AMPLIFICATION ATTACKS

The Butterfly Effect Of The Cyber World

Prepared : **Musa ŞANA**

Advisor : **Zeydin PALA**

BÖLÜM I

Temel Tanımlar ve DoS/DDoS Saldırıları

Tanımlar

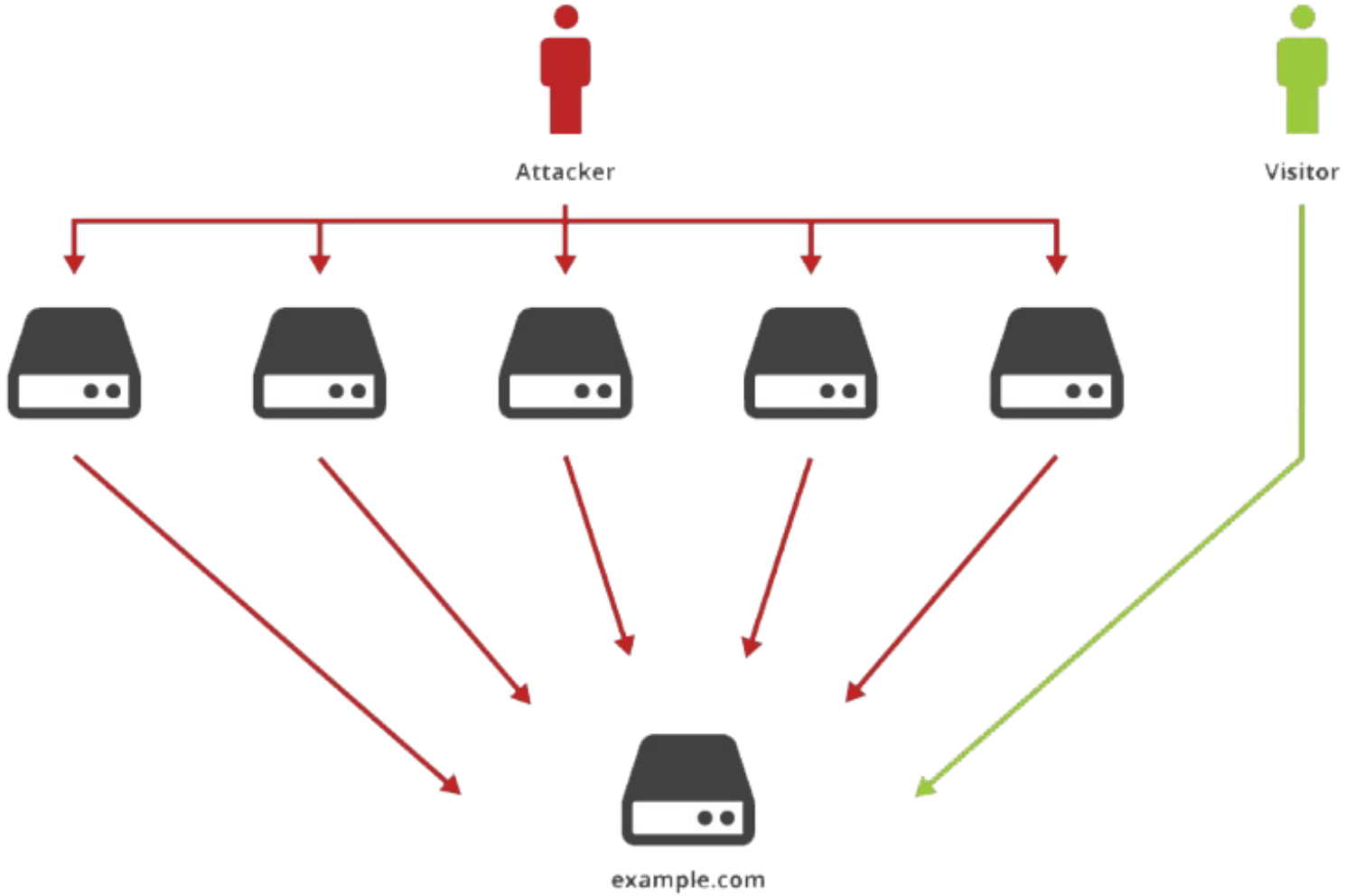
- Denial Of Service ve Distributed Denial of Service Nedir?
- Neyi Amaçlar ? (Bandwidth ve Kaynak istismarı)
- İnternetin ilk yıllarından beridir var olmasına rağmen hala nasıl kesin çözüme bulunamamıştır ?

