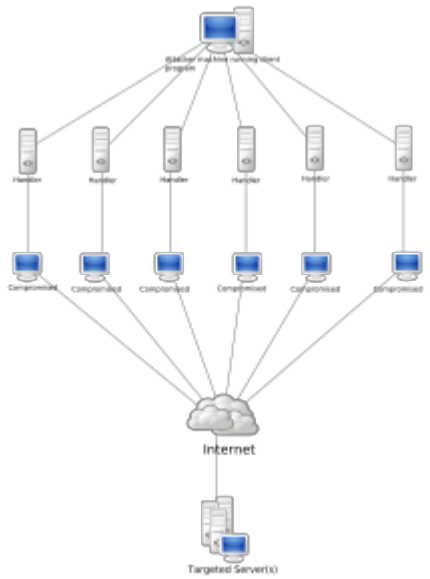
WIKIPEDIA

Denial-of-service attack

In computing, a **denial-of-service attack** (**DoS attack**) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1]

In a **distributed denial-of-service attack** (**DDoS attack**), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, disrupting trade.



DDoS Stacheldraht attack diagram.

Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail[2][3][4] and activism[5] can motivate these attacks.

Contents

History

Court testimony shows that the first demonstration of DoS attack was made by Khan C. Smith in 1997 during a DEF CON event, disrupting Internet access to the Las Vegas Strip for over an hour. The release of sample code during the event led to the online attack of Sprint, EarthLink, E-Trade, and other major corporations in the year to follow.[6]

On March 5, 2018, an unnamed customer of the US-based service provider Arbor Networks fell victim to the largest DDoS in history, reaching a peak of about 1.7 terabits per second.[7] The previous record was set a few days earlier, on March 1, 2018, GitHub was hit by an attack of 1.35 terabits per second.[8]

Types

Denial-of-service attacks are characterized by an explicit attempt by attackers to prevent legitimate use of a service. There are two general forms of DoS attacks: those that crash services and those that flood services. The most serious attacks are distributed.[9]

Distributed DoS

A **distributed denial-of-service** (**DDoS**) is a large-scale DoS attack where the perpetrator uses more than one unique IP address, often thousands of them.[10] A distributed denial of service attack typically involves more than around 3–5 nodes on different networks; fewer nodes may qualify as a DoS attack but is not a DDoS attack.[11][12] Since the incoming traffic flooding the victim originates from different sources, it may be impossible to stop the attack simply by using ingress filtering. It also makes it difficult to distinguish legitimate user traffic from attack traffic when spread across multiple points of origin. As an alternative or augmentation of a DDoS, attacks may involve forging of IP sender addresses (IP address spoofing) further complicating identifying and defeating the attack.

The scale of DDoS attacks has continued to rise over recent years, by 2016 exceeding a terabit per second.[13][14] Some common examples of DDoS attacks are fraggle, smurf, and SYN flooding.[15]

Application layer attacks

An **application layer DDoS attack** (sometimes referred to as **layer 7 DDoS attack**) is a form of DDoS attack where attackers target application-layer processes.[16][11] The attack over-exercises specific functions or features of a website with the intention to disable those functions or features. This application-layer attack is different from an entire network attack, and is often used against financial institutions to distract IT and security personnel from security breaches.[17] In 2013, application-layer DDoS attacks represented 20% of all DDoS attacks.[18] According to research by Akamai Technologies, there have been "51 percent more application layer attacks" from Q4 2013 to Q4 2014 and "16 percent more" from Q3 2014 over Q4 2014.[19] In November 2017; Junade Ali, a Computer Scientist at Cloudflare noted that whilst network-level attacks continue to be of high capacity, they are occurring less frequently. Ali further notes that although network-level attacks are becoming less frequent, data from Cloudflare demonstrates that application-layer attacks are still showing no sign of slowing down.[20]

Application layer

The OSI model (ISO/IEC 7498-1) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO). The model groups similar communication functions into one of seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the communications path needed by applications above it, while it calls the next lower layer to send and receive packets that traverse that path.

In the OSI model, the definition of its application layer is narrower in scope than is often implemented. The OSI

model defines the application layer as being the user interface. The OSI application layer is responsible for displaying data and images to the user in a human-recognizable format and to interface with the presentation layer below it. In an implementation, the application and presentation layers are frequently combined.

Method of attack

An application layer DDoS attack is done mainly for specific targeted purposes, including disrupting transactions and access to databases. It requires fewer resources than network layer attacks but often accompanies them.[21] An attack may be disguised to look like legitimate traffic, except it targets specific application packets or functions. The attack on the application layer can disrupt services such as the retrieval of information or search functions on a website.[18]

Advanced persistent DoS

An **advanced persistent DoS** (APDoS) is more likely to be perpetrated by an advanced persistent threat (APT): attackers who are well-resourced, exceptionally skilled and have access to substantial commercial grade computer resources and capacity. APDoS attacks represent a clear and emerging threat needing specialised monitoring and incident response services and the defensive capabilities of specialised DDoS mitigation service providers.

This type of attack involves massive network layer DDoS attacks through to focused application layer (HTTP) floods, followed by repeated (at varying intervals) SQLi and XSS attacks.[22] Typically, the perpetrators can simultaneously use from 2 to 5 attack vectors involving up to several tens of millions of requests per second, often accompanied by large SYN floods that can not only attack the victim but also any service provider implementing any sort of managed DDoS mitigation capability. These attacks can persist for several weeks. The longest continuous period noted so far lasted 38 days.[23] This attack involved approximately 50+ petabits (50,000+ terabits) of malicious traffic.

Attackers in this scenario may tactically switch between several targets to create a diversion to evade defensive DDoS countermeasures but all the while eventually concentrating the main thrust of the attack onto a single victim. In this scenario, attackers with continuous access to several very powerful network resources are capable of sustaining a prolonged campaign generating enormous levels of un-amplified DDoS traffic.

APDoS attacks are characterised by:

- advanced reconnaissance (pre-attack OSINT and extensive decoyed scanning crafted to evade detection over long periods)
- tactical execution (attack with both primary and secondary victims but focus is on primary)
- explicit motivation (a calculated end game/goal target)
- large computing capacity (access to substantial computer power and network bandwidth)
- simultaneous multi-threaded OSI layer attacks (sophisticated tools operating at layers 3 through 7)
- persistence over extended periods (combining all the above into a concerted, well managed attack across a range of targets).[24]

Denial-of-service as a service

Some vendors provide so-called "booter" or "stresser" services, which have simple web-based front ends, and accept payment over the web. Marketed and promoted as stress-testing tools, they can be used to perform unauthorized denial-of-service attacks, and allow technically unsophisticated attackers access to sophisticated attack tools without the need for the attacker to understand their use.[25] Usually powered by a botnet, the traffic produced by a consumer stresser can range anywhere from 5-50 Gbit/s, which can, in most cases, deny the average home user internet access.

Symptoms

The United States Computer Emergency Readiness Team (US-CERT) has identified symptoms of a denial-of-service attack to include:[26]

- unusually slow network performance (opening files or accessing web sites)
- unavailability of a particular web site
- inability to access any web site
- dramatic increase in the number of spam emails received (this type of DoS attack is considered an e-mail bomb).

Additional symptoms may include:

- disconnection of a wireless or wired internet connection
- long-term denial of access to the web or any internet services.

If the attack is conducted on a sufficiently large scale, entire geographical regions of Internet connectivity can be compromised without the attacker's knowledge or intent by incorrectly configured or flimsy network infrastructure equipment.

