PurpleBox

An Army of Zombies

- MIRAI -

www.prplbx.com

$whoami

Ömer Faruk Çulha

PurpleBox -> Cyber Security Engineer

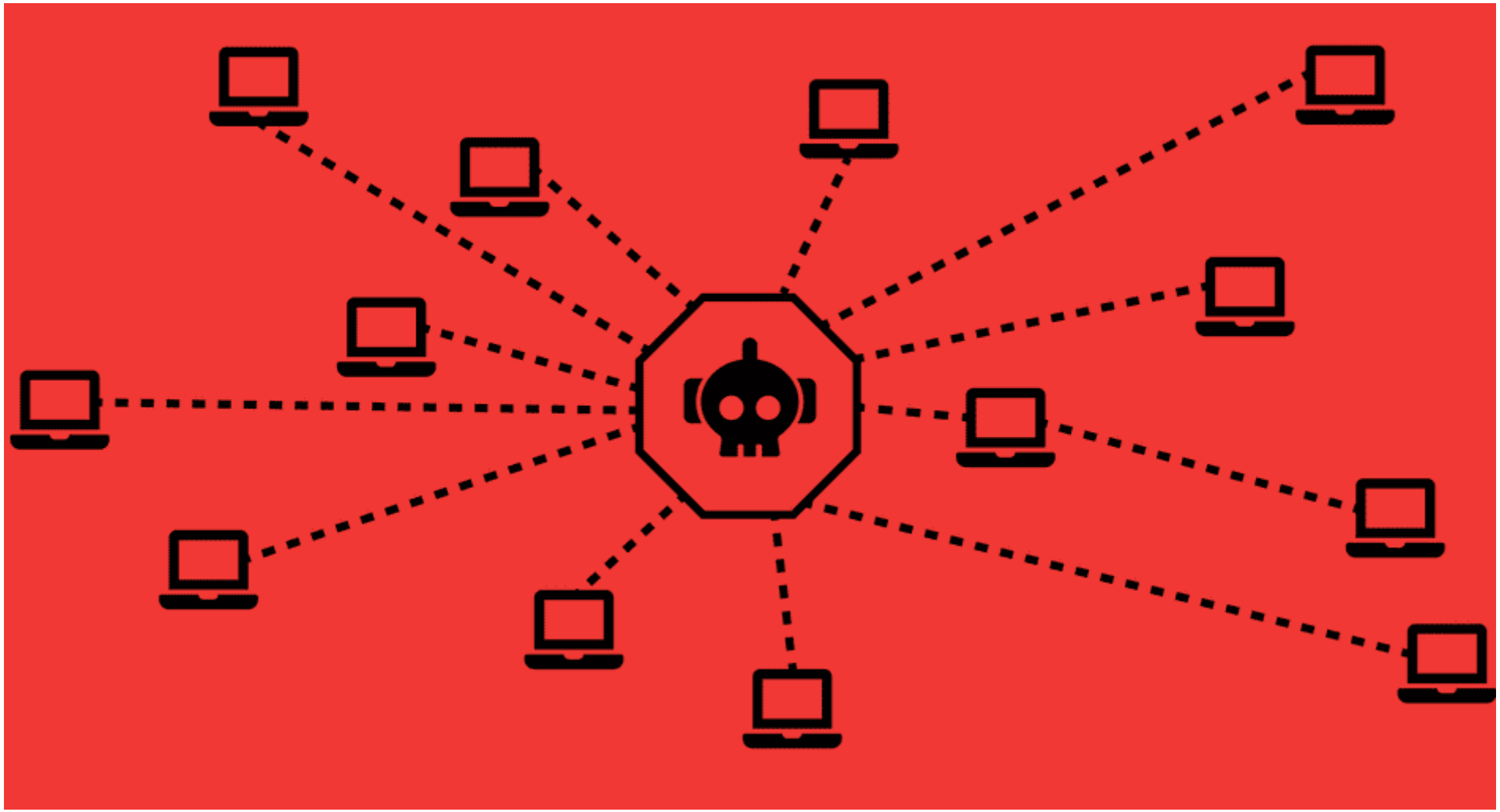
Sakarya Üniversitesi -> Makine Müh.

