Distributed Denial-of-Service Playbook

What is Distributed Denial-of-Service?

A Denial-of-Service (DoS) attack refers to a malicious attempt by cybercriminals to render computer services or resources unavailable to the intended user(s). A successful DoS attack exhausts all available network or system resources temporarily or indefinitely by overwhelming the target or its surrounding infrastructure with fraudulent internet traffic, resulting in a slowdown or server crash.

When multiple computer systems (or botnets - made up of networks of compromised devices) are coordinating a DoS attack, this is referred to as a Distributed Denial-of-Service (DDoS) attack. DDoS attacks are particularly destructive as a well-timed attack during peak hours or an attack against time-sensitive services could have substantial impact on business operations.

This playbook provides guidance to organisations on how to identify, contain and mitigate Distributed Denial-of-Service (DDoS) attacks, while minimising impact to business operations. The goal is to equip incident response teams with the tools and information needed to effectively respond to DDoS incidents and ensure that measures are taken to protect the organisation's critical systems and data. This playbook comprises four main sections:

- Possible Signs of DDoS
- How does DDoS Work
- How to Protect Against DDoS
- Incident Response Steps

Possible Signs of DDoS

Common indicators of DDoS attacks include:

- Sudden influx of requests to a specific endpoint or webpage
- Sudden spike of traffic that occurs at regular intervals or at unusual time frames from a single IP address or multiple IP addresses
- Unusually slow network or Wi-Fi performance

- Sluggish application performance
- Prolonged inability to access websites or system files
- High processor and memory usage
- Frequent disconnection from wireless or wired internet connection
- Increased volume of spam emails

How does DDoS Work

While the goal of a DDoS attack is to overwhelm a target system, the tools, tactics and procedures (TTPs) employed could differ. There are three broad categories of DDoS attacks as listed below. Refer to Appendix A for other common types of DDoS attacks.

Volumetric DDoS Attacks

This category of attacks attempts to overwhelm the target system and create congestion by generating large volumes of traffic and consuming all available bandwidth of the target. Volumetric attacks can be achieved through simple flooding techniques, such as User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) flooding, where the attacker sends a large number of network requests to the target system.

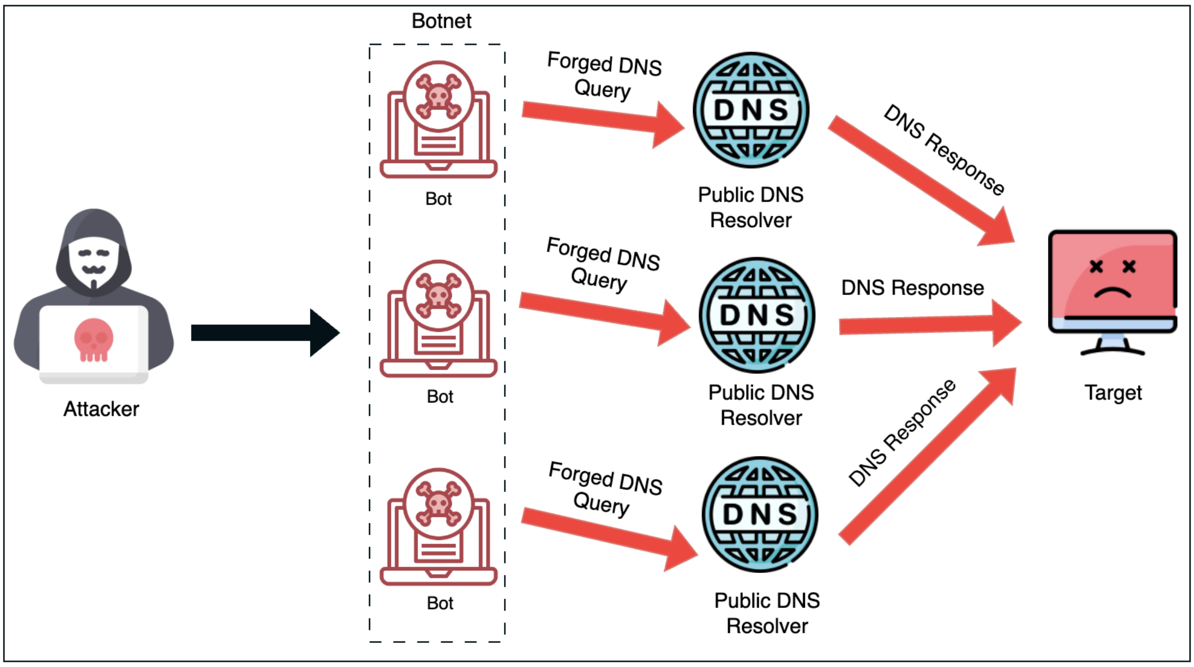

Figure 1 - DNS Amplification Attack

The most common example of a volumetric attack is called a Domain Name System (DNS) Amplification attack. As shown in Figure 1, an attacker substantially amplifies the DNS response to the target by sending specially crafted DNS requests to a public DNS server using a spoofed IP address. When done at a larger scale with the help of botnets, the influx of DNS responses can significantly impact the performance or shut down the target server.

Protocol-based DDoS Attacks

This category of attacks attempts to render a target inaccessible by exploiting specific weaknesses in the targeted system's Layer 3 (Network Layer) or Layer 4 (Transport Layer) network protocol stack. These attacks aim to disrupt the normal function of the targeted system by exploiting vulnerabilities in the way the system handles incoming requests.

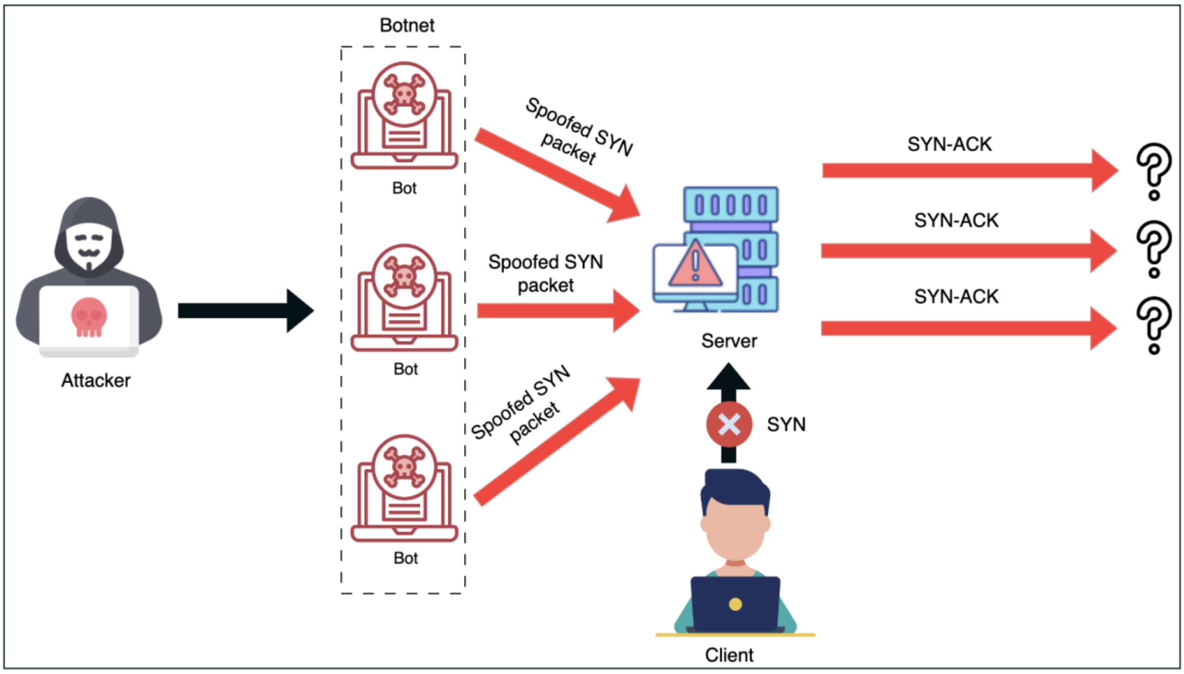

Figure 2 - SYN Flood Attack

The most common example of a protocol-based attack is the Synchronise (SYN) Flood attack. As shown in Figure 2, an attacker exploits the Transmission Control Protocol (TCP) handshake process, which consists of a sequence of communications between two computers to initiate a network connection. By sending a large number of TCP "Initial Connection Request" SYN packets with a spoofed IP address, it causes the target system to allocate resources, such as sockets or connections, to process each incoming request. The fraudulent TCP requests from the attacker will consume these resources and eventually lead to a complete exhaustion of resources and a denial-of-service condition for legitimate users.

Application Layer DDoS Attacks

This category of attack targets specific vulnerabilities in the targeted system's Layer 7 (Application Layer) network protocol stack, such as a web server or a database. This type of attack aims to disrupt the normal function of the targeted system by sending a high volume of requests to specific application functions or features. Application Layer attacks are sophisticated and challenging to identify and mitigate, as they often appear as legitimate requests, and security measures such as firewalls may not be able to help distinguish them from genuine traffic.

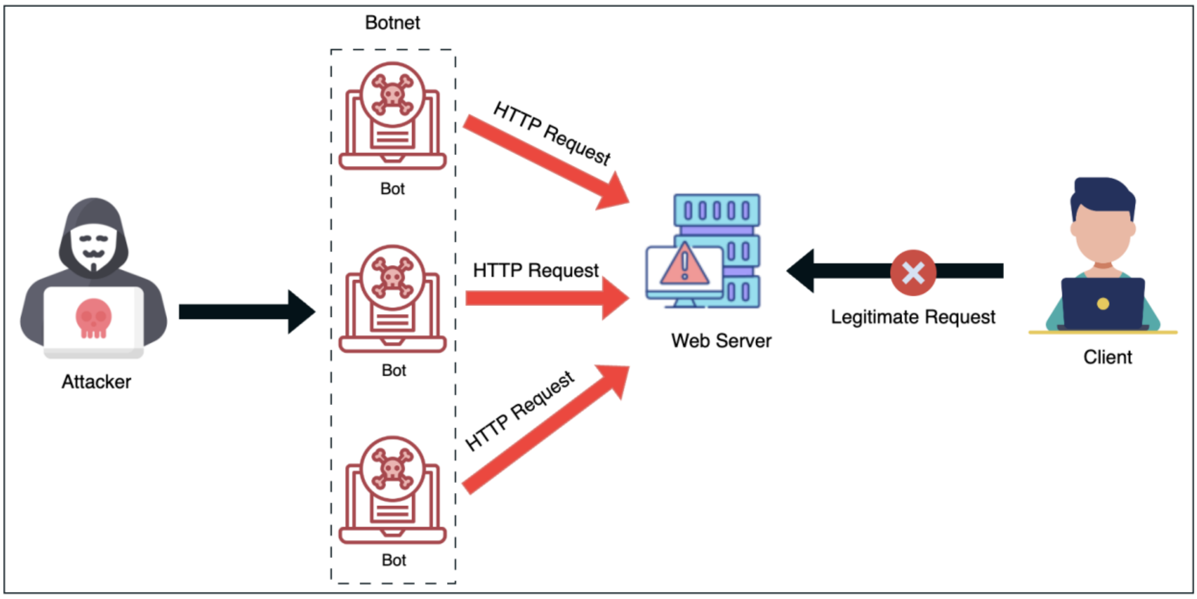

Figure 3 - HTTP Flood Attack

The most common type of application layer attack is the Hypertext Transfer Protocol (HTTP) flood attack. As shown in Figure 3, an attacker sends a large number of HTTP GET requests by repeatedly requesting the same resource using different machines to flood a target web server, resulting in it being unresponsive and inaccessible. The attack makes it difficult to distinguish malicious traffic from legitimate traffic as they often appear as legitimate requests.

How to Protect Against DDoS Attacks

Organisations should review their processes and implement appropriate defensive measures to create a more cyber-resilient environment and reduce the risk of DDoS attacks on their network. The following measures may help to prevent and mitigate DDoS attacks.

Use Strong Passwords and Enable 2FA

By enforcing a strong password policy and implementing two-factor authentication, organisations can minimise the risk of unauthorised access and prevent attackers from compromising their systems, reducing the risk of DDoS attacks. Organisations are advised to:

- Change all default passwords of your devices and routers to strong passwords (i.e. at least 12 characters with upper- and lower-case letters, numbers, and special characters)
- Enable two-factor authentication (2FA) as an additional layer of security to prevent unauthorised access and possible takeover of your network devices and routers in the event of compromised credentials

Monitor and Examine Network Traffic for Unusual or Suspicious Activities

By monitoring and examining network traffic, organisations can detect and respond to DDoS attacks more quickly, reducing the impact of the attack. Organisations are advised to:

- Understand baseline traffic patterns by regularly measuring the type of network devices used and volume of protocol traffic (i.e., UDP, TCP or ICMP)
- Continuously monitor the network traffic by configuring firewalls and intrusion detection/prevention systems to detect anomalous traffic types, system capacity overloads and rogue devices connected to the network

- Report suspicious activities to the relevant IT vendor/department for further analysis

Protect Your Network Perimeter

Implement protections at the network perimeter as a first line of defence to protect your organisation's private networks against DDoS attacks. Such protections can come in the form of demilitarised zone (DMZ) firewalls placed between internal networks and external connectivity points (i.e., internet-facing networks). Organisations are advised to:

- Configure firewalls and routers to only accept traffic detailed in your organisation's security policy required for business operations and drop network packets that meet specific criteria (i.e., malformed and spoofed)
- Define strict "*TCP keepalive*" and "*maximum connection*" on all perimeter devices, such as firewalls and proxy servers to prevent SYN flood attacks
- Rate limit the number of requests a server will accept over a certain time window to prevent volumetric DDoS attacks
- Consider port and packet size filtering
- Set acceptable thresholds for SYN, ICMP and UDP traffic

Maintain System Hygiene

By maintaining system hygiene, it can help to protect against DDoS attacks by minimising the attack surface and improving the overall security status of the targeted systems. Organisations are advised to:

- Regularly check for potentially exploitable DDoS vulnerabilities and remediate them by applying the latest security patches to all devices and routers after appropriate testing
- Enable automatic updates for anti-virus/anti-malware software and perform a full scan of the machines in your network regularly
- Discontinue vulnerable devices that are approaching End of Life (EoL) or no longer supported by the vendor

- Remove unused programs and applications which can become vulnerable over time as they may not receive security updates, making them an attractive target for attackers
- Disable Universal Plug and Play (UPnP) on routers unless required for business operations
- Block unauthorised IP addresses, close or hide unused ports/IP addresses and disable port forwarding to protect your organisation from a targeted DoS/DDoS attack

Increase Network Bandwidth

By increasing the amount of available bandwidth, organisations can absorb the traffic generated by a DDoS attack and prevent target systems from being overwhelmed. Organisations are advised to:

- Use content delivery networks (CDNs). CDNs are large, distributed networks of servers that help to distribute content for organisations and provide some degree of protection against DDoS attacks
- Implement Internet Service Providers and cloud-based DDoS protection services which provide additional bandwidth and filtering capabilities to defend against DDoS attacks. These services work by redirecting traffic to a cloud-based scrubbing centre where incoming traffic is filtered, and only legitimate traffic is forwarded to the targeted systems
- Ensure server redundancy by using a load-balancer and having multiple servers that can take over and continue to handle the workload. This helps to ensure that the targeted systems remain available, even if one server is unable to handle the traffic generated by a DDoS attack
- Implement Bastion Routers either on the outside of the firewall or inside a demilitarised zone (DMZ). These routers are public-facing and are designed to withstand high-bandwidth attacks through the internet.

Raise Awareness

Organisations should conduct regular security awareness trainings for your employees, including how to identify suspicious activity and respond to DDoS attacks.

Additionally, employees should be trained on the organisation's response plan and how to implement it in the event of an attack.

Incident Response Steps

If your organisation is a victim of a DoS or DDoS attack, the following steps may assist in containment, remediation, and system recovery:

Step 1: Identify the Attack

- Verify that the suspicious traffic is indeed a DDoS attack by checking system logs and network traffic data
    - Ensure that the loss of service is not due to other factors such as an internal server fault, or an Internet/Cloud Service Provider outage
    - Check if the organisation is expecting a large volume of traffic (i.e. New service or product launch, time-limited promotions, etc.)
- Identify the critical assets such as servers and databases that are being targeted by the attack
    - Obtain the IP addresses of the systems being targeted
    - Obtain the network diagram for the targeted systems
    - Identify the services that the system provides (i.e. Web Server, DNS, Mail Server, etc.)
- Identify the type of DDoS attack (Volumetric, Amplification, Syn Flood, Protocol, etc.)
    - Get more details on the malicious packets (OSI layer, Destination Port Number, Communication Protocol, etc.)

Step 2: Contain the Attack

- Identify if the DDoS attack exploits a particular service (i.e. ICMP) or is attacking a particular port. Disable that service or close the port if they are not essential to the operation of the targeted system
- Obtain the IP addresses of the incoming DDoS packets and implement access control to block those IP addresses

- Implement rate-limiting to restrict the number of packets that can be sent from a single IP address
- Check if the Internet or Cloud Service providers are able to provide the organisation with any form of DDoS defences:
    - Scrubbing/Clean Pipe
    - Sinkholing (Block known malicious IP addresses)
    - Null routing (Implement as a last resort)
- Divert traffic and swing operations to alternative servers, if any

Step 3: Acquire Forensic Evidence for Root Cause Analysis

Collecting forensic evidence will provide insights into the nature of the attack, including the type of DDoS attack, the source of the attack traffic, the impact of the attack and the types of systems targeted. Analyse the data to determine the root cause of the attack and identify any vulnerabilities that may have been exploited.

The types of forensic evidence to collect include:

- Network traffic logs from firewalls, routers, switches, and other network devices to identify the source and type of traffic involved in the attack
- System logs from servers and other systems to identify any unusual activity or performance issues
- Network flow data to analyse the volume and direction of traffic, and identify any patterns or anomalies
- Packet captures to analyse the contents of network traffic and identify any malicious payloads or exploits

Step 4: Harden your Systems

System hardening can help protect websites and networks against DDoS attacks and is crucial to ensure that the website remains available and accessible to legitimate users. Here are some steps to harden web resources:

- Use web application firewalls (WAFs) to filter out traffic from known malicious IP addresses or ranges

- Implement rate limiting to restrict the amount of traffic that can be sent to the website from a single source or IP address
- Deploy load balancers to distribute incoming traffic across multiple servers, preventing a single server from being overloaded by a DDoS attack
- Keep network devices up to date with the latest firmware and security patches to address known vulnerabilities
- Review and update firewall and network security configurations to limit access to systems and protect against unauthorised traffic
- Perform network segmentation to separate critical assets from public-facing servers
- Subscribe to a DDoS protection service from either the Internet or Cloud Service Providers

Step 4: Notify Stakeholders and Report the Incident

- If you are an organisation, notify your customers, clients, suppliers and employees about potential system downtimes or compromised network devices
- If you suspect your organisation to be a victim of DDoS attacks, you are strongly advised to report the case to SingCERT via our Incident Reporting Form as the information could help alert and assist other individuals and organisations
- If monetary loss(es) or criminal activity is involved, you may lodge a police report at any neighbourhood police post or online here.

Appendix A: Common DDoS Attack Types

Name	**Type**	**Description**
ICMP (Ping) Flood	Volumetric	An ICMP flood involves an attacker overwhelming a targeted device with ICMP Echo Request (ping) packets and rendering it inaccessible to normal traffic.
Ping of Death	Protocol-based	A ping of death attack involves an attacker sending multiple malformed or oversized packets while using a simple ping command to a target computer. The maximum packet length of an IP packet (including the header) is 65,535 bytes. However, when a maliciously large packet is transmitted from the attacker to the target, the packet becomes fragmented into segments, each of which is below the maximum size limit. When the target computer attempts to put the pieces together, the total exceeds the size limit and a buffer overflow can occur, causing it to freeze, crash or reboot.
Slowloris	Application Layer	A slowloris attack involves an attacker attempting to establish multiple TCP connections on a target web server and hold them open for as long as possible by sending partial requests to the server with the aim of overwhelming its ability to process and respond and rendering it inaccessible to any legitimate requests.

UDP Flood	Volumetric	An UDP flood involves an attacker flooding a targeted server with a large number of UDP packets with the aim of overwhelming its ability to process and respond, rendering it inaccessible to any legitimate requests.
Network Time Protocol (NTP) Amplification	Volumetric	A NTP Amplification attack involves an attacker exploiting a NTP server functionality with the aim of overwhelming a targeted network or server with an amplified amount of UDP traffic, rendering the target and its surrounding infrastructure inaccessible to regular traffic.

Note: Several steps in incident response may be highly technical. If necessary, organisations should consider engaging a cybersecurity services vendor to assist with the investigation and/or remediation. Please refer to this list of Cybersecurity Advisory and Consultancy service providers (if required): https://sgtech-prod-api.sgtech.org.sg/api/Common/GetPDF?type=artical&&fileName=f509e67b-1734-4f68-b03e-743fdd659e95.pdf.

Disclaimer: This playbook provides guidelines and recommendations on how to prevent and respond to possible DDoS incidents. It is intended purely as a guide and is not exhaustive. Always consult a trained cybersecurity professional for advice before making any business-critical decisions within your organisation.