(Distributed) Denial of Service ((D)DoS)

Part 1: Introduction and Generic Attacks

Network Security AS 2020

3 November 2020

Markus Legner
(based on slides by A. Perrig, S. Frei, T. Dübendorfer, H.-C. Hsiao)

ETH zürich

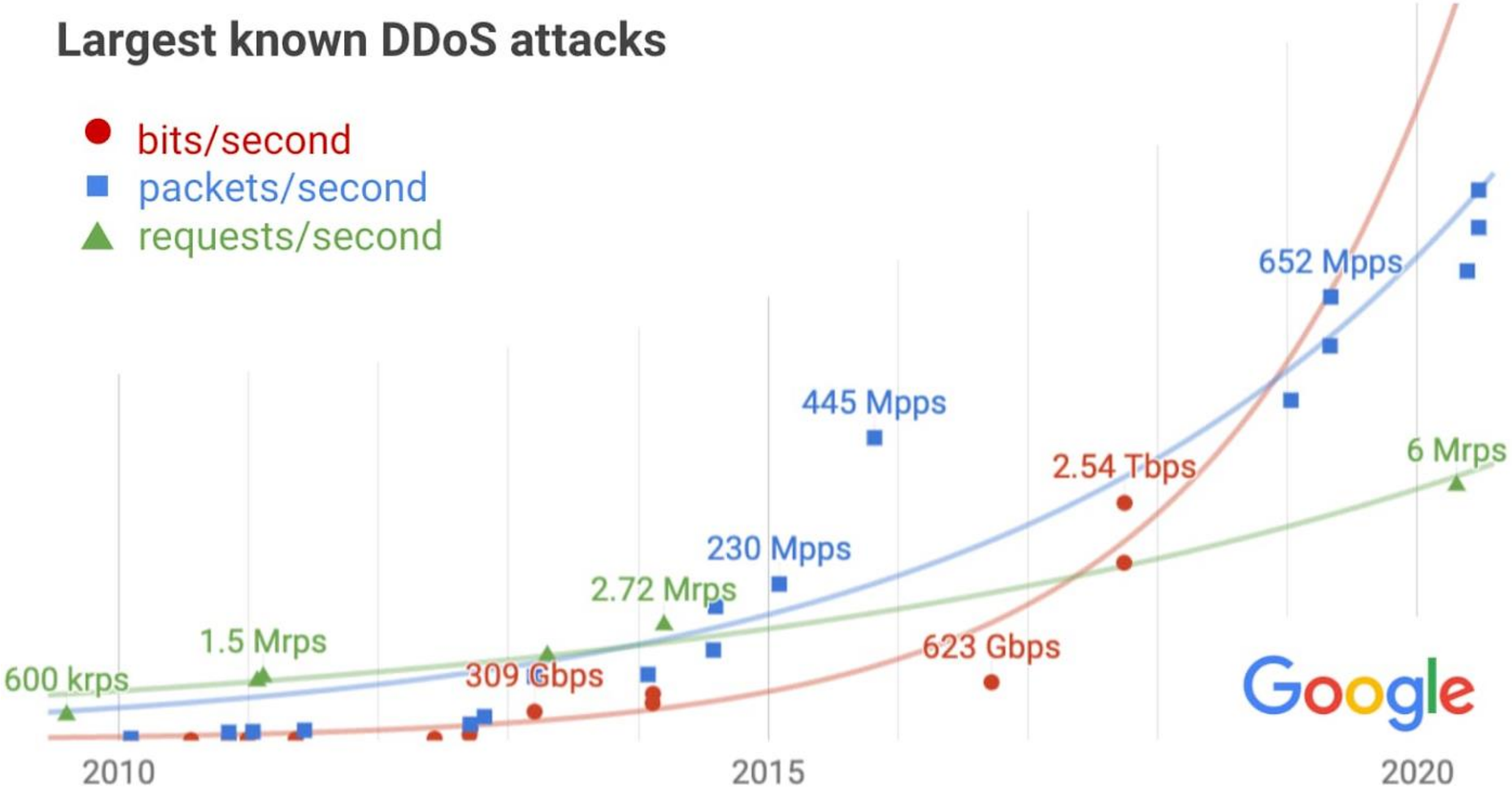
What are (distributed) denial-of-service attacks?

- Denial-of-service (DoS) attacks try to **make a service or network resource unavailable** to its intended/legitimate users.
- Typically achieved by **exhausting available resources** by sending an excessive amount of traffic/packets/requests.
- Distributed DoS (DDoS) attacks use many different sources simultaneously, often by creating and using so-called *botnets*.
- DDoS attacks are often used to extort companies: “Pay XX bitcoin and the attack will stop”

