Lecture 27: Network Security

CS 105

Spring 2023

Networking Stack

4 - Transport	Deliver (un)reliably	TCP/UDP
3 - Network	Deliver globally	IP
2 - Data Link	Deliver locally	Ethernet
1 - Physical	Deliver signals	0s and 1s

Defining security

"This tops the list of recommendations for upgrading your online security."

Functional Requirements

- **Security** = **does what it should** + nothing more
- Functional Requirements
  - e.g., As a professor, I can create a new assignment by specifying its name, number of possible points, and due date.
  - e.g., As a student, I can upload a file as a solution to an assignment.
  - e.g., As a professor, I can assign grades to student solutions.

Security Goals

- **Security** = does what it should + **nothing more**
- Functional Requirements
  - e.g., As a professor, I can create a new assignment by specifying its name, number of possible points, and due date.
  - e.g., As a student, I can upload a file as a solution to an assignment.
  - e.g., As a professor, I can assign grades to student solutions.
- Security Goals
  - e.g., "The system shall prevent students from accessing assignments that are not theirs"
  - e.g., "The system shall prevent grades from being changed by anyone but the professor"

Confidentiality
Integrity
Availability

Availability Attacks

- Goal: violate availability by making system unable to respond to requests from legitimate users

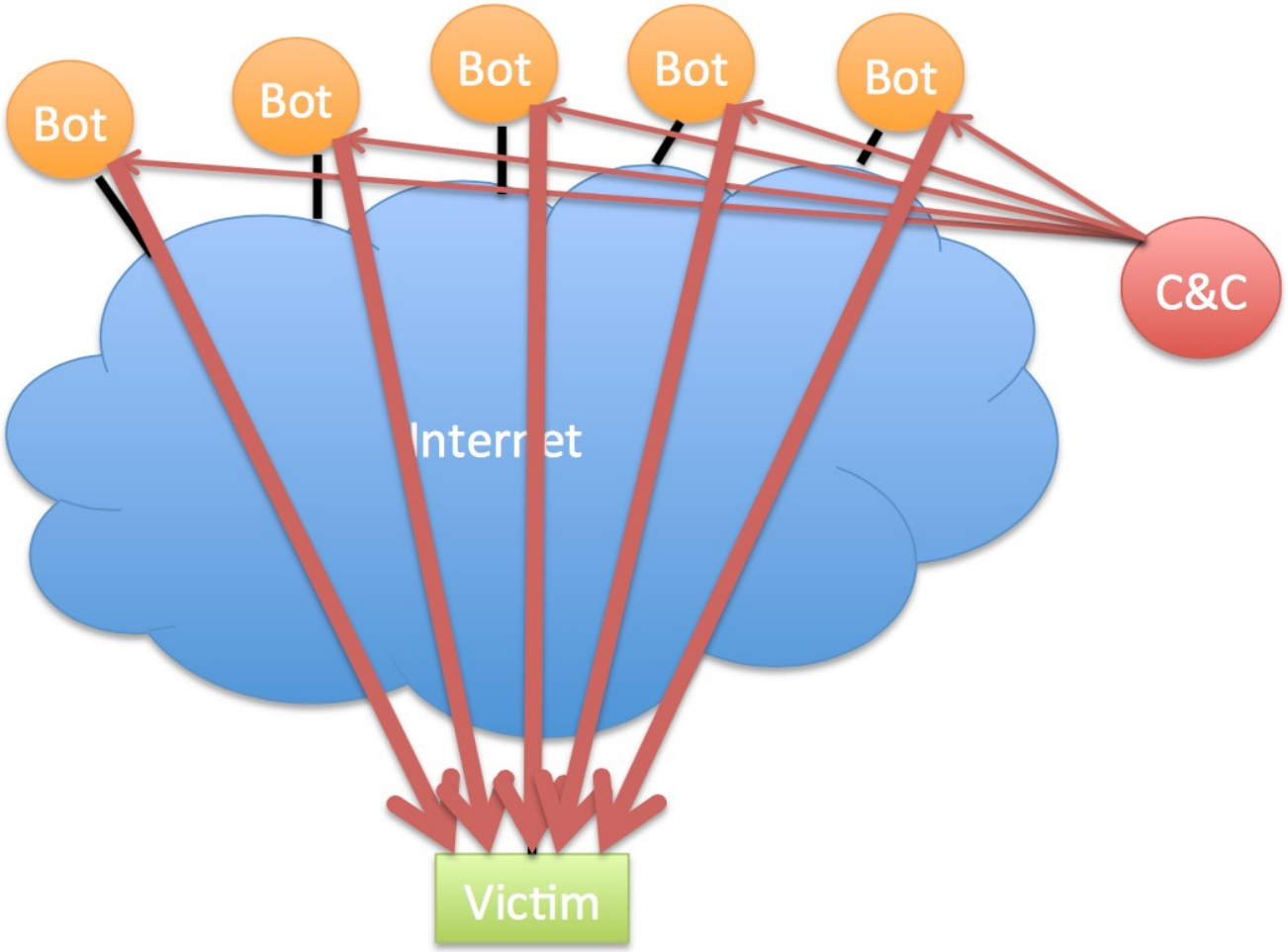
1. Resource-saturation attacks ("Denial of Service")
2. Vulnerability-based attacks

