Distributed denial of service attacks—Prevention and preparation

CANADIAN CENTRE FOR CYBER SECURITY

December 2023 | ITSAP.80.110

Distributed denial of service (DDoS) is a type of cyber attack in which threat actors aim to disrupt and prevent legitimate users from accessing a networked system, service, website, or application. One example of a traditional DDoS attack involves threat actors flooding a targeted financial institution's website with fake traffic to disrupt its clients online banking activity. Other DDoS attacks are strategically executed in response to geopolitical events or used as an extortion technique against victims by overwhelming and disrupting the target's online services. All organizations across different industries, sectors, or institutions rely on network resources and are potential targets of a DDoS attack. Your organization can suffer business revenue loss, reputational damage, decreased client or consumer confidence, and potential legal liabilities (in the event of a privacy breach) as a result of a DDoS attack. With increases in scale and complexity of DDoS attacks, it's important for your organization to prevent and prepare against them. This publication provides guidance on the actions you can take when a DDoS attack occurs and what you can do to mitigate the impact.

What are the types of DDoS attacks?

DDoS attacks can be launched by a single threat actor using a botnet, which is a group of Internet-connected devices that might be compromised or voluntarily made available. DDoS attacks can also be carried out by a coordinated group of threat actors using multiple machines to attack one target. Regardless of the method, a DDoS attack makes it harder to identify the true source of the attack and increases the impact to the victim. There are three broad categories of DDoS attacks, depending on which part of the network layer that is targeted.

Example of a large-scale DDoS attack: HTTP/2 rapid reset

A vulnerability known as Rapid Reset (CVE-2023-44487) was observed by security researchers between August and October 2023. This type of attack exploits a weakness in the HTTP/2 protocol and would allow a threat actor to flood your server with send and cancel requests repeatedly. Threat actors can manipulate this vulnerability to overwhelm target websites and launch a DDoS attack on a massive scale.

Volume-based attacks

Threat actor goal: To exhaust the network bandwidth and processing capabilities by flooding it with false data requests. Volume-based DDoS attacks are one of the most common and are often accomplished by using botnets.

Example: Domain name server (DNS) amplification is a scenario where threat actors:

- spoof their target's web address
- craft a DNS name lookup request that amplifies the size of the response (such as requesting domain information and not just the IP address)
- send the DNS name request to a public DNS server with the spoofed address and the DNS server sends the response to the target

Protocol-based attacks

Threat actor goal: To overwhelm the processing capacity of your organization's network infrastructure resources such as servers, firewalls, and load balancers with malicious connection requests.

Example: Synchronize (SYN) flood attack is a scenario where threat actors send a repeated and excessive amount of transmission control protocol (TCP) connection requests to the target without finalizing the connection. The target servers resources are consumed with waiting to complete connections, which ties up the system from accepting legitimate connection requests

Application-based attacks

Threat actor goal: To overload specific elements of an application server infrastructure such as web servers, which are commonly targeted. Application-based DDoS attacks are less common but tend to be more complex and harder to detect as they resemble legitimate website traffic.

Example: Hypertext Transfer Protocol (HTTP) flood is a scenario where threat actors inundate a web server or application with multiple HTTP requests that trigger complex and intensive server-side processing

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Distributed denial of service attacks—Prevention and preparation

CANADIAN CENTRE FOR CYBER SECURITY

December 2023 | ITSAP.80.110

A DDoS attack on your organization, regardless of its size, can have significant and sometimes devastating consequences. The following actions can help your organization prevent a DDoS attack and effectively address it in when an attack occurs.

Prepare and prevent

- ☐ **Establish a baseline for normal network activity** to understand what is acceptable traffic that the hosts/nodes on your network typically receive. This baseline information can be compared against elevated levels of traffic detected at a particular host.
- ☐ **Deploy web application firewalls (WAFs)** to create a shield between the Internet and your applications. These allow you to control the incoming traffic based on a predefined set of security rules.
- ☐ **Continuously monitor network traffic** using various tools such as a security information and event management (SIEM) solution, so that you can quickly detect anomalies in data traffic patterns.
- ☐ **Minimize your attack surface** by keeping your devices and security patches updated, using multi-factor authentication (MFA) to protect accounts, and training users to be vigilant of potential phishing or malicious emails.
- ☐ **Create an incident response plan** that includes processes, procedures, and contact information related to how your organization detects, responds to, and recovers from incidents.
- ☐ **Conduct regular risk assessments and audits** on your infrastructure to validate that security measures work as intended, as well as in order to identify vulnerabilities and mitigate them earlier.
- ☐ **Understand what capabilities your Internet service provider (ISP) and cloud service provider (CSP)** can provide to protect you from DDoS attacks. Review the service level agreement (SLA) and ensure that contractual support related to DDoS remediation is in place.

Detect and analyze

- ☐ **Contact your network administrator** to confirm if there's an expected service outage based on scheduled maintenance or an in-house network issue.
- ☐ **Contact your ISP and CSP** to confirm if there's a known outage on their end or if their network is under DDoS attack.
- ☐ **Deploy your incident response team** to collect the necessary information to quickly analyze and validate the incident. If organizational resources allow, consider using a third-party service provider that has expertise and tools to quickly diagnose and analyze the type of DDoS attacks.

Contain and eradicate

- ☐ **Isolate your most critical networks** from Internet connection and if possible, all interconnected systems until all vulnerabilities are mitigated and any malware is removed.
- ☐ **Use blackholing countermeasures** to redirect all network traffic away from the target server to a null route. This is effective in some situations as it can shield your larger network from the adverse effects of the attack.
- ☐ **Immediately patch affected systems** as soon as updates become available.
- ☐ **Restrict Internet access to your web applications** based on known malicious IP addresses or geographic locations, where possible.
- ☐ **Consider using third-party DDoS mitigation services** to leverage their tools and expertise to help you more quickly contain and eradicate the attack.

Learn more

- ☐ Developing your incident response plan (ITSAP.40.003)
- ☐ Developing your IT recovery plan (ITSAP.40.004)
- ☐ Network security logging and monitoring (ITSAP.80.085)
- ☐ Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)
- ☐ Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)
- ☐ Domain Name Service (DNS) tampering (ITSAP.40.021)
- ☐ Cybersecurity and Infrastructure Security Agency's (CISA) DDoS Quick Guide

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada