Outline

- What’s a botnet?
- Botnet: Past and Present
- Botnet Architecture
- Botnet Protocols
What’s a botnet?
Botnet: Past

- Khan C. Smith
- Phishing and spam botnet
- 12% of all Earthlink’s Email traffic
- Estimated to have made around $3 Million...
- ... but sued for $25 Million
Botnet: Present

- Phorphiex / Trik botnet
  - Phorpiex trojan
  - 450,000 infected Windows computers
  - Sextortion and spam
  - $115K in 5 months
Other Notable Botnets:

- Storm (2007): 250,000 - 1,000,000 bots
- Kraken (2008): 500,000 bots
- Mirai (2016): 600,000 bots
Botnet Architecture
Centralized

C&C

BOT

BOT

BOT

BOT

BOT
Centralized

Advantages:
- simple
  - low latency
  - high scalability
  - easy implementation

Disadvantages:
- low robustness
  - single point (or a few points) of failure
  - easily detectable
Decentralized Peer-to-Peer
Decentralized Peer-to-Peer (fully meshed)

Advantages:
- low latency
  - no relaying
- high robustness
  - requires a minimum of 2 bots

Disadvantages:
- low scalability
  - 65,535 maximum bots if using TCP/UDP
- high visibility
  - too many connections
  - requires many coordination messages
- hard to implement
Hybrid

Advantages:
- high scalability
- low visibility
  - if the number of bots in proxy layer is kept low
- medium robustness
  - entry nodes point to C&C

Disadvantages:
- hard to implement
- high latency
  - relaying
Botnet Protocols
Communicating within the botnet

- Choice of protocol dependant on architecture of the botnet
- Not uncommon to use a combination of protocols
  - Especially true in hybrid botnets
Centralized Botnets

- **IRC**
  - Designed for text based communication
  - IRC clients implement file sharing over Direct Client-to-Client (DCC)
  - Declining usage
Centralized Botnets

- HTTP
  - Ubiquitous
  - Uses request/response structure
  - Inferior to IRC in many regards
    - No group communication
    - Higher latency
  - More common in botnets
P2P botnets

- P2P Protocols
  - Many options to choose from
  - Examples
    - Bittorrent
    - Gnutella
  - Most have all the features you need built in
    - Message relaying
    - Reliability
P2P botnets

- Neoteric Protocols
  - UDP
    - Lacks features
    - More lightweight than TCP
      - 8 bytes vs 20 bytes
    - Allows more concurrent connections
Communicating with the web

- Send spam emails
  - Simple Mail Transfer Protocol
- Generate ad revenue
  - HTTP, HTTPS
- DDoS attack
  - HTTP, UDP and TCP
Works Cited

  om-mass-spamming-sextortion-emails/
- https://pdfs.semanticscholar.org/bfae/82b6ff8044ac7d20c8c2556b62088af4a415.p
  df
- https://publik.tuwien.ac.at/files/publik_262720.pdf
- https://www.whiteops.com/blog/9-of-the-most-notable-botnets

Art and Graphics

- https://opengameart.org
- www.openpixelproject.com
- https://www.slidescarnival.com/aliena-free-presentation-template/4597