Ping

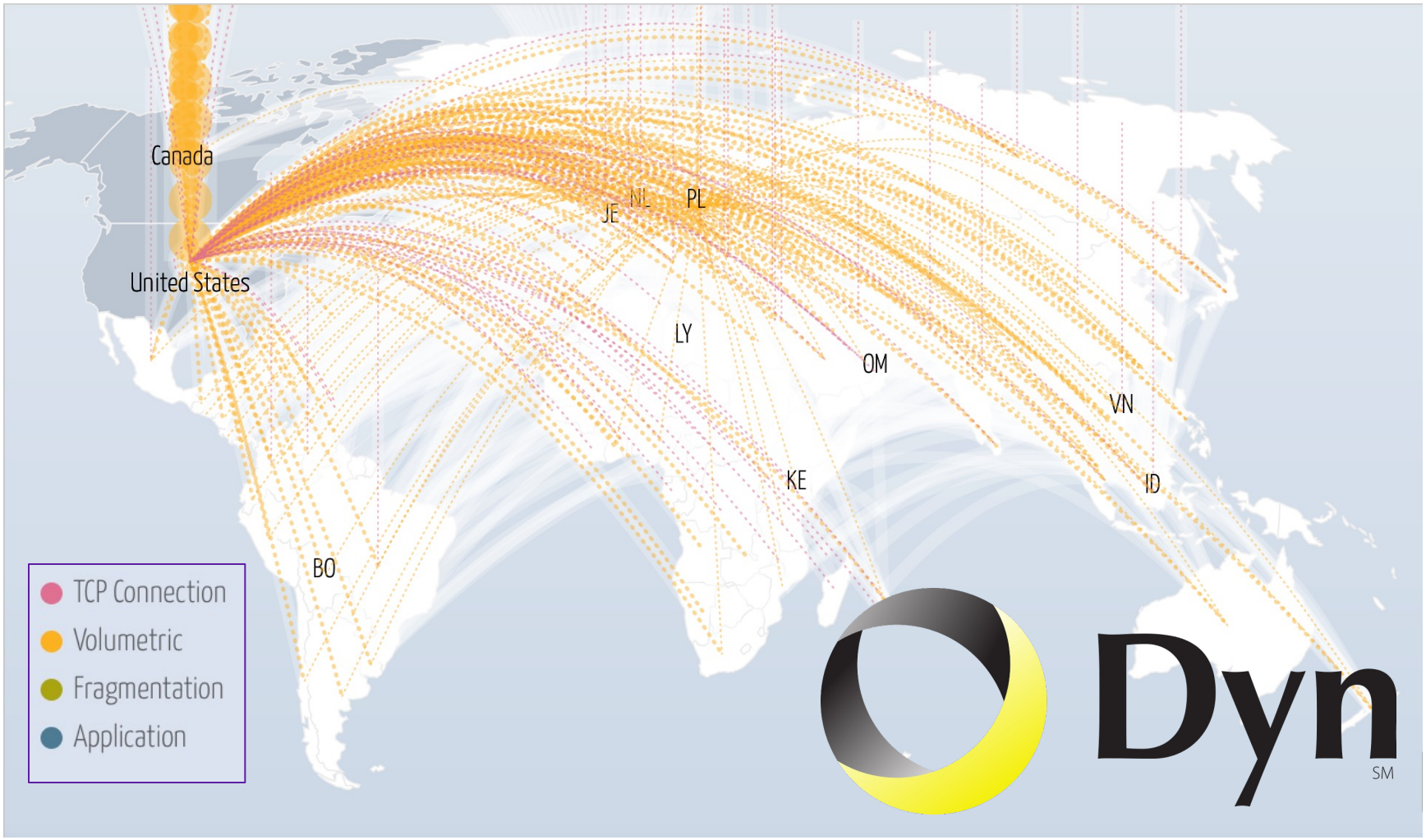
- The **Internet Control Message Protocol (ICMP)** is an network-layer support protocol used to pass operational information and error messages

- **ping:** test reachability of a host in an IP network
  - sends ICMP echo request packet to target host and waits for ICMP echo reply
  - Uses CPU, network bandwidth
- **traceroute:** display path to a host in an IP network
  - traditionally uses ping

Ping Flood

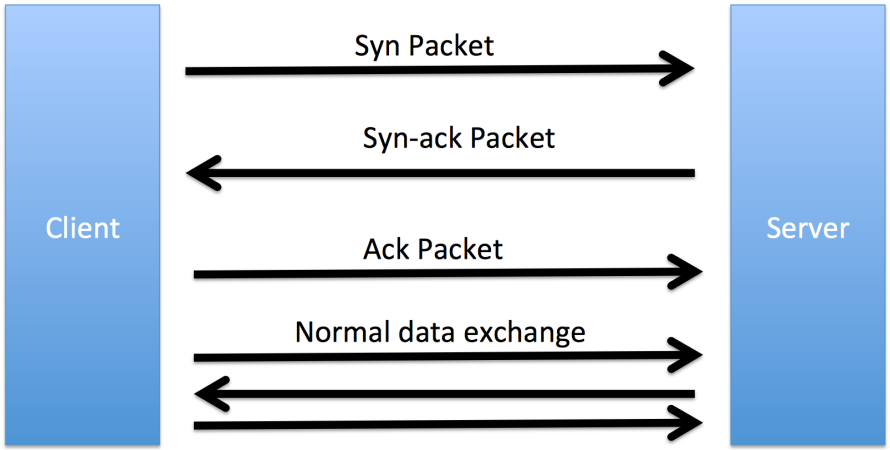


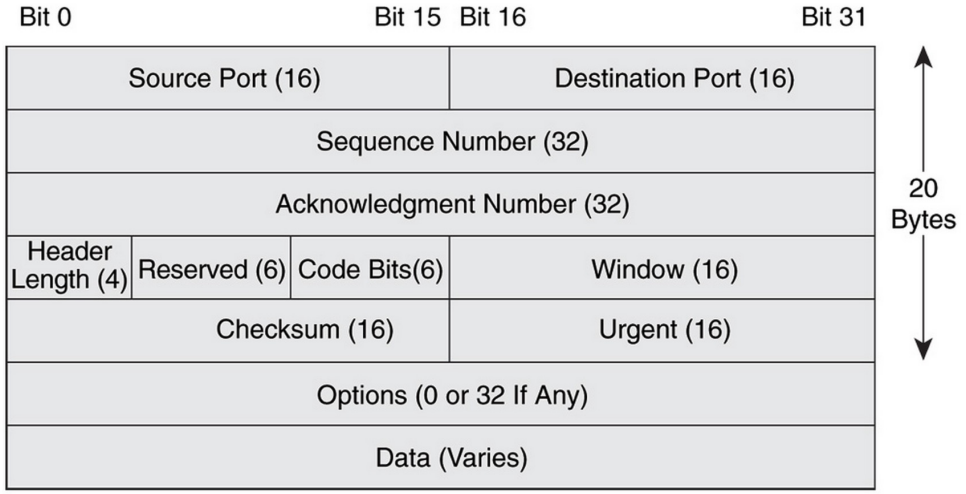
DNS Flood


Canada
United States
NL
PL
JE
LY
OM
VN
ID
KE
BO
TCP Connection
Volumetric
Fragmentation
Application
Dyn
SM

