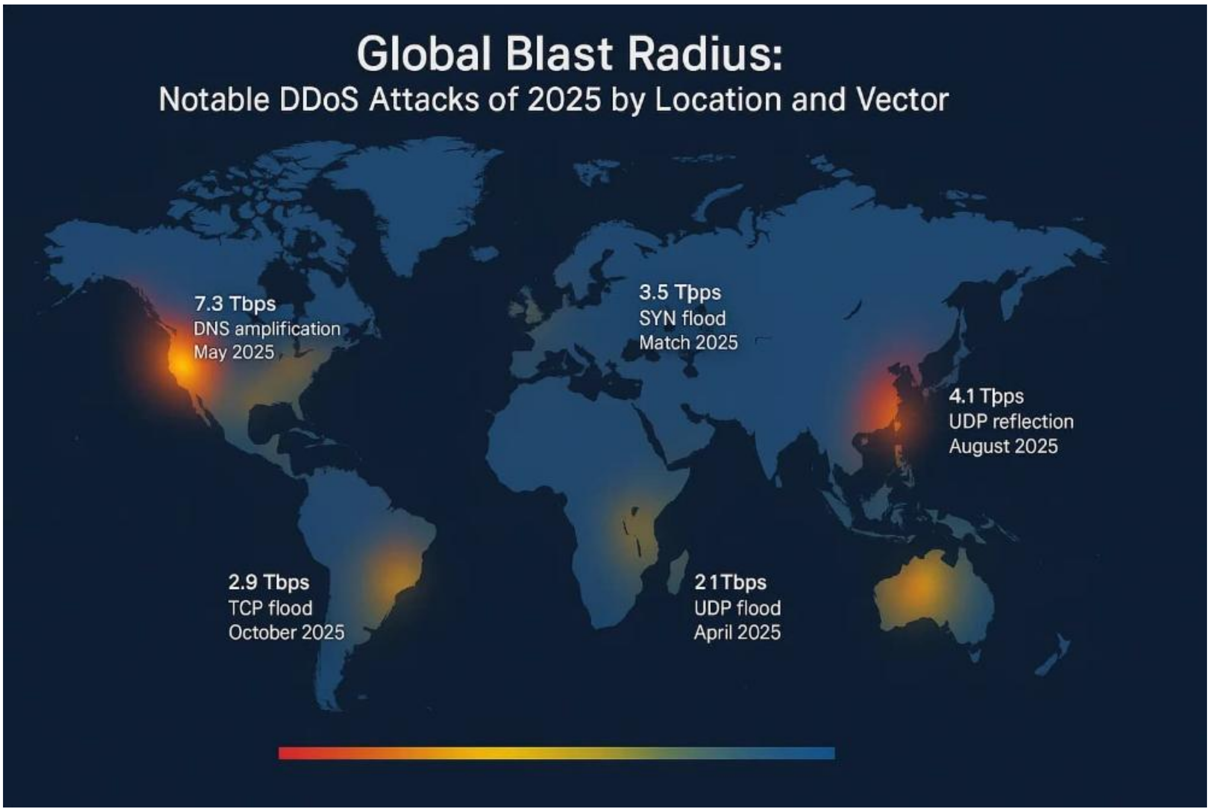
Distributed Denial of Service (DDoS) Attack Response Playbook

The Threat to Availability

A Distributed Denial of Service (DDoS) attack is a direct assault on the availability of our services. Unlike a data breach, which focuses on secrecy, a DDoS event aims to overwhelm systems, making critical applications unavailable to our customers and internal teams. The goal of this playbook is to outline a rapid, disciplined response strategy to maintain essential business functions and ensure service continuity during an event. Time is the most valuable commodity in a DDoS attack, and speed is paramount. A report by DeepStrike shows the impact of DDOS.



Phase One: Attack Identification

The first challenge is to accurately identify an attack and distinguish malicious traffic from a legitimate surge in user demand, such as a flash sale or a highly successful marketing campaign. Misclassification wastes valuable time and resources.

Clear Identification Parameters

1. **Network Traffic Pattern Analysis:** The security team must analyze network traffic to separate organic, legitimate traffic surges from the signature of an attack. Legitimate traffic usually follows predictable patterns and geographical origins, whereas attack traffic is often highly randomized, coming from thousands of disparate sources that suddenly appear simultaneously.
2. **Application Performance Degradation:** We establish specific, measurable performance degradation thresholds. If latency spikes beyond a defined metric, or if the server response time slows past an acceptable limit, it immediately triggers an investigation. These metrics serve as the tripwires that initiate a formal security response.
3. **Attack Signature Recognition:** We rely on systems to quickly recognize signatures for common attack methods. This includes volumetric attacks that flood the network pipe, protocol attacks that exploit weaknesses in the network layer, and complex application layer attacks that target specific server resources. Rapid signature matching allows for quicker mitigation deployment.
4. **Multi Point Monitoring:** Teams must leverage tools that provide simultaneous views of the network. This multi point monitoring is crucial to determine the **scope of the attack** and pinpoint the exact entry points being exploited. Understanding the full picture helps prevent localized, minor incidents from escalating into a system wide failure.
5. **Classification and Impact Framework:** Once confirmed, the attack is immediately classified based on its **severity** and the **potential business impact**. A low severity attack targeting a nonessential service will follow a different track than a high severity attack targeting a primary revenue generating application. This framework guides the resources allocated to the response.