Attack techniques

A wide array of programs are used to launch DoS-attacks.

Attack tools

In cases such as MyDoom and Slowloris the tools are embedded in malware, and launch their attacks without the knowledge of the system owner. Stacheldraht is a classic example of a DDoS tool. It uses a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.[27]

In other cases a machine may become part of a DDoS attack with the owner's consent, for example, in Operation Payback, organized by the group Anonymous. The LOIC has typically been used in this way. Along with HOIC a wide variety of DDoS tools are available today, including paid and free versions, with different features available. There is an underground market for these in hacker related forums and IRC channels.

UK's GCHQ has tools built for DDoS, named PREDATORS FACE and ROLLING THUNDER.[28]

Application-layer floods

Various DoS-causing exploits such as buffer overflow can cause server-running software to get confused and fill the disk space or consume all available memory or CPU time.

Other kinds of DoS rely primarily on brute force, flooding the target with an overwhelming flux of packets, oversaturating its connection bandwidth or depleting the target's system resources. Bandwidth-saturating floods rely on the attacker having higher bandwidth available than the victim; a common way of achieving this today is via distributed denial-of-service, employing a botnet. Another target of DDoS attacks may be to produce added costs for the application operator, when the latter uses resources based on cloud computing. In this case normally application used resources are tied to a needed Quality of Service level (e.g. responses should be less than 200 ms) and this rule is usually linked to automated software (e.g. Amazon CloudWatch[29]) to raise more virtual resources from the provider in order to meet the defined QoS levels for the increased requests.The main incentive behind such attacks may be to drive the application owner to raise the elasticity levels in order to handle the increased application traffic, in order to cause financial losses or force them to become less competitive. Other floods may use specific packet types or connection requests to saturate finite resources by, for example, occupying the maximum number of open connections or filling the victim's disk space with logs.

A "banana attack" is another particular type of DoS. It involves redirecting outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets. A LAND attack is of this type.

An attacker with shell-level access to a victim's computer may slow it until it is unusable or crash it by using a fork bomb.

A kind of application-level DoS attack is XDoS (or XML DoS) which can be controlled by modern web application firewalls (WAFs).

Degradation-of-service attacks

"Pulsing" zombies are compromised computers that are directed to launch intermittent and short-lived floodings of victim websites with the intent of merely slowing it rather than crashing it. This type of attack, referred to as "degradation-of-service" rather than "denial-of-service", can be more difficult to detect than regular zombie invasions and can disrupt and hamper connection to websites for prolonged periods of time, potentially causing more disruption than concentrated floods.[30][31] Exposure of degradation-of-service attacks is complicated further by the matter of discerning whether the server is really being attacked or under normal traffic loads.[32]

Denial-of-service Level II

The goal of DoS L2 (possibly DDoS) attack is to cause a launching of a defense mechanism which blocks the network segment from which the attack originated. In case of distributed attack or IP header modification (that depends on the kind of security behavior) it will fully block the attacked network from the Internet, but without system crash.[22]

Distributed DoS attack

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.[9] Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic. A botnet is a network of zombie computers programmed to receive commands without the owners' knowledge.[33] When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This, after all, will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

A system may also be compromised with a trojan, allowing the attacker to download a zombie agent, or the trojan may contain one. Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web. Stacheldraht is a classic example of a DDoS tool. It uses a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.[27] In some cases a machine may become part of a DDoS attack with the owner's consent, for example, in Operation Payback, organized by the group Anonymous. These attacks can use different types of internet packets such as: TCP, UDP, ICMP etc.

These collections of systems compromisers are known as botnets / rootservers. DDoS tools like Stacheldraht still use classic DoS attack methods centered on IP spoofing and amplification like smurf attacks and fraggle attacks (these are also known as bandwidth consumption attacks). SYN floods (also known as resource starvation attacks) may also be used. Newer tools can use DNS servers for DoS purposes. Unlike MyDoom's DDoS mechanism, botnets can be turned against any IP address. Script kiddies use them to deny the availability of well known websites to legitimate users.[34] More sophisticated attackers use DDoS tools for the purposes of extortion – even against their business rivals.[35]

Simple attacks such as SYN floods may appear with a wide range of source IP addresses, giving the appearance of a well distributed DoS. These flood attacks do not require completion of the TCP three way handshake and attempt to exhaust the destination SYN queue or the server bandwidth. Because the source IP addresses can be trivially spoofed, an attack could come from a limited set of sources, or may even originate from a single host. Stack enhancements such as syn cookies may be effective mitigation against SYN queue flooding, however complete bandwidth exhaustion may require involvement.

If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a denial-of-service attack. On the other hand, if an attacker uses many systems to simultaneously launch attacks against a remote host, this would be classified as a DDoS attack.

It has been reported that there are new attacks from internet of things which have been involved in denial of service attacks. [36] In one noted attack that was made peaked at around 20,000 requests per second which came from around 900 CCTV cameras. [37]

UK's GCHQ has tools built for DDoS, named PREDATORS FACE and ROLLING THUNDER.[28]

DDoS extortion

In 2015, DDoS botnets such as DD4BC grew in prominence, taking aim at financial institutions.[38] Cyber-extortionists typically begin with a low-level attack and a warning that a larger attack will be carried out if a ransom is not paid in Bitcoin.[39] Security experts recommend targeted websites to not pay the ransom. The attackers tend to get into an extended extortion scheme once they recognize that the target is ready to pay.[40]

HTTP POST DoS attack

First discovered in 2009, the HTTP POST attack sends a complete, legitimate HTTP POST header, which includes a 'Content-Length' field to specify the size of the message body to follow. However, the attacker then proceeds to send the actual message body at an extremely slow rate (e.g. 1 byte/110 seconds). Due to the entire message being correct and complete, the target server will attempt to obey the 'Content-Length' field in the header, and wait for the entire body of the message to be transmitted, which can take a very long time. The attacker establishes hundreds or even thousands of such connections, until all resources for incoming connections on the server (the victim) are used up, hence making any further (including legitimate) connections impossible until all data has been sent. It is notable that unlike many other (D)DoS attacks, which try to subdue the server by overloading its network or CPU, a HTTP POST attack targets the *logical* resources of the victim, which means the victim would still have enough network bandwidth and processing power to operate.[41] Further combined with the fact that Apache will, by default, accept requests up to 2GB in size, this attack can be particularly powerful. HTTP POST attacks are difficult to differentiate from legitimate connections, and are therefore able to bypass some protection systems. OWASP, an open source web application security project, has released a testing tool (https://www.owasp.org/index.php/OWASP_HTTP_Post_Tool) to test the security of servers against this type of attacks.

Internet Control Message Protocol (ICMP) flood

A smurf attack relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The attacker will send large numbers of IP packets with the source address faked to appear to be the address of the victim. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This overloads the victim computer and can even make it unusable during such attack.[42]

Ping flood is based on sending the victim an overwhelming number of ping packets, usually using the "ping" command from Unix-like hosts (the -t flag on Windows systems is much less capable of overwhelming a target, also the -l (size) flag does not allow sent packet size greater than 65500 in Windows). It is very simple to launch, the primary requirement being access to greater bandwidth than the victim.

Ping of death is based on sending the victim a malformed ping packet, which will lead to a system crash on a vulnerable system.

The BlackNurse attack is an example of an attack taking advantage of the required Destination Port Unreachable ICMP packets.

Nuke

A Nuke is an old denial-of-service attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.

