Detectie van peer-to-peer botnets

Reinier Schoof & **Ralph Koning**
System and Network Engineering
University van Amsterdam

9 februari 2007

Inhoudsopgave

Introductie

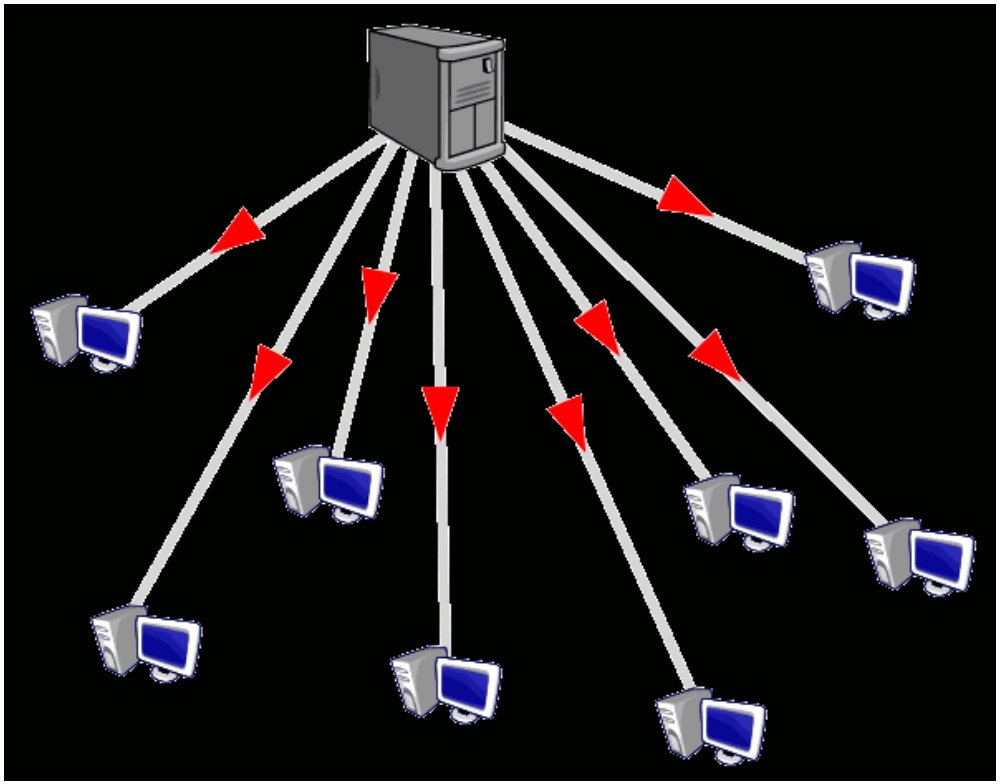
- Bedreigingen op het internet
- Opkomst p2p botnets

Achtergrond

- Peer-to-peer
- Botnets

Achtergrond - Peer-to-peer

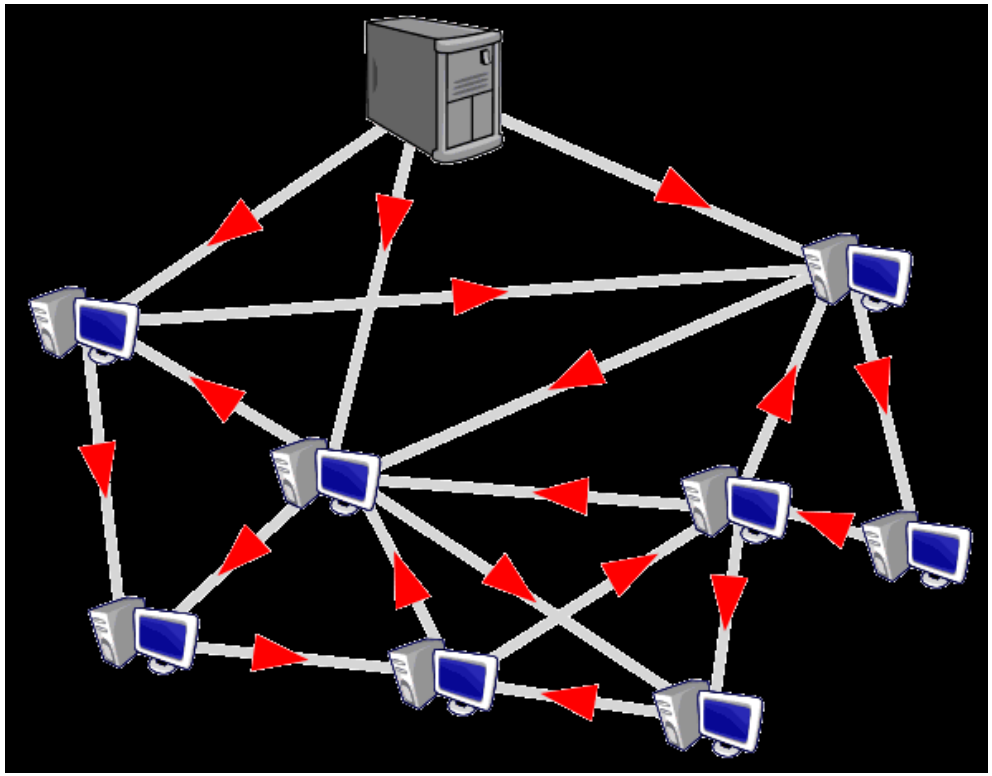
Centraal punt dat met alle clients in verbinding staat



Figuur: Klassiek server-client model

Achtergrond - Peer-to-peer

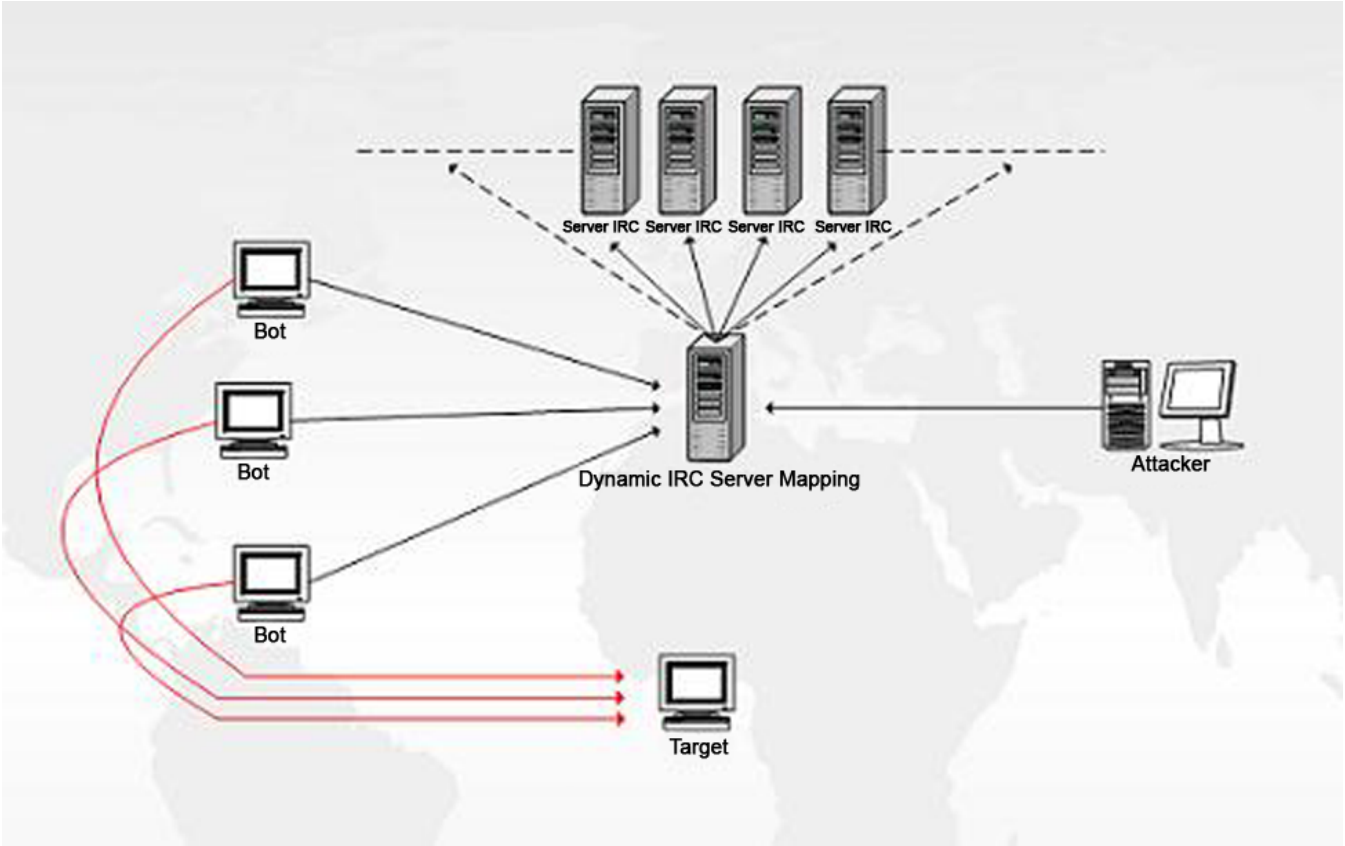
Alle peers hebben onderling verbindingen



