DDoS Overview and Incident Response Guide

July 2014

Contents

1. Target Audience

This document is aimed at general IT staff that has undertaken the responsibility of being prepared in response to DDoS incident. This document only provides high-level guidelines. It does not supersede any specific applicable policies or procedures, which should be followed if they exist.

Different approaches are possible and may be valid. This document should rather be seen as a guideline in case of the absence of more specific local policies and procedures related to this topic.

In case of doubts or any additional questions about this document, do not hesitate to seek further advice and assistance from your respective authorities or CERT-EU team.

2. Introduction

A distributed denial-of-service attack (DDoS attack) is a malicious attempt from multiple systems to make computer or network resources unavailable to its intended users, usually by interrupting or suspending services connected to the Internet.[1]

The concept of distributed denial of service (DDoS) attacks has changed radically in recent years. High-profile attacks against institutions, governments and private bodies have highlighted the importance of availability. This has profound implications on the threat landscape, risk profile and network architecture. The need for multi-layered defense and cooperation is essential.[2]

Strategies to mitigate DDoS, initially with prevention but eventually by designing multilayered defense strategies need to be adopted. Therefore, DDoS threats should be taken into account on risk planning much like site selection, power outages and natural disasters.

CERT-EU has focused on procedures for securing IT infrastructure from threats against Availability. CERT-EU studies and utilises proven DDoS identification and mitigation methods that can effectively and efficiently respond to DDoS attacks.

3. The Growing DDoS Problem

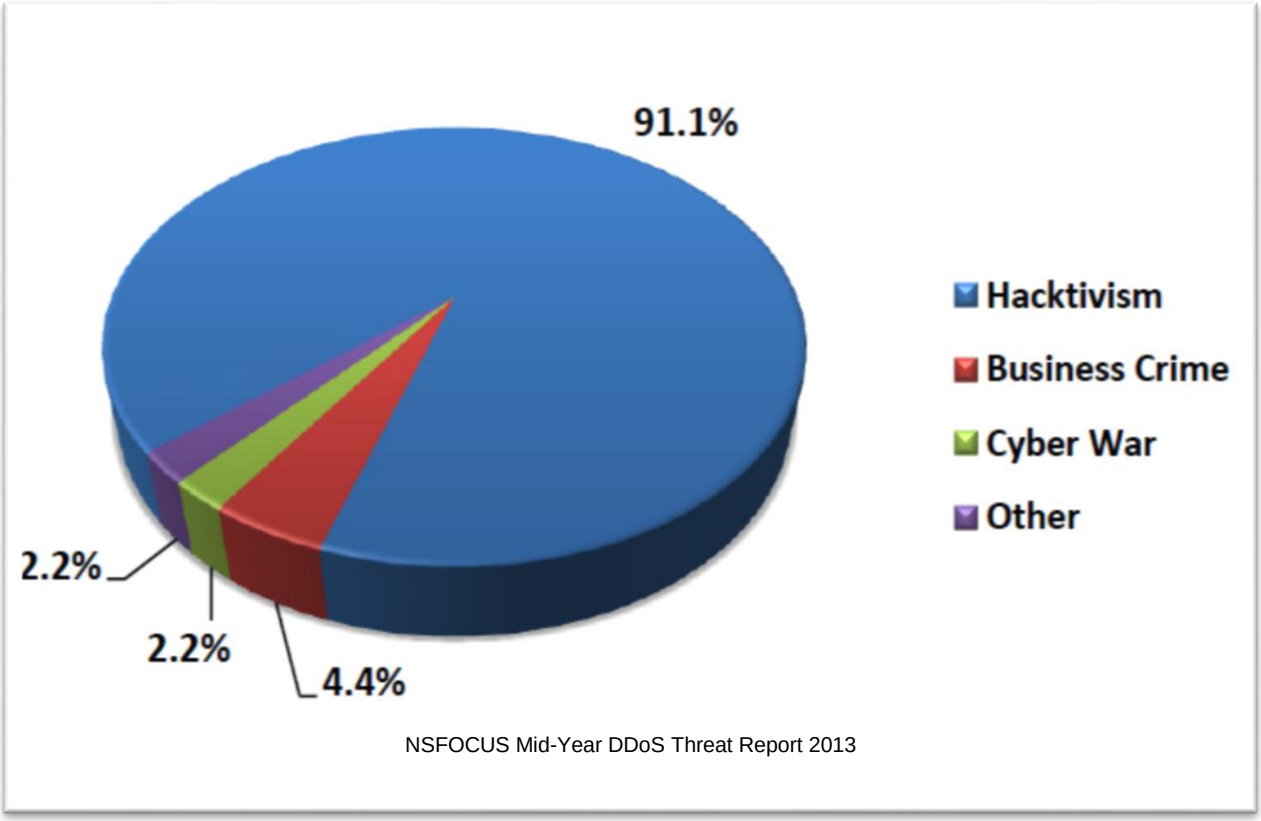
DoS attacks largely derive from people with anger or complaints against organisations, companies and web sites. Criminal activity, cyber warfare and unethical competition are also factors that systematically abuse high profile/high gain services. DDoS can also be used as a mean of distraction. In the case of Sony (2011) and in U.S. banking industry (2013), DDoS attacks intended to mask parallel intrusions into systems with sensitive personal and financial data[3].

