 55 66 55 00 09 00 00 D8 13 00 00 D8 13 00 00  gUfU....Ø...Ø...
00000010: 08 00 02 00 00 00 00 00 08 00 2A 00 00 00 65 00  ..........*...e.
00000020: 3A 00 5C 00 73 00 65 00 63 00 75 00 72 00 69 00  :.\.s.e.c.u.r.i.
00000030: 74 00 79 00 5F 00 61 00 73 00 65 00 63 00 2E 00  t.y._.a.s.e.c...
00000040: 73 00 77 00 66 00 00 00 08 00 2A 00 00 00 65 00  s.w.f.....*...e.
00000050: 3A 00 5C 00 73 00 65 00 63 00 75 00 72 00 69 00  :.\.s.e.c.u.r.i.
00000060: 74 00 79 00 5F 00 61 00 73 00 65 00 63 00 2E 00  t.y._.a.s.e.c...
00000070: 73 00 77 00 66 00 00 00 08 00 0E 00 00 00 57 00  s.w.f.........W.
00000080: 69 00 6E 00 64 00 6F 00 77 00 00 00 08 00 04 00  i.n.d.o.w.......
00000090: 00 00 30 00 00 00 08 00 06 00 00 00 2D 00 31 00  ..0.........-.1.
000000A0: 00 00 08 00 0A 00 00 00 48 00 69 00 67 00 68 00  ........H.i.g.h.
000000B0: 00 00 08 00 02 00 00 00 00 00 08 00 06 00 00 00  ................
000000C0: 2D 00 31 00 00 00 08 00 2A 00 00 00 65 00 3A 00  -.1.....*...e.:.
000000D0: 5C 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00  \.s.e.c.u.r.i.t.
000000E0: 79 00 5F 00 61 00 73 00 65 00 63 00 2E 00 73 00  y._.a.s.e.c...s.
000000F0: 77 00 66 00 00 00 08 00 02 00 00 00 00 00 08 00  w.f.............
00000100: 10 00 00 00 53 00 68 00 6F 00 77 00 41 00 6C 00  ....S.h.o.w.A.l.
00000110: 6C 00 00 00 08 00 04 00 00 00 30 00 00 00 08 00  l.........0.....
00000120: 04 00 00 00 30 00 00 00 08 00 02 00 00 00 00 00  ....0...........
00000130: 08 00 00 00 00 00 08 00 02 00 00 00 00 00 0D 00  ................
00000140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000150: 08 00 04 00 00 00 31 00 00 00 08 00 04 00 00 00  ......1.........
00000160: 30 00 00 00 08 00 00 00 00 00 08 00 04 00 00 00  0...............
00000170: 30 00 00 00 08 00 08 00 00 00 61 00 6C 00 6C 00  0.........a.l.l.
00000180: 00 00 08 00 0C 00 00 00 66 00 61 00 6C 00 73 00  ........f.a.l.s.
```

Offset: 0x00000100 (256)

Main Flash Vulnerabilities

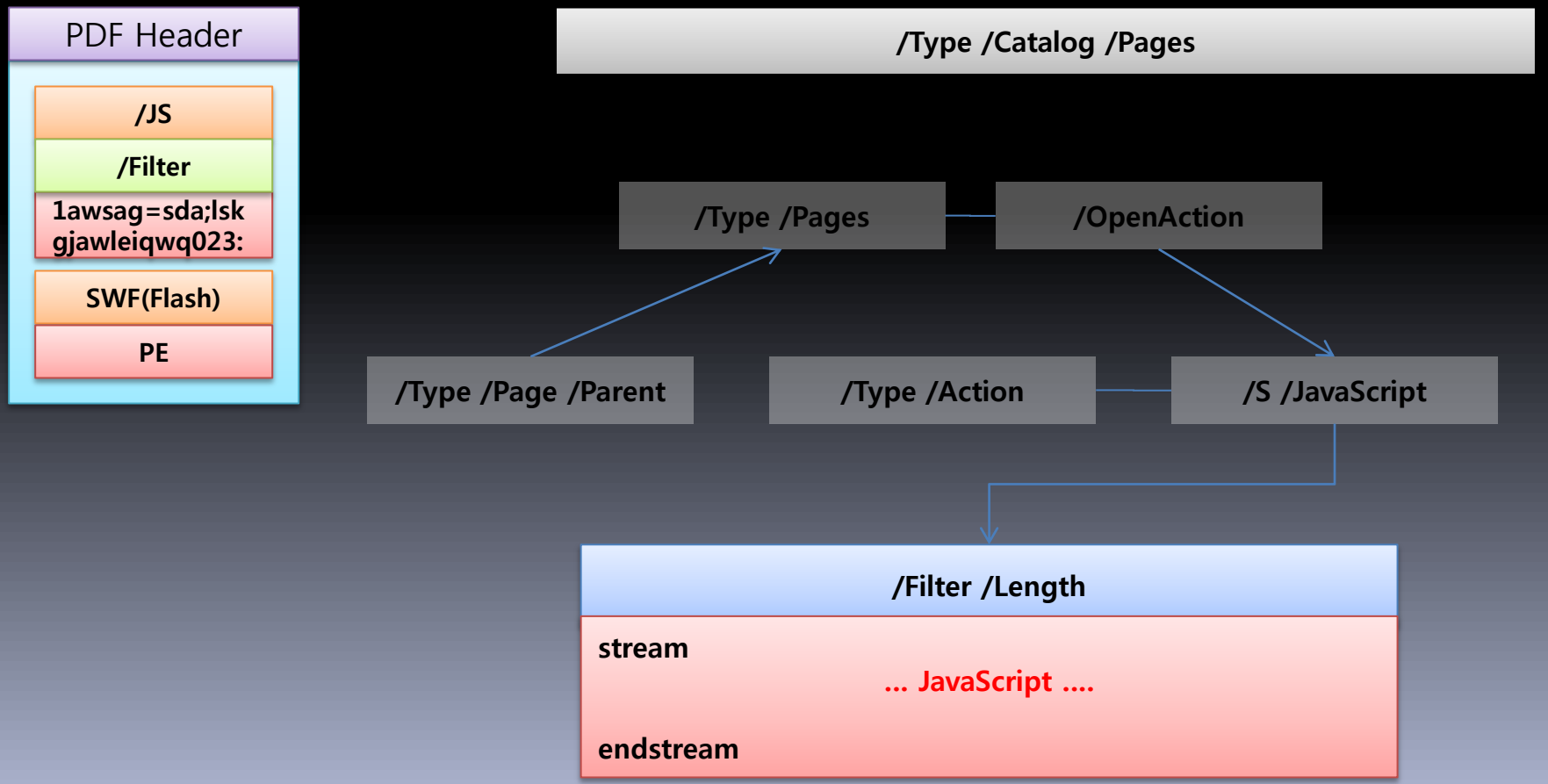
- Bug in SWF File Format (CVE-2007-0071)
- Bug in Action Script (CVE-2010-1297)
- Others…

Complexity To Simplicity

ShellCode

- Other contents in File
- HeapSpray
  - JavaScript (HTML)
  - AcroJS (PDF)
  - ActionScript (Flash)

HeapSpray – PDF(AcroJS)



HeapSpray – Flash(ActionScript)