https://twitter.com/0x1337root

https://tryhackme.com/p/0x1337root

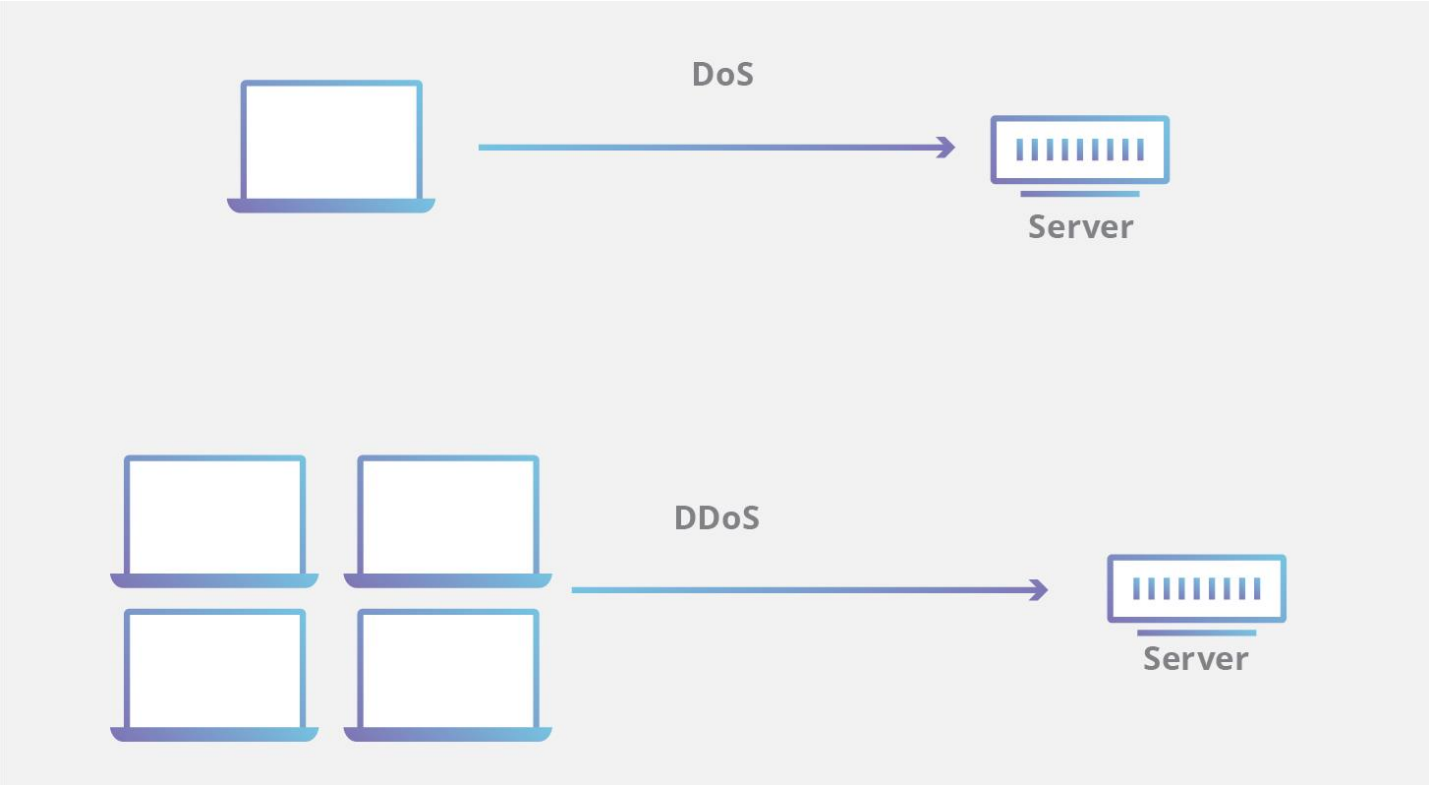
https://www.linkedin.com/in/ömer-faruk-çulha-b95880195

MIRAI Nedir?



