Circumventing Exploit Kit Encryption

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER

@jareddemott www.vdalabs.com

Overview

- Homework Review
- Exploit Kits
- Continue .htm analysis
- Continue .swf analysis

```
    first_time = 1
    index=0
    for e in events:
        if e['eventclass']=='File System':
            if is_exe(e['target_path']):
                if first_time:
                    is_web_attack(events, index)
                    first_time = 0
                try:
                    print '| %-10s | %-20s | %-40s |'%(e['time'], e['process'], e['description'])
                except UnicodeEncodeError as err:
                    print str(err)
                    print e
        index+=1
    print '_'*93
```

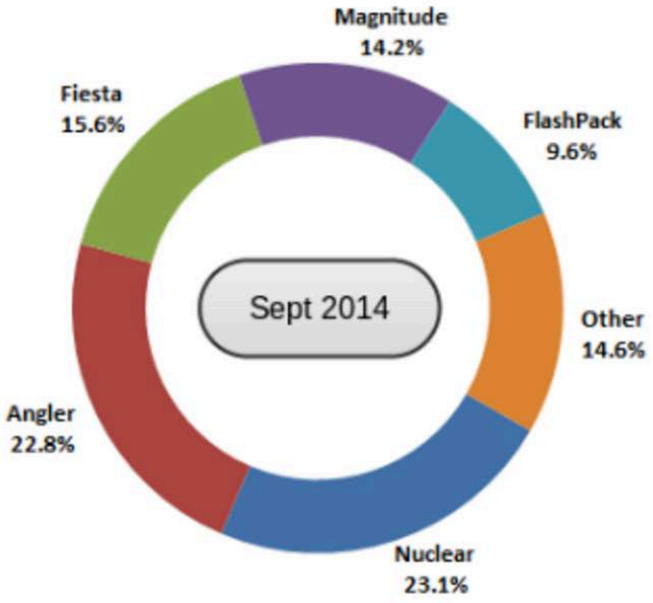
```
494
495  def is_web_attack(events, index):
496      extensions = ['.htm', '.jar', '.swf']
497      #from this point
498      #walk backwards and print last 5 files that have these web attack extensions
499      files = []
500      count = 0
501      for e in reversed( events[:index] ):
502          if e['eventclass']=='File System':
503              path = e['target_path']
504              for ext in extensions:
505                  if path.endswith(ext):
506                      files.append(e)
507                      count+=1
508          if count == 5:
509              break
510      for f in reversed(files):
511          try:
512              print '| %-10s | %-20s | %-40s |'%(f['time'], f['process'], f['description'])
513          except UnicodeEncodeError as err:
514              print str(err)
515              print f
516
517      return True
518
```