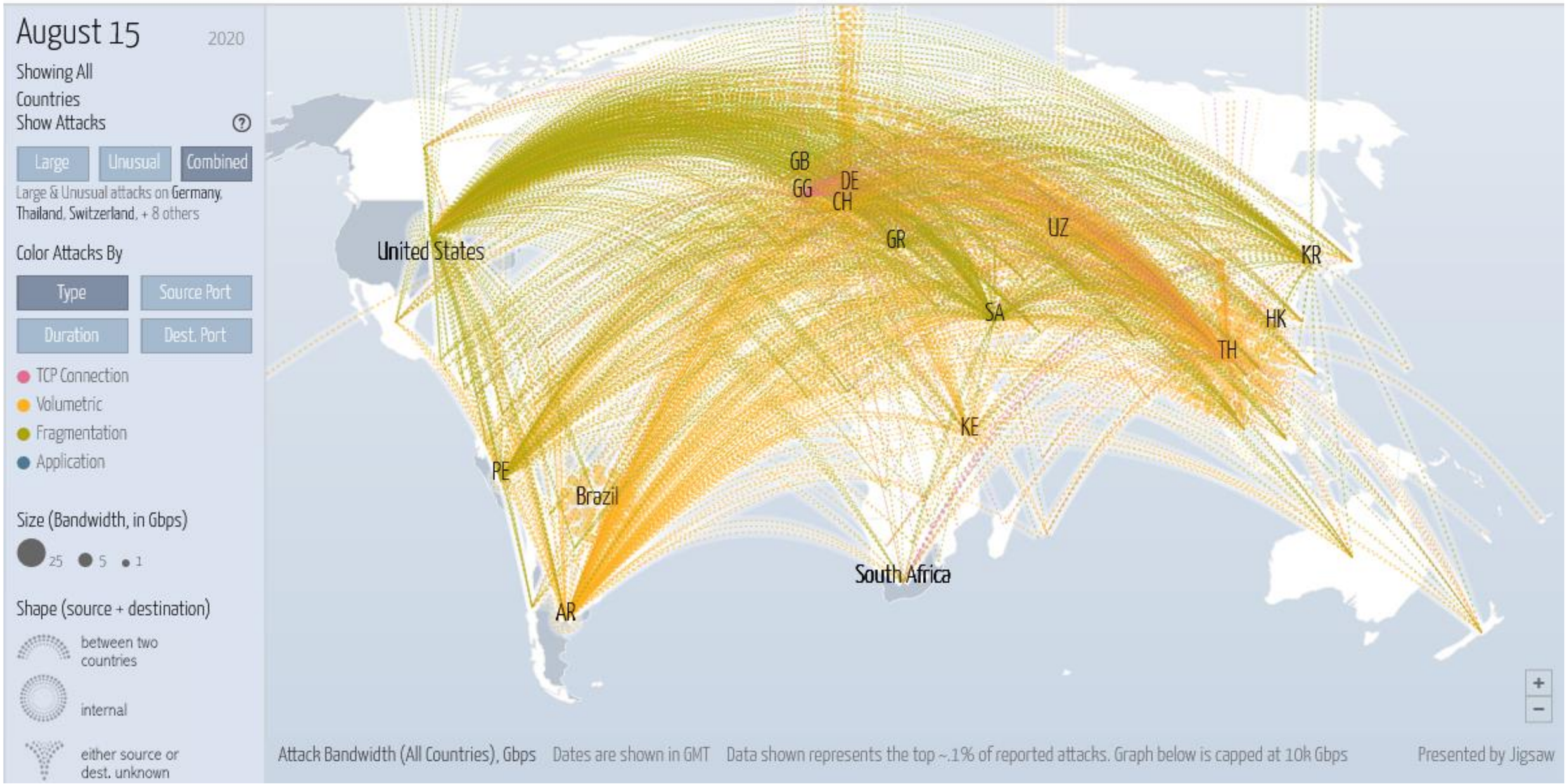
What are attack targets?

	Network links	Network devices / networking stack	Applications
Description	Volumetric attack	Protocol attack	Application-layer attack
Unit of measurement	Bits per second (bps)	Packets per second (pps)	Requests per second (rps)
Used mechanisms / examples	• Reflection and amplification • Shrew attack	• Reflection • State exhaustion • SYN/ACK floods • Fragmentation	• Computational complexity • Hash collisions • Slowloris
Defenses	• Filtering, traffic scrubbing • Black-hole filtering	• Cookies • Rate-limiting	• Randomized/keyed hash functions

