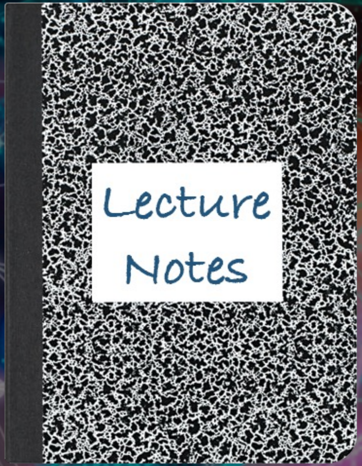


CS 419: Computer Security

Week 11: Network Attacks

DDoS: Amplification Attacks

Paul Krzyzanowski

Denial of Service (DoS) Attacks

Denial of service attack

Disable a service so it cannot do its work

How can we do this?

1. **Exploit vulnerabilities: Get the system or service to crash**
   - Exploit vulnerabilities to get a program or system to crash
   - This is ideal but usually not feasible
2. **Flood a service with requests**
   - Legitimate requests cannot be processed
3. **Flood the network with traffic**
   - The gateway router (or system or ISP) will be overwhelmed with traffic that legitimate requests cannot get through

Forms of overwhelming a system for DoS

- **Volumetric attack**

  Generate more traffic than the target's network link(s) can handle

- **Packet-per-second (PPS) attack**
  Requests-per-second (RPS) attack

  Generate a higher packet or request rate than an application (or OS or routers) can process

Attack Techniques

Challenge: ***How do we overwhelm targets bigger than us?***

Some techniques

- **Find asymmetries**
  - Cases where processing requests is more expensive than issuing them
- **Avoid getting responses**
  - Spoof return addresses so you don't have to deal with feedback
- **Use indirection**
  - Send requests with spoofed return addresses so the responses go to the victim
- **Join forces**
  - Get lots of systems to attack at the same time

Bugs & Asymmetric attacks

- **Challenge Collapser**
  - Attacker sends URLs that require time-consuming operations on the server
  - For example, complex database queries, searches, generative AI operations
- **ICMP attacks**
  - Ping flood
    - Send ICMP Echo Request messages with responses that go to the target
  - Ping of Death
    - Send fragmented IP packets so that they will be >64KB when reassembled ⇒ buffer overflow
    - This was the classic easy DoS attack – but the bug has been fixed on all IP stacks
  - Send spoofed source addresses to unreachable destinations
    - Routers will return *Destination Unreachable* to the target

Application-Layer Loop DoS

- **Spoof UDP packets to cause a pair of systems to communicate indefinitely**
  - Affects DNS, DTP, TFTP, and other protocols
  - First documented in March 2024
- **A trigger message with a spoofed source IP address is sent to one target**
  - It responds to the service in the spoofed source IP address, which creates and endless sequence of back-and-forth responses
  - For example: send a spoofed error message to a TFTP server, that will respond back with an error to another TFTP server, which will respond back, …
- **Puts 300,000+ systems at risk**