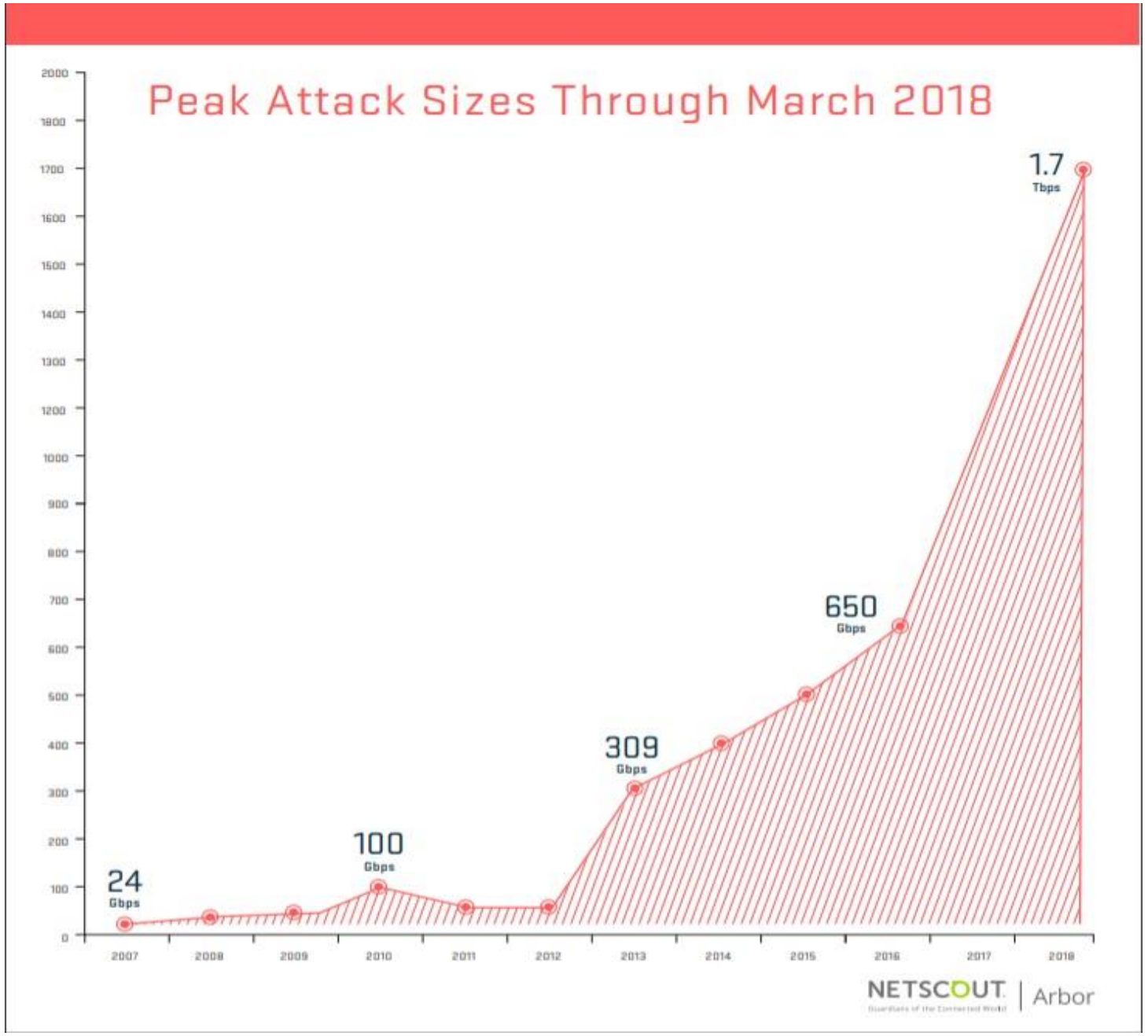
Neyden kaynaklanmaktadır ?

- Protokol veya uygulama çalışma yapısının istismar edilmesiden kaynaklanır.
  - UDP (User Datagram Protocol)
    - UDP Flood Attack
    - UDP Fragmentation
    - Fraggle
    - Teardrop
  - ICMP (Internet Message Control Protocol)
    - icmp/ping Flood (echo request,Type 0 Code 8), max packet size 64KB
    - Smurf (Default gelen yapılandırma ayarlarıyla günümüzde artık rastlanılmamaktadır.)
    - Ping Of Death
  - Diğerleri
    - Dns flood, syn flood, http flood, ntp, dns reflection ...
    - Veya uygulama seviyesindeki saldırılar; wordpress, adobe flash player, internet explorer vs.

Normal DDoS Diyagramı

- Tek Kural: Ne kadar (zombi) makine, o kadar trafik...





https://www.netscout.com/sites/default/files/inline-images/memcached%201.jpg

Geçmişten Günümüze Yapılan En Büyük DDoS Saldırıları

- 2007 = ~24 Gbps
- 2010 = ~100 Gbps
- 2013 = ~309 Gbps
- 2016 = ~650 Gbps
- 2018 = ~1.7 Tbps

BÖLÜM II

Amplification Saldırıları

Tanım, Metod, Metodoloji…

- Amplification saldırıları, DoS/DDoS saldırılarında kullanılan bir metoddur.

- Az bir kaynak kulllanılarak çok büyük traffik oluşturulabilir. Bu durum bazen 1’e 1000 seviyelerine bile çıkabilmektedir.

- Tekil bir kullanıcı sistemli bir yol izleyerek birçok ülkenin çıkış trafiğinden daha fazla trafik üreterek hedefe yönlendirebilir.