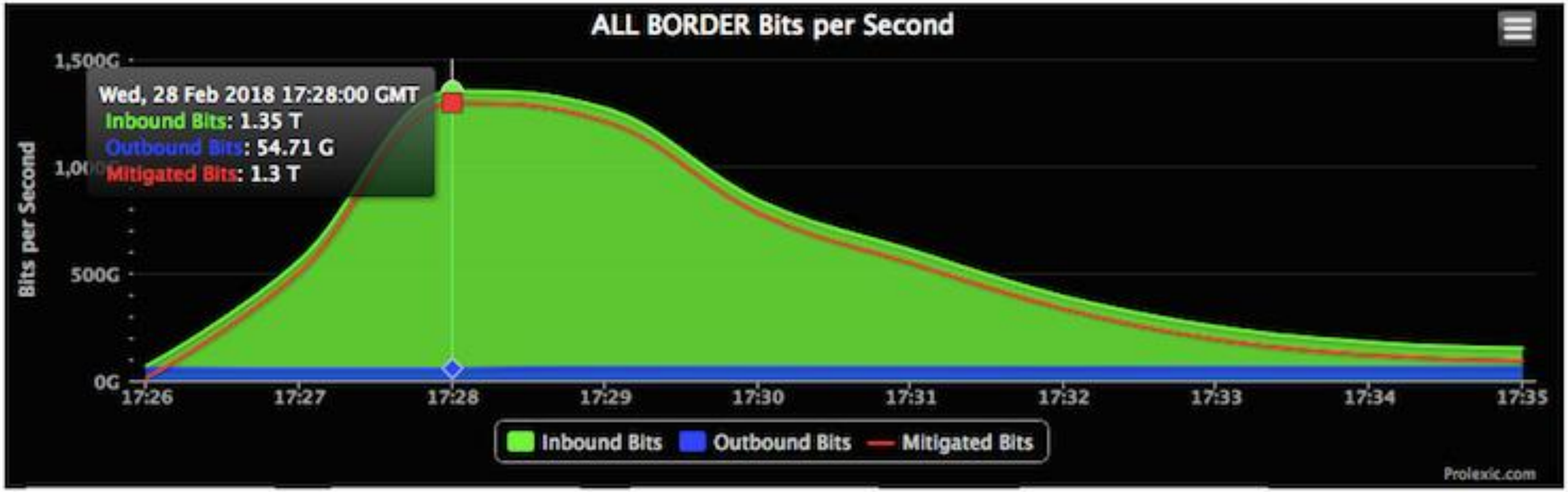
Largest known DDoS attacks



https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks

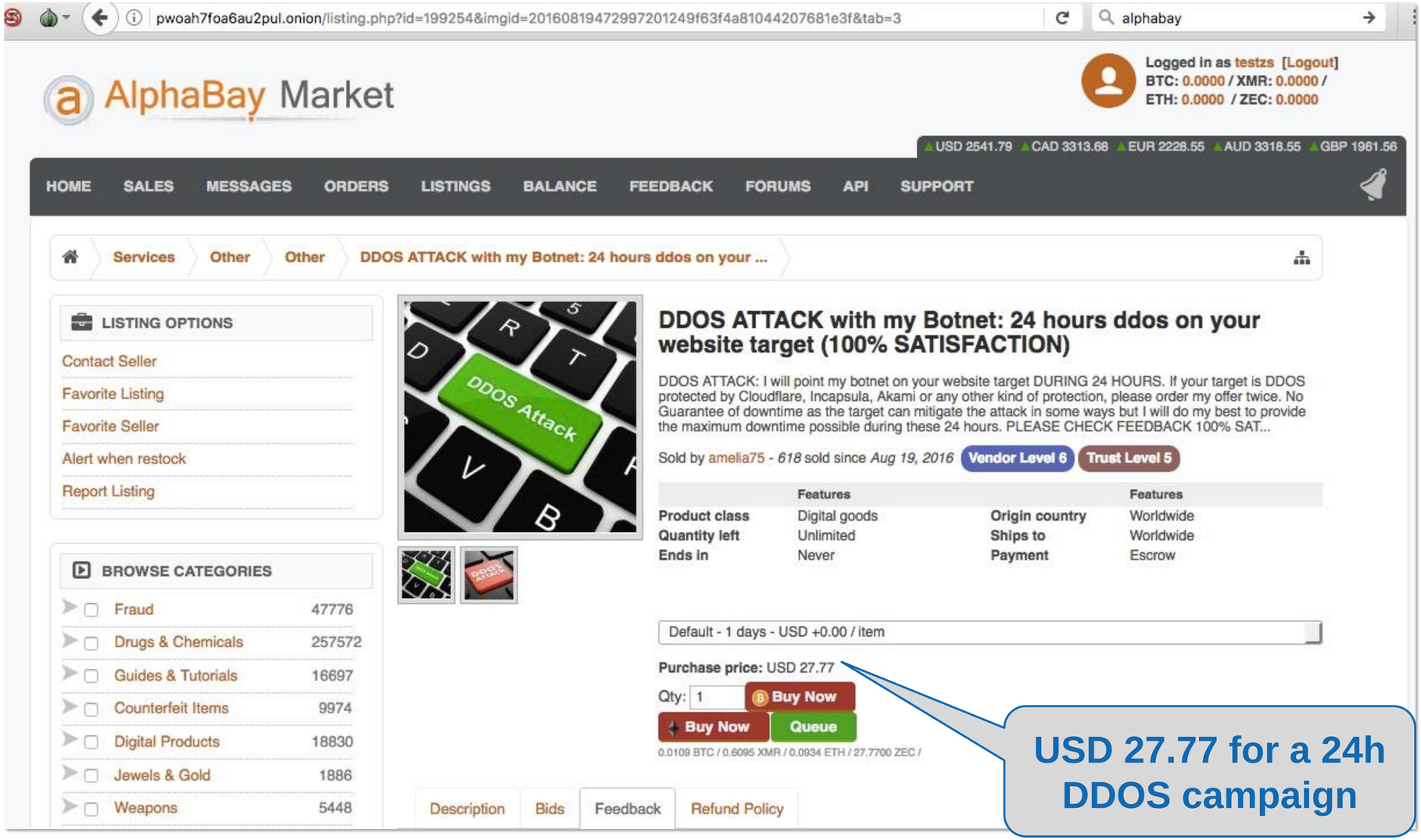

Digital Attack Map
Top daily DDoS attacks worldwide
Map · Gallery · Understanding DDoS · FAQ · About
August 15
2020
Showing All
Countries
Show Attacks
Large
Unusual
Combined
Large & Unusual attacks on Germany, Thailand, Switzerland, + 8 others
Color Attacks By
Type
Source Port
Duration
Dest. Port
TCP Connection
Volumetric
Fragmentation
Application
Size (Bandwidth, in Gbps)
25
5
1
Shape (source + destination)
between two countries
internal
either source or dest. unknown
United States
GB
GG
DE
CH
GR
UZ
KR
SA
HK
TH
KE
PE
Brazil
South Africa
AR
Attack Bandwidth (All Countries), Gbps
Dates are shown in GMT
Data shown represents the top ~1% of reported attacks. Graph below is capped at 10k Gbps
Presented by Jigsaw
https://www.digitalattackmap.com