See: https://cispa.de/en/loop-dos

Amplification Attacks

Goal: send a small request that produces a large response

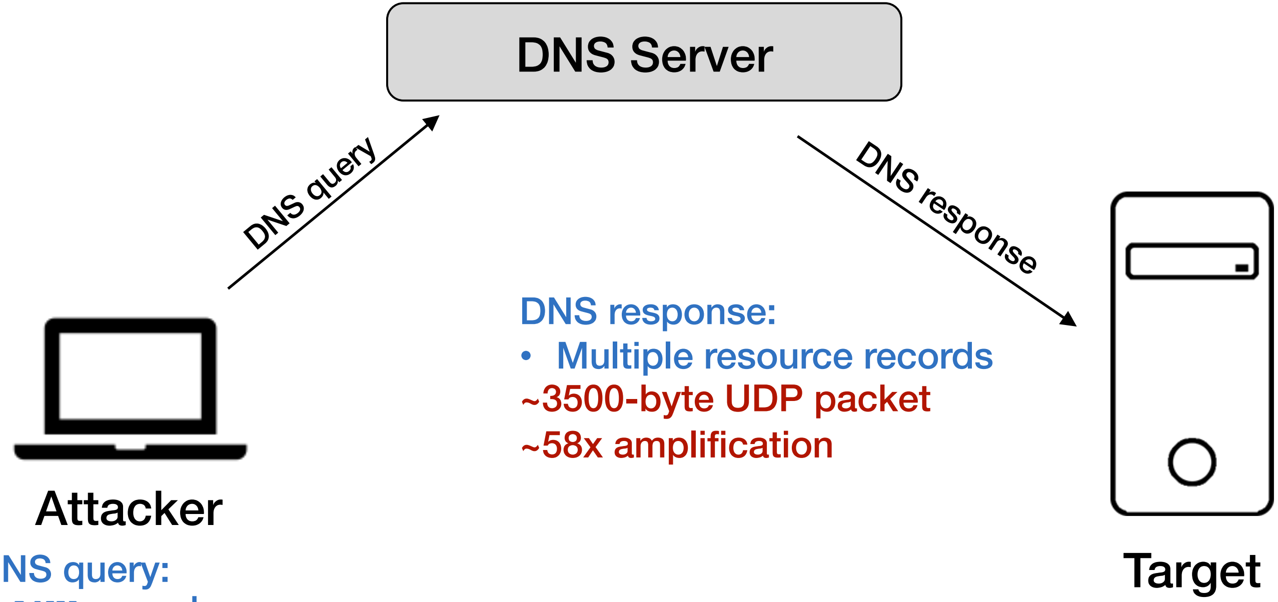
Reflection amplification attack

- Attacker sends packets with the target's IP address as the return address
- Sends request to a service — server responds to the target (the return address)
- Need UDP services so there's no connection state

Amplification attacks generate a lot of traffic for targets

- They magnify the response size relative to the request
- They obscure the origin of the attack
- Exploit services that generate a lot of traffic to a small query

Amplification Example: DNS



DNS response:

- Multiple resource records

~3500-byte UDP packet

~58x amplification

DNS query:

- `ANY` records
  (returns all records for the domain)

60-byte UDP packet with forged source address of the target

Some services vulnerable to amplification attacks

Memcached

- Attacker enters a large payload onto an exposed memcached server
- Spoofs an HTTP GET request with IP address of target (often requesting web cache data)
- Amplification factor: up to 51,200

Network Time Protocol (NTP)

- *Monlist* command causes NTP to respond with the last 600 source IP addresses of requests which have been made to the server
- Amplification factor: 556

Domain Name System (DNS) Server

- Send a DNS lookup request for as much info as possible with a spoofed source address
- Amplification factor: 50 - 179

