Understanding DoS and DDoS Attacks

A Denial of Service (DoS) attack involves an attacker flooding a target system, like a server or network, with excessive traffic or requests to render it unavailable to legitimate users. A Distributed Denial of Service (DDoS) attack scales this up by using multiple compromised devices—often forming a botnet—to launch a coordinated assault from various sources, making it harder to block. Both aim to overwhelm resources such as bandwidth, processing power, or memory, but DDoS attacks are more complex and impactful due to their distributed nature.

How DoS and DDoS Attacks Work

In a Do Humbug, a single source generates overwhelming traffic to exhaust the target's resources, causing slowdowns or crashes. DDoS attacks amplify this by leveraging a network of infected devices, such as computers or IoT gadgets, controlled remotely to bombard the target with synchronized data floods. Attackers often infect devices via malware, directing them to disrupt normal operations without necessarily breaching data.

Techniques Used to Execute Them

DoS and DDoS attacks employ various methods, including:

Volumetric Attacks: Flood the target with massive data volumes to consume bandwidth, such as UDP floods.

Protocol Attacks: Exploit weaknesses in network protocols, like SYN floods that tie up server connections.

Application-Layer Attacks: Target specific applications with seemingly legitimate requests, such as HTTP floods, to drain processing resources.

Amplification Attacks: Use third-party servers to multiply traffic, like DNS or NTP amplification, where small queries yield large responses.

Reflection Attacks: Spoof the target's IP to trick servers into sending responses back to it.

These methods can be combined in multi-vector attacks for greater impact.

Impacts on Systems

The primary impact is service unavailability, leading to downtime that can last from minutes to days. This causes financial losses from lost revenue, especially for e-commerce or online services, potentially costing millions. Reputational damage erodes user trust, while secondary effects include increased vulnerability to other threats like data theft during distractions. Overloaded systems may face hardware strain, higher operational costs for response teams, and legal issues if service-level agreements are breached.

Mitigation Strategies

Effective defense involves layered approaches to detect, absorb, and block malicious traffic. Key strategies include:

Monitoring and Detection: Use real-time tools with AI to identify anomalies in traffic patterns.

Traffic Filtering: Implement rate limiting, web application firewalls (WAFs), and blackholing to drop suspicious packets.

Capacity Planning: Employ content delivery networks (CDNs) and anycast routing to distribute traffic across global servers.

Partnerships: Collaborate with DDoS mitigation providers for scrubbing services that reroute and clean traffic.

Preparation: Conduct regular simulations, maintain incident response plans, and secure devices to prevent botnet inclusion.

Organizations should also focus on ingress filtering (e.g., BCP38) to prevent IP spoofing and restrict vulnerable protocols.

Examples and Case Studies

DDoS attacks have surged, with a 358% year-over-year increase in mitigated attacks during Q1 2025. Below are notable examples:

Mirai Botnet (Dyn, 2016): A botnet of IoT devices flooded Dyn’s DNS services with 1-1.5 Tbps, knocking major sites like Twitter and Netflix offline. The multi-vector attack caused widespread disruption, highlighting the need for IoT security and mitigation partnerships.

GitHub (2018): A Memcached amplification attack hit GitHub with 1.35 Tbps, causing a temporary outage for developers worldwide. Traffic was rerouted to mitigation partners, and transit capacity was expanded to recover.

AWS (2020): A CLDAP reflection attack targeted an AWS customer with 2.3 Tbps over three days, potentially causing revenue loss. AWS’s built-in defenses contained it, emphasizing protections against reflection attacks.

French Home Supply Store (2025): An HTTP/2 Rapid Reset attack combined with traditional floods at 6M requests per second lasted over two hours, causing downtime, financial losses, and reputational harm. AI-driven detection and multi-layered defenses like WAFs were recommended.

Indonesian Government Agency (2025): A staged HTTP/2 Rapid Reset attack at 10M requests per second for 14 hours led to extended slowdowns and service loss. Incident response plans and traffic analysis tools were critical for mitigation.

Cloudflare Customer (2025): A 7.3 Tbps carpet-bombing attack across multiple ports targeted a hosting provider but was contained. Cloudflare’s autonomous systems blocked it, underscoring the need for advanced protections.

These cases highlight the escalating scale and sophistication of DDoS attacks in 2025, emphasizing the importance of proactive, tech-driven defenses.