Botnet Attacks and Web Application Defenses

This battle for control isn’t personal, it’s business.

Gunter Ollmann,
Vice President of Research

DAMBALLA
About

- **Gunter Ollmann**
  - VP of Research, Damballa Inc.
  - Board of Advisors, IOActive Inc.

- **Brief Bio:**
  - Been in IT industry for two decades – Built and run international pentest teams, R&D groups and consulting practices around the world.
  - Formerly Chief Security Strategist for IBM, Director of X-Force for ISS, Professional Services Director for NGS Software, Head of Attack Services EMEA, etc.
  - Frequent writer, columnist and blogger with lots of whitepapers…
    - [http://blog.damballa.com](http://blog.damballa.com) & [http://technicalinfodotnet.blogspot.com](http://technicalinfodotnet.blogspot.com/)
What crimeware are criminals using?
- Tools that speed up the defacement process
  - Not necessarily targeted
- Defacement submissions
SQL Injection Attack Tools

- Automatic page rank verification
- Search engine integration for finding "vulnerable" sites
- Prioritization of results based on probability for successful injection
- Reverse domain name resolution
- etc.
Bots...
### IRC CnC – Host Controls

#### Agobot

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>harvest.cdkeys</td>
<td>Return a list of CD keys</td>
</tr>
<tr>
<td>harvest.emails</td>
<td>Return a list of emails</td>
</tr>
<tr>
<td>harvest.emailshttp</td>
<td>Return a list of emails via HTTP</td>
</tr>
<tr>
<td>harvest.aol</td>
<td>Return a list of AOL specific information</td>
</tr>
<tr>
<td>harvest.registry</td>
<td>Return registry information for specific registries</td>
</tr>
<tr>
<td>harvest.windowskeys</td>
<td>Return Windows registry information</td>
</tr>
<tr>
<td>pctrl.list</td>
<td>Return list of all processes</td>
</tr>
<tr>
<td>pctrl.kill</td>
<td>Kill specified process set from service file</td>
</tr>
<tr>
<td>pctrl.listsvc</td>
<td>Return list of all services that are running</td>
</tr>
<tr>
<td>pctrl.killsvc</td>
<td>Delete/stop a specified service</td>
</tr>
<tr>
<td>pctrl.killpid</td>
<td>Kill specified process</td>
</tr>
<tr>
<td>inst.asadd</td>
<td>Add an autostart entry</td>
</tr>
<tr>
<td>inst.asdel</td>
<td>Delete an autostart entry</td>
</tr>
<tr>
<td>inst.svccadd</td>
<td>Adds a service to SCM</td>
</tr>
<tr>
<td>inst.svcdel</td>
<td>Delete a service from SCM</td>
</tr>
</tbody>
</table>

#### SpyBot

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete &lt;filename&gt;</td>
<td>Delete a specified file</td>
</tr>
<tr>
<td>execute &lt;filename&gt;</td>
<td>Execute a specified file</td>
</tr>
<tr>
<td>rename &lt;origfilename&gt; &lt;newfile&gt;</td>
<td>Rename a specified file</td>
</tr>
<tr>
<td>makedir &lt;dirname&gt;</td>
<td>Create a specified directory</td>
</tr>
<tr>
<td>startkeylogger</td>
<td>Starts the on-line keylogger</td>
</tr>
<tr>
<td>stopkeylogger</td>
<td>Stops the keylogger</td>
</tr>
<tr>
<td>sendkeys &lt;keys&gt;</td>
<td>Simulates key presses</td>
</tr>
<tr>
<td>keyboardlights</td>
<td>Flashes remote keyboard lights 50x</td>
</tr>
<tr>
<td>passwords</td>
<td>Lists the RAS passwords in Windows 9x systems</td>
</tr>
<tr>
<td>listprocesses</td>
<td>Return a list of all running processes</td>
</tr>
<tr>
<td>killprocess &lt;processname&gt;</td>
<td>Kills the specified process</td>
</tr>
<tr>
<td>threads</td>
<td>Returns a list of all running threads</td>
</tr>
<tr>
<td>killthread &lt;number&gt;</td>
<td>Kills a specified thread</td>
</tr>
<tr>
<td>disconnect &lt;number&gt;</td>
<td>Disconnect the bot for number seconds</td>
</tr>
<tr>
<td>reboot</td>
<td>Reboot the system</td>
</tr>
<tr>
<td>cd-rom 0/1</td>
<td>Open/close cd-rom. cd-rom 1 = open, cd-rom 0 = close</td>
</tr>
<tr>
<td>opencmd</td>
<td>Starts cmd.exe (hidden)</td>
</tr>
<tr>
<td>cmd &lt;command&gt;</td>
<td>Sends a command to cmd.exe</td>
</tr>
</tbody>
</table>