A specific example of a nuke attack that gained some prominence is the WinNuke, which exploited the vulnerability in the NetBIOS handler in Windows 95. A string of out-of-band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a Blue Screen of Death (BSOD).

Peer-to-peer attacks

Attackers have found a way to exploit a number of bugs in peer-to-peer servers to initiate DDoS attacks. The most aggressive of these peer-to-peer-DDoS attacks exploits DC++. With peer-to-peer there is no botnet and the attacker does not have to communicate with the clients it subverts. Instead, the attacker acts as a "puppet master," instructing clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead.[43][44][45]

Permanent denial-of-service attacks

Permanent denial-of-service (PDoS), also known loosely as phlashing,[46] is an attack that damages a system so badly that it requires replacement or reinstallation of hardware.[47] Unlike the distributed denial-of-service attack, a PDoS attack exploits security flaws which allow remote administration on the management interfaces of the victim's hardware, such as routers, printers, or other networking hardware. The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt, or defective firmware image—a process which when done legitimately is known as *flashing*. This therefore "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced.

The PDoS is a pure hardware targeted attack which can be much faster and requires fewer resources than using a botnet or a root/vserver in a DDoS attack. Because of these features, and the potential and high probability of security exploits on Network Enabled Embedded Devices (NEEDs), this technique has come to the attention of numerous hacking communities. BrickerBot, a piece of malware that targeted Internet of Things devices, used PDoS attacks to disable its targets.[48]

PhlashDance is a tool created by Rich Smith (an employee of Hewlett-Packard's Systems Security Lab) used to detect and demonstrate PDoS vulnerabilities at the 2008 EUSecWest Applied Security Conference (http://eusecwest.com/) in London.[49]

Reflected / spoofed attack

A distributed denial-of-service attack may involve sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target. (This reflected attack form is sometimes called a "DRDOS".[50])

ICMP Echo Request attacks (Smurf attack) can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mis-configured networks, thereby enticing hosts to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack.

Amplification

Amplification attacks are used to magnify the bandwidth that is sent to a victim. This is typically done through publicly accessible DNS servers that are used to cause congestion on the target system using DNS response traffic. Many services can be exploited to act as reflectors, some harder to block than others.[51] US-CERT have observed that different services implies in different amplification factors, as tabulated below:[52]

UDP-based Amplification Attacks

Protocol	Bandwidth Amplification Factor
Memcached	50000 (fixed in version 1.5.6)[53]
NTP	556.9 (fixed in version 4.2.7p26)[54]
CharGen	358.8
DNS	up to 179 [55]
QOTD	140.3
Quake Network Protocol	63.9 (fixed in version 71)
BitTorrent	4.0 - 54.3 [56] (fixed in libuTP since 2015)
SSDP	30.8
Kad	16.3
SNMPv2	6.3
Steam Protocol	5.5
NetBIOS	3.8

DNS amplification attacks involve a new mechanism that increased the amplification effect, using a much larger list of DNS servers than seen earlier. The process typically involves an attacker sending a DNS name look up request to a public DNS server, spoofing the source IP address of the targeted victim. The attacker tries to request as much information as possible, thus amplifying the DNS response that is sent to the targeted victim. Since the size of the request is significantly smaller than the response, the attacker is easily able to increase the amount of traffic directed at the target.[57][58] SNMP and NTP can also be exploited as reflector in an amplification attack.

An example of an amplified DDoS attack through the Network Time Protocol (NTP) is through a command called

monlist, which sends the details of the last 600 hosts that have requested the time from the NTP server back to the requester. A small request to this time server can be sent using a spoofed source IP address of some victim, which results in a response 556.9 times the size of the request being sent to the victim. This becomes amplified when using botnets that all send requests with the same spoofed IP source, which will result a massive amount of data being sent back to the victim.

It is very difficult to defend against these types of attacks because the response data is coming from legitimate servers. These attack requests are also sent through UDP, which does not require a connection to the server. This means that the source IP is not verified when a request is received by the server. In order to bring awareness of these vulnerabilities, campaigns have been started that are dedicated to finding amplification vectors which has led to people fixing their resolvers or having the resolvers shut down completely.

Mirai botnet

This attack works by using a worm to infect hundreds of thousands of IoT devices across the internet. The worm propagates through networks and systems taking control of poorly protected IoT devices such as thermostats, Wi-Fi enabled clocks and washing machines.[59] When the device becomes enslaved usually the owner or user will have no immediate indication. The IoT device itself is not the direct target of the attack, it is used as a part of a larger attack.[60] These newly enslaved devices are called slaves or bots. Once the hacker has acquired the desired number of bots, they instruct the bots to try and contact an ISP. In October 2016, a Mirai botnet attacked Dyn which is the ISP for sites such as Twitter, Netflix, etc.[59] As soon as this occurred, these websites were all unreachable for several hours. This type of attack is not physically damaging, but it will certainly be costly for any large internet companies that get attacked.

R-U-Dead-Yet? (RUDY)

RUDY (https://sourceforge.net/projects/r-u-dead-yet/) attack targets web applications by starvation of available sessions on the web server. Much like Slowloris, RUDY keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

Shrew attack

The shrew attack is a denial-of-service attack on the Transmission Control Protocol. It uses short synchronized bursts of traffic to disrupt TCP connections on the same link, by exploiting a weakness in TCP's re-transmission timeout mechanism.[61]

Slow Read attack

A slow read attack sends legitimate application layer requests, but reads responses very slowly, thus trying to exhaust the server's connection pool. It is achieved by advertising a very small number for the TCP Receive Window size, and at the same time emptying clients' TCP receive buffer slowly, which causes a very low data flow rate.

Sophisticated low-bandwidth Distributed Denial-of-Service Attack

A sophisticated low-bandwidth DDoS attack is a form of DoS that uses less traffic and increases their effectiveness by aiming at a weak point in the victim's system design, i.e., the attacker sends traffic consisting of complicated requests to the system.[62] Essentially, a sophisticated DDoS attack is lower in cost due to its use of less traffic, is smaller in size making it more difficult to identify, and it has the ability to hurt systems which are protected by flow control mechanisms.[62][63]

(S)SYN flood

A SYN flood occurs when a host sends a flood of TCP/SYN packets, often with a forged sender address. Each of these packets are handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet). However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server can make, keeping it from responding to legitimate requests until after the attack ends.[64]

Teardrop attacks

A teardrop attack involves sending mangled IP fragments with overlapping, oversized payloads to the target machine. This can crash various operating systems because of a bug in their TCP/IP fragmentation re-assembly code.[65] Windows 3.1x, Windows 95 and Windows NT operating systems, as well as versions of Linux prior to versions 2.0.32 and 2.1.63 are vulnerable to this attack.

(Although in September 2009, a vulnerability in Windows Vista was referred to as a "teardrop attack", this targeted SMB2 which is a higher layer than the TCP packets that teardrop used).[66][67]

One of the fields in an IP header is the “fragment offset” field, indicating the starting position, or offset, of the data contained in a fragmented packet relative to the data in the original packet. If the sum of the offset and size of one fragmented packet differs from that of the next fragmented packet, the packets overlap. When this happens, a server vulnerable to teardrop attacks is unable to reassemble the packets - resulting in a denial-of-service condition.

Telephony denial-of-service (TDoS)

Voice over IP has made abusive origination of large numbers of telephone voice calls inexpensive and readily automated while permitting call origins to be misrepresented through caller ID spoofing.

