Recognizing the Exploit Vector

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER

@jareddemott www.vdalabs.com

Overview

Typical exploitation scenarios

Show steps to determine exploit vector

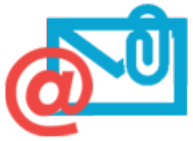
Analyze malware sample

ANATOMY OF A SPEAR PHISHING ATTACK

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.



4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

6. The email is opened because they 'know' the sender.

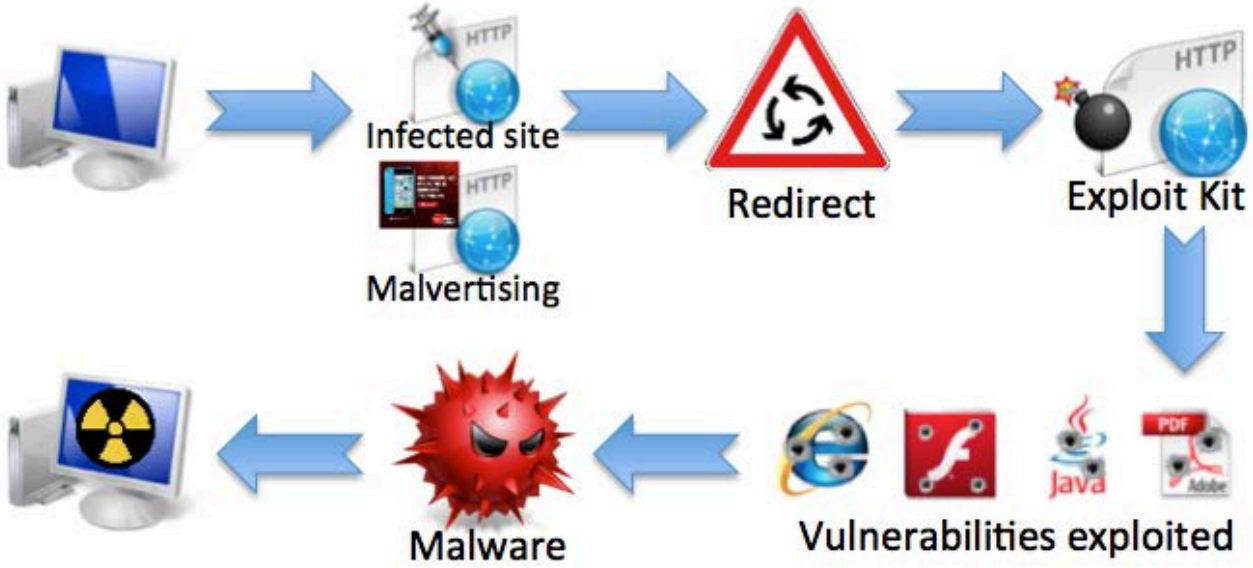
7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

