<Insert Institution>

Distributed Denial of Service

(DDoS)

Incident Response Playbook

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Version: 1.0**

**Approved:**

**Approval Authority:**

# Introduction

This playbook is a reference process for handling DDoS incidents which should be exercised, deployed and governed as part of the incident management function.

## Playbook Applicability - DDoS

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

**­­­­­DDoS Playbook**

* 1. **Verify DDoS**
		1. **Check logs**
			1. Cyber Security
				1. SIEM
				2. IDS/IPS
				3. WireShark
				4. Web Proxy/DLP
				5. Contact MSSP or SOC to check logs.
			2. Infrastructure
				1. ASA Firewalls
				2. Load Balancer
			3. Dev OPS Monitoring
				1. Check external latency🡪Check latency of websites outbound🡪in.
				2. Check outages.
				3. Check degradation of services/systems.
				4. Contact Monitoring Service/NOC to check logs.
			4. All Departments
				1. Check for unknown or unexpected incoming traffic.
				2. Detection of unknown/unidentified packets from unknown senders.
				3. Check IT Services to see impact.
				4. Check Critical Systems referenced in Business Continuity Plan (BCP)/Business Impact Assessment (BIA).
		2. **Communicate with 3rd party vendors**
			1. Cyber Security
				1. Check with DHS NCCIC.
				2. Check with REN-ISAC.
				3. Check with Cloud Hosting Service Providers.
				4. If DNS related, contact InfoBlox or DNS service provider.
			2. Marketing Team
				1. Check with Cloud Service Provider hosting their materials.
				2. Check Social Media.
		3. **Global issues**
			1. Are there reports of global issues where the institution would be collateral damage?
				1. Check internet health and traffic reports to rule out global issues.
				2. Check Akamai Content Delivery Network (CDN).
		4. **Validate organization communication**
			1. Email
			2. Voice LAN Lines
	2. **DDoS Verified**
		1. **Infrastructure**
			1. Contacts Verizon or Internet Service Provider.
			2. Notifies Verizon of potential DDoS.
			3. Requests assistance to filter IP.
			4. Communicate with CISO.
		2. **Cyber Security**
			1. Determine type of DDoS🡪Reference Appendix A.
			2. Assess impacted systems.
				1. Minimal Impact-Monitor for escalation and prep for potential Major.
				2. Major Impact-CISO notifies IR team.
				3. Continue to coordinate with DEV Ops.
				4. Communicate with InfoBlox if DNS related.
				5. Communicate with IDS/IPS provider.
				6. PCAP Analysis (If required).
	3. **Mitigation🡪**
		1. **Cyber Security**
			1. Evaluate mitigation options for Source Address.
				1. Can Source Address be blocked at Firewall?
				2. Can source address or addresses be GeoBlocked by Firewall and/or IPS/IDS?

Consider business impact of GeoBlocking.

* + - 1. Can Patching mitigate (as some DDOS exploits a missing patch or vulnerability)?
			2. Is attack Host Based or IP Based?

IP Based Attack

Change Public IP address (Example, .133 would be changed to .134).

Consider failing over to DR site.

Host Based

Continuing pursuing Verizon assistance.

* + 1. **Mitigating specific applications**
			1. If prior mitigating solutions fail to cease DDOS traffic, next step would be to mitigate specific applications. These attacks may look like normal traffic but have anomalies that disrupt behavior in the server, application, or database tier.
		2. **Mitigating multiple attack vectors**
			1. If there are too many attackers to make blocking by IP address or region feasible, you may have to develop a plan to unwind the attack by mitigating “backwards”— that is, defending the site from the database tier to the application tier, and then to the web servers, load balancers, and finally the firewalls.
				1. As you identify the different mix of attack vectors, check the table below for remediation specific to individual attacks.



* + 1. **Network Layer Mitigation Techniques**
			1. Null Routing/Blackhole Routing
				1. Appendix A
			2. DNS Sinkholing
				1. Reference document/link in Appendix A that details process of Sinkholing.
			3. Scrubbing
				1. Reference document/link in Appendix that details process of Scrubbing.
		2. **Constrain resources**
			1. Reference document/link in Appendix A that details process of how to Constrain Resources.
	1. **Initiate Risk Assessment with Risk Manager**
		1. **Business impact**
			1. Customers affected by incident
			2. Good/Services affected by attack
			3. Worst case scenario if unable to mitigate
			4. Internal/External knowledge of attack (PR)
	2. **Document Attack Summary by Cyber Security Team**
		1. Document details of the attack to better help mitigating future occurrences.
	3. **Coordinate Public Relations with Corporate Communications Team**
	4. **DDoS Postmortem**
		1. **WHO**
			1. Bad Actor
				1. Did anyone take credit for the DDoS?
				2. Did they target your organization or were you collateral damage?
			2. Resolution Team
				1. Who internally/externally was engaged to assist?
				2. Were the internal resources the correct resources to engage?
		2. **WHAT**
			1. What was targeted?
				1. Did the DDoS target an IP, Host, URL, or App?
				2. What was impacted?
				3. What was the scope of impact?

