Threat Update: DDoS durch DNS Amplification Attacks

Lukas Feiler, Achim Brock

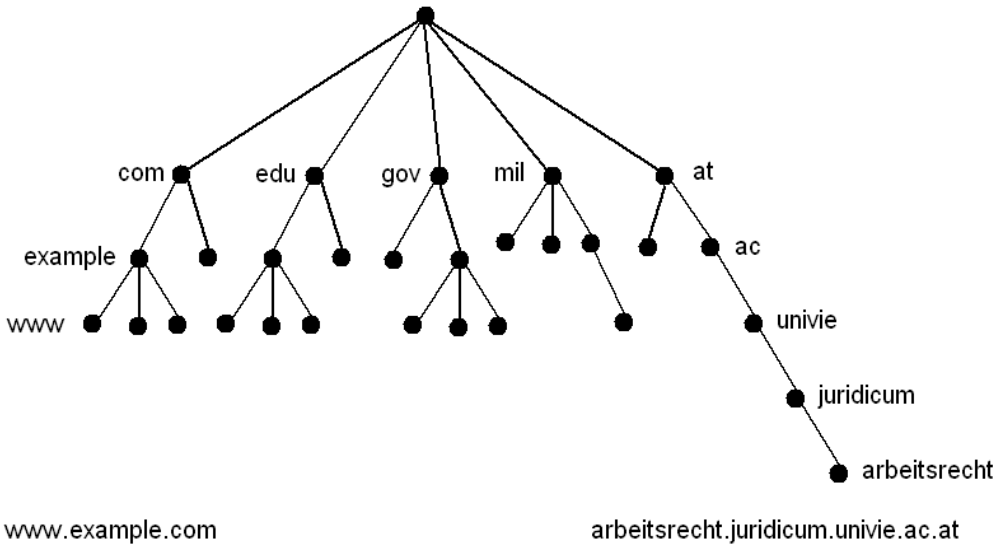
23. März 2006

Inhalt

1. Einleitung: DNS – das Domain Name System
2. Technische Beschaffenheit des Angriffs
3. Auswirkungen von DNS Amplification Attacks
4. Strafrechtliche Beurteilung
5. Gegenmaßnahmen
6. Quellen

1. Einleitung: DNS – das Domain Name System

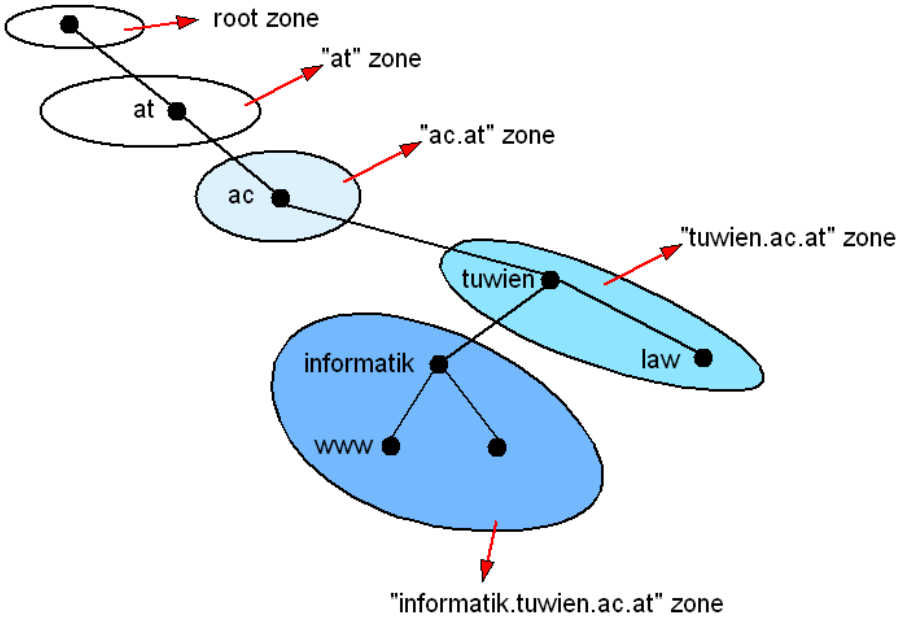
Das Domain Name System (DNS) ist eine weltweite, dezentrale Datenbank in der Informationen über IP-Adressen und Domainnamen gespeichert werden. Es dient vor allem dazu Domainnamen in IP-Adressen aufzulösen. Das Domain Name System kann zutreffend als „verkehrter Baum“ dargestellt werden:



Die in der ersten Ebene des Baumes enthaltene Elemente (hier exemplarisch: com, edu, gov, mil, at) bezeichnet man als Top Level Domains (TLDs) oder First Level Domains. Elemente der zweiten Ebene (z.B. example.com od. ac.at) werden als Second Level Domain bezeichnet.

Der dezentrale Aspekt von DNS manifestiert sich in der Möglichkeit die Autorität für sog. Zones delegieren zu können. Die Zone höchster ebene ist die sog. Root-Zone. In dieser ist die Information gespeichert welche DNS-Server die Autorität für die „Top-Level-Zones“ besitzen (z.B. welche DNS-Server die Autorität für die Zone „at“ besitzt). Jeder DNS-Server, der die Autorität für eine Zone hat ist in der Lage – ähnlich einem guten Manager – bestimmte Teile zu delegieren für andere jedoch selbst die Autorität zu behalten. In folgendem (fiktiven) Beispiel wurde einem bestimmten DNS-Server die Autorität für die Zone tuwien.ac.at zugewiesen. Dieser delegiert nur die Autorität für informatik.tuwien.ac.at an einen anderen DNS-Server. law.tuwien.ac.at bleibt demgegenüber jedoch in der Zone tuwien.ac.at. Wollen

die Informatiker der TU nun einen neuen Domainnamen – z.B. ftp.informatik.tuwien.ac.at anlegen, so können sie dies autonom tun, da sie die Autorität für ihre Zone besitzen. Die Juristen der TU können ohne Zustimmung von zentraler Stelle jedoch keine neue Sub-Domain anlegen, da sich nicht die Autorität für ihre Zone besitzen:

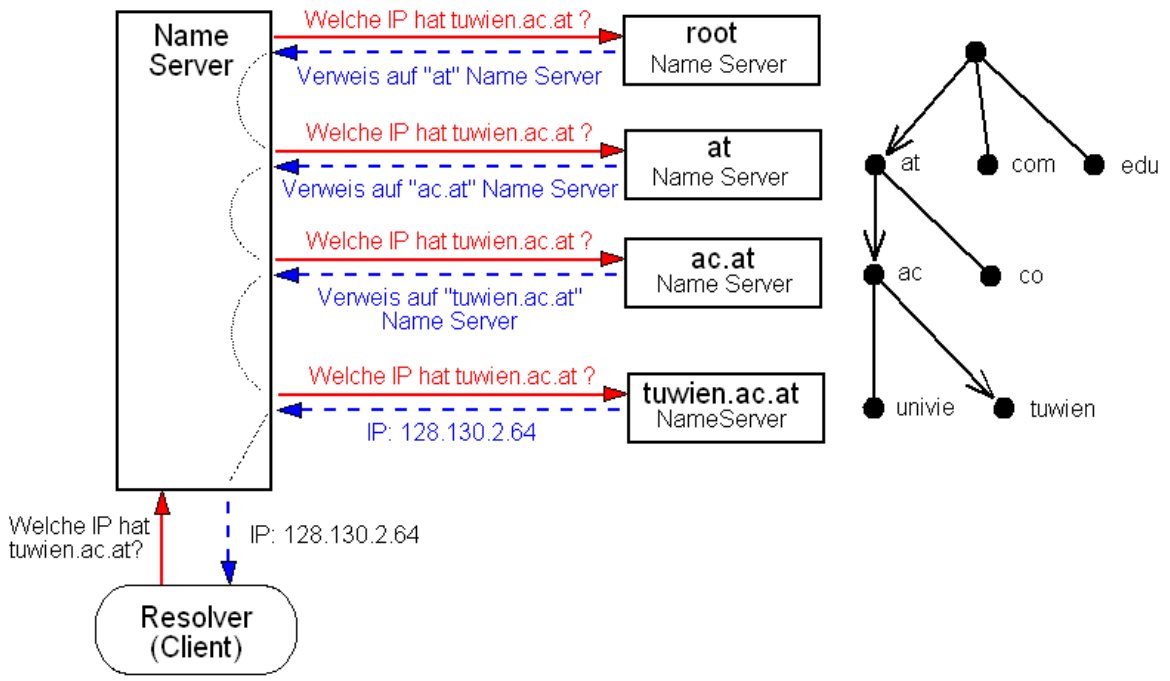


Praktischer Hinweis: Die manuelle Auflösung eines Domainnamens in eine IP-Adresse ist mit dem Command-Line-Tool nslookup möglich. Es ist sowohl unter Windows als auch unter Unix/Linux verfügbar. So gibt folgender Befehl die IP-Adresse von www.example.com aus:

```
nslookup www.example.com
```

Der Prozess der Auflösung eines Domainnamens in eine IP-Adresse wird als Name Resolution bezeichnet. Hat ein DNS-Server die Autorität für die Zone aus der der aufzulösende Domainname stammt, so kann er selbst unmittelbar eine Antwort liefern. Wird bei einem DNS-Server jedoch von einem Client (genannt Resolver) um die Auflösung eines Domainnamens angefragt, für den er nicht die Autorität besitzt so bieten sich für ihn zwei Möglichkeiten:

1) Da der befragte DNS-Server die Antwort selbst nicht unmittelbar geben kann, verweist er auf andere DNS-Server.
2) Er führt eine sog. rekursive Anfrage („recursive query“) aus. Hierbei versucht der DNS-Server selbst die richtige Antwort dadurch zu ermitteln, dass er andere DNS-Server befragt. Den benötigten Einstiegspunkt in das Domain Name System liefern jedenfalls die Root-Name Server. Diese besitzen die Autorität für die Root-Zone und sind daher jedenfalls in der Lage nähere Informationen zu geben. Soll beispielsweise der Domainname tuwien.ac.at aufgelöst werden, so ist es den Root-Name Server jedenfalls möglich auf den bzw. die DNS-Server zu verweisen, die die Autorität für die Zone „at“ besitzen. Diese sind wiederum in der Lage auf die DNS-Server der Zone „ac.at“ zu verweisen, die dann den, für die Zone „tuwien.ac.at“ zuständigen DNS-Server benennen können. Dieser autoritative DNS-Server kann dann befragt werden. Dieser Ablauf ist in der folgenden Abbildung dargestellt:



Ein DNS-Server, der jedermann die Durchführung von rekursiven DNS-Anfragen ermöglicht wird als „Open Resolver“ bezeichnet.

Ein weiterer wichtiger Aspekt von DNS ist die Tatsache, dass Anfragen grundsätzlich unter Verwendung des Protokolls UDP erfolgen. Im Unterschied zu TCP ist UDP kein verbindungsorientiertes sondern ein paketorientiertes Protokoll. Dies hat den Vorteil, dass zum Austausch kleiner Datenmengen, wie sie bei DNS-Anfragen typischer Weise gegeben sind kein expliziter Verbindungsaufbau[1] erfolgen muss.