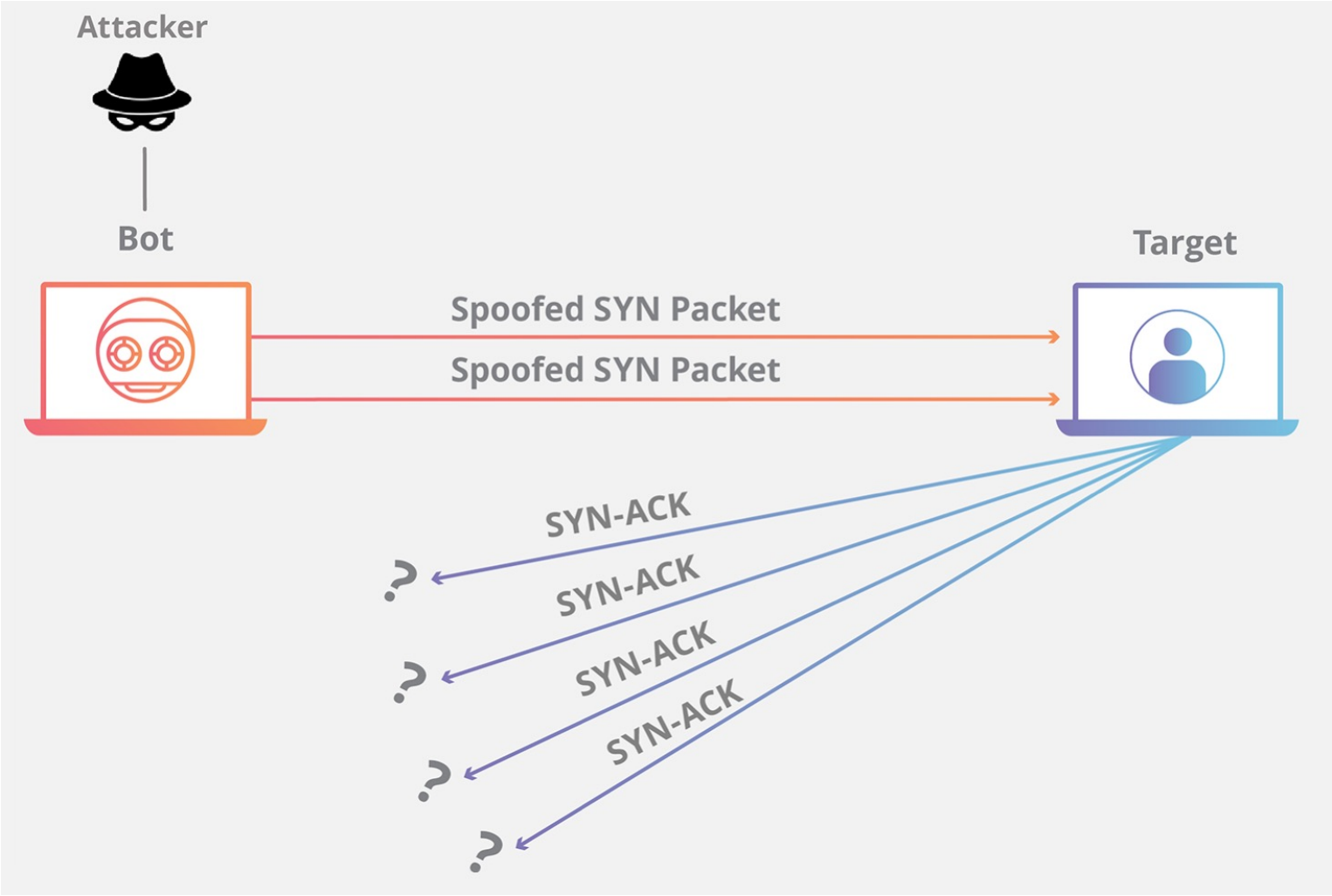
TCP

- Reliable
  - acknowledgement
  - checksum
  - sequence number
- In-order
  - sequence number
- Congestion control
  - slow start
  - congestion avoidance
  - fast retransmit
  - fast recovery





