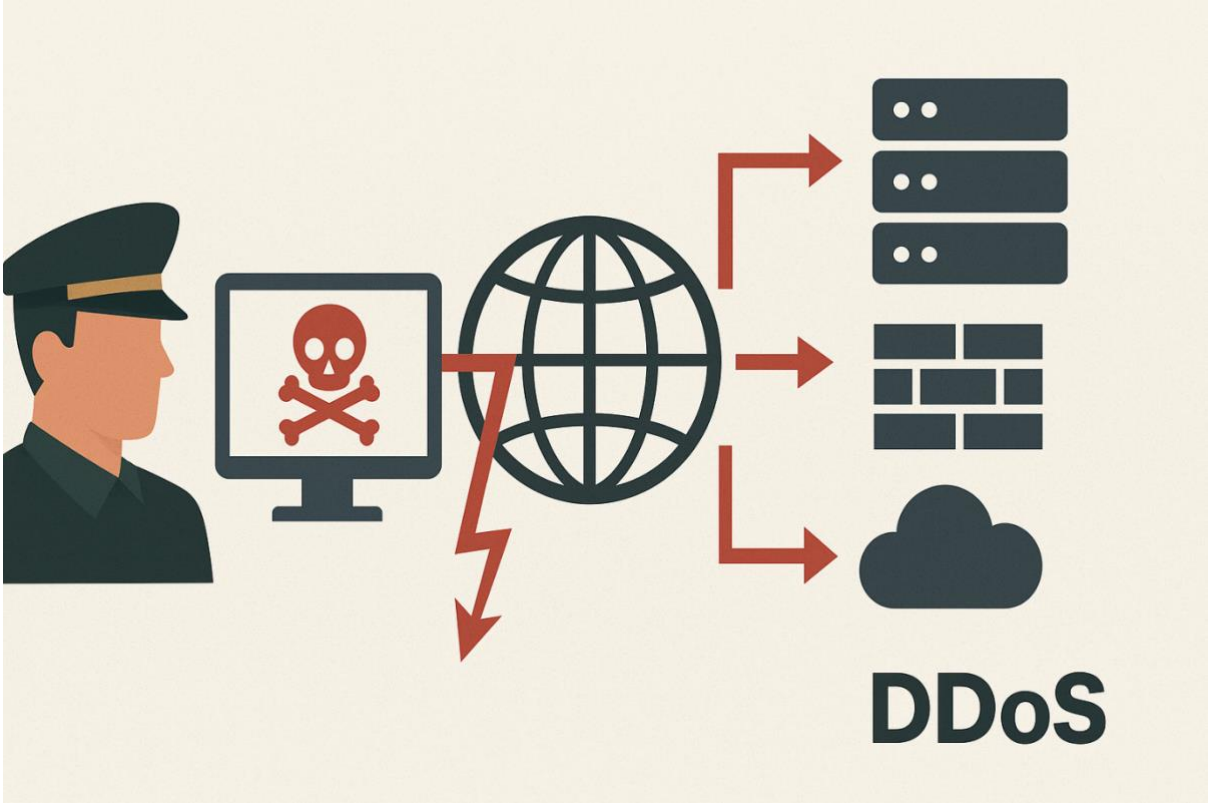
H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER COMMAND
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2025-11

Understanding and Mitigating Distributed Denial of Service (DDoS) Attacks



Overview

DDoS attacks are among the most common and disruptive forms of cyber-attacks. In a DDoS attack, adversaries flood a target network, server, or service with massive traffic, often coming from thousands of compromised devices until the system becomes slow, unresponsive, or completely unavailable. These attacks can cripple websites, interrupt critical services, and cause widespread operational delays.

DDoS attacks typically leverage large-scale “botnets” networks of infected or hijacked computers, IoT devices, or servers controlled by attackers. When activated, the botnet sends huge volumes of traffic toward a target. This overloads bandwidth, exhausts system resources, or exploits specific network protocols.

Common types of DDoS attacks include:

- **Volumetric Attacks** – Overwhelm bandwidth using massive amounts of data traffic.
- **Protocol Attacks** – Exploit network protocols like SYN, UDP, or ICMP to exhaust system resources.

- **Application Layer Attacks** – Imitate legitimate user activity to overload high-level services, such as HTTP or DNS.

AFP personnel monitoring their networks and information systems must be alert of the following red flags which may indicate a DDoS attack:

- Sudden slowdown or unresponsiveness of AFP websites or services
- Repeated connection timeouts
- Unusually high spikes in network traffic
- Service unavailability even with normal system load
- Multiple connection attempts from unfamiliar or foreign IP addresses

If such attacks were not promptly addressed, this could result in disrupted information systems services, delayed internal communications, compromised mission continuity, reduced accessibility of command systems and increased vulnerability to follow-on attacks.

Recommendations

In this regard, AFP personnel are advised of the following measures:

- Implement load balancing, firewalls, and anti-DDoS filtering systems.
- Monitor network traffic patterns for anomaly detection
- Coordinate with ISPs for immediate traffic rerouting or rate limiting
- Report any unusual system performance or accessibility issues
- Avoid clicking suspicious links that may activate botnet malware.
- Ensure work devices are updated and protected by antivirus and endpoint security
- Strictly use AFP secured networks when accessing official platforms

Conclusion

DDoS attacks remain one of the most disruptive and accessible weapons available to cyber adversaries, from hacktivists to state-sponsored actors. Their ability to overwhelm systems, degrade mission-critical services, and create widespread confusion makes them a persistent threat to both civilian institutions and military operations. By strengthening network defenses, enhancing monitoring capabilities, coordinating closely with service providers, and continuously educating personnel, organizations can significantly reduce their vulnerability to these attacks. As the threat landscape evolves, proactive cybersecurity readiness, combined with disciplined reporting and rapid response is essential to maintaining operational continuity and protecting national security interests.

References:

a. *https://www.akamai.com/glossary/what-is-ddos*
b. *https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/*
c. *https://www.cisa.gov/sites/default/files/2024-03/understanding-and-responding-to-distributed-denial-of-service-attacks_508c.pdf*