

Denial of Service (DoS)

- attack on availability of a service
- stop legitimate users from using service
- stop a service from running

Why DoS is hard

- huge attack surface
 - basically anything on the internet that can receive packets
- no skill necessary
 - attacks can come from anywhere
- simplest attack is to consume bandwidth
 - If I have 10 MiB/s and so does the server, I can take it all
- Distributed DoS (DDoS)
 - use the combined bandwidth of a whole lot of machines

Why do a DoS attack?

Why do a DoS attack?
think back to the adversarial categorical schema

What might motivate a DoS attack from:

- foreign intelligence
- terrorists
- politically motivated adversaries
- industrial espionage agents
- organized crime
- lesser criminals, e.g., “script kiddies”
- malicious insiders, e.g., disgruntled employees
- non-malicious employees, e.g., USB stick pluggers-in
- researchers, casual hackers, and bug bounty hunters

Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen  February 4, 2009 | 12:13 pm | Categories: [Cybarmageddon!](#)



What's the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.

Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen  February 4, 2009 | 12:13 pm | Categories: [Cybarmageddon!](#)



"Do you get annoyed all the time because of skids on xBox Live? Do you want to take down your competitors' servers or Web site?," reads the site's ad, apparently recorded by [this paid actor at Fiverr.com](#). "Well, boy, do we have the product for you! Now, with asylumstresser, you can take your enemies offline for just 30 cents for a 10 minute time period. Sounds awesome, right? Well, it gets even better: For only \$18 per month, you can have an unlimited number of attacks with an increased boot time. We also offer Skype and tiny chat IP resolvers."



What's the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.

Extortion via DDoS on the rise


By [Denise Pappalardo](#) and [Ellen Messmer](#), Network World, 05/16/05

Criminals are increasingly targeting corporations with distributed denial-of-service attacks designed not to disrupt business networks but to extort thousands of dollars from the companies.

Ivan Maksakov, Alexander Petrov and Denis Stepanov were accused of receiving \$4 million from firms that they threatened with cyberattacks.

The trio concentrated on U.K. Internet gambling sites, according to the prosecution. One bookmaker, which refused to pay a demand for \$10,000, was attacked and brought offline--which reportedly cost it more than \$200,000 a day in lost business.

U.S. Charges 37 Alleged Mules and Others in Online Bank Fraud Scheme

By [Kim Zetter](#)  September 30, 2010 | 3:07 pm | Categories: [Crime](#), [Cybersecurity](#), [Hacks and Cracks](#)

 Follow @KimZetter

120

 Tweet

0

+1



 Share

Beyrouti, Babbo and Vitello worked with hackers who breached brokerage accounts at E-Trade and TD Ameritrade. The hackers then executed fraudulent sales of securities and transferred the proceeds from the sale to the mules' accounts. The receiving accounts were set up in the names of shell companies and linked to the hacked accounts.

Meanwhile, the victims' phones received a barrage of calls to prevent the brokerage firms from contacting them to confirm the legitimacy of the transactions. When the victims answered their phone, they would hear silence or a recorded message. About \$1.2 million was transferred to shell accounts opened by the suspects, who then transferred the money to other accounts in Asia or withdraw the money from ATMs in the New York area.

'Operation Payback' Attacks Fell Visa.com

By ROBERT MACKEY



Operation: Payback Operation:

A message posted on Twitter by a group of Internet activists announcing the start of an attack on Visa's Web site, in retaliation for the company's actions against WikiLeaks.

Last Updated | 6:54 p.m. A group of Internet activists took credit for crashing the Visa.com Web site on Wednesday afternoon, hours after they launched [a similar attack on MasterCard](#). The cyber attacks, by activists who call themselves Anonymous, are aimed at punishing companies that have acted to stop the flow of donations to WikiLeaks in recent days.

The group explained that its [distributed denial of service attacks](#) — in which they essentially flood Web sites with traffic to slow them down or knock them offline — were part of a broader effort called Operation Payback, which






Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites

Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey[†]

The Berkman Center for Internet & Society at Harvard University

December 2010

9. In the past year, has your site been subjected to a denial of service attack, meaning an attacker prevented or attempted to prevent access to your site altogether?

