Botnets

Organize infected hosts (bots) into a network for controlling them

Uses:

- Distributed denial-of-service (DDoS) attacks
- Spamming
- Sniffing traffic
- Keylogging
- Spreading new malware
- Manipulating online polls/games
Command and Control

Control through an IRC server
- Bots join a specific channel on this server and treat incoming messages as commands

Over HTTP
- HTTP cannot be easily filtered by a network administration

Over peer-to-peer protocols
- Prevents a single-point of failure for the botnet

The latest and greatest – Domain Generation Algorithms
Naïve Command and Control

http://101.200.201.66
GET /last_command.php
Naïve Command and Control

http://101.200.201.66
GET /last_command.php

Zombies be no more
Slightly Less Naïve C&C

http://mymaster.net
GET /last_command.php
Slightly Less Naïve C&C

http://www.mymaster.net

What’s the address for www.mymaster.net

101.200.201.66

Bring down the Ukrainian government’s website

http://101.200.201.66
GET /last_command.php

DNS Server for mymaster.net

101.200.201.66
Slightly Less Naïve C&C

http://www.mymaster.net

What’s the address for www.mymaster.net

101.200.201.66

DNS Server for mymaster.net

101.200.201.66
Slightly Less Naïve C&C

http://www.mymaster.net

DNS Server for mymaster.net

Update IP for www.mymaster.net

101.200.222.66
What’s the address for **www.mymaster.net**

101.200.222.66

Blocks

101.200.201.66

101.200.222.66

http://www.mymaster.net

DNS Server for mymaster.net

http://101.200.222.66

GET /last_command.php
Blocking DNS Lookups

http://www.mymaster.net

What's the address for www.mymaster.net

How can you block certain DNS requests?

101.200.222.66

DNS Server for mymaster.net
Blocking DNS Lookups

Block access to untrusted DNS servers
  ▪ E.g., Through port number and IP

Filter outgoing DNS query packets

Filter incoming DNS response packets

All of the above is probably required, because
  ▪ Custom DNS server can be run on arbitrary port
  ▪ Custom DNS server over HTTPS
  ▪ Could-based DNS available
Blacklisting C&C

Blacklist 101.200.201.66
...

Monitor registration of malicious domains

What’s the address for www.mymaster.net

101.200.222.66

Update IP for www.mymaster.net

DNS Server for mymaster.net

http://www.mymaster.net
Less Naïve C&C

http://www.sdsds4gd.com

What’s the address for **www.sdsds4gd.net**

101.200.222.66

http://101.200.222.66
GET /last_command.php

101.200.222.66

DNS Server for sdsds4gd.com
Less Naïve C&C

http://www.fghsaddff.com

What's the address for www.fghsaddff.com

101.200.224.66

DNS Server for sdsds4gd.com and fghsaddff.com

http://101.200.224.66
GET /last_command.php

101.200.224.66
Domain Generation Algorithms (DGAs)

Bots use DGAs to automatically generate domain names

- E.g., using a pseudorandom number generator

The master registers the domain names before they are used

###.133. ###.247 – idpd1y###-elywj.com
###.133. ###.247 – k7-cwubgsrqj###rb.com
###.133. ###.247 – omz###1k1vgrqf.com
###.133. ###.247 – taqwucpzj###an.com
###.133. ###.247 – vhrey###-ooz6ig.com
###.133. ###.75 – o###pp1k1vgrqf.com
###.133. ###.75 – rm6dol7###cxje-ajl.com
###.133. ###.191 – id###yzib-e###j.com
###.133. ###.191 – k7-c###gsrqjebzrb.com
###.133. ###.191 – ###gpp1k1vgrqf.com
###.133. ###.191 – rm6dol###wcxje-ajl.com
###.133. ###.191 – taqwucpzj###an.com
###.133. ###.191 – vhreyveh-ooz###.com
DGA-based Solutions

Identify DGA-generated domains

- Reverse engineer algorithms
- Look for high-entropy domain names
- Look for domain names with no words in any language

Prevent communication with known DGA-generated domain names

Be proactive → register domains before the botnet master