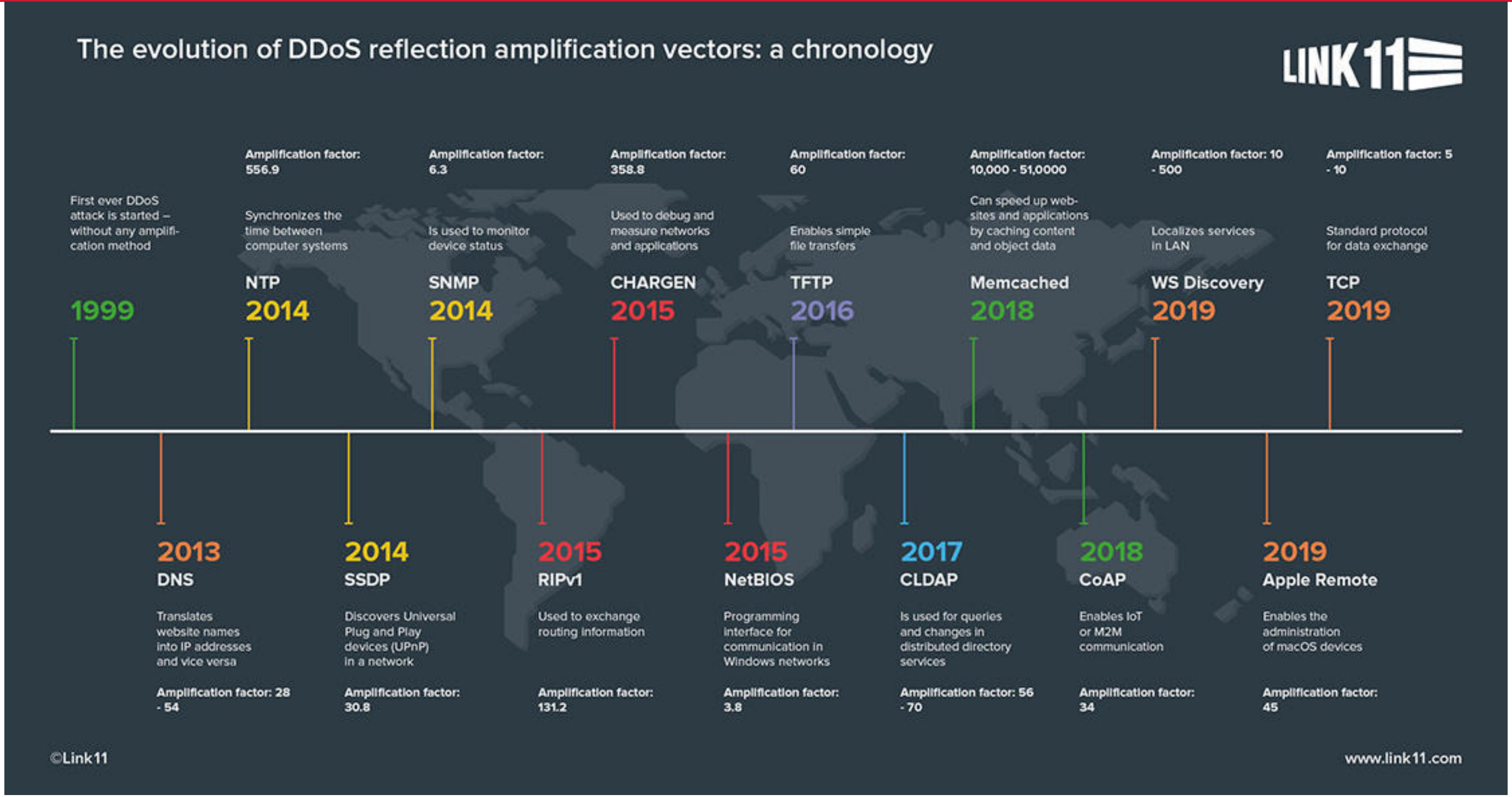
Datagram TLS (D/TLS; TLS over UDP)

- Because it's UDP (connectionless), protocol is spoofable
- Affects misconfigured servers: attackers send small DTLS packets and get large responses sent to spoofed addresses
- Amplification factor: 37

CLDAP (Microsoft derivative of the Lightweight Directory Access Protocol over UDP)

- Affects Windows servers running domain controllers with CLDAP enabled and exposed on the public Internet [link]
- Amplification factor: 56 - 70

Amplification Vectors



The evolution of DDoS reflection amplification vectors: a chronology

1999
First ever DDoS attack is started – without any amplification method

2013
DNS
Translates website names into IP addresses and vice versa
Amplification factor: 28 - 54

NTP
2014
Amplification factor: 556.9
Synchronizes the time between computer systems

2014
SSDP
Discovers Universal Plug and Play devices (UPnP) in a network
Amplification factor: 30.8

SNMP
2014
Amplification factor: 6.3
Is used to monitor device status

2015
RIPv1
Used to exchange routing information
Amplification factor: 131.2

CHARGEN
2015
Amplification factor: 358.8
Used to debug and measure networks and applications