Example Volumetric Attack: Reflection Attack on github.com, 2018



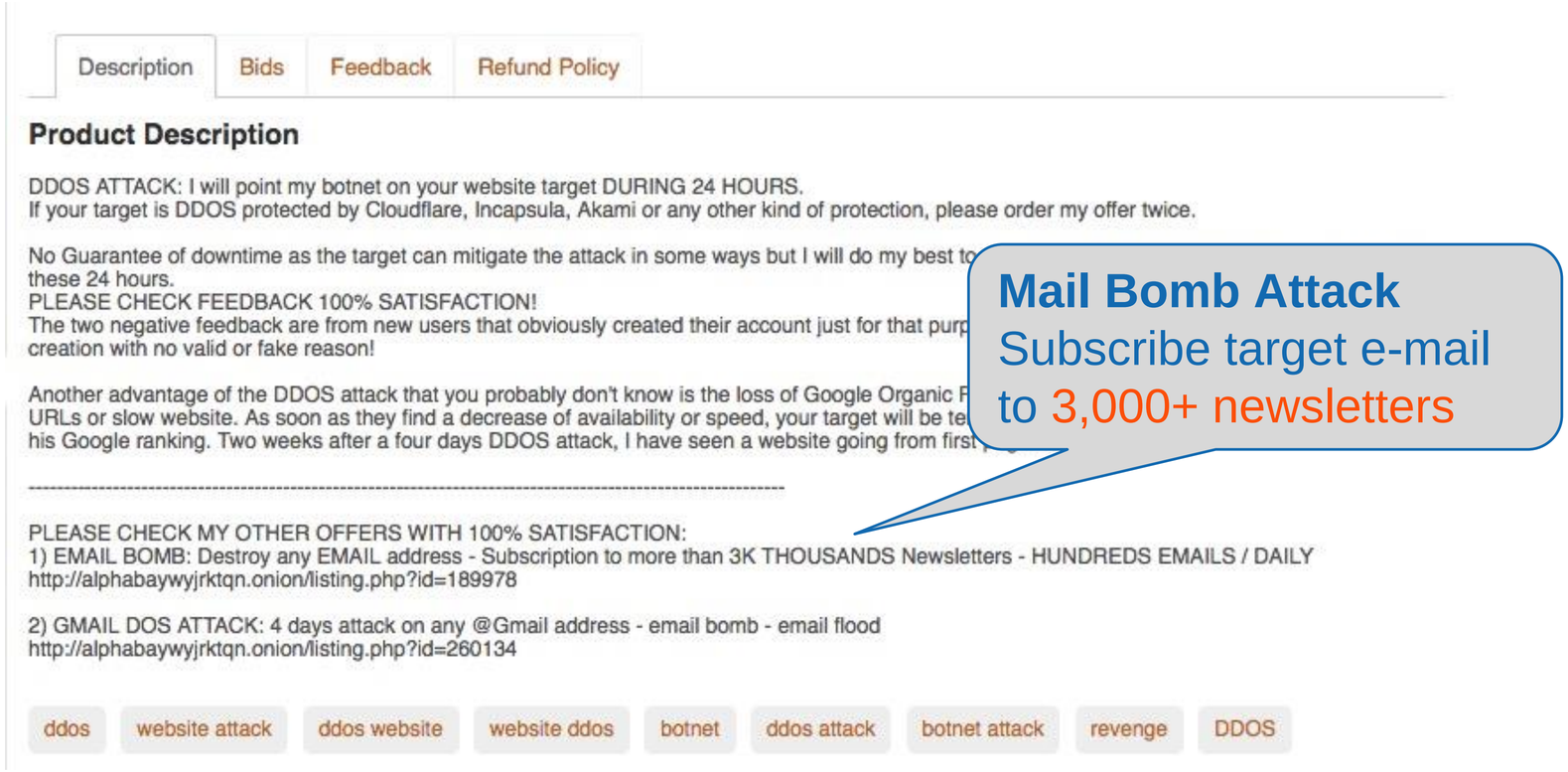
https://blogs.akamai.com/2018/02/memcached-udp-reflection-attacks.html

DDoS Offers in the Darknet



AlphaBay: Tor hidden service until 2017 (accessed 2017-06-29)

DDoS Offers in the Darknet



Description | Bids | Feedback | Refund Policy

Product Description

DDOS ATTACK: I will point my botnet on your website target DURING 24 HOURS.
If your target is DDOS protected by Cloudflare, Incapsula, Akami or any other kind of protection, please order my offer twice.

No Guarantee of downtime as the target can mitigate the attack in some ways but I will do my best to
these 24 hours.
PLEASE CHECK FEEDBACK 100% SATISFACTION!
The two negative feedback are from new users that obviously created their account just for that purp
creation with no valid or fake reason!