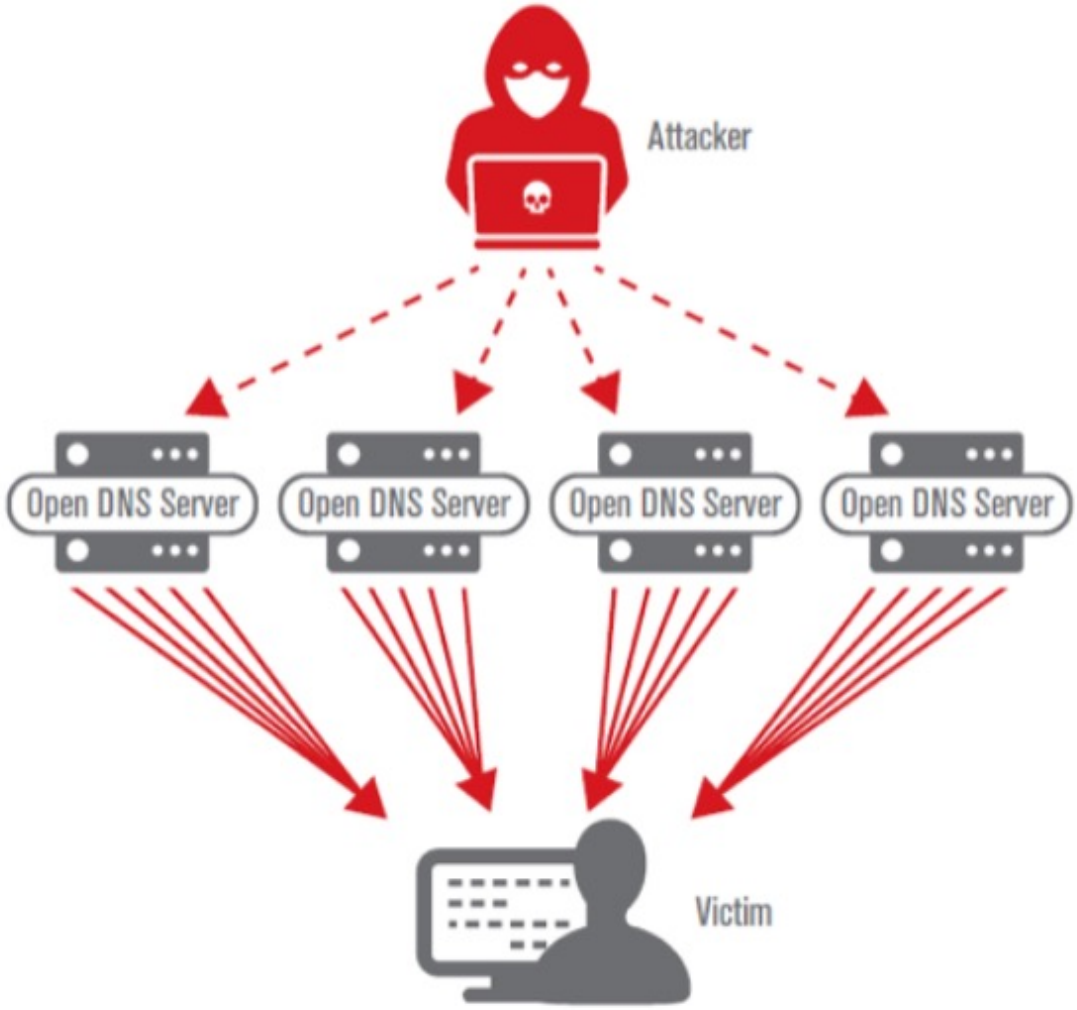
SYN Flood


Attacker
Bot
Target
Spoofed SYN Packet
Spoofed SYN Packet
SYN-ACK
SYN-ACK
SYN-ACK
SYN-ACK
?
?
?
?

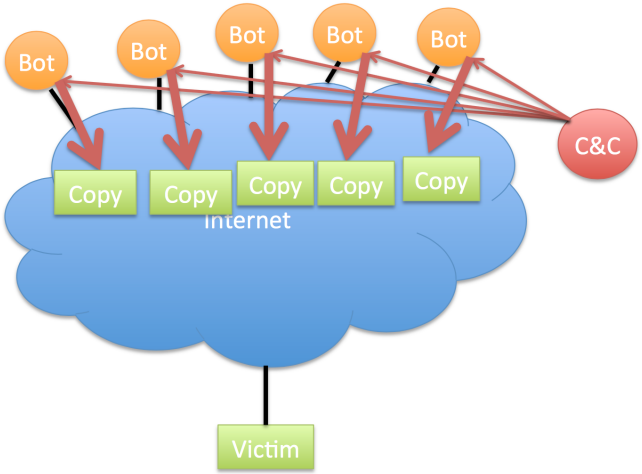
Defending Against SYN Floods

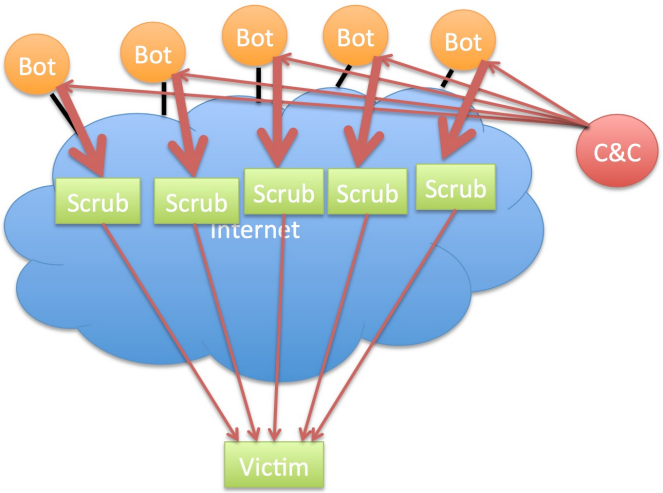
- Increase RECV queue size
- Recycle oldest half-open connections
- SYN cookies

