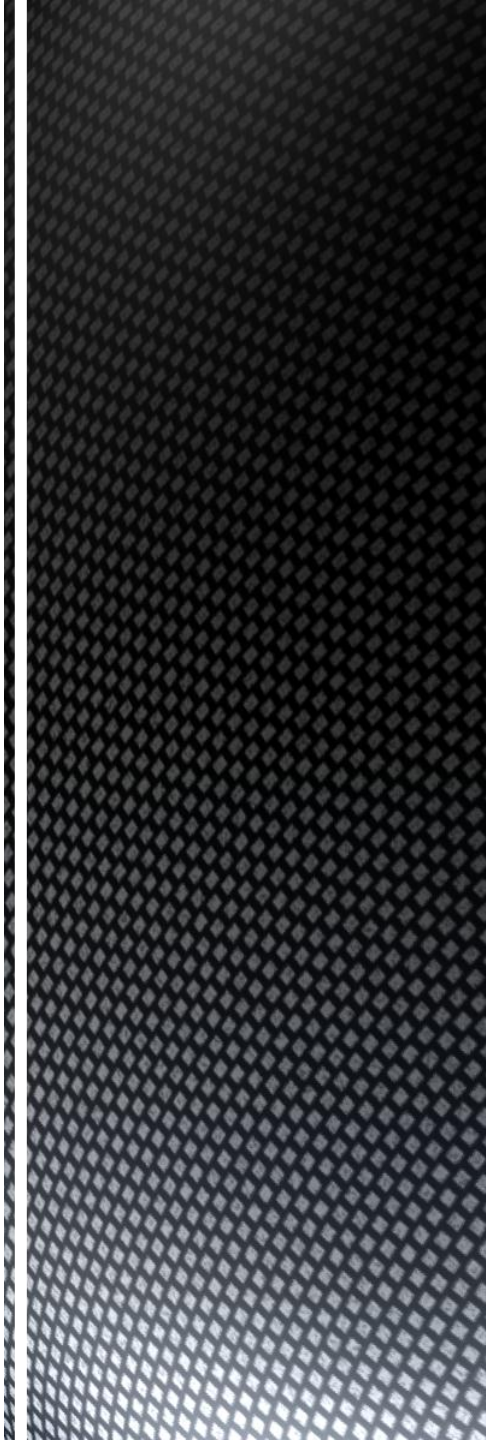
# Botnetze und DDoS

Patrick Rappensberger

Robert Löschinger

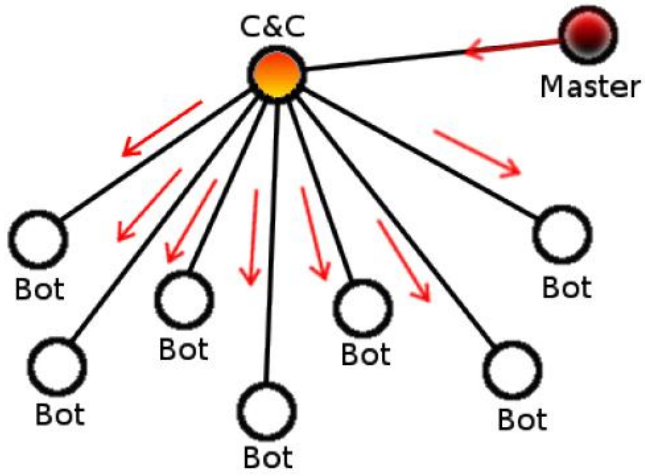


# Botnetze (Teilnehmer)

- Kontrollserver
- Zombies (Clients)
  - Malware
  - Downloads
  - Exploits
  - Manuelle Installation
- Botnetzbetreiber
- Auftraggeber

# Botnetze Kontrollarten (IRC & DNS)

- Command & Control mit IRC
- Interaktiv & Voll-duplex
- Mehrere Botnetze mit einem Server
- Private / Globale Nachrichten
- Command & Control über DNS
- Multihoming & Domain Names
- Schwerer gesamtes Netz auszuschalten

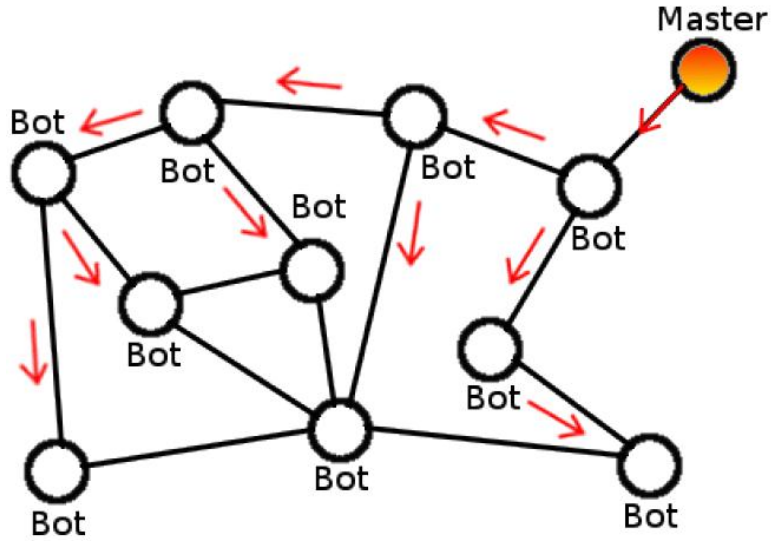


# Botnetze Kontrollarten (HTTP)

- web-basierte Command und Control Engine
- Zombies schicken SYN-Pakete zu Servern
- Keine persistente Verbindung!
- Schwieriger zu entdecken wegen Port 80
- Besser Skalierbar

# Botnetze Kontrollarten (P2P)

- Dezentral
- Zombies sind Client oder Server
- Verbreitung wie Kettenreaktion
- Leichter zu entdecken
- Identifikation des Auslösers fast unmöglich



# Botnetze Kontrollarten (FTP)

- Kaum verbreitet / Experimentell
- Phishing- oder Banking-Trojaner
- Man-on-the-Inside-Attack
- Gestohlenen Daten werden auf FTP-Servern gespeichert

# Botnetze Hauptverwendung

- Spam

| Name | Infizierte Rechner | Mrd. Spammails/Tag |
|---|---|---|
| BredoLab | 30.000.000 | 3,6 |
| Conficker | 10.500.000 | 10 |
| Cutwail | 1.500.000 | 74 |
| Grum | 560.000 | 39,9 |
| Srizibi | 450.000 | 60 |
| Rustock | 150.000 | 30 |

- Proxy
- Klickbetrug
- Botnetz interne Angriffe
- DDoS

# DDoS (DistributedDenial of Service)

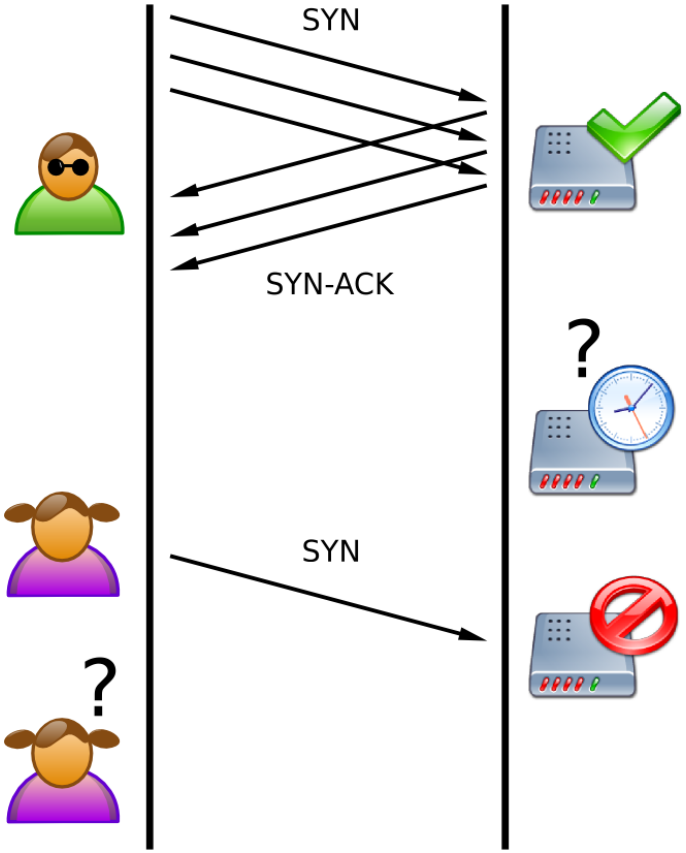
- Überlastung von Infrastrukturen
- Angreifer nicht identifizierbar

