(Distributed) Denial of Service

Robert Meyer

December 9, 2016

Inhaltsverzeichnis

Einführung

- In den letzten Wochen gab es immer wieder Ausfälle von grösseren Diensten.
- Das gemeinsame dieser Vorfälle war, dass diese Dienste mit riesigen Mengen an Anfragen bombardiert wurden.
- Zudem waren überwiegend Geräte aus dem so genannten Internet of Things beteiligt.

Die Ereignisse im Überblick

- 23.09.2016: Security-Journalist Brian Krebs war Ziel eines DDOS Angriffs (600 Gb/s). Trotz professionellem DDOS Schutz ist die Seite zeitweise nicht erreichbar.
- 29.09.2016: Der Hoster OVH wird attackiert. Traffic: ca. 1 Tb/s.
- 11.10.2016: Der Source Code des Mirai Botnetzes wird veröffentlicht.

Die Ereignisse im Überblick II

- 21.10.2016: Der DNS Provider Dyn wird mit Spitzenwerten von 1.2 Tb/s angegriffen. Viele populäre Angebote, die von Dyn gehostet werden, sind zeitweise nicht erreichbar (Twitter, Ebay, Netflix ...). Im nach hinein hat sich herausgestellt, dass das eigentliche Ziel das Playstation Netzwerk war.
- 27.11.2016: Grossstörung im Netz der Telekom. Ursprünglich ging man davon aus, dass eine Schwachstelle im TR-069 angegriffen wurde. Mittlerweile hat es sich herausgestellt, dass Scans auf diesen Port die Router zum Absturz gebracht haben.

Definition

- Hinter DDOS Angriffen steckt immer die Idee, die Verfügbarkeit eines angebotenen Dienstes zu verschlechtern.
- Die Datenintegrität wird nicht angegriffen.
- Es ist ist im Allgemeinen nicht das Ziel, den Host zu übernehmen.
- Es gibt unterschiedliche Möglichkeiten, derartige Angriffe durchzuführen.
- Meistens wird das Opfer mit Anfragen überlastet.

Techniken

- Softwarefehler ausnutzen z.B. ping of death.
- Reflection Attacks z.B. snurf Attack
- Traffic Amplification (z.B. ntp, dns)
- Einsatz von Botnetzen.

Botnetze

- Die ersten Botnetze tauchten Anfang dieses Jahrtausends auf.
- Jedes Botnetz besteht aus einem Command and Controll Server und vielen infizierten clients.
- Die Clients werden meist über Sicherheitlücken infiziert. Traditionell waren das früher meist Windows Systeme.
- Die Kommunikation zwischen C&C und Bots verlief früher meist über IRC. Mittlerweile werden oft HTTP(S) verwendet (Firewalls).
- Hauptverwendungszweck sind DDOS oder dictionary Atacken sowie Spamversand.
- Mittlerweile kann man Botnetze mieten.

