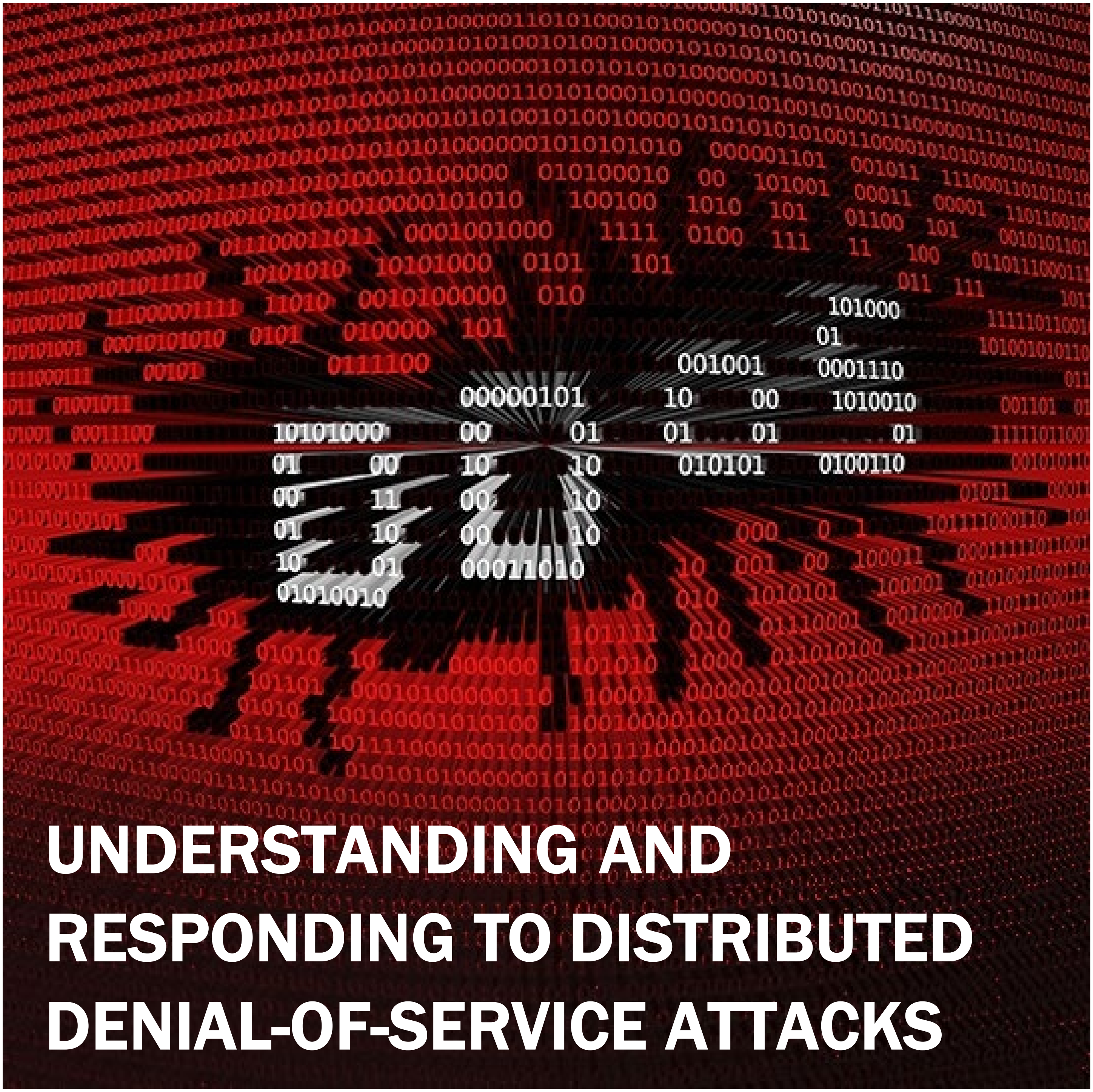


UNDERSTANDING AND RESPONDING TO DISTRIBUTED DENIAL-OF-SERVICE ATTACKS

Publication: March 21, 2024

Disclaimer: *This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.*

Change Record

Version	Date	Revision/Change Description	Section/Page Affected
1.0	October 2022	Initial Version	
2.0	March 2024	• Categorizes DDoS and DoS techniques into three types: Volumetric, Protocol, and Application. • Added DDoS technical definitions and nine visual aids. • Added mitigations for defending against the types of DDoS techniques outlined in the guide	• p.4 through p.15

Table of Contents

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 distributed denial-of-service (DDoS) attack guidance for federal, state, local, tribal, and territorial government entities to serve as a comprehensive resource to address the specific needs and challenges faced by government agencies in defending against DDoS attacks.

Distributed denial-of-service attacks typically originate from multiple sources, making them difficult to trace and effectively block the attacking internet protocol (IP) addresses. This guide provides an overview of the denial-of-service (DoS) and DDoS landscapes, including attack types, motivations, and potential impacts on government operations, as well as practical steps on implementing preventative measures, and incident response for each of the defined DDoS and DoS technique types. Additionally, it highlights why it is important for organizations to focus their planning efforts on emerging DDoS trends and technologies to better defend against malicious DDoS activity.

DoS and DDoS

A DoS and a DDoS attack are similar in that they both aim to disrupt the availability of a target system or network. However, there are key differences between the two.

1. DoS Attack: A DoS attack involves a single source used to overwhelm the target system with a flood of traffic or resource-consuming requests. The malicious actor typically uses one computer or a small number of computers to generate the attack. The goal of a DoS attack is to render the target system unavailable to its intended users and deny them access to resources or services.
2. DDoS Attack: A DDoS attack involves multiple sources. Often, a multitude of compromised computers—known as botnets—are coordinated to launch the attack. Each machine in the botnet sends a flood of traffic or requests to the target system simultaneously to amplify the follow-on impact. Due to the distributed nature of a DDoS attack, defending targeted networks has increased difficulty compared to a DoS attack.

The main advantage of a DDoS attack over a DoS attack is the ability to generate a significantly higher volume of traffic, overwhelming the target system's resources to a greater extent. DDoS attacks can also employ various techniques, such as IP spoofing, which involves a malicious actor manipulating the source IP address and botnets to disguise the origin of the attack and make it more difficult to trace it back to them.

In terms of impact, both DoS and DDoS attacks can disrupt the availability of a targeted system or network, leading to service outages, financial losses, and reputational damage.

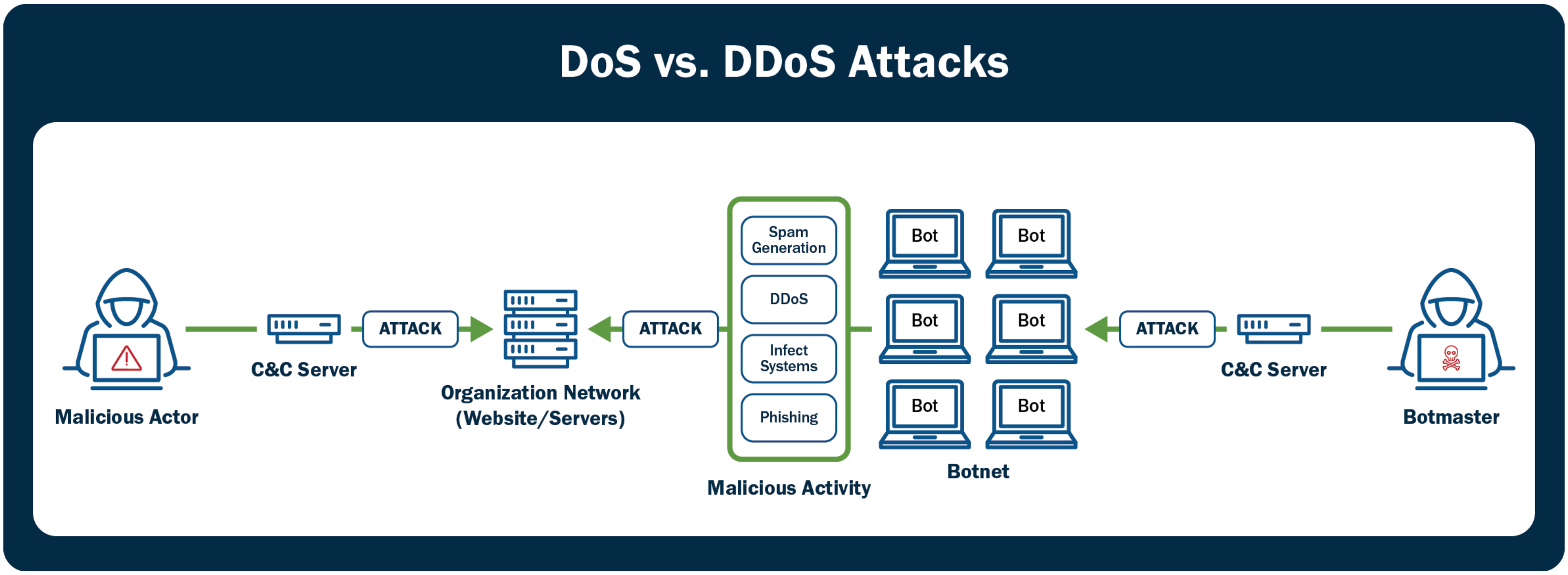
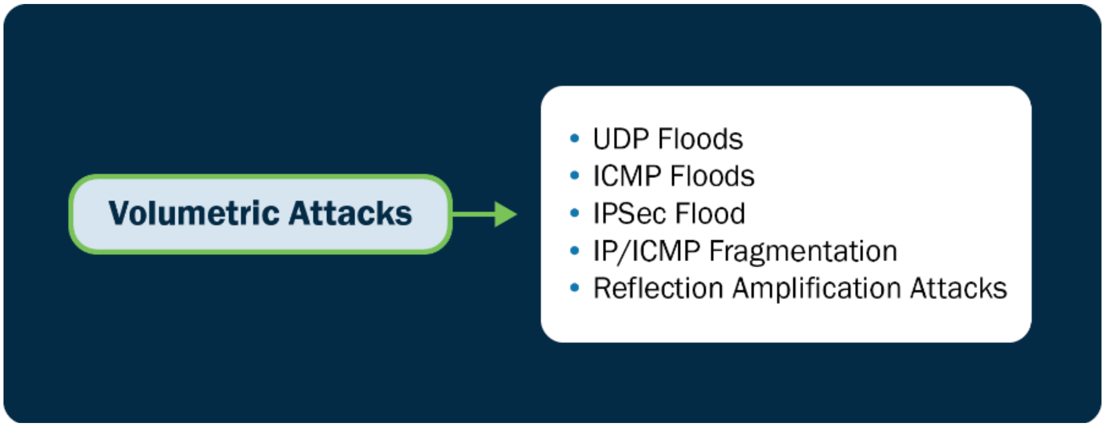


Figure 1: DoS vs. DDoS Attacks

DoS and DDoS Attacks Categorized Into Three Technique Types

1. **Volume-Based Attacks:** These attacks aim to consume the available bandwidth or system resources of the target by overwhelming it with a massive volume of traffic. The goal is to saturate the network or exhaust the target's resources, rendering it unable to handle legitimate requests.



Volumetric Attacks

- UDP Floods
- ICMP Floods
- IPSec Flood
- IP/ICMP Fragmentation
- Reflection Amplification Attacks

Figure 2: Volumetric-Based Attacks

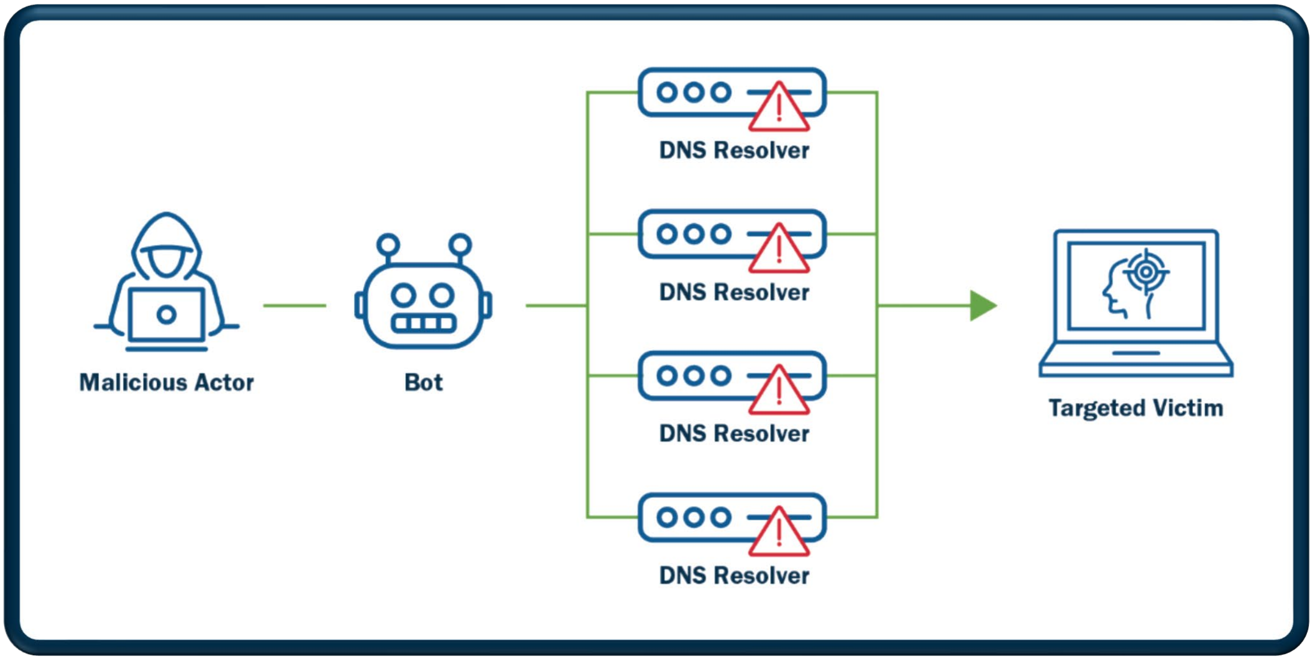
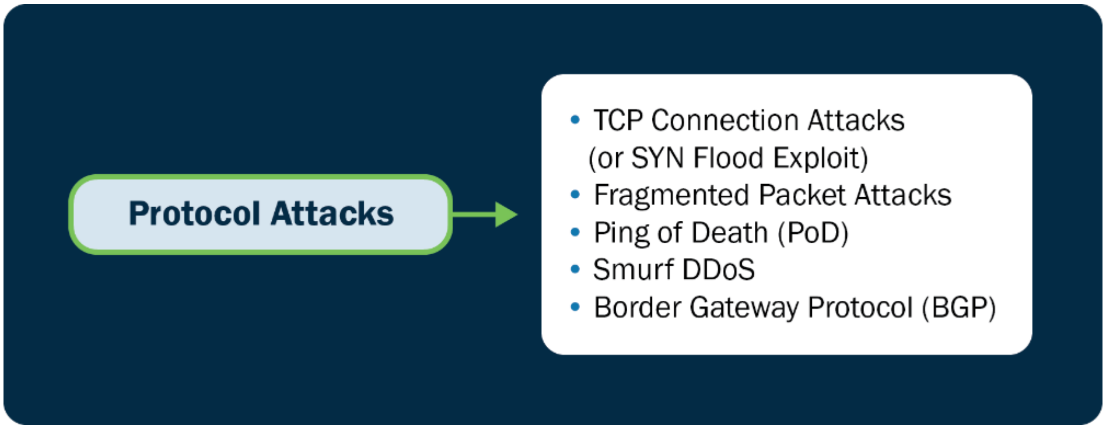


