الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

Cyber Security Guidelines

Distributed Denial of Service (DDoS) Attacks

Public

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled “Cyber Security Guidelines for DDoS Attacks” - V 2.0 - to help organizations, understand and mitigate DDoS attacks.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the “Cyber Security Guidelines for DDoS Attacks”.

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the NCSA. NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

Document Control

Document Details	
Document ID	IAG-NGE- DDOS
Version	V 2.0
Classification & Type	Public
Abstract	This document is intended as a guidance to help organizations understand and mitigate the threat of Distributed Denial of Service attacks.

Review / Approval

Department/Role	Reviewed/Approved	Version	Date
National Cyber Governance and Assurance Affairs		2.0	

Revision History

Version	Author(s)	Revision description	Date
1.0	CSPS	Published	March 2018
2.0	CSPS	Published	January 2023
2.0	CSPS	Published with minor corrections	December 2023

LEGAL MANDATE(S)

Emiri decree No. (1) of the year 2021 regarding the establishment of National Cyber Security Agency, sets the mandate for the National Cyber Security Agency (hereinafter referred to as “NCSA”). The NCSA has the authority to supervise, regulate and protect the security of the National Critical Infrastructure via proposing and issuing policies and standards and ensuring compliance.

This document has been prepared taking into consideration current applicable laws of the State of Qatar. In the event a conflict arises between this document (specific provision or clauses) and the laws of Qatar, the latter (law), shall take precedence. Any such term (specific provision or clauses), to that extent shall be deemed omitted from this Document, without affecting the remaining provisions of this document. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Table of Contents

1 Introduction

1.1 Context

Information systems today face unprecedented risks from a range of threat actors. These risks include non-availability of information. This risk is perpetrated through several attacks such as APT attacks which wipeout the storage systems, network denial and distributed denial of services attacks, physical attacks on the information systems and its processing facilities etc.

Distributed Denial of Service (DDoS) flooding attacks are one of the biggest concerns for organizations networks availability nowadays. Whereas there is no compromise of the information systems itself, the attacks render the system inaccessible for its legitimate users through a network flood attack.

Distributed denial of service (DDoS) attacks is growing, in terms of size, complexity, and malice.

2 Purpose, Scope, and Usage

2.1 Purpose

This document aims to help organizations in the state of Qatar to understand DDoS attacks and strategies and techniques to mitigate such attacks.

2.2 Scope

All organizations with publicly accessible services in the state of Qatar.

2.3 Usage

The guidance provided in this document will help organizations secure their public facing infrastructure against DDoS attacks. The document provides an understanding of different kind of DDoS attacks and remediation against the same.

3 Key Definitions

Organizations	Any organization including government / semi-government agencies, commercial organizations etc.

4 Guidelines

4.1 What is a DDoS Attack?

A denial of service (DoS) attack is any attack that prevents a legitimate user from accessing a network resource. A distributed denial of service (DDoS) attack is one that uses multiple network resources as the source of the specific attack vector. The use of multiple resources is primarily intended as a method to amplify the capabilities of a single attacker, but it can also help to conceal the identity of an attacker and complicate mitigation efforts.

There are different types of DDoS attacks. Volumetric attacks are the most common types of DDoS attack. These attacks use multiple infected systems—which are often part of a botnet– to flood the network layers with a substantial amount of traffic that impede the passage of legitimate traffic causing unavailability of systems for the period of the attack. Non-volumetric attack explores many technics like protocol attacks and applications attacks by rendering target in accessible by exploring weakness of protocols. While the application attacks explore vulnerabilities and business logic flaws. Reflection attacks is a hybrid attack in which the attacker uses forged source IP addresses in conjunction with specific protocol susceptibility to amplify and direct a DDoS attack

In most cases, the attacker uses compromised computer resources without the knowledge of the owner. Within the larger scope of information security, DDoS attacks fall within the "availability" pillar of the CIA Triad.

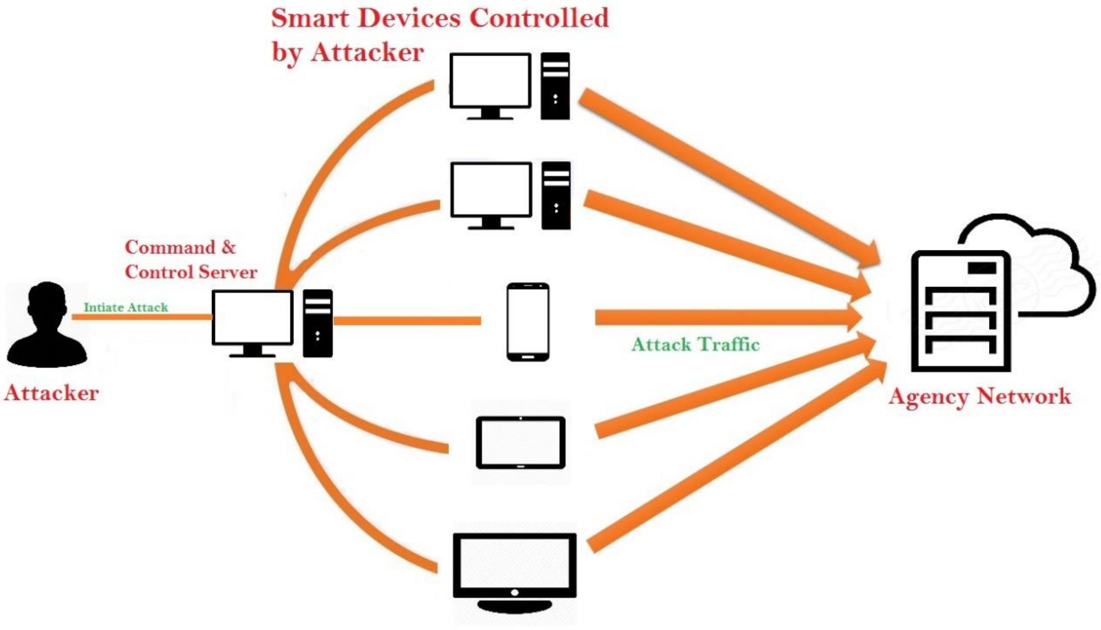

Figure 1 Illustration of a Distributed Denial of Service

4.2 Types of DDoS Attacks

4.2.1 Volumetric Attack

Volumetric (Bandwidth) attacks are the most common DDoS attacks, a volumetric DDoS attack is any attack that attempts to overwhelm the target by saturating the available network capacity. Volumetric DDoS attacks are possible due to the relatively small network capacity of a target compared to the overall capacity of all Internet connected devices. Especially nowadays with the emergence of the Internet of Things (IoT), there are hundreds of millions of devices that attackers can use to send bogus traffic to target, Example is the attack of DYN on 21 Oct 2016 where attackers used thousands of CCTVs which are connected to the internet to initiate an attack on DYN company causing disruption on critical services which impacted big companies like Amazon, Spotify and HPO.

4.2.2 Protocol Attack

Protocol attacks are a diverse collection of various attacks intended to cause disruption to an environment by exploiting a specific weakness or inefficiency in the protocol. Many of these attacks exploit weaknesses of Layer 3 and 4 protocols such as TCP, IP and UDP. Protocol attacks consume all the processing capacity of the attacked-target or intermediate critical resources like a firewall causing service disruption.

4.2.3 Application Attack

Application-level attacks or layer 7 in the OSI model attacks are a diverse collection of attacks intended to cause disruption to an environment by exploiting specific weaknesses or inefficiencies in an application. The key differentiator between application-level and other attacks is that the attack traffic is "in protocol," meaning that the traffic is legitimate from a protocol perspective. By being "in protocol," the attacks are often difficult to distinguish from legitimate traffic. Application attacks establish a connection with the target and then exhaust the server resources by monopolizing processes and transactions.

4.2.4 Low-Rate DDoS Attack

A very hard attack to detect attack in which the attacker sends malicious traffic at lower transmission rate to mislead traditional anomaly-based DDoS detection techniques. These attacks often aim at leaving connections open on the target by creating a relatively low number of connections over a period and leaving those sessions open for as long as possible. Common methods include sending partial http requests, such as Slowloris, and Slowpost (a DDoS tool which completes the handshake) and sending small data packets or keep alive in order to keep the session from going to idle timeout. These attack vectors are often intermingled with the high-rate volumetric attacks and fly under the radar making them not only very hard to block but also to detect.

4.3 Understand the Risk

Not all companies, government organizations are common target nor have high-risk profile of being attacked. Most organizations need to understand their profile within an attack scenario. Financial institutions, organizations involved in big events (i.e. world cup, elections) and few others have a much higher risk than other organizations that are not in aforementioned profile. Organization needs to evaluate their current profile, historical information about past two-year attacks to determine the level of risk. Also, there other criteria that need an evaluation. Which systems are considered as critical and which system can survive to a DDoS attack without disrupting any critical service? That will help determine which level of DDoS protection (investment) will be necessary to maintain availability.

4.3.1 Likelihood of being attacked:

This risk classification is primarily based upon the size and industry of the organization, historical information (if the organizations has been attacked in the last few years?) and how it might relate to the motivations of an attacker. For this task, refer to our Information Security Risk Management Framework (ISRMF).