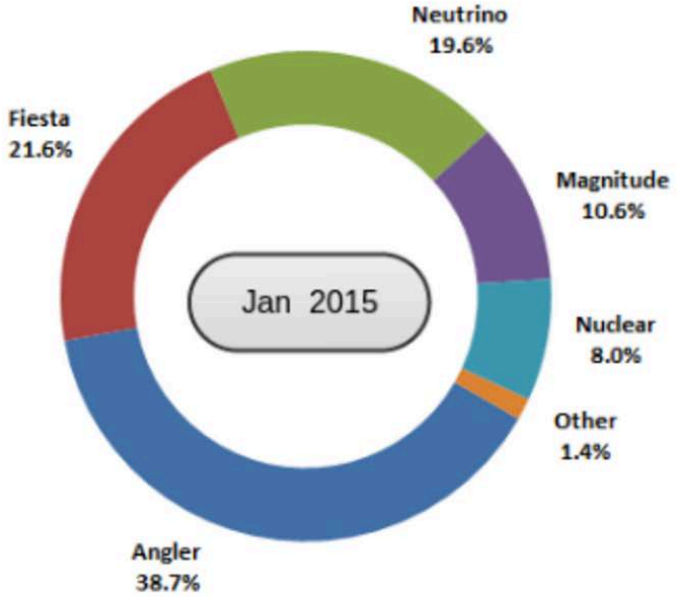
FILE SYSTEM ACTIVITY

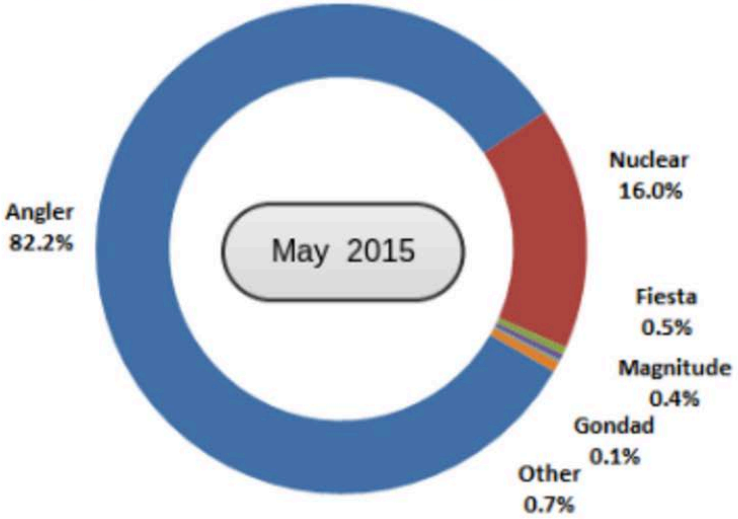
22:46:55	iexplore.exe	Modify Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\QCK733FM\adview[2].htm
22:46:57	iexplore.exe	Modify Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B1HEOTM2\pixel[2].htm
22:46:57	iexplore.exe	Modify Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\B1HEOTM2\push[1].htm
22:46:59	iexplore.exe	Modify Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\8HF45JJI\index[1].htm
22:47:03	iexplore.exe	Modify Users\bruser1729\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\MJ280M1Y\limit[1].swf
22:47:27	conhost.exe	Modify Users\bruser1729\AppData\Local\Temp\{EBAB6D64-C85A-4316-8C91-A08274E2730E}\api-ms-win-system-umpo-l1-1-0.dll
22:47:27	conhost.exe	Modify Users\bruser1729\AppData\Local\Temp\{23F1EF22-CF34-4E1A-A11C-0BCE4BFD39FA}\apds62.dll
22:47:29	regsvr32.exe	Modify Users\bruser1729\AppData\Local\Temp\{23F1EF22-CF34-4E1A-A11C-0BCE4BFD39FA}\apds62.dll
22:47:29	regsvr32.exe	Delete File Users\bruser1729\AppData\Local\Temp\{23F1EF22-CF34-4E1A-A11C-0BCE4BFD39FA}\apds62.dll
22:47:29	regsvr32.exe	Modify ProgramData\LurkEctod\NodNiwn.dll
22:49:01	conhost.exe	Modify ProgramData\{70F91289-E876-4AF3-8A5B-4B7AB475D18F}\browser.dll
22:49:01	conhost.exe	Modify ProgramData\{70F91289-E876-4AF3-8A5B-4B7AB475D18F}\browser.dll

Exploit Kit

Complex system of computer compromise tools and techniques used by organized crime.