Figure 3: Volumetric-Based Attack Example

2. **Protocol-Based Attacks:** These attacks exploit vulnerabilities in network protocols or services to disrupt the target. By focusing on weak protocol implementations, the malicious actor can degrade the target's performance or cause it to malfunction. Protocol-based DDoS attacks typically target Layers 3 (network layer) and 4 (transport layer) of the Open Systems Interconnection (OSI) model.



Protocol Attacks

- TCP Connection Attacks (or SYN Flood Exploit)
- Fragmented Packet Attacks
- Ping of Death (PoD)
- Smurf DDoS
- Border Gateway Protocol (BGP)

Figure 4: Protocol-Based Attacks

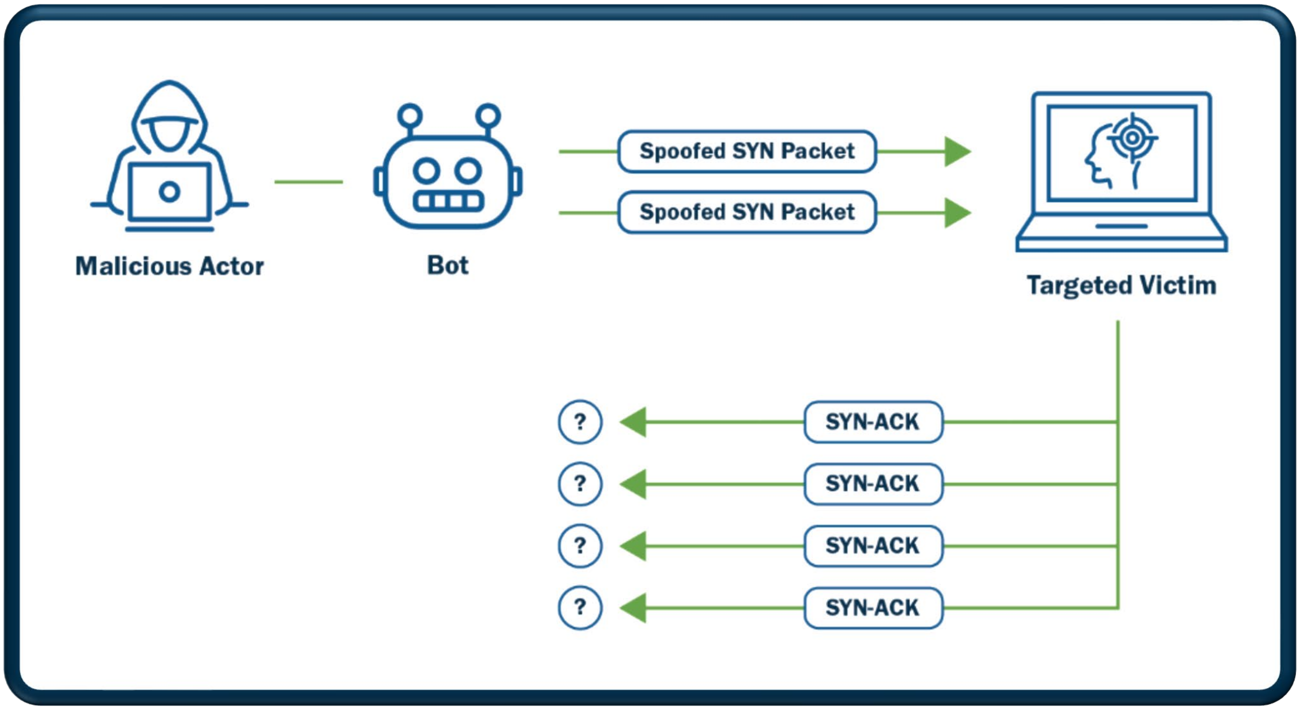
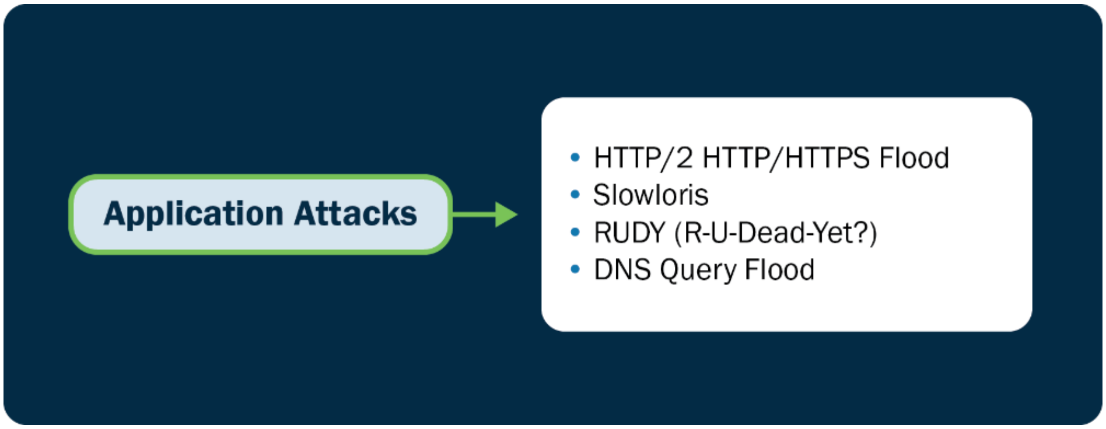


