Botnetze

Funktionsweise und Sicherheitsmaßnahmen

Heiko Herrmann
Jakob Gehrmann

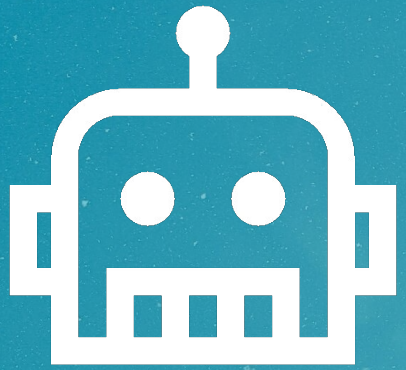
Was wir erarbeitet haben

Grundlagen:
- geschichtlich Entwicklung
- Methoden von Cyberangriffen
- Lebenszklus eines Botnetz
- Botnetz Architektur

Botznetz Arbeitsweisen und Einsatz
- Gutartige Botnetze
- Botnetz Angriffe
- Verbreitung
- Schutzmechanismen
- Verschleierung ihrer Präsenz
- Erkennungsmethoden
- Schutz gegen Botnetze

Praxisaspekt:
- Mirai-Analyse
- Simulation
- Reverseshell-Code

Gesellschaftlicher Blick
- Social Bots
- Gesetzliche Sicht
- Botnetz Ökonomie



Was sind Botnetze?

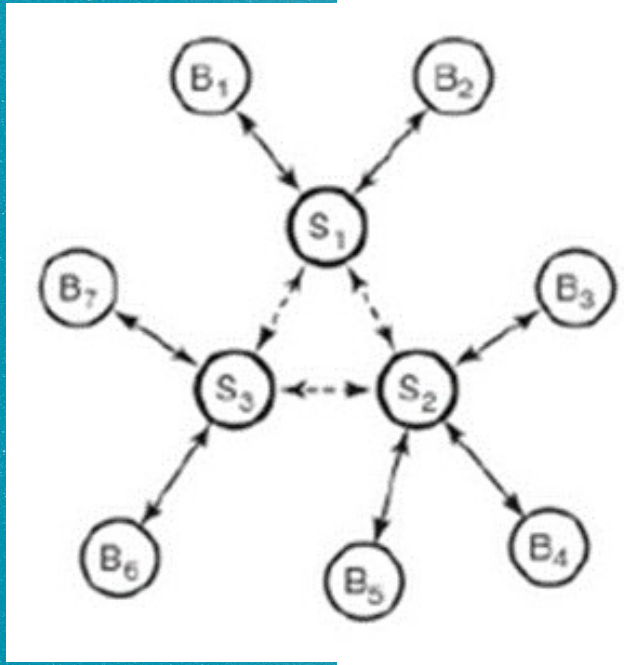
Unbemerkte Infiltrierung der Opfer-Geräte

Netzwerk aus infzierten Rechnern (Bots)

Befehlsausführung einer Kontollinstanz (Botmaster)

Meist eingsätzt von Cybercriminellen

Multi-Server



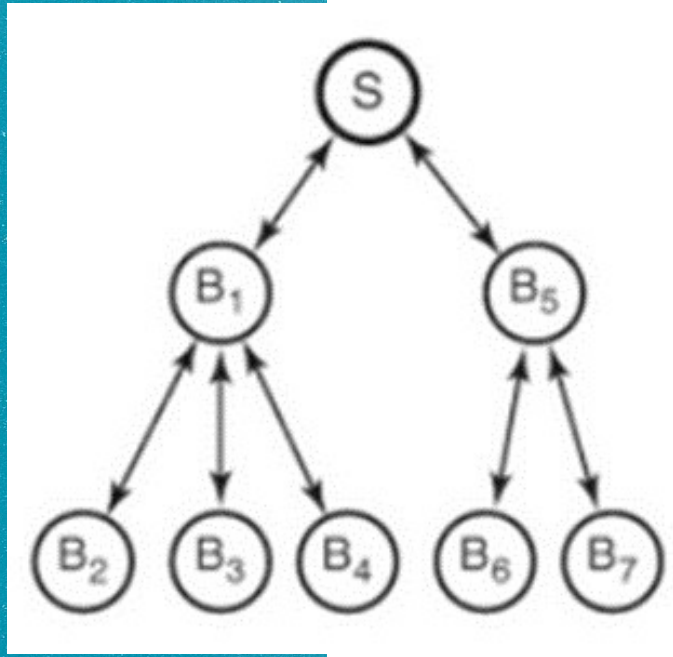
Redundanz

Vermeidung von SPOF durch den Einsatz von mehreren C&C-Servers

Dirkte Ansprache

Durch deine eindeutige verbindung zu den C&C-Servern können die Bots explzit angesprochen werden

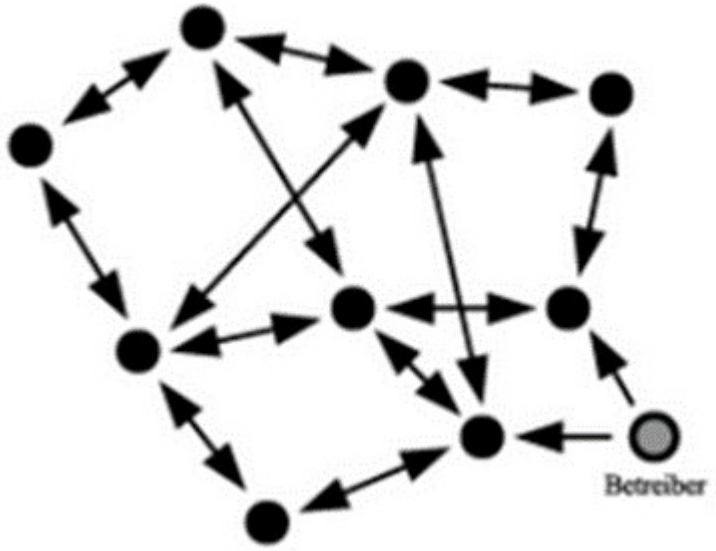
Hierarchie



Sicherheit

Erweiterung des Netzes um eine Proxyebene, zur Verschleierung des C&C-Channel

Peer to Peer



Dezentral

Steigerung der Ausfallsicherheit durch Dezentralisierung der Kommunikation, zur Befehlsübermittlung

Angriffsmethoden

DDoS

Überwältigen der Opfersysteme durch Senden großer Mengen an Traffic

Flood-Attacks

Spezialisierung der DdoS-Attacken auf Protokolle wie UDP, TCP, HTTPS, DNS

Spam

Die Verbritung von bösartigen Nachrichten an eine große Menge an Nutzergeräten

Infektion

E-Mail

E-Mails (Spam) mit Links auf infizierte Ressourcen oder bösartige Anhänge

Malvertisment

Fake Werbung die Nutzerinteraktion provoziert um zu infizieren

Drive by Download

Laden von infizierten seiten ohne das wissen von Nutzern

Evil USB

USB-Speicher als Eingabegerät, zum Ausführen des Inhalts

Thank you