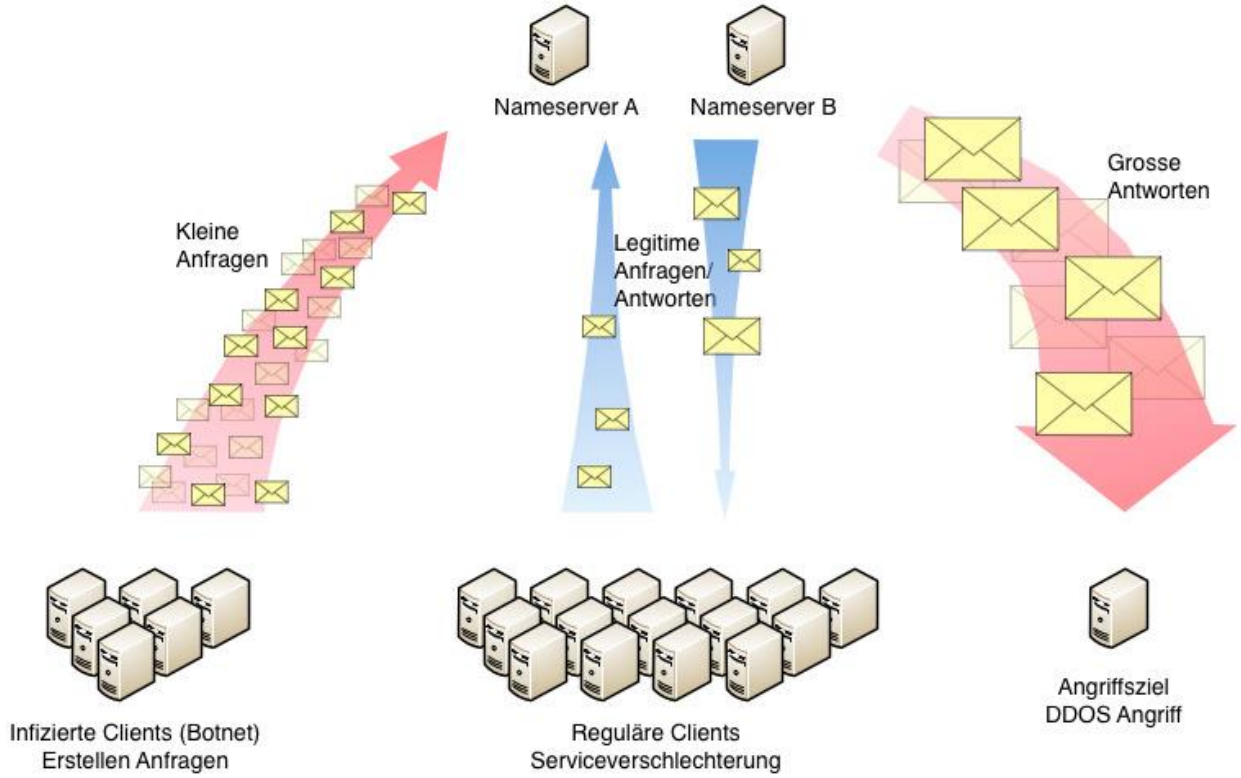
(Distributed) Denial-of-Service Attack



Inhalt

- **Was ist ein DDoS Angriff?**
- **Verschiedene Angriffsmethoden**
- **CH-Zone Opfer eines DNS-Amplifikations-Angriffes**

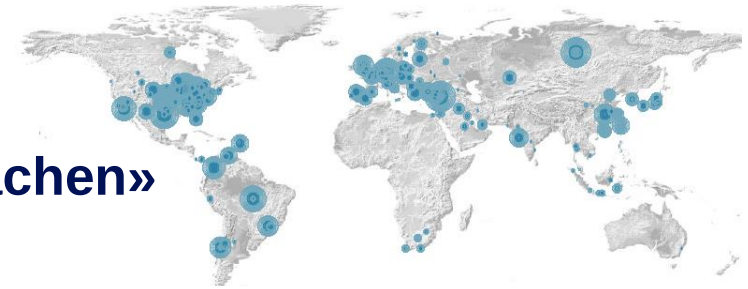
Quelle Titelblatt: http://www.switch.ch/de/about/news/2013/ddos.html/ (Stand: 13.01.2013)