#	Answer	Bar	Response	%
1	yes		21	62%
2	no		8	24%
3	not sure		5	15%
	Total		34	

Row over Korean election DDoS attack heats up

Ruling party staffer accused of disrupting Seoul mayoral by-election

By **John Leyden** • [Get more from this author](#)

Posted in [Security](#), 7th December 2011 09:23 GMT

[Free whitepaper – IBM System Networking RackSwitch G8124](#)

A political scandal is brewing in Korea over alleged denial of service attacks against the National Election Commission (NEC) website.

Police have arrested the 27-year-old personal assistant of ruling Grand National Party politician Choi Gu-sik over the alleged cyber-assault, which disrupted a Seoul mayoral by-election back in October.

However, security experts said that they doubt the suspect, identified only by his surname "Gong", had the technical expertise or resources needed to pull off the sophisticated attack.

Row over Korean election DDoS attack heats up

Ruling party staffer accused of disrupting Seoul mayoral by-election

By [John Leyden](#) • [Get more from this author](#)

Posted in [Security](#), 7th December 2011 09:23 GMT

[Free whitepaper – IBM System Networking RackSwitch G8124](#)

A political scandal is brewing in Korea over alleged denial of service attacks against the National Election Commission (NEC) website.

Police have arrested the 27-year-old personal assistant of ruling Grand National Party politician Choi Gu-sik over the alleged cyber-assault, which disrupted a Seoul mayoral by-election back in October.

However, security experts said that they doubt the suspect, identified only by his surname "Gong", had the technical expertise or resources needed to pull off the sophisticated attack.

Gong continues to protest his innocence, a factor that has led opposition politicians to speculate that he is covering up for higher-ranking officials who ordered the attack.

Democratic Party politician Baek Won-woo told [The HankYoreh](#): "We need to determine quickly and precisely whether there was someone up the line who ordered the attack, and whether there was compensation." ®

Federal Court won't remove MPs over election robocalls



Judge finds that fraud occurred, linked to the Conservative Party's CIMS database

Laura Payton · CBC News · Posted: May 23, 2013 8:14 PM ET | Last Updated: May 23, 2013



Voters backed by the Council of Canadians challenged the 2011 election victories by Conservative MPs, clockwise from top-left, Kelly Block, John Duncan, Jay Aspin, Joyce Bateman, Joe Daniel, Lawrence Toet and Ryan Leef. The challenge against Daniel was dropped Oct. 23. The Federal Court says it won't throw six MPs out of seats over allegations of widespread vote suppression through automated robocalls. (Conservative.ca/CBC)

[3] The calls struck at the integrity of the electoral process by attempting to dissuade voters from casting ballots for their preferred candidates. This form of “voter suppression”, was, until the 41st General Election, largely unknown in this country.

[4] The evidence presented in these applications points to a concerted campaign by persons who had access to a database of voter information maintained by a political party. It was not alleged that any of the candidates of that party, including those who were successful in the six ridings at issue, were responsible for this campaign but that others took it upon themselves to attempt to influence the election results in their favour.

Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

Ian Traynor in Brussels
The Guardian, Thursday 17 May 2007
[Article history](#)



Bronze Soldier, the Soviet war memorial removed from Tallinn.
Nisametdinov/AP

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.

August 11th, 2008

Coordinated Russia vs Georgia cyber attack in progress

Posted by Dancho Danchev @ 4:23 pm

Categories: [Black Hat](#), [Botnets](#), [Denial of Service \(DoS\)](#), [Governments](#), [Hackers...](#)

Tags: [Security](#), [Cyber Warfare](#), [DDoS](#), [Georgia](#), [South Osetia...](#)

 **62** TalkBacks
  SHARE
  PRINT
  E-MAIL
  WORTHWHILE
  +18
  24 VOTES

In the wake of the [Russian-Georgian conflict](#), a week worth of speculations around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia's Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S, with [Georgia's Ministry of Foreign](#)

[illegible]

Affairs undertaking a desperate step in order to disseminate real-time

AIRPORTS

Russian Cyber Attack Hits Websites of Multiple U.S. Airports

BY HELWING VILLAMIZAR  OCTOBER 10, 2022  2 MINUTES READ



DALLAS – A Russian cyber attack has targeted the websites of airports in New York, Atlanta, Los Angeles, Chicago, and Des Moines. The attack did not affect airport operations, only their websites.

A source person briefed on the matter told [ABC News](#) that an attacker within the Russian Federation targeted some of the country's busiest airports for cyberattacks on Monday. The targeted systems do not handle air traffic control, internal airline communications, and coordination, or transportation security.