DNS Reflection Attacks



Mitigating DoS Attacks





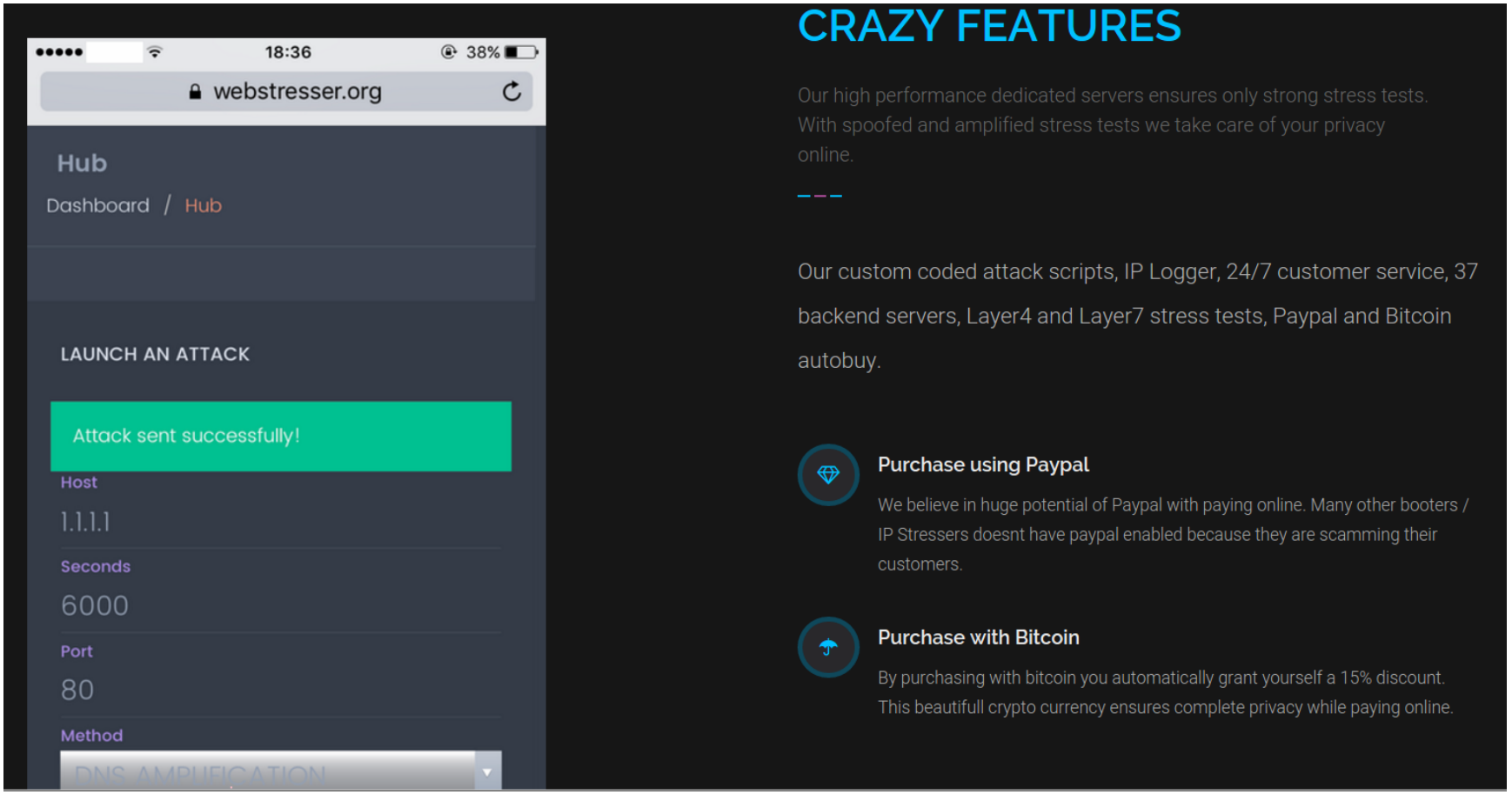
Mitigating DoS Attacks

	Gold Award	2	3	4	5	6	7	8	9	10
	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes
Web Application Firewall	✓	✓		✓			✓	✓	✓	✓
Rate Limiting	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Automatic Bot Discernment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP Blocking	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
BGP	✓	✓	✓	✓	✓	✓		✓	✓	N/A
DNS	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A
Web Proxy	✓	✓		✓	✓	✓	✓	✓	✓	N/A
Real Time Monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Deep Packet Inspection	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A