- Nicht Böswillig:
  - Verkaufsstart von populären Produkten
  - Unerwartet beliebte Artikel (News)
- Böswillig:
  - SYN-Flooding
  - DRDoS

# SYN-Flooding

- Vorgangsweise
  - Angreifer schickt SYN-Pakete an das Opfer.
  - Host schickt SYN-ACK zurück.
  - Angreifer antwortet nicht.
  - Angreifer schickt weitere SYN-Pakete

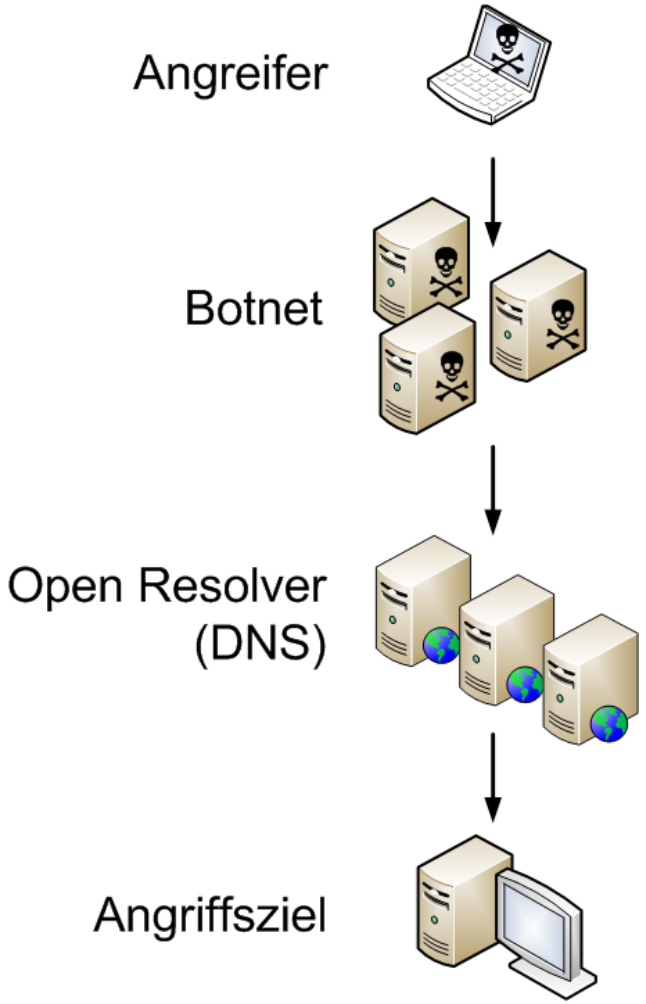
    → Netzwerkstack am Server voll




- Schutzmechanismen
  - Syn-Cookie:
    - Stackinfo wird im SYN-ACK eingebettet.
  - Mit Botnetz trotzdem eine Störung möglich.

# DRDoS (*Distributed-Reflected-Denial-of-Service)*

- IP-Spoofing
- DNS Amplification Attack
- Angriffsfaktor mal 50
- Anonymisierung
- Theoretische Gegenmaßnahmen
  - Ingress-Filter
  - TCP bei DNS



# Beispiele

- Beabsichtigte:
- Dezember 2010: Mastercard ,Visa, Paypal & Amazon im Zuge von Wikileaks Sperrung (Kollektiv)
- Mai 2012: Webseite der Stadt Frankfurt

- Unbeabsichtigte:
- 19.01.2012 Mega Registrierung wird freigegeben
- 13.11.2012 Verkaufsstart Nexus 4 (Google)
- 2009 Tod von Michael Jackson (Google & Twitter)
- News, Link- Sites

# Quellen

- Wikipedia.org
- Heise.de
- Kaspersky.com