According to the US Federal Bureau of Investigation, telephony denial-of-service (TDoS) has appeared as part of various fraudulent schemes:

- A scammer contacts the victim's banker or broker, impersonating the victim to request a funds transfer. The banker's attempt to contact the victim for verification of the transfer fails as the victim's telephone lines are being flooded with thousands of bogus calls, rendering the victim unreachable.[68]
- A scammer contacts consumers with a bogus claim to collect an outstanding payday loan for thousands of dollars. When the consumer objects, the scammer retaliates by flooding the victim's employer with thousands of automated calls. In some cases, displayed caller ID is spoofed to impersonate police or law

enforcement agencies.[69]

- A scammer contacts consumers with a bogus debt collection demand and threatens to send police; when the victim balks, the scammer floods local police numbers with calls on which caller ID is spoofed to display the victims number. Police soon arrive at the victim's residence attempting to find the origin of the calls.

Telephony denial-of-service can exist even without Internet telephony. In the 2002 New Hampshire Senate election phone jamming scandal, telemarketers were used to flood political opponents with spurious calls to jam phone banks on election day. Widespread publication of a number can also flood it with enough calls to render it unusable, as happened by accident in 1981 with multiple +1-area code-867-5309 subscribers inundated by hundreds of misdialed calls daily in response to the song 867-5309/Jenny.

TDoS differs from other telephone harassment (such as prank calls and obscene phone calls) by the number of calls originated; by occupying lines continuously with repeated automated calls, the victim is prevented from making or receiving both routine and emergency telephone calls.

Related exploits include SMS flooding attacks and black fax or fax loop transmission.

UPnP attack

This attack uses an existing vulnerability in Universal Plug and Play (UPnP) protocol to get around a considerable amount of the present defense methods and flood a target's network and servers. The attack is based on a DNS amplification technique, but the attack mechanism is a UPnP router which forwards requests from one outer source to another disregarding UPnP behavior rules. Using the UPnP router returns the data on an unexpected UDP port from a bogus IP address, making it harder to take simple action to shut down the traffic flood. According to the Imperva researchers, the most effective way to stop this attack is for companies to lock down UPnP routers.[70][71]

Defense techniques

Defensive responses to denial-of-service attacks typically involve the use of a combination of attack detection, traffic classification and response tools, aiming to block traffic that they identify as illegitimate and allow traffic that they identify as legitimate.[72] A list of prevention and response tools is provided below:

Application front end hardware

Application front-end hardware is intelligent hardware placed on the network before traffic reaches the servers. It can be used on networks in conjunction with routers and switches. Application front end hardware analyzes data packets as they enter the system, and then identifies them as priority, regular, or dangerous. There are more than 25 bandwidth management vendors.

Application level Key Completion Indicators

Approaches to DDoS attacks against cloud-based applications may be based on an application layer analysis, indicating whether incoming bulk traffic is legitimate and thus triggering elasticity decisions without the economical implications of a DDoS attack.[73] These approaches mainly rely on an identified path of value inside the application and monitor the progress of requests on this path, through markers called Key Completion

Indicators.[74]

In essence, these technique are statistical methods of assessing the behavior of incoming requests to detect if something unusual or abnormal is going on.

An analogy is to a bricks-and-mortar department store where customers spend, on average, a known percentage of their time on different activities such as picking up items and examining them, putting them back, filling a basket, waiting to pay, paying, and leaving. These high-level activities correspond to the Key Completion Indicators in a service or site, and once normal behavior is determined, abnormal behavior can be identified. If a mob of customers arrived in store and spent all their time picking up items and putting them back, but never made any purchases, this could be flagged as unusual behavior.

The department store can attempt to adjust to periods of high activity by bringing in a reserve of employees at short notice. But if it did this routinely, were a mob to start showing up but never buying anything, this could ruin the store with the extra employee costs. Soon the store would identify the mob activity and scale back the number of employees, recognising that the mob provides no profit and should not be served. While this may make it more difficult for legitimate customers to get served during the mob's presence, it saves the store from total ruin.

In the case of elastic cloud services where a huge and abnormal additional workload may incur significant charges from the cloud service provider, this technique can be used to scale back or even stop the expansion of server availability to protect from economic loss.

Blackholing and sinkholing

With blackhole routing, all the traffic to the attacked DNS or IP address is sent to a "black hole" (null interface or a non-existent server). To be more efficient and avoid affecting network connectivity, it can be managed by the ISP.[75]

A DNS sinkhole routes traffic to a valid IP address which analyzes traffic and rejects bad packets. Sinkholing is not efficient for most severe attacks.

IPS based prevention

Intrusion prevention systems (IPS) are effective if the attacks have signatures associated with them. However, the trend among the attacks is to have legitimate content but bad intent. Intrusion-prevention systems which work on content recognition cannot block behavior-based DoS attacks.[22]

An ASIC based IPS may detect and block denial-of-service attacks because they have the processing power and the granularity to analyze the attacks and act like a circuit breaker in an automated way.[22]

A rate-based IPS (RBIPS) must analyze traffic granularly and continuously monitor the traffic pattern and determine if there is traffic anomaly. It must let the legitimate traffic flow while blocking the DoS attack traffic.[76]

DDS based defense

More focused on the problem than IPS, a DoS defense system (DDS) can block connection-based DoS attacks and those with legitimate content but bad intent. A DDS can also address both protocol attacks (such as teardrop and ping of death) and rate-based attacks (such as ICMP floods and SYN floods).

Firewalls

In the case of a simple attack, a firewall could have a simple rule added to deny all incoming traffic from the attackers, based on protocols, ports or the originating IP addresses.

More complex attacks will however be hard to block with simple rules: for example, if there is an ongoing attack on port 80 (web service), it is not possible to drop all incoming traffic on this port because doing so will prevent the server from serving legitimate traffic.[77] Additionally, firewalls may be too deep in the network hierarchy, with routers being adversely affected before the traffic gets to the firewall. Also, many security tools still do not support IPv6 or may not be configured properly, so the firewalls often might get bypassed during the attacks.[78]

Routers

Similar to switches, routers have some rate-limiting and ACL capability. They, too, are manually set. Most routers can be easily overwhelmed under a DoS attack. Cisco IOS has optional features that can reduce the impact of flooding.[79]

Switches

Most switches have some rate-limiting and ACL capability. Some switches provide automatic and/or system-wide rate limiting, traffic shaping, delayed binding (TCP splicing), deep packet inspection and Bogon filtering (bogus IP filtering) to detect and remediate DoS attacks through automatic rate filtering and WAN Link failover and balancing.[22]

These schemes will work as long as the DoS attacks can be prevented by using them. For example, SYN flood can be prevented using delayed binding or TCP splicing. Similarly content based DoS may be prevented using deep packet inspection. Attacks originating from dark addresses or going to dark addresses can be prevented using bogon filtering. Automatic rate filtering can work as long as set rate-thresholds have been set correctly. Wan-link failover will work as long as both links have DoS/DDoS prevention mechanism.[22]

Upstream filtering

All traffic is passed through a "cleaning center" or a "scrubbing center" via various methods such as proxies, tunnels, digital cross connects, or even direct circuits, which separates "bad" traffic (DDoS and also other common internet attacks) and only sends good traffic beyond to the server. The provider needs central connectivity to the Internet to manage this kind of service unless they happen to be located within the same facility as the "cleaning center" or "scrubbing center". DDoS attacks can overwhelm any type of hardware firewall, and passing malicious traffic through large and mature networks becomes more and more effective and economically sustainable against DDoS.[80]

Unintentional denial-of-service

An unintentional denial-of-service can occur when a system ends up denied, not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity. This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a news story. The result is that a significant proportion of the primary site's regular users – potentially hundreds of thousands of people – click that link in the space of a few hours, having the same effect on the target website as a DDoS attack. A VIPDoS is the same, but specifically when the link was posted by a celebrity.