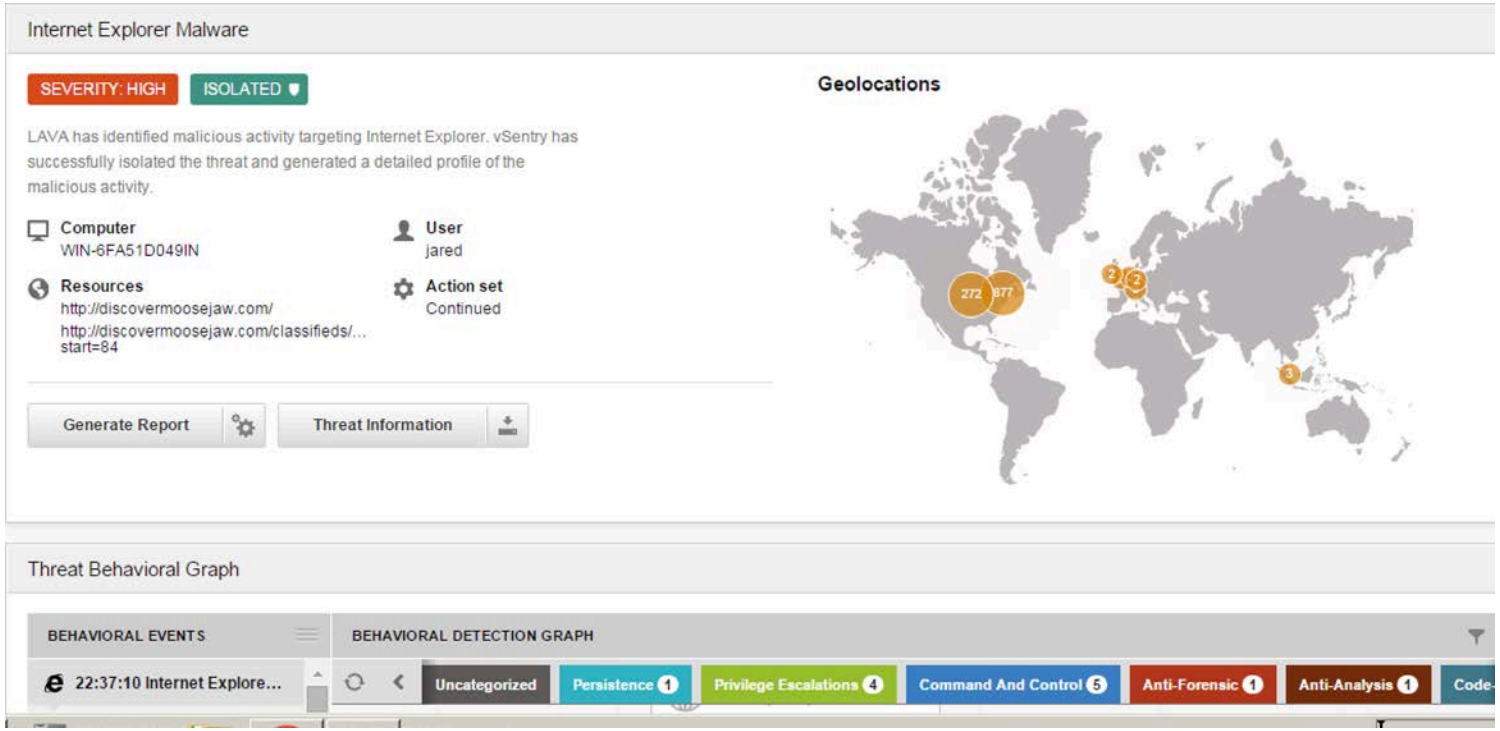
8b. Opened attachment causes malware to infect the computer/ smartphone/network.

9. The hacker uses the backdoor to steal information

Drive-by


HTTP
Infected site
HTTP
Malvertising
Redirect
HTTP
Exploit Kit
Java
PDF
Adobe
Vulnerabilities exploited
Malware

Real sample from the wild



Can we determine what the exploit was?

22:46:57 Network
22:46:57 Network
22:47:01 Network
22:47:05 Network
22:47:05 Network
22:47:10 Network
22:47:12 Network
22:47:12 Invoked
22:47:27 Invoked
22:47:27 Invoked
22:47:27 Dropped and Executed
22:47:28 Dropped and Loaded
22:47:29 Registry Settings Upd...
22:47:29 Dropped DLL Deleted
22:47:29 Process Opened
22:47:29 Shellcode Injection
22:47:32 Privilege Escalations ...
22:47:32 Privilege Escalations

Uncategorized | Persistence 1 | Privilege Escalations 4 | Command And Control 5 | Anti-Forensic 1 | Anti-Analysis 1 | Co

conhost.exe

Network
Nov 27, 2015, 22:47:10
iexplore.exe

Network
Nov 27, 2015, 22:47:12
iexplore.exe

Invoked
Nov 27, 2015, 22:47:27
regsvr32.exe

Dropped and Executed
Nov 27, 2015, 22:47:27
TMPAA04.tmp

Registry Settings Updated...
Nov 27, 2015, 22:47:29
{FF76ABD7-C401-47AD-B64C-...