Internal Systems, Network/Internet Access, Customer facing systems, Business partners, etc.?

* + - * 1. What early warning indicators of impending attack exist?
			1. What Systems alerted/failed to alert?
			2. What was the goal of attack? Successful?
		1. **WHEN**
			1. When did the event occur (holiday, weekend, night, day?)
			2. Did the event occur at a business-critical time?
				1. Financial Reporting
				2. Busy time of day
				3. Special activity occurring
		2. **WHERE**
			1. Where was the attack focused?
				1. Web Sites
				2. Branch office
				3. Corporate presence
			2. Are you sure?
				1. Is it possible the DDoS was a distraction to obfuscate an exfiltration?
		3. **WHY**
			1. Why were you attacked?
				1. Was the attack designed to gain notoriety?
			2. Why did the bad actor select the specific target?
				1. Was the attack designed to hide other activity?
			3. Why did we react the way we did?
				1. Was our reaction appropriate?
		4. **HOW**
			1. How were you attacked?
				1. Did the attacker use a strategy?
				2. Did the attack appear well coordinated?
			2. How did you respond?
				1. Did we take the correct response actions?
				2. Was the attack designed to hide the other activity?
		5. **NOW WHAT?**
			1. Document the answers posed to the questions.
			2. Document the responses to the incident.
			3. Document the identified gaps.
			4. Document the process improvements.