Botnets

DDoS as a Service

DDoS as a Service

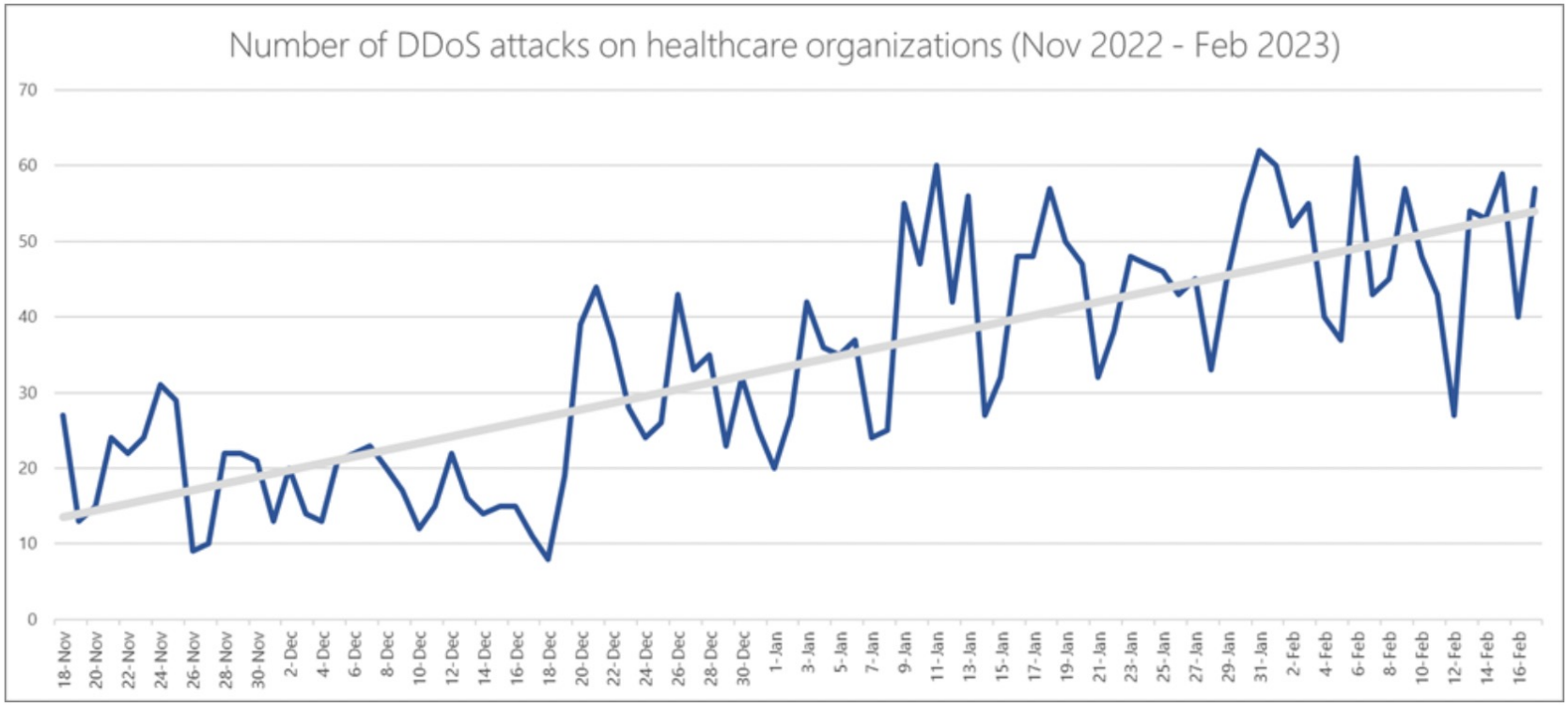


DDOS Attacks Today

- 29.3 attacks per day (2022 Q4)
- largest attack in 2022 was 1.46Tbps
- Most attacks under 30 mins, some over 24 hours

DNS	26%
TCP SYN	23%
Static Filtering	18%
UDP	14%
Invalid packets	11%
Other volumetric	2%
TCP ACK	1%
HTTP	1%
SIP	0.9%
Other	2%

Targeted Attacks

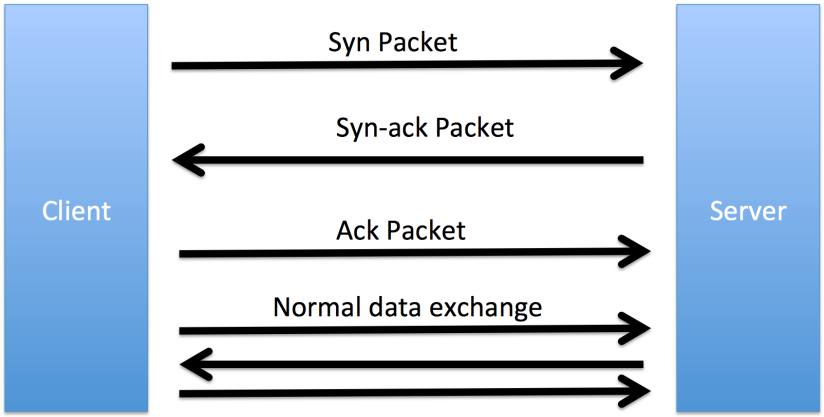


Availability Attacks

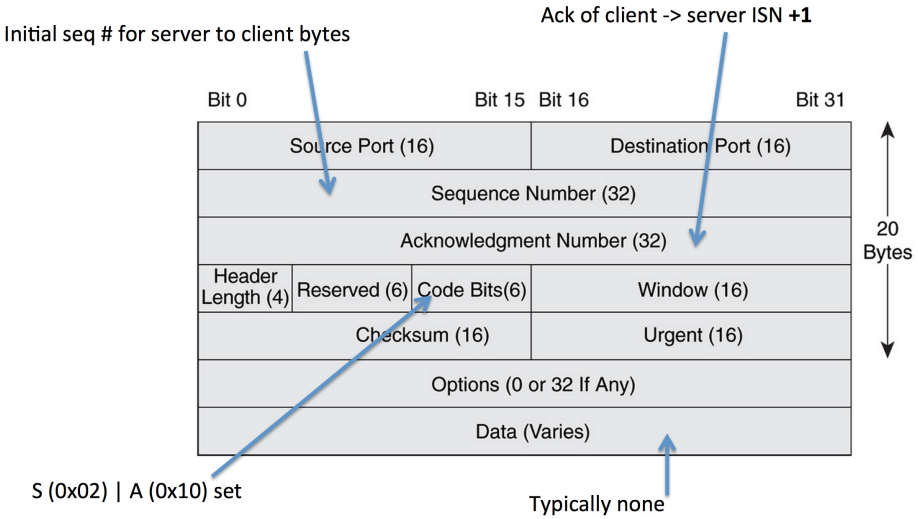
- Goal: violate availability by making system unable to respond to requests from legitimate users

1. Resource-saturation attacks ("Denial of Service")
2. Vulnerability-based attacks

Remote Requests



Port Open



Port Closed

- No machine
  - ICMP response from router
- Machine but port closed
  - TCP reset packet
- Intercepted
  - Silence (depends on config)