Gerek ve Yeter Şartlar

- Amplification saldırıları için iki temel şart gerekir.
  - 1) UDP Protokolü olması – (IP Spoofing yapmak için*)
  - 2) Gönderilen bir requeste dönecek olan response boyutunun requestin

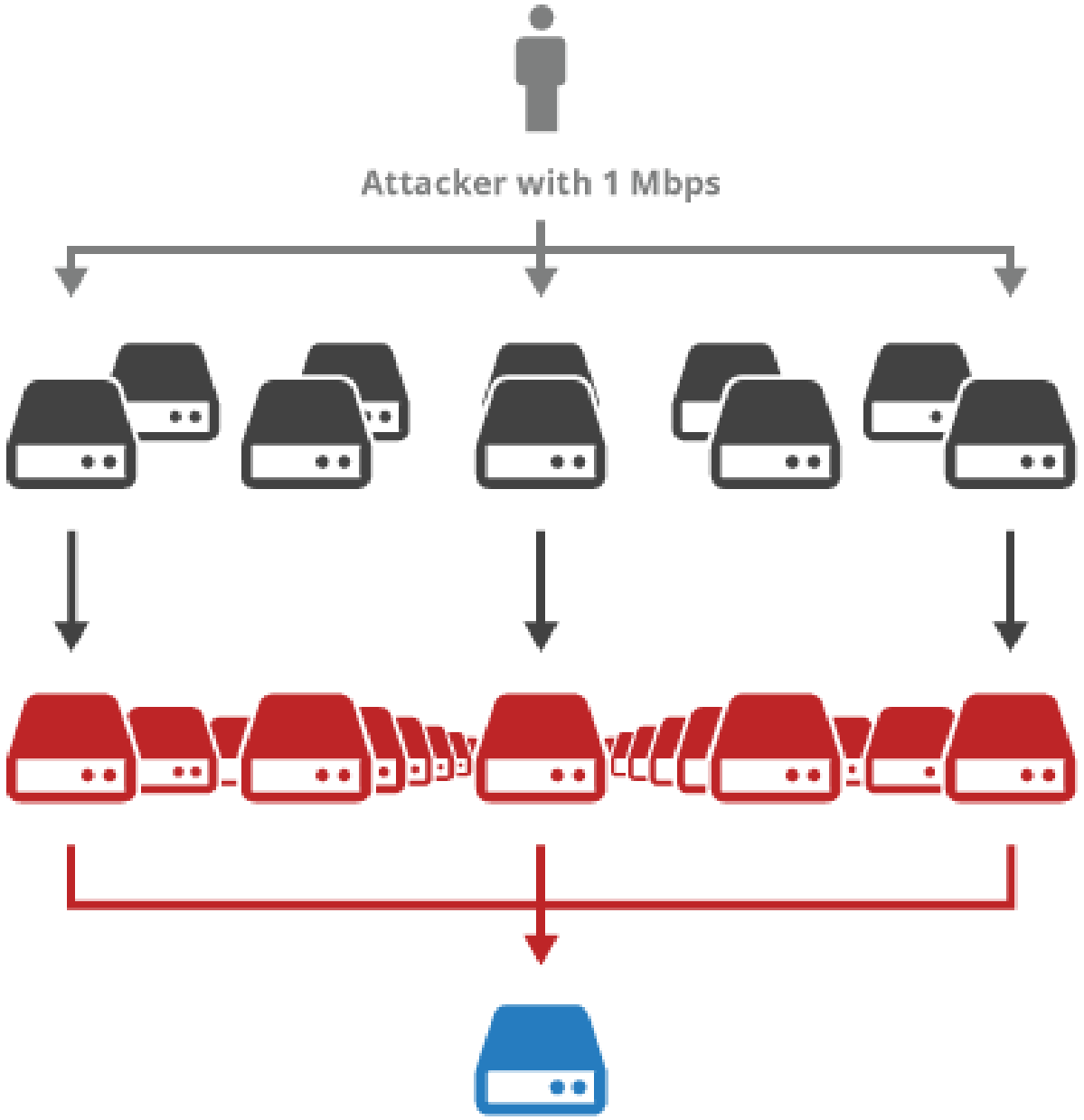
  (en az) onlarca katı büyüklüğünde olması gerekir.

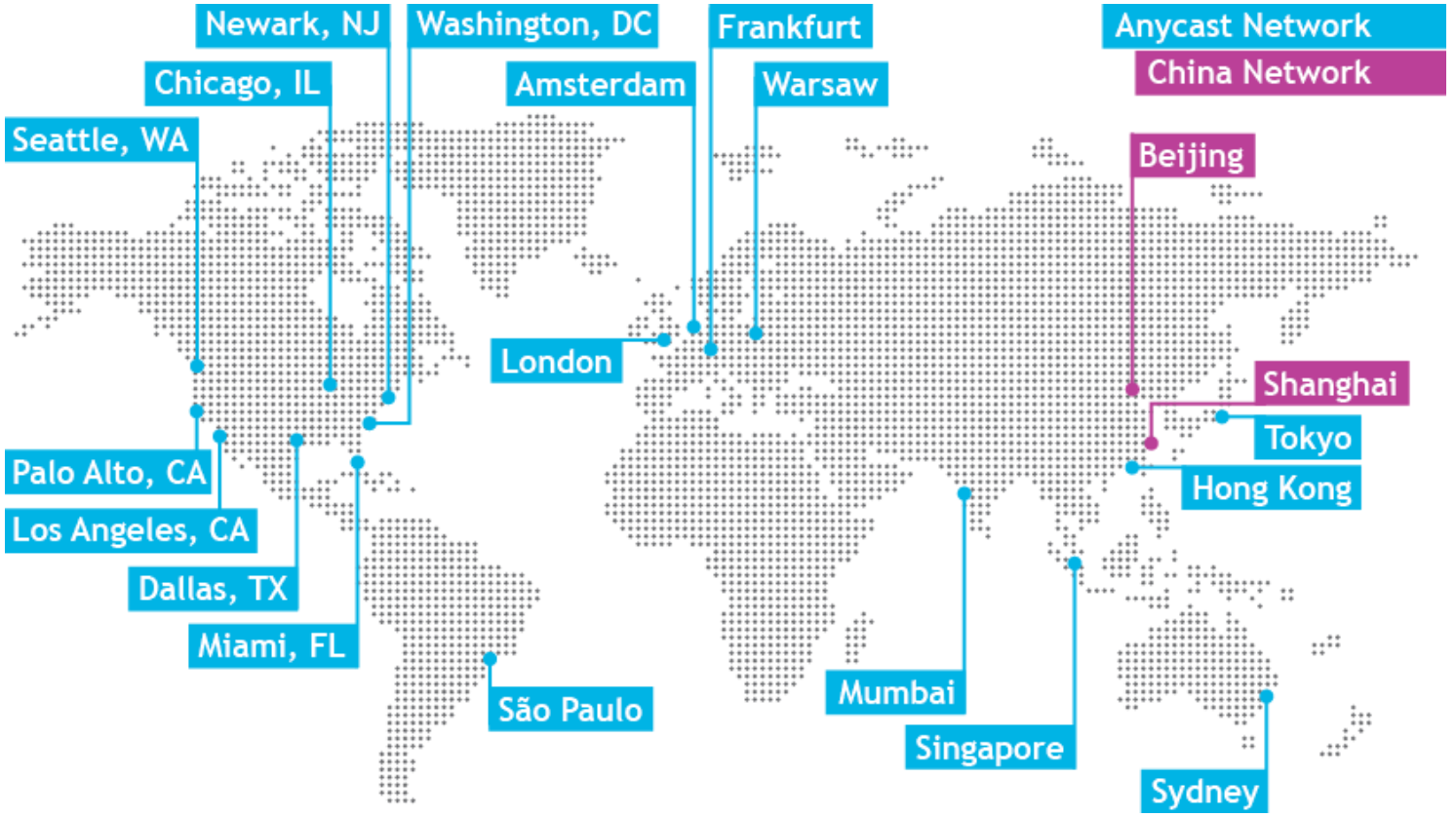
  * Uygulama seviyesinde alınabilen birkaç ufak önlem vardır.

Saldırganlar için biçilmiş kaftan

- Amplification metodu saldırgana iki büyük avantaj sağlar.
  - 1) Source ip değerinin manipüle edilebilir olmasından dolayı **gizlilik**
  - 2) Sahip olunan bant genişiğinin yüzlerce katı **daha fazla trafik** üretebilme

  ... daha ne olsun ?


Attacker with 1 Mbps
1 Mbps connection
10 compromised trigger machines with 1 Gbps
1 Gbps connection x10
400 'amplifier' machines
Amplification factor of 50x
500 Gbps hits target machine from amplifiers



DOMAIN NAME SYSTEM (DNS)

« Sanal dünyanın adres defteri»

DNS Amplification

- İki tür DNS sorgusu vardır.
  - 1) İterative Sorgular
    - a) Yapılan sorguya ya cevap döner,
    - b) ya bilmediğini ve başka dns suncusuna yönlendirir.
  - 2) Recursive Sorgular
    - a) Yapılan sorguya ya cevap döner
    - b) ya hata mesajı döner.
    - c) üst dns sunucularına sorabilir. (Duruma göre)

```
xubuntu ~ dig +short musana.net @1.1.1.1
104.27.158.210
104.27.159.210
xubuntu ~ dig +short musana.net @dns1.alparslan.edu.tr
xubuntu ~
```

- DNS hem TCP hem de UDP üzerinde çalışır.
  - **TCP/53 if Truncated == 1 else UDP/53**

```
xubuntu ~ sudo hping3 -S -p 53 dns1.alparslan.edu.tr -c 2
HPING dns1.alparslan.edu.tr (wlp9s0 79.123.134.134): S set, 40 headers + 0 data bytes
len=44 ip=79.123.134.134 ttl=51 DF id=0 sport=53 flags=SA seq=0 win=14600 rtt=167.9 ms
len=44 ip=79.123.134.134 ttl=51 DF id=0 sport=53 flags=SA seq=1 win=14600 rtt=191.7 ms

--- dns1.alparslan.edu.tr hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 167.9/179.8/191.7 ms
```

```
xubuntu ~ sudo hping3 -S -p 53 ns1.namebrightdns.com -c 2
HPING ns1.namebrightdns.com (wlp9s0 54.236.164.22): S set, 40 headers + 0 data bytes

--- ns1.namebrightdns.com hping statistic ---
2 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

1 query = 40bytes – 60bytes

```
xubuntu ~ dig alparslan.edu.tr

; <<>> DiG 9.10.3-P4-Ubuntu <<>> alparslan.edu.tr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52923
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;alparslan.edu.tr.              IN      A