Another advantage of the DDOS attack that you probably don't know is the loss of Google Organic F
URLs or slow website. As soon as they find a decrease of availability or speed, your target will be te
his Google ranking. Two weeks after a four days DDOS attack, I have seen a website going from first

---

PLEASE CHECK MY OTHER OFFERS WITH 100% SATISFACTION:
1) EMAIL BOMB: Destroy any EMAIL address - Subscription to more than 3K THOUSANDS Newsletters - HUNDREDS EMAILS / DAILY
http://alphabaywyjrktqn.onion/listing.php?id=189978

2) GMAIL DOS ATTACK: 4 days attack on any @Gmail address - email bomb - email flood
http://alphabaywyjrktqn.onion/listing.php?id=260134

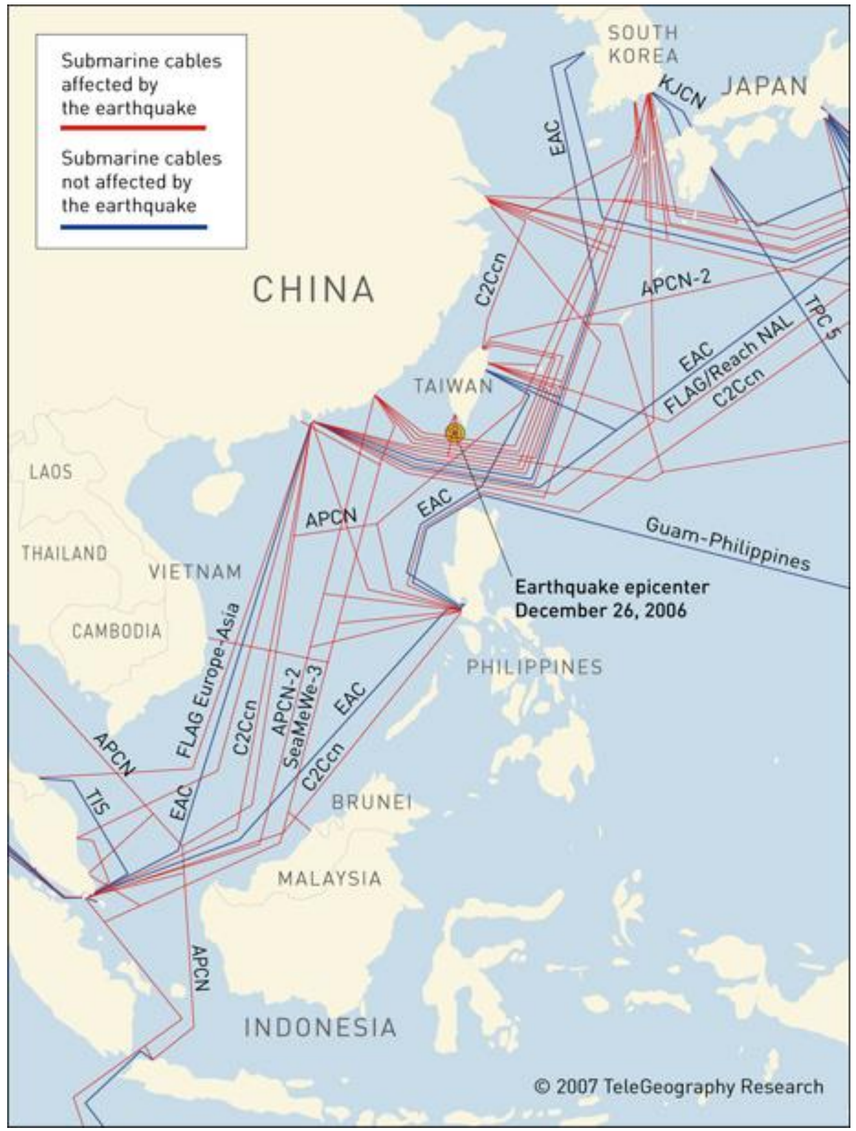
ddos | website attack | ddos website | website ddos | botnet | ddos attack | botnet attack | revenge | DDOS

Mail Bomb Attack
Subscribe target e-mail
to 3,000+ newsletters

AlphaBay: Tor hidden service until 2017 (accessed 2017-06-29)

Not every outage is a DDoS attack...

- 2006 Earthquake
  - Impaired seven out of nine geographically co-located cables in the Luzon Strait
  - A six-hour outage for more than two thousand IP prefixes
- Demonstrates vulnerability of current Internet infrastructure



General DoS Attack Techniques

What features facilitate DoS attacks?

- Attacker **controls significantly more** resources than victim.
- Attacker needs to **expend significantly less** resources than victim.
- Attacker can **hide his identity** or continually change it.
- Victim needs to **expend a significant amount of resources** before being able to assess the legitimacy of requests.
- Attacker can **instruct/trick other entities to send traffic** on her behalf.