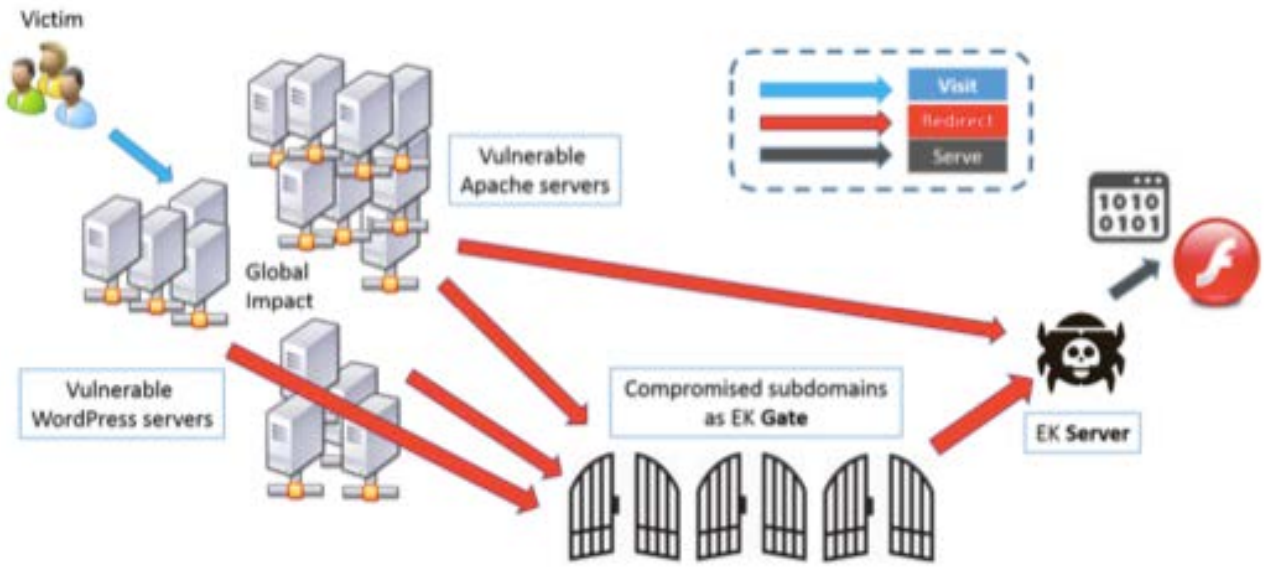

Sept 2014
Magnitude
14.2%
FlashPack
9.6%
Other
14.6%
Nuclear
23.1%
Angler
22.8%
Fiesta
15.6%

