CENTRE FOR CYBERSECURITY BELGIUM

DDOS: PREVENTION AND PROTECTION

TECHNICAL GUIDELINE 2024

Belnet

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Date: February 2024
Version: 2.1 English
Author: The Centre for Cybersecurity Belgium (CCB) with the valuable input of Belnet

The Centre for Cybersecurity Belgium (CCB) is the national authority for cybersecurity in Belgium. The CCB was established by Royal Decree of 10 October 2014 and operates under the authority of the Prime Minister.

Based on its legal mission, the CCB tries to inform and advise organisations on protection against DDoS attacks. This document serves as a technical guideline, help and advice in light of the Belgian elections 2024 to prevent and protect against DDoS attacks.

EXECUTIVE SUMMARY

This guideline on DDoS mitigations measures has been drafted in the context of the Belgian elections in 2024. At a federal level, different stakeholders have an important role in the elections process. Effective protection against DDoS attacks requires a coordinated approach between the various stakeholders.

The document starts with explaining what a DDoS attack is, the different types of DDoS attacks, the impact and the reasons behind a DDoS attack. Chapter two provides proactive measures to be prepared for an DDoS attack and outlines mitigation solutions. Chapter three describes how to react when your organisation is the victim of a DDoS attack and describes technical mitigation measures. The final chapter consists of a checklist whereby the first part holds a proactive checklist. The second part highlights the incident response steps as described in chapter three.

The guideline is advisory in nature and helps to be prepared and having response capabilities when a DDoS attack happens.

This document was created with the valuable input of Belnet.

Table of content

Glossary

ASN	Autonomous system number
Botnet	A collection of connected devices, often within an IoT network, that becomes infected and controlled by malware to benefit cybercriminals.
CCB	Centre for Cybersecurity Belgium
CDN	Content delivery network
CSIRT	Cyber security incident response team
C2 server	Command and Control server
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
Drupal	Content management software
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ISP	Internet Service Provider
NSM	Network Security Monitoring
OSI-model	The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.
SIP	Session Initiation Protocol
SIEM	Security Information and Event Management system
SMTP	Simple Mail Transfer Protocol
SYN flood	A type of denial-of-service (DDoS) attack which aims to make a server unavailable to legitimate traffic by consuming all available server resources.
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
WAF	Web Application Firewall

1. Introduction

1.1. GENERAL

A Denial of Service, or DoS, is a cyber-attack that aims to disrupt the availability of a particular service. A DoS attack uses one computer and one Internet connection. When the attack is distributed and uses multiple computers and their Internet connections we call it a DDoS, Distributed Denial of Service. It is important to stress that although distributed in nature the computers taking part in a DDoS share a common goal and the attack is coordinated. It can have a major impact on the operations of organisations and businesses.

There are different types of DDoS attacks, that are discussed in depth in 1.4. Types of DDoS attacks.

1.2. REASONS FOR DDOS ATTACKS

A DDoS attack with malicious intent can occur for multiple reasons: blackmailing, ideologic or hate related attacks, competition, politics, electronic protest, smokescreen, probing, experiment, hacktivism, prestige/challenge or extortion. For example, hacktivists have targeted election-related websites with mainly DDoS attacks, which involve sending massive amounts of traffic to servers in an attempt to block internet users from accessing websites. These attacks are often politically motivated and aim to disrupt the democratic process, cause chaos, or protest political decisions.

The current principal hacktivism threat when it comes to DDoS attacks is the DDoSia project launched in early 2022. This DDoS project is related to a nationalist Russian hacktivist group and launches a lot of attacks against Ukrainian and NATO related countries and services.

1.3. SOURCE OF DDOS ATTACKS

The majority of DDoS attacks are done via a botnet.

These botnets are mostly “hired” for a couple of hours to conduct the attack, similar to “DDoS as a service”. The owners of the botnets are typically not the people conducting the attack. A botnet consists of a large number of computers infected with some form of malware. The malware has an agent component that performs the actual attack. Note that most malware has different features where DDoS capabilities is often only one of them. The agent that runs on the infected machine gets his commands from a C2 server (Command and Control server). This C2 controls the different agents and tells them what to do. Owners of infected machines are usually unaware that their machines are infected and are contributing to a DDoS attack. It is important to emphasise that almost everyone can launch a DDoS attack.

There are plenty of tools and resources (botnets) available. Anyone with a limited skillset but with enough determination (or money - although botnets are not that expensive) can conduct a DDoS attack.

