Botnets

Peter Moody
University of California at Santa Cruz
Information and Technology Services
peter@ucsc.edu
Agenda: Botnets

- What are they?
- Where are they?
- What do they do?
- How are they detected?
- How do we mitigate this problem?
Terms

- Bot/Zombie
- Botnet
- C&C
  - Command and Control
- Miscreant
  - The person controlling the C&C
- Darknet
  - Unallocated monitored IP space.
- IRC
  - Internet Relay Chat “IRC is just multiplayer notepad”
What are they?

Remotely controlled zombie computers
Connect back programs installed on infected computers.
Lots of infection vectors

Windows:
- lsass
- dcom
- Messenger service
- Weak passwords
- Open network shares
- Brittney_Spears.JPG.exe

Unix:
- ssh vulnerabilities
- misconfigured services

MJ and the original zombie army
Where are they?

- Widely seen in large unsecured networks.
  - University residential networks.
    - Academic networks not immune
  - Home broadband connected computers.
  - Everywhere

<anon.hero> Where are they? <anon.hero> _everywhere_ <anon.hero> and I do mean everywhere
What do they do?

- Anything the owner wants them to.
  - Spread the love.
  - DDoS.
    - Personal fame and glory or
    - For hire.

- Spam farms
  - Spam expert Steve Linford says that 70 percent of spam now comes from botnets – ZDNet UK, September 22, 2004.
    - http://news.zdnet.co.uk/internet/security/0,39020375,39167561,00.htm

- Information capture
  - CC numbers
  - Financial institution logins

- Adware/Spyware
- In short - Profit.

“If it don't make dollars – It don't make sense” - Master P
Botnet Operation – points of interest

Of Note:

Any host in the botnet can become the controller in a matter of seconds.

Short TTLs on the A-record mean that every member of the botnet will update to the new controller in a matter of minutes.
Botnet Operation – IP migration

h4cker.example.com points machine in university A. University A gets word and cleans the machine.

H4cker finds out and quickly updates A record for h4cker.example.com to point to a compromised computer on a cable modem in New York.

```dns
;; ANSWER SECTION:
h4cker.example.com. 60 IN A 10.1.1.1

;; AUTHORITY SECTION:
example.com. 43200 IN NS ns1.example-nameservice.com.
exmaple.com. 43200 IN NS ns2.example-nameservice.com.
```

```dns
;; ANSWER SECTION:
h4cker.example.com. 60 IN A 192.168.1.1

;; AUTHORITY SECTION:
example.com. 43200 IN NS ns1.example-nameservice.com.
exmaple.com. 43200 IN NS ns2.example-nameservice.com.
```
Whack-a-mole

UCSC security team attacking bots
How are they detected – traffic analysis

- Netflow analysis
- DNS log analysis
  - A records are hard-coded. Who's looking for “evil” records?
  - What else are they looking for?
  - Not doing DNS logging? It’s critical. (bind version recommendation)
- tcpdump/ngrep/snort/ethereal
  pcap capture analyzed in ethereal and “follow stream” turned on for one resnet host.

-> JOIN #^r3s-3^# r00t
<- NetworkHub 302 xaziwphjt:xaziwphjt=+~qbglnxtgr@XXX.resnet.ucsc.edu
<- xaziwphjt!~qbglnxtgr@XXX.resnet.ucsc.edu JOIN :#^r3s-3^#
<- NetworkHub 332 xaziwphjt:^r3s-3^#:%advscan dcom135 150 2 999 -b -r -s

- Very tedious, not always successful but useful in convincing DNS operators, colo security folk and registrars to take action

- Honey pots/Reverse Engineering/etc.
How are they detected - dns

Home-grown tools for examining DNS logs.