#### SDbot

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>download &lt;url&gt; &lt;dest&gt; &lt;action&gt;</td>
<td>Downloaded specified file and execute if action is 1</td>
</tr>
<tr>
<td>killthread &lt;thread#&gt;</td>
<td>Kill specified thread</td>
</tr>
<tr>
<td>update &lt;url&gt; &lt;id&gt;</td>
<td>If bot ID is different than current, download “sdbot executable” and update</td>
</tr>
<tr>
<td>sysinfo</td>
<td>List host system information (CPU/RAM/OS and uptime)</td>
</tr>
<tr>
<td>execute &lt;visibility&gt; &lt;file&gt; parameters</td>
<td>Run a specified program (visibility is 0/1)</td>
</tr>
<tr>
<td>cdkey/getcdkey</td>
<td>Return keys of popular games e.g., Halflife, Soldier of Fortune etc.</td>
</tr>
</tbody>
</table>
### Current Tasks

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Description</th>
<th>Priority</th>
<th>Performed</th>
<th>Speed</th>
<th>State</th>
<th>Type</th>
<th>Delivered Letters</th>
<th>Recipient not found</th>
<th>Total addresses count</th>
<th>Running Time</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASH</td>
<td></td>
<td>1</td>
<td>51.0%</td>
<td>1210</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>97469</td>
<td>58626</td>
<td>306203</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>relite</td>
<td>https://</td>
<td>2</td>
<td>0.0%</td>
<td>-</td>
<td>Queued</td>
<td>Direct Sending</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>audit</td>
<td>index.htm</td>
<td>2</td>
<td>0.0%</td>
<td>-</td>
<td>Queued</td>
<td>Direct Sending</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fin</td>
<td>index.htm</td>
<td>2</td>
<td>15.0%</td>
<td>3215</td>
<td>Running</td>
<td>Direct Sending</td>
<td>24596</td>
<td>23035</td>
<td>306204</td>
<td>14:14:55</td>
<td>Stop</td>
</tr>
<tr>
<td>sabuv</td>
<td>http://</td>
<td>2</td>
<td>50.0%</td>
<td>1255</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>97556</td>
<td>50085</td>
<td>306203</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>bek</td>
<td>http://</td>
<td>1</td>
<td>43.9%</td>
<td>1302</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>85033</td>
<td>64800</td>
<td>306204</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>pran</td>
<td>index.htm</td>
<td>2</td>
<td>49.0%</td>
<td>1251</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>84063</td>
<td>68076</td>
<td>306204</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>prl</td>
<td>index.htm</td>
<td>1</td>
<td>51.5%</td>
<td>1253</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>99932</td>
<td>57652</td>
<td>306203</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>astrea</td>
<td>index.htm</td>
<td>2</td>
<td>51.3%</td>
<td>1275</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>91073</td>
<td>65864</td>
<td>306204</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>http://</td>
<td>index.htm</td>
<td></td>
<td>49.1%</td>
<td>1231</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>93662</td>
<td>58620</td>
<td>306203</td>
<td>0</td>
<td>Info</td>
</tr>
</tbody>
</table>

### Main System Stats

- **Number of Bots:** 1872
- **Number of RS:** 1
- **Number of Working RS:** 1

**Bots by OS:**
- Win XP - 462

**Bots by Version:**
- v56 - 121
- v56 - 1551

**Bots by Count:**
- Total Bots - 1872
- Bots with Status - 428
- Bots with Status - 311
- Bots with Status - 428
- Bots with Status - 315