Process Opened
Nov 27, 2015, 22:47:29
uXenClipboard.exe

Privilege Escalations thr...
Nov 27, 2015, 22:47:32

Dropped and Executed
File size: 275536
MD5 checksum: 0983FFA855D8AB95854D7ECB616F02E1
SHA1 checksum: 9BAAB72574324AB80BA7FF58822FAE4D9CD0550A

22:45:00 22:46:00 22:47:00 22:50:00

Privilege Escalations thr...

HTML?

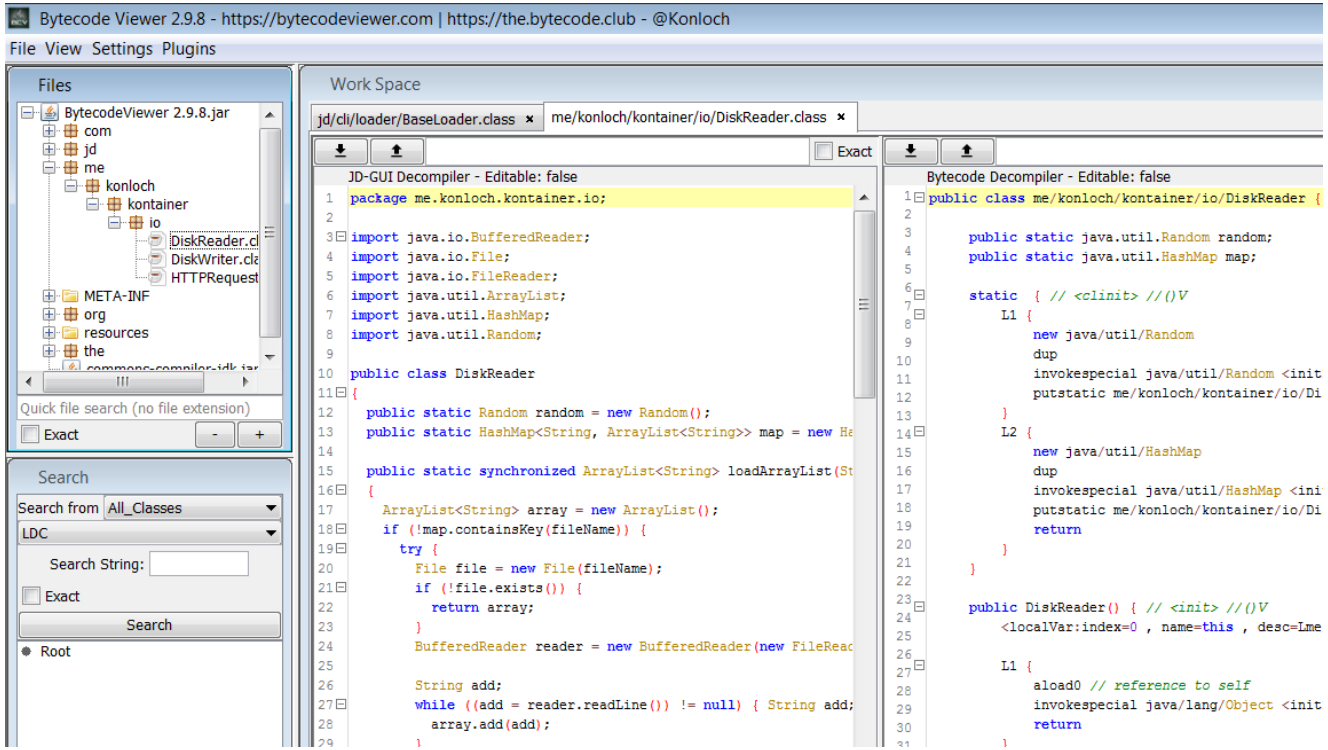
Jar?

SWF?