1.4. TYPES OF DDOS ATTACKS

Generally, the most common forms of DDoS attacks can be categorised in three categories:

1. **Volumetric**: the volume-based DDoS attack method is designed to disrupt normal traffic or requests by overwhelming the network layer of a target service with a flood of fraudulent traffic from numerous sources. This results in a degraded or completely unavailable service, even for legitimate users. This is often referred to as a layer 3 attack. Examples include reflective/amplification attacks (UDP flood) and ICMP (Internet Control Message Protocol) flood.

2. **Protocol**: the protocol-based DDoS attack relies on weaknesses within internet communication protocols. Protocols such as TCP (Transmission Control Protocol) and ICMP can be used to launch protocol-based DDoS attacks. Typical protocol level DDoS will initiate a lot of connection without fully starting them (e.g.: SYN flood) to exhaust the number of connections that the server can handle. Since the principal vector for this type of attack is SYN Flood (TCP), this attack is often referred to as a layer 4 DDoS attack.

3. **Application attack**: the application-based attack is also known as Layer 7 DDoS attack. This method targets the application layer of the network stack - which is the layer responsible for processing specific protocols, such as HTTP, SMTP (Simple Mail Transfer Protocol), or DNS. Application layer attacks

generally require the most knowledge of victim infrastructure, and if executed correctly requires the least amount of resources from an attacker. Typical application level DDoS attacks will post random data on a website search form to produce load on the database or request random non-existing subdomains to the DNS server. An example of an application attack is a HTTP slow post attack, where an attacker deliberately sends announced data very slowly, to keep connections open and eventually exhaust the server's resources.

2. Proactive measures

This chapter lists a number of proactive measures, both technical and non-technical, that can be taken to limit the impact of a possible DDoS attack.

2.1. KNOW YOUR NETWORK

It is important to have knowledge about your network. Know what public services and networks you have. Make sure you do not forget your off-site (for example: cloud) services. If your internet connection is down, you will not be able to access these services.

It is recommended to have a complete inventory, including network typologies, external and internal IP addresses. This documentation is essential during an attack. Make sure you also have offline access to the documentation during a cyberattack.

Running a regular network scanner off-network to inventory your publicly available devices and services helps mapping what you expose to the internet. Make sure that you have a list available of service owners and a list of people responsible (both technical and non-technical) for all your exposed assets.

2.2. KNOW YOUR APPLICATIONS

It is important to have knowledge about your applications and prepare mitigations accordingly. DDoS attacks tend to exploit specific parts of the applications to increase the load on multiple systems. Being aware of those weak points can help you prepare dedicated mitigations.

On a website, some pages can induce a high load on the database (for example: a search form), those pages may be targeted to overload the database of the website. Those pages are also often the ones that can't be effectively placed behind a cache. Keeping an inventory of them and prepare a procedure to disable those pages if they are targeted can help to mitigate the DDoS attack. A static copy of the site could also be prepared as a temporary replacement during the attack.

2.3. INCIDENT RESPONSE PROCEDURE

Draft an incident response plan and keep this plan up to date. When facing a DDoS attack, it is important to react in a prompt and efficient manner.

An incident response procedure describes what should be done in the event of a cyber-attack. Define a number of standard operating procedures in case of a DDoS attack:

- Identify the assets of your organisation
- Implement a Business Continuity Plan/Disaster Recovery Plan
- Assign business priorities for recovery
- Document how your systems work and keep this documentation up to date
- Assign responsibilities and role to people with the right skills
- Prepare an out-of-band communication channel
- Make a contact list
- Call up on experts about cyber incident response
- Prepare a communication strategy – for more information: https://atwork.safeonweb.be/recent-news-tips-and-warning/crisis-communication-event-cyber-attack

For DDoS attacks specifically, it is crucial to pay special attention to the following points:

- Consult your Internet Service Provider (ISP) beforehand: discuss what your ISP has in place for preventing DDoS attacks and what the ISP can do in case of a DDoS attack. This could be, for example: geo-blocking, changing public IP, packet scrubbing, etc.

- Prepare Service Level Agreements (SLA's) with your ISP in case a DDoS occurs and prepare SLA's for DDoS attacks on every level of the network.

- Check and review existing contracts with your ISP, Cloud and Hosting provider for DDoS protection.