"It's an inconvenience," the source said. The attacks have resulted in targeted "denial of public access" to public-facing web domains that report airport wait times and congestion.

Over a dozen airport websites were impacted by the Denial-of-Service (DoS) attack, according to John Hultquist, head of intelligence analysis at the cybersecurity firm Mandiant who spoke to *ABC*.



The BBC's Rory Cellan-Jones explains why the attack is like a "motorway jam", alongside expert David Emm from Kaspersky Lab

The internet around the world has been slowed down in what security experts are describing as the biggest cyber-attack of its kind in history.

A row between a spam-fighting group and hosting firm has sparked retaliation attacks affecting the wider internet.

Experts worry that the row could escalate to affect banking and email systems.

Five national cyber-police-forces are investigating the attacks.

Spamhaus, a group based in both London and Geneva, is a non-profit organisation that aims to help email providers filter out spam and other unwanted content.

Two Basic Approaches

- deny service via a **program flaw**
 - “*NULL”
 - give input that crashes a server
 - trick a server into shutting down
- deny service via **resource exhaustion**
 - “while(1);”
 - consume CPU, memory, disk, network
- both a violation of RELUCTANT ALLOCATION

- Internet Control Message Protocol
- provides feedback about network operations
- error reporting, congestion control, reachability
 - destination unreachable
 - time exceeded
 - reachability test
 - message transit time

Ping of Death

Ping of Death

If an old Windows machine received an ICMP packet with a payload longer than 64K, it would crash or reboot

Ping of Death

If an old Windows machine received an ICMP packet with a payload longer than 64K, it would crash or reboot

Why?

Packets of this length are illegal, so programmers of Windows code did not account for them.

Ping of Death

If an old Windows machine received an ICMP packet with a payload longer than 64K, it would crash or reboot

Why?

Packets of this length are illegal, so programmers of Windows code did not account for them.

Attackers induce zero-probability failures

Smurf Reflector Attack

Smurf Reflector Attack
Attacker sends a ICMP echo request

Smurf Reflector Attack

Attacker sends a ICMP echo request
but with the victim's IP as source

Smurf Reflector Attack

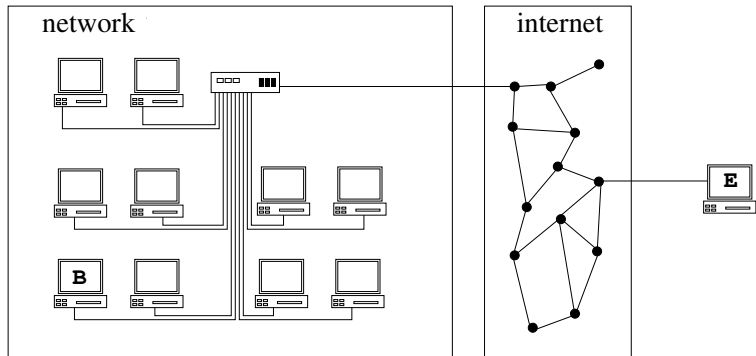
Attacker sends a ICMP echo request
but with the victim's IP as source
sends to to the broadcast address