JS Detox

Cerbero Profiler

My first choice for viewing jar files



My first choice for viewing SWF files

Open... | Save | Save as... | Save as Exe... | Reload | Close | Close all
File

Export to FLA | Export SWF XML | Export all parts | Export selection
Export

Import SWF XML | Import text | Import script | Import Symbol-Class
Import

Run (F6) | Debug (CTRL+F5) | Stop
Start

Resources | Hex dump
View

own3d[1].swf
- header
- frames
- others
- scripts
  - DebugUtils
  - Main
  - MyClass
  - MyClass1
  - MyClass2
  - MyUtils
  - ShellWin32

Traits | Constants

- private function init(param1:Event = null) : void
- instance initializer
- class initializer

ActionScript source

Main

```
5
6   public class Main extends Sprite
7   {
8
9       public function Main()
10      {
11          super();
12          if(stage)
13          {
14              this.init();
15          }
16          else
17          {
18              addEventListener(Event.ADDED_TO_STAGE,this.init);
19          }
20      }
21
22      private function init(param1:Event = null) : void
23      {
24          removeEventListener(Event.ADDED_TO_STAGE,this.init);
25          MyClass.TryExpl();
26      }
27  }
28 }
```

Edit (Experimental)

Method/Getter/Setter

init

```
1  trait method Qna
2  method
3  name null
4  flag HAS_OPTIONA
5  flag HAS_OPTIONA
6  param Qname(Pack
7  optional null
8  returns Qname(Pa
9
10 body
11 maxstack 3
12 localcount 2
13 initscopedepth 9
14 maxscopedepth 10
15
16 code
17 getlocal_0
18 pushscope
19 findpropstrict Q
20 getlex Qname(Pac
21 getproperty Qnam
22 getlocal_0
23 getproperty Qnam
24 callpropvoid Qna
```

Edit

What files are in our case study?

```
jared@WIN-6FA51D049IN /c/Users/jared/Desktop/ExamineAlerts/moose/files
$ file * | wc -l
1412

jared@WIN-6FA51D049IN /c/Users/jared/Desktop/ExamineAlerts/moose/files
$ file * | grep -i htm | wc -l
92

jared@WIN-6FA51D049IN /c/Users/jared/Desktop/ExamineAlerts/moose/files
$ file * | grep -i swf
en-728x90-hd-BlackFriday-Flyer-wk43[1].swf:
                              Macromedia Flash data (compressed), version 9
limit[1].swf:
                              Macromedia Flash data (compressed), version 13

jared@WIN-6FA51D049IN /c/Users/jared/Desktop/ExamineAlerts/moose/files
$ file * | grep -i java

jared@WIN-6FA51D049IN /c/Users/jared/Desktop/ExamineAlerts/moose/files
$
```

53318	22:47:03	FileMon	\program files (x86)\internet explorer\iexplore.exe (2028)	MODIFIED \Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\MJ280M1Y\limit[1].swf	EventType=65536, EvAction=BRO_RULE_ACTION_ALLOW, EvRuleID=0	Unknown

\program files (x86)\internet explorer\iexplore.exe

Geolocation

95.211.205.229

Netherlands

Invoked

\Windows\syswow64\regsvr32.exe "C:\windows\SysWOW64\regsvr32.exe -s "C:\Users\bruser1729\AppData\Local\Temp\{EBAB6D64-C85A-4316-8C91-A08274E2730E}\api-ms-win-system-umpo-l1-1-0.dll""

Invoked

\Windows\syswow64\regsvr32.exe "C:\windows\SysWOW64\regsvr32.exe -s "C:\Users\bruser1729\AppData\Local\Temp\{23F1EF22-CF34-4E1A-A11C-0BCE4BFD39FA}\apds62.dll""

Network

Nov 27, 2015, 22:47:12

iexplore.exe

Invoked

Nov 27, 2015, 22:47:27

regsvr32.exe

Dropped and Executed

Nov 27, 2015, 22:47:27

TMPAA04.tmp

Registry Settings Updated...

Nov 27, 2015, 22:47:29

{FF76ABD7-C401-47AD-B64C-...

Process Opened

Nov 27, 2015, 22:47:29

uXenClipboard.exe

Privilege Escalations thr...

