Who Am I

- Anzen Computing (2000-2001)
- University of Michigan (2004-2013)
- Arbor ASERT
- Brewer of life altering beer
- mbing@arbor.net
- @mattbing
Arbor Security Engineering Response Team

ATLAS

Honeypots & SPAM Traps

Security Community

100K Malware samples/day

Sandbox of Virtual Machines run malware (look for botnet C&C, files, network behavior)

Report and PCAP stored in database

“Tracker” DDoS Attack Auto-classification and analysis every 24 hrs.
Botnets

Source: https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/wang/wang_html/figure1.png
Why Botnets?

- Steal banking credentials
- Bitcoin mining
- Spam
- Clickfraud
- DDoS
- Nation-state espionage
- Targeted data exfiltration
- Hacktivism
- Some amalgamation
Malware Analysis

IDA - Z:\Downloads\fd.exe

- Call sub_4047E0
- Mov ecx, [esp+8+arg_0]
- Mov esi, eax
- Test ecx, ecx
- Jz short loc_403BE4

- Test edi, edi
- Jz short loc_403BE4

- Sub ecx, esi

Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Can not set debug privilege: Not all privileges or groups referenced are assigned to the caller.

Python 2.7.2 (default, Jun 12 2011, 15:08:59) [MSC v.1500 32 bit (Intel)]

AU: idle Down Disk: 26GB
Is Like This..

Source: http://manyheadedmonster.files.wordpress.com/2013/09/sword.jpg
..And Not This

Source: http://upload.wikimedia.org/wikipedia/commons/6/64/Grunwald_bitwa.jpg
Tracking Malware

• What is the intent of the botmaster?
• How is the malware installed?
  – Drive-by, social engineering
• How many are affected?
  – Who are they? Where are they?
• What is the impact?
  – Stolen data, DDoS targets, exposed passwords
• How does this compare to other botnets?
  – Should people care?
Tracking C&Cs

• Access to the command-and-control
  – Location and size estimate of those affected
  – Some better clues as to the motivation
  – Attribution is still really hard

• Methods
  – Sinkholing domains
  – Monitor live traffic
  – Monitor passive DNS
That's All Really Hard..
Brute Force Attacks Build WordPress Botnet

Security experts are warning that an escalating series of online attacks designed to break into poorly-secured WordPress blogs is fueling the growth of an unusually powerful botnet currently made up of more than 90,000 Web servers.

Dissecting a WordPress Brute Force Attack

By Tony Perez on July 22, 2013  •  15 Comments

Over the past few months there has been a lot of discussion about WordPress Brute Force attacks. With that discussion has come a lot of speculation as well. What are they doing? Is it a giant WordPress botnet? Is it going to destroy the internet? Well, as you would expect of any good geeks we set out to find a way to find out.
What Is Fort Disco

• Windows-based botnet
  – Discovered July 2013, dates back to May 2013
  – 18 known variations
  – 21 command-and-control sites

<table>
<thead>
<tr>
<th>PE signature block</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Copyright</strong></td>
</tr>
<tr>
<td><strong>Publisher</strong></td>
</tr>
<tr>
<td><strong>Product</strong></td>
</tr>
<tr>
<td><strong>Original name</strong></td>
</tr>
<tr>
<td><strong>Internal name</strong></td>
</tr>
<tr>
<td><strong>File version</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
It’s Also A Funny Name..

Botnet Operation

• Malware unpacks itself with a modified UPX
• Main code written in Delphi
• Writes a copy of itself to one of
  - C:\Documents and Settings\{user}\Start Menu\Programs\Startup\n  - C:\Documents and Settings\All Users\Application Data\System\ & HKCU\Software\Microsoft\Windows\CurrentVersion\Run
• Connects to the C&C control address hardcoded in the binary
• Starts to send a huge number of HTTP login requests to many different sites
First HTTP Request

POST /cmd.php HTTP/1.0
Host: [xxx]
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/4.0 (compatible; Synapse)
Content-Type: application/x-www-form-urlencoded
Content-Length: 8

status=0
Second HTTP Request

GET /cmd.php HTTP/1.0

HTTP/1.1 200 OK
[snip]

1
30
http://[xxx]/pass_bot_pull/1162735.txt
admin
580
Second HTTP Request

GET /cmd.php HTTP/1.0

HTTP/1.1 200 OK

1 ← status, 1 = attack, 0 = idle

30

http://[xxx]/pass_bot_pull/1162735.txt

admin

580
Second HTTP Request

GET /cmd.php HTTP/1.0

HTTP/1.1 200 OK
[snip]

1
30 ← number of threads
http://[xxx]/pass_bot_pull/1162735.txt
admin
580
Second HTTP Request

GET /cmd.php HTTP/1.0

HTTP/1.1 200 OK
[snip]

1
30

http://[xxx]/pass_bot_pull/1162735.txt ←
   target URL list

admin
580
Second HTTP Request

GET /cmd.php HTTP/1.0

HTTP/1.1 200 OK

[snip]