[1] Incapsula. "Denial of Service Attacks". <http://www.incapsula.com/ddos/ddos-attacks/denial-of-service>.

[2] Frost & Sullivan. "Why Anti-DDoS Products and Services are Critical for Today's Business Environment"

[3] Corero. "Network Security Reports on Top 5 DDoS Attacks of 2011". <http://www.corero.com/en/company/news_and_events?item_id=4>

The picture below shows the composition of DDoS attacks related to the attack motive.



NSFOCUS Mid-Year DDoS Threat Report 2013

NSFOCUS Mid-Year DDoS Threat Report 2013, states that major DDoS events happen every two days, and one common DDoS attack happened every two minutes.[4]

In general, DDoS attacks are becoming more powerful. On March 18 2013, a DDoS attack was launched against Spamhaus' website, e-mail servers, and DNS IPs. In the attempt to affect Spamhaus' services different techniques were used, such as DNS amplification and BGP hijacking. The peak volume of this attack was reported to be 300Gbps. [5]

Arbor Networks reports that the average size of an attack is 2,64 Gbps, an increase of 78% percent from 2012. Interestingly, duration is reduced. About 87% percent of the attacks last less than one hour.[6]

4 NSFOCUS. "Mid-Year DDoS Threat Report 2013".<http://en.nsfocus.com/SecurityReport/2013%20NSFOCUS%20Mid-Year%20DDoS%20Threat%20Report.pdf>
5 Spamhaus. " Answers about recent DDoS attack on Spamhaus". < http://www.spamhaus.org/news/article/695/>
6 Arbor Networks. "Arbor Networks Releases Q3 Global DDoS Attack Trends Data". < http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5026-arbor-networks-releases-q3-global-ddos-attack-trends-data>