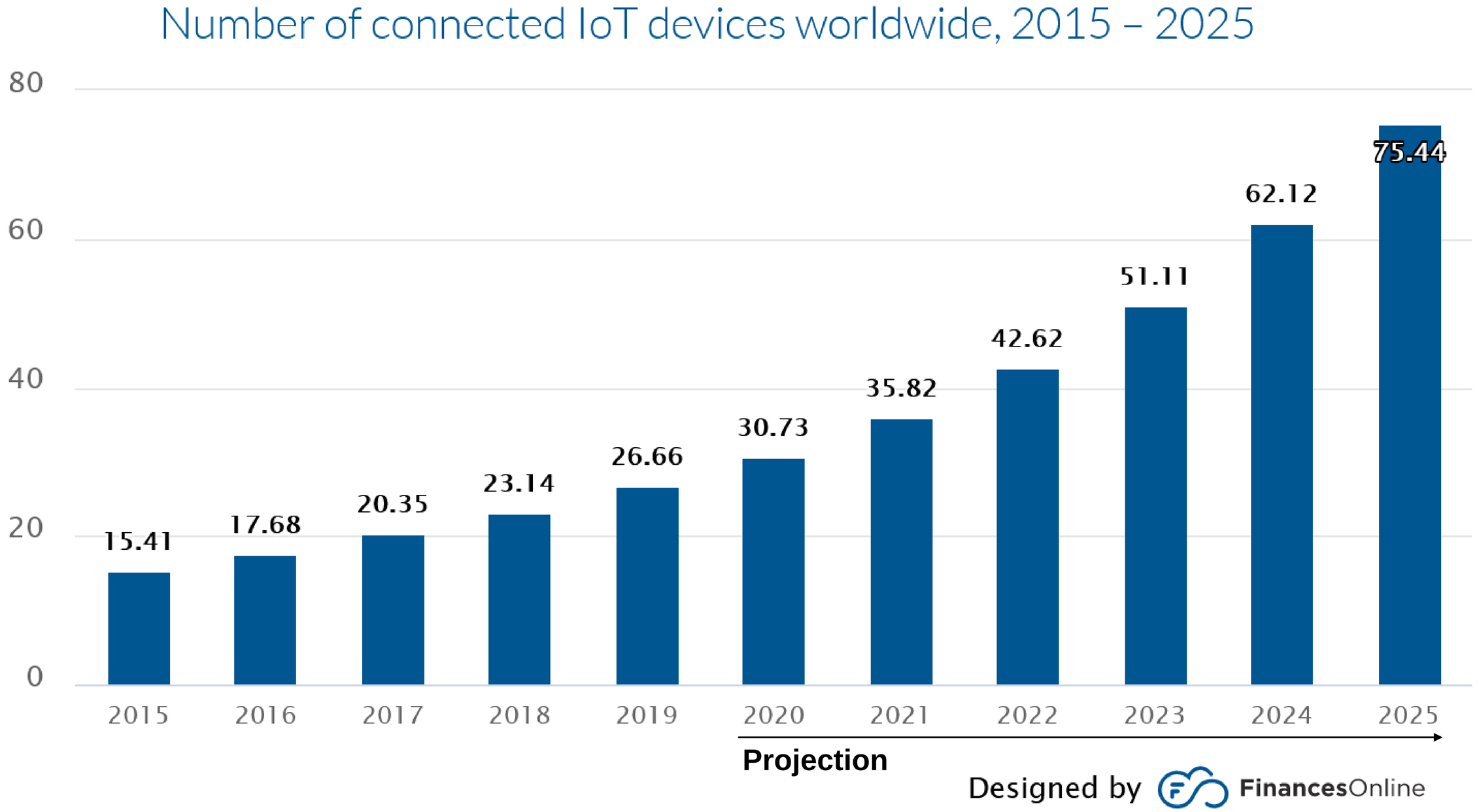
(IoT) Botnets

What is a botnet?

- A (large) set of compromised machines connected to the Internet
- Execute malicious code and can be controlled via command and control (C&C) systems
- Often geographically distributed

Internet of Things (IoT) devices are perfect for constructing botnets…

- Many devices with uniform configuration
- Often very poorly secured, e.g., hardcoded credentials
  - Enables automatic scanning
- Often no security updates after few years
  - In particular when manufacturer goes out of business
- Often connected to the Internet without bandwidth limitations
- Example: Mirai botnet
  - Mostly consists of vulnerable webcams



https://financesonline.com/number-of-internet-of-things-connected-devices/

Possible Mitigations

Patch

- Manufacturers should provide **automatic security updates**
- Provide **patches for the full lifetime** of devices