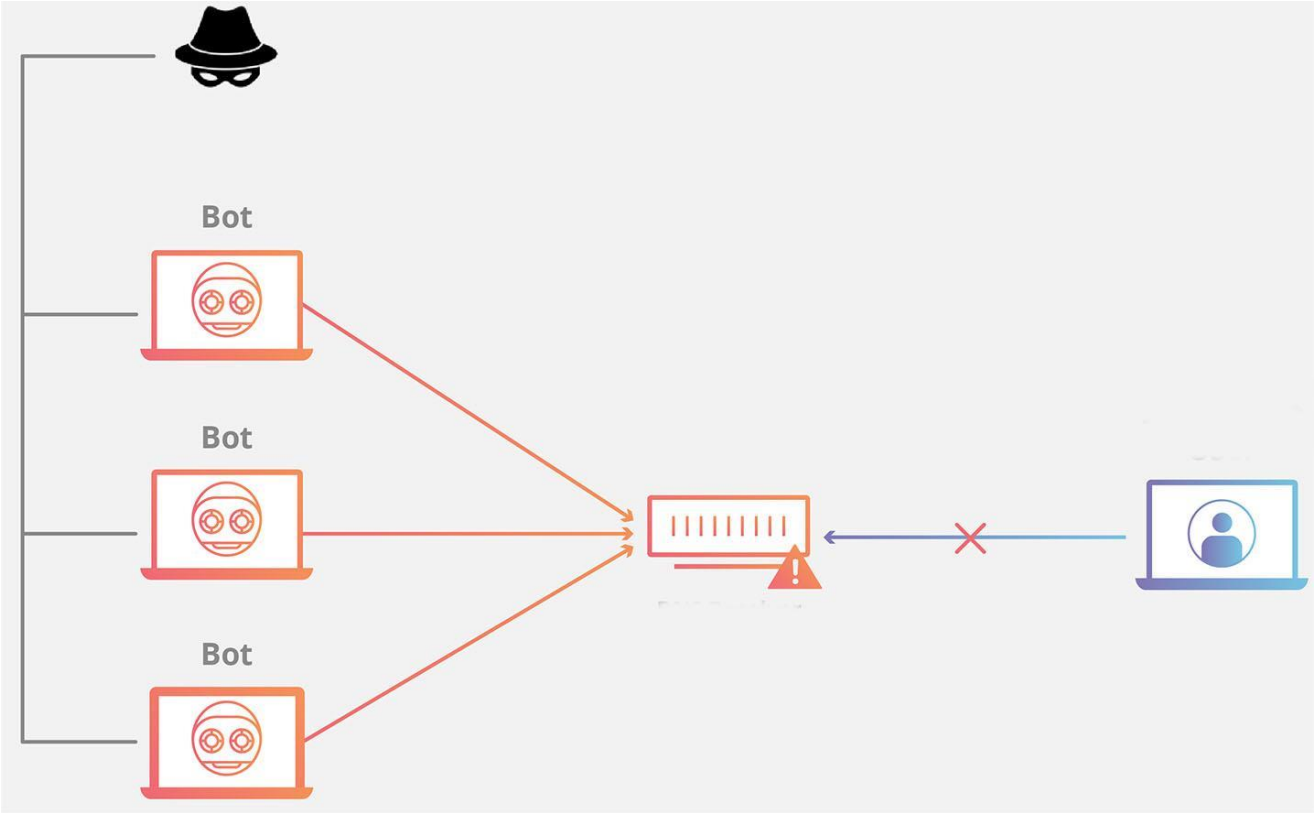
DoS - DDoS ?