Port Scanning

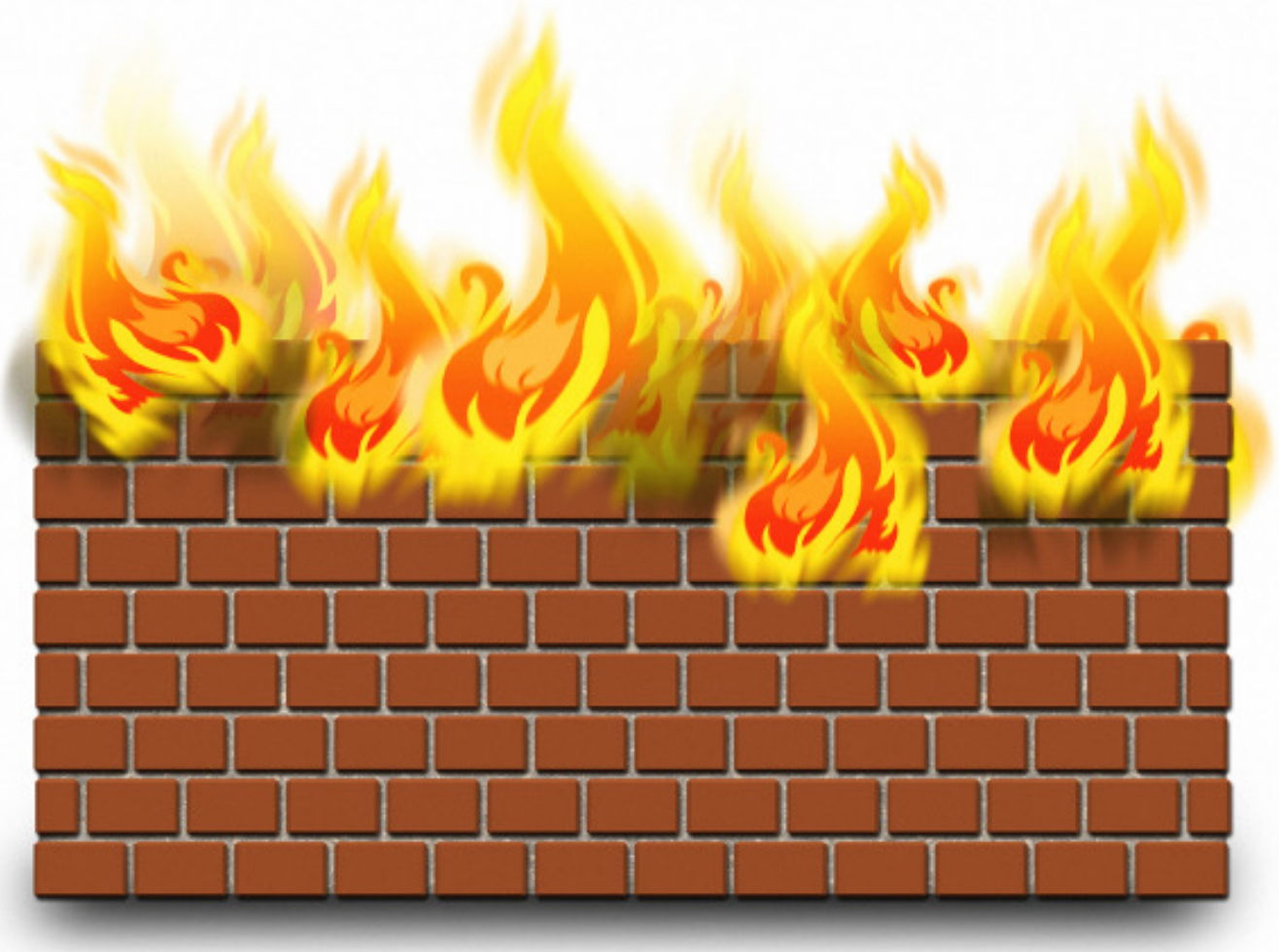
```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-18 21:43 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed ports

PORT      STATE SERVICE    VERSION
21/tcp    open  ftp
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
554/tcp   open  rtsp
7070/tcp  open  realserver
9929/tcp  open  nping-echo Nping echo
31337/tcp open  Elite

Device type: general purpose
Running (JUST GUESSING): Linux 3.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:3.13
Aggressive OS guesses: Linux 3.13 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 20.31 seconds
```

