DoS-Attacken

Patrick Ober

6. Juni 2013

1 Einleitung

Denial-Of-Service (DoS) attacken gibt es seit den frühen Anfängen der Netzwerktechnologie und stellt auch heute noch eine immense Bedrohung für jeden Teilnehmer, vorallem für Unternehmen, im World Wide Web dar. Die Einfachheit der Durchführung und die komplexität dies zu verhindert stellt Organisationen, die auf Sicherheit im Netz spezialisiert sind, vor eine große Herausforderung. Sie müssen sich neben den Bedrohungen durch DoS attacken auch mit denen der DDoS (Distributed Denial of Service), sowie DRDoS (Distributed Reflector Denial of Service) auseinandersetzen.
DoS-Angriffe zielen darauf ab, öffentlich angebotene Dienste in einem hohen Grad zu überlasten, indem vertrauenswürdige Anfragen gesendet werden, welche gezielt die zur Verfügung stehenden Resourcen aufbrauchen und somit anderen Nutzern den Service unterbinden. Bei DDoS attacken erfolgt der eingriff über viele verteilte Rechner, die durch ihre Vielzahl an anfragen die Verfügbarkeit des Opfers lahmlegen. Bei diesem verteilten System, bestehend aus der großen Anzahl von angreifenden Quellen, spricht man von einem Botnet.
Die vorliegende Arbeit beschreibt die Entwicklung der Angriffe und geht auf die Begriffe DoS, DDoS und auf ihre Methoden des Angriffes näher ein.

2 Evolution

Obwohl sich die Methoden und Motive hinter den DoS-Attacken geändert haben, so bleibt das Ziel der Angriffe, das Aufbrauchen verfügbarer Resourcen und folgliche Lahmlegung der Verfügbarkeit für legitime Nutzer, das selbe.

Die Entwicklung und Abwandlungen von DoS-Attacken basieren auf dem selben Prinzip: stelle einen Zustand her bei dem ein öffentlicher Service ausgenutzt wird ohne dabei geschnappt zu werden. Die Täter Entdecken dabei immer neue Möglichkeiten um neue Technologien auszuhebeln um ihr Ziel zu erreichen. Sie entwickeln neue Techniken um die Effizienz der Angriffe zu erhöhen und sich gleichzeit weiter vom Opfer zu distanzieren. Die Entwicklung der Attacken bezieht sich immer mehr auf die Verwendung von Botnetzen. Sie stellen ein perfektes Hilfswerkzeug, zur Verstärkung des Angriffs und distanzierung, dar.

2.1 Botnetze

Botnetze spielen vorallem bei DDoS attacken eine große Rolle. Hierbei besteht die Quelle des Angriffs aus mehreren Rechnern. Der Täter kann dabei nicht nur die Anzahl an Attacken erhöhen, sondern somit auch seine IP Adresse verschleiern. Je mehr Schichten zwischen Täter und Opfer liegen, desto geringer ist die möglichkeit geschnappt zu werden. Moderne DoS Angriffe beziehen sich ausnahmslos auf solch verteilte Systeme bei denen fremde Rechner für böse Absichten missbraucht werden. Aber wie passiert das? Der Täter erlangt kontrolle über ein fremdes Gerät, indem er schwachstellen im Betriebssystem oder in anderer Software ausnutzt. Um dies zu erreichen, müssen fremde Rechner infiziert werden. Dies geschieht, indem der Benutzer unseriöse Seiten im Internet besucht, die gerne von Angreifern genutzt werden um Schadsoftware, sowie auch Bots, zu verteilen. Aufgrund der rapiden Ausbreitung des Internets und dem Mangel zureichender Sicherheitsmaßnahmen ist die Anzahl der Bots im Millionenbereich. Eines der größten bekannten Botnetze, unter dem Namen Mariposa, umfasste 12,7 Millionen [1] Rechner.

[1] `http://defintel.com/docs/Mariposa_Analysis.pdf`

3 Die Arten von DoS Attacken

3.1 DoS - Denial of Service

> [2] *Dabei handelt es sich um einen Angriff, bei welchem Internet-Hosts (z.B. Web-Server) durch eine Flut von Anfragen (z.B. HTTP-Requests) so stark beschäftigt werden, dass sie anderen Benutzern nicht mehr zur Verfügung stehen oder gar vollständig abstürzen.*

Eine Denial of Service Attacke ist ein Hackangriff, der versucht, legitimen Traffic zwischen einem Client und Server zu verhindern. Sprich, ein Webserver, Fileserver oder jegliche andere Art von Server auf die sich ein Client verbinden kann, stellt Resourcen für diese Verbindung bereit. Die Idee hinter einem DoS Angriff ist, einen Server bis zu einem Punkt zu attackieren bis alle Resourcen des Servers für den Angriff aufgebraucht sind und somit den legitimen Datenaustausch mit anderen Nutzern unterbindet, da besagte Resourcen nicht mehr zur Verfügung stehen. Es gibt verschiedene Arten von DoS Attacken.

- Eine klassische Methode ist der "Ping Flood". Dabei geht der Angriff von mehreren Computern aus, die alle einen gewissen Server an Pingen. Startet man diesen Denial of Service mit genügend Rechnern, so kann man erreichen, dass die Resourcen des Servers damit verwendet werden um jeder Ping-Anfrage eine Antwort zu schicken und somit den Server nach außen hin für andere Benutzer lahm legen.

