DEFINITION

denial-of-service attack

By **Kevin Ferguson** | **Peter Loshin,** Former Senior Technology Editor

What is a denial-of-service attack?

A denial-of-service (DoS) attack is a security threat that occurs when an attacker makes it impossible for legitimate users to access computer systems, network, services or other information technology (IT) resources. Attackers in these types of attacks typically flood web servers, systems or networks with traffic that overwhelms the victim's resources and makes it difficult or impossible for anyone else to access them.

Restarting a system will usually fix an attack that crashes a server, but flooding attacks are more difficult to recover from. Recovering from a distributed DoS (DDoS) attack in which attack traffic comes from a large number of sources is even more difficult.

DoS and DDoS attacks often take advantage of vulnerabilities in networking protocols and how they handle network traffic. For example, an attacker might overwhelm the service by transmitting many packets to a vulnerable network service from different Internet Protocol (IP) addresses.

How does a DoS attack work?

DoS and DDoS attacks target one or more of the seven layers of the Open Systems Interconnection (OSI) model. The most common OSI targets include Layer 3 (network), Layer 4 (transport), Layer 6 (presentation) and Layer 7 (application).

Diagram of the layers of the Open Systems Interconnection model

Layers 3, 4, 6 and 7 are the most common layers for attacks of the Open Systems Interconnection model.

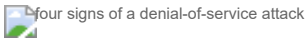
Malicious actors have different ways of attacking the OSI layers. Using User Datagram Protocol (UDP) packets is one common way. UDP speeds transmission transferring data before the receiving party sends its agreement. Another common attack method is SYN (synchronization) packet attacks. In these attacks, packets are sent to all open ports on a server, using spoofed, or fake, IP addresses. UDP and SYN attacks typically target OSI Layers 3 and 4.

Protocol handshakes launched from internet of things (IoT) devices are now commonly used to launch attacks on Layers 6 and 7. These attacks can be difficult to identify and preempt because IoT devices are everywhere and each is a discrete intelligent client.

Signs of a DoS attack

The United States Computer Emergency Readiness Team, also known as US-CERT, provides guidelines to determine when a DoS attack may be in progress. According to US-CERT, the following may indicate an attack is underway:

- slower or otherwise degraded network performance that is particularly noticeable when trying to access a website or open files on the network;
- inability to access a website; or
- more spam email than usual.


four signs of a denial-of-service attack

Learn the signs of a bot-driven denial-of-service attack.

Preventing a DoS attack

Experts recommend several strategies to defend against DoS and DDoS attacks, starting with preparing an incident response plan well in advance.

An enterprise that suspects a DoS attack is underway should contact its internet service provider (ISP) to determine whether slow performance or other indications are from an attack or some other factor. The ISP can reroute the malicious traffic to counter the attack. It can also use load balancers to mitigate the severity of the attack.

ISPs also have products that detect DoS attacks, as do some intrusion detection systems (IDSes), intrusion prevention systems (IPSes) and firewalls. Other strategies include contracting with a backup ISP and using cloud-based anti-DoS measures.

There have been instances where attackers have demanded payment from victims to end DoS or DDoS attacks, but financial profit is not usually the motive behind these attacks. In many cases, the attackers wish to harm the business or reputation of the organization or individual targeted in the attack.

Types of DoS attacks

DoS and DDoS attacks have a variety of methods of attack. Common types of denial-of-service attacks include the following:

- **Application layer.** These attacks generate fake traffic to internet application servers, especially domain name system (DNS) servers or Hypertext Transfer Protocol (HTTP) servers. Some application layer DoS attacks flood the target servers with network data; others target the victim's application server or protocol, looking for vulnerabilities.
- **Buffer overflow.** This type of attack is one that sends more traffic to a network resource than it was designed to handle.
- **DNS amplification.** In a DNS DoS attack, the attacker generates DNS requests that appear to have originated from an IP address in the targeted network and sends them to misconfigured DNS servers managed by third parties. The amplification occurs as the intermediate DNS servers respond to the fake DNS requests. The responses from intermediate DNS servers to the requests may contain more data than ordinary DNS responses, which requires more resources to process. This can result in legitimate users being denied access to the service.
- **Ping of death.** These attacks abuse the ping protocol by sending request messages with oversized payloads, causing the target systems to become overwhelmed, to stop responding to legitimate requests for service and to possibly crash the victim's systems.
- **State exhaustion.** These attacks -- also known as *Transmission Control Protocol (TCP) attacks* -- occur when an attacker targets the state tables held in firewalls, routers and other network devices and fills them with attack data. When these devices incorporate stateful inspection of network circuits, attackers may be able to fill the state tables by opening more TCP circuits than the victim's system can handle at once, preventing legitimate users from accessing the network resource.