```
public var array:Array;

public function sample2()
{
    addFrameScript(0, this.frame1);
    return;
}// end function

function frame1()
{
    this.a = unescape("%u0d0d%u0d0d");
    this.t = this.a;
    this.b = unescape("%u0d0d%u0d0d%u0d0d%u0d0d%u0d0d%u0d0d%u0d0d%u0d0d%u0d0d%u0d0d%u0d0d%u0d0d%u0d0d%u0
    this.len = 1048576 - this.b.length - 256;
    while (this.a.length < this.len)
    {
        // label
        this.a = this.a + this.t;
    }// end while
    this.a = this.a + this.b;
    this.array = new Array();
    this.i = 0;
    while (this.i < 200)
    {
        // label
        this.array[this.i] = new ByteArray();
        this.array[this.i].writeMultiByte(this.a, "unicode");
        this.i = this.i + 1;
        // label
    }// end while
```

Advanced Malicious Features

- Execution Constraint
  - Environment Check
  - Security Setting
- Dynamic construction(Reconstruction)
  - Using an External Parameter
  - Interaction with the External JavaScript
  - Creating a SWF Dynamically
- Obfuscation/Encryption

Conclusion

- Flash have two-sides (Useful vs. Malicious)
- Document File Analysis (including flash) could be important starting point for Incident Analysis.
- Malicious flash has been advanced such as malicious code.
- In the future, i will study about symptoms and signs, when a malicious document file is executed, from forensic perspective.

Q&A