**Task Speed Graph:**
- Number of Delivered Letters vs. Task Running Time in Minutes

**Bots by Count:**
- Total Bots - 1872
- Bots with Status - 428
- Bots with Status - 311
- Bots with Status - 428
- Bots with Status - 315
Builder Battling

- Zeus  – Worlds most popular malware DIY malware construction kit
- Helps clear your system before making the malware
ZEUS DIY Kit

- **RRP:** $400 (street price ~$50)
- Botnet CnC package with Web management frontend.
- **Very popular** – many plug-ins developed to extend functionality
Свободные боты. Take over для помещения их в список ботов, которым выделяются задания.

### Free bots

<table>
<thead>
<tr>
<th>Id</th>
<th>Version</th>
<th>S</th>
<th>MX</th>
<th>Ip</th>
<th>Serial</th>
<th>Last seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>17971</td>
<td>15</td>
<td>✓</td>
<td>✓</td>
<td>1.8</td>
<td>7002-190E</td>
<td>0 seconds</td>
</tr>
<tr>
<td>18001</td>
<td>15</td>
<td>✓</td>
<td>✓</td>
<td>2.103</td>
<td>A86C-668C</td>
<td>0 seconds</td>
</tr>
<tr>
<td>19406</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>255.44</td>
<td>2124-7CS3</td>
<td>0 seconds</td>
</tr>
<tr>
<td>20689</td>
<td>15</td>
<td>✓</td>
<td>✓</td>
<td>86.62</td>
<td>0707-565F</td>
<td>0 seconds</td>
</tr>
<tr>
<td>21179</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>72.16</td>
<td>4BE4-E459</td>
<td>0 seconds</td>
</tr>
<tr>
<td>22340</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>90.129</td>
<td>287D-8EC2</td>
<td>0 seconds</td>
</tr>
<tr>
<td>23199</td>
<td>15</td>
<td>✓</td>
<td>✓</td>
<td>3.60</td>
<td>C885-66AC</td>
<td>0 seconds</td>
</tr>
<tr>
<td>23247</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>1.140</td>
<td>4697-1209</td>
<td>0 seconds</td>
</tr>
<tr>
<td>25183</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>01.105</td>
<td>3440-BBAE</td>
<td>0 seconds</td>
</tr>
<tr>
<td>25692</td>
<td>15</td>
<td>✓</td>
<td>✓</td>
<td>174.205</td>
<td>18EF-22EF</td>
<td>0 seconds</td>
</tr>
<tr>
<td>27778</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>3.76</td>
<td>EC6B-F57F</td>
<td>0 seconds</td>
</tr>
<tr>
<td>28212</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>.51</td>
<td>3C29-FCE8</td>
<td>0 seconds</td>
</tr>
<tr>
<td>28777</td>
<td>15</td>
<td>✓</td>
<td>✓</td>
<td>43.120</td>
<td>A40F-290D</td>
<td>0 seconds</td>
</tr>
<tr>
<td>29308</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>62.50</td>
<td>782A-E2E</td>
<td>0 seconds</td>
</tr>
<tr>
<td>30668</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>94.21</td>
<td>2092-335B</td>
<td>0 seconds</td>
</tr>
<tr>
<td>2127</td>
<td>14</td>
<td>✓</td>
<td></td>
<td>65.223</td>
<td>0053-BCAE</td>
<td>1 second</td>
</tr>
<tr>
<td>17115</td>
<td>15</td>
<td>✓</td>
<td></td>
<td>40.199</td>
<td>45C4-FBFF</td>
<td>1 second</td>
</tr>
</tbody>
</table>
Battling at the Victims Host

- Similar kit to Zeus
- “Kill Zeus”
Sophisticated Management

Spy Eye v1.2

Get Certificates

Bot GUID:

Report date region:
15/07/2010 .. 20/07/2010 clean

Data:

Limit:
100

Show useless certificates:

Submit
SpyEye Stats

Statistic by IE version

IE 8
IE 7
IE 6
IE 5
IE ?

