FEDERAL MINISTRY OF
COMMUNICATIONS AND
DIGITAL ECONOMY, NIGERIA

NITDA
National Information Technology
Development Agency

CERRT.NG

ADVISORY ON DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK TARGETED TOWARDS CRITICAL DIGITAL INFRASTRUCTURE

NCA-010823-01

Overview

In the wake of significant cyber-attacks globally, most especially distributed denial-of-service (DDoS) attacks that has affected critical digital infrastructure, resulting in disruption of essential government services. The occurrence of these attacks underscores the undeniable and concerning fact that cyber-attacks are not a distant threat but rather a looming danger that resides much closer to us than we may have previously acknowledged. This realization compels us to recognize the urgency of reinforcing our cyber front, fortifying our digital defenses to shield against these malicious intrusions and secure the safety of our critical information and infrastructure.

Impact

The consequences of such cyber-attack are always severe and may have wide-ranging impacts which includes: Disruption of critical services, Economic Losses, as well as Public Trust and Reputational Loss.

Preventive Measures

To guide against attacks targeted towards Government Institutions and other critical sectors, the National Information Technology Development Agency's Computer Emergency Readiness and Response Team (NITDA-CERRT) seek to advise all Ministries, Departments, and Agencies, including other providers of critical services in the country to ensure the implementation of measures to prevent against DDOS attacks, such as:

a. Deploying DDoS Monitoring systems to watch out for signs of DDoS attacks.
b. Minimize the attack surface area thereby limiting the options for attackers and allowing you to build protections in a single place. E.g. obscuring the target, closing unused ports and protocols, hence minimizing possible points of attacks.
c. Implement or subscribe to DDoS Protection features, applications or services to fortify your cyber defenses against disruptive DDoS attacks. e.g. rate limiting, load balancing, traffic filtering, Content Delivery Network (CDN), Web application Firewalls, etc.
d. Ensuring that hosting providers offer abundant redundant Internet connectivity, enabling systems to manage significant volumes of traffic effectively.

Furthermore, enhancement of all critical national infrastructure such as financial services providers, telecommunications providers, and relevant government service providers should ensure cybersecurity readiness and resilience by implementing necessary cybersecurity measures to safeguard against potential attacks.

For further enquiries, please contact CERRT.NG through the following channels:

cerrt@nitda.gov.ng

+234 817 877 4580

www.cerrt.ng

@NITDANigeria | www.nitda.gov.ng