- Denial of Service
- Distributed Denial of Service

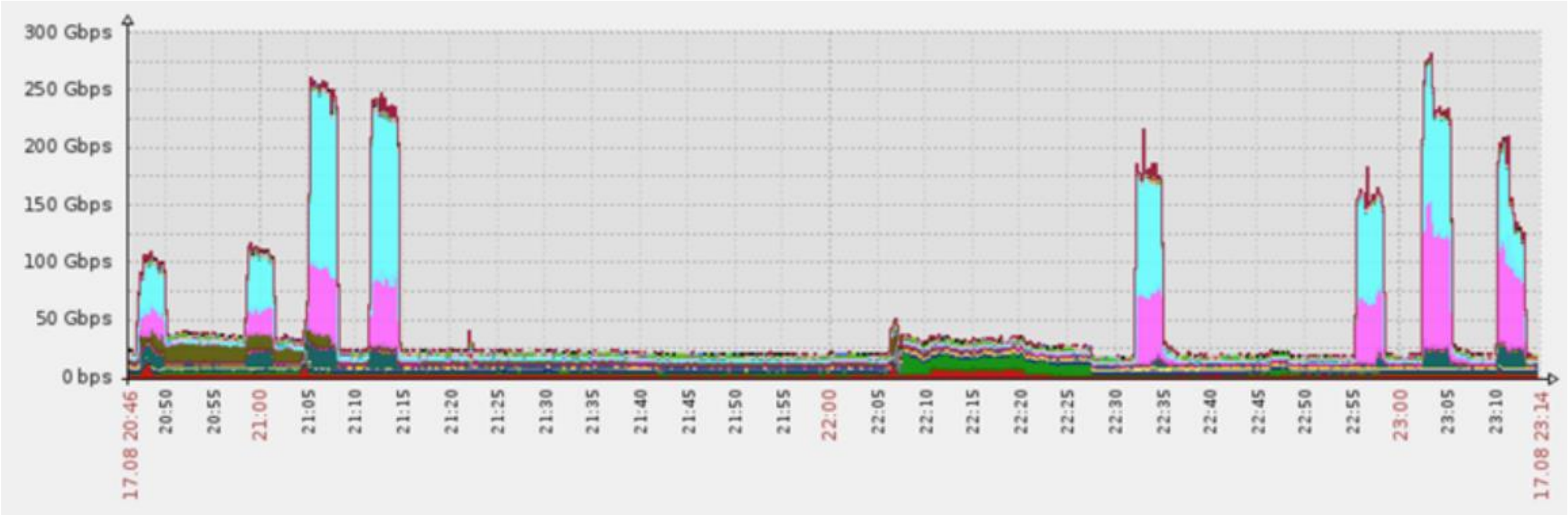


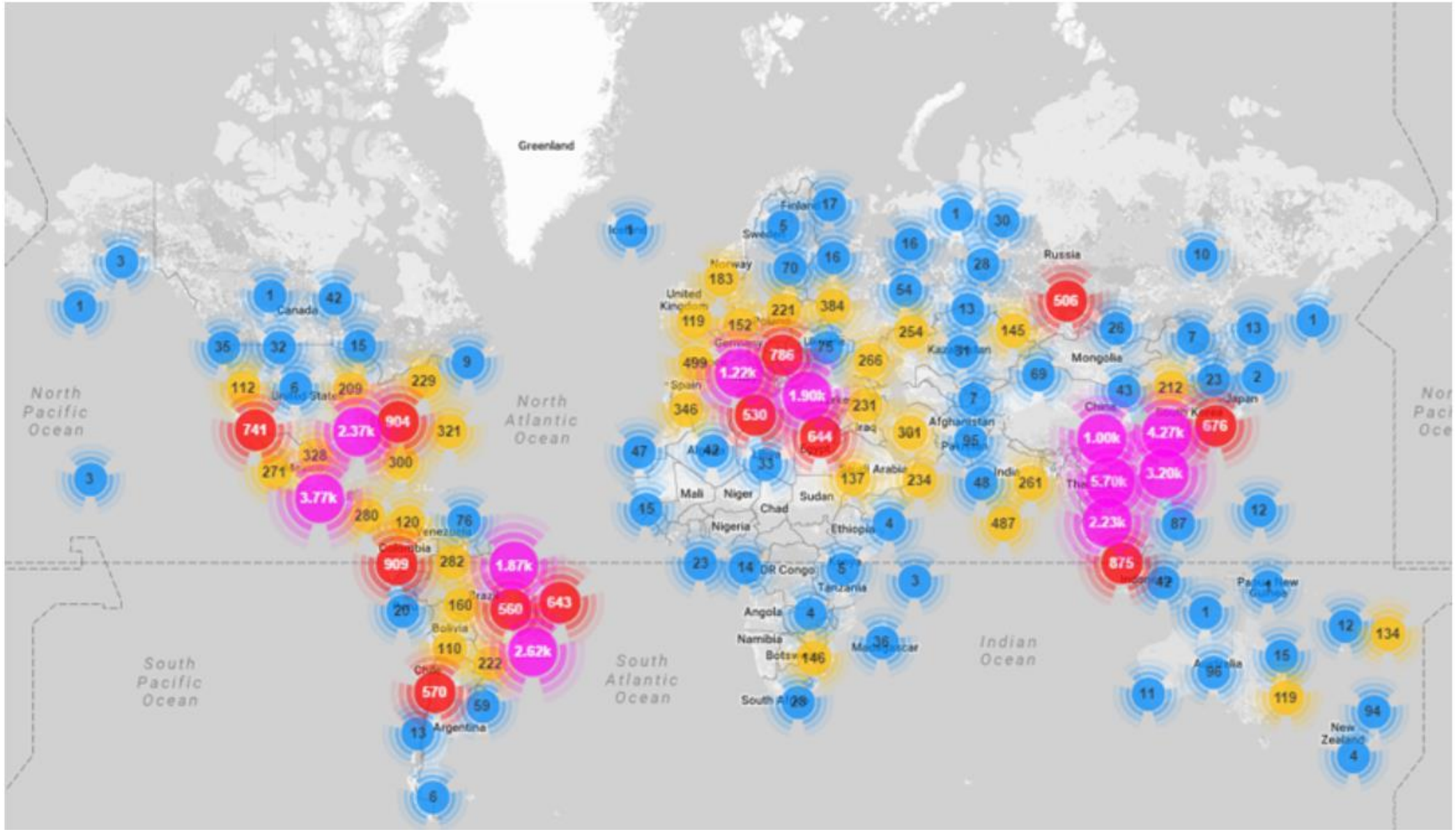
DDoS Çeşitleri ?

- Ağ ve Taşıma Katmanı
  - TCP SYN Flood
  - UDP Flood
  - TCP RST Flood
  - TCP FIN Flood
- Uygula Katmanı
  - HTTP Flood
  - DNS Flood



"I'm no expert, but I think it's some kind of cyber attack!"