Statistic by User Type

User
Admin

Statistic by OS

Windows Server 2003
Windows Vista
Windows 7
Unknown
Windows 2000
Windows XP
**Sophisticated Management**

<table>
<thead>
<tr>
<th>ID</th>
<th>Note</th>
<th>Start Time</th>
<th>Finish Time</th>
<th>Bots Count</th>
<th>Tasks Processing (%)</th>
<th>[Detail]</th>
<th>[Controls]</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td></td>
<td>2009-10-19 14:13:42</td>
<td>2009-11-10 00:13:42</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>301</td>
<td></td>
<td>2009-10-27 14:23:17</td>
<td>2009-11-10 00:23:17</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Bots with cards for Global Task # 301**

<table>
<thead>
<tr>
<th>[Restart]</th>
<th>[New Time]</th>
<th>ID</th>
<th>Task</th>
<th>Planned Time</th>
<th>Begin Time</th>
<th>End Time</th>
<th>E-Mail</th>
<th>Message Log</th>
<th>Client's info</th>
<th>Id Bot</th>
</tr>
</thead>
<tbody>
<tr>
<td>don't</td>
<td></td>
<td>4102</td>
<td></td>
<td>2009-10-27 17:08:53</td>
<td>2009-10-27 17:09:10</td>
<td>2009-10-27 17:15:52</td>
<td><a href="mailto:trunguyen82@newhampshire.usa.com">trunguyen82@newhampshire.usa.com</a></td>
<td></td>
<td>6.0.5000 8.0.6001.19862 User</td>
<td></td>
</tr>
<tr>
<td>don't</td>
<td></td>
<td>4106</td>
<td></td>
<td>2009-10-29 19:03:29</td>
<td>2009-10-29 19:03:43</td>
<td>2009-10-29 19:05:43</td>
<td><a href="mailto:vallierip34@delhimail.com">vallierip34@delhimail.com</a></td>
<td></td>
<td>5.1.2600 8.0.28001.1106 Admin</td>
<td></td>
</tr>
<tr>
<td>don't</td>
<td></td>
<td>4108</td>
<td></td>
<td>2009-10-30 05:32:05</td>
<td>2009-10-30 05:33:23</td>
<td>2009-10-30 05:34:52</td>
<td><a href="mailto:paddybaby0242@sister.com">paddybaby0242@sister.com</a></td>
<td></td>
<td>5.1.2600 7.0.5730.11 Admin</td>
<td></td>
</tr>
<tr>
<td>don't</td>
<td></td>
<td>4113</td>
<td></td>
<td>2009-10-31 10:37:05</td>
<td>2009-10-31 13:06:51</td>
<td>2009-10-31 13:06:17</td>
<td><a href="mailto:jcropp18@hour.com">jcropp18@hour.com</a></td>
<td></td>
<td>5.1.2600 7.0.5730.11 Admin</td>
<td></td>
</tr>
<tr>
<td>don't</td>
<td></td>
<td>4117</td>
<td></td>
<td>2009-11-02 04:28:41</td>
<td>2009-11-02 04:33:09</td>
<td></td>
<td><a href="mailto:velicajamess29@kittymail.com">velicajamess29@kittymail.com</a></td>
<td>ERROR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>4120</td>
<td></td>
<td>2009-11-02 10:50:17</td>
<td>2009-11-03 13:53:25</td>
<td></td>
<td><a href="mailto:gregorysmith2@atheist.com">gregorysmith2@atheist.com</a></td>
<td>ERROR</td>
<td>5.1.2600 7.0.5730.11 Admin</td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>4122</td>
<td></td>
<td>2009-11-04 07:46:05</td>
<td>2009-11-04 14:00:16</td>
<td>2009-11-04 14:01:53</td>
<td><a href="mailto:hendess1142@seductive.com">hendess1142@seductive.com</a></td>
<td></td>
<td>5.1.2600 7.0.5730.13 Admin</td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>4123</td>
<td></td>
<td>2009-12-21 08:50:41</td>
<td>2009-12-22 07:14:57</td>
<td></td>
<td><a href="mailto:tcdalessandro95@alaska.usa.com">tcdalessandro95@alaska.usa.com</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>id</td>
<td>bot_guid</td>
<td>process_name</td>
<td>hooked_func</td>
<td>date_rep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------</td>
<td>----------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P006333211051-L323-4449FCDB</td>
<td>C:\Program Files\Internet Explorer\explore.exe</td>
<td>HttpSendRequestW</td>
<td>2010-07-02 20:24:53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|             |                                         | https://online.citibank.com/US/JPS/portal/Home.do | GET /US/JPS/portal/Home.do HTTP/1.1  
|             |                                         |   Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/xaml+xml, application/vnd.ms-xmldocument, application/vnd.ms-xpsdocument, application/x-ms-xbap, application/vnd.ms-application, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*  
|             |                                         |   Referer: https://online.citibank.com/US/JPS/portal/Index.do  
|             |                                         |   Accept-Language: en-us  
|             |                                         | https://online.citibank.com/US/usba/ci/presentCheckImage.do  
|             |                                         | POST /US/usba/ci/presentCheckImage.do HTTP/1.1  
|             |                                         |   Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/xaml+xml, application/vnd.ms-xmldocument, application/vnd.ms-xpsdocument, application/x-ms-xbap, application/vnd.ms-application, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*  
|             |                                         |   Referer: https://online.citibank.com/jba/ada/ViewImage.do?selectedTJIndex=16  
|             |                                         |   searchScreen=false  
|             | P006333211051-L323-4449FCDB             | C:\Program Files\Internet Explorer\explore.exe   | HttpSendRequestW    | 2010-07-03 00:11:14 |
|             |                                         | https://online.citibank.com/US/JPS/portal/Home.do |
Visibility...
Kit Hunting Isn’t Rocket Science…
- Commercial “dual-use” Trojan creator
- V.4 New features
  - Remote Desktop
  - Webcam Streaming
  - Audio Streaming
  - Remote passwords
  - MSN Sniffer
  - Remote Shell
  - Advanced File Manager
  - Online & Offline keylogger
  - Information about remote computer
  - Etc..
- Three versions
  - Gold, Silver & Bronze
Platform: software running on MAC OS to Windows
Multitasking: have the capacity to work on multiple projects
Speed and responsibility: at the highest level
Pre-payment for new customers: 50% of the whole price, 30% pre-pay of the whole price for repeated customers
Rates: starting from 100 euros

