# Distributed Denial-of-Service (DDoS)

Archived: 2026-04-05 22:00:56 UTC

A tool favored by many threat actors, Distributed Denial-of-Service (DDoS) attacks seek to make a targeted machine or network resource unavailable to its users. They use overwhelming amounts of traffic, such as incoming messages, connection requests, and malformed packets. This substantially slows the system, or forces it to crash.

In this article, we explore how DDoS attacks work, types of DDoS attacks, and their damaging impact. We also provide tips on how to prepare for, prevent, and respond to a DDoS attack.

## How Distributed Denial of Service Attacks Work

To accomplish this, a distributed denial-of-service attack uses a botnet. A botnet is a network of computers controlled by malware. It sends requests to the target's IP address. The use of botnets distinguishes DDoS attacks from DoS (Denial-of-Service) attacks. In a DoS attack, overloading traffic is sent from only one attacking machine. Botnets make attacks appear to come from multiple devices and locations. This makes them difficult to defend against.

DDoS activity is seeing a major increase. Sources state that over six million attacks were observed in 2022 H1. Organizations should also be aware that this trend will likely continue. This is because botnets are becoming more publicly available via crimeware. This allows an individual to rent DDoS capabilities via illicit marketplaces. It enables low-skilled individuals or groups to perform more complex attacks. Threat actors can also use vulnerability exploits to conduct DDoS attacks.

## Types of DDoS Attacks

In general, there are three types of DDoS attacks: application layer attacks, network layer attacks, and volumetric attacks. Organizations should also be aware that DDoS attacks can be achieved by exploiting the vulnerabilities affecting their IT resources. Modern attacks use a variety of DDoS tools, like booters or stressors. Tactics can be used alone, or combined for more complex, multi-vector attacks.

### Application Layer Attacks

The application layer of a network connection is where a server creates a response to a request. For example, loading a webpage in response to a user entering an HTTP request in their browser. Application layer attacks make repeated requests to overwhelm the server. These attacks are categorized as "layer 7."

### Network Layer Attacks

Network layer attacks focus on an earlier stage in a network connection. They exhaust server resources like firewalls or routing engines. For example, an attacker may overwhelm a target server with SYN packets. These

packets are used to start a secure connection between two computers. These attacks are categorized as “layer 4,” which denotes attacks at the transport layer such as TCP.

**Volumetric Attack**

Volumetric attacks overwhelm the target server’s bandwidth. They usually do this by making repeated queries to an open domain name system (DNS) resolver using the target’s own IP address. In other words, the attacker makes multiple requests to DNS resolvers. This makes it look like they’re coming from the target server.

## The Impact of DDoS Attacks

Any business or industry can be at-risk of a DDoS attack. This is because most organizations have internet-facing websites or assets. Furthermore, DDoS attacks can cause lengthy shutdowns and downtime. This can result in major financial losses, customer dissatisfaction, and reputational loss. According to Imperva, the average attack can cost victims around $500,000 total or $40,000 per hour of downtime.

DDoS attacks can also cause data loss. They can mask other cybercriminal activities that could breach the target’s security. More serious attacks can prompt civil unrest or be considered a type of warfare. These are attacks leveraged by advanced persistent threat (APT) groups. An example is the Russian-Ukraine War, where Russian hackers DDoS’d Ukrainian government portals and banking websites days before the invasion. According to Kaspersky, DDoS attack volumes have increased 4.5 times since the conflict first began.

> “In Q1 2022 we witnessed an all-time high number of DDoS attacks. The upward trend was largely affected by the geopolitical situation…Some of the attacks we observed lasted for days and even weeks, suggesting that they might have been conducted by ideologically motivated cyberactivists. We’ve also seen that many organizations were not prepared to combat such threats.”ALEXANDER GUTNIKOV, KASPERSKY

In addition, it is reported that the sophisticated and powerful DDoS tools developed for the war are being adopted by other threat actors worldwide.

### DDoS Attack Targets

In 2023, analysts observed a large increase in DDoS attacks on various industries. Major tech companies have reported on reducing the largest DDoS attacks in 2023. Cloudflare reported that automatically identified and reduced DDoS attacks have increased by 65 percent in Q3. Computers and servers were the top targets for DDoS attacks, accounting for 92 percent of attacks carried out. Attack length and frequency decreased by 55 percent. However, attack size grew exceptionally by 233 percent.

In August 2023, a major search engine detected and successfully reduced a DDoS attack. It peaked at 398 million requests per second. This attack has been one of the largest DDoS attacks conducted so far. Another large tech company also reported an unusual increase in HTTP/2 requests. This peaked at 155 million requests per second in late August.

## Steps to Prevent DDoS Attacks

One out of five companies with over 50 employees have been a victim of at least one DDoS attack. The proliferation of DDoS means that attempts against your organization may occur—but there are still some strategies you can use to proactively identify, or prevent and minimize damage from an attack:

1. **Monitor network traffic for abnormal activities.** This includes unexpected traffic influxes, traffic originating from suspicious locations, slow servers, or even an increase in spam emails—signs that an attack could be imminent.
2. **Plan an attack response proactively.** This could involve simulation testing or establishing procedures for IT personnel and other impacted stakeholders in the event of an attack.
3. **Filter legitimate traffic from DDoS traffic** by using mitigation strategies like black hole routing, rate limiting, or a web application firewall.
4. **Identify exploitable vulnerabilities** using tools like Flashpoint's VulnDB. In addition to disrupting traffic, attacks may also leverage vulnerabilities within an organization's applications. Having comprehensive vulnerability intelligence allows organizations to patch vulnerabilities before they're exploited.
5. **Track publicly-available websites**, like paste bins, social media, or forums, for conversations that may indicate a potential attack. Specialized open source intelligence tools like Echosec allows users to uncover hidden threats on a variety of sources, like the dark web.
6. **Stay informed on the latest malware trends**. Threat actors are constantly finding new ways to compromise their victims. Staying up-to-date on malware strains such as Mirai, Meris, and Androxgh0st is critical. Therefore, using a comprehensive source of threat intelligence is vital.

## Stay Prepared with Flashpoint

Industry research shows that DDoS attacks are not only on the rise, but their approaches are becoming more sophisticated. While the Russia-Ukraine war is primarily responsible for this, nevertheless, these types of attacks will continue to plague organizations. However, organizations do have tools and strategies that can help them mitigate the risk that DDoS attacks can introduce. Request a demo to gain visibility into threat actor channels and activity.

## Frequently Asked Questions (FAQ)

### Q: What is a DDoS attack and what is a botnet?

**A:** A DDoS attack makes a targeted network resource unavailable by overwhelming it with requests. It achieves this by using a botnet, which is a network of compromised computers that send traffic from multiple locations, making the attack difficult to defend against.

### Q: What are the three main types of DDoS attacks?

**A:** The three main types are Application Layer Attacks (which overwhelm the server's response process, or Layer 7), Network Layer Attacks (which exhaust server resources like firewalls, or Layer 4), and Volumetric Attacks (which overwhelm the target's network bandwidth).

### Q: How does Flashpoint intelligence help organizations prevent DDoS risks?

**A:** Flashpoint helps by providing vulnerability intelligence (VulnDB) to patch exploited flaws used to launch attacks. Flashpoint also offers Open Source Intelligence (OSINT) tools to track public and illicit forums for threat actor chatter that may indicate an imminent attack.

---