Figure 5: Protocol-Based Attack Example

3. Application Layer-Based Attacks: These attacks target vulnerabilities in specific applications or services running on the target system. Instead of overwhelming the network or system resources, application layer attacks exploit weaknesses in the targeted application, consuming its processing power or causing it to malfunction. Application-based DDoS attacks target Layer 7, the application layer, of the OSI model.



Application Attacks

- HTTP/2 HTTP/HTTPS Flood
- Slowloris
- RUDY (R-U-Dead-Yet?)
- DNS Query Flood

Figure 6: Application-Based Attacks

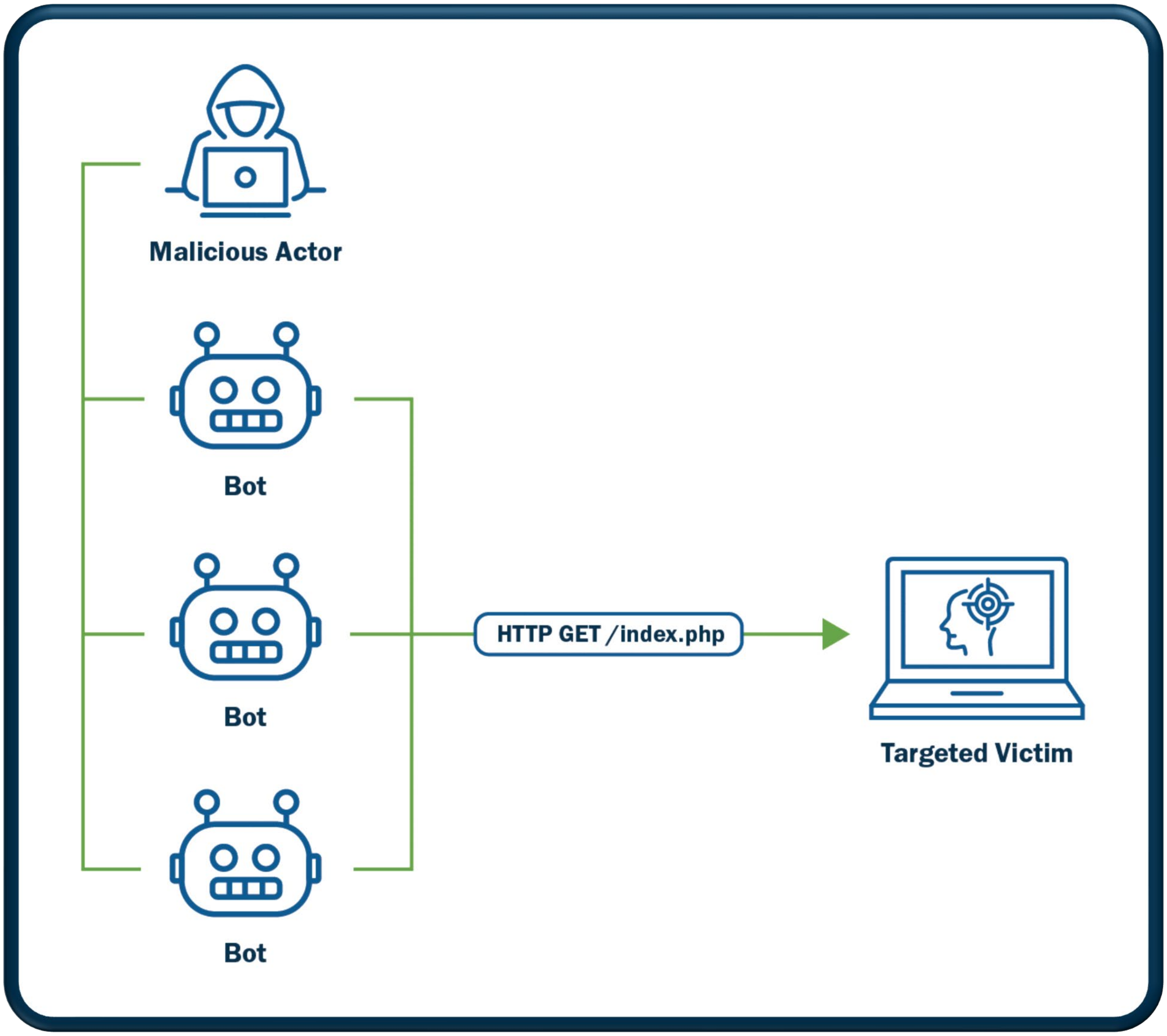


Figure 7: Application-Based Attack Example

Note: These categories are not mutually exclusive, and malicious actors can combine multiple techniques to launch sophisticated DoS and DDoS attacks. Additionally, new attack methods and variations constantly emerge as malicious actors adapt and evolve their tactics, techniques, and procedures (TTPs).