I can also offer you another deal, I will share the complete source code in exchange to access to a botnet with at least 4000 infected hosts because I don't have time to play around with me bot right now.
Other models exist for hire-a-malware-coder pricing

Component/functionality based pricing

- Loader €300
- FTP & Grabber €150
- Assembler Spam bases €220
- Socks 4/5 €70
- Botnet manager €600
- Scripts €70
- Password stealers (IE, MSN, etc.) €70
- AV-remover €70
- Screen-grabber €70
IP Flux

- Single-flux
  - Cycling of hundreds/thousands of IP’s with short TTL’s
- Double-flux
  - Cycling of DNS server IP’s too.

Domain Flux

- Domain wildcarding
  - Random FQDN’s all point to same address
- Domain generation algorithms
  - Dynamic list of FQDN’s generated daily
Dynamic Domain Generation

- Designed to thwart domain hijacking/closure

**Sinowal**
fhwwhkis.com
fhksvbjj.com
kixxgxhi.com
dfhkxefj.biz
xchtucfx.com
ehbcihsng.com
htiuuhwbc.com
xddjvng.com
ivfjxxvf.com
icdkvcj.f.com

**Bobax/Torpig**
cfzxkefy.2mydns.net
ozzlcjfwxy.mykgb.com
uavpmphb.zipitover.com
nlnmg.widescreendozrd.tv
mohuajixthb.afraid.org
vemogoftiv.zipitover.com
fwsdqcxozozi.mycoding.com
iagukau.afraid.org
pxkakigm.dx.mario.org
zxyeptqgn.mario.org

**Conficker A/B**
jstlzacccs.cc
kupgc.info
gyagluso.info
ezfoozq.biz
hxqbgkyw.org
nxmezi.org
sayklyqfhk.org
eplgu.org
hlgkiyogcs.ws
oyvkt.cn

**Conficker C**
bjxqjx.com.sv
dgtqwe.be
cnxnp.com.py
btuutlevt.com.mt
bmjlezym.com.pe
bynzopen.com.mx
daagsup.com.bo
cesqun.ca
cxcsicbqsn.ch
dcmrfv.gs
Hack-back

- **Curiosity killed the cat**
  - Turn botnet against CnC investigators

- **Identifying the researcher**
  - Repeated lookup of name servers
  - Resolution request for CnC host name
  - Wrong port/protocol in CnC connection
  - Missing handshake or keys
  - Identify sandbox/VM being used

- **Response tactics**
  - DDoS the IP address or netblock
  - Spam flood the researcher
  - Exploit and breakout of sandbox/VM
  - Give different (benign) responses to the researcher
Buyers & Sellers

- **Where to look?**
  - Most hacker and carding forums

- **Mechanisms for validation of buyer/seller**
  - Rating systems of buyers/sellers
  - Try-before -you-buy plus “free” disclosures

- **How to pay**
  - Non-revocable money transfers
  - Volumes of stolen credentials
  - Segments of a botnet
### Buying Botnet Victims

![Botnet Victim Website Screenshot](image)

<table>
<thead>
<tr>
<th>Country</th>
<th>Price for 1k</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU</td>
<td>$300</td>
</tr>
<tr>
<td>DE</td>
<td>$220</td>
</tr>
<tr>
<td>GB</td>
<td>$210</td>
</tr>
<tr>
<td>IT</td>
<td>$200</td>
</tr>
<tr>
<td>NZ</td>
<td>$200</td>
</tr>
<tr>
<td>ES</td>
<td>$200</td>
</tr>
<tr>
<td>US</td>
<td>$110</td>
</tr>
<tr>
<td>BG</td>
<td>$100</td>
</tr>
<tr>
<td>DK</td>
<td>$100</td>
</tr>
<tr>
<td>FR</td>
<td>$100</td>
</tr>
<tr>
<td>PT</td>
<td>$100</td>
</tr>
<tr>
<td>NL</td>
<td>$100</td>
</tr>
<tr>
<td>NO</td>
<td>$80</td>
</tr>
<tr>
<td>SE</td>
<td>$70</td>
</tr>
<tr>
<td>BR</td>
<td>$60</td>
</tr>
<tr>
<td>TR</td>
<td>$60</td>
</tr>
<tr>
<td>NO</td>
<td>$50</td>
</tr>
</tbody>
</table>

Copyright © 2009-2010 Damballa, Inc. All Rights Reserved
Web-based portal bot-management
For a small fee, attackers can rent/purchase members of a larger botnet.
Online tools enable remote management and configuration of the botnet agents
Portals include performance monitoring tools - how fast is the spam being sent, DDoS throughput, etc.
Worth less than you imagine

How much?
1/400\textsuperscript{th} of a cent per 24 hours
The botnet advantage

The use of botnets in attacking Web applications holds several advantages...

- Anonymity
  - Chaining of several agents to disguise source of attack
- Dispersed hosts
  - Slipping under threshold limits
- The power of many
  - A force multiplier
- Native automation
  - Advanced scripting engines & user manipulation
Anonymity through botnet agents

Many tools and services rely upon compromised hosts (typically botnet agents) to provide SOCKS proxies as anonymous exit/jump points.
Anonymity Services

SOCKS chaining
A method of chaining multiple compromised machines together to anonymously tunnel data

Starting from $40 and going to $300 for a quarter of access, with the price increasing based on the level of anonymity added.
Looking for a soft target?
Intercepting Traffic – Man-in-the-browser

Man-in-the-browser
Malware hooks inside the Web browser

Traditional Malware
Operates and intercepts data at points through which the Web browser must communicate

**System Reconfiguration**
DNS Settings, Local HOST file, Routing tables, WPAD and Proxy settings

**Trojan Application**
Local Proxy Agent

**OS Hooking**
Keyloggers, Screen grabber

**TCP/IP Stack Interception**
Packet inspection, pre/post SSL logging
API Hooking Malware

**Clean System**

- Application
  - The Web browser

- WinInet
  - `httpsendrequest()`, `navigateto()`

- Winsock
  - TCP/IP stack

**Infected System**

- Application
  - The Web browser

- Malware
  - Proxying Web browser data

- WinInet
  - `httpsendrequest()`, `navigateto()`

- Winsock
  - TCP/IP stack

**Manipulate**

- Copy, redirect, script, change, insert, sell.

Internet

Internet
MITB – Grabbing Login Credentials

- Steal login credentials, and ask for more…
  
  **Pre-login**
  First page of login sequence is manipulated

  **Login**
  Multiple fields & pages added to the login sequence

  **Post-login**
  Authenticated user asked additional security questions

- Requests for additional data are easy to socially engineer
  
  - Ask for credit/debit card details, including PIN and CVV
  - Additional “security” questions – SSN, mother’s maiden name, address, home phone number, mobile/cell phone number
  - Type in all numbers of one-time-keypad scratch-card
  - “Change password” for anti-keylogging partial-password system
  - “Test” or “resynchronize” password/transaction calculators

- SSL/TLS encryption bypassed, “padlock” intact
By way of example... Online Banking
Traditional Banking Malware

- Focused on stealing login information:
  - Bank number, UID, password(s), session keys

- Techniques include:
  - Keylogging, screen-grabbing, video-recording of mouse movements
  - Redirection to counterfeit site (domain/host substitution)
  - Replacement and pop-up windows
  - Session hijacking (duplicating session cookies)
  - Screen overlays (superimposed counterfeit web forms)
MITB – Grabbing Login Credentials

Original pre-login fields
UID, password & site

Modified pre-login fields
Now with ATM details and MMN

New fields added
MITB malware inserted additional fields. Records them, and sends them to the attacker.
Modified pre-login fields
Now with ATM details and MMN

Programmable Interfaces
Malware authors developing an extensible platform that can be sold or rented to other criminals
MITB – Focusing on the Money Transfer

- **Change in tactic’s – move from login to the money transfer**
  - First malware generation captured in early 2007 (South America)

- **Change driven by:**
  - Widespread use of temporal multi-factor keys for authentication
  - Backend application heuristics for spotting login patterns
  - Inter-bank sharing of login and transfer “physical” location info
  - Improved malware techniques…

- Transfers happen after the customer logs in, *from their own computer*, while they are logged in.

- “Session Riding” – can be conducted manually (attacker C&C) or scripted
MITB – State-of-the-art Banking Proxy Trojan

Victim logs in to the bank “securely” and banks “normally”

Proxy Trojan starts functioning once the victim logs in

Intercepts each transaction

Attacker makes off with the money and the victim is unaware a transaction has occurred

Modifies the page that appears to the victim

Calculates what is supposed to be in the account

Steals some money

Copyright © 2009-2010 Damballa, Inc. All Rights Reserved
Honing in on the Transaction – Malware Injection

**Payment Details**
Customer enters their transfer payment details

**Background Malware**
In the background, the proxy Trojan has created it's own transfer details

**Submission**
Customer clicks “Submit” to proceed

**Validation**
Customer enters another validation code

**Malware Fakes**
The malware fakes a “validation failure” even though the fake transaction worked. Prompts user to “try again”

**2nd Submission**
Customer clicks “Submit” again

**Confirmation**
2nd transaction is confirmed back to the customer. In reality, two transfers have been conducted

**2nd Submission**
Customer clicks “Submit” again

**3rd Submission**
Malware submits the original “real” customer transfer information

**Confirmation**
2nd transaction is confirmed back to the customer. In reality, two transfers have been conducted
SQL Injection?
Botnet SQL Injection (SQLi)

Botnet Master

CnC Server

New exploit

Attack sites vulnerable to ....
... inject the following iFrame

Query search engine for vulnerable

Compile list of targets

Try to exploit server

Inject iFrame

Next target...

Copyright © 2009-2010 Damballa, Inc. All Rights Reserved
Automated SQL Injection with search engines

- Several commercial SQL Injection tools make use of backend services/C&C to receive latest exploits.

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Vulnerability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan (Google)</td>
<td>Milw0rm Joomla Component Expose</td>
<td>Vuln 4194</td>
</tr>
<tr>
<td>Scan (Google)</td>
<td>QuickEStore</td>
<td>Vuln 4193</td>
</tr>
<tr>
<td>Scan (Google)</td>
<td>Vivo CMS</td>
<td>Vuln 4192</td>
</tr>
<tr>
<td>Scan (Google)</td>
<td>Pictures Rating</td>
<td>Vuln 4191</td>
</tr>
<tr>
<td>Scan (Google)</td>
<td>Data Dynamics ActiveBar Active Insecure Methods</td>
<td>Vuln 4190</td>
</tr>
<tr>
<td>Scan (Google)</td>
<td>Expert Advisor</td>
<td>Vuln 4189</td>
</tr>
<tr>
<td>Scan (Google)</td>
<td>Flash Player/Plugin Video file parsing Remote Code Execution POC</td>
<td>Vuln 4188</td>
</tr>
</tbody>
</table>

- Many rely upon search engine queries to identify likely vulnerable Web servers before commencing their automated attack.
Botnet SQL Injection (newer!)

Botnet Master

New exploit

Attack sites vulnerable to ....
... inject the following iFrame ...

CnC Server actions:
1. Query Google
2. Compile list of targets
3. Batch targets
4. Issue batches
5. Manage batch results

Copyright © 2009-2010 Damballa, Inc. All Rights Reserved
Blind SQLi

- Very slow to enumerate a database
  - Pentesters and tools may “prove” the vulnerability exists – but too time consuming to do it for real

- Add botnet agents to the mix...
  - 10,000 bot agents
  - Parallel SQLi on a single host = ~30 rps (4 rps SSL)
  - \(1.08 \times 10^9\) rph
    \((1.44 \times 10^8\) rph SSL\)
What can you do about this threat?
Protection Improvement Mindset

• Most important factor? – reduce complexity
  • Is it likely additional pages or fields would be spotted by a customer?
  • Is it clear to the customer what’s expected of them?
  • How many pages must customers navigate through or scroll through?
  • Are all the steps logical?
  • Are important questions and steps presented as text or as graphics?
  • How would a customer recognize changes to page content?
  • Could the interface be simplified further?
Location Limitations

- Geographically distributed attacks
  - Multiple requests from very different locations
  - DHCP churn can affect sources as well (depending on length of attack)
- Can’t really block by country or netblock
- IP churn may result in wrong customers being blocked during prolonged attacks

- Optimal Response…
  *Throttling responses based upon IP/browser combo + maintaining state*
Can the customer change everything online?
- Address details, delivery details, contact numbers, PIN numbers, passwords, password recovery questions, new accounts, etc.

What out-of-band verification of changes are there?
- Change notification sent to previous contact details?
- Are there delays before going “live”?

How visible are customer initiated changes?
- What contact info has changed?
- Change history goes back how far?

Transaction history in HTML and Print/PDF for reconciliation?
Backend Processing

- How much protection/detection can be done with “backend” thresholds?
  - Does the system implement thresholds on transactions per minute?
  - Is there a delay between creation of a new “payee” account, and ability to transfer money to that account?

- Anomaly detection of transfers?
  - Is information being shared on *To:* accounts?
  - Frequency of *To:* account by other customers
  - Could you identify a frequent mule account?

- Identity Changes?
  - Primary contact number changing to cellphone?
Conclusions

- Application complexity is a root-cause
- Vigilance in monitoring applications and patching
- Increased investment by criminals in to new crimeware tools

- *Crimeware is a bigger Webapp threat than some angry pentester...*
Further Reading...

- Continuing Business with Malware Infected Customers
  - http://www.technicalinfo.net/papers/MalwareInfectedCustomers.html

- Anti-fraud Image Solutions
  - http://www.technicalinfo.net/papers/AntiFraudImageSolutions.html