;; ANSWER SECTION:
alparslan.edu.tr.       42619   IN      A       79.123.134.2

;; Query time: 13 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Fri Apr 27 11:48:04 +03 2018
;; MSG SIZE  rcvd: 50
```

Bir dns sunucusuna kendisinde olmayan bir domain sorgulatıldığında ?

- Eğer recursive sorguya kapalı ise;
  - Sorguyu yapana olumsuz cevap döner.

- Eğer recursive sorguya açık ise;
  - Sorgulanan domaine ait kayıt kendisinde olmadığından dolayı bir üst dns sunucuna sorar
  - (Eğer bir üst dns sunucunda da yoksa o da bir üst dns sunucusana sorar)
  - Bu durum, sorgulanan domaine ait cevap verecek bir dns sunucusu bulunana kadar devam eder.
  - Eğer cevap veren dns sunucu çıkar ise sorgulayana/istemciye cevap döner.
  - Eğer geriye soracak dns sunucusu kalmadıysa istemciye ilgili domain ait cevap bulamadığını söyler. (Bu durumda ya sorgulanan domain yoktur, yada sorgulanan domainden sorumlu name server servis dışıdır.)

DNS'de olmayan bir domain sorgulatıldığında

```
xubuntu ~ dig musana.net @dns1.alparslan.edu.tr any

; <<>> DiG 9.10.3-P4-Ubuntu <<>> musana.net @dns1.alparslan.edu.tr any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 3010
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;musana.net.                    IN      ANY

;; Query time: 166 msec
;; SERVER: 79.123.134.134#53(79.123.134.134)
;; WHEN: Fri Apr 27 11:42:38 +03 2018
;; MSG SIZE  rcvd: 39
```

1x Request, 11x Response

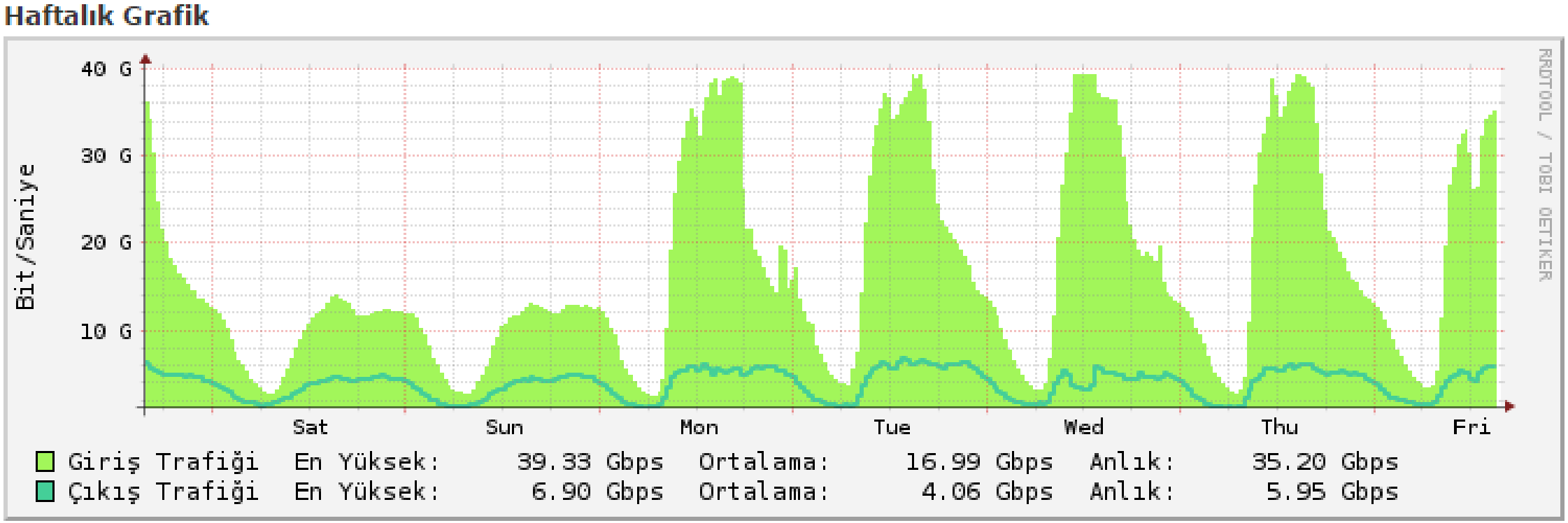
```
;; QUESTION SECTION:
;alparslan.edu.tr.              IN      ANY

;; ANSWER SECTION:
alparslan.edu.tr.       3600    IN      MX      5 ALT2.ASPMX.L.GOOGLE.COM.
alparslan.edu.tr.       3600    IN      MX      10 ALT3.ASPMX.L.GOOGLE.COM.
alparslan.edu.tr.       3600    IN      MX      10 ALT4.ASPMX.L.GOOGLE.COM.
alparslan.edu.tr.       3600    IN      MX      1 ASPMX.L.GOOGLE.COM.
alparslan.edu.tr.       3600    IN      MX      5 ALT1.ASPMX.L.GOOGLE.COM.
alparslan.edu.tr.       86400   IN      SOA     dns1.alparslan.edu.tr. hostmaster.alp
alparslan.edu.tr.       86400   IN      NS      dns1.alparslan.edu.tr.
alparslan.edu.tr.       86400   IN      NS      dns2.alparslan.edu.tr.
alparslan.edu.tr.       86400   IN      A       79.123.134.2
alparslan.edu.tr.       86400   IN      TXT     "google-site-verification=nUsae_cAyaw
alparslan.edu.tr.       86400   IN      TXT     "v=spf1 include:aspmx.googlemail.com
alparslan.edu.tr.       86400   IN      TXT     "MS=ms55992898" "3600"

