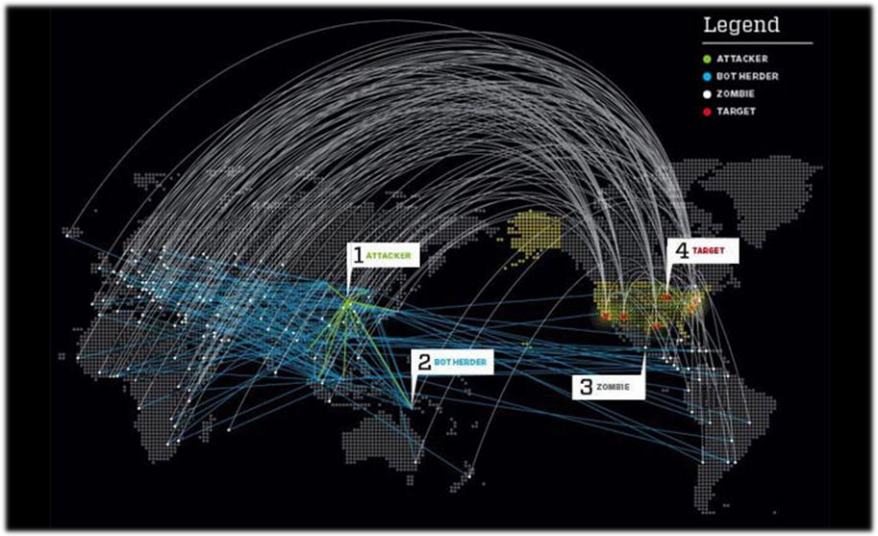
(Distributed) Denial-of-Service Attack



Inhalt

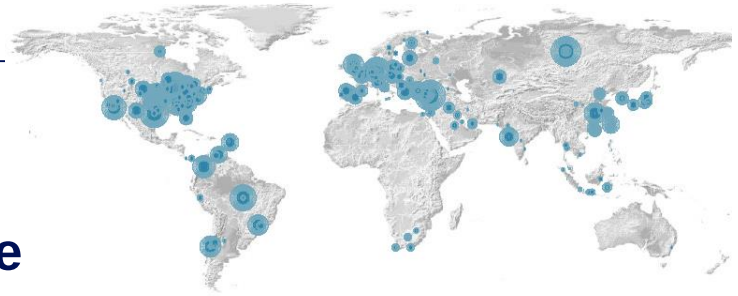
- **Was ist ein DDoS Angriff?**
- **Verschiedene Angriffsmethoden**
- **Mögliche Angriffs-Strategien**
- **Abwehrmassnahmen**
- **Historische DDoS-Attacken**
- **Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken**
- **Rechtliche Situation**

Quelle Titelblatt: http://www.blacklotus.net/ (Stand: 13.12.2012)

Was ist ein DDoS Angriff?

- **Denial of Service (DoS)**
  - Nichtverfügbarkeit eines Dienstes durch Überlastung
  - mutwilligen Angriff auf PC, Server, Netzwerk (Systeme)
- **Distributed Denial of Service (DDoS)**
  - Verteilter Angriff von einer grösseren Anzahl Systeme
- **Motivation**
  - Ansehen in der Gruppe, Wirtschaftliche / Politische Zwecke

Funktionsweise von DDoS-Attacken



- Überlastung der **Bandbreite**
- Überlastung der **Server / Systeme**
- Ausnutzung von **Sicherheitslücken** und dadurch das System zum **Absturz** bringen

Attack Subclass	Number of Attacks	Percentage
Total Traffic	577	31.0%
Bandwidth	355	19.1%
TCP SYN	306	16.5%
Protocol	240	12.9%
udp	100	5.4%
TCP NULL	99	5.3%
TCP RST	55	3.0%
ICMP	51	2.7%
Private Address Space	46	2.5%
IP Fragment	29	1.6%
other	2	0.1%

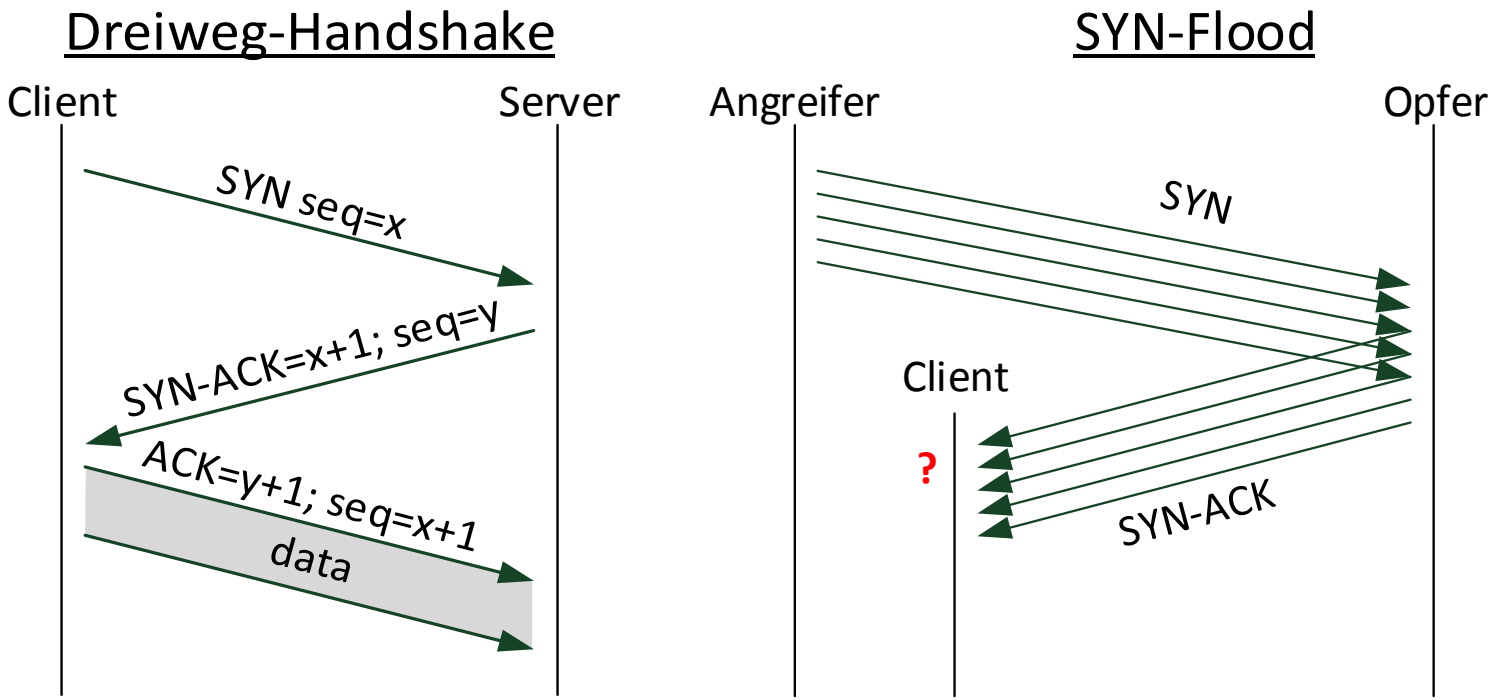
Quelle: http://atlas.arbor.net/ (Stand: 07.12.2012)

Verschiedene Angriffsmethoden 1/4

- **UDP Flood**
  - Verbindungsloses Protokoll
  - «Angreifer» sendet UDP Packet an zufällig gewählten Port
  - «Opfer» antwortet mit ICMP Destination Unreachable

- **TCP Flood**
  - Dreiweg-Handschake (SYN, SYN-ACK, ACK)
  - «Angreifer» sendet SYN-Request inkl. IP Spoofing
  - «Opfer» antwortet mit SYN-ACK an falsche IP und wartet auf ACK