2015
NetBIOS
Programming interface for communication in Windows networks
Amplification factor: 3.8

TFTP
2016
Amplification factor: 60
Enables simple file transfers

2017
CLDAP
Is used for queries and changes in distributed directory services
Amplification factor: 56 - 70

Memcached
2018
Amplification factor: 10,000 - 51,0000
Can speed up websites and applications by caching content and object data

2018
CoAP
Enables IoT or M2M communication
Amplification factor: 34

WS Discovery
2019
Amplification factor: 10 - 500
Localizes services in LAN

2019
Apple Remote
Enables the administration of macOS devices
Amplification factor: 45

TCP
2019
Amplification factor: 5 - 10
Standard protocol for data exchange

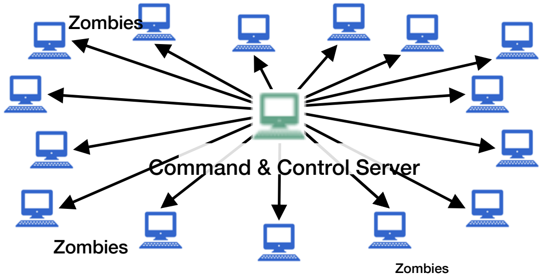
©Link11

www.link11.com

https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

DDoS: Distributed Denial of Service

- **A DDoS attack is one where many systems attack a target**
  - This provides a better opportunity for overwhelming the target with traffic
  - Many systems can generate more data than one and aren't limited by the network bandwidth of any one system
- **Huge numbers of compromised systems reduce need for amplification**
  - The network of attackers is a collection of millions of compromised machines
  - Each system waits for directions from a **command & control** (**C&C**) **server**
  - Blocking a distributed attack is harder because the data doesn't come from one IP address or even one range of addresses
  - Identifying the origin of the attack is difficult for the same reason
- **Some targets are too big to hurt with traffic**
  - Amazon, Google, sites using CDNs (content delivery networks) such as Akamai



AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever

2020

The previous record for the largest DDoS attack ever recorded was of 1.7 Tbps, recorded in March 2018.

Catalin Cimpanu • June 17, 2020

Amazon said its AWS Shield service mitigated the largest DDoS attack ever recorded, stopping a 2.3 Tbps attack in mid-February this year.

The incident was disclosed in the company's AWS Shield Threat Landscape, a report detailing web attacks mitigated by Amazon's AWS Shield protection service.

The report didn't identify the targeted AWS customer but said the attack was carried out using hijacked CLDAP web servers and caused three days of "elevated threat" for its AWS Shield staff.

CLDAP (Connection-less Lightweight Directory Access Protocol) is an alternative to the older LDAP protocol and is used to connect, search, and modify Internet-shared directories.

The protocol has been abused for DDoS attacks since late 2016, and CLDAP servers are known to amplify DDoS traffic by 56 to 70 times its initial size, making it a highly sought-after protocol and a common option provided by DDoS-for-hire services.

https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

Two record DDoSes disclosed this week underscore their growing menace

2020

More bots + better DDoS traps = ever-growing amounts of junk traffic.

Dan Goodin • June 25, 2020

The race upward is showing no signs of slowing. Last week, Amazon reported that its AWS Shield DDoS mitigation service went head-to-head with a 2.3 Tbps attack, a 35-percent increase over the 2018 record. Meanwhile, network provider Akamai said on Thursday that its Prolexic service repelled a DDoS that generated 809 million packets per second. That's a 35-percent increase over what's believed to be the previous high-water mark of the 600Mpps DDoS that Roland Dobbins, principal engineer at competing mitigation service Netscout Arbor, said his company handled.

“We anticipate continued innovation in the area of DDoS attack vectors due to the various financial, ideological, and social motivations of attackers,” Dobbins told me. “DDoS attacks allow attackers to have a hugely disproportionate negative impact on both the intended targets of attacks, as well as uninvolved bystanders.”

