Understanding and Responding to Distributed Denial-of-Service Attacks

Publication: October 28, 2022

Cybersecurity and Infrastructure Security Agency

Table of Contents

Overview 3
DoS and DDoS 3
What Steps Should You Take Before a DDoS Attack? 4
What Do You Do If You Think You Are Experiencing an Attack? 6
What Do You Do After a DDoS Attack? 8
Reporting 8
Acknowledgements 9
Disclaimer 9
Resources 9

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint guide to provide organizations proactive steps to reduce the likelihood and impact of distributed denial-of-service (DDoS) attacks. These attacks can cost an organization time and money and may impose reputational costs while resources and services are inaccessible.

DoS and DDoS

Denial-of-service (DoS) attacks are a type of cyberattack targeting a specific application or website with the goal of exhausting the target system's resources, which, in turn, renders the target unreachable or inaccessible, denying legitimate users access to the service. Although many forms of DoS attacks exist, the most common types are the following:

1. Network resource overload consumes all available network hardware, software, or bandwidth of the target.
    a. In a direct network resource overload attack, the cyber threat actor overloads resources using tactics, such as exploiting a server vulnerability or inundating servers with requests.
    b. In a reflection amplification attack, the threat actor consumes network resources by reflecting a high volume of network traffic to the target. The actor use a third-party server (the "reflector") as an intermediary that hosts and responds to the given spoofed source IP address.
2. Protocol resource overload consumes the available session or connection resources of the target.
3. Application resource overload consumes the available compute or storage resources of the target.

A DoS attack is categorized as a distributed denial-of-service (DDoS) attack when the overloading traffic originates from more than one attacking machine operating in concert. DDoS attackers often leverage a botnet—a group of hijacked internet-connected devices—to carry out large-scale attacks that appear, from the targeted entity's perspective, to come from many different attackers. A wide variety of devices may make up a botnet, including Internet of Things (IoT) devices. IoT devices are internet-connected and often use default passwords and lack sound security postures, making them vulnerable to compromise and exploitation. Because infections of IoT devices often go unnoticed by users, an attacker could easily assemble hundreds of thousands of these devices into a formidable botnet capable of conducting a high-volume attack. Further, after establishing a botnet, a cyber threat actor may

rent it out to other potential attackers in an "attack-for-hire" scheme, which enables unskilled users to launch DDoS attacks.

The more traffic a DDoS attack produces, the more difficulty an organization will have responding and recovering from the attack. The increase in traffic also increases the difficulty of attribution because it makes the true source of the attack harder to identify. Although the impact of DDoS attacks may often be negligible—depending on the scale of the attack—it could be severe and include loss or degradation of critical services, loss of productivity, extensive remediation costs, and acute reputational damage. Organizations should include steps to address these potential effects in their incident response and continuity of operations playbooks.

Although a DDoS attack is unlikely to impact the confidentiality or integrity of a system and associated data, it does affect availability by interfering with the legitimate use of that system. Because a cyber threat actor may use a DDoS attack to divert attention away from more malicious acts they are carrying out—e.g., malware insertion or data exfiltration—victims should stay on guard to other possible compromises throughout a DDoS response. Victims should not become so focused on defending against a DDoS attack that they ignore other security monitoring.

In a progressively interconnected world with additional post-pandemic remote connectivity requirements, maintaining the availability of business-essential external-facing resources can be challenging for even the most mature IT and incident response teams. It is impossible to completely avoid becoming a target of a DDoS attack. However, there are proactive steps organizations can take to reduce the effects of an attack on the availability of their resources.

What Steps Should You Take Before a DDoS Attack?

- **Understand your critical assets and services.** Identify the services you have exposed to the public internet and the vulnerabilities of those services. Prioritize assets based on mission criticality and need for availability. Implement ways to lower the risk of an attack by committing to good cyber hygiene (e.g., server hardening, patching). Determine whether your web application firewall (WAF) covers your critical assets and is configured in a `Deny` state.
- **Understand how your users connect to your network.** Identify the disparate ways your user base connects to your organization's network, whether onsite or remotely via virtual private networks (VPNs). Identify potential network chokepoints and any mitigations that may minimize disruptions to key personnel.
- **Enroll in a DDoS protection service.** Many internet service providers (ISPs) have DDoS protections, but a dedicated DDoS protection service may have more robust protections against larger or more advanced DDoS attacks. Protect systems and

services by enrolling in a DDoS protection service that can monitor network traffic, confirm the presence of an attack, identify the source, and mitigate the situation by rerouting malicious traffic away from your network. Organizations should enroll in a DDoS protection service after completing a review of critical assets and services. See CISA's Free Cybersecurity Services Catalog for services that may be freely available.