Verschiedene Angriffsmethoden 2/4
TCP Flood

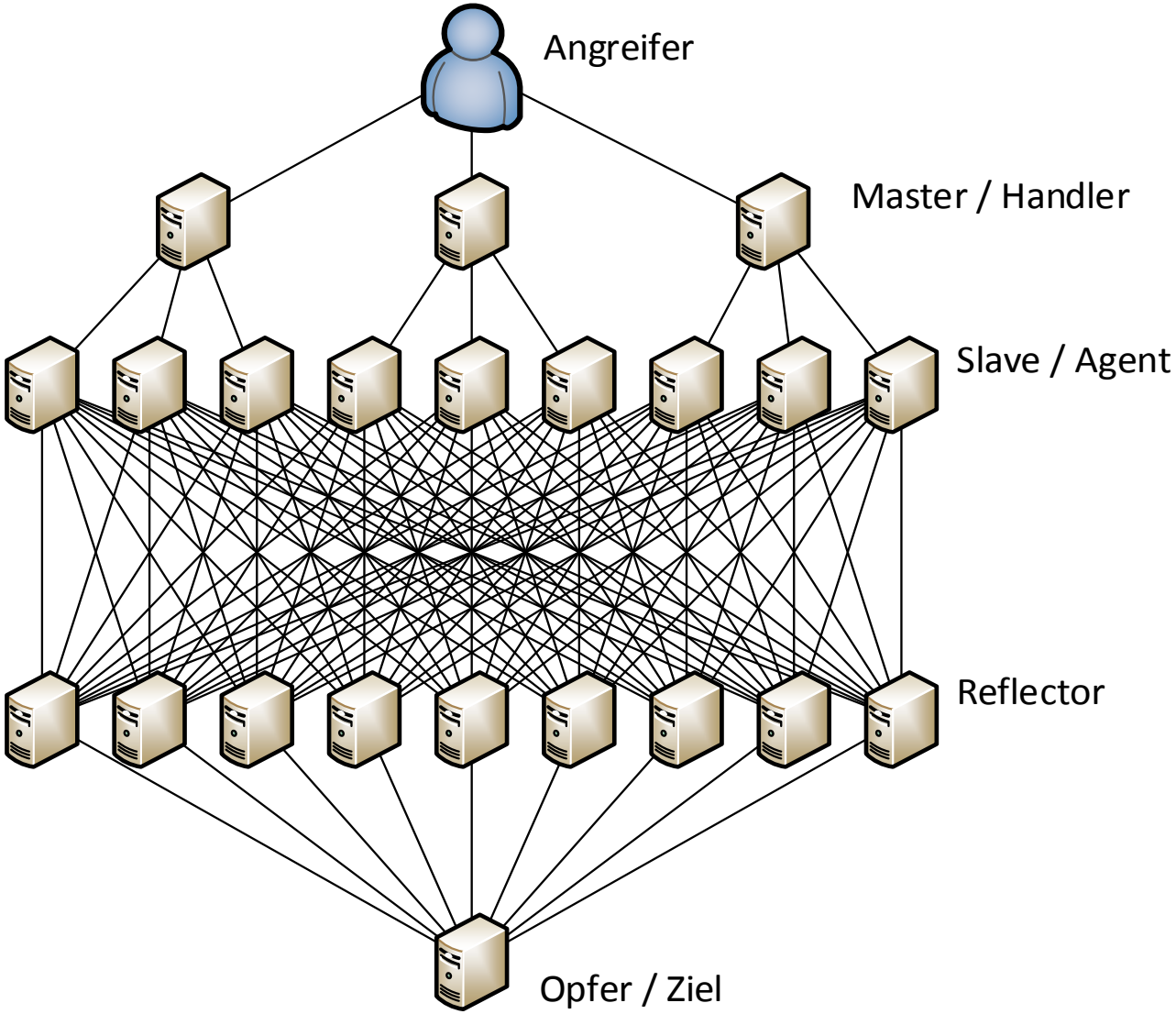


Verschiedene Angriffsmethoden 3/4

- **ICMP Flood**
  - «Angreifer» sendet ICMP Echo Request (inkl. IP Spoofing) an eine Broadcast-Adresse im Ziel-Netzwerk. Router vom Ziel-Netzwerk leitet die Anfrage an alle Clients weiter, diese Antworten auf die gefälschte Adresse des Opfers.
  - «Opfer» wird durch die vielen ICMP Echo Replay überlastet