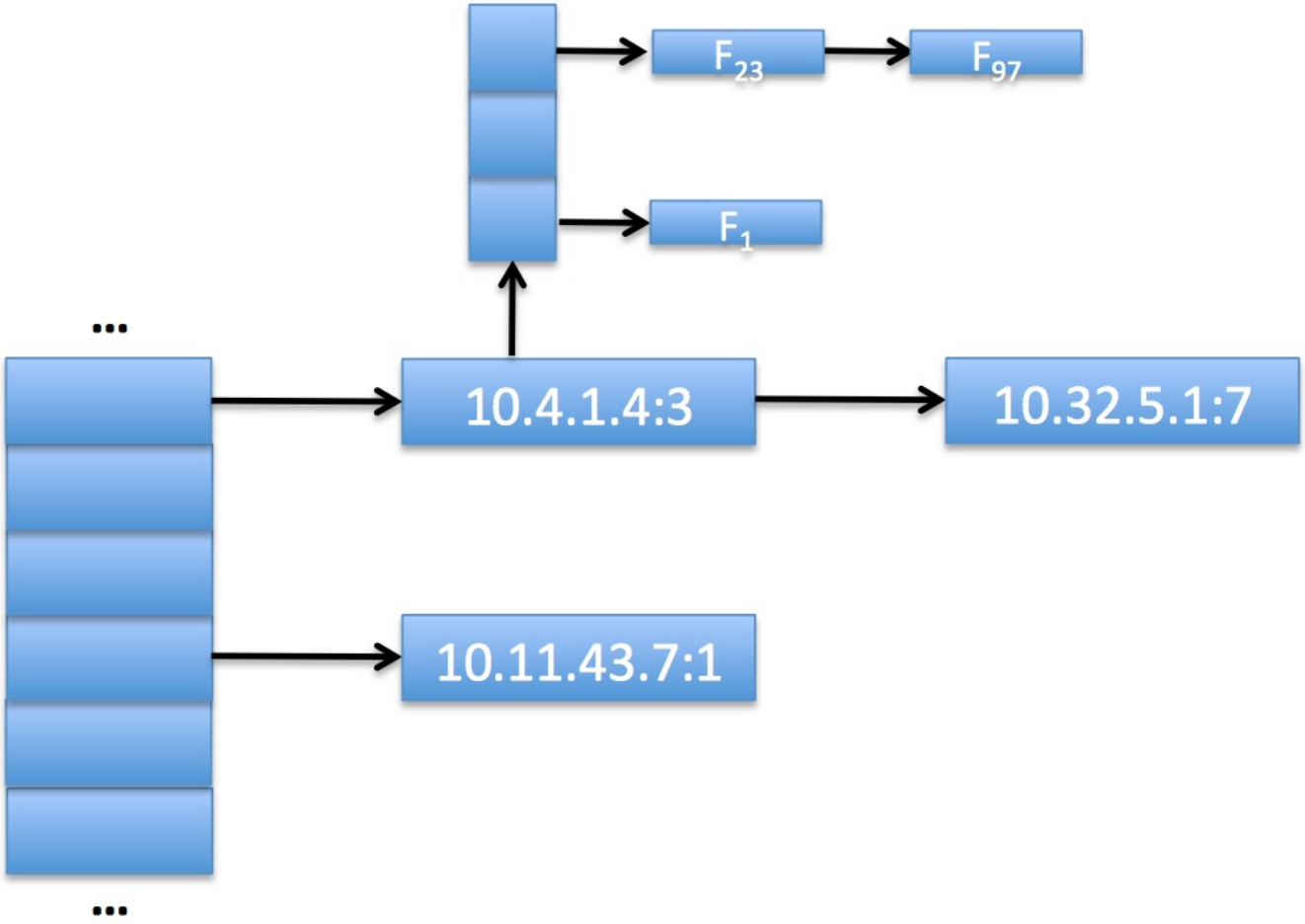
Firewalls



Packet Filtering

Protocol	Source IP	Dest. IP	Dest. Port	Action
TCP	*	192.168.1.*	25	Permit
UDP	*	192.168.1.*	69	Permit
TCP	192.168.1.*	*	80	Permit
TCP	*	192.168.1.18	80	Permit
TCP	*	192.168.1.*	*	Deny
TCP	*	192.168.1.*	*	Deny

Stateful Inspection



Deep-Packet Inspection

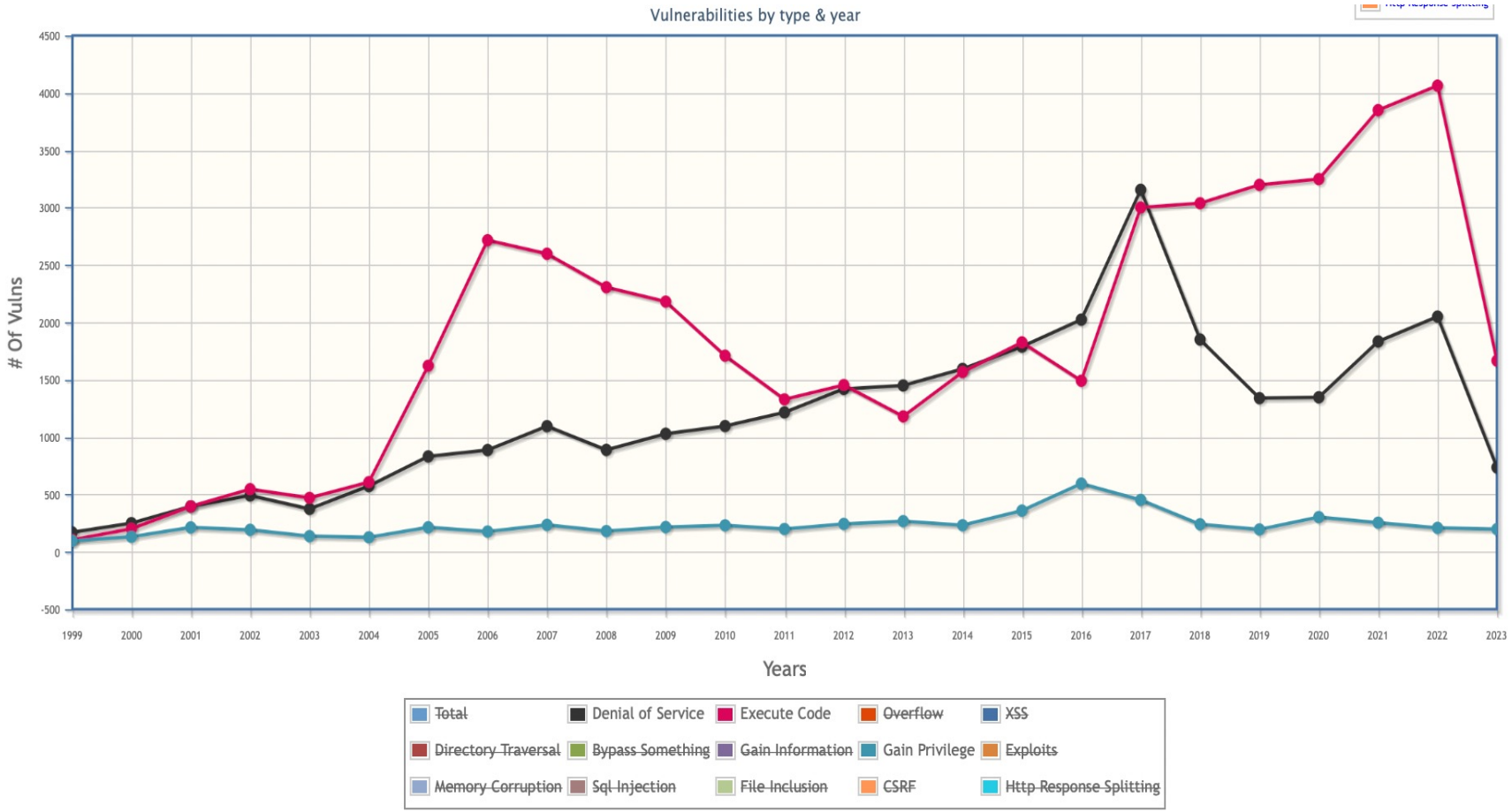

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"OS-LINUX
OS-LINUX x86 Linux overflow attempt";
flow:to_server,established; content:"1|C0 B0 02 CD 80 85
C0|uL|EB|L^|B0|"; metadata:ruleset community, service dns;
classtype:attempted-admin; sid:264; rev:13;)
```

Palo Alto Networks Launches World's First ML-Powered NGFW Making Security Intelligent and Proactive -- Defending Networks and IoT Devices Against Most Known and Unknown Threats Instantly

NEWS PROVIDED BY
Palo Alto Networks, Inc. →
Jun 17, 2020, 08:00 ET

SHARE THIS ARTICLE

Network Security



Network Security