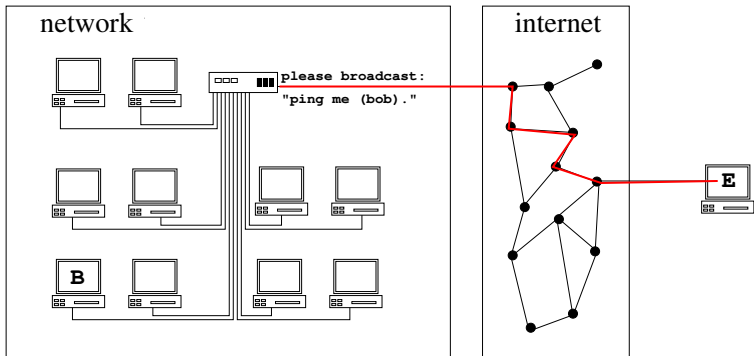
Smurf Reflector Attack

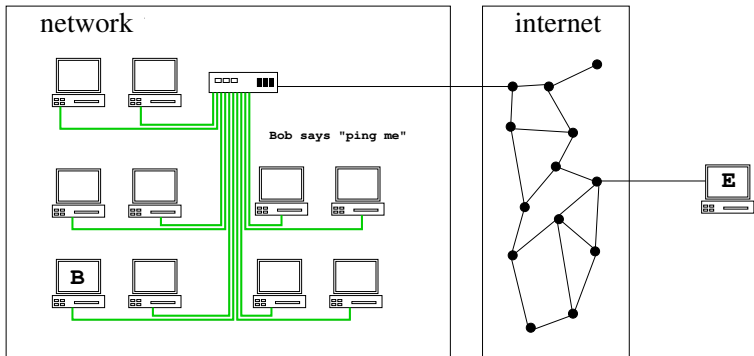
Attacker sends a ICMP echo request
but with the victim's IP as source
sends to to the broadcast address
bad gateways allowed this from outside

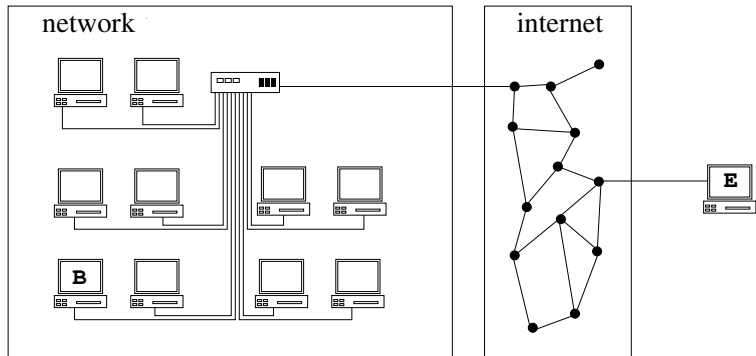
Smurf Reflector Attack

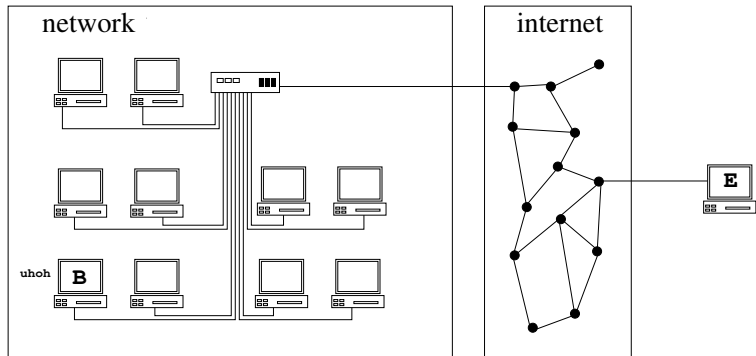
Attacker sends a ICMP echo request
but with the victim's IP as source
sends to to the broadcast address
bad gateways allowed this from outside
stream of pings from all computers
on the network overwhelm victim

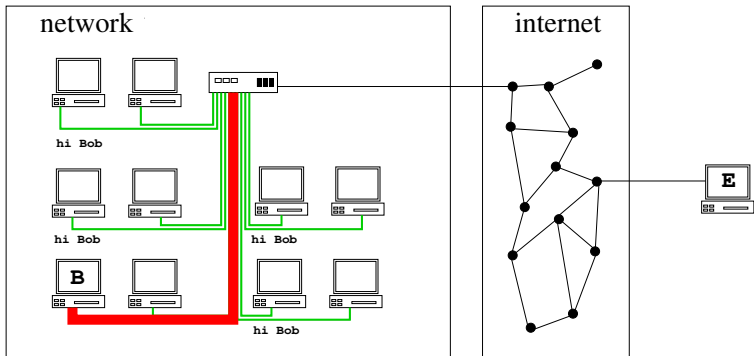


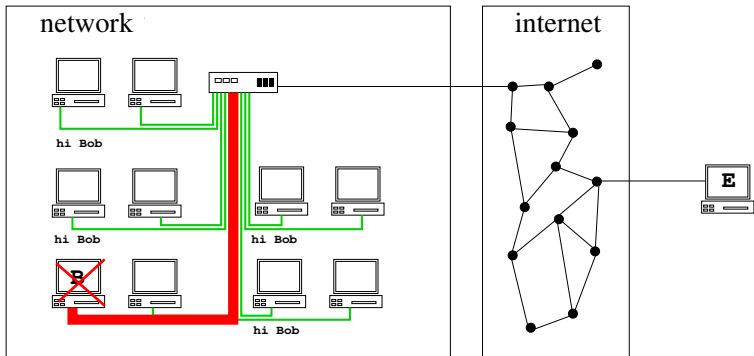












Bonk and Teardrop

- IP packet has offset field for fragmentation
- attacker can set offset to overlapping
 - bad implementations will crash on reassembly
 - COMPLETE MEDIATION
- attacker can set offset to very large value
 - bad implementations will crash
 - COMPLETE MEDIATION

