Botnetze
und
DDOS Attacken

Übersicht

- Was ist ein Botnetz?
- Zusammenhang Botnetz DDOS Attacken
- Was sind DDOS Attacken?

Was ist ein Botnetz?

- Entstehung
- Entwicklung
- Aufbau & Kommunikation
- Motivation
- Heutige Dimensionen
- Erkennung
- Gegenmaßnahmen

Was ist ein Botnetz? (1) – Entstehung

- Ursprung im IRC
- Anfangs nicht negativ
- Virtuelles Individuum
- Automatisierte Prozesse
- Erste Fehlerausnutzung der IRC-Clients
- Würmer, Trojaner usw.

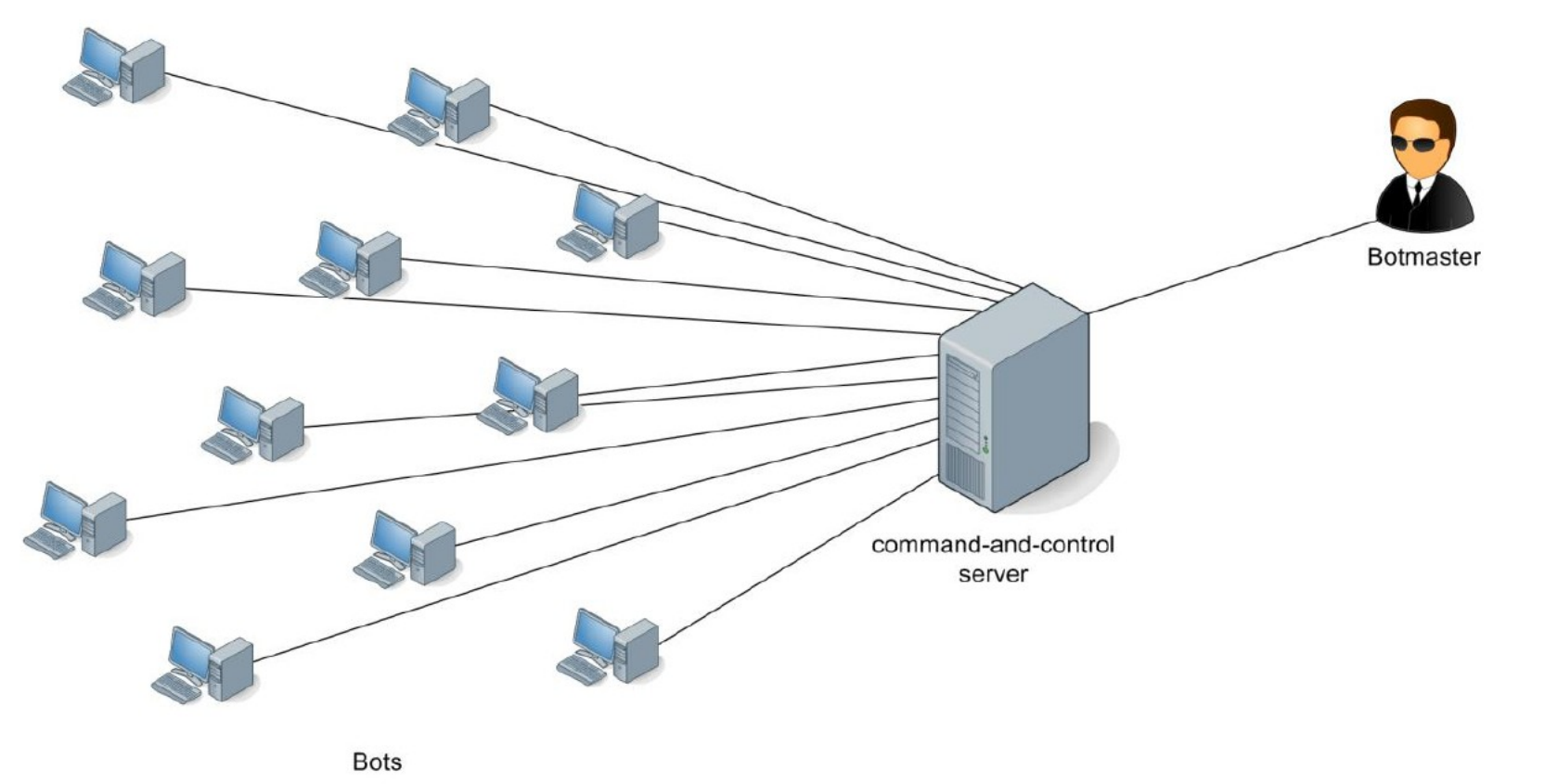
Was ist ein Botnetz? (2) – Entwicklung

- Würmer nutzen IRC-Bots zu:
  - *Kommunikation*
  - *nehmen Befehle an*
- Bot → Botnetz (Viele Zombie PCs)
- Später über p2p u.ä.