The attack, which Akamai said hit an unnamed European bank, was notable for how quickly it ramped up. As the image below illustrates, attackers needed less than three minutes to unleash its peak of 809 Mpps.

https://arstechnica.com/information-technology/2020/06/two-record-ddoses-disclosed-this-week-underscore-their-growing-menace/

Microsoft fends off record-breaking 3.47 Tbps DDoS attack

2022

While a crude brute-force attack, DDoSes are growing ever more potent.

Dan Goodin • January 28, 2022

The company's Azure DDoS Protection team said that in November, it fended off what industry experts say is likely the biggest distributed denial-of-service attack ever: a torrent of junk data with a throughput of 3.47 terabits per second. The record DDoS came from more than 10,000 sources located in at least 10 countries around the world.

The DDoS targeted an unidentified Azure customer in Asia and lasted for about two minutes. The following month, Microsoft said, Azure warded off two other monster DDoSes. Weighing in at 3.25Tbps, the first one came in four bursts and lasted about 15 minutes.

… The 3.7Tbps attack delivered roughly 340 million packets per second.

…

Sadly, the Internet is awash with millions of misconfigured servers that make reflection amplification attacks possible. These Internet nuisances played a big role in the 3.47Tbps attack Microsoft reported.

…

Most of those attacks came from Internet-of-Things devices infected with the open source Mirai botnet malware and lower-volume UDP protocol attacks. The vast majority were UDP spoof floods. A much smaller portion used UDP reflection and amplification, mostly SSDP, memcached, and NTP.

https://arstechnica.com/information-technology/2022/01/microsoft-fends-off-record-breaking-3-47-tbps-ddos-attack/

Google Cloud Stops Monster DDoS Attack

2022

Google successfully fended off an HTTPS Distributed Denial of Service (DDoS) attack, which peaked at 46 million requests per second (RPS) -- the largest Layer 7, the application layer, DDoS reported to date.

Steven Vaughan-Nichols • August 22, 2022

Distributed Denial of Service (DDoS) attacks don’t need to be big to wreak havoc on a target, but it doesn’t hurt. In the latest biggest of all times attacks, Google fended off an HTTPS DDoS attack, which peaked at 46 million requests per second (RPS). That made it the largest Layer 7, the application layer, DDoS reported to date. It was 76% larger than the previously reported record.

So how big is that? Imagine a day’s worth of requests to Wikipedia hammering down in just 10 seconds.

Yeah, that’s a lot.

Welcome to the 2022 internet. A few weeks earlier, Cloudflare had beat off a then record 26 million RPS DDoS attack. Before that, Cloudflare, in August 2021, handled a 17.2M RPS HTTP DDoS attack. Gigantic DDoS attacks are happening ever more often. These put the top DDoS attacks of the past to shame.

https://thenewstack.io/google-cloud-stops-monster-ddos-attack/

Google Cloud, AWS, and Cloudflare report largest DDoS attacks ever

2023

The attack on Google Cloud was 7½ times larger than any previously recorded DDoS attack. Here's what else you need to know

Steven Vaughan-Nichols • October 10, 2023

The Google Cloud was hit by the largest DDoS attack in history this past August, with the digital onslaught peaking at an unprecedented **398 million requests per second (RPS).** How big is that? According to Google, in two minutes, the Google Cloud was slammed by more RPS than Wikipedia saw in all of September 2023.

That's big. The attack on Google Cloud, which employed a novel "Rapid Reset" technique, was 7½ times larger than any previously recorded DDoS attack. 2022's largest-recorded DDoS attack peaked at "only" 46 million RPS.

