Who I am

- MessageLabs Senior Anti-Spam Technologist
- One of the original SpamAssassin developers
- Member of a private community of botnet trackers
Who I am NOT

- Black/grey hat
- “Hacker/Cracker” of any sort
- IDS expert
- Malware expert
Botnet Evolution
- Botnets previously used by hackers as toys
- 2004: MyDoom mass mailer
  - Spam botnet creator on a massive scale
- Bots are a spammer’s commodity
1. Virus writer sends malware onto the Internet to infect vulnerable machines.

2. Virus finds vulnerable machines and "recruits" them into a botnet.

3. Attacker sends command to an IRC server.

4. Botnet "zombies" execute attack.

Denial of service attacks, spam distribution, etc.

Botnet

Thousands to millions of "zombies" machines awaiting instructions to launch an attack.

Internet
Status 2008

- Bots responsible for 90% of spam
- Billions of emails every hour
- Botnets built, sold and rented for financial gain
- Millions of infected PCs
- We currently track spamming botnets by IP
  - 6 million IPs active daily
How did we get here?

- Distribution is so much easier
- Money is involved: “spam may be bigger than the global drug trade” -- US LEO
- AV sucks
The AV Situation

- Team Cymru tested 30k virus samples from 1 day
- Tested against over 30 AV engines
  - Day 0: 20% detected
  - Day 30: 50% detected
- This will not stand, ya know
The AV Situation

- “I’ve tried 3 AV engines and found nothing”
- Malware removes AV
  - Or installs “custom” version
- The Linux problem -- plenty of malware, very poor AV
New Botnet Power

- Kernel based mail engines
- P2P communication with supernodes
- Encryption generated C&C hostnames
- Fast Flux hosting
- Auto-retool -- Mail, DDoS, DNS Server, Web Server
Current Mega-Botnets
Storm

- High profile botnet in the Press
- High academic interest
  - Automatic re-tool
  - Very large scale P2P distribution
  - Encrypted communication
- Temporarily killed by community action
- Currently <100k nodes
Storm’s KO

Storm/Nuwar to MSRT

October Patch Tuesday

November Patch Tuesday

December Patch Tuesday

January Patch Tuesday

February Patch Tuesday

Thousands

Aug-07  Sep-07  Oct-07  Nov-07  Dec-07  Jan-08  Feb-08  Mar-08  Apr-08
Ozdok/Mega-D

- 150,000 IPs
- But wait...
  - Now ... gone
- C&C DNS Hosted on Intercage
Asprox

- 100k IPs
- Specifically built for phishing and SQL injection attacks
- SQL injection used to infect legit sites for propagation
- Currently sending Abbey National (UK bank) Phish
Asprox
Gheg [internal name]

- 500k IPs
- Misidentified by almost all AV as Virtumonde/Mondera or Tofsee or Saturn Proxy (not a proxy)
- Sending French spams and Pharma spams
Gheg
Cutwail

- 900k IPs
- 25% of all spam
- Penis enlargement spams, propagation by greeting cards
Cutwail
Srizbi

- 1.3 million IPs
- Kernel level SMTP engine
  - Avoids software firewalls
  - VERY fast, scalable mail sender
  - Custom TCP stack
- 50% of all spam
- Reactor Mailer’s botnet
Srizbi
Detecting a Botnet - Email

How to detect botnet emails
Simple Tip

- use zen.spamhaus.org in your blocklists
- Blocks botnets and dynamic IP space
- Will take care of 80+% of your spam problem
- Very low false positive rate
- (and it’s free - this isn’t an advert!)
Botnet Mistakes

- Every spammer wants his botnet to look “legit”
- But spammers are stupid
- All major botnets send direct-to-MX
  - Rate limiting on ISP mail servers make anything else hard to scale
- Two choices:
  - 1) Add no Received headers
  - 2) Add forged Received headers
HELO/EHLO Fun

- Some (very few) skip HELO altogether
- Many exhibit “multiple personality disorder”
- Some impersonate a “famous” name
- Some impersonate the receiving server (mostly Linux malware)
- Some issue EHLO 12.34.45.67 (an RFC violation)
- HELO localhost.localdomain
More Faked Headers

- All match top Received header
- `Received: from [%IP%] by ...; (Cutwail)`
- `Received =~ /\Q({nChar[8-12]} {nChar[4-6]})\E/` (Ozdok)
- `Message-Id =~ /\<[0-9a-f]{12}\@[0-9a-f]{8}\@[0-9a-f]{8}\@[a-z]{4,10}>\$/` (Srizbi)
- Learn to spot patterns
SMTP Patterns

- Srizbi Example:
  - EHLO hostname
  - MAIL From:<spoofed@example.com>
  - RCPT To:<recipient@example.com>

Matches Sendmail style

But no Received headers
SMTP Patterns

- Gheg
  - `ehlo hostname`
    - `mail from:<...>`
    - `rcpt to:<...>`
  - And no Received headers
Detecting Fast Flux

1. Email message arrives with malicious URL

2. Victim clicks on link and the victim's computer makes a DNS request

3. DNS server returns list of IP addresses: The attacker is exploiting DNS and providing a rapidly changing set of IP addresses which point to bots on a botnet

4. Victim's computer follows the IP to the bot acting as a webserver

5. Victim is forwarded to site with malicious content

6. If the victim were to click the link at any other time they would get a different IP from the DNS, be forwarded via a different member of the botnet but end up at the same end location

7. This exploit of DNS means that it is very hard to identify the actual site that needs to be shut down
Detecting Fast Flux