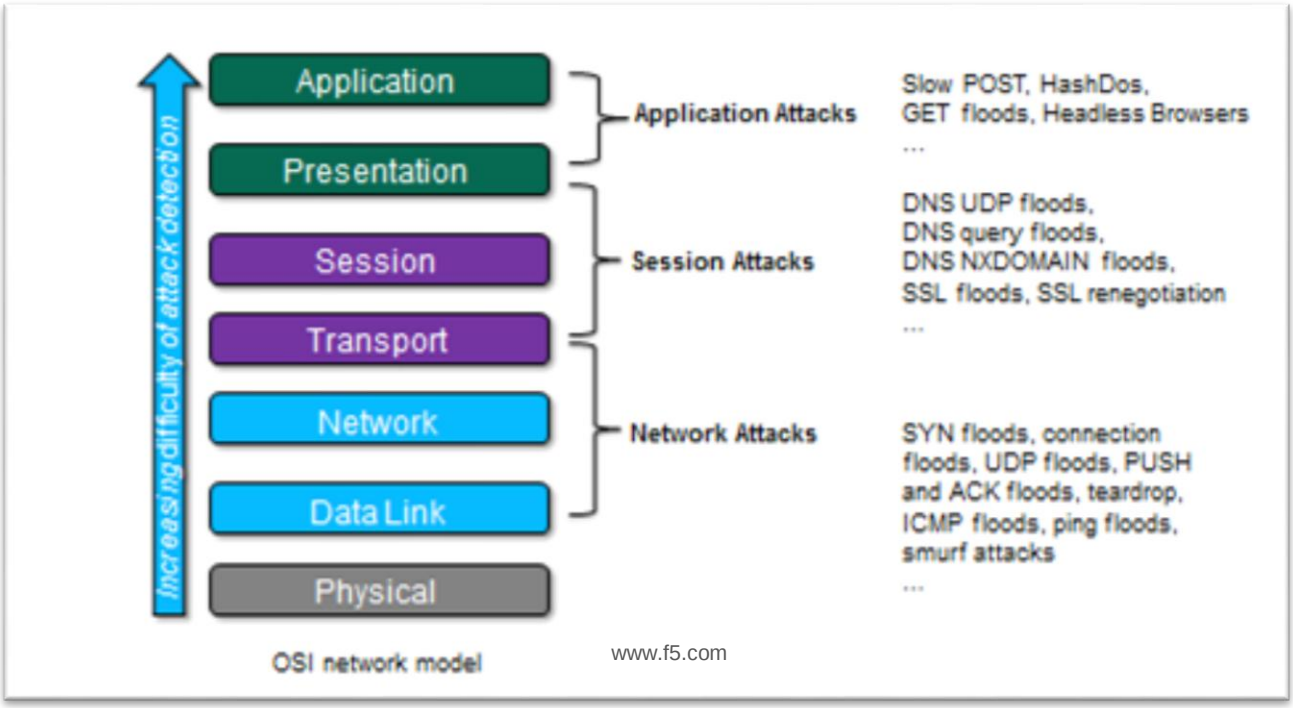
4. DDoS Attack Categories

There are three primary categories of DDoS attacks[7]:

Volume Based Attacks: Include UDP, ICMP, and other spoofed-packet floods. The attack aims to saturate the bandwidth of the targeted resource. Magnitude is measured in bits per second.

Protocol Attacks: Include SYN floods, fragmented packet attacks, Smurf DDoS and more. This type of attack consumes actual server resources, or resources on the intermediate equipment, such as firewalls and load balancers. Magnitude is measured in packets per second.

Application Layer Attacks: Include slow POST, HashDos, GET flood, clogging and more. This attack sends data according to specific features of well-known applications such as HTTP, DNS, SMTP, SSL. Comprised of seemingly legitimate packets, the goal of these attacks is the depletion of certain resources in the application. Magnitude is measured in requests per second.
The picture below shows the layering of DDoS attacks on the OSI network model



[7] INCAPSULA. "Distributed Denial of Service Attacks". < http://www.incapsula.com/ddos/ddos-attacks>

5. DDoS Mitigation

An effective, immediate response is difficult and may depend on third parties, such as ISPs and DDoS mitigation specialists. These external partners have large scale infrastructures and use a variety of technologies for identification, containment and remediation. Therefore, DDoS attacks can be identified and mitigated before they reach the organisation's premises. Additional tasks, especially on attack types at Network layer like bandwidth prioritisation and sinkholing may be performed at End User/ Organisation level.