Credentials

- **No hardcoded credentials**
- Force users to **change default passwords**

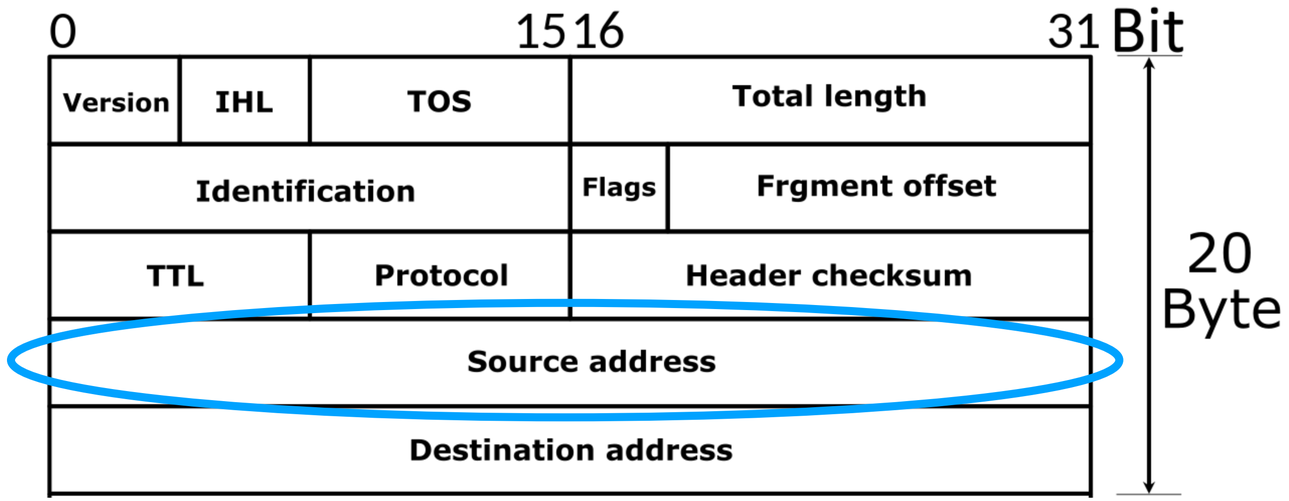
Monitoring

- ISPs should actively **monitor their network** for suspicious traffic

Reflection and Amplification

Address Spoofing

- Source address in IP header can be set by sender
- In a connectionless protocol (UDP), server cannot confirm actual sender



Defenses against address spoofing

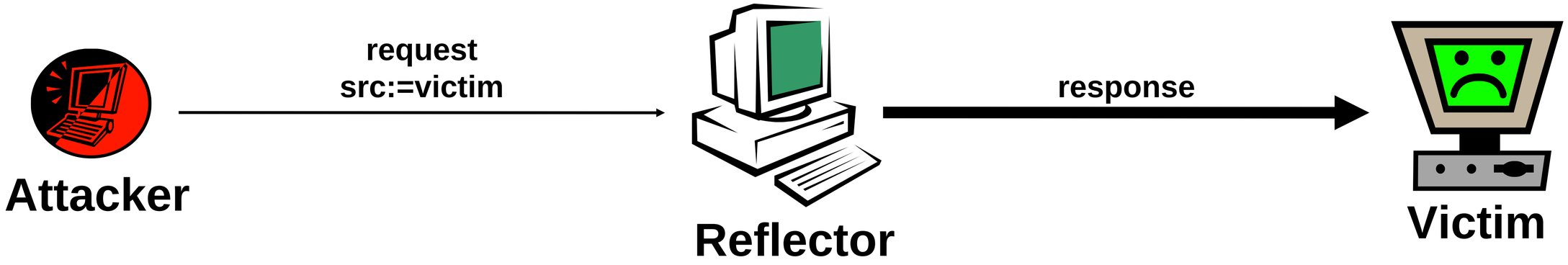
- Address filtering by ISPs: ensure that hosts use their own addresses
  - Needs to be globally deployed
  - Poor incentives for ISPs to deploy it (only other ISPs profit)
- Use connection-based protocols (e.g., TCP)
  - Additional latency
  - Potentially additional DoS attack vector (state exhaustion)
- Cryptographic source authentication
  - Additional DoS attack vector if built on (expensive) asymmetric cryptography
  - Requires symmetric key distribution or PKIs

Reflection and Amplification

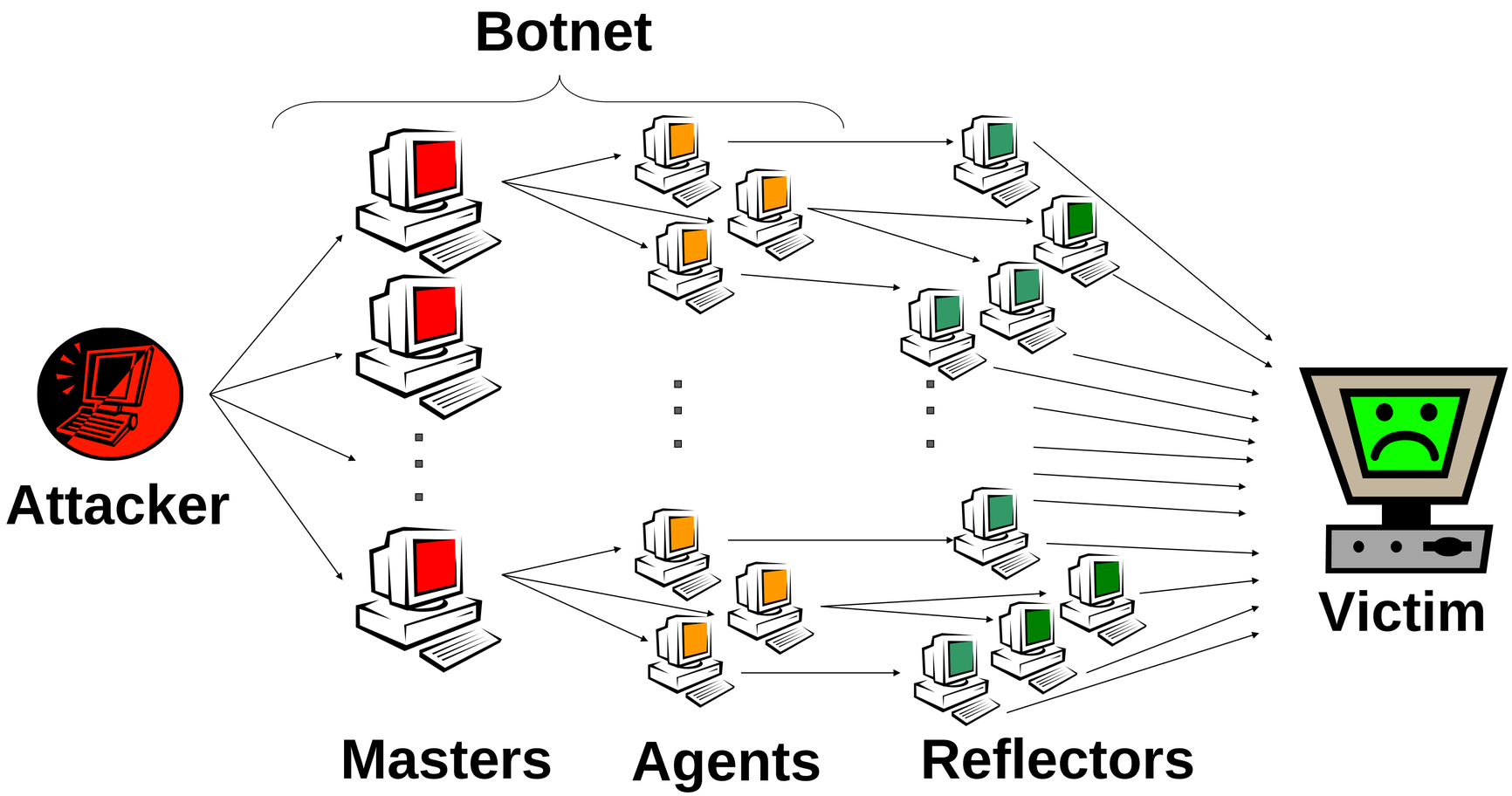
- Requirements:
  - Ability to spoof source address
  - Publicly accessible servers
  - Ideally: response is (much) larger than request → amplification
    - Either number of packets or size of packets increased
- Typical reflectors (and maximal amplification factors):
  - DNS (up to ~180)
  - NTP (up to ~500); vulnerability was closed in version 4.2.7p26
  - Memcached (up to ~50 000); UDP disabled by default in version 1.5.6