<table>
<thead>
<tr>
<th>client</th>
<th>up</th>
<th>class</th>
<th>type</th>
<th>query</th>
<th>time</th>
<th>dns</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.114.XXX.XXX</td>
<td>NoTest</td>
<td>E</td>
<td>A</td>
<td>badguy.example.org</td>
<td>Nov 5 14:29:55</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>169.233.xx.x</td>
<td>NoTest</td>
<td>E</td>
<td>A</td>
<td>badguy.example.info</td>
<td>Nov 5 10:03:53</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td>169.233.xx.xx</td>
<td>NoTest</td>
<td>E</td>
<td>A</td>
<td>pwned.example.net</td>
<td>Nov 5 00:21:22</td>
<td>192.168.99.99</td>
</tr>
<tr>
<td>169.233.xx.xx</td>
<td>NoTest</td>
<td>E</td>
<td>A</td>
<td>1.br34k.computers.example.info</td>
<td>Nov 5 09:48:29</td>
<td>10.3.9.39</td>
</tr>
<tr>
<td>169.233.xx.xxx</td>
<td>NoTest</td>
<td>E</td>
<td>A</td>
<td>r00t.example.info</td>
<td>Nov 4 23:31:23</td>
<td>10.33.44.55</td>
</tr>
<tr>
<td>169.233.xx.xxx</td>
<td>NoTest</td>
<td>E</td>
<td>A</td>
<td>b4dirc.example.info</td>
<td>Nov 5 09:13:25</td>
<td>192.168.2.3</td>
</tr>
<tr>
<td>169.233.xx.xxx</td>
<td>NoTest</td>
<td>E</td>
<td>A</td>
<td>i.c4n.h4ck.example.info</td>
<td>Nov 5 09:36:45</td>
<td>172.16.99.99</td>
</tr>
</tbody>
</table>

Anything to help increase the signal to noise ratio of a standard day's logs (~1 million records at UCSC)
How are they detected - darknet

DarkNets and Argus.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>TTL</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>0.0.0.5</td>
<td>v2.0</td>
<td>10.0.1.128</td>
<td>6667</td>
<td>tcp</td>
<td>1</td>
<td>man</td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>128.114.XX.XX</td>
<td>20816</td>
<td>10.0.1.128</td>
<td>6667</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>128.114.XX.XX</td>
<td>4028</td>
<td>10.0.1.128</td>
<td>9036</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>128.114.XX.XX</td>
<td>2306</td>
<td>10.0.1.128</td>
<td>9036</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>128.114.XX.XX</td>
<td>9033</td>
<td>10.0.1.128</td>
<td>9036</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>128.114.XX.XX</td>
<td>3305</td>
<td>10.0.1.128</td>
<td>6667</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>128.114.XX.XX</td>
<td>40383</td>
<td>10.0.1.128</td>
<td>9036</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>128.114.XX.XX</td>
<td>50321</td>
<td>10.0.1.128</td>
<td>9036</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>128.114.XX.XX</td>
<td>49478</td>
<td>10.0.1.128</td>
<td>9036</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>128.114.XX.XX</td>
<td>24893</td>
<td>10.0.1.128</td>
<td>6667</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>12-15-04</td>
<td>15:26</td>
<td>169.233.XXX.XXX</td>
<td>1582</td>
<td>10.0.1.128</td>
<td>54123</td>
<td>tcp</td>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>

Have a client (from argus) looking for 10.0.1.128:54123/tcp

```
$ ./bin/cc.pl -d 1 -l -c 169.233.XXX.XXX | grep 10\.0\.1\.128
169.233.XXX.XXX NoTest        A   1.4m.1337.example.com                 Dec 15 15:20:39  10.0.1.128
169.233.XXX.XXX NoTest        A   1.4m.1337.example.com                 Dec 15 15:21:39  10.0.1.128
169.233.XXX.XXX NoTest        A   1.4m.1337.example.com                 Dec 15 15:22:39  10.0.1.128
169.233.XXX.XXX NoTest        A   1.4m.1337.example.com                 Dec 15 15:23:39  10.0.1.128
```

Peter Moody – UCSC – peter@ucsc.edu
Getting rid of the problem.

So how do we stop these guys?

Their reliance on DNS is currently the easiest weakness to take advantage of.
Three main ways to get them shut

- **IP termination** - Ask the IP owner to kill the machine they are using.
- **DNS termination** - Ask the DNS operator hosting the miscreant's domain to blackhole the hostname/domain or kill the account.
- **Domain termination** – Ask the registrar to kill the miscreant's domain.
Shutdown – Law Enforcement

- Most effective.
- Most difficult.
- Most commitment.

Often overworked/Understaffed. (aren't we all?)

Have the ability to compel unresponsive registrars and ns providers to act.
How are they shutdown?