Figuur: Peer-to-peer model

Achtergrond - Botnets

Bots verbonden met IRC server



Figuur: IRC botnet

P2P botnets

- Geen centraal commandpoint
- Verspreiding over P2P netwerken
- Mogelijk gebruik van reeds bestaande P2P netwerken

P2P bot analyse

- Proefopstelling:
  - 3 XP machines
  - BSD router met softflowd en nfdump
  - Tcpdump
- Sinit:
  - Verspreiding malware.
  - Random IPs
  - Verstuurt pakketen naar UDP port 53
  - Webserver op TCP port 53
- Nugache:
  - DoS aanvallen
  - Hardcoded lijst met 22 IPs
  - Communiceert over TCP port 8

andere P2P bots

- Phatbot
  - DoS Aanvallen, Persoonlijke informatie stelen
  - NullSoft WASTE protocol
  - Gnutella cacheservers
- SpamThru
  - Versturen van spam.
  - Centraal commandpoint
  - Gebruikt P2P als noodoplossing
  - Kaspersky

P2P botnet-detectie

- Open poorten
  - Actieve poortscans mogelijk.
  - Lastiger door gebruik van bekende poorten.
- Mislukte verbindingen
  - ICMP Unreachable
  - TCP Reset
  - Onvolledige TCP handshakes.
- Monitor *peer discovery*
  - IP lijst valt te monitoren.
  - Alternatief is mislukte verbindingen.
- Packet-inspectie
  - IDS
  - Signatures

Tegenmaatregelen

- Nugache:
  - Hosts van hardcoded lijst blokkeren
  - Verkeer op poort 8 monitoren/blokkeren
- Phatbot:
  - Gebruikt clientstring 'GNUT'
  - Gnutella beheerders benaderen
- Sinit:
  - Monitor UDP 53 verkeer met IDS
  - Niet DNS verkeer wordt verdacht.
- SpamThru:
  - Verkeer naar command server monitoren
  - Command server blokkeren

Conclusie

- Zolang er geld te verdienen is met botnet activiteiten proberen schrijvers detectie moeilijker te maken.
- Peer discovery en open poorten blijven lastig op te lossen.
- Er zijn per bot specifieke detectieregels nodig.

Vragen

Stel gerust uw vraag!