When Michael Jackson died in 2009, websites such as Google and Twitter slowed down or even crashed.[81] Many sites' servers thought the requests were from a virus or spyware trying to cause a denial-of-service attack, warning users that their queries looked like "automated requests from a computer virus or spyware application".[82]

News sites and link sites – sites whose primary function is to provide links to interesting content elsewhere on the Internet – are most likely to cause this phenomenon. The canonical example is the Slashdot effect when receiving traffic from Slashdot. It is also known as "the Reddit hug of death" and "the Digg effect".

Routers have also been known to create unintentional DoS attacks, as both D-Link and Netgear routers have overloaded NTP servers by flooding NTP servers without respecting the restrictions of client types or geographical limitations.

Similar unintentional denials-of-service can also occur via other media, e.g. when a URL is mentioned on television. If a server is being indexed by Google or another search engine during peak periods of activity, or does not have a lot of available bandwidth while being indexed, it can also experience the effects of a DoS attack.[22]

Legal action has been taken in at least one such case. In 2006, Universal Tube & Rollform Equipment Corporation sued YouTube: massive numbers of would-be youtube.com users accidentally typed the tube company's URL, utube.com. As a result, the tube company ended up having to spend large amounts of money on upgrading their bandwidth.[83] The company appears to have taken advantage of the situation, with utube.com now containing ads for advertisement revenue.

In March 2014, after Malaysia Airlines Flight 370 went missing, DigitalGlobe launched a crowdsourcing service on which users could help search for the missing jet in satellite images. The response overwhelmed the company's servers.[84]

An unintentional denial-of-service may also result from a prescheduled event created by the website itself, as was the case of the Census in Australia in 2016.[85] This could be caused when a server provides some service at a specific time. This might be a university website setting the grades to be available where it will result in many more login requests at that time than any other.

Side effects of attacks

Backscatter

In computer network security, backscatter is a side-effect of a spoofed denial-of-service attack. In this kind of attack, the attacker spoofs (or forges) the source address in IP packets sent to the victim. In general, the victim machine cannot distinguish between the spoofed packets and legitimate packets, so the victim responds to the spoofed packets as it normally would. These response packets are known as backscatter.[86]

If the attacker is spoofing source addresses randomly, the backscatter response packets from the victim will be sent back to random destinations. This effect can be used by network telescopes as indirect evidence of such attacks.

The term "backscatter analysis" refers to observing backscatter packets arriving at a statistically significant portion of the IP address space to determine characteristics of DoS attacks and victims.

Legality

Many jurisdictions have laws under which denial-of-service attacks are illegal.

Numerous websites offering tools to conduct a DDoS attack were seized by the FBI under the Computer Fraud and Abuse Act.[87]

- In the US, denial-of-service attacks may be considered a federal crime under the Computer Fraud and Abuse Act with penalties that include years of imprisonment.[88] The Computer Crime and Intellectual Property Section of the US Department of Justice handles cases of (D)DoS.
- In European countries, committing criminal denial-of-service attacks may, as a minimum, lead to arrest.[89] The United Kingdom is unusual in that it specifically outlawed denial-of-service attacks and set a maximum penalty of 10 years in prison with the Police and Justice Act 2006, which amended Section 3 of the Computer Misuse Act 1990.[90]
- In January 2019, Europol announced that “actions are currently underway worldwide to track down the users” of Webstresser.org, a former DDoS marketplace that was shut down in April 2018 as part of Operation Power Off.[91] Europol said UK police were conducting a number of “live operations” targeting over 250 users of Webstresser and other DDoS services.[92]

On January 7, 2013, Anonymous posted a petition on the whitehouse.gov site asking that DDoS be recognized as a legal form of protest similar to the Occupy protests, the claim being that the similarity in purpose of both are same.[93][94]

See also

- Application layer DDoS attack
- BASHLITE
- Billion laughs
- Botnet
- Blaster (computer worm)
- Dendroid (malware)
- Fork bomb
- High Orbit Ion Cannon (HOIC)
- Hit-and-run DDoS
- Industrial espionage
- Infinite loop

- Intrusion detection system
- Low Orbit Ion Cannon (LOIC)
- Network intrusion detection system
- October 2016 Dyn cyberattack
- Paper terrorism
- Project Shield
- ReDoS
- Resource exhaustion attack
- SlowDroid
- Slowloris (computer security)
- UDP Unicorn
- Virtual sit-in
- Warzapping
- Wireless signal jammer
- XML denial-of-service attack
- Xor DDoS
- Zemra
- Zombie (computer science)

References

1. "Understanding Denial-of-Service Attacks" (https://www.us-cert.gov/ncas/tips/ST04-015). US-CERT. 6 February 2013. Retrieved 26 May 2016.
2. Prince, Matthew (25 April 2016). "Empty DDoS Threats: Meet the Armada Collective" (https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/). *CloudFlare*. Retrieved 18 May 2016.
3. "Brand.com President Mike Zammuto Reveals Blackmail Attempt" (https://web.archive.org/web/20140311070205/http://www.interpacket.com/42882/brand-com-victim-blackmail-attempt-says-president-mike-zammuto/). 5 March 2014. Archived from the original (http://www.interpacket.com/42882/brand-com-victim-blackmail-attempt-says-president-mike-zammuto/) on 11 March 2014.
4. "Brand.com's Mike Zammuto Discusses Meetup.com Extortion" (https://web.archive.org/web/20140513044100/http://dailyglobe.com/61817/brand-coms-mike-zammuto-discusses-meetup-com-extortion/). 5 March 2014. Archived from the original (http://dailyglobe.com/61817/brand-coms-mike-zammuto-discusses-meetup-com-extortion/) on 13 May 2014.
5. "The Philosophy of Anonymous" (http://www.radicalphilosophy.com/article/the-philosophy-of-anonymous). Radicalphilosophy.com. 2010-12-17. Retrieved 2013-09-10.
6. Smith, Steve. "5 Famous Botnets that held the internet hostage" (https://tqaweekly.com/episodes/season5/tqa-se5ep11.php). tqaweekly. Retrieved November 20, 2014.
7. https://arstechnica.com/information-technology/2018/03/us-service-provider-survives-the-biggest-recorded-ddos-in-history/
8. Ranger, Steve. "GitHub hit with the largest DDoS attack ever seen | ZDNet" (https://www.zdnet.com/article/github-was-hit-with-the-largest-ddos-attack-ever-seen/). *ZDNet*. Retrieved 2018-10-14.
9. Taghavi Zargar, Saman (November 2013). "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks" (http://d-scholarship.pitt.edu/19225/1/FinalVersion.pdf) (PDF). IEEE COMMUNICATIONS SURVEYS & TUTORIALS. pp. 2046–2069. Retrieved 2014-03-07.

