von Michael Bernhardt

Inhaltsverzeichnis

Was ist eine Denial of Service-Attacke?

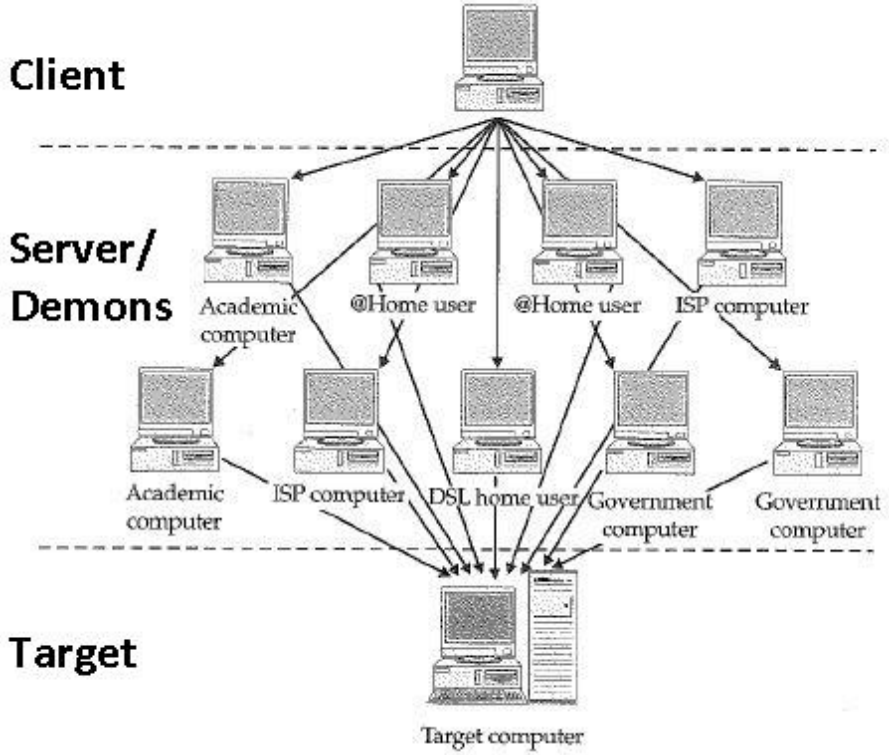
- Massenhaft eingehende Verbindungen auf ein System/Dienst bis dieser nicht mehr in der Lage ist neue Anfragen zu beantworten.

  Somit ist eine Kommunikation in dem betroffenen Netz kaum, oder sogar gar nicht mehr möglich.

Was ist eine Distributed DoS-Attacke?

Hierbei handelt es sich um einen „verteilten“ DoS-Angriff.

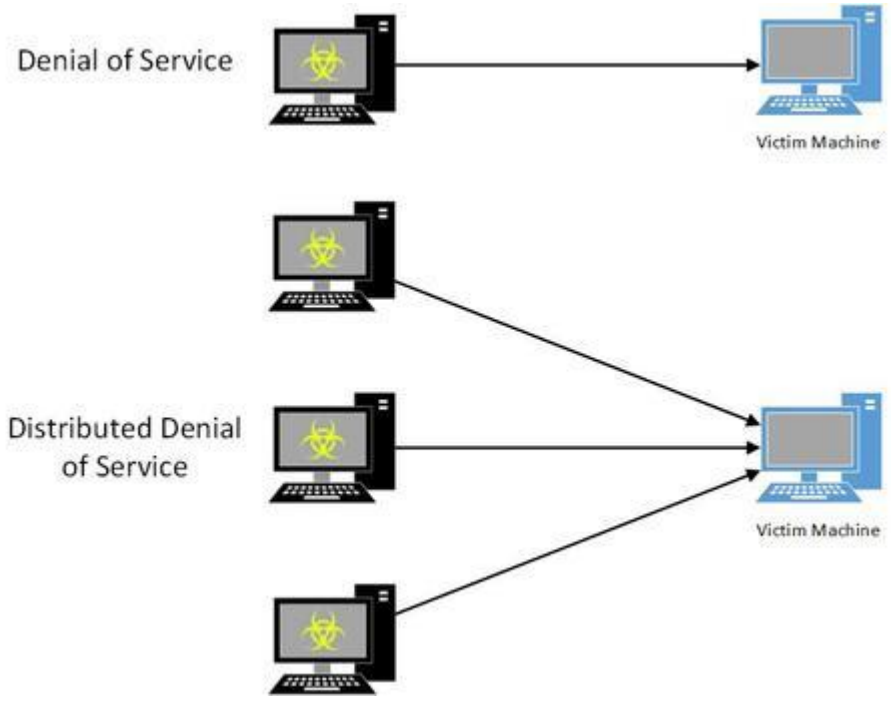
- Basiert auf ein Client/Server Modell
- Client = Angreifer
- Server/Demons (Botnetz) = im Internet gefährdete Systeme mit Schadsoftware.
- Target = Opfer des Angriffs