;; ADDITIONAL SECTION:
dns1.alparslan.edu.tr.  86400   IN      A       79.123.134.134
dns1.alparslan.edu.tr.  86400   IN      AAAA    2002::4f7b:8686
dns2.alparslan.edu.tr.  86400   IN      A       79.123.135.135
dns2.alparslan.edu.tr.  86400   IN      AAAA    2002::4f7b:8787

;; Query time: 203 msec
;; SERVER: 79.123.134.134#53(79.123.134.134)
;; WHEN: Fri Apr 27 11:43:13 +03 2018
;; MSG SIZE  rcvd: 546
```

Request Query Size : 50 Bytes

Reponse Size : 546 Bytes

İyi de neden DNS sunucuları ?

- Rusya «.tr» alan adından sorumlu olan isim sunucularına ddos düzenledi. - 14 Aralık 2015 - bbc.com
- ODTÜ: Dünya tarihinde yaşanmış en yoğun saldırı - tr.sputniknews.com



NETWORK TIME PROTOCOL (NTP)

NTP Genel Bilgi

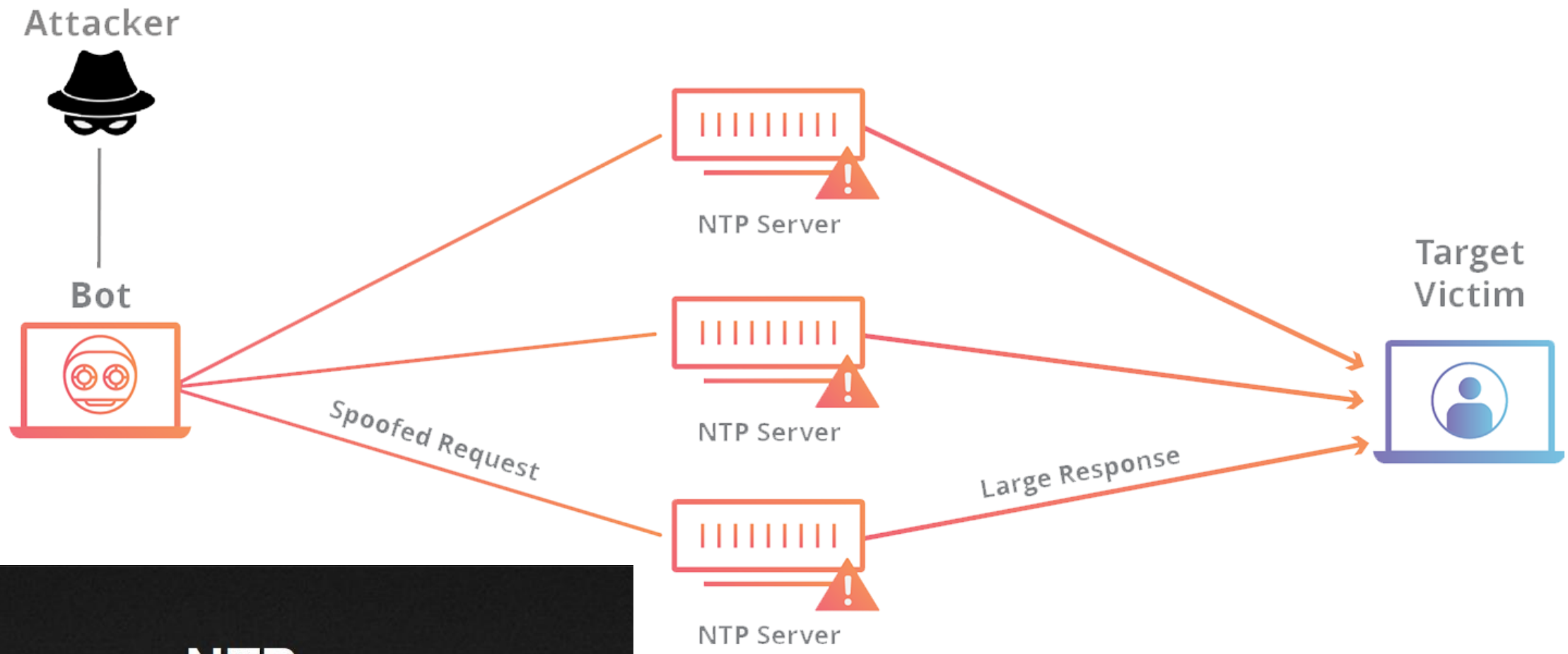
- Ntp, bir ağda bulunan cihazların saat ayarlarının senkron çalışabilmesi kullanılan bir protokoldur.