- Eine weitere Methode ist der SYN Flood. Dabei wird der 3 Way Handshake einer TCP Verbindung ausgenutzt. Bei einem Verbindungsaufbau von einem Client mit einem Server ist das erste Paket ein SYN Paket. Es dient zur Synchronisation. Daraufhin antwortet der Server mit einer Bestätigung. Im Normalfall schickt darauffolgend der Client wiederum eine Bestätigung und die Verbindung zum Datenaustausch ist gewährleistet. Während der Bestätigung des Servers, werden Session Resourcen geöffnet um mit dem Client zu kommunizieren. Was bei einem SYN Flood nun passiert, ist, dass der Client nun nicht mehr mit einer Bestätgung antwortet. Was folgt daraus? Der Server hat bereits Resourcen für eine Session mit dem Client geöffnet, doch sie wird

[2] Uwe Schneider und Dieter Werner, Taschenbuch der Informatik 6. Auflage, Hanser Verlag 2007

nicht bestätigt. Die anzahl an simultan geöffneten Sessions, die ein Server ausführen kann, ist jedoch begrenzt. Wird ein SYN Flood nun von mehreren Rechnern ausgeführt, und alle Session Resourcen des Servers wurden aufgebraucht, so ist es für einen unschuldigen Client nicht mehr möglich eine Verbindung mit dem Server aufzubauen.

3.2 DDoS - Distributed Denial of Service

Bei früheren DoS Attacken genügte oft bereits ein Host um Angriffe durchzuführen. Aufgrund der einfachen Rückverfolgung und geringen Auswirkung, entwickelte sich die Auslegung auf ein verteiltes System. Hier kommen Botnetze zum Einsatz. Sind erst mal genügend fremde Rechner infiziert, nehmen diese Kommunikation mit einem Controler auf. Über diesen Controler kann der Hacker die Befehle zum Angriff geben und schützt sich, durch diese weitere Schicht, einmal mehr ab. Der Täter kann nun alle Bots **gleichzeitig** auf einen Zielserver richten um anderen Teilnehmern wiederum dessen Service zu unterbinden.

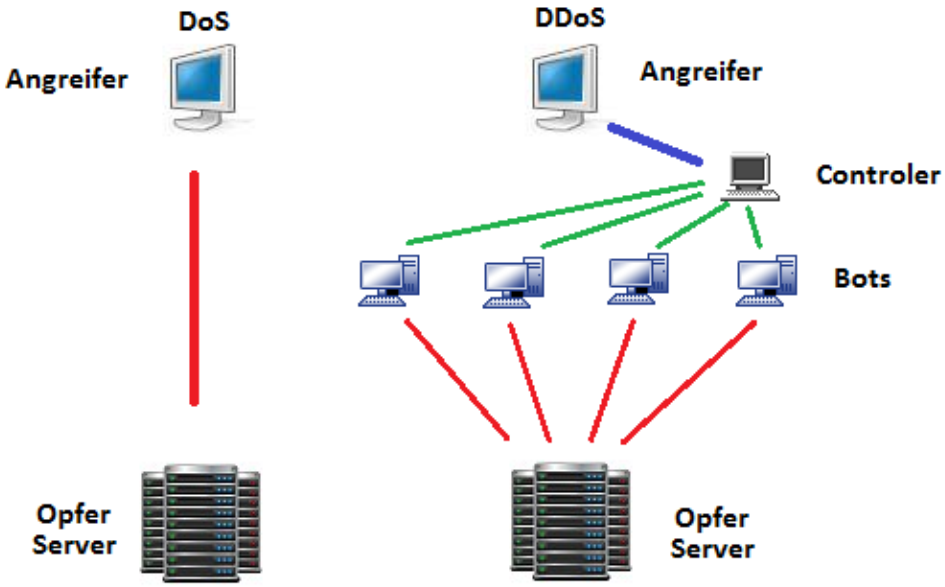

Abbildung 1: DoS and DDoS

4 Schlusswort

Mit DDoS Attacken werden weder Daten geklaut, noch langhaltiger Schaden verursacht, es ist ein temporärer Angriff der für eine Bestimmte Zeit anhält. Also warum finden diese Angriffe statt? Größtenteils ist das Motiv aggressiver Protest. Vorallem "Hacktivisten"Bewegungen wie z.B. Anonymous verwenden DDoS Attacken gegen Banken oder politische Einrichtungen um ihrer Unzufriedenheit, mit deren Entscheidungen, Ausdruck zu verleihen.
Die Erkennung und Bekämpfung von Angriffen ist äußerst schwierig. Deshalb wird von Serverbetreibern oft auf eine breitere Backbone zurückgegriffen um die große Menge an Anfragen bearbeiten zu können.

Literatur

[1] `http://www14.in.tum.de/personen/scheideler/lectures/2a-Alhawash.pdf`, Kahtan Alhawash

[2] `http://www.us-cert.gov/ncas/tips/ST04-015`, Mindi McDowell , US-Cert 2009

[3] `https://www.imperva.com/docs/HII_Denial_of_Service_Attacks-Trends_Techniques_and_Technologies.pdf` Imperva 2012