Grafik: George Kurtz, Stuart McClure, Joel Scambray: „Das Anti-Hacker-Buch“, 3. Auflage, 2002, Seite 685

DoS vs. DDoS

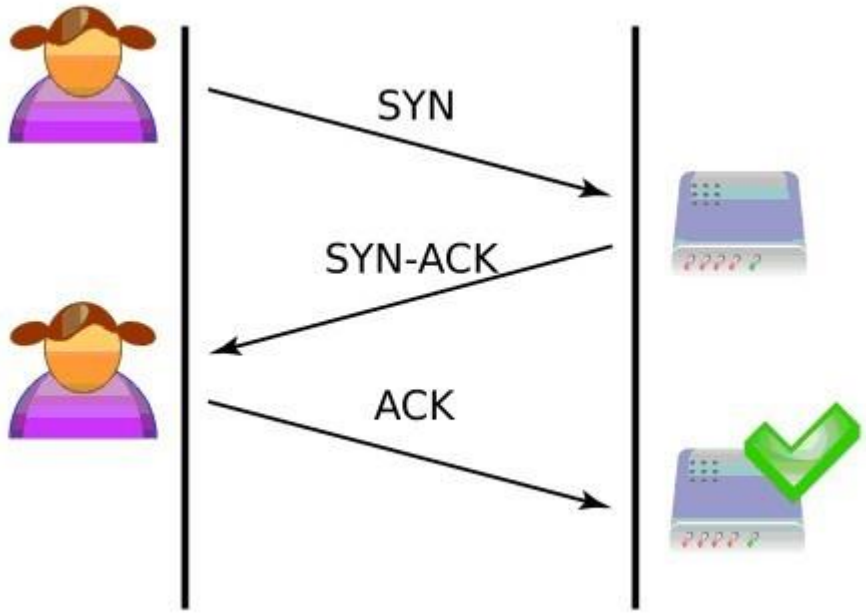
DOS	DDOS
1 Client	n Clients
1 Internetleitung	n Internetleitungen
Schaden	n-facher Schaden
eher altmodisch	sehr beliebt

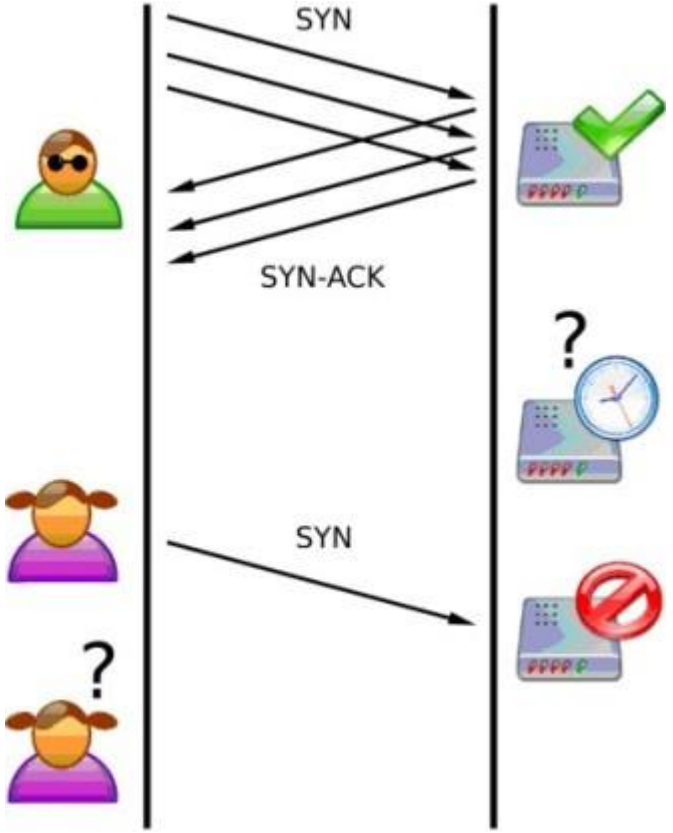


Grafik: http://www.dillonhale.com/blog/information-security/dos-vs-ddos-attacks-what-are-differences/