- **IP provider can be contacted.**
  - Often points to University network space – we tend to react rather quickly to reports of C&C's on our network
  - Occasionally an Evil record will point to the same address for an extended period of time.
  - Almost guaranteed to lead to whack-a-mole.
  - Established relationship will get you quicker service.
    - Knowing the key-words to get your complaint elevated
  - Rapport.
How are they shutdown – dns admins

;; AUTHORITY SECTION:
h4cker.biz. 43200 IN NS ns1.example-nameservice.com.
h4cker.biz. 43200 IN NS ns2.example-nameservice.com.

- pcap files aid tremendously.
- Rapport, building a relationship.
  - quickly find which Providers actually respond to complaints
  - find ways to bypass those providers who don't respond.
  - upstreams/coordination among peers/registrars

- Can get into the ever enjoyable game of “name server whack-a-mole”
  - 1 or 2 shutdowns and the miscreants usually go away (*)

(*) Important to note that by “go away”, I don’t mean that the baddies up and leave, I mean that they figure their particular A record has been compromised and they go off to create a new one.
dns admin communication

• Information that helps your reports.
  - dig output:

    dig shows it currently points to:

    ;; ANSWER SECTION:
    h4cker.example.com. 60 IN A 10.1.1.1
    ;; AUTHORITY SECTION:
    example.com. 43200 IN NS ns1.example.com.
    example.com. 43200 IN NS ns2.example.com.

  - History of Movement:

    A quick rundown of their dns mobility:
    1 Nov  –  first-name-service.com
    3 Nov  –  second-name-service.com
    4 Nov  –  third-name-service.com
    10 Nov  –  fourth-name-service.com

  - History/Relationship with DNS admins.
    • An established relationship will yield quicker results.
How are they shutdown - registrar

- The holy grail – the Registrar.
  - Very difficult to convince on merit alone.
  - Complaint threshold.
    - Hearing a lot about this domain? Shut us up. Kill him!
  - If all else fails, is the whois information correct?
    - Are they sure?
      - Are they really sure?
  - No whack-a-mole.
  - Rapport, Rapport, Rapport.
Shutdown policies that would help

DNS Admins -
- Extended TTL's on shut records and RR's
  - Caching servers
- Unified address for shut records
  - CNAME to locked record
    - Helps us determine that record has been already id'd.
    - Flag on users pointing to that (hiding out)
  - 127.0.0.1/localhost – keeps all traffic off the net

Registrars -
- REGISTRAR LOCK for shut RR's
  
  REGISTRAR-LOCK flag can be used to prohibit domain name transfer from one registrar to another.
Other things that would help

Registrars -
  - AUPs which permit shutdowns.
    - Forged whois/Credit Card/Address
    - Complaint threshold.
    - Three strikes.
  - Consistency in enforcement, across registrars
  • Consistency across Name Service Provider AUPs.
  • More registrars and DNS operators who shutdown for AUP violations.
    - This problem isn't getting any better – their lack of action is helping the bad guys
Trends


Controlling over alternate protocols
- IM
- HTTP
- P2P (phatbot)

Malware exploiting bugs in other malware.
What can we expect from here - How can they make our lives harder?

- **Use of encryption.**
  - Not as common as one would expect but already in use today.
- **Use some method other than DNS to resolve the controller.**
- **Recursive resolvers**
Important points to take away

- This is not going away any time soon
  - As long as there is motivation, there are people who will do this.
    - Take away motivation – Get Law Enforcement involved as often as possible
  - Likely just going to get more difficult to spot.
Best practices

- **Reformat Reinstall**
  - Our experience has been that throwing multiple AV/Anti-Spyware products at an infection may solve the problem. But is it worth your time?

- **If you do decide to try - remember**
  - No **one** tool is ever going to catch everything.
  - Comprehensive arsenal is a must.
    - What you typically see will determine what you use.

- **More to go here**
Resources/References/Tools

- **John Kristoff** (from whom I have shamelessly stolen at every opportunity)
  - [http://www.nanog.org/mtg-0410/real/botnets.ram](http://www.nanog.org/mtg-0410/real/botnets.ram)
  - `<jtk>: pjm: don't think i can help much more than that, internet2.edu folks are strange beasts sometimes.`

- **Team Cymru**
  - [http://www.cymru.com](http://www.cymru.com)

- **Nsp-security**

- **Unisog – UNIversity Security Operators Group**

- **Argus**
Questions?