2. Technische Beschaffenheit des Angriffs

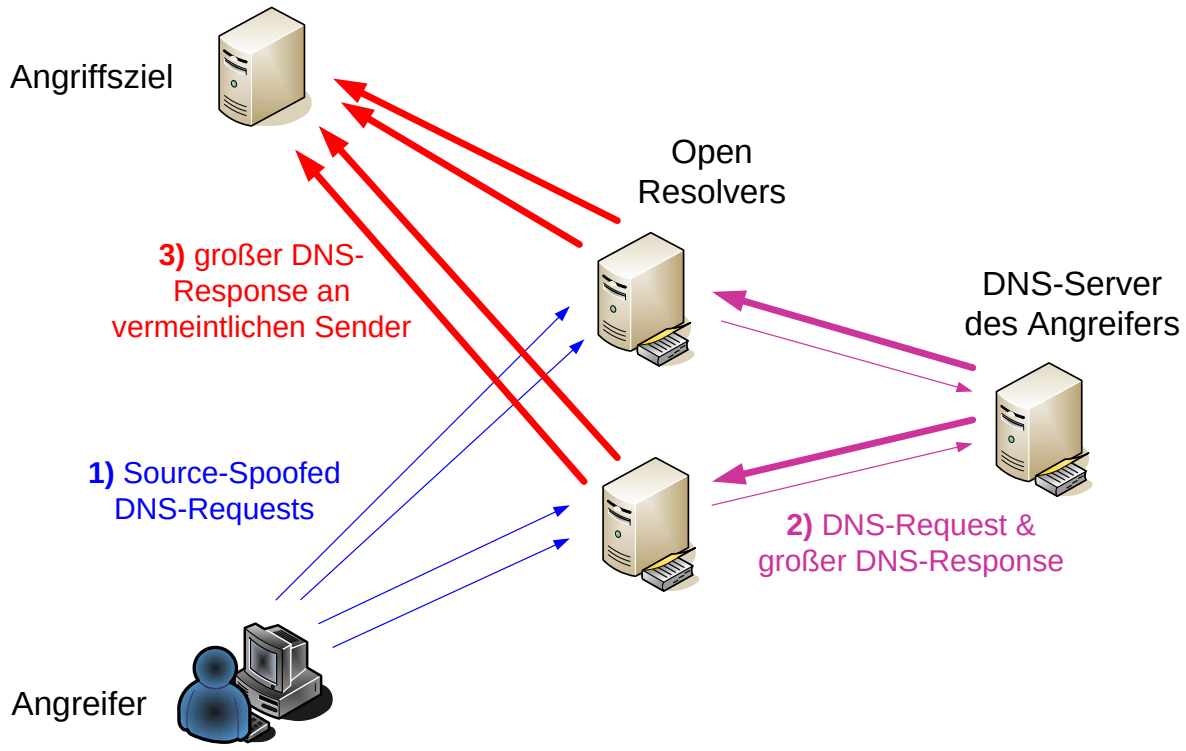
Wie andere DDoS (Distributed Denial of Service)-Angriffe bedient sich ein DNS Amplification Attack zweier Maßnahmen:
a) der Vergrößerung („amplification“) der ursprünglich gesendeten Datenmenge
b) der Fälschung von Absender-IP-Adressen (IP-Spoofing)

Ziel eines DDoS-Angriffes ist es, ein System derart mit Anfragen zu überladen, dass es nicht mehr in der Lage ist auf legitime Anfrage zu antworten. Ein DDoS-Angriff unterscheidet sich von einem gewöhnlichen DoS-Angriff dadurch, dass er verteilt, von mehreren Systemen aus erfolgt. Da die Bandbreite des angegriffenen Systems die, dem Angreifer unmittelbar zur Verfügung stehende Bandbreite idR bei weitem übersteigt, benötigt der Angreifer ein Mittel zur Verstärkung seines Angriffs.
Bei klassischen Smurf[2]-Angriffen erfolgte die Verstärkung durch das Senden von ICMP-Paketen vom Typ „echo request“ an eine Broadcast-Adresse, woraufhin jedes der, in dem so bezeichneten Netzwerk befindliche System antwortete. Im Unterschied zu Smurf besteht bei DNS Amplification Attacks die Verstärkung darin, dass DNS-Server auf kleine Request-Pakete mit ausgesprochen großen Response-Paketen antworten können. Lag die maximale Größe eine UDP Response-Pakets nach der ursprünglichen Spezifikation von DNS noch bei