**APPENDIX A**

1. **DDoS**🡪 A malicious attempt to make a server or a network resource unavailable to legitimate users, by overloading it with massive amounts of fake traffic.
	* **DDoS Types**
		+ Volumetric
			- Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack’s goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).
		+ Protocol
			- Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).
		+ Application Layer
			- Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second (Rps).
	* **DDoS Attacks**
		+ DNS amplification
			- DNS amplification is a Distributed Denial of Service (DDoS) attack in which the attacker exploits vulnerabilities in domain name system (DNS) servers to turn initially small queries into much larger payloads, which are used to bring down the victim’s servers.
		+ DNS Flood
			- DNS flood is a type of Distributed Denial of Service (DDoS) attack in which the attacker targets one or more Domain Name System (DNS) servers belonging to a given zone, attempting to hamper resolution of resource records of that zone and its sub-zones.
		+ Fork Bomb
			- A fork is a system call used in Unix and Linux systems that takes an existing process (a.k.a, a parent) and replicates it, forming a new process (a.k.a, a child). This allows both processes to carry out unique tasks simultaneously. A fork bomb (also known as a “rabbit virus”) is a denial of service (DoS) attack in which the fork system call is recursively used until all system resources execute a command. The system eventually becomes overloaded and is unable to respond to any input.
		+ HTTP Flood Attack
			- HTTP flood is a type of Distributed Denial of Service (DDoS) attack in which the attacker exploits seemingly legitimate HTTP GET or POST requests to attack a web server or application. HTTP flood attacks are volumetric attacks, often using a botnet “zombie army”—a group of Internet-connected computers, each of which has been maliciously taken over, usually with the assistance of malware like Trojan Horses. A sophisticated Layer 7 attack, HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. As such, they demand more in-depth understanding about the targeted site or application, and each attack must be specially crafted to be effective. This makes HTTP flood attacks significantly harder to detect and block.
		+ Fragmentation Attack
			- IP fragmentation attacks are a common form of denial of service attack, in which the perpetrator overbears a network by exploiting datagram fragmentation mechanisms. Understanding the attack starts with understanding the process of IP fragmentation, a communication procedure in which IP datagrams are broken down into small packets, transmitted across a network and then reassembled back into the original datagram.
		+ NTP Amplification Attack
			- NTP amplification is a type of Distributed Denial of Service (DDoS) attack in which the attacker exploits publicly accessible Network Time Protocol (NTP) servers to overwhelm the targeted with User Datagram Protocol (UDP) traffic.
		+ Ping Flood
			- Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings. The attack involves flooding the victim's network with request packets, knowing that the network will respond with an equal number of reply packets. Additional methods for bringing down a target with ICMP requests include the use of custom tools or code, such as [hping](https://en.wikipedia.org/wiki/Hping) and [scapy](https://en.wikipedia.org/wiki/Scapy).
		+ Ping of Death
			- Ping of Death (a.k.a. PoD) is a type of Denial of Service ([DoS](https://www.incapsula.com/ddos/denial-of-service.html)) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command. While PoD attacks exploit legacy weaknesses, which may have been patched in target systems. However, in an unpatched system, the attack is still relevant and dangerous.
		+ Smurf Attack
			- Smurf is a network layer distributed denial of service (DDoS) attack, named after the DDoS.Smurf malware that enables it execution. Smurf attacks are somewhat like ping floods, as both are carried out by sending a slew of ICMP Echo request packets. Unlike the regular ping flood, however, Smurf is an amplification attack vector that boosts its damage potential by exploiting characteristics of broadcast networks.
		+ SNMP Reflection
			- An SNMP reflection is a type of Distributed Denial of Service (DDoS) attack that is reminiscent of earlier generations of DNS amplification attacks. Instead of Domain Name Servers (DNS), SNMP reflection attacks use the Simple Network Management Protocol (SNMP) - a common network management protocol used for configuring and collecting information from network devices like servers, hubs, switches, routers and printers. SNMP reflection attacks can generate attack volumes of hundreds of gigabits per second, which can be directed at attack targets from multiple broadband networks. Attacks are sometimes hours in duration, are highly disruptive to attack targets, and can be very challenging to mitigate.
		+ TCP SYN Flood
			- TCP SYN flood (a.k.a. SYN flood) is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.
		+ UDP Flood
			- “UDP flood” is a type of Denial of Service ([DoS](https://www.incapsula.com/ddos/denial-of-service.html)) attack in which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams. The receiving host checks for applications associated with these datagrams and—finding none—sends back a “Destination Unreachable” packet. As more and more UDP packets are received and answered, the system becomes overwhelmed and unresponsive to other clients. In the framework of a UDP flood attack, the attacker may also spoof the IP address of the packets, both to make sure that the return ICMP packets don’t reach their host, and to anonymize the attack. There are several commercially available software packages that can be used to perform a UDP flood attack (e.g., UDP Unicorn).
2. **Mitigation**
	* + GeoBlocking
			- GeoBlocking, as it pertains to the institution, is the ability to block traffic to and from a certain region/area.
		+ Null/Blackhole Routing
			- A null/blackhole route is a network route (routing table entry) that goes nowhere. Matching packets are dropped/ignored rather than forwarded, acting as a kind of very limited firewall.
		+ DNS Sinkholing
			- A sinkhole is a standard DNS server that has been configured to hand out non-routable addresses for all domains in the sinkhole, so that every computer that uses it will fail to get access to the real website. The higher up the DNS resolution chain the sinkhole is, the more requests it will block as it will supply answers to a greater number of lower NS servers that in turn will serve a greater number of clients.
		+ Scrubbing (Scrubbing Centers are typically used)
			- A scrubbing center is a centralized data cleansing station where traffic to your website is analyzed and malicious traffic (SQL injection, XSS, DDoS and other known exploits) is removed. Scrubbing centers are often used by ISPs and cloud providers because they prefer to route potential malicious traffic to an out of path data cleansing station rather than keeping it in network and bogging down the legitimate traffic. With an on-demand scrubbing center, when an attack is detected, the traffic is redirected (typically using DNS or BGP (Border Gateway Protocol)) to a local scrubbing center where the traffic is analyzed (usually using deep packet inspection) and the attack traffic is filtered out while the clean traffic passes back to the network for delivery.
		+ **Constrain Resources**
			- If previous steps fail, simply constraining resources, like rate and connection limit is a last resort – it can turn away both good and bad traffic. Instead, you may want to disable or blackhole an application.
3. **Key Personnel Contact Information**
	* **<Institution Insert who needs to be part of the solution to counter DDOS.>**
4. **3rd Party Vendor Contact Information**
	* Monitoring Service. **<Institution Insert who needs to be part of the solution to counter DDOS.>**
	* DHS NCCIC
		+ Email🡪notification@us-cert.gov
		+ Phone #🡪1-888-282-0870
	* Ren-ISAC
		+ Email🡪soc@ren-isac.net
	* InfoBlox-Org # 303776
		+ Phone #🡪1-888-463-6259; 1-408-986-4700
	* MSSP