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**
- Ausnützen von «**Protokollschwächen**»



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 1/2

- **UDP Flood**
  - UDP: verbindungsloses Protokoll
  - «Angreifer» sendet UDP Packet (inkl. IP Spoofing) an zufällig gewählten Port
  - «Opfer» antwortet mit ICMP Destination Unreachable

- **TCP Flood**
  - TCP: 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 2/2

- **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

CH-Zone Opfer eines Reflected-DDoS

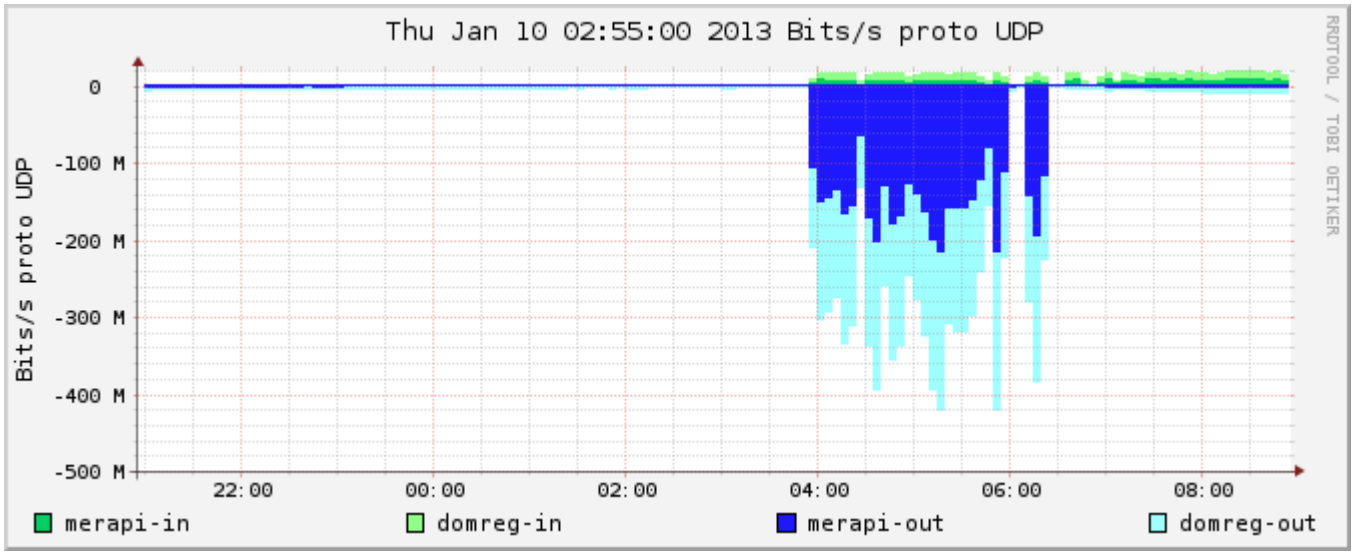
- **DNS-Anfrage:**
  - Domain: «ch»
  - Query-Typ: «any»
  - EDNS-Erweiterung aktiviert (UDP Antwort >512Bytes)
  - IP-Spoofing

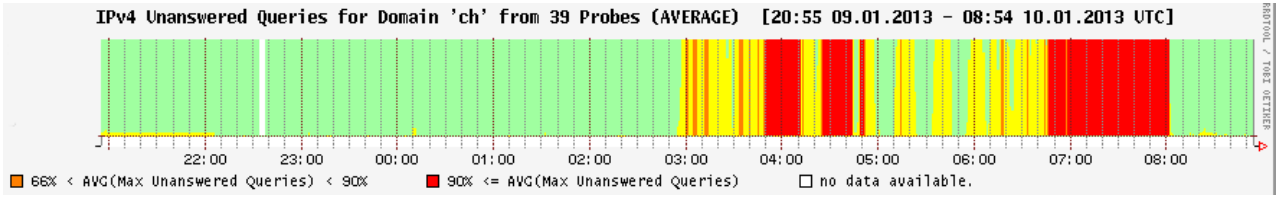
- **Situation / DNS-Server Antwort:**
  - Angriff am 13.01.2013
  - DNSSEC Signierungs-Algorithmus-Rollover: doppelt signiert
  - ➔Amplifikation: 75 !
  - ➔4MBit/s Anfragen➔ 300MBit/s Antworten