[1] Bei TCP durch einen sog. Three-Way-Handshake.
[2] vgl. CERT Advisory CA-1998-01, http://www.cert.org/advisories/CA-1998-01.html

512 Bytes, so wurde sie durch Erweiterungen des Protokolls für IPv6, DNSSEC[3] oder NAPTR[4] auf über 4000 Bytes erhöht.[5] Aus dem Verhältnis eines DNS-Request-Pakets minimaler Größe (60 Byte) und der Größe des Response-Pakets (4000 Bytes) ergibt sich ein theoretischer Verstärkungsfaktor von ca. 70.

Die zweite Maßnahme für eine erfolgreichen DNS Amplification Attack besteht darin, die Absender-IP-Adresse der Request-Pakaete zu fälschen. Da DNS auf dem verbindungslosen Protokoll UDP aufbaut, ist dies protokolltechnisch leicht möglich. Die um den Faktor 70 größeren Response-Pakete werden vom DNS-Server dann an die gefälschte Absenderadresse übermittelt. Diese bezeichnet das eigentliche Angriffsziel:



Wie hier dargestellt, handelt es sich deshalb um einen DDoS-Angriff und nicht um einen gewöhnlichen DoS-Angriff, da mehrere Open Resolver[6] für den Angriff verwendet werden. Jüngst vorgenommenen Untersuchungen[7] zufolge war es möglich 580.000 DNS-Server auszumachen, die als Open Resolvers konfiguriert sind und daher für derartige Angriffe verwendet werden können.
Open Resolvers sind erforderlich, um eine Befragung des DNS-Servers des Angreifers zu ermögliche. Auf diesem sind außergewöhnlich große DNS-Records gespeichert, die zu entsprechend großen Response-Pakete führen. Da die Open Resolvers nur bei dem aller ersten Request des Angreifers den DNS-Server des Angreifers kontaktieren, entsteht für diesen nur eine sehr geringe Last.

---

[3] *Erdmann/Wegener*, Dienstschutz, DNS-Sicherheit: Der Stand der Dinge, iX 12/2005, S. 142; bezügl. einer Liste der einschlägigen RFCs vgl. http://www.dnssec.net/rfc
[4] vgl. RFC 2915
[5] DNS Amplification Attacks machen sich tatsächlich RFC 2671 zu Nutze um größere Antwortpakete zu erzwingen.
[6] Zum Begriff vgl. bereits oben.
[7] Dan Kaminsky und Mike Schiffman auf der ShmooCon (2006) Konferenz; http://www.shmoocon.org/speakers.html#kaminsky

3. Auswirkungen von DNS Amplification Attacks

Mit DNS Amplification Attacks ist es möglich sehr effektive DoS-Angriffe durchzuführen. Die, dem Angriffsziel zur Verfügung stehende Bandbreite kann idR weitgehend konsumiert werden. Berichten zufolge[8] wurde in manchen Fällen durch DNS Amplification Attacks bereits ein Datenvolumen von ca. 2,8 Gbps[9] erzeugt.
Durch derartige Angriffe ist es daher möglich gezielt einzelne Server bzw. ganze Netze effektiv offline zu bringen.

4. Strafrechtliche Beurteilung

Da ein DoS eine schwere Störung der Funktionsfähigkeit eines Computersystems darstellt, ist – Eventualvorsatz vorausgesetzt – eine Strafbarkeit gem. § 126b StGB zweifellos zu bejahen. Auf Grund des IP-Spoofings und der großen Verfügbarkeit von Open Resolvers stehen der Strafverfolgung jedoch erhebliche faktische Hindernisse entgegen.