4.3.2 Who may attack your organization?

DDoS attack threat actors could be either internal or external. Internal threat agents include internal employee/s, contractors etc. External threat agents include hacktivists, cyber criminals, and state-sponsored actors.

Defining your threat actors help organizations to understand the attacker's capabilities and the attack complexity also it's a strong factor on deciding on the organizations' mitigation strategies.

4.3.3 Attacker Motivation:

Attacker's motivations can vary from financial gain, personal vendetta, self-acclaim, patriotism, political or religious affiliations, activism or any other different reason.

4.3.4 Identify Areas of Risk:

For an organization to identify the areas of risk they need to:

1. Understand overall industry risks
2. Identify business critical systems
3. Cost of downtime

And on the technical side organization need to:

1. Validate capacity of network equipment
2. Identify all publicly accessible services
3. Create an inventory of dynamic contents areas

4.3.5 Why are DDoS attacks so effective?

Several factors have helped in making DDoS attacks widely used, its easiness comes on top of the list as the attacker does not need to study on the target infrastructure or platform to perform a DDoS attack, nevertheless DDoS attacks can be complex sometimes, especially using internet of things and CDNs.

Other important factors being that DDoS attacks are difficult to diagnose, require minimal attacker resources and spoofed sources as the attack source IP address can be and usually is forged.

4.3.6 DDoS Impact:

Depending on the type of DDoS attack, the impact could be one or more of the following:

Link saturation: When more traffic is sent to a link than it can transmit, excess traffic is dropped by the upstream network device. This results in significant packet loss, causing either performance degradation or a full network outage.

Increased load on network devices: Causes higher than normal resource utilization on network devices such as routers, switches, and firewalls. The devices may reboot, hang, or otherwise degrade in performance.

Increased memory usage on network devices: DDoS attacks may result in exhausting memory on devices that track network connection state like firewalls, IPS/IDS, or load balancers.

Increased resource usage on application servers: Application DDoS attacks will cause sudden increase in CPU or memory utilization.

Increased resource usage on database systems: Application DDoS attacks can cause increase resource usage on application supporting systems such as a database server.

Reach arbitrary limits: DDoS attack may cause reaching the network stack limit “if specified” which results in rejecting other legitimate connections

Increased network costs: DDoS attack can raise IT costs by artificially increasing link utilization

Conceal other attack vectors: DDoS attack produces so much traffic that it may make it difficult to detect more subtle attacks that may be occurring simultaneously.

Irrespective of the technical impact on the device as listed above, invariably it leads to loss or unavailability of service, which may have a financial, reputational or legal impact.

4.4 How to Mitigate DDoS Attacks

4.4.1 General Controls – Being prepared

1. Design:
   a. Protect critical services such as DNS servers and other critical services such as e-mail, web etc.
   b. Use different IP ranges for different services based on criticality.
   c. Consider appropriate DDoS mitigation techniques like “scrubbing” when designing your network.
   d. Ensure you have a business continuity plan and appropriate disaster recovery procedures in place, refer to *4-9 Business Continuity Management [BC] in the NIAS*. Organizations should create a playbook to deal with DDoS crisis, which includes communication plan, incident response strategy.
2. Document:
   a. Document your IT infrastructure details, this should include IP address assignments, network topology diagrams, routing settings, network and security devices configurations, hardware, and software details etc. Refer to *NIAS 4-12 Documentation [DC] and Section 5-2 Network Security [NS]*.
   b. Create a whitelist of IP addresses (internal and external) and protocols that must be always allowed and its priorities.

3. Technical:
    a. Harden your Infrastructure (network. Platforms, applications, OSSs) that could be affected by a DDoS attack.
    b. Use source address rate limiting.
    c. Use HTTP/HTTPS JavaScript challenge to recognize the legitimate browser-based clients.
    d. Adhere to best practices while configuring DNS time-to-live (TTL) settings. Lower values can facilitate DBS re-direction if the original IP addresses is attacked. 600, is a good TTL value.
4. Monitoring:
    a. Baseline your infrastructure's performance so that anomalies can be identified quickly.
    b. Use anomaly detection to watch your performance metrics and detect if a DDoS attack is in progress.
5. Emergency Contact:
    a. Create a Contact list to reach out to personnel (internal teams and support vendors) during an incident including DDoS attack. Refer *to 4-8 Incident management [IM] in the NIAS*.
    b. Establish contact with NCSA, law enforcement agencies and your ISP
6. Evaluate third-party offerings:
    a. Consider deploying a 24 ×7 emergency response using advanced Anti-DDoS technology (e.g., provided by an anti-DDoS vendor or your ISP).
    b. Consider a combination of services/technologies (cloud and on-premises) to close gaps. Examples would be DNS protection, web application firewalls, scrubbing centers, on-premises appliances for non-volumetric attacks, API protection.
    c. Consider using content distribution network (CDN), a geographically distributed network of proxy servers and their data centers. CDNs provide massive capabilities of mitigating DDoS attacks.