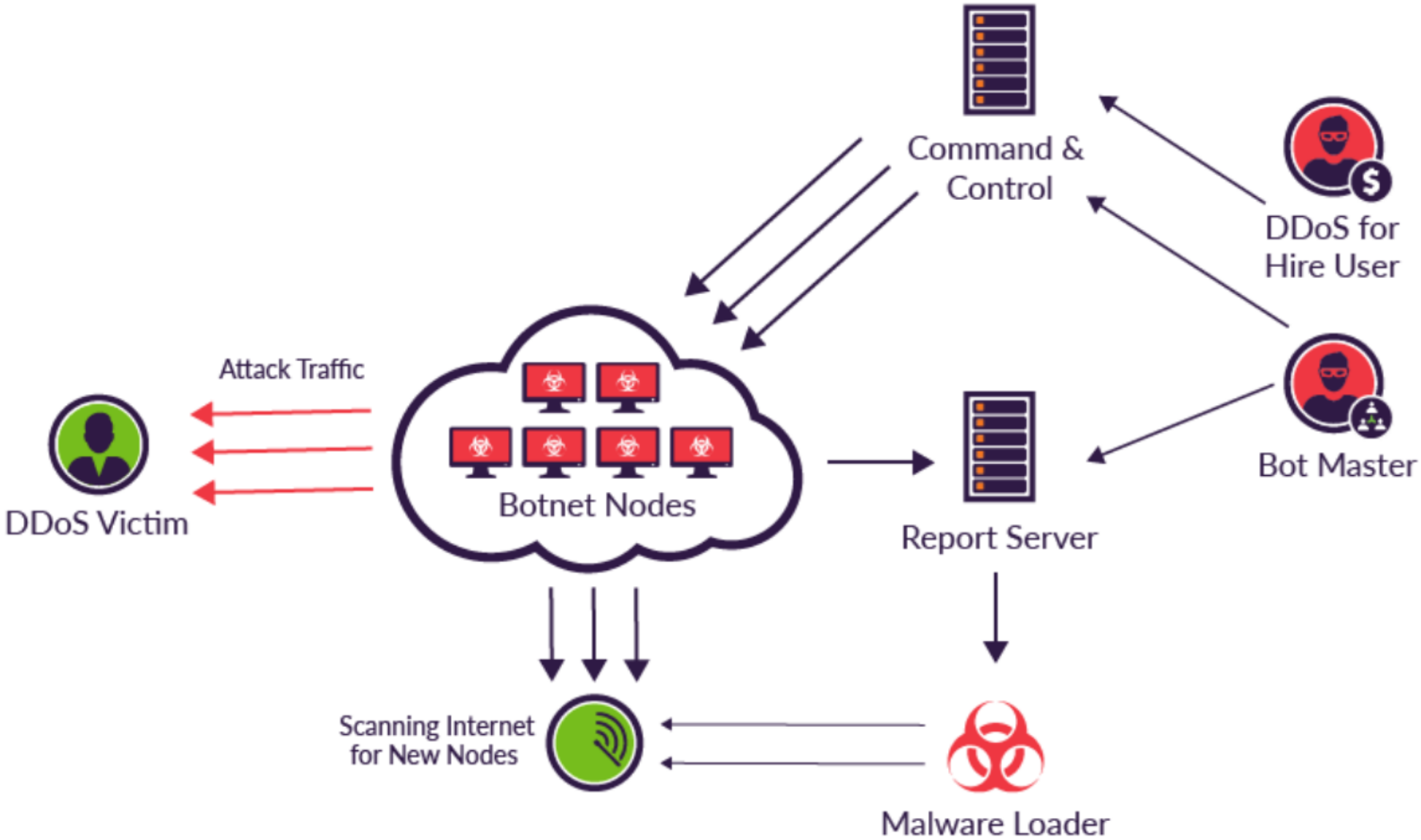

300 Gbps
250 Gbps
200 Gbps
150 Gbps
100 Gbps
50 Gbps
0 bps
17.08 20:46
20:50
20:55
21:00
21:05
21:10
21:15
21:20
21:25
21:30
21:35
21:40
21:45
21:50
21:55
22:00
22:05
22:10
22:15
22:20
22:25
22:30
22:35
22:40
22:45
22:50
22:55
23:00
23:05
23:10
17.08 23:14


Greenland
North Pacific Ocean
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Canada
Russia
Mongolia
Japan
Afghanistan
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Angola
Namibia
Tanzania
Argentina
Bolivia
New Zealand

Peki Nasıl ?