- UDP üzerinde çalışır.
- Default olarak 123 portunu kullanır.
- İç veya dış networklere hizmet verebilir.
- Zaman senkronizasyonu yapan protokol ne kadar tehlikeli olabilir ki ?

1x Request, 210x Response

- Public olan bir NTP sunucuda monlist modu aktif ise, o NTP sunucusu en son etkileşimde bulunduğu 600 makineye ait ip bilgilerini dönderebilir.

- Bu spoof edilmiş bir ip adresinden gönderilen 234byte boyutunda bir pakete yaklaşık ~50k cevap dönebileceği anlamına gelir.

NTP Saldırı Diyagramı



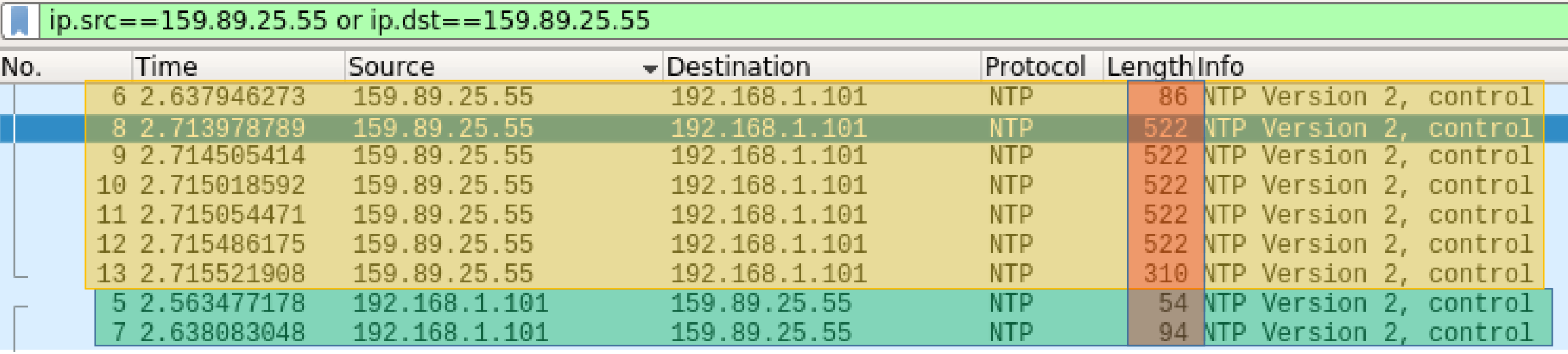
NTP

Search for ntp port:123 returned 10,900,362 results on 27-04-2018

Network Time Protokol(NTP) Amplification

- 2013 NTP ile yapılan DDoS saldırısında 400 gbps boyutlarına ulaşmıştır. – Türkiye çıkış trafiğine denk..

- Request: ~150bytes, Response: ~3kB