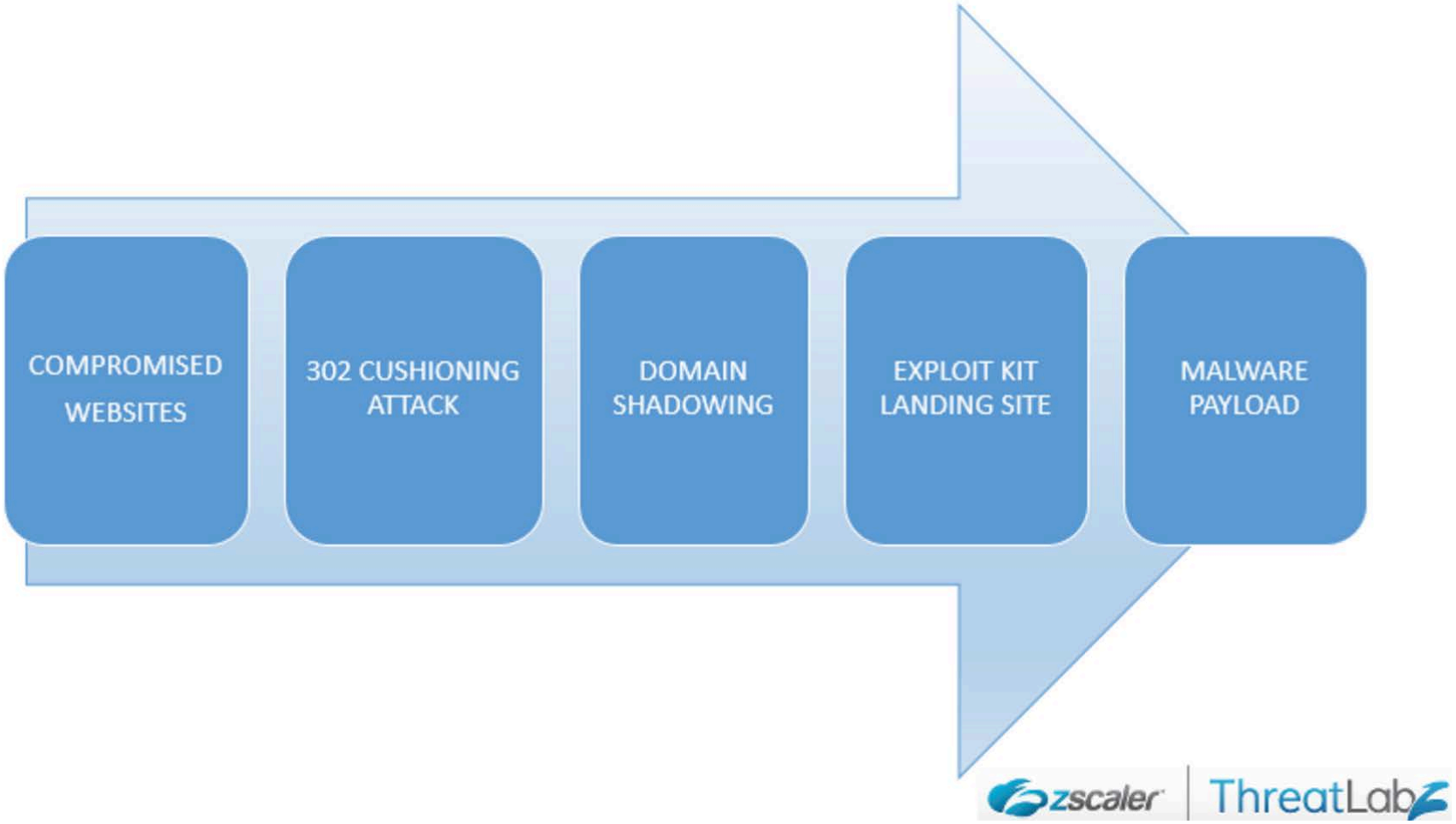

Jan 2015
Neutrino
19.6%
Magnitude
10.6%
Nuclear
8.0%
Other
1.4%
Angler
38.7%
Fiesta
21.6%


May 2015
Nuclear
16.0%
Fiesta
0.5%
Magnitude
0.4%
Gondad
0.1%
Other
0.7%
Angler
82.2%

Exploit Kits

MaaS by OCGs



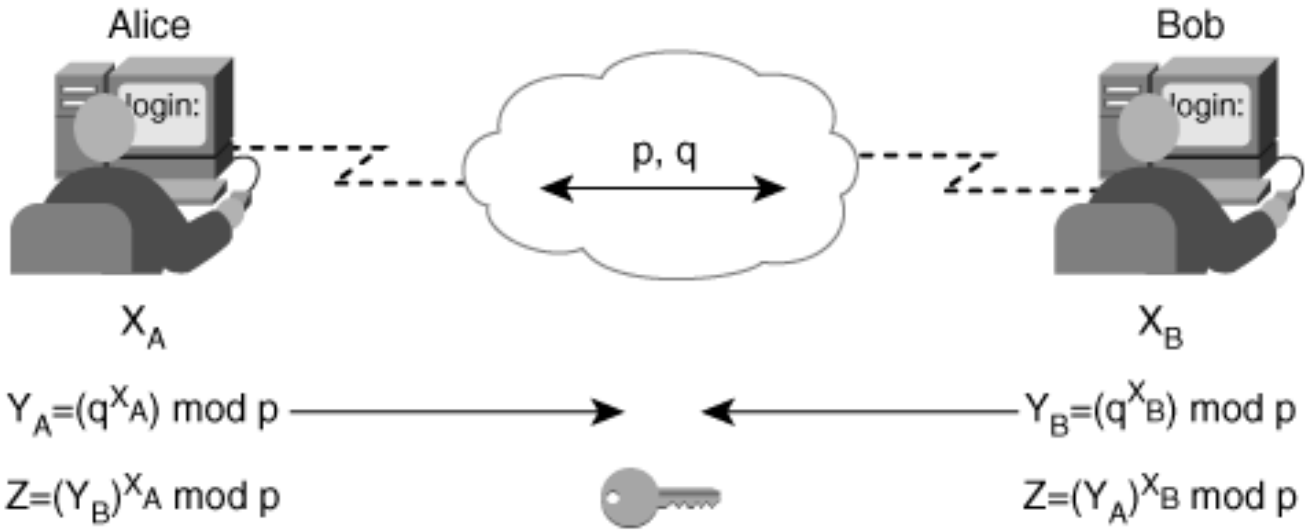

COMPROMISED WEBSITES
302 CUSHIONING ATTACK
DOMAIN SHADOWING
EXPLOIT KIT LANDING SITE
MALWARE PAYLOAD
zscaler
ThreatLabz

EK

- Evade
  - Exploit
- Evade
  - Infect
- Evade
  - Monetize
- Evade
  - Control

Encryption in EKs

- DH
- XTEA
- RC4
- Encoding



What’s up with the HTM?

Scripts for dealing with various ek's

7 commits | 1 branch | 0 releases | 1 contributor

Branch: **master** | New pull request | New file | Find file | HTTPS | https://github.com/mak/ek | Download ZIP

mak angler: addd _ to var regex — Latest commit `fb7e838` on Dec 11, 2015

angler	angler: addd _ to var regex	2 months ago
nuclear	Nuclear: script for downloading paylaod	3 months ago
.gitignore	Initial commit	3 months ago
README.md	Update README.md	3 months ago