DoS in General Terms

- defending against program flaws requires
 - careful coding, testing, and review
 - careful authentication for incoming commands
 - e.g., shutdown or unlink
 - fuzz testing
 - throw random input at a program
 - if it crashes that is bad
- defending against resource exhaustion is really hard
 - isolation
 - keep adversary's consumption separate from others
 - Internet lacks isolation between traffic of different users
 - reliable identification of users
 - don't handle adversary's requests

Performing a DoS

- goal is to exhaust the **bottleneck link** for target's Internet connection
 - all traffic to/from the target goes through this link
 - this link becomes completely filled up with useless traffic
- two approaches
 - use all the bandwidth
 - send maximum-size packets
 - overwhelm the rate that the **bottleneck router** processes packets
 - send minimum-size packets (why?)

Defending DoS

- suppose attacker has access to lots of bandwidth
 - use to to send packets to target
- target can simply filter out their traffic
 - drop all packets from the attacker
 - filtering is an **isolation mechanism**
 - what can go wrong?

Filtering Flaws

- attacker can spoof source IP address
 - just use random ones each time
 - what can defender do?
 - nothing unless the traffic is otherwise conspicuous
 - hope more ISPs implement **anti-spoofing** mechanisms

Filtering Flaws

- attacker can **use** many actual machines to send traffic
 - distributed denial of service
 - now defender's filters become much more complicated
 - botnets already exist and can be rented out for this purpose
 - real machines can use real IP

DoS Amplification

- attacker makes the victim use more bandwidth than the attacker
- makes DoS easier and cheap
- security is hard because of these asymmetries

Recall DNS:

- DNS is critical UDP protocol
- converts hostnames into IP addresses
- query: what is IP for ucalgary.ca
- response: the IP for ucalgary.ca is 136.159.96.125
- response repeats query and adds more information

DNS DoS Amplification

- reply to DNS includes the query and all the answers
- reply is therefore larger than the query
- attacker spoofs DNS requests as though it came from victim
 - this can be done with **blind spoofing**
 - UDP has a query-response nature
 - victim never learns attacker's IP
 - victim cannot disable DNS
 - blocking victim IP is unproductive (why?)
- can give 100x amplification

Alert (TA14-013A)

[More Alerts](#)

NTP Amplification Attacks Using CVE-2013-5211

Original release date: January 13, 2014 | Last [revised](#): October 06, 2016

 Print

 Tweet

 Send

 Share

Systems Affected

NTP servers

Overview

A Network Time Protocol (NTP) Amplification attack is an emerging form of Distributed Denial of Service (DDoS) that relies on the use of publically accessible NTP servers to overwhelm a victim system with UDP traffic.

Description

The NTP service supports a monitoring service that allows administrators to query the server for traffic counts of connected clients. This information is provided via the "monlist" command. The basic attack technique consists of an attacker sending a "get monlist" request to a vulnerable NTP server, with the source address spoofed to be the victim's address.

Impact

The attack relies on the exploitation of the 'monlist' feature of NTP, as described in CVE-2013-5211, which is enabled by default on older NTP-capable devices. This command causes a list of the last 600 IP addresses which connected to the NTP server to be sent to the victim. Due to the spoofed source address, when the NTP server sends the response it is sent instead to the victim. Because the size of the response is typically considerably larger than the request, the attacker is able to amplify the volume of traffic directed at the victim. Additionally, because the responses are legitimate data coming from valid servers, it is especially difficult to block these types of attacks. The solution is to disable "monlist" within the NTP server or to upgrade to the latest version of NTP (4.2.7) which disables the "monlist" functionality.