Was ist ein Botnetz? (3) – Aufbau & Kommunikation

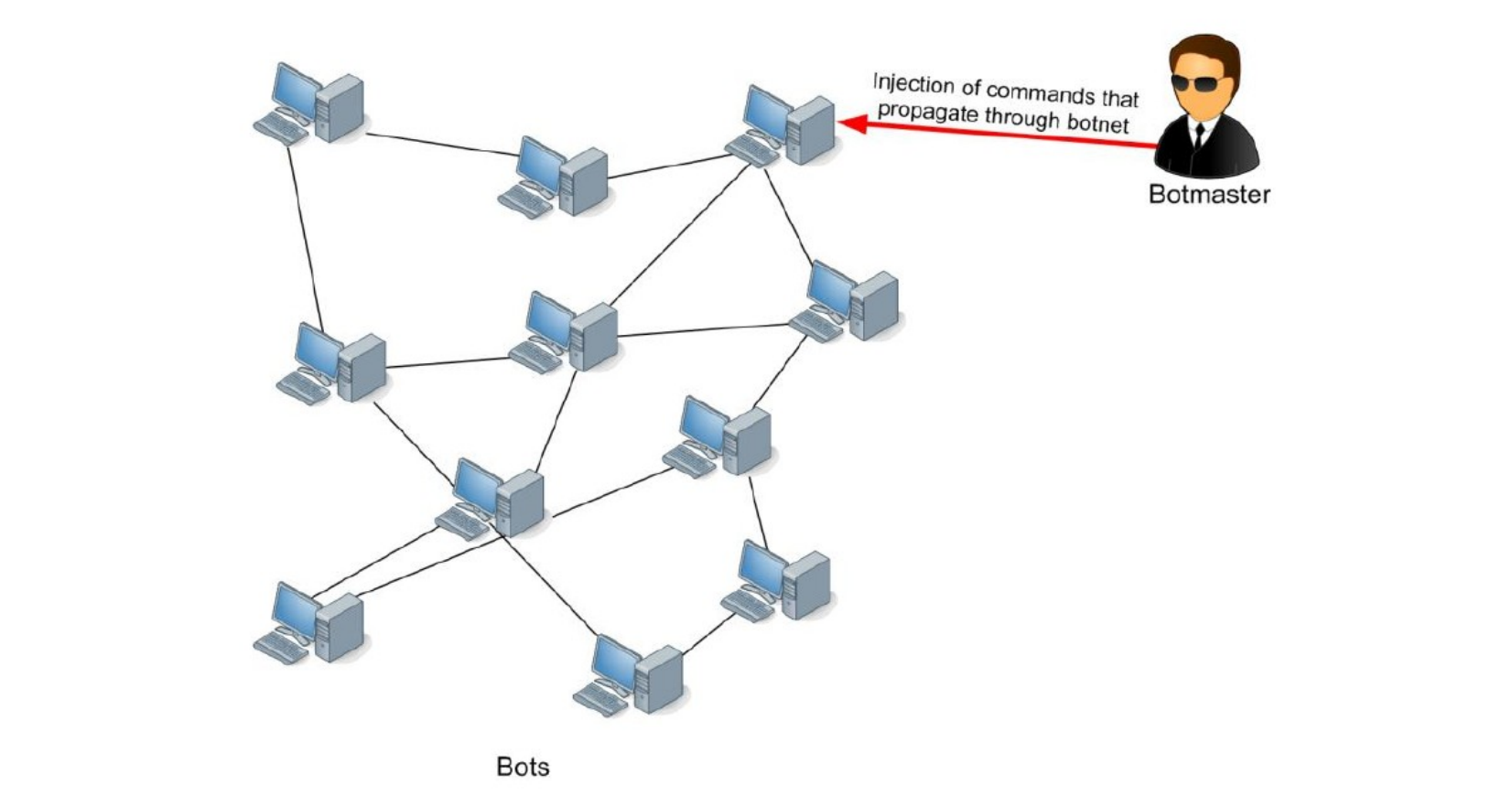
- Ähnlichkeiten mit Clouds (Dark Clouds)
  - Dezentralisiertes Scheduling
  - Unterschiedliche und unterbrechbare Ressourcen
  - Ausfallsicherheit
- Botmaster
- Command-and-control Infrastruktur
  - Zentralisiert
  - Dezentralisiert

Was ist ein Botnetz? (3) – Aufbau & Kommunikation Zentralisiert



Quelle: http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

Was ist ein Botnetz? (3) – Aufbau & Kommunikation Dezentralisiert



Quelle: http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

Was ist ein Botnetz? (4) – Motivation

- Kriminelle, politische und ideologische Zwecke
- Finanzieller Gewinn
- Informationen benutzen

Was ist ein Botnetz? (5) – Verwendung

- Informationsverbreitung Spam
- Informationen sammeln
  - Phishing
  - Kontaktdaten
  - Finanzdaten
- Informationsverarbeitung
  - z.B. Passwort aus Hash berechnen
- DDOS
- Dark Clouds