- **Understand service provider defenses.** Engage with your ISP and cloud service provider (CSP) to understand existing their DDoS protections. Review service agreements to determine:
    - the protections your service providers offer to assist in mitigating DDoS attacks and
    - any risks posed by gaps or limitations in coverage.

  Speak with your service providers about best practices for hosting web servers while using their DDoS protections.
- **Understand your dedicated edge network defenses.** Speak with a managed service provider (MSP) about specific managed services that guard against DDoS attacks. MSPs offering different technologies on the "edge" can assist with a customization of edge defenses. Edge defense services can reduce downtime caused by DDoS attacks. Edge defense, detect, and mitigation services reduce the risk of malicious traffic reaching its target, and greatly increase the chances of legitimate users reaching your websites/web applications.
- **Design and review (High-Availability/Load-Balancing/Colocation) designs.** Review system/network designs and eliminate single points of failure, such as a high-value-assets (HVA) hosted on a single node. Ensure HVAs are capable of high-availability (HA) and/or load-balancing (LB) across multiple nodes. Colocation of HVA services serves as a good technique for business continuity. However, the best method to guard against DDoS is stopping the attack by either upstream service provider defenses or DDoS protections in your local datacenter.
- **Develop an organization DDoS response plan.** The response plan should guide your organization through identifying, mitigating, and rapidly recovering from DDoS attacks. All internal stakeholders—including your organization's leaders and network defenders—and service providers should understand their roles and responsibilities through all stages of a DDoS attack. At a minimum, the plan should include understanding the nature of a DDoS attack, confirming a DDoS attack, deploying mitigations, monitoring and recovery. **Note:** your DDoS response plan should be part of your organization's disaster recovery plan.

- **Develop an organization DDoS business continuity plan.** In the plan, identify alternatives for your critical applications, especially for communications. Specifically, ensure the plan includes a way for leadership to quickly communicate decisions to internal network defenders or external service providers should a DDoS attack overwhelm your network.
- **Consider how a DDoS attack will impact physical backups for your network.** Determine how your organization can function should a DDoS attack limit connections to hardware.
- **Conduct a DDoS tabletop exercise and/or regularly test your DDoS response plan.** Regularly practicing your organization's DDoS response plan with all internal and external stakeholders, including service providers, will:
    - Ensure that each participant fully understands their role and responsibility during the DDoS attack.
    - Help identify gaps and issues before a real event.
    - Give stakeholders the sense of urgency and cadence they will need to move with during a real event.
    - Build confidence in the plan.

  Conduct an after-action review (AAR) after each tabletop exercise or test and update the DDoS response plan based upon lessons learned.

What Do You Do If You Think You Are Experiencing an Attack?

- **Confirmation of a DDoS attack.** DDoS attacks vary in lengths of time. Indicators of a DDoS incident could include, but are not limited to:
    - Network latency or unusually slow network performance in opening files or accessing websites.
    - Sluggish application performance.
    - High processor and memory utilization.
    - Abnormally high network traffic.
    - Unavailability or inaccessibility of websites.

  If you think you or your organization is experiencing a DDoS attack, it is critical that you contact the appropriate technical professionals for assistance.
- **Contact your ISP** to determine if there is an outage on their end or if their network is the target of the attack and you are an indirect victim. They may be able to advise you on an appropriate course of action. Communicate the findings to and work with service providers to better understand the attack.