Quelle: http://securityblog.switch.ch/2013/01/10/ch-zone-dns-angriff// (Stand: 13.01.2013)

Switch CH-Zone DNS-Server 10.01.2013

Ein- und Ausgehender Datenverkehr der SWITCH CH-Nameserver



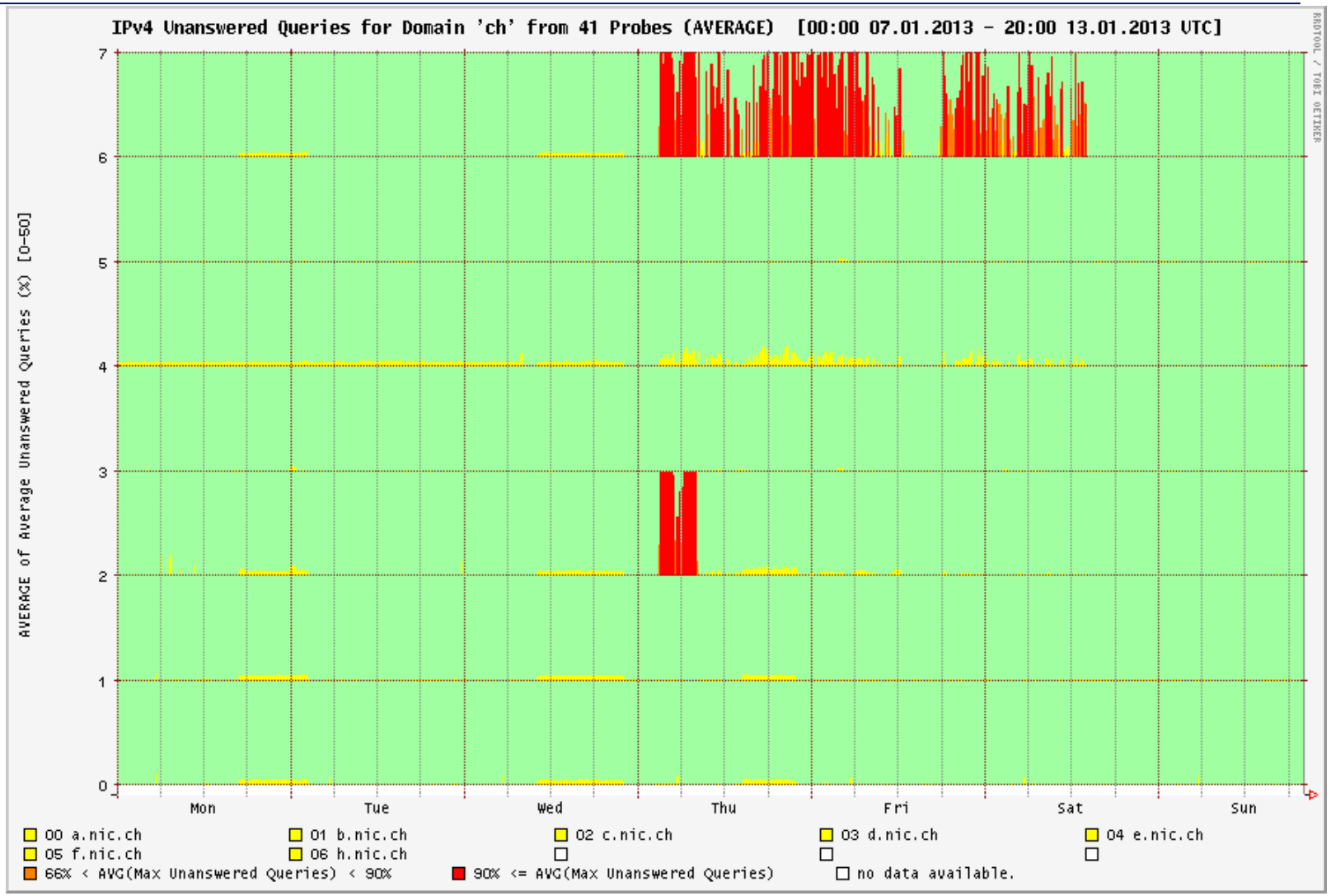


IPv4 Unanswered Queries for Domain ‘ch’ by c.nic.ch

Quelle: http://securityblog.switch.ch/2013/01/10/ch-zone-dns-angriff// (Stand: 13.01.2013)