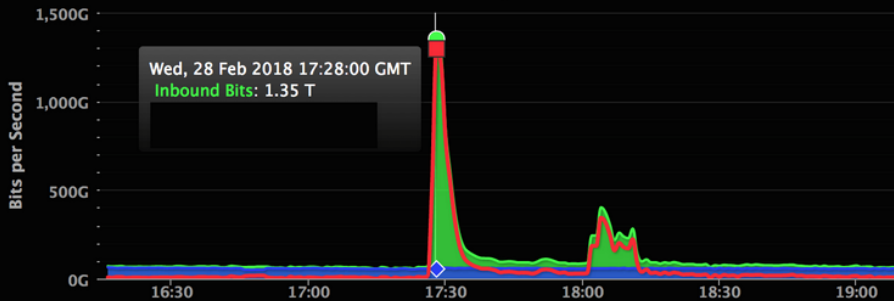
NTP monlist command gives 500x amplification

NTP monlist command gives 500x amplification
Anyone running a publicly accessible NTP
server can be used in the attack.

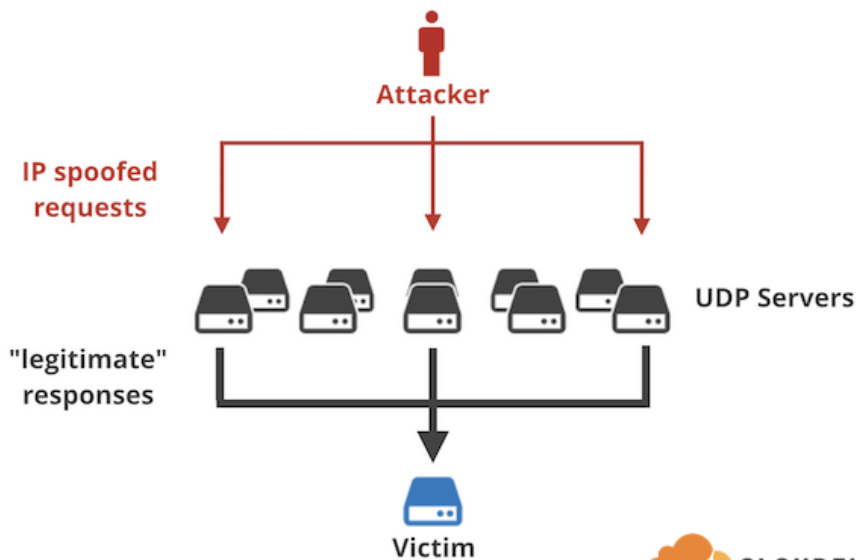
Memcached DoS Amplification

- memcache is a distributed memory cache
 - client store key-value pairs to a server
 - client requests values by using its key
- what can go wrong?
- what was the fix?

ALL BORDER Bits per Second



At the peak of the attack, GitHub was flooded with data coming in at 1.35Tbps. The previous largest DDoS attack ever recorded was closer to 1.1Tbps. The second phase of the attack, which was causing intermittent interruptions, was only spiking at around 400Gbps.



- 2013 Spamhaus at 300 Gbps
 - DNS open recursers
 - make attributing spammers hard by taking off service
- 2015 GitHub from PRoC
 - targetted projects to evade golden shield
 - injected javascript on those visiting Baidu
- 2016 Dyn (DNS provider) using IoT
 - Mirai botnet scanned web for vulnerable IoT devices
 - default usernames and password
 - motive may have been flexing
 - authors may have wanted to sell antiDoS “insurance” to minecraft server operators

DDoS Events

- 2017 Google at 2.54 Tbps
 - kept secret for 3 years
 - attributed to state sponsored actor
 - Google absorbed it without impact
- 2018 GitHub at 1.3 Tbps
 - used memcached
 - have seen amplifications of 51200x
 - perpetrator and motive unknown
- 2020 AWS at 2.3 Tbps
 - used CLDAP (rfc 1798)
 - the C stands for “connection-less”
 - 50–70x amplification

- major anti-DoS/DDoS vendor
- key methods
 - enormous bandwidth capacity
 - many sites may use it
 - won't all need full capacity need simultaneously
 - actual IP you visit is geographically distributed
 - local spikes do not impact most users
 - impose extra challenges on some users
 - IP-based reputation
 - dynamic rate limited based on observation

Summary

- many different adversaries want to use DoS attacks
- DoS attacks on the Internet are hard to stop
 - hard to identify honest queries from identical malicious ones
 - IP spoofing hides origin
 - DDoS from Botnets makes it easier and seem more legitimate
- UDP protocols can allow IP spoofing to combine with amplification
 - small query generates a big response that it aimed at victim