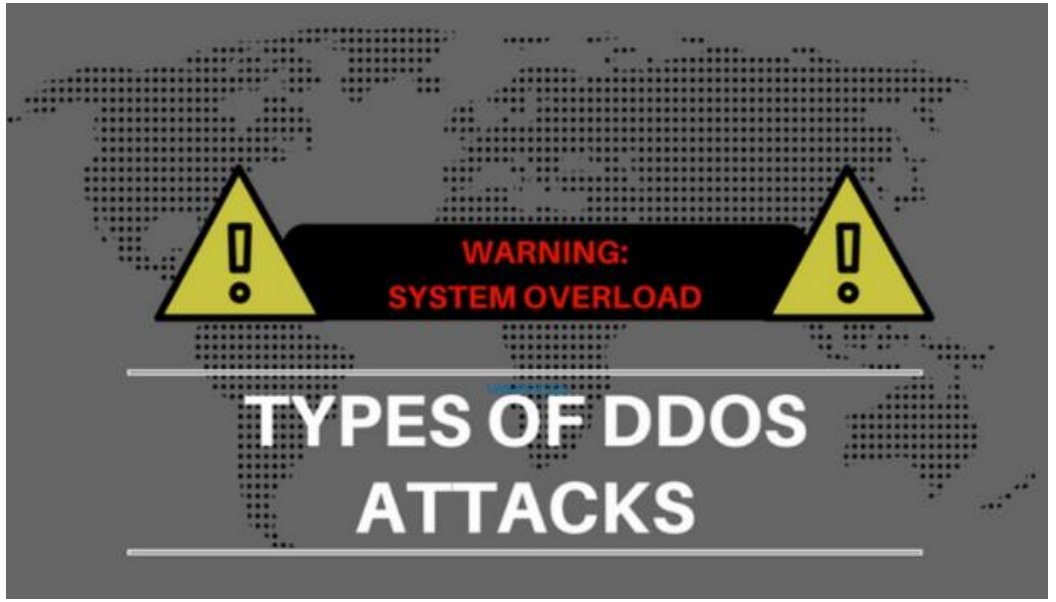
- Geniş ağ taramaları
- TELNET (port:23)
- Varsayılan kullanıcı adı ve şifre kombinasyonları
- Brute-Force (Kaba-Kuvvet) saldırıları

root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456


Command &
Control
DDoS for
Hire User
Attack Traffic
DDoS Victim
Botnet Nodes
Report Server
Bot Master
Scanning Internet
for New Nodes
Malware Loader

Potansiyel ?

- TCP
  - SYN
  - ACK
  - STOMP
- UDP
  - UDP
  - VSE
  - DNS
  - UDPPLAIN
- GRE
  - GRE-IP
  - GRE-ETHERNET
- Application
  - HTTP



```
127.0.0.0/8             - Loopback
0.0.0.0/8               - Invalid address space
3.0.0.0/8               - General Electric (GE)
15.0.0.0/7              - Hewlett-Packard (HP)
56.0.0.0/8              - US Postal Service
10.0.0.0/8              - Internal network
192.168.0.0/16          - Internal network
172.16.0.0/14           - Internal network
100.64.0.0/10           - IANA NAT reserved
169.254.0.0/16          - IANA NAT reserved
198.18.0.0/15           - IANA Special use
224.*.*.*+              - Multicast
```

```
6.0.0.0/7               - Department of Defense
11.0.0.0/8              - Department of Defense
21.0.0.0/8              - Department of Defense
22.0.0.0/8              - Department of Defense
26.0.0.0/8              - Department of Defense
28.0.0.0/7              - Department of Defense
30.0.0.0/8              - Department of Defense
33.0.0.0/8              - Department of Defense
55.0.0.0/8              - Department of Defense
214.0.0.0/7             - Department of Defense
```

```
#define TABLE_ATK_DOSARREST             45  // "server: dosarrest"
#define TABLE_ATK_CLOUDFLARE_NGINX      46  // "server: cloudflare-nginx"

if (util_stristr(generic_memes, ret, table_retrieve_val(TABLE_ATK_CLOUDFLARE_NGINX, NULL)) != -1)
                        conn->protection_type = HTTP_PROT_CLOUDFLARE;

if (util_stristr(generic_memes, ret, table_retrieve_val(TABLE_ATK_DOSARREST, NULL)) != -1)
                        conn->protection_type = HTTP_PROT_DOSARREST;
```

```
searching for .anime process
        table_unlock_val(TABLE_KILLER_ANIME);
                // If path contains ".anime" kill.
                if (util_stristr(realpath, rp_len - 1, table_retrieve_val(TABLE_KILLER_ANIME, NULL)) != -1)
                {
                    unlink(realpath);
                    kill(pid, 9);
                }
 table_lock_val(TABLE_KILLER_ANIME);
```

Referanslar

- https://heimdalsecurity.com/blog/mirai-botnet-phenomenon
- https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/
- https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

Thank you!
Any Questions?