- Close monitoring of key infrastructure is needed to spot increased resource use/exhaustion quickly to enable a prompt response. Define responsibilities and roles regarding this monitoring.
- Ensure that a clear baseline exists for network traffic, to spot abnormal/attack traffic more easily.
- Investigate the possibility of scaling up your infrastructure in case of an attack. Especially for the instances running in the cloud (for example: Azure).
- Perform regular stress testing to ensure the infrastructure and mitigations perform as expected.
- Prepare an out-of-band communication channel: a secure communication platform needs to operate on a separate network not subject to those attacks. Some examples are: Phone (unsecure), Signal, Threema, etc.… Also clearly decide in advance which group of people will communicate with which means.
- Make an offline contact list: it is important to have an offline (printed) contact list of persons who can help you or who you need to inform. This can be either internal (management, employees, IT-service) or external (ISP, security expert, customers).
- Besides technical expertise, availability for staff able to make executive decisions is also required. Both of these roles should be documented in a Business Continuity Plan/Disaster Recovery Plan.
- Maintain a permanent threat list for known botnets and malicious IP's, and block these permanently or at least be able to quickly enable it when needed.
- Spread the different services on your IP space to minimize potential side effects and to ease mitigation. Do not aggregate different services that are independent of each other behind a same IP.
- Never use same public IP for services/applications and internet access of the people within your organisation.

3. Steps to perform incident response for a DDoS attack

Chapter three describes how to react when your organisation is the victim of a DDoS attack. The mitigations steps outlined below are the minimum ones that an organisation will need to follow in case of a DDoS attack. Be aware that there is no one-size-fits-all solution.

It is important to highlight to a victim of a DDoS attack that this process requires technical expertise as well as access to technical resources on their end.

3.1. DETERMINE AND CONFIRM THE EXTENT OF THE ATTACK

Before jumping to conclusions and thinking that a DDoS attack is going on, it is necessary to assess the resource unavailability (for example: only unavailable for a limited number of people or for everyone).

Gather as much information as possible about the attack. To determine the impact of the DDoS, it is important to make an inventory of the affected systems. This can be done based on complaints from users for example.

3.2. VISIBILITY INTO THE ATTACK

Once the impact of the attack has been documented and understood it is important to investigate what is causing this unavailability. A good understanding of how the attack works is key in implementing effective countermeasures.

- If available, a Security Information and Event Management system (SIEM) or Network Security Monitoring (NSM) can be tremendously helpful to look into what's going on.
- If no monitoring/logging solution is available, look at the logs from network equipment/applications directly.
- Provided you have a baseline of your network traffic, use this knowledge to determine what kind of attack patterns are used by the adversary. Examples include a significant raise in requests to a webserver or (increased) queries for non-existing domains (DNS).
- Discuss with your ISP what can be done to improve the situation and have proactive monitoring.

3.3. ASK FOR HELP FROM YOUR ISP OR IMPLEMENT A THIRD PARTY ANTI-DDOS SOLUTION

- Contact your ISP or your third-party anti-DDoS solution provider as soon as possible and provide them as much information as possible about the attack you are experiencing. Information should at least include targeted Ips, type of DDoS (see 1.4. Types of DDOS attacks) and potential attack vectors, etc.
- The impact and the effects of the attack can also be given to help your ISP understand what you are facing and what can be done about it.
- If you are able to provide them the baseline of legitimate traffic, it will help them to have an idea of the volume of traffic they should block.
- Ask to open a communication channel to ease the communication during the attack. Attacks vectors are often changing during the attack to go around the mitigations put in place. It will also allow you to give feedback of the measures taken. The ISP will be able to react more quickly to measures too aggressive that block legitimate traffic or too soft that allow too many packets from the attack.
- Despite ISP probably won't be able to mitigate a L7 attacks if they are not hosting or managing your applications, consider involving them as they could be able to mitigate some vectors being used at the same time.
- Keep in mind that however ISP should have some form of DDoS protection (in-house or via a third party) that will be able to mitigate a lot of the Layer 3 and 4 volumetric attacks, mitigation is never 100 percent.
- As last resort only and if one specific IP (not a perimeter device) is the target, and the protection isn't enough. Consider asking your provider to temporarily "blackhole" this IP. This of course does mean the resource won't be available, thus making the attack partially successful, but at least the collaterals are mitigated, and the organisation remains operational to a certain extent.

3.4. STEPS A VICTIM CAN TAKE

The below steps assume external connectivity is still available. If the gateway or external firewall is completely exhausted due to the attack, contact the ISP.

If you have monitoring/logs available, investigate them. If you don't have them freely available, you could do a PCAP on the external side of the firewall to analyze or gather logs directly from applications/devices.

3.4.1. UNDERSTANDING THE ATTACK

- Determine the target of the attack.
- What type of resources are being targeted by the attacker?
- Determine the type of DDOS attack (on which layer of the OSI layer, layer 3-4 or up to 7).
- Perform statistical analysis of the source of the attack: are there any source or countries that stand out? Are there any ASN's that stand out? Visualizations/dashboards typically available in a NSM are very helpful for this.

3.4.2. GENERAL DDOS MITIGATIONS

It is generally a good idea to do some quick filtering of the attack traffic, to give your network some breathing room. At this time, it is probably acceptable to be very restrictive on the blocking. Health of your network and applications, as well as availability to your core constituency is your primary concern here. This allows you to buy yourself some time to dig deeper and come up with the more elegant / tailored mitigations specifically for the attack vector used.

- Temporary blocking of attacking IPs: create a (preferably separate) blacklist that specifies which IP addresses should be (temporarily) denied access. If the IP address that sent the request is on the blacklist, the system intercepts the connection and denies access. This denial can take different forms, such as displaying an error message, redirecting the user to another page, or dropping the connection without any response.

- Temporary geoblocking/geofencing of specific IP-ranges: block access from an entire geographical region.

- ASN blocking: if the malicious traffic is coming from distinct ASN's, block this ASN, or network blocks thereof.

- Load-balancing and upscaling: load-balancing techniques distribute incoming traffic across multiple servers or data centers. By spreading the traffic load, it can prevent a single server or resource from being overwhelmed by a DDoS attack. Having the ability to temporarily increase the capacity of a service during an attack can limit the impact.

- Isolate: if the attacked service is on a server that also provides other services, move the attacked service to a dedicated machine to reduce the collateral impact from the attack to a minimum.

- Strip down: strip down a service to its bare minimum.

- Remotely triggered black hole: divert all traffic to a specific target IP to a "null interface", dropping the malicious traffic before it reaches its destination.

- Stop targeted services and/or applications: this measure does not block attacks; however it can protect the application/service from malfunctioning. Be aware that this can generate a substantial loss of data and services.

3.4.3. SPECIFIC MITIGATIONS MEASURES BY ATTACK VECTOR

In case of DDoS attack: look for protocol (Layer3/Layer4) or application (Layer 7) specific patterns such as:

Overview Layer 3 and Layer 4

Protocol	Attack vector	Mitigation measures
UDP	Reflective/Amplification	• Can be blocked if this traffic is not used/expected on the target system. • Have to rely on volumetric/ DDoS scrubbing technologies otherwise.
TCP	SYN Flood	• Implement syn cookie. • Tuning timeout settings. • Recycling oldest half-open TCP.

Overview Layer 7

Application	Attack vector	Mitigation measures
DNS	NX Flood (Legitimate) request flood	• Protect DNS server cache from being polluted with NX answers. • Drop DNS queries based on whitelist of (sub-)domains. • Rate limiting by source IP.
HTTP/HTTPS	Low/slow Targeted URL flood	• Tune timeout settings more aggressively. • More aggressive rate limiting for most targeted URLs. • If widespread impact on the web server: consider dropping all requests to most targeted URLs (effectively rendering them unavailable). • If available: look at referrer URL.

3.4.4. OTHER MITIGATIONS MEASURES TO CONSIDER

- Implement an anti-DDOS appliance that can mitigate DDoS attacks. Note that this is an expensive solution. However, if DDoS attacks on your environment are frequent, this cost could be justifiable.
- For web applications: replace dynamic content with static content. Disabling the dynamic content like search forms, using low-res images and compress and minify the CSS and JavaScript files can reduce the traffic load.

- Improve resiliency by (permanently) implementing a Content Delivery Network (CDN) solution.
- Consider further segmentation in your network. Avoid sharing infrastructure where possible.
- DNS records: setting a higher Time To Live (TTL) for DNS records. A TTL of one day (24h) could limit impact on other services if DNS servers go down. One should keep in mind though, that a longer TTL also has implications when applying changes.
- For web applications such as websites: implement a Web Application Firewall (WAF) and Advanced Global CDN. The WAF monitors and blocks malicious traffic to your website/server based on a set of rules. It detects/blocks known malicious IP addresses, suspicious user agents and other activity which is out of the ordinary such as repeated brute-force attack attempts on your website. The AG CDN adds further protection against DDoS attacks on your website by preventing any surge in requests from hitting your main (origin) server which may otherwise result in your website becoming unavailable. Many CDN providers will handle the WAF on their end, as part of a paid service.
- When using cloud resources that are accessible from public internet, consider activating the DDoS protection mechanisms of the cloud provider.

3.5. EVIDENCE GATHERING

Regardless of whether you report the incident in the post-incident phase to your ISP, to the national CSIRT, to the legal authorities or to any other partner you will have to produce some form of evidence. You can provide evidence on a NetFlow level, network level and application level. Ideally you can produce all of these.

3.6. RECOVERY

The DDoS attack is finished when your network traffic returns to the earlier set baseline.

Note that sometimes DDoS attacks come in waves. Attackers can launch multiple waves. This can make you believe that the attack has stopped, hoping you let your guard down and then re-launch a new, more powerful, attack. Methodology of attack can also change between the waves to probe which technique is the most impactful. Once the DDoS attack is stopped, the disabled services can be restarted.

Afterwards, verify that everything works normally. If everything works properly, communicate this to users.

3.7. EVALUATION

Once the attack has been dealt with, a lesson learned meeting should be organized with all stakeholders involved. Evaluate what went well and what went not so well. Perform regular stress testing to ensure the infrastructure and mitigations perform as expected.

Evaluate the working points and convert these into concrete action points in the preparation phase and adapt the incident procedure for the future.

This includes but is not limited to:

- Consider changing back-end server IPs that are known by attackers.
- Correctly scale your internet connection bandwidth, typical day-to-day activities should only consume about 50 percent of your total bandwidth.
- Review your architecture based on weak points observed during the DDoS attack.

4. Checklist

The below checklist is divided into two parts. The first part consists of a proactive checklist. The second part highlights the incident response steps as described in chapter three.

4.1. PROACTIVE CHECKLIST

☐ Know which networks, hosts, and services that you expose, update your inventory regularly, be aware of possible bottlenecks:

- Evaluate the risk and importance of exposed business assets.
- Have a written down and approved list of service owners.
- Have up-to-date network and services diagrams.
- Have out-of-band communication channels.
- Have offline or hardcopies of contact persons.

☐ Make sure your ISP and national CSIRT know your organisation and your contact points and vice versa.

☐ Know exactly what your ISP can do and what your ISP can not do during a DDoS attack.

☐ Prepare SLA's with your ISP in case of DDoS attacks.

☐ Review your firewall rules on a regular basis.

☐ Ensure automatic security updates of operating systems, programs, and routers.

☐ Use services in the cloud where possible, for example websites, mail services or other online platforms are very vulnerable if you host locally on a server. Cloud services are less likely to be impacted by DDoS due to their wide availability.

☐ Prepare a crisis communication plan

4.2. INCIDENT RESPONSE STEPS

☐ Have internal incident response capabilities.

☐ Use a properly configured load balancer and make use of up-scaling.

☐ Implement a reverse proxy.

☐ Implement a WAF and Advanced Global CDN.

☐ Review and harden your network devices and follow good practices.

☐ Prepare a stripped version of your services to be deployed when under attack.

☐ For web applications: replace dynamic generated contact with static content.

☐ Improve resiliency by implementing a Content Delivery Network (CDN) solution.

☐ Think of splitting out the internal and public DNS infrastructure.

☐ DNS records: setting a higher Time To Live (TTL) for DNS records. A TTL of one day (24h) could limit impact on other services if DNS servers go down in a future attack.

☐ For web applications (for example Drupal): implement a Web Application Firewall (WAF) and Advanced Global CDN.

☐ Consider to activate/ask DDoS protection of your (cloud) providers.

☐ Temporary block malicious IP's.

☐ Temporary geoblocking/geofencing of specific IP-ranges.

☐ ASN blocking: if the malicious traffic is coming from distinct ASN's, block this ASN, or network blocks thereof.

☐ Load-balancing and upscaling: load-balancing techniques distribute incoming traffic across multiple servers or data centers. By spreading the traffic load, it can prevent a single server or resource from being overwhelmed by a DDoS attack.

☐ Packet scrubbing: the traffic destined for a particular IP address range is redirected to datacenters, where the attack traffic is "scrubbed" or cleaned. Only clean traffic is then forwarded to the target destination.

☐ Stop targeted services and/or applications.

☐ Remotely triggered black hole.