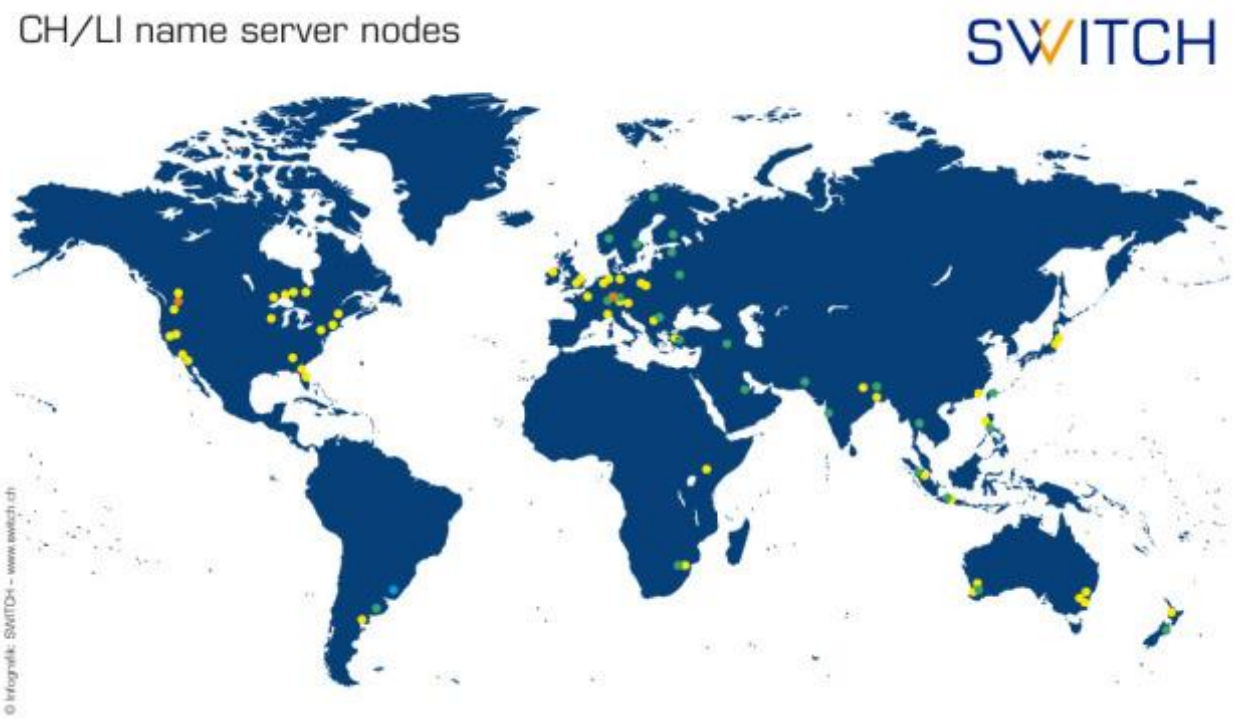
Quelle: http://dnsmon.ripe.net/dns-servmon/domain/ (Stand: 13.01.2013)

CH-Zone DNS Server Verfügbarkeit



Quelle: http://dnsmon.ripe.net/dns-servmon/ (Stand: 13.01.2013)

(Distributed) Denial-of-Service Attack



Vielen Dank für die Aufmerksamkeit!

Quelle: http://securityblog.switch.ch/2013/01/10/ch-zone-dns-angriff// (Stand: 13.01.2013)