Google wasn't the only one to get hit. Cloudflare, a leading cloud delivery network (CDN), and Amazon Web Services (AWS), the world's biggest cloud provider, also reported getting blasted. Cloudflare fended off a 201 million RPS attack, while AWS held off a 155 million RPS assault.

https://www.zdnet.com/article/google-cloud-aws-and-cloudflare-report-largest-ddos-attacks-ever/

Cloudflare blocks largest recorded DDoS attack peaking at 3.8Tbps

2024

Ionut Ilascu • October 3, 2024

During a distributed denial-of-service campaign targeting organizations in the financial services, internet, and telecommunications sectors, volumetric attacks peaked at 3.8 terabits per second, the largest publicly recorded to date. The assault consisted of a “month-long” barrage of more than 100 hyper-volumetric DDoS attacks flooding the network infrastructure with garbage data.

In a volumetric DDoS attack, the target is overwhelmed with large amounts of data to the point that they consume the bandwidth or exhaust the resources of applications and devices, leaving legitimate users with no access.

Asus routers, MikroTik devices, DVRs, and web servers
Many of the attacks aimed at the target’s network infrastructure (network and transport layers L3/4) exceeded two billion packets per second (pps) and three terabits per second (Tbps).

According to researchers at internet infrastructure company Cloudflare, the infected devices were spread across the globe but many of them were located in Russia, Vietnam, the U.S., Brazil, and Spain.

https://www.bleepingcomputer.com/news/security/cloudflare-blocks-largest-recorded-ddos-attack-peaking-at-38tbps/

Another new DDoS record in 2024

2024

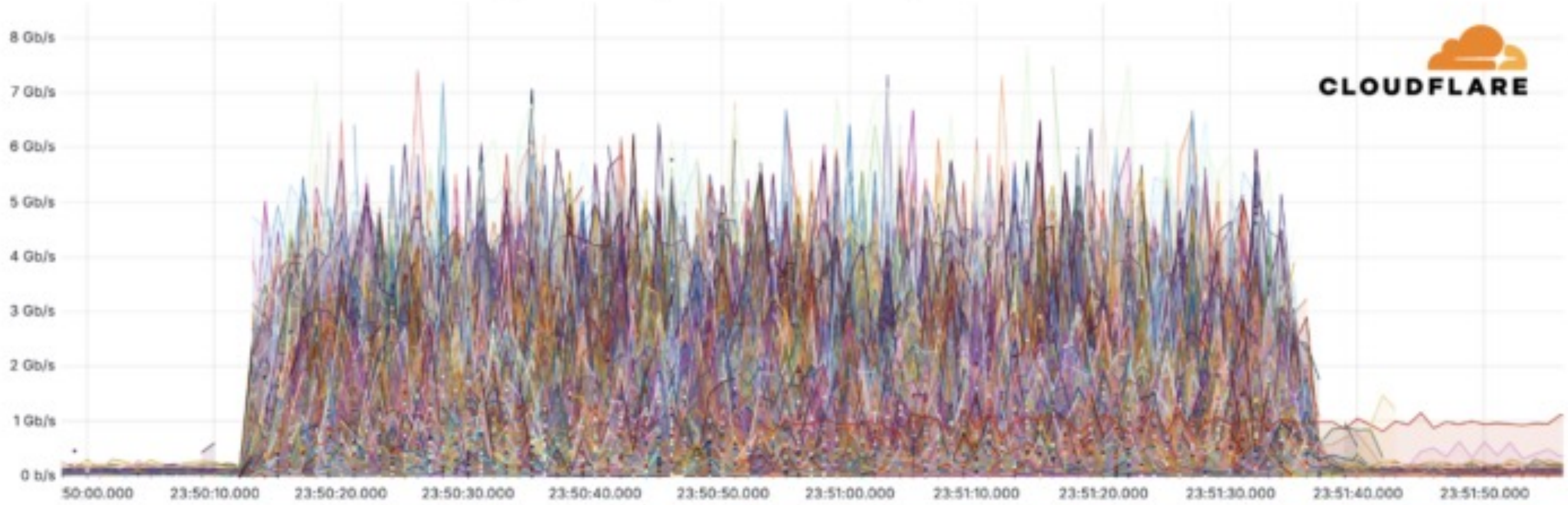
In 2024, Cloudflare mitigated the largest distributed denial-of-service (DDoS) attack ever reported, an attack that reached 5.6 terabits per second (Tbps) and 666 million packets per second at its peak. The attack lasted about 80 seconds and was part of a larger ongoing campaign of hyper-volumetric DDoS attacks. The Cloudflare network automatically mitigated the 5.6 Tbps attack and all other attacks that were part of the campaign, protecting Cloudflare customers.