How reflection and amplification works

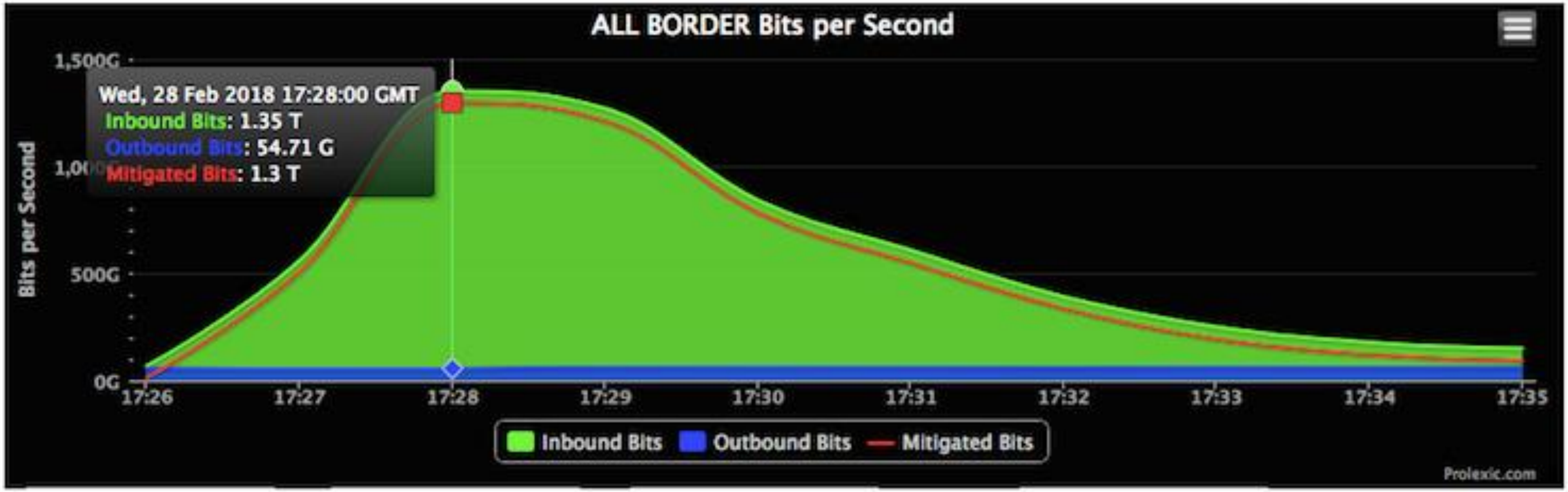
1. Choose open service (e.g., open DNS resolver) as reflector
2. Craft request that triggers (much) larger response
3. Send packet where source address is set to victim's address
4. Reflector sends reply to victim



Distributed DoS with Reflectors



2018 attack on github.com used vulnerable Memcached servers



https://blogs.akamai.com/2018/02/memcached-udp-reflection-attacks.html

Mitigations

- Prevent address spoofing (see before)
- Perform access control
  - For example, DNS servers deployed within an organization or ISP should only server clients from this organization
- Implement response rate limiting (RRL)
  - Limit the number of responses to a client IP
- Ensure small amplification factors (ideally < 1)
  - Example: WireGuard ensures that the responder's first message is *smaller* than the initiator's

Summary

Summary of (D)DoS attacks

- Goal of DoS attack: prevent legitimate users from accessing/using a service/resource
- Numerous attack possibilities:
  - volumetric attacks (network congestion)
  - protocol-level attacks
  - application-level attacks
- Typical approaches:
  - Reflection and amplification
  - Botnets