10. Khalifeh,, Soltanian, Mohammad Reza. *Theoretical and experimental methods for defending against DDoS attacks* (https://www.worldcat.org/oclc/930795667). Amiri, Iraj Sadegh, 1977-. Waltham, MA. ISBN 0128053992. OCLC 930795667 (https://www.worldcat.org/oclc/930795667).
11. "Layer Seven DDoS Attacks". *Infosec Institute*.
12. Raghavan, S.V. (2011). *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks*. Springer. ISBN 9788132202776.
13. Goodin, Dan (28 September 2016). "Record-breaking DDoS reportedly delivered by >145k hacked cameras" (https://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/). Ars Technica. Archived (https://web.archive.org/web/20161002000235/http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/) from the original on 2 October 2016.
14. Khandelwal, Swati (26 September 2016). "World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices" (https://thehackernews.com/2016/09/ddos-attack-iot.html). The Hacker News. Archived (https://web.archive.org/web/20160930031903/https://thehackernews.com/2016/09/ddos-attack-iot.html) from the original on 30 September 2016.
15. Kumar,, Bhattacharyya, Dhruba. *DDoS attacks : evolution, detection, prevention, reaction, and tolerance* (https://www.worldcat.org/oclc/948286117). Kalita, Jugal Kumar,. Boca Raton, FL. ISBN 9781498729659. OCLC 948286117 (https://www.worldcat.org/oclc/948286117).
16. Lee, Newton (2013). *Counterterrorism and Cybersecurity: Total Information Awareness*. Springer. ISBN 9781461472056.
17. "Gartner Says 25 Percent of Distributed Denial of Services Attacks in 2013 Will Be Application - Based" (http://www.gartner.com/newsroom/id/2344217). *Gartner*. 21 February 2013. Retrieved 28 January 2014.
18. Ginovsky, John (27 January 2014). "What you should know about worsening DDoS attacks" (https://web.archive.org/web/20140209003822/http://ababj.com/component/k2/item/4354-what-you-should-know-about-worsening-ddos-attacks). *ABA Banking Journal*. Archived from the original (http://www.ababj.com/component/k2/item/4354-what-you-should-know-about-worsening-ddos-attacks) on 2014-02-09.
19. "Q4 2014 State of the Internet - Security Report: Numbers - The Akamai Blog" (https://blogs.akamai.com/2015/01/q4-2014-state-of-the-internet---security-report-some-numbers.html). *blogs.akamai.com*.
20. Ali, Junade (23 November 2017). "The New DDoS Landscape" (https://blog.cloudflare.com/the-new-ddos-landscape/). *Cloudflare Blog*.
21. Higgins, Kelly Jackson (17 October 2013). "DDoS Attack Used 'Headless' Browser In 150-Hour Siege" (https://web.archive.org/web/20140122165039/http://www.darkreading.com/attacks-breaches/ddos-attack-used-headless-browsers-in-15/240162777). *Dark Reading*. InformationWeek. Archived from the original (http://www.darkreading.com/attacks-breaches/ddos-attack-used-headless-browsers-in-15/240162777) on January 22, 2014. Retrieved 28 January 2014.
22. Kiyuna and Conyers (2015). *Cyberwarfare Sourcebook*. ISBN 1329063945.
23. Ilascu, Ionut (Aug 21, 2014). "38-Day Long DDoS Siege Amounts to Over 50 Petabits in Bad Traffic" (https://news.softpedia.com/news/38-Day-Long-DDoS-Siege-Amounts-to-Over-50-Petabits-in-Bad-Traffic-455722.shtml). Softpedia News. Retrieved 29 July 2018.
24. Gold, Steve (21 August 2014). "Video games company hit by 38-day DDoS attack" (http://www.scmagazineuk.com/video-games-company-hit-by-38-day-ddos-attack/article/367329/). *SC Magazine UK*. Retrieved 4 February 2016.
25. Krebs, Brian (August 15, 2015). "Stress-Testing the Booter Services, Financially" (http://krebsonsecurity.com/2015/08/stress-testing-the-booter-services-financially/). *Krebs on Security*. Retrieved 2016-09-09.

26. McDowell, Mindi (November 4, 2009). "Cyber Security Tip ST04-015 - Understanding Denial-of-Service Attacks" (http://www.us-cert.gov/ncas/tips/st04-015). United States Computer Emergency Readiness Team. Archived (https://web.archive.org/web/20131104052804/http://www.us-cert.gov/ncas/tips/st04-015) from the original on 2013-11-04. Retrieved December 11, 2013.
27. Dittrich, David (December 31, 1999). "The "stacheldraht" distributed denial of service attack tool" (http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt). University of Washington. Retrieved 2013-12-11.
28. Glenn Greenwald (2014-07-15). "HACKING ONLINE POLLS AND OTHER WAYS BRITISH SPIES SEEK TO CONTROL THE INTERNET" (https://theintercept.com/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/). The Intercept_. Retrieved 2015-12-25.
29. "Amazon CloudWatch" (http://aws.amazon.com/cloudwatch/). *Amazon Web Services, Inc*.
30. *Encyclopaedia Of Information Technology*. Atlantic Publishers & Distributors. 2007. p. 397. ISBN 81-269-0752-5.
31. Schwabach, Aaron (2006). *Internet and the Law*. ABC-CLIO. p. 325. ISBN 1-85109-731-7.
32. Lu, Xicheng; Wei Zhao (2005). *Networking and Mobile Computing*. Birkhäuser. p. 424. ISBN 3-540-28102-9.
33. "Has Your Website Been Bitten By a Zombie?" (http://blog.cloudbric.com/2015/08/has-your-website-been-bitten-by-zombie.html). Cloudbric. 3 August 2015. Retrieved 15 September 2015.
34. Boyle, Phillip (2000). "SANS Institute – Intrusion Detection FAQ: Distributed Denial of Service Attack Tools: n/a" (http://www.sans.org/resources/idfaq/trinoo.php). SANS Institute. Retrieved 2008-05-02.
35. Leyden, John (2004-09-23). "US credit card firm fights DDoS attack" (https://www.theregister.co.uk/2004/09/23/authorize_ddos_attack/). *The Register*. Retrieved 2011-12-02.
36. Swati Khandelwal (23 October 2015). "Hacking CCTV Cameras to Launch DDoS Attacks" (http://thehackernews.com/2015/10/cctv-camera-hacking.html). *The Hacker News*.
37. Zeifman, Igal; Gayer, Ofer; Wilder, Or (21 October 2015). "CCTV DDoS Botnet In Our Own Back Yard" (https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html). *incapsula.com*.
38. "Who's Behind DDoS Attacks and How Can You Protect Your Website?" (http://blog.cloudbric.com/2015/09/whos-behind-ddos-attacks-and-how-can.html). Cloudbric. 10 September 2015. Retrieved 15 September 2015.
39. Solon, Olivia (9 September 2015). "Cyber-Extortionists Targeting the Financial Sector Are Demanding Bitcoin Ransoms" (https://www.bloomberg.com/news/articles/2015-09-09/bitcoin-ddos-ransom-demands-raise-dd4bc-profile?mod=djemRiskCompliance). Bloomberg. Retrieved 15 September 2015.
40. Greenberg, Adam (14 September 2015). "Akamai warns of increased activity from DDoS extortion group" (http://www.scmagazineuk.com/akamai-warns-of-increased-activity-from-ddos-extortion-group/article/438333/). SC Magazine. Retrieved 15 September 2015.
41. "OWASP Plan - Strawman - Layer_7_DDOS.pdf" (https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf) (PDF). *Open Web Application Security Project*. 18 March 2014. Retrieved 18 March 2014.
42. "Types of DDoS Attacks" (https://web.archive.org/web/20100914222536/http://anml.iu.edu/ddos/types.html). *Distributed Denial of Service Attacks(DDoS) Resources, Pervasive Technology Labs at Indiana University*. Advanced Networking Management Lab (ANML). December 3, 2009. Archived from the original (http://anml.iu.edu/ddos/types.html) on 2010-09-14. Retrieved December 11, 2013.
43. Paul Sop (May 2007). "Prolexic Distributed Denial of Service Attack Alert" (https://web.archive.org/web/20070803175513/http://www.prolexic.com/news/20070514-alert.php). *Prolexic Technologies Inc*. Prolexic Technologies Inc. Archived from the original (http://www.prolexic.com/news/20070514-alert.php) on 2007-08-03. Retrieved 2007-08-22.

44. Robert Lemos (May 2007). "Peer-to-peer networks co-opted for DOS attacks" (http://www.securityfocus.com/news/11466). SecurityFocus. Retrieved 2007-08-22.
45. Fredrik Ullner (May 2007). "Denying distributed attacks" (http://dcpp.wordpress.com/2007/05/22/denying-distributed-attacks/). DC++: Just These Guys, Ya Know?. Retrieved 2007-08-22.
46. Leyden, John (2008-05-21). "Phlashing attack thrashes embedded systems" (https://www.theregister.co.uk/2008/05/21/phlashing/). *The Register*. Retrieved 2009-03-07.
47. Jackson Higgins, Kelly (May 19, 2008). "Permanent Denial-of-Service Attack Sabotages Hardware" (https://web.archive.org/web/20081208002732/http://www.darkreading.com/security/management/showArticle.jhtml?articleID=211201088). Dark Reading. Archived from the original (http://www.darkreading.com/document.asp?doc_id=154270&WT.svl=news1_1) on December 8, 2008.
48. " "BrickerBot" Results In PDoS Attack" (https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/). *Radware*. Radware. May 4, 2017. Retrieved January 22, 2019.
49. "EUSecWest Applied Security Conference: London, U.K." (https://web.archive.org/web/20090201173324/http://eusecwest.com/speakers.html#PhlashDance) EUSecWest. 2008. Archived from the original (http://eusecwest.com/speakers.html#PhlashDance) on 2009-02-01.
50. Rossow, Christian (February 2014). "Amplification Hell: Revisiting Network Protocols for DDoS Abuse" (http://www.internetsociety.org/sites/default/files/01_5.pdf) (PDF). Internet Society. Retrieved 4 February 2016.
51. Paxson, Vern (2001). "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks" (http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html). ICIR.org.
52. "Alert (TA14-017A) UDP-based Amplification Attacks" (http://www.us-cert.gov/ncas/alerts/TA14-017A). US-CERT. July 8, 2014. Retrieved 2014-07-08.
53. "Memcached 1.5.6 Release Notes" (https://github.com/memcached/memcached/wiki/ReleaseNotes156). 2018-02-27. Retrieved 3 March 2018.
54. "DRDoS / Amplification Attack using ntpdc monlist command" (http://support.ntp.org/bin/view/Main/SecurityNotice#April_2010_DRDoS_Amplification_A). support.ntp.org. 2010-04-24. Retrieved 2014-04-13.
55. van Rijswijk-Deij, Roland (2014). "DNSSEC and its potential for DDoS attacks". *DNSSEC and its potential for DDoS attacks - a comprehensive measurement study*. ACM Press. pp. 449–460. doi:10.1145/2663716.2663731 (https://doi.org/10.1145%2F2663716.2663731). ISBN 9781450332132.
56. Adamsky, Florian (2015). "P2P File-Sharing in Hell: Exploiting BitTorrent Vulnerabilities to Launch Distributed Reflective DoS Attacks" (https://www.usenix.org/conference/woot15/workshop-program/presentation/p2p-file-sharing-hell-exploiting-bittorrent).
57. Vaughn, Randal; Evron, Gadi (2006). "DNS Amplification Attacks" (https://web.archive.org/web/20101214074629/http://www.isotf.org/news/DNS-Amplification-Attacks.pdf) (PDF). ISOTF. Archived from the original (http://www.isotf.org/news/DNS-Amplification-Attacks.pdf) (PDF) on 2010-12-14.
58. "Alert (TA13-088A) DNS Amplification Attacks" (http://www.us-cert.gov/ncas/alerts/TA13-088A). US-CERT. July 8, 2013. Retrieved 2013-07-17.
59. "DDoS in the IoT: Mirai and Other Botnets" (http://ieeexplore.ieee.org/document/7971869/). doi:10.1109/MC.2017.201 (https://doi.org/10.1109%2FMC.2017.201). Retrieved 2018-12-31.
60. Kuzmanovic, Aleksandar; Knightly, Edward W. (2003-08-25). "Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants" (http://dl.acm.org/citation.cfm?id=863955.863966). ACM: 75–86. doi:10.1145/863955.863966 (https://doi.org/10.1145%2F863955.863966). ISBN 1581137354.

61. Yu Chen; Kai Hwang; Yu-Kwong Kwok (2005). "Filtering of shrew DDoS attacks in frequency domain". *The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05)l*. pp. 8 pp. doi:10.1109/LCN.2005.70 (https://doi.org/10.1109%2FLCN.2005.70). ISBN 0-7695-2421-4.
62. Ben-Porat, U.; Bremler-Barr, A.; Levy, H. (2013-05-01). "Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks" (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6158635). *IEEE Transactions on Computers*. **62** (5): 1031–1043. doi:10.1109/TC.2012.49 (https://doi.org/10.1109%2FTC.2012.49). ISSN 0018-9340 (https://www.worldcat.org/issn/0018-9340).
63. orbitalsatelite. "Slow HTTP Test" (https://sourceforge.net/projects/slow-http-test/). *SourceForge*.
64. "TCP SYN Flooding Attacks and Common Mitigations" (http://tools.ietf.org/html/rfc4987). *Tools.ietf.org*. August 2007. RFC 4987 (https://tools.ietf.org/html/rfc4987). Retrieved 2011-12-02.
65. "CERT Advisory CA-1997-28 IP Denial-of-Service Attacks" (http://www.cert.org/historical/advisories/ca-1997-28.cfm). CERT. 1998. Retrieved July 18, 2014.
66. "Windows 7, Vista exposed to 'teardrop attack' " (http://www.zdnet.com/blog/security/windows-7-vista-exposed-to-teardrop-attack/4222). ZDNet. September 8, 2009. Retrieved 2013-12-11.
67. "Microsoft Security Advisory (975497): Vulnerabilities in SMB Could Allow Remote Code Execution" (http://www.microsoft.com/technet/security/advisory/975497.mspx). Microsoft.com. September 8, 2009. Retrieved 2011-12-02.
68. "FBI — Phony Phone Calls Distract Consumers from Genuine Theft" (https://www.fbi.gov/newark/press-releases/2010/nk051110.htm). FBI.gov. 2010-05-11. Retrieved 2013-09-10.
69. "Internet Crime Complaint Center's (IC3) Scam Alerts January 7, 2013" (http://www.ic3.gov/media/2013/130107.aspx). *IC3.gov*. 2013-01-07. Retrieved 2013-09-10.
70. "New DDoS Attack Method Leverages UPnP" (https://www.darkreading.com/new-ddos-attack-method-leverages-upnp/d/d-id/1331799). *Dark Reading*. Retrieved 2018-05-29.
71. "New DDoS Attack Method Demands a Fresh Approach to Amplification Assault Mitigation – Blog | Imperva" (https://www.imperva.com/blog/2018/05/new-ddos-attack-method-demands-a-fresh-approach-to-amplification-assault-mitigation/). *Blog | Imperva*. 2018-05-14. Retrieved 2018-05-29.
72. Loukas, G.; Oke, G. (September 2010) [August 2009]. "Protection Against Denial of Service Attacks: A Survey" (http://staffweb.cms.gre.ac.uk/~lg47/publications/LoukasOke-DoSSurveyComputerJournal.pdf) (PDF). *Comput. J.* **53** (7): 1020–1037. doi:10.1093/comjnl/bxp078 (https://doi.org/10.1093%2Fcomjnl%2Fbxp078).
73. Alqahtani, S.; Gamble, R. F. (1 January 2015). "DDoS Attacks in Service Clouds". *2015 48th Hawaii International Conference on System Sciences (HICSS)*: 5331–5340. doi:10.1109/HICSS.2015.627 (https://doi.org/10.1109%2FHICSS.2015.627).
74. Kousiouris, George (2014). "KEY COMPLETION INDICATORS:minimizing the effect of DoS attacks on elastic Cloud-based applications based on application-level markov chain checkpoints" (http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0004963006220628). *CLOSER Conference*. Retrieved 2015-05-24.
75. Patrikakis, C.; Masikos, M.; Zouraraki, O. (December 2004). "Distributed Denial of Service Attacks" (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html). *The Internet Protocol Journal*. **7** (4): 13–35.
76. Abante, Carl (March 2, 2013). "Relationship between Firewalls and Protection against DDoS" (http://www.ecommercewisdom.com/relationship-firewalls-protection-ddos/). *Ecommerce Wisdom*. Retrieved 2013-05-24.
77. Froutan, Paul (June 24, 2004). "How to defend against DDoS attacks" (http://www.computerworld.com/s/article/94014/How_to_defend_against_DDoS_attacks). *Computerworld*. Retrieved May 15, 2010.