Beispiel einer DoS-Attacke(Syn-flooding)

3-Wege Handshake





Grafik: F5 Networks

Weitere DoS-Angriffstypen

Smurf-Angriff:

1. Angreifer sendet gefälschtes Ping-ICMP-Paket(Typ Echo-Request) an die direkte Broadcast-Adresse eines Opfer-Netzwerkes.
2. Alle Netzwerkteilnehmer bekommen dieses Paket und antworten darauf ***1 Paket, 100 Clients = 100 fache Wirkung!***

DNS-Angriff:

1. Der Angreifer schickt eine DNS-Anfrage(UDP) mit gefälschter Absender-IP-Adresse. Um möglichst viel Traffic zu erzeugen wird nach möglichst großen TXT-Records angefragt.
2. Der DNS-Server schickt die Anfrage an die Absender-Adresse zurück.

DDoS-Angriffstypen(Tools)

Die Anzahl an DDoS-Tools steigt ständig, daher ist eine vollständige und aktuelle Analyse unmöglich!

Tribe Flood Network(TFN):

- Von einem Hacker namens Mixter geschrieben (1999)
- Erstes öffentlich verfügbare DDoS-Tool auf dem Markt.
- UNIX-basiertes Programm mit Client- und Serverkomponente.
- Bietet Angriffsarten: ICMP, Smurf, UDP- und SYN-Flood.

DDoS-Angriffstypen(Tools)

Trinoo:

- Funktioniert nach ähnlichen Prinzip wie TFN
- Unterschied: Zwischen den Clients und den Servern befinden sich noch Handler (höhere Schachtelung).

Stacheldraht:

- Verbindet Merkmale von Trinoo mit denen von TFN.
- Unterschied: Die Kommunikation ist verschlüsselt.
- Zusätzlich: verschlüsselte Telnet-Sessions zwischen Handler und Servern

Welche Absichten hat der Angreifer?

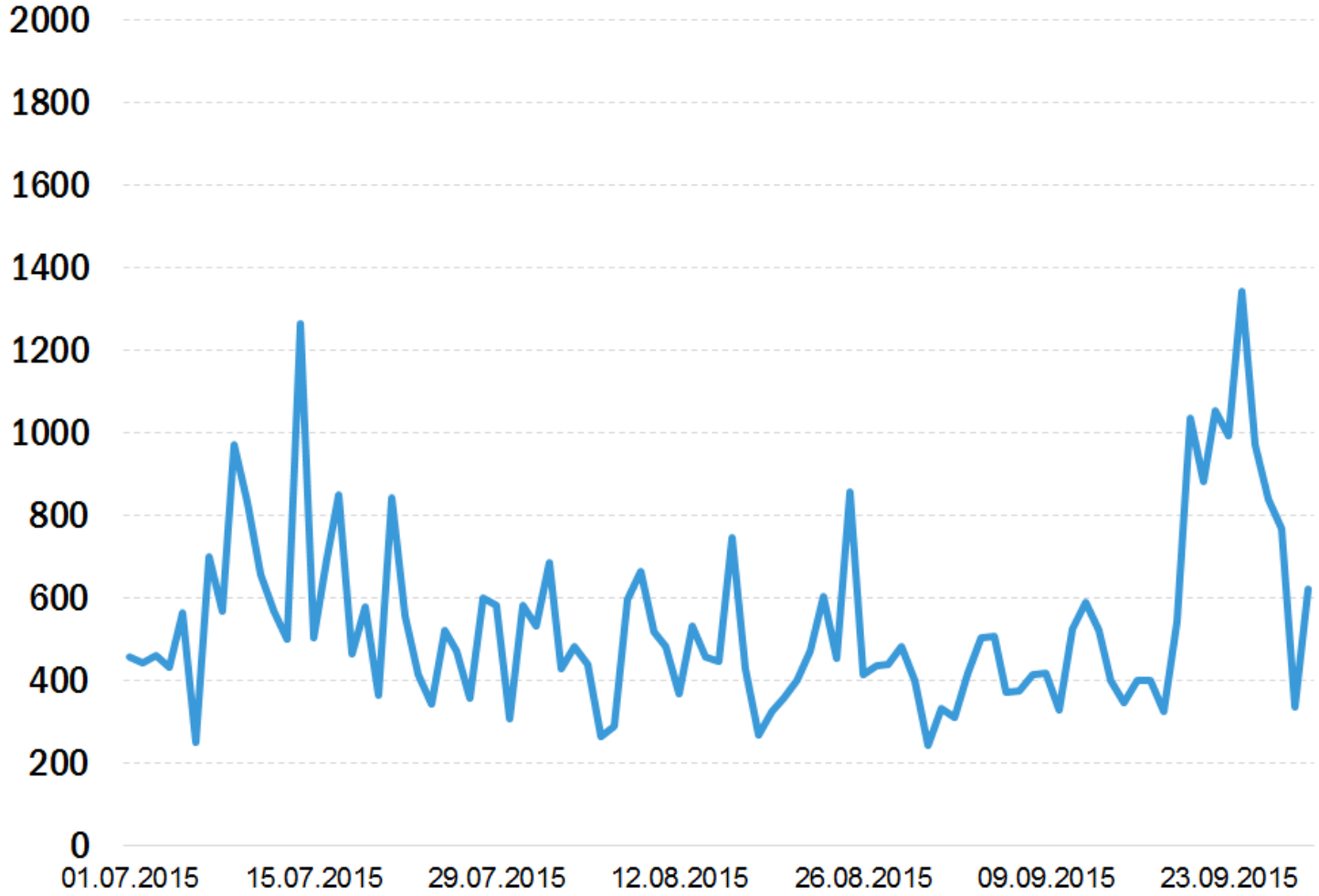
- ***Verfügbarkeit eines Systems/Service einschränken oder ausschalten.***