What Steps Should Your Organization Take Before Experiencing a DDoS Attack?

No organization can predict when a DDoS attack will occur. However, malicious actors often look for gaps in security systems to launch a DDoS attack; therefore, it is imperative that an organization's network defenders implement best practices to minimize the potential damage of a DDoS attack. The following is a list of proactive DDoS steps to consider:

1. **Risk Assessment**: Conduct a thorough and proactive risk assessment to determine your organizations vulnerability to DDoS attacks. Risk assessments can identify potential vulnerabilities in your network infrastructure, systems, and applications. Such an assessment will also help your organization understand the potential impact of a DDoS attack and aid in prioritizing and implementing appropriate security measures.
2. **Network Monitoring:** Implement robust network monitoring tools and intrusion detection systems (IDS) to identify any unusual or suspicious traffic patterns. This can heighten your organization's ability to detect and respond to DDoS attacks.
3. **Traffic Analysis:** Regularly analyze your network traffic to establish a baseline of normal traffic patterns. This helps you identify any significant deviations during an attack.
4. **Implement Captcha:** Integrating a Captcha challenge into a website or online service to help differentiate between human users and automated bots, which helps prevent DDoS attacks. By requiring human interaction to access or interact with websites, Captcha acts as preventive barrier against DDoS attacks.
5. **Incident Response Plan:** Develop a comprehensive incident response plan that outlines the steps to be taken in the event of a DDoS attack. The plan should include roles and responsibilities, communication channels, and predefined mitigation strategies.
6. **DDoS Mitigation Service:** Consider employing the services of a DDoS mitigation provider. They possess the expertise and specialized infrastructure to handle large-scale attacks and can help filter out malicious traffic before it reaches your network.
7. **Bandwidth Capacity Planning:** Evaluate your current bandwidth capacity and consider increasing it to handle sudden spikes in traffic during an attack. This can help minimize the impact on legitimate users.
8. **Load Balancing:** Implement load balancing solutions to distribute traffic across multiple servers or data centers. This can help distribute the load and prevent a single point of failure during an attack.
9. **Firewall Configuration:** Configure your firewalls to filter out suspicious traffic patterns and/or block traffic from known malicious IP addresses. Keep the firewall rules updated and consider implementing rate limitations to prevent overwhelming traffic.

10. **Patch and Update Systems:** Regularly update and patch all software, operating systems, and network devices to address known vulnerabilities. Vulnerable systems can be exploited to amplify the impact of a DDoS attack.
11. **Web Application Security:** Implement secure coding practices and conduct regular security assessments of your web applications. Vulnerable applications can be targeted to exhaust server resources during an attack.
12. **Redundancy and Failover:** Implement redundant network infrastructure and ensure failover mechanisms are in place. This will help maintain service availability during an attack by quickly redirecting traffic to alternative resources.
13. **Employee Awareness and Training:** Educate employees about DDoS attacks, their impact, and how to recognize and report suspicious activities. This will help minimize the risk of falling victim to social engineering attacks that can aid in launching a DDoS attack.
14. **Communication Plan:** Develop a communication plan to keep stakeholders informed during an attack. This includes internal teams, customers, and third-party service providers. Clear communication helps manage expectations and coordinates response efforts.
15. **Backup and Recovery:** Regularly back up critical data and ensure you have a tested and updated disaster recovery plan. This will help you recover quickly after an attack and minimize potential data loss.

Note: These steps can help mitigate the impact of a DDoS attack, it's crucial for organizations to remain vigilant to these types of attacks and remain in constant communication with their organization cybersecurity professionals and stay updated on the latest security practices to effectively defend against evolving threats.

How Does Your Organization Know If It's Experiencing a DDoS Attack?

Identifying whether your organizations is experiencing a DDoS attack can be challenging, as symptoms can vary depending on the attack type and intensity. The following is a wide-ranging list to help network defenders determine if there is a DDoS attack occurring:

1. **Website or Service Unavailability:** The most common symptom of a DDoS attack is the unavailability of a website or online service. If a website suddenly becomes inaccessible or experiences significant slowdowns, it could be a sign of a DDoS attack.
2. **Network Congestion:** If there is a sudden increase in network traffic or congestion, it may indicate a DDoS attack. Network monitoring tools, or bandwidth usage reports can help identify abnormal spikes in traffic.
3. **Unusual Traffic Patterns:** Look for unusual traffic patterns in network logs or monitoring systems. This can include a significant increase in requests from specific IP addresses or a high volume of traffic targeting a specific resource or URL.
4. **Server or Application Crashes:** DDoS attacks can overwhelm your servers or applications, leading to crashes or unresponsiveness. If networks suffer from frequent server or application failures without an apparent reason, it could be a sign of an attack.
5. **High Resource Utilization:** Monitor server and network resource utilization metrics, such as CPU usage, memory consumption, or bandwidth usage. A sudden and sustained increase in resource consumption may indicate a DDoS attack.
6. **Inability To Access Other Network Services:** Websites or services may not be the only target of a DDoS attack, other critical network infrastructure components (such as DNS servers or firewalls) may also be at risk. If there are difficulties associated with accessing these services, it could be a sign of an attack.
7. **Anomalies in User Behavior:** Monitor user behavior on your website or service. If there is a significant increase in the number of requests from a single IP address or unusual patterns, it may be a sign of a DDoS attack.
8. **Flood of Spam or Malicious Emails:** DDoS attacks can be launched in conjunction with other types of attacks, such as email spam campaigns. If there is a sudden surge in spam or malicious emails originating from organizational networks, it could be part of a coordinated DDoS attack.
9. **Notifications From DDoS Protection Service:** If you have engaged a DDoS protection service, they may proactively alert you if they detect an ongoing attack on your network.

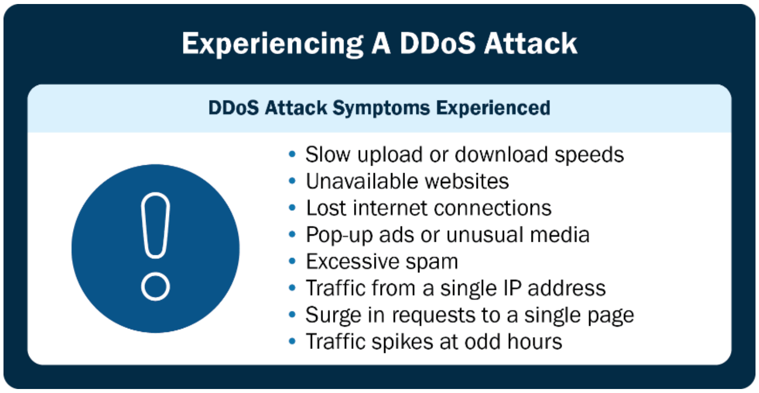
10. **Communication Disruptions:** DDoS attacks can target communication channels, such as Voice over Internet Protocol (VoIP) services or messaging platforms. If there are disruptions or quality degradation in network communication services, it may be an indication of an attack.

How Organizations Can Respond to a DDoS Incident

Organizations experiencing a DDoS attack, are encouraged to initiate incident response plans, contact DDoS protection service provider (if applicable), and engage with your network security team to mitigate the attack and restore normal operations. The following is a list of steps to consider:

1. **Identify the Attack:** Recognize the signs of a DDoS attack, such as a sudden surge in traffic, increased network latency, or unavailability of services. Use network monitoring tools and traffic analysis to confirm the attack.
2. **Activate Incident Response Plan:** Implement your organization's documented and approved incident response plan immediately. This plan should outline the roles and responsibilities of key personnel, communication channels, and the steps to be taken during a DDoS attack.
3. **Notify Service Providers:** Contact internet service providers (ISP) or hosting providers to inform them about the attack. They may have mitigation measures in place or be able to reroute traffic to help mitigate the impact.
4. **Gather Evidence**: Document and collect as much information as possible about the attack, including timestamps, IP addresses, packet captures, and any logs or alerts generated by your network infrastructure. This evidence can be useful for reporting the incident to law enforcement agencies or for future analysis.
5. **Implement Traffic Filtering:** Configure network infrastructure, firewalls, or intrusion prevention systems to filter out malicious traffic. Use rate-limitation or access control lists to block traffic from suspicious IP addresses or specific protocols commonly used in DDoS attacks.
6. **Enable DDoS Mitigation Services**: If available, activate DDoS mitigation services provided by your ISP or third-party vendors specializing in DDoS protection. These services can help filter and divert malicious traffic, allowing legitimate traffic to reach your network.
7. **Scale Up Bandwidth and Resources:** If your organization has the capacity, consider scaling up your network bandwidth and resources to absorb the attack traffic. This may involve adding additional servers or increasing your network capacity temporarily.
8. **Enable Content Delivery Network (CDN):** Utilize a CDN service to distribute content across multiple servers and data centers geographically. CDNs can help mitigate DDoS attacks by absorbing and distributing traffic, minimizing the impact on your infrastructure.

9. **Communicate Internally and Externally**: Maintain clear and regular communication with key stakeholders, including employees, customers, partners, and vendors. Provide updates on the situation, steps taken to mitigate the attack, and expected timelines for resolution.
10. **Learn From the Attack:** After the situation is resolved, conduct a thorough post-incident analysis to understand the attack vectors, vulnerabilities exposed, and lessons learned. Update your incident response plan and security measures accordingly to prevent future attacks.
11. **Use Mitigations Outlined in the MS-ISAC Guide to DDoS Attacks**. Immediate mitigations include:
    - 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.