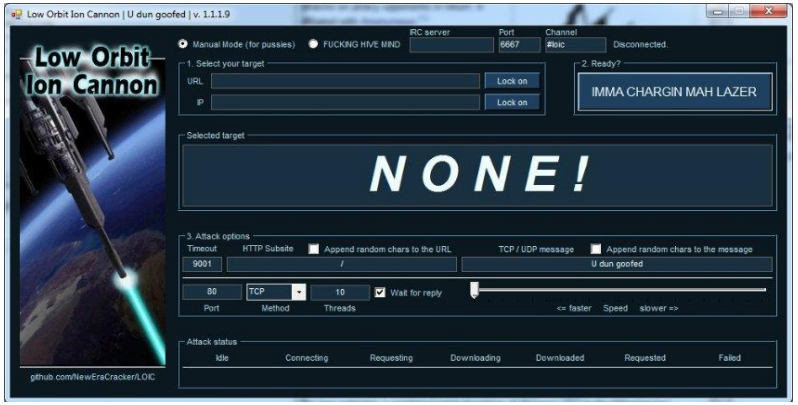
- **Reflected DDoS-Attacke / DRDoS**
  - «Angreifer» sendet eine Anfrage (inkl. IP Spoofing) an einen regulären Internet-Dienst, dieser antwortet und schickt die Antwort zum Opfer.
  - «Opfer» wird durch die vielen Datenpakete überlastet

Verschiedene Angriffsmethoden 4/4
Reflected DDoS-Attacke / DRDoS



Mögliche Angriffs-Strategien 1/2

- **Software**
  - Trinoo, Tribe Flood Network
  - Stacheldraht
  - LOIC – Low Orbit Ion Cannon
  - etc.

