CERT.be

DDoS

Proactive and Reactive measures

TLP: White

Author: **Koen Van Impe**

The
Federal Cyber
Emergency Team

Content

Document version: **15 October 2015**

1 INTRODUCTION

SCOPE OF THIS DOCUMENT

1.1 Scope

This document is a summary