Botnetze

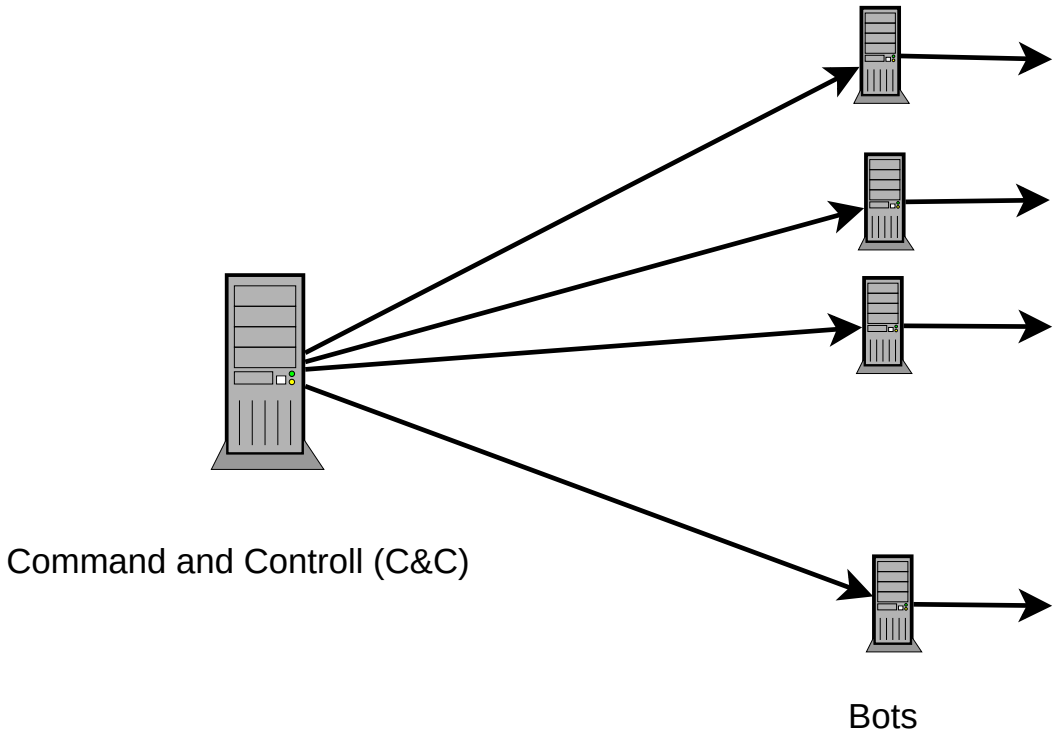
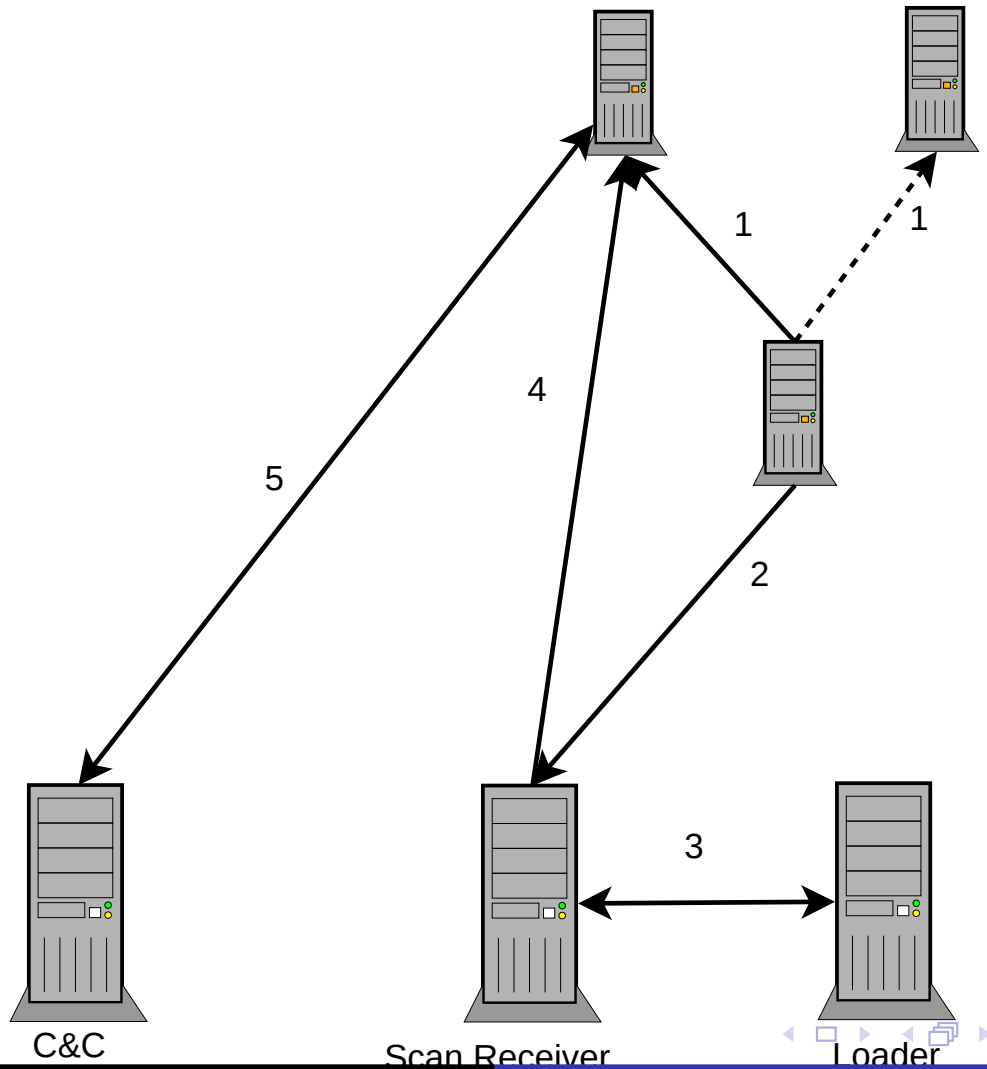