The following table summarises a proposed DDoS mitigation guide

STAGE	ACTIONS
1. Preparation	• **Contacts and Procedures** • **ISP and specialized support** • **Network & Infrastructure setups**
2. Identification	• **Detection and Alerting** • **Attack analysis** • **Motivation identification** • **Mitigation acquirement / refinement** • **Traceback**
3. Containment	• **Network modifications** • **Content delivery control** • **Traffic control**
4. Remediation	• **Bandwidth prioritization and blocking** • **Traffic-scrubbing** • **Sinkholing**
5. Recovery	• **Normal state verification** • **Rollback**
6. Aftermath	• **Incident review and information disclosure** • **Law enforcement**

Proposed course of action per mitigation stage

1. Preparation

Contacts and procedures:

- Maintain contact information for team members and others within and outside the organization such as ISP, CDN services, response teams and law enforcement authorities
- Establish communication mechanisms. For data communications make sure that non-saturated lines will be used
- Update the Recovery and Continuity Plan on new DDoS developments. Define a clear response escalation path
- Ensure that the capacity of the entire infrastructure is not restricted by a single or limited number of resources
- Dedicate Hardware and Software for DDoS mitigation (workstations, servers, network monitoring and analysis tools)

- Establish alternative service and Internet gateways

ISP and specialized support:

- Update on ISP's mitigation services
- Establish DDoS protection contracts and SLAs. Secure immediate activation of agreed services
- Obtain a clear overview on infrastructure's performance in order to identify deviations derived from an attack
- Establish specialized support from DDoS mitigation experts

Network & infrastructure setups:

- Create ACLs for traffic prioritization
- Set up alternative communication on critical services using VPN
- Use Reverse path forwarding (RPF)
- Apply inbound and outbound traffic filtering
- Introduce weak authentication phase prior to the actual on authentication protocols
- Apply limits for
    - ICMP packet rate
    - SYN packet rate
    - DNS TTL for the exposed systems
- Secure network, operating systems, servers, applications and components

2. Identification

Detection and alerting:

- Search for traffic patterns to expose known attacks (signature detection)
- Compare parameters of the observed network traffic with normal traffic (anomaly detection)
- Contact CERT-EU for early warnings and indicator notices

Attack analysis:

- Identify the abused systems and services
- Understand if you are the target of the attack or a collateral victim
- Get a list of attacking IPs by tracing them onto the log files
- Define the attack's profile by using network monitoring and traffic analysis tools

Motivation identification:

- Make a list of potential DDoS attack initiators
- Investigate possible motives

Mitigation acquirement /refinement:

- Contact ISP to report the attack
- Ask for assessment and visibility into the attack
- Enable remediation measures
- Notify executives and law enforcement services

Traceback

- If possible identify the inbound points (by ACLs, NetFlow or backscatter mechanisms)

3. Containment

Network modifications:

- Switch to alternative sites or networks using DNS or other mechanism

- Distribute attack traffic across network of data centers
- Route traffic on scrubbing services and products

Content delivery control:

- Use Caching/Proxing
- Enable alternative communication channels (VPN)

Traffic control:

- Terminate unwanted connections or processes on servers and routers
- Configure outbound filters for reducing DDoS response footprint
- Control content delivery based on user and session details

4. Remediation

Bandwidth prioritization and blocking:

- Deny connections using geographic information
- Deny connections based on IP and traffic signatures
- Place limits on the amount of traffic, maximum burst size, traffic priority on individual packet types

Traffic scrubbing:

- Use dedicated devices and modules with high-performing hardware that can support focused scrubbing algorithms

Sinkholing:

- Attract DDoS traffic on the IP blocks advertised by the sinkhole to apply specialized analysis

5. Recovery

Normal state verification:

- Verify that traffic is nominal with no sharp increases. Let a period of time since last violation before the traffic flow is considered normal
- Ensure that the impacted services can be operational again
- Ensure that your infrastructure performance is back to your baseline
- Ensure that there are no collateral damages

Rollback:

- Initiate suspended services, applications and modules
- Rollback the mitigation measures
- Announce the end of the incident
- Revert to your original network

6. Aftermath

Incident review and information Disclosure:

- Evaluate the effectiveness of response
- Review the measures that could be taken to better address the incident response

- Review and refine attack-handling tools and procedures taken during the incident
- Create an incident review
- Measure the operational impact and costs

Law enforcement:

- Ensure the attack evidences are valid for forensic analysis
- Collaborate with law enforcement services