- **Understand the nature of the attack.**
    - What are the ranges of IP addresses used to propagate the attack?
    - Look for a particular attack against certain running services.
    - Correlate server CPU/memory utilization with network traffic logs and application availability.
    - Once you obtain an understanding of the attack, deploy mitigations.
    - Directly conduct packet captures (PCAPs) of the DDoS activity or work with security/network providers to obtain PCAPs. Analyze PCAPs to verify the firewall is blocking malicious traffic and allowing legitimate traffic to pass.
- **Deploy mitigations.** Continue working with the service providers to get the DDoS attacks blocked. Other mitigations that involve making configuration changes to the current environment and initiating business continuity plans may assist in response and recovery. Thoroughly discuss mitigation measures during "testing and monitoring." All stakeholders should know and understand their role in response and recovery.
- **Monitor other network assets.** During an attack, do not lose sight of the other hosts, assets, or services residing on your network. Threat attackers have been observed conducting DDoS attacks to deflect attention away from their intended target and using the opportunity to conduct secondary attacks on other services within a network. Continue monitoring attacked assets while mitigating and recovering to an operational state. During the recover stage, look out for other anomalies or indicators of compromise. Make certain the DDoS was not just a distraction away from more malicious activity going on within your network.
- **Use mitigations outlined in the MS-ISAC Guide to DDoS Attacks**, including:
    - Provide attacking IP addresses to your ISP. They can implement restrictions to prevent further traffic.
        - Keep in mind that reflection DDoS attacks typically originate from legitimate public servers.
        - Consider asking your ISP to implement port and packet size filtering.
    - Enable firewall logging of accepted and denied traffic to determine where the DDoS may have originated.
    - To minimize your organization becoming a reflector in a DDoS against others, deny Network Time Protocol (NTP) `monlist` request traffic (by disabling the `monlist` command) altogether or enforce that the requests come from valid (permitted) source addresses.

- Define strict `TCP keepalive` and `maximum connection` configurations on all perimeter devices.
- Configure firewalls to block, as a minimum, inbound traffic sourced from IP addresses that are:
  - Reserved (`0/8`)
  - Loopback (`127.0.0.0/8`)
  - Private (RFC 1918 blocks `10.0.0.0/8`, `172.16.0.0/12`, and `192.168.0.0/16`)
  - Unassigned DHCP clients (`169.254.0.0/16`)
  - TEST-NET-1/2/3 (`192.0.2.0/24`, `198.51.100.0/24`, and `203.0.113.0/24`)
  - Multicast (`224.0.0.0/4`)
  - Experimental (`240.0.0.0/4`)

  Note: Monitor network traffic after configuring firewall blocks to ensure that blocks are implemented correctly and not blocking legitimate traffic.

What Do You Do After a DDoS Attack?

- **Continue to monitor other network assets** for any additional anomalous or suspicious activity that could indicate a secondary attack.
- **Update your DDoS response plan to improve response to future DDoS attacks.** Include improvements drawn from any lessons learned regarding communication, mitigation, and recovery. Continue to regularly test your DDoS response plan.
- **Proactively monitor your network to quickly identify DDoS attacks.** Monitoring allows your organization to create a baseline of normal activity on network, storage, and computer systems. This baseline should include activity on both average and high-traffic days. Using this baseline in proactive network monitoring can provide an early warning of a DDoS attack. Alerts can be configured to generate notification, enabling administrators to start responsive techniques at the start of the attack.

Reporting

CISA and FBI urge you to promptly report DDoS incidents to a local FBI Field Office, or to CISA at report@cisa.gov or (888) 282-0870. State, local, tribal, and territorial government entities can also report to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).

Acknowledgements

CISA, FBI, and the MS-ISAC would like to thank Akamai, Cloudflare, and Google for their contributions to this advisory.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA, FBI, and the MS-ISAC do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA, FBI, or the MS-ISAC.

Resources

- See CISA's Cybersecurity Toolkit to Protect Elections for DDoS-specific information.
- See MS-ISAC's Guide to DDoS Attacks for additional DDoS remediation efforts.
- See NIST Special Publication (NIST SP) - 800-189: Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation for additional DDoS mitigations
- See CISA's DDoS Quick Guide for possible attack methods per OSI layer, potential impact, possible DDoS traffic type descriptions, and the applicable recommended mitigation strategies and relevant hardware.
- See CISA's Tip: Understanding Denial-of-Service Attacks for additional information.
- See FBI Private Industry Notification on Potential Cyber Activities During the 2022 Beijing Winter Olympics and Paralympics about cyber actors using DDoS to disrupt events.
- For additional information regarding hacktivism or DDoS attacks, see the following Public Service Announcements on IC3.gov.
    - Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting
    - Booter and Stresser Services Increase the Scale and Frequency of Distributed Denial of Service Attacks
- See MITRE ATT&CK for Detection and Mitigation techniques for:
    - Network Denial of Service [T1498]
    - Direct Network Flood [T1498.001]
    - Reflection Amplification [T1498.002]
- CISA Tabletop Exercise Packages