README.md

ekdeco

Scripts for dealing with various ek's

```
$ python landing.py files/index\[1\].htm
[+] found posible configuration var eAyySf
[+] found posible configuration var jX5
[+] found posible configuration var fsbniVBGGL
[+] found posible configuration var rxRb3
[+] found posible configuration var BqS
[+] found posible configuration var Og0
[+] found posible configuration var ddezk
[+] found posible configuration var Va9
[+] found posible configuration var jdRk
[+] found posible configuration var uUMTn
[+] found posible configuration var b9R9Db
[+] found posible configuration var wvt
[+] found posible configuration var qPD
[+] found posible configuration var AX
[+] found posible configuration var sXIln
[+] found posible configuration var uGlzK
[+] found posible configuration var p3
[+] found posible configuration var o1g
[+] found posible configuration var dCxTiwblXRYkVUlA
[*] testing key: string
[*] testing key: boolean
[*] testing key: K8jJmRx1MbtAHnwP01Wh
[+] found key_var meCmg[0]
[-] err cant find key variable
```

REGEX for meCmg[0]

```
if 'meCmg = ' in scr:
    key_var = re.findall('meCmg = (\[\'([\w]*)\',)',scr,re.I)[0][1]
    print '[+] found key_var',key_var
```

What’s up with the .swf?

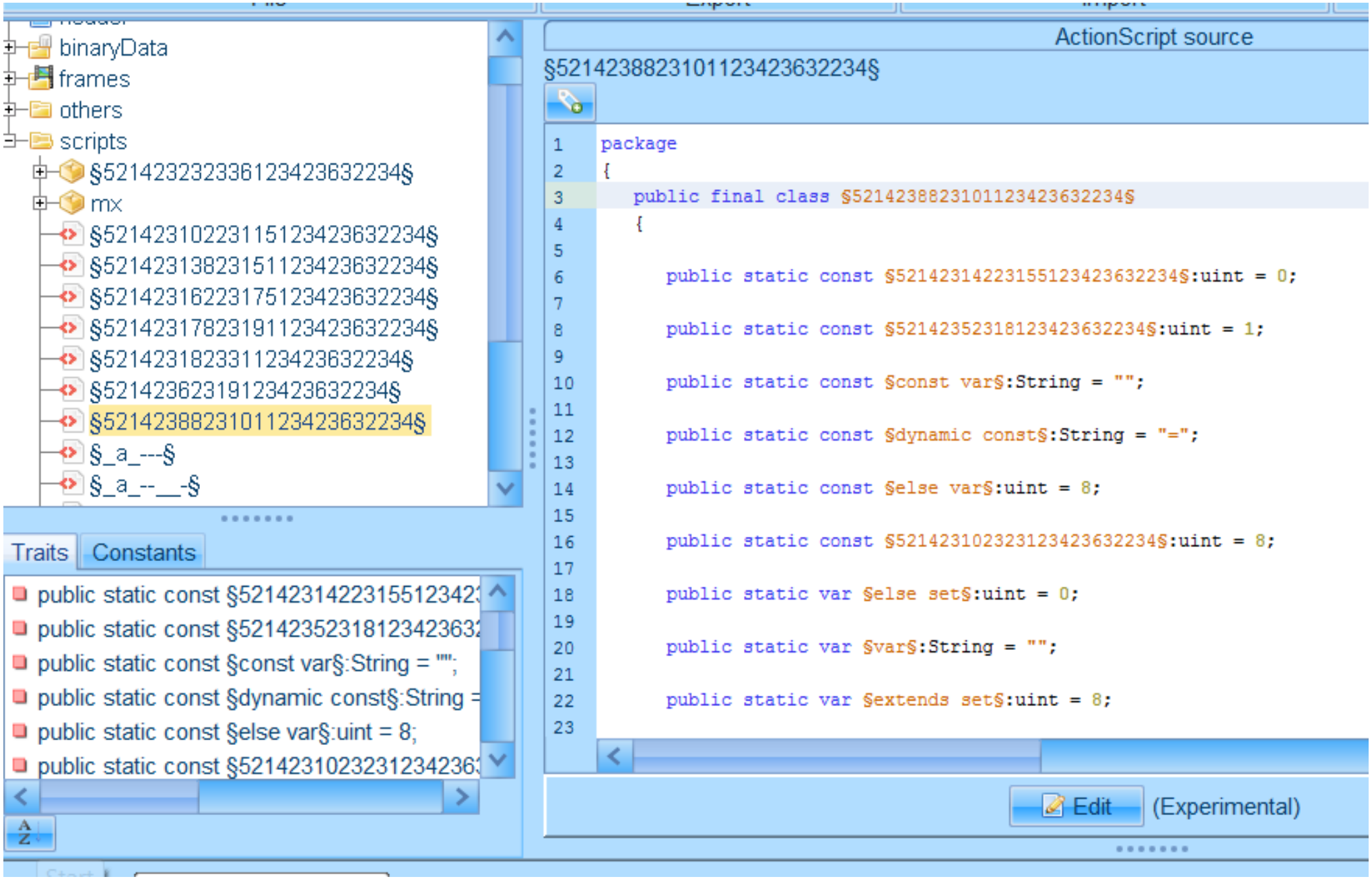
virustotal

URL:	http://futoi-fishfinger.quillesthon.com/limit.wn?position=SoWcB&improve=HW29Ju&or=x-zGV6&experiment=&stand=1Qvgvcpr&agree=83II4HmiZI4J2qf6CWZHXUP
Detection ratio:	3 / 66
Analysis date:	2016-01-26 17:20:29 UTC (0 minutes ago)

Analysis | Additional information | Comments | Votes

URL Scanner	Result
BitDefender	Malware site
Fortinet	Malware site
Kaspersky	Malware site

```
37          output[index] = output[_loc8_];
38          output[_loc8_] = _loc13_;
39          _loc7_ = (_loc7_ + 1) % len(key);
40          index+=1;
41
42      index = 0;
43      while(index < len(blob)):
44          _loc5_ = _loc5_ + 1 & 255;
45          _loc6_ = (output[_loc5_] & 255) + _loc6_ & 255;
46          _loc13_ = output[_loc5_];
47          output[_loc5_] = output[_loc6_];
48          output[_loc6_] = _loc13_;
49          _loc9_ = (output[_loc5_] & 255) + (output[_loc6_] & 255) & 255;
50          blob[index] = ord(blob[index]) ^ output[_loc9_]
51          index+=1;
52
53      return blob
54
55
56  f = open("1.bin", "rb")
57  blob=zlib.decompress(f.read())
58  data=list(blob)
59  f.close()
60
61  secret = "4Fgbspl50L3n8"
62  output = decrypt_blog(data, secret)
63
64  f = open("output.swf", "wb")
65  for b in output:
66      f.write( chr(b) )
67  f.close()
68
```


binaryData
frames
others
scripts
§5214232323361234236322234§
mx
§5214231022311512342363223 4§
§5214231382315112342363223 4§
§5214231622317512342363223 4§
§5214231782319112342363223 4§
§5214231823311234236322 34§
§5214236231912342363223 4§
§5214238823101123423632234§
§_a_---§
§_a_--__-§
Traits
Constants
public static const §5214231422315512342
public static const §5214235231812342363
public static const §const var§:String = "";
public static const §dynamic const§:String =
public static const §else var§:uint = 8;
public static const §5214231023231234236
ActionScript source
§5214238823101123423632234§
package
{
public final class §5214238823101123423632234§
{
public static const §5214231422315512342363223 4§:uint = 0;
public static const §5214235231812342363223 4§:uint = 1;
public static const §const var§:String = "";
public static const §dynamic const§:String = "=";
public static const §else var§:uint = 8;
public static const §5214231023231234236322 34§:uint = 8;
public static var §else set§:uint = 0;
public static var §var§:String = "";
public static var §extends set§:uint = 8;
Edit
(Experimental)

SHA256: c5b8e2d2bd0fd45fa02b6c35062500cd58767d23358c73067bd48197fbbabac3

File name: SecondStage.swf

Detection ratio: 19 / 54

Analysis date: 2016-01-26 00:30:47 UTC (1 day, 14 hours ago)

Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result	Update
AVG	SWF/Exploit.DC	20160125
AegisLab	Exploit.Swf.Agent!c	20160125
AhnLab-V3	SWF/Exploit	20160125
Antiy-AVL	Trojan[Exploit]/SWF.SWF.Generic	20160125
Avast	SWF:Agent-FH [Expl]	20160126
CAT-QuickHeal	Exp.SWF.CVE-2014-0515	20160125

CVE-ID	
CVE-2014-0515	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Buffer overflow in Adobe Flash Player before 11.7.700.279 and 11.8.x through 13.0.x before 13.0.0.206 on Windows and OS X, and before 11.2.202.356 on Linux, allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in April 2014.	

Summary

Learn more about landing page

Learn more about the inner swf