COMCAST BUSINESS

The Anatomy of a DDoS Attack

A look at the types and timelines of typical DDoS attacks

What is a DDoS Attack?

A distributed denial of service (DDoS) attack is one of the most common types of cyberattacks. They take advantage of the capacity limits of any network resource—such as the infrastructure enabling an organization's website—and overload them. The DDoS attack sends multiple requests to the web resource, aiming to exceed its capacity to handle multiple requests, prevent proper function, and take it offline.

Not all DDoS attacks, though, are created equal—and there are several different types. DDoS attacks have grown increasingly sophisticated and differentiated over the years, as hackers have tried to keep up with—and stay ahead of—security safeguards.

High-profile DDoS attacks and targets sometimes make the headlines, but many unnamed, undocumented, yet successful attacks happen consistently. The reality: Any organization of any size with a server, web property, or other network resource is vulnerable. Understanding the risks surrounding DDoS attacks and how they work will help you take the proper steps to help protect your data.

DDoS Attacks By the Numbers

The risk of a DDoS attack has only increased as the world becomes more interconnected. The explosion of digital applications and growth of technologies such as the Internet of Things (IoT), cloud applications, and edge computing has created a massive attack surface, giving cybercriminals more endpoints and potential vulnerabilities to target.

~13M
DDoS attacks worldwide[1]

29.3
DDoS attacks per day in Q4 of 2022[2]

10X
Increase in attack frequency since 2005[1]

$218K
The average cost of a DDoS attack in the US, without factoring in any ransomware costs[3]

$250
The price for a midsize attack that lasts for a whole day on the dark web[3]

The Hidden Costs

Heavily trafficked Internet sites such as ecommerce, gaming, and web hosting can lose hundreds of thousands of dollars every minute their websites are down. And while DDoS attacks can cost organizations significant losses in revenue due to downtime, **there are many other negative effects to consider:**

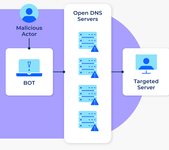
- Remediation & compensatory costs
- Reputational damage
- Loss of customers
- Threat of legal action

Types of DDoS Attacks

Generally speaking, DDoS attacks can be divided into three types

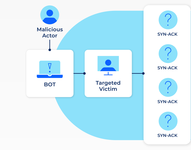
01. Volumetric attacks

This type is the classic type of DDoS. These attacks use methods to generate massive traffic volumes to thoroughly saturate bandwidth, manufacturing a traffic jam that makes it impossible for legitimate traffic to flow in or out of the targeted resource.



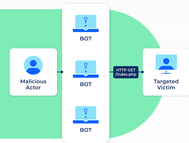
02. Protocol attacks

By targeting Layer 3 (network) and Layer 4 (transport) protocol communications with malicious connection requests, cybercriminals designed this method to reduce the processing capacity of network infrastructure resources, such as servers, firewalls, and load balancers.



03. Application attacks

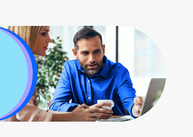
These are some of the more advanced DDoS methods used today. By opening connections and initiating process and transaction requests that consume finite resources, such as available memory and disk space, these attacks exploit weaknesses in Layer 7, the application layer.



Timeline of an Attack

Before a DDoS Attack

Typically, cyber arms dealers recruit a botnet and sell ready-made DDoS 'services' to cybercriminals. A botnet (short for "robot network") is a network of devices infected by malware under the control of a single attacking party. A typical DDoS attack is executed using a botnet.



Infected Devices
Cyberattackers create a network of infected devices called bots, which can be used as a source of attack origination.

Target Identification
The motivations behind DDoS attacks are many. Extortion, ransom, hacktivism, cyber warfare, malicious intent, and more.

Attack Initiation
Affected systems send a flood of requests to the target server or network.

Crash
Huge amount of traffic exhausts target resource and brings it offline.

DDoS Mitigation

Help safeguard your network. Your organization can ensure network health with a simple DDoS mitigation plan from a service provider that can help prevent significant costs and reputational damage.

Detection
DDoS mitigation service providers monitor traffic for a set of IP addresses to detect suspect and malicious traffic.

Drop and rate limiting
As a first line of defense, traffic is dropped or rate-limited as Layer 3 or Layer 4 malicious traffic at the network's edge.

Diversion
Service providers can then divert Border Gateway Protocol (BGP) Route Layer 7 traffic to distributed scrubbing centers.

Delivery
Clean, legitimate traffic is delivered to your network via a secure tunnel, preserving Internet uptime.

Learn more about DDoS mitigation services from Comcast Business

Learn more

Sources:
1. 2023 Netscout DDoS Threat Intelligence Report
2. Radware, 2022 Global Threat Analysis Report
3. Corero Whitepaper – The Need for Always-On, Real-Time DDoS Security Solutions

COMCAST BUSINESS