Nov 27, 2015, 22:47:32

MD5 checksum: 0983FFA855D8AB95854D7ECB616F02E1

SHA1 checksum: 9BAAB72574324AB80BA7FF58822FAE4D9CD0550A

\Windows\System32\conhost.exe -> \Users\bruser1729\AppData\Local\Temp\{2669969D-4E7A-4A6A-A030-7A40E54BF42F}\TMPAA04.tmp

22:45:00 22:46:00 22:47:00

```
_____________________________________________________________________________________
PROCESS INVOCATIONS
_____________________________________________________________________________________
| 22:47:12   | iexplore.exe         | Execute Windows\System32\conhost.exe C:\windows\system32\conhost.exe |
| 22:47:27   | conhost.exe          | Execute Windows\syswow64\regsvr32.exe C:\windows\SysWOW64\regsvr32.exe -s
"C:\Users\bruser1729\AppData\Local\Temp\{EBAB6D64-C85A-4316-8C91-A08274E2730E}\api-ms-win-system-umpo-l1-1-0.dll" |
| 22:47:27   | conhost.exe          | Execute Windows\syswow64\regsvr32.exe C:\windows\SysWOW64\regsvr32.exe -s
"C:\Users\bruser1729\AppData\Local\Temp\{23F1EF22-CF34-4E1A-A11C-0BCE4BFD39FA}\apds62.dll" |
| 22:47:27   | conhost.exe          | Execute Users\bruser1729\AppData\Local\Temp\{2669969D-4E7A-4A6A-A030-7A40E54BF42F}\TMPAA04.tmp
C:\Users\bruser1729\AppData\Local\Temp\{2669969D-4E7A-4A6A-A030-7A40E54BF42F}\TMPAA04.tmp |
| 22:48:41   | iexplore.exe         | Execute Windows\syswow64\regsvr32.exe C:\windows\SysWOW64\regsvr32.exe |
_____________________________________________________________________________________
```

- DefineButton2 (78)
- DefineButton2 (79)
- DefineButton2 (80)
- DefineButton2 (81)
- DefineButton2 (82)
- DefineSprite (23)
- DefineSprite (38)
- DefineSprite (49)
- DefineSprite (55)
- DefineSprite (60)
- frame 1
  - PlaceObject2 (3: Enabler) (: Enabler
  - DoAction
- frame 119

Basic tag info

Name	Value
Tag Type	DoAction (12)
Offset	1366 (0x556)
Length	484 (0x1e4)

ActionScript source

```
function my_delayedFunction()
{
   if(arrowClicked == false)
   {
      play();
   }
}
container1.exit_btn.onRelease = function()
{
   enabler.exit("Product_Exit_1");
   trace("exit1");
};
container2.exit_btn.onRelease = function()
{
   enabler.exit("Product_Exit_2");
   trace("exit2");
};
container3.exit_btn.onRelease = function()
{
   enabler.exit("Product_Exit_3");
   trace("exit3");
};
container4.exit_btn.onRelease = function()
{
   enabler.exit("Product_Exit_4");
   trace("exit4");
};
var count = 0;
var delay = 3500;
var arrowClicked = false;
```

Edit (Experimental)

P-code source

```
ConstantPool "arrowClicked" "container1" "exit_btn"
DefineFunction "my_delayedFunction" 0  {
Push "arrowClicked"
GetVariable
Push false
Equals2
Not
If loc00eb
Play
}
loc00eb:Push "container1"
GetVariable
Push "exit_btn"
GetMember
Push "onRelease"
DefineFunction "" 0  {
Push "Product_Exit_1" 1 "enabler"
GetVariable
Push "exit"
CallMethod
Pop
Push "exit1"
Trace
}
SetMember
Push "container2"
GetVariable
Push "exit_btn"
GetMember
Push "onRelease"
DefineFunction "" 0  {
```

Edit

limit[1].swf
- header
- binaryData
- frames
- others
- scripts
  - §1111§
  - llll
  - l111

Traits | Constants

- private var ll1ll:String = "4Fgbspl50L3n8";
- private var llll;
- private function llll1(param1:Object = null) : v
- public function ll11() : int
- private function llll() : *
- public function llll(param1:*) : *