Figure: Struktur von Botnetzen

Mirai Botnet

- Ein infiziertes Gerät startet brute-force Attacken um sich via Telnet auf andere Geräte einloggen zu können.
- Falls ein Login erfolgreich war, wir diese Information an den "Scan receiver" geschickt.
- Der "Scan Receiver" merkt sich die Details, holt sich die malware vom "Loader" und ladet diese hoch.
- Das infizierte Gerät nimmt Kontakt mit dem "Command and Control" Server auf und wartet darauf, bei einer DDOS Attacke mitzumachen.

Mirai Botnet II



Besonderheiten

- Das Einfallstor für die Infektion sind Gerëte des Internet of Things mit default Passwörtern.
- Der command and control Server wird via DNS gefunden, kann also einach ersetzt werden.
- Der Schadcode kann jederzeit ersetzt werden.
- Es bleiben keine Dateien auf dem Filesystem zurück.

IOT

Als IOT (Internet of Things) werden Geräte bezeichnet, die wir für den Alltag brauchen und die mit dem Internet verbunden sind. Beispiele reichen von Kameras über digitale Videorecorder bis zu Automatisierungen im Haushalt. Oft gelten folgende Aussagen

- Meist sind die Geräte nicht sehr teuer. Entsprechend gering sind die Gewinnmargen der Hersteller. Das macht den Support unrentabel.
- Die Bedienung sollte möglichst einfach sein und keine Kenntnisse der Informatik voraussetzen.
- Updates von Sicherheitslücken gibt es oft nicht.

Opfer

Wenn man von einem Botnetz angegriffen wird, muss man sicher stellen, dass man mehr Resourcen hat, als dem Angreifer zur Verfügung stehen.

- Services verteilen (Geographisch und Netzwerk-Technisch).
- Anycast
- Firewall
- IDS
- Kommerzieller Schutz

Täter

Um nicht Bestandteil eines Botnetzes zu werden, muss man dafür sorgen, dass die eigenen Devices nicht übernommen werden können.

- Security Mailinglisten lesen.
- Regelmässige Updates.
- Traffic Monitoring.
- Unsichere Devices natten.
- Staatliche Zertifizierung von allen Geräten, die Netzwerkfähig sind.

Andere Aspekte

- DDOS ist Zensur.
- Gemäss einer Studie von Incapsula beträgt der durchschnittliche Schaden von DDOS Attacken ca. 40.000 US-Dollar pro Stunde. (https://www.incapsula.com/blog/ddos-impact-cost-of-ddos-attack.html).
- Kollateralschäden sind meist schwer auszuschliessen.