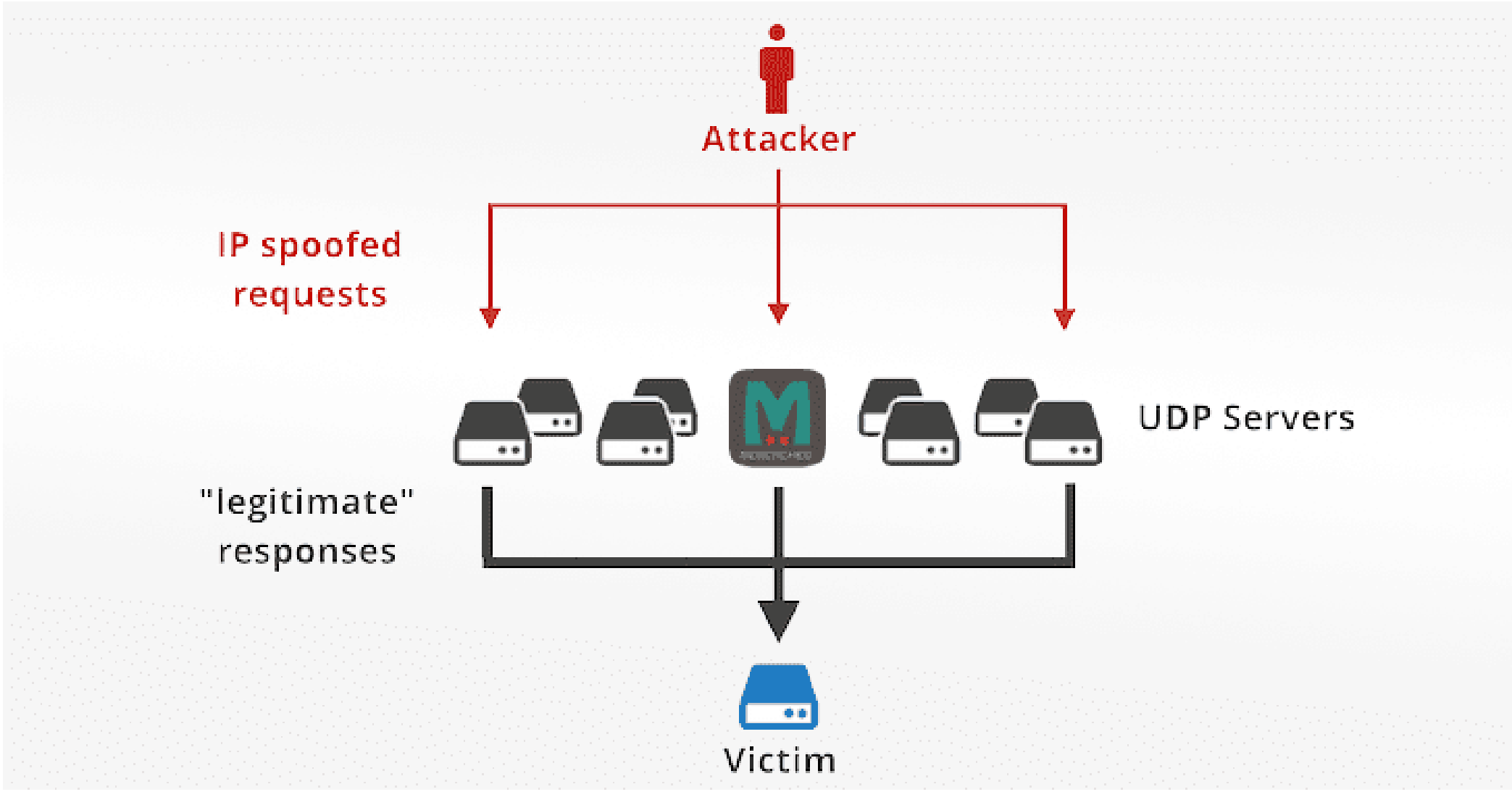
Ddos ile memcache ne alaka ?

Memcache Genel Bilgi

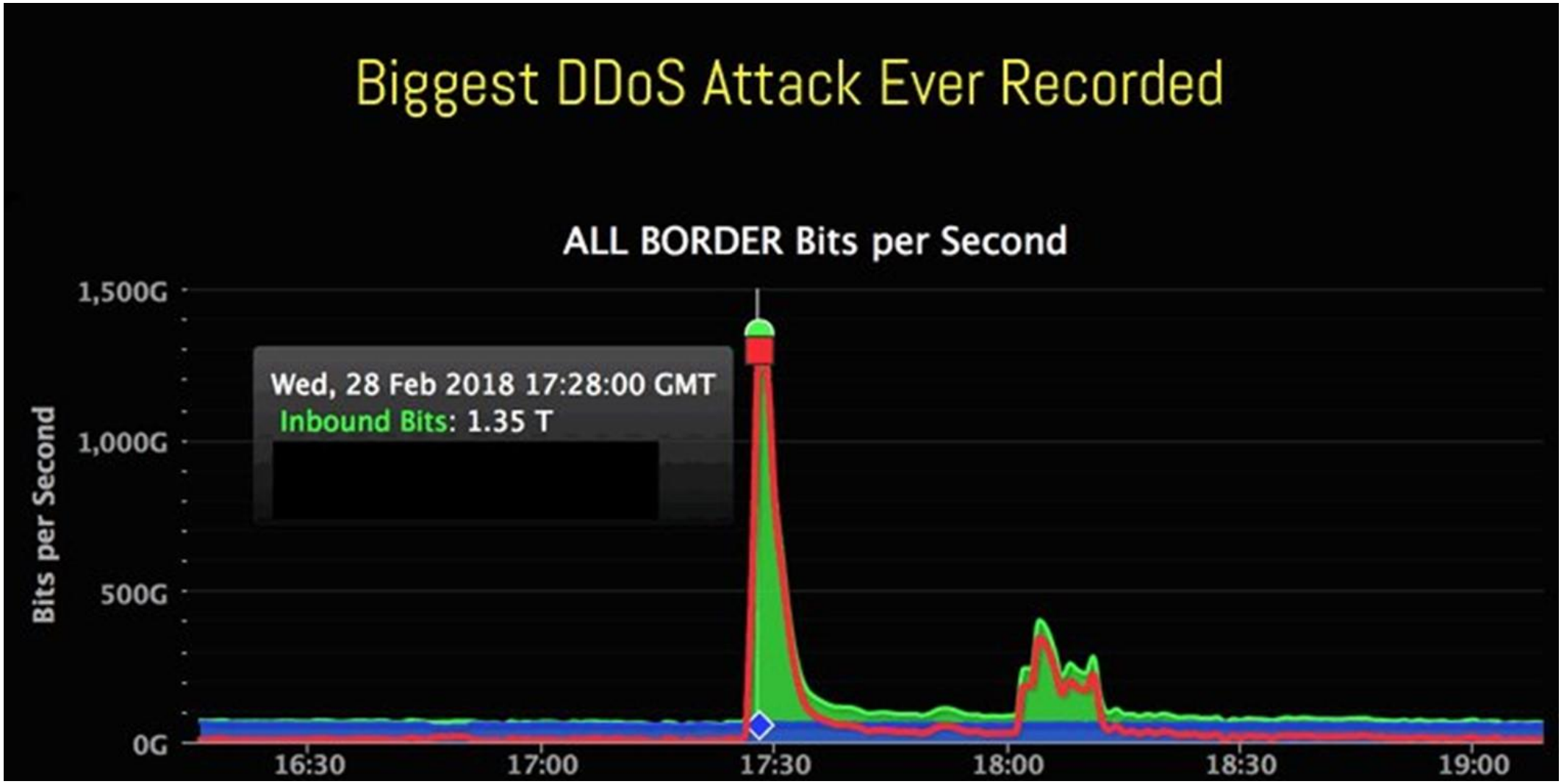
- Memcache, (genellikle)database işlemlerin olduğu sistemlerde databasede sık sık yapılan aynı sorgu sonuçlarını bellekte tutarak bir daha ilgili sorgunun gelmesi durumunda database üzerinde sorgu çalıştırmak yerine cachelediği değeri döndererek hız ve performans sağlayan bir önbellek mekanizmasıdır.

- UDP üzerinde 11211 portunda çalışır.

Memcache Saldırı Diyagramı



15 byte boyutundaki bir isteğe dönen cevap paketi **~700kB** olabilmektedir.
Yaklaşık 51.000 kat daha fazla... Sonuç : **1.35 TeraBit**



Evde denemeyin !

SORULAR

musana.net | github.com/musana

- Diyagramlar **cloudflare**'dan alınmıştır.

* Sunum dosyasına musana.net adresinden ulaşabilirsiniz.