Was ist ein Botnetz? (6) – Beispiele

- Anonymous (4-chan, youtube, bot-netzte)
  - Angriff Sony PS3 Netzwerk
  - Kreditkartenanbieter
  - Amazon (nicht erfolgreich)
- Regierungen
  - USA gegen Iran (Stuxnet?)
  - China, USA, Russland

Was ist ein Botnetz? (7) – Heutige Dimensionen

Name	#Zombies	Spam-Kapazität
BredoLab	30 000 000	3,6 Mrd./Tag
Mariposa	12 000 000	?
Conficker	10 500 000	10 Mrd./Tag
Zeus	3 600 000	?
Cutwail	1 500 000	74 Mrd./Tag

Quelle: http://en.wikipedia.org/wiki/Botnet#Historical_list_of_botnets

Was ist ein Botnetz? (8) – Erkennung

- Auf Rechner selbst Antiviren-Software
- Polling Activity
- Erkennen woher die Kommandos kommen
- Signatur- oder Anomalieerkennung im Netzverkehr
- Verdächtige erkennen und Netzverkehr isolieren
- Honey Pots

Was ist ein Botnetz? (9) – Gegenmaßnahmen

- Kommunikation unterbrechen
- Kommandos verändern
- Botnetz Kommandos senden (z.B. ausschalten)
- Infizierte Rechner lokalisieren und reinigen

Was ist ein Botnetz? (9) – Gegenmaßnahmen Aktuelles

- US-Behörden wollen Coreflood-Bot von Rechnern löschen
  - Rechtliche Grauzone
  - Eingriffe Regierung in Privatspähre
- BSI ist mit Anti-Botnet-Initiative zufrieden
- Microsoft geht juristisch gegen Botnet vor
  - 277 Internet-Adressen vom Netz nehmen

Zusammenhang Botnetz DDOS Attacken

- Unterschied DOS – DDOS:
  - DOS: Denial Of Service
    - *Einzelner Rechner*
  - DDOS: Distributed Denial Of Service
    - *Verteiltes Netz (z.b.: Botnetz)*

Was sind DDOS Attacken?

- Typen
  - ICMP flood
  - Peer-to-peer attacks
  - Permanent DOS attack
- Gegenmaßnahmen

Was sind DDOS Attacken? – Typen

- ICMP flood
- Peer-to-peer attacks
- Permanent denial-of-service attacks
- Application-level floods
- Nuke
- Reflected attack
- Denial-of-Service Level II
- Blind denial of service

Was sind DDOS Attacken? – ICMP flood

- Ping flood
  - Massive Ping anfragen
- Ping of death
  - Senden von fehlerhaften Pings
  - Führt zu Systemabsturz
- SYN flood
  - Ständiger Verbindungsaufbau (ACK/SYNC)

Was sind DDOS Attacken? – Peer-to-peer attacks

- Client Software wird Exploited
- Client führt DOS Angriff aus
- Leicht zu erkennen (Basis: Signatur)
- Enorme Anzahl an Angreifern

Was sind DDOS Attacken? – Permanent DOS attacks

- Gegen Embedded Systems
- Exploited das System
- Zwingt System zu Firmwareänderung
  - Verändert
  - Fehlerhaft
  - Korrupt

Was sind DDOS Attacken? – Gegenmaßnahmen

- Verteilte Systeme verwenden
  - Cloud-Service Nutzen
  - Serverfarmen
  - Server dezentralisieren
- Signatur-, Anomalienerkennung
- Verkehr Sperren
- Firewall (gegen Korrupte Packete: z.b. Ping of Death)

Quellen

- http://ntu.botnet.tw/presentation.php -> Army of Bots
- http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard_html/
- http://www.ciresearchgroup.org/publications -> Involuntary Computing: Hacking the Cloud
- http://www.heise.de/security/meldung/US-Behoerden-wollen-Coreflood-Bot-von-Rechnern-loeschen-1234752.html
- http://www.webreaders.de/wp-content/uploads/2007/08/zombie-pc.jpg
- http://www.heise.de/newsticker/meldung/BSI-ist-mit-Anti-Botnet-Initiative-zufrieden-1200044.html
- http://www.heise.de/security/meldung/Microsoft-geht-juristisch-gegen-Botnet-vor-940227.html
- http://www.theregister.co.uk/2008/05/21/phlashing/

Fragen und howto Botnetz

- Trojaner anschaffen: Programmieren, download, kaufen
- Nütze Lücke:
  - Social Hacking
  - Website komprimitieren
  - Programme (Browser)
  - Betriebssystem (lnk-Lücke)
- Steuerung des Botnetzes
  - Webinterface, IRC, Websites, P2P, eigener Server

- *Danke für Eure Aufmerksamkeit!*