- **SYN flood.** This attack abuses the TCP handshake protocol by which a client establishes a TCP connection with a server. In a SYN flood attack, the attacker directs a high-volume stream of requests to open TCP connections with the victim server with no intention of completing the circuits. A successful attack can deny legitimate users access to the targeted server.
- **Teardrop.** These attacks exploit flaws like how older operating systems (OSes) handled fragmented IP packets. The IP specification enables packet fragmentation when the packets are too large to be handled by intermediary routers, and it requires packet fragments to specify fragment offsets. In teardrop attacks, the fragment offsets are set to overlap each other. Hosts running affected OSes are then unable to reassemble the fragments, and the attack can crash the system.
- **Volumetric.** These DoS attacks use all the bandwidth available to reach network resources. To do this, attackers must direct a high volume of network traffic at the victim's systems. Volumetric DoS attacks flood a victim's devices with network packets using UDP or Internet Control Message Protocol (ICMP). These protocols require relatively little overhead to generate large volumes of traffic, while, at the same time, the victim's network devices are overwhelmed with network packets, trying to process the incoming malicious datagrams.

More on distributed denial-of-service attacks

Want to know more about DDoS attacks, where bad actors flood systems and networks from multiple sources? Check out the following articles:

DDoS mitigation strategies needed to maintain availability during pandemic

How an IoT botnet attacks with DDoS and infects devices

3 ways to prevent DDoS attacks on networks

How traffic scrubbing can guard against DDoS attacks

What is DDoS and how does it compare to DoS?

Many high-profile DoS attacks are actually distributed attacks, where the attack traffic comes from multiple attack systems. DoS attacks originating from one source or IP address can be easier to counter because defenders can block network traffic from the offending source. Attacks from multiple attacking systems are far more

difficult to detect and defend against. It can be difficult to differentiate legitimate traffic from malicious traffic and filter out malicious packets when they are being sent from IP addresses seemingly located all over the internet.

In a distributed denial-of-service attack, the attacker may use computers or other network-connected devices that have been infected by malware and made part of a botnet. DDoS attacks use command-and-control servers (C&C servers) to control the botnets that are part of the attack. The C&C servers dictate what kind of attack to launch, what types of data to transmit, and what systems or network connectivity resources to target with the attack.

History of denial-of-service attacks

DoS attacks on internet-connected systems have a long history that arguably started with the Robert Morris worm attack in 1988. In that attack, Morris, a graduate student at Massuchusetts Institute of Technology (MIT), released a self-reproducing piece of malware -- a worm -- that quickly spread through the internet and triggered buffer overflows and DoS attacks on the affected systems.

Those connected to the internet at the time were mostly research and academic institutions, but it was estimated that as many as 10% of the 60,000 systems in the U.S. were affected. Damage was estimated to be as high as $10 million, according to the U.S. General Accounting Office (GAO), now known as the Government Accountability Office. Prosecuted under the 1986 Computer Fraud and Abuse Act

(CFAA), Morris was sentenced to 400 community service hours and three years' probation. He was also fined $10,000.

DoS and DDoS attacks have become common since then. Some recent attacks include the following:

- **GitHub.** On Feb. 28, 2018, GitHub.com was unavailable because of a DDoS attack. GitHub said it was offline for under 10 minutes. The attack came "across tens of thousands of endpoints … that peaked at 1.35 terabits per second (Tbps) via 126.9 million packets per second," according to GitHub.
- **Imperva.** On April 30, 2019, network security vendor Imperva said it recorded a large DDoS attack against one of its clients. The attack peaked at 580 million packets per second but was mitigated by its DDoS protection software, the company said.
- **Amazon Web Services (AWS).** In the AWS Shield Threat Landscape Report Q1 2020, the cloud service provider (CSP) said it mitigated one of the largest DDoS attack it had ever seen in February 2020. It was 44% larger than anything AWS had encountered. The volume of the attack was 2.3 Tbps and used a type of UDP vector known as a Connection-less Lightweight Directory Access Protocol (CLDAP) reflection. Amazon said it used its AWS Shield to counter the attack.

This was last updated in April 2021

Continue Reading About denial-of-service attack

- 6 common types of cyber attacks and how to prevent them
- The ultimate guide to cybersecurity planning for businesses
- 10 types of security incidents and how to handle them
- Credential stuffing: When DDoS isn't DDoS
- The dark web in 2021: Should enterprises be worried?

Related Terms

What is access control?

Access control is a security technique that regulates who or what can view or use resources in a computing environment. See complete definition

What is Android System WebView and should you uninstall it?

Android System WebView is a system component for the Android operating system (OS) that enables Android apps to display web ... See complete definition

What is WPA3 (Wi-Fi Protected Access 3)?

WPA3, also known as Wi-Fi Protected Access 3, is the third iteration of a security certification standard developed by the Wi-Fi ... See complete definition

Dig Deeper on Network security

6 types of DNS attacks and how to prevent them

By: Ravi Das

DNS attack

By: Rahul Awati

DoS vs. DDoS: How they differ and the damage they cause

By: Ravi Das

What to know about UDP vulnerabilities and security

By: David Jacobs

Networking

Latest TechTarget
resources

- NETWORKING
- CIO
- ENTERPRISE DESKTOP
- CLOUD COMPUTING
- COMPUTER WEEKLY

The push to make network engineering cool again

What does it mean to make networking cool again? To most network engineers, it means building awareness about networking and ...

The role of network sandboxing and testing

Network sandboxing provides network teams with a risk-free environment to test changes and run potential threat scenarios. This ...