Phase Two: Mitigation Activation

Once an attack is confirmed and classified, the playbook dictates the rapid activation of defensive measures designed to absorb or redirect the malicious traffic.

Specific Mitigation Strategies

1. **Traffic Filtering Rule Implementation:** Security operations teams must have predefined, tested procedures for implementing **traffic filtering rules**. These rules are rapidly deployed on firewalls and edge devices to block known

malicious source IP addresses or specific traffic patterns associated with the attack type.

2. **BGP Routing Adjustment Protocols:** For large scale volumetric attacks, internal BGP routing protocols are used to redirect incoming traffic. This process funnels the massive traffic volumes through specialized **scrubbing centers**, which are designed to filter out the malicious packets while allowing legitimate user requests to continue unimpeded.
3. **Cloud Based Protection Service Activation:** The organization relies on external, cloud based DDoS protection services as a primary defense layer. The playbook specifies the precise procedures required to activate and integrate these services immediately, shifting the burden of traffic absorption away from our own infrastructure.
4. **CDN Failover Mechanisms:** For application layer attacks, content delivery network (CDN) failover mechanisms are critical. By directing traffic through the CDN, we leverage its distributed capacity to handle the load and apply application specific protection, shielding the core application servers.
5. **Rate Limiting Implementation:** We use specific guidelines for implementing **rate limiting** on targeted applications. This involves capping the number of requests accepted from any single user or IP address over a short period, which helps protect application resources from being exhausted by botnets.
6. **Geographical Blocking:** In certain circumstances, especially when attacks are clearly originating from specific, known hostile regions with no legitimate business ties, the playbook permits the temporary consideration of **geographical blocking** to reduce the immediate attack surface.

Phase Three: Business Continuity Integration

Mitigation is only half the battle. This phase ensures that essential operations can continue even while the network is under stress.

Service Preservation and Communication

1. **Critical Service Prioritization:** The playbook includes a framework for **critical service prioritization**. During limited capacity situations, bandwidth and resources are diverted to maintain essential functions like payment processing or regulatory reporting, even if noncritical services must be temporarily degraded.
2. **Alternate Access Pathway Activation:** For internal teams, we must activate **alternate access pathways** to ensure essential employees can continue

operations. This might involve segregated VPNs or specific out of band management networks.

3. **Degraded Mode Operation:** Customer facing systems implement **degraded mode operation** procedures. This means temporarily serving stripped down versions of websites or applications that rely on minimal resources, allowing core functionalities to remain available to users.
4. **Internal and External Communication:** Clear **communication templates** are defined for both internal stakeholders and external customers. These templates provide timely, accurate updates on the service impacts, managing expectations and maintaining trust during a stressful period.
5. **Escalation Criteria:** The playbook provides clear escalation criteria for activating the **broader business continuity plan** if the attack severity exceeds the capacity of the standard IT response teams.

Phase Four: Post Attack Analysis

After the attack has been successfully mitigated and services are fully restored, the response team must immediately transition into a forensic and learning phase.

Review and Improvement

1. **Traffic Pattern Characterization:** Detailed traffic pattern analysis is performed to fully **characterize the attack**, including its duration, origin, volume, and specific tactics used. This deep understanding informs all future protection efforts.
2. **Infrastructure Resilience Assessment:** The team conducts a thorough **resilience assessment** of the infrastructure based on the attack impact. Did a specific component fail unnecessarily? This identifies weak points that require immediate attention.
3. **Protection Service Efficacy:** We formally evaluate the **efficacy** of the protection services used, noting any configurations that failed or performed poorly, and provide adjustment recommendations to ensure better performance during the next event.
4. **Attacker Identification:** Security analysts conduct forensics to determine if the attack left behind any identifying evidence that could lead to the **potential attacker identification**, which is shared with law enforcement if appropriate.
5. **Security Posture Improvements:** The most vital step is to translate these findings into tangible **security posture improvements**. All lessons learned are

incorporated into permanent, stronger controls and configuration changes to better withstand future, more sophisticated attacks.

This detailed plan ensures that when a DDoS event occurs, our response is unified, efficient, and immediately focused on protecting service availability and learning from the experience.