78. "Cyber security vulnerability concerns skyrocket" (https://www.computerweekly.com/news/252445613/Cyber-security-vulnerability-concerns-skyrocket). *ComputerWeekly.com*. Retrieved 2018-08-13.
79. Suzen, Mehmet. "Some IoS tips for Internet Service (Providers)" (https://web.archive.org/web/20080910202908/http://mehmet.suzen.googlepages.com/qos_ios_dos_suzen2005.pdf) (PDF). Archived from the original (http://mehmet.suzen.googlepages.com/qos_ios_dos_suzen2005.pdf) (PDF) on 2008-09-10.
80. "DDoS Mitigation via Regional Cleaning Centers (Jan 2004)" (https://web.archive.org/web/20080921012859/http://research.sprintlabs.com/publications/uploads/RR04-ATL-013177.pdf) (PDF). *SprintLabs.com*. Sprint ATL Research. Archived from the original (https://research.sprintlabs.com/publications/uploads/RR04-ATL-013177.pdf) (PDF) on 2008-09-21. Retrieved 2011-12-02.
81. Shiels, Maggie (2009-06-26). "Web slows after Jackson's death" (http://news.bbc.co.uk/1/hi/8120324.stm). *BBC News*.
82. "We're Sorry. Automated Query error" (http://productforums.google.com/forum/?#!category-topic/websearch/unexpected-search-results/uFcXXixhiBw). *Google Product Forums › Google Search Forum*. Google.com. October 20, 2009. Retrieved 2012-02-11.
83. "YouTube sued by sound-alike site" (http://news.bbc.co.uk/2/hi/business/6108502.stm). *BBC News*. 2006-11-02.
84. Bill Chappell (12 March 2014). "People Overload Website, Hoping To Help Search For Missing Jet" (http://wnmufm.org/post/people-overload-website-hoping-help-search-missing-jet). NPR. Retrieved 4 February 2016.
85. Palmer, Daniel (19 August 2016). "Experts cast doubt on Census DDoS claims" (https://delimiter.com.au/2016/08/19/experts-cast-doubt-census-ddos-claims/). Delimiter. Retrieved 31 January 2018.
86. "Backscatter Analysis (2001)" (http://www.caida.org/publications/animations/). *Animations* (video). Cooperative Association for Internet Data Analysis. Retrieved December 11, 2013.
87. "FBI Seizes 15 DDoS-For-Hire Websites" (https://kotaku.com/fbi-seizes-15-ddos-for-hire-websites-1831239141). *Kotaku*. 6 January 2019.
88. "United States Code: Title 18,1030. Fraud and related activity in connection with computers | Government Printing Office" (http://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap47-sec1030.htm). www.gpo.gov. 2002-10-25. Retrieved 2014-01-15.
89. "International Action Against DD4BC Cybercriminal Group" (https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group). *EUROPOL*. 12 January 2016.
90. "Computer Misuse Act 1990" (http://www.legislation.gov.uk/ukpga/1990/18/section/3). *legislation.gov.uk — The National Archives, of UK*. 10 January 2008.
91. "Newsroom" (https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down). *Europol*. Retrieved 29 January 2019.
92. "Authorities across the world going after users of biggest DDoS-for-hire website" (https://www.europol.europa.eu/newsroom/news/authorities-across-world-going-after-users-of-biggest-ddos-for-hire-website). *Europol*. Retrieved 29 January 2019.
93. "Anonymous DDoS Petition: Group Calls On White House To Recognize Distributed Denial Of Service As Protest" (http://www.huffingtonpost.com/2013/01/12/anonymous-ddos-petition-white-house_n_2463009.html). HuffingtonPost.com. 2013-01-12.
94. "DDOS Attack: crime or virtual sit-in?" (https://www.youtube.com/watch?v=59AlNnX_Ksg). RT.com. YouTube.com. October 6, 2011.

Further reading

- Ethan Zuckerman; Hal Roberts; Ryan McGrady; Jillian York; John Palfrey (December 2011). "Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites" (https://www.webcitation.org/5ws9RPpXi?url=http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf) (PDF). The Berkman Center for Internet & Society at Harvard University. Archived from the original (http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf) (PDF) on 2011-03-02. Retrieved 2011-03-02.
- "DDOS Public Media Reports" (https://www.webcitation.org/5ws9nHATo?url=http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/DDoS%20Public%20Media%20Reports_0.xls). Harvard. Archived from the original (http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/DDoS%20Public%20Media%20Reports_0.xls) on 2011-03-02.
- PC World - Application Layer DDoS Attacks are Becoming Increasingly Sophisticated (http://www.pcworld.com/article/2056805/applicationlayer-ddos-attacks-are-becoming-increasingly-sophisticated.html)

External links

- RFC 4732 (https://tools.ietf.org/html/rfc4732) Internet Denial-of-Service Considerations
- Akamai State of the Internet Security Report (https://www.akamai.com/soti) - Quarterly Security and Internet trend statistics
- W3C The World Wide Web Security FAQ (http://www.w3.org/Security/Faq/wwwsf6.html)
- cert.org (http://www.cert.org/tech_tips/denial_of_service.html) CERT's Guide to DoS attacks. (historic document)
- ATLAS Summary Report (http://atlas.arbor.net/summary/dos) – Real-time global report of DDoS attacks.
- Low Orbit Ion Cannon (https://sourceforge.net/projects/loic0/) - The Well Known Network Stress Testing Tool
- High Orbit Ion Cannon (https://sourceforge.net/projects/high-orbit-ion-cannon/) - A Simple HTTP Flooder
- LOIC SLOW (https://sourceforge.net/projects/loicslow/) An Attempt to Bring SlowLoris and Slow Network Tools on LOIC