ActionScript source

l111

```
27      private function lIll1(param1:Object = null) : void
28      {
29         this[Illl.§1II1§](Illl.IIll,this.lIll1);
30         this.llll1();
31      }
32
33      public function lll1() : int
34      {
35         var _loc1_:* = "someString|someOtherPart|oneMorePart";
36         var _loc2_:Array = _loc1_.split("|");
37         var _loc3_:* = new §1111§();
38         _loc3_[Illl.I1111]();
39         _loc3_ = this.lllI(_loc3_);
40         var _loc4_:* = new (this.llII[Illl.§11II§](Illl.§1III§) as Class)();
41         _loc4_[Illl.lIIl](_loc3_);
42         this[Illl.§1II1§](_loc4_);
43         return -1;
44      }
45
46      private function lIII() : *
47      {
48         var _loc3_:uint = 0;
49         var _loc1_:* = new (this.llII[Illl.§11II§](Illl.I1lI) as Class)();
50         var _loc2_:* = 0;
```

Edit (Experimental)

Method/Gett

ll11

```
1  trait me
2  method
3  name nul
4  returns
5
6  body
7  maxstack
8  localcou
9  initscop
10 maxscope
11
12 code
13 getlocal
14 pushscop
15 pushstri
16 setlocal
17 getlocal
18 pushstri
19 callprop
20 coerce Q
21 setlocal
22 findprop
23 construc
24 coerce a
```

Main.as | exploit.as | bytearray.as

```
32      }
33
34      public function ExploitCode() : int
35      {
36          var _loc1_:* = "someString|someOtherPart|oneMorePart";
37          var _loc2_:Array = _loc1_.split("|");
38          var secretResourceToLoad:* = new bytearray();
39          //trace( secretResourceToLoad);
40          secretResourceToLoad[exploit.uncompress]();
41          //trace( secretResourceToLoad );
42          secretResourceToLoad = this.moreDecoding(secretResourceToLoad);
43          trace("secretResourceToLoad = " + secretResourceToLoad );
44          var loader:* = new (this.llII[exploit.getDefinition](exploit.flash_display_Loader) as Class)();
45          loader[exploit.loadBytes](secretResourceToLoad);
46          trace( "loader=" + loader );
47          //this[exploit.addChild](loader);
48          return -1;
49      }
50
51      private function decodeSecret() : *
52      {
53          var _loc3_:uint = 0;
```

Project

- moose_fd_proj (AS3)
  - References
  - bin
  - src
    - bytearray.as
    - exploit.as
    - Main.as

JSDetox Analysis About

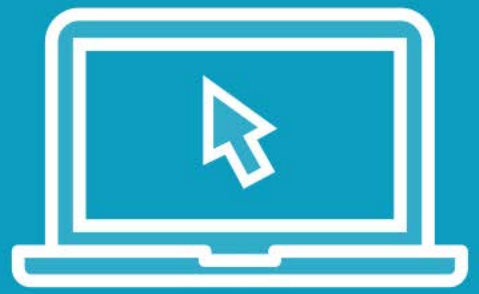
Send up

Formatted Edit

```
var dIWQnuWUTCcE;
var LBqLJpIGKmP = function() {
  if(typeof jQuerry === "string") {

  }
  var target = arguments[0] || { }, i = 1, length = arguments.length, deep = false;
  if(typeof target === "boolean") {
    deep = target;
    target = arguments[i] || { };
    i++;
  }
};
var KQrZSMyngFWA, fsbnivBGGL;
var zoFjRbTiTDef;
var eAyySf = 'sb', jX5 = 'e';
var mM = "replace";
fsbnivBGGL = 'str';
fsbnivBGGL = "substr";
var EHs4d = 'pro' + 'yo'["replace"]('y', 't') + 'type';
var oi = this['Array'][EHs4d];
var rxRb3 = 'ex';
rxRb3 = "Ridex";
if(!oi["Ridex"]) {
  oi[rxRb3] = (function(H9vaw, Bgs) {
    var BqS = 'ngth';
    BqS = "length";
    for(var hXevH = Bgs || 0, ETo = this[BqS]; hXevH < ETo; hXevH++) {
      if(this[hXevH] === H9vaw) {
        return hXevH;
```

Demo



Lets see the tools in action

Summary

Discussed typical hardships with determining exploit

- Lab