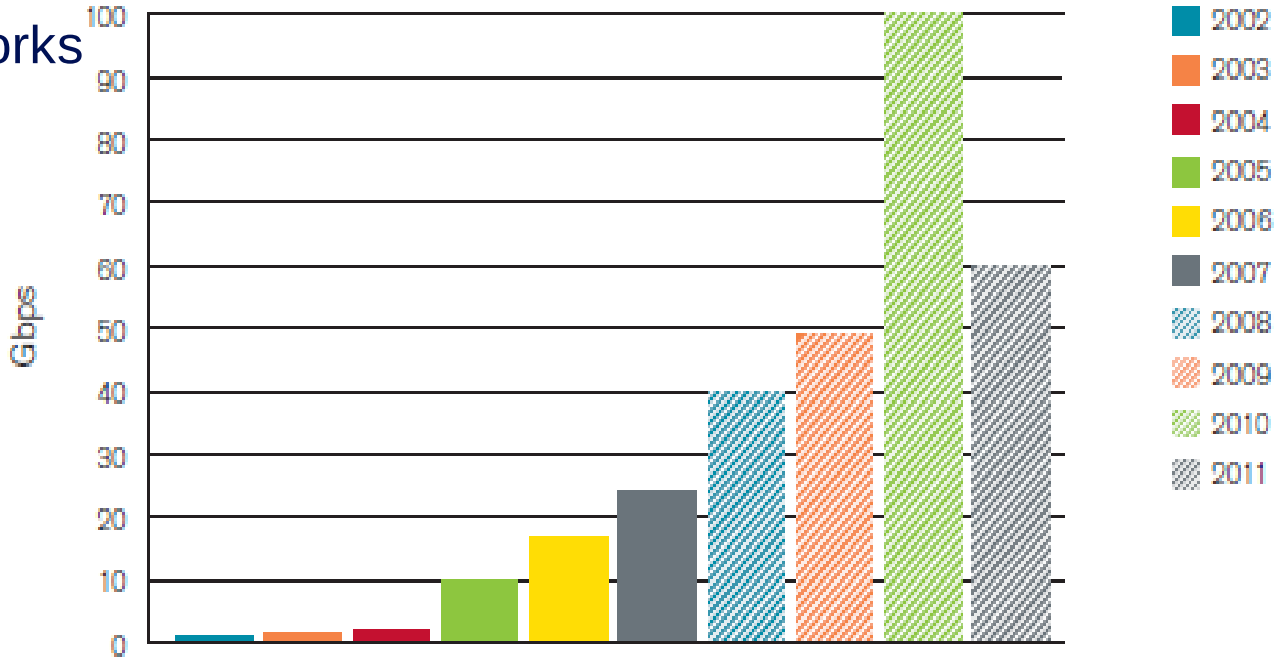


- **Bot-Netzwerk**
  - Command & Control Server (Master / Slave Architektur)
  - P2P-Netzwerk: Victim kann Master und Slave sein
  - 50$ für 1’000 Bots/24h

Mögliche Angriffs-Strategien 2/2

- **Benötigte Bandbreite** (Kaspersky Lab)
  - Durchschnittliche Bandbreite (2011): 110 Mbit/sec
  - Maximale Bandbreite (2011): 600 Mbit/sec
    - 1’100’000 packets/sec, UDP-Flood, Packet: 64bytes

- Arbor Networks



Quelle: Arbor SERT

Abwehrmassnahmen
Präventive Massnahmen

- Datensammlung zentralisieren und Trends verstehen
- Klare Abwehrstrategie definieren
- Mehrschichtige Filter nutzen
- Flexibilität und Skalierbarkeit einplanen
- Anwendungs- und Konfigurationsprobleme ansprechen

Abwehrmassnahmen
Netzwerktechnische Möglichkeiten

- Serversoftware
- Softwarefirewall
- Hardwarefirewall
- Spezialhardware (IDS Intrusion Detection System, IPS Intrusion Prevention System)

Abwehrmassnahmen
Netzwerktechnische Möglichkeiten

- QoS (Quality of Service) einsetzen
- SYN Proxy
- Anzahl neuer Verbindungen beschränken
- Dark Address Prevention
- Mehrere Rechenzentren mittels Anycast verwenden

Abwehrmassnahmen
Allgemeine Punkte

- Genügend Systemressourcen einplanen
- Firewallregeln mit Sperrlisten abgleichen
- Dynamische Filterung aktivieren
- DDoS-Mitigation
- IP-Adressen(n) der Angreifer sperren
- Server vom Netz nehmen

Abwehrmassnahmen
DDoS Attack Mitigation Appliance

Historische Angriffe

- **Oktober 2002:** Root DNS Server
- **Dezember 2010:** postfinance.ch
- Genauere Angaben im Term Paper

Nationale Strategie in der Schweiz

- **Die Ziele des Bundesrates:**
  - die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich,
  - die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen,
  - die wirksame Reduktion von Cyber-Risiken, insbesondere Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage.

- **Integration von Cyber-Risiken in bestehende Risikomanagementprozesse**

Rechtliche Situation

- **StGB Art. 143** Unbefugte Datenbeschaffung
- **StGB Art. 143bis** Unbefugtes Eindringen in ein Datenverarbeitungssystem (Hacker-Paragraph)
- **StGB Art. 144bis** Datenbeschädigung
- **StGB Art. 147** Betrügerischer Missbrauch einer Datenverarbeitungsanlage

- **StGB Art. 150** Erschleichen einer Leistung
- **StGB Art. 148** Check- und Kreditkartenmissbrauch

StGB Art. 143bis
«Hacker-Paragraph»

- **StGB Art. 143bis** Unbefugtes Eindringen in ein Datenverarbeitungssystem (Auszug)
- [1] Wer auf dem Wege von Datenübertragungseinrichtungen unbefugter weise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
- [2] Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz 1 verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

(Distributed) Denial-of-Service Attack

Fragen?