This attack originated from over 13,000 compromised Internet of Things devices that were made part of a Mirai botnet.

DDoS attacks in 2024 increased by 53% from 2023.
Hyper-volumetric attacks exceeding 1 terabit per second grew by 1,885% in the fourth quarter of 2024.

https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/
https://www.cloudflare.com/learning/ddos/famous-ddos-attacks

5.6 Tbps DDoS attack delivered by an average of 5,500 unique source IPs per second



The 13,000 source IP addresses that launched the 5.6 Tbps DDoS attack

2025: Largest Observed Volumetric Attack

2025

Hyper-volumetric attacks" overwhelmed networks with traffic up to 6.5 Tbps

Nokia security researchers are tracking a botnet, dubbed Eleven11bot, that has been delivering what is likely the largest directed denial-of-service attack ever recorded. An estimated 30,000 webcams and video recorders make up the massive botnet. The network is international, but Nokia says the highest concentration of compromised devices (24.4%) is in the United States. While not the largest botnet ever recorded, it has pulled off the biggest observed attack ever seen, peaking at 6.5 terabits per second, surpassing the previous record of 5.6 Tbps set in January, according to Cloudflare.

Greynoise researchers believe Eleven11bot is a new variant of Mirai, the infamous malware that first surfaced in 2016. Mirai-based botnets typically infect Internet of Things (IoT) devices by exploiting default credentials or software vulnerabilities. Researchers believe the Eleven11bot variant uses a newly discovered exploit to compromise Shenzhen TVT-NVMS 9000 digital video recorders running on HiSilicon chips.

https://www.techspot.com/news/107049-massive-botnet-compromises-30000-devices-record-breaking-ddos.html

https://arstechnica.com/security/2025/03/massive-botnet-that-appeared-overnight-is-delivering-record-size-ddoses/

Techniques for Dealing With DDoS Attacks

Protection from DDoS attacks is difficult in general

- **In a large-scale DDoS attack, attacks may come from:**
  - Multiple geographic regions
  - A large set of IP addresses
  - Multiple ISPs
- **Attempts to block traffic may be useless if your router or network is getting congested with traffic**

Techniques for Dealing With DDoS Attacks

Protection from DDoS attacks is difficult in general

Network-Level Mitigations – operations on the router or firewall

Rate Limiting	Restrict the number of requests a client can make in a given time
IP Blacklisting	Drop traffic from specific IP addresses or geographic regions
Traffic Shaping	Prioritize or limit certain types of packets (e.g., allow HTTP but not suspicious UDP)
Traffic Filtering	Drop traffic with specific source/destination addresses or ports
Blackhole Routing	Drop all traffic to the targeted IP address to protect the network

Techniques for Dealing With DDoS Attacks

Application-Level Mitigations – protect services from being overwhelmed

Web Application Firewalls	These allow you to detect and block specific types of HTTP/HTTPS traffic
CAPTCHAs	Prevent bot-driven requests from reaching critical services
Content Delivery Networks (CDNs)	Services (like Akamai) that cache and serve content from a huge collection of servers so the origin doesn't get the traffic

Outsource!

Techniques for Dealing With DDoS Attacks

Participation Mitigations – don't accidentally participate in a DDoS attack

Disable Services	Disable unnecessary UDP services
Monitor Traffic	Detect systems generating unusual volumes of traffic, especially for common services (like DNS or NTP)

The End