Denial of Service mit deinem Toaster*

Sascha Ohms

*dies ist kein Vortrag über IoT-Botnetze

Slowloris / Slow HTTP Attack

- geringe Bandbreite benötigt
- quasi keine CPU-Last (auf beiden Seiten)
- primäres Ziel: Webserver
- Apache aber auch Nginx und Lighttpd

Funktionsweise

- Normaler Request

```
GET / HTTP/1.1\r\n
Host: example.org:80\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2)\r\n
\r\n
```

- Slowloris

```
GET / HTTP/1.1\r\n
Host: example.org:80\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2)\r\n
X-rnejiHypfUBGSqJFR4: kqFPTVbdQpRchxLGns\r\n
X-AmksLJXtCYy9dRBjaE: jG6WN9TXs2DP4rZEMh\r\n
```

Funktionsweise - Erklärung

- Limit von maximal möglichen Verbindungen ausnutzen
- Requests möglichst lange aufrecht halten
- Timeout zurücksetzen, indem weitere Daten gesendet werden

Schutz

- Anzahl möglicher Verbindungen einer IP limitieren
  - ModSecurity oder mod_reqtimeout für Apache
  - Firewall-Regeln
- Connection Timeout erheblich verringern (60s → 5s)
- Limit maximal gleichzeitiger Verbindungen erhöhen

Livedemo, olé

Beobachtung

- keine spürbare CPU-Last
- kein unauffälliger Traffic im Netzwerk
- keine Log-Einträge (außer Socket wird geschlossen)
- einzige Auffälligkeit: viele **aktiv bleibende** Verbindungen

Quellen

- https://github.com/gkbrk/slowloris
- https://github.com/valyala/goloris
- http://security.ge.cnr.it/?q=slowdroidmitigation
- https://blog.qualys.com/securitylabs/2011/11/02/how-to-protect-against-slow-http-attacks
- https://blog.qualys.com/securitylabs/2011/08/25/new-open-source-tool-for-slow-http-attack-vulnerabilities
- https://commons.wikimedia.org/wiki/File:Nycticebus_coucang_002.jpg