- Ausfallzeiten verursachen
- Einen wirtschaftlichen Schaden verursachen
- Erpressung
- Politische Gründe
- Machtgefühl

Vorfälle in der Praxis

Sommer 2014: Ein bis dahin nicht vorstellbarer 300 Gbps DDoS-Angriff nutzt 100.000 ungepatchte Server für ein Botnetz. Ein ungenanntes Datencenter wurde Ziel dieses extrem großen DDoS-Angriffs.
Juli 2015: Das New York Magazine erfährt eine DDoS-Attacke kurz nachdem die Interviews von 35 Frauen, die Bill Cosby der sexuellen Nötigung bezichtigen, veröffentlicht werden.
Dezember 2015: DDoS-Angriffe gegen Microsofts Xbox Live Dienst und PlayStation-Network. Konsolenbesitzer konnten nicht mehr Online-spielen.
Januar 2016: Einige HSBC-Bank Kunden können zwei Tage vor Abgabefrist der Steuererklärung in Großbritannien ihre Online-Accounts nicht aufrufen.

Fazit



Fazit

- „Das gefährliche an DoS-Attacken ist, dass sie in den meisten Fällen ohne großen Aufwand durchgeführt werden können. Jedoch wird man sich dagegen nie wirklich zur Wehr setzen können, da Computer bekanntlich miteinander kommunizieren müssen und die meisten Attacken über die Kommunikationsprotokolle UDP,TCP/IP durchgeführt werden.“

Quellen

- George Kurtz, Stuart McClure, Joel Scambray: „Das Anti-Hacker-Buch“, 3. Auflage, 2002
- Manu Carus: „Ethical Hacking“, 2008
- Kai Fuhrberg, Dirk Häger, Stefan Wolf: „Internet-Sicherheit“, 3. Auflage, 2001
- http://www.heise.de/security/meldung/DDoS-auf-Heise-ueber-zu-offene-DNS-Server-1674636.html
- http://www.computerlexikon.com/begriff-ddos-attacke
- https://www.globalsign.com/de-de/blog/denial-of-service-im-iot/
- http://www.exali.de/Info-Base/ddos-attacke
- https://www.link11.de/ddos-schutz/was-sind-ddos-attacken.html?gclid=COGx6sb6vcwCFYEy0wodDbUGSg
- http://www.computerwoche.de/a/kein-anschluss-unter-dieser-url,2504910,3
- http://www.dillonhale.com/blog/information-security/dos-vs-ddos-attacks-what-are-differences/
- http://www.techiwarehouse.com/userfiles/Denial%20Of%20Service.jpg