[msergeant@hp-monitor msergeant]$ dig couldhistory.com

;; DiG 9.4.1-P1 <<> couldhistory.com
;; global options: printcmd
;; Got answer:
;; ====>HEADER<=== opcode: QUERY, status: NOERROR, id: 29978
;; flags: qr rd ra; QUERY: 1, ANSWER: 20, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
couldhistory.com. IN A

;; ANSWER SECTION:
couldhistory.com. 138 IN A 125.142.87.197
couldhistory.com. 138 IN A 210.155.8.197
couldhistory.com. 138 IN A 218.233.144.195
couldhistory.com. 138 IN A 218.252.230.218
couldhistory.com. 138 IN A 61.47.203.13
couldhistory.com. 138 IN A 63.64.58.33
couldhistory.com. 138 IN A 67.183.235.161
couldhistory.com. 138 IN A 69.253.247.206
couldhistory.com. 138 IN A 70.69.107.6
couldhistory.com. 138 IN A 71.130.195.107
couldhistory.com. 138 IN A 71.176.85.91
couldhistory.com. 138 IN A 76.249.160.46
couldhistory.com. 138 IN A 78.186.118.200
couldhistory.com. 138 IN A 81.5.96.244
couldhistory.com. 138 IN A 81.183.153.206
couldhistory.com. 138 IN A 82.114.213.183
couldhistory.com. 138 IN A 89.160.2.63
couldhistory.com. 138 IN A 89.208.164.109
couldhistory.com. 138 IN A 122.121.38.136

;; AUTHORITY SECTION:
couldhistory.com. 138 IN NS ns0.isthisfantastish.com.
couldhistory.com. 138 IN NS ns0.whynowithus.com.
couldhistory.com. 138 IN NS ns0.yayothergood.com.
couldhistory.com. 138 IN NS ns0.iwantfreshmeet.com.

;; Query time: 1 msec
;; SERVER: 172.17.2.11#53(172.17.2.11)
;; WHEN: Wed Mar 5 20:02:18 2008
;; MSG SIZE  rcvd: 483
Detecting Fast Flux

- Extract hostnames from URLs
- Look for low TTL A records (<=600s)
- Look for multiple /16s
- Check they flux when querying the NS directly
- Block all emails containing FF URLs
- Block mails from FF IPs
Detecting a Botnet Locally
How to know when and where your network is infected
Block port 25

- Step 1 for any network
- Block in **BOTH** directions, except to your mail server
- Firewall logs will point out PCs trying to spam
- [http://www.maawg.org/port25](http://www.maawg.org/port25)
DNS Monitoring

- Botneted PCs will do *way* more DNS queries
- MX lookups in particular
  - Normal PCs almost *never* do MX lookups
- Also check for .ru, .cn and .info lookups
- Often represent C&C hosts
Using TCP Fingerprinting

- Srizbi
- Custom TCP stack
- 24000 TCP Window Size
- `sudo tcpdump -vvv -n ip | grep 'win 24000'`
Passive Detection

- Spam Zombies are mostly pipelines, not factories
- Lots of output, lots of **input**
  - email addresses
  - DATA section
  - Obfu text
- Hosts receiving lots of data are unusual
Passive Detection

- Before doing this - please consult legal counsel
- Get flow data
  - IOS netflow or other vendor flow generators
  - flow-tools
- Many articles if you google them
- Or use a truly passive method - optical splitter
Processing Flow Data

- Archive as much as you can
- SYN$s$ often enough
- Gather feedback loop reports (AOL Scomp, Spamcop, Karmashpere, analyse XBL data)
- For IPs causing problems, analyse flow data
What you will find

- With rare exceptions, sources are US and .ca Colo.
- Proxy chaining is rare, almost non-existant
- Source IPs are easily blockable at the router, and there aren’t that many
Yes, this doesn’t help YOUR spam problem

- As responsible network admins we need to help the internet as a whole.
- I recommend investigating taking legal action against C&C hosts - that MAY ultimately have a positive impact on global spam levels, including yours
A Walled Garden

- Very useful to fence-off infected hosts
- Allow access to AV solutions
  - Perhaps on your own network rather than external
- Allow access to OS updates
- Provide web based redirect to inform user
  - And provide contact details in case remediation fails
Implementing a Darknet

- Many organisations have “Dark” IP space
- Light up that space and monitor traffic to it
- All traffic aberrant by its nature
- Larger networks will get internal traffic to the darknet
- Zero FP rate (compared to IDS)
- [http://www.team-cymru.org/Services/darknets.html](http://www.team-cymru.org/Services/darknets.html)
An infected Honeynet

- **DO NOT TRY THIS AT HOME**

- Much can be found out about malware by watching traffic flow to an infected PC

- Purposely infecting a PC with malware is DANGEROUS - please do not try this unless you know what you are doing

- Your IP will likely end up on various blacklists if you allow outbound traffic from the honeypot - though modern malware can detect throttled honeypots so you may need to allow this, and just cope with the blacklisting
Honeynet software

- A router with flow analysis
- Microsoft Windows :-(
What you will see

- Lists of emails
- Sometimes target hosts (if MX lookup done externally)
- Templates
- Some botnets use encrypted communication
  - SYN traffic still useful there
- DNS traffic always fascinating
- Outbound emails tell you what each botnet is sending, and how (e.g. SMTP patterns)
Further Reading
- http://www.uoregon.edu/~joe/zombies.pdf
- http://www.honeynet.org/
- http://www.maawg.org/about/publishedDocuments/
- http://www.messagelabs.com/threats/ - images from this presentation
Any Questions?