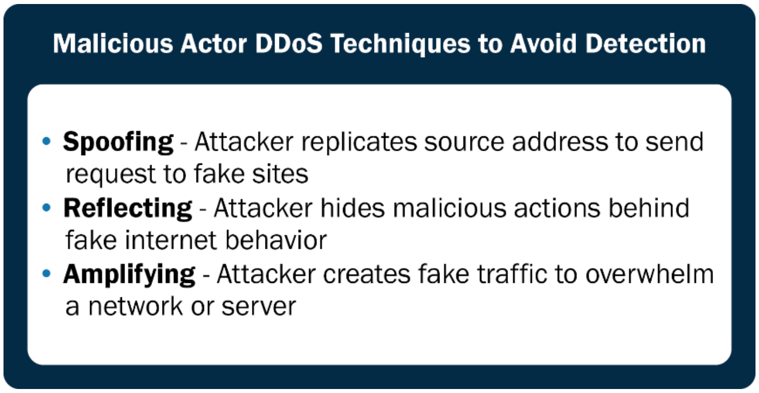


Experiencing A DDoS Attack

DDoS Attack Symptoms Experienced

- Slow upload or download speeds
- Unavailable websites
- Lost internet connections
- Pop-up ads or unusual media
- Excessive spam
- Traffic from a single IP address
- Surge in requests to a single page
- Traffic spikes at odd hours

Figure 8: Potential Symptoms of a DDoS Attack



Malicious Actor DDoS Techniques to Avoid Detection

- **Spoofing** - Attacker replicates source address to send request to fake sites
- **Reflecting** - Attacker hides malicious actions behind fake internet behavior
- **Amplifying** - Attacker creates fake traffic to overwhelm a network or server

Figure 9: DDoS Malicious Actor Techniques To Avoid Detection

Note: Every DDoS attack is unique, and the appropriate response may vary based on the nature and severity of the attack. It is advisable to consult cybersecurity professionals or incident response experts to assist your organization in responding to and mitigating DDoS attacks effectively.

What Steps Should Your Organization Take If It Has Suffered a DDoS Attack?

If your organization has suffered a DDoS attack, there are several important steps your organization can take to recover and mitigate any potential damages. Here is a list of actions to consider:

1. **Assess the Impact:** Evaluate the impact of the DDoS attack on your systems, network, and services. Identify any areas of disruption, data loss, or compromised systems. This assessment will help you understand the extent of the damage and prioritize recovery efforts.
2. **Restore Services**: Restore affected services and systems to normal operations. Depending on the nature of the attack and the systems involved, this may involve restarting servers, reconfiguring network devices, or restoring data from backups. Work closely with your IT teams to ensure a smooth recovery process.
3. **Perform a Post-Incident Analysis:** Conduct a thorough analysis of the attack to understand its characteristics, vulnerabilities exploited, and attack vectors used. This analysis will help you identify any weaknesses in your infrastructure or security measures and guide future improvements.
4. **Implement Remediation Measures:** Based on the post-incident analysis, implement remediation measures to address any identified vulnerabilities or weaknesses. This may involve patching systems, updating security configurations, or enhancing network defenses.
5. **Review Security Controls:** Evaluate existing security controls, such as firewalls, intrusion detection systems, and DDoS mitigation services. Ensure they are properly configured and up to date with the latest threat intelligence. Make any necessary adjustments to enhance your defenses against future attacks.
6. **Update Incident Response Plan:** Update your incident response plan to incorporate lessons learned from the DDoS attack. Revise roles and responsibilities, communication channels, and mitigation strategies based on the insights gained. This will help in responding more effectively to future incidents.
7. **Educate Employees:** Provide training and awareness programs for employees to educate them about DDoS attacks, their impact, and how to recognize and report suspicious activities. Enhancing employee awareness can help prevent social engineering attacks and improve overall cybersecurity hygiene.
8. **Enhance Network Monitoring:** Strengthen your network monitoring capabilities to effectively detect and respond to future DDoS attacks. Implement real-time traffic analysis, intrusion detection systems, and anomaly detection mechanisms to identify and mitigate attacks in a timely manner.
9. **Engage With Law Enforcement:** If the DDoS attack was severe or involved criminal activity, consider engaging with law enforcement agencies. Provide them with any available evidence and cooperate with their investigations to potentially bring the

perpetrators to justice.

10. **Communicate With Stakeholders:** Maintain open and transparent communication with stakeholders, including customers, partners, and vendors. Inform them about the attack, the actions taken to mitigate it, and any potential impacts on services or data. Clear communication helps manage expectations and maintain trust.
11. **Backup and Disaster Recovery**: Review your backup and disaster recovery processes to ensure they are robust and up to date. Regularly back up critical data and test the restoration process to verify its efficacy. This will help you quickly recover in the event of future attacks.
12. **Continuous Improvement:** DDoS attacks are constantly evolving, so it is essential to continuously improve your security posture. Keep abreast of the latest threat intelligence, follow industry best practices, and regularly assess and enhance your security controls.

Note: Recovering from a DDoS attack requires coordinated effort and ongoing vigilance. Engage your organization's cybersecurity professionals to assist in the recovery process and to help strengthen your defenses against future DDoS attacks and report DDoS attacks to the appropriate authorities.

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

Akamai, Cloudflare, and Google contributed to this guide.

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 entity, product, company, or service, including any entities, products, or services linked or referenced within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring 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].
- See CISA Tabletop Exercise Packages.