4.4.2 When the Attack Begins:

4.4.2.1 Analyze the attack

1. Identify the flow of attack. Ascertain if you are the target, a collateral victim, or a part of the compromised botnet.
2. Make necessary copies of the log files for servers, network and security devices that are impacted as forensic evidence
3. Identify the services that are impacted, the source of attack IP addresses, the protocols and the ports used in the attack.
4. Check if there was any potential warning or threat issued prior to the attack.

4.4.2.2 Mitigate the attack

1. Based on the information collected try mitigating the attack:
    a. Block the malicious traffic on your network by either blocking malicious source IPs, protocols or specific ports on the boundary routers, firewalls or gateway devices if possible.
    b. If possible, request your ISP to block the malicious traffic at their end.
    c. Shutdown, if possible, any application or a particular feature of an application that is being targeted (as long as it is not a core business application).
    d. Terminate unwanted connections or services on the servers and routers.
    e. If the DDoS has compromised a vulnerability in the systems (servers, application, network, and security devices), use alternatives such as application

firewalls, host intrusion detection systems (HIDS), virtual patching to work around until the system is patched.

f. If possible and if required, invoke your BCP / DRP to switch your IT Operations to alternate sites

g. Report the incident to Q-CERT and law enforcement agencies as required by the regulations and laws.

h. Apply specific controls based on attack type, such as:

<u>Volumetric:</u>

1. IPs Blocking "clean pipes" from the ISP, this approach can be effective at mitigating simplistic attacks, but will often be unable to mitigate more complex scenarios.
2. Consider using null routes with border gateways protocol (BGB) to help prevent devices on the internet from sending traffic to the organization's IP.
3. Use threat intelligence solutions to identify which traffic to discard or allow based on the source history of malicious or legitimate traffic.

<u>Protocol Attacks:</u>

1. Blocking with on-premises devices. IDS/IPS may provide limited help, application firewalls (e.g., web application firewalls (WAF)) may provide better protection against these attacks.
2. A dedicated DDoS mitigation service, like that provided by third party vendors, is often the most effective, with advanced capabilities specific to identifying and blocking protocol DDoS traffic.
3. Using SYN cookies to protect the server SYN queue from filling up under TCP SYN floods (a DoS attack that relies on abusing the standard way that a TCP connection is established).

<u>Application Attacks:</u>

1. Just like protocol attacks, blocking with on-premises devices such as IDS/IPS and firewalls may be successful due to the low bandwidth nature of these attacks. The success may be limited in a major attack.
2. Solutions like WAF, Anti BOT solutions, Anti DNS solutions or specialized devices may provide a better protection.
3. Application blocking (temporarily disabling a feature) may also be considered in certain cases if the service being attacked is not used or does not have a significant impact on business.

4.4.3 When the Attack Stops:

4.4.3.1 Recovery from attack

1. Ensure that the DDoS attack has ended and that all the services are reachable again.
2. Ensure that the performance of your system is in line with your baseline performance.
3. Ensure that any mitigating measures such as blocking of specific traffic, protocol or ports are rolled back.
4. Switch back the systems from DR site to the original site (if DR / BC invoked).

5. Review the incident from beginning; identify the lessons learnt including what could have been done better?
6. Put in a plan to implement the lessons learnt to avoid a similar experience in future

5 Compliance and Enforcement

5.1 Compliance and Enforcement

This guideline is published to help organizations better understand the threat of DDoS attack and how to mitigate against such threats. The guideline complements the National Information Assurance Standard and the National Data Classification Policy.

6 Annexes

6.1 Acronyms

APT	Advanced persistent threat
BGB	Border gateways protocol
CDN	Content distribution network
DDoS	Distributed Denial of Service
DoS	Denial of Service
HIDS	Host intrusion detection systems
ISP	Internet service provider
IP	Internet protocol
IoT	Internet of Things
ISRMF	Information security risk management framework
OSI Model	Open systems interconnection model
UDP	User datagram protocol
TCP	Transmission control protocol
WAF	Web application firewalls
NCSA	National Cyber Security Agency
NIAS	National Information Assurance Standard
DCLS	National Data Classification Policy

6.2 References

No references

6.3 List of Figures

6.4 Reporting Incidents to NCSA

Agencies that are experiencing a DDoS attack may report an incident to NCSA in one of the following ways:

Call NCSA Hotline at 16555 (24 x 7 service)

Email NCSA at ncsoc@ncsa.gov.qa

Agencies may also find the following guidelines useful to prepare themselves to face an attack / incident.

Guidelines for Incident Management – Pre-requisite Measures