1
30

http://[xxx]/pass_bot_pull/1162735.txt

admin ← username (can also be a URL)

580
Second HTTP Request

GET /cmd.php HTTP/1.0

HTTP/1.1 200 OK

[snip]

1
30

http://[xxx]/pass_bot_pull/1162735.txt

admin

580 ← target timeout value
Botnet Operation

• The botnet controller sets
  – List of target URLs
  – Username
  – List of passwords

• Army of infected machine
  – Spin up attack threads
  – Try target URLs with various combinations of usernames and passwords
  – Successful username/password combinations are POSTed to the C&C at /bruteres.php
Target HTTP Login

POST /administrator/index.php HTTP/1.0
Host: [target]
Keep-Alive: 300
Connection: keep-alive
Cookie: 89850dd76e06caal7bb8a7aff28da85e=0b9726a831ecad362155f69f69b7ba08
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 99
Referer: [victim]/administrator/index.php

username=admin&passwd=jonathan&lang=&option=com_login&task=login&c584303d082ebf9768a02f5d4c1b6de0=1
POST /administrator/index.php HTTP/1.0
Host: [target]
Keep-Alive: 300
Connection: keep-alive
Cookie: 89850dd76e06caa17bb8a7aff28da85e=0b9726a831ecd362155f69f69b7ba08
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 99
Referer: [victim]/administrator/index.php

username=admin&passwd=jonathan&lang=&option=com_login&task=login&c584303d082ebf9768a02f5d4c1b6de0=1
Passwords

- Supports dynamic values
  - "{domain}" and "{zone}"
  - Assume target is "http://umich.edu/wp-login.php"
    - "{domain}" -> "umich"
    - "{zone}" -> "edu"
    - "{domain}.zone" -> umich.edu
- Password list varies from 150 – 10,000 entries
  - Common "admin", "password", "batman"
  - Also "12345678900987654321", "{domain}123"
Usernames & Target Lists

• Usually a small list of usernames
  – ~1-5
  – Normally “admin”, “administrator” or “{domain}”

• ~500,000 target sites per C&C
  – Usually doled out around 5,000 sites at a time
    • Lots of overlap between infections
How Does The Malware Get Installed?

Original filenames supply some clues

maykl_lyuis_bolshaya_igra_na_ponizhenie.exe
proxycap_crack.exe
MICHAEL LEWIS

THE BIG SHORT

INSIDE THE DOOMSDAY MACHINE
Order ProxyCap

All you need is a valid credit card and an email address! Your license key will be emailed to you immediately after ordering. Simply choose your product below and you will be taken to a secure order form:

- **ProxyCap for Windows**
- **ProxyCap for Mac**
- **ProxyCap for Windows Phones**

Each license includes 3 years of updates. This means your license key will work with new versions released up to 3 years after the date of the original purchase.

We offer volume discounts on purchases of 2 or more licenses of ProxyCap. Discounts are automatically calculated during checkout.

If you have any questions about the status of your order or pricing options, please feel free to contact us.
How Does The Malware Get Installed?

• Collaboration with other researchers provided some more clues
  – PPI = “pay per install”

@thedude13 @botherder @mattbing
Infection vector in this case was Russian PPI network, probably using this botnet
exposedbotnets.com/2013/09/towi4-...
Are We Done Yet?

• If we were focused on just the malware we’d be done with our analysis

BUT
Remember This?

```bash
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php BAD TXT <3 temp_brut st
GET cmd.php BAD TXT <3 temp_brut st
GET cmd.php good status 1(brut REST
GET cmd.php BAD TXT <3 temp_brut st
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
GET cmd.php BAD TXT <3 temp_brut st
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php BAD TXT <3 temp_brut st
GET cmd.php BAD file_exists temp_br
GET cmd.php BAD TXT <3 temp_brut st
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
GET cmd.php BAD TXT <3 temp_brut st
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
GET cmd.php BAD TXT <3 temp_brut st
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
GET cmd.php BAD TXT <3 temp_brut st
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
GET cmd.php pass_bot NULL, ip bot:
GET cmd.php select 5000 new URL, ip
```
Oops
Bad Luck Botnet Operator

ONLINE CRIMINAL EMPIRE

PUBLISHES DETAILED LOGS
Oops

- Publicly accessible logs reveal
  - Infected IP addresses
  - Successfully compromised sites
  - Sites that have been backdoored
- The botmaster caught on changed the C&C code around July
- 25,000+ infected machines
- 6,000+ compromised sites
- 700+ backdoored sites
Infected Machines
Infected Machines

• Top countries
  – Philippines
  – Peru
  – Mexico

• Seriously under represented
  – United States
  – Western Europe
Targeted Sites

- All content management systems (CMS)
  - Joomla
    - /administrator/index.php
  - WordPress
    - /wp-login.php
  - Datalife Engine
    - /admin.php
Compromised Sites