5. Gegenmaßnahmen

Sich als Unternehmen vor DNS Amplification Attacks zu schützen gestaltet sich deshalb äußerst schwierig, da alle konventionelle Anti-(D)DoS-Maßnahmen grundsätzlich nicht vor einer gänzlichen Konsumption der Bandbreite schützen.[10]

Um DNS Amplification Attacks grundsätzlich zu verhindern, gilt es die Anzahl der Open Resolvers zu reduzieren. Dies ist jedoch angesichts ihrer Anzahl ein äußerst langwieriger Prozess.

Eine weitere Maßnahme, die nicht nur gegen DNS Amplification Attacks, sondern auch andere DDoS-Attacks wie Smurf wirksam wäre und schon lange von Experten gefordert wird, besteht darin IP-Spoofing durch entsprechendes Engress-Filtering[11] seitens der Access Provider gänzlich zu unterbinden. Denn übermittelt ein Access Provider nur Datenpakete ins Internet, die Absenderadressen des eigenen Netzwerkes tragen, ist IP-Spoofing für Kunden dieses Access Providers effektiv nicht mehr möglich. Eine solche Maßnahme würde einen erheblichen Beitrag zur allgemeinen Sicherheit des Internets leisten.

6. Quellen

US-CERT, The Continuing Denial of Service Threat Posed by DNS Recursion, http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf

Erdmann/Wegener, Dienstschutz, DNS-Sicherheit: Der Stand der Dinge, iX 12/2005, S. 142

Vaughn/Evron, DNS Amplification Attacks, March 17, 2006, http://isotf.org/news/DNS-Amplification-Attacks.pdf

CERT statistic mentioned in US-CERT document:
http://cyber.law.harvard.edu/icann/mdr2001/archive/pres/Cert.pdf

Northcutt/Zeltser/Winters/Fredrick/Ritchey, Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems, Sams, Indiana 2002

---

[8] *Vaughn/Evron*, DNS Amplification Attacks, 2
[9] 2,8 Giga-Bits pro Sekunde, d.h. 2.800.000.000 Bits, dies entspricht ca. 333 MB (Mega Byte) pro Sekunde
[10] *Puppe/Maier*, Von allen Seiten, Maßnahmen gegen Distributed-Denial-of-Service-Angriffe, iX 4/2005, S. 107
[11] *Northcutt/Zeltser/Winters/Fredrick/Ritchey*, 36 f

University of Oregon, Computing Center,
http://cc.uoregon.edu/cnews/winter2006/recursive.htm

(CIAC 1999) J-063: Domain Name System (DNS) Denial of Service (DoS) Attacks,
http://www.ciac.org/ciac/bulletins/j-063.shtml

SANS NewsBites, Volume 8, Issue 23, 21. März 2006,
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=23#202

RFCs

Vixie, Extension Mechanisms for DNS (EDNS0), RFC 2671, 1999, ftp://ftp.rfc-editor.org/in-notes/rfc2671.txt

Mealling/Daniel, The Naming Authority Pointer (NAPTR) DNS Resource Record, RFC 2915, 2000, ftp://ftp.rfc-editor.org/in-notes/rfc2915.txt

Mailing Lists:

dns-operations
http://lists.oarci.net/pipermail/dns-operations/2006-March/000338.html

bugtraq
http://marc.theaimsgroup.com/?l=bugtraq&m=114123795230123&w=2

Mediale Berichterstattung:

Große Welle von mysteriösen DoS-Attacken im Netz, 18. März 2006, Der Standard,
http://derstandard.at/?url=/?id=2382759

Kawamoto, New denial-of-service threat emerges, 17. März 2006, CNET News.com,
http://www.zdnetasia.com/news/security/printfriendly.htm?AT=39344151-39000005c

Vijayan, VeriSign reveals details of DDoS assaults, 17. März 2006, Computerworld (US online), http://www.techworld.com/security/news/index.cfm?NewsID=5586

Attacks target Internet traffic cops, 16. März 2006, CNN,
http://www.cnn.com/2006/TECH/internet/03/16/internet.attack.ap/index.html