- Joomla: 3,361
- Wordpress: 2,520
- Datalife Engine: 246
<table>
<thead>
<tr>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>RU</td>
<td>2582</td>
</tr>
<tr>
<td>COM</td>
<td>1601</td>
</tr>
<tr>
<td>UA</td>
<td>348</td>
</tr>
<tr>
<td>NET</td>
<td>329</td>
</tr>
<tr>
<td>ORG</td>
<td>254</td>
</tr>
<tr>
<td>INFO</td>
<td>110</td>
</tr>
<tr>
<td>KZ</td>
<td>99</td>
</tr>
<tr>
<td>US</td>
<td>84</td>
</tr>
<tr>
<td>BY</td>
<td>76</td>
</tr>
<tr>
<td>xn--p1ai (рф)</td>
<td>65</td>
</tr>
<tr>
<td>Password</td>
<td>Count</td>
</tr>
<tr>
<td>--------------</td>
<td>-------</td>
</tr>
<tr>
<td>admin</td>
<td>893</td>
</tr>
<tr>
<td>123456</td>
<td>588</td>
</tr>
<tr>
<td>123123</td>
<td>371</td>
</tr>
<tr>
<td>12345</td>
<td>360</td>
</tr>
<tr>
<td>{domain}</td>
<td>248</td>
</tr>
<tr>
<td>pass</td>
<td>218</td>
</tr>
<tr>
<td>123456789</td>
<td>171</td>
</tr>
<tr>
<td>1234</td>
<td>150</td>
</tr>
<tr>
<td>abc123</td>
<td>136</td>
</tr>
<tr>
<td>123321</td>
<td>131</td>
</tr>
</tbody>
</table>
What Did The Attacker Do?

• Installed the FilesMan PHP backdoor on 700+ sites
  – Upload/download files
  – Execute commands
  – Elevate privileges
    – As mod_system.php or jm.php
    – Password protected

• Several PHP scripts to import Tumblr posts
  – Not used?
### File manager

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Modify</th>
<th>Owner/Group</th>
<th>Permissions</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<td>mod_system.php</td>
<td>64.56 KB</td>
<td>2013-06-19 13:25:23</td>
<td></td>
<td>drwxr-xr-x</td>
<td>R T</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Change dir:

- Make dir: (Writeable)
- Execute:

#### Read file:

- Make file: (Writeable)
- Upload file: (Writeable)
  - Browse...
What Did The Attacker Do?

- Styx exploit kit on 5 sites
  - NOT activated
  - Client-side drive-by exploits
  - PHP script that redirects to second stage
    - If browser is one of “MSIE”, “Firefox”, or “Opera”
if(isset($_POST['result']) and strlen($_POST['result'])>3)
{
Also be careful with putting image behind text... most of the time that's frowned upon in
the design world, unless it's a simple gradient or something... Copy that text and
paste it into pastebin or something, then give us a link..... bot_stop [0,1]

#logs("->POST bruteres.php good result: ".$_POST['result']." id:".$out_bot['id']
["]." ip": ".$_SERVER['REMOTE_ADDR'].":$_date('Y-m-d h:i:s');

$g = explode("\r\n",trim($_POST['result']));

MAKE 3D TEXT IN SONY VEGAS PRO 11... ALSO READ the readme txt file. It has
Attribution Is The New Hotness

• This is rampant speculation
• *The botmaster is Russian*
  – The majority of compromised sites are in Russia and the Ukraine
  – Most of the C&C sites are in Russia or the Ukraine
  – An error string was found “Не могу подключиться к базе данных!”
    • “Unable to connect to database!”
  – The default charset of FilesMan was “Windows-1251”
    • Cyrillic
Attribution Is The New Hotness

• More rampant speculation
• *The botmaster is Russian*
  – The bot was written in Delphi, favored by Russian malware
  – The Datalife Engine platform is popular in Russia
  – Some of the variants may have been installed as part of a Russian PPI campaign
• It’s not clear if all the C&Cs are part of the same campaign or same actors
  – I could be, and probably am, wrong
Fort Disco Variants

• Fort Disco was active late May 2013 and continues today

• Early variant targeted FTP
  – Successfully finds anonymous FTP accounts. i.e., negligible value

• Sept 2013 a new variant appeared that targets POP3 accounts
  – 141 e-mail accounts
Soooo... Who Cares?

• These attacks are targets of opportunity
  – Passwords are weakest of the weak
  – The bad guys always go for the soft underbelly
  – Sometimes blogs are poorly managed or forgotten

• How is this different than a set of compromised Windows machines?
Which Has More Bandwidth? This..
..Or This?
Soooo... Who Cares?

• Brobot attacks in late 2012 – early 2013
  – Utilized compromised WordPress sites to launch massive DDoS attacks on US financials
  – Operation Ababil
• No evidence Fort Disco is related to this
• Seamy underbelly of the botnet world
• Limits of static and dynamic malware analysis
• Fort Disco affords a rare opportunity to examine the innards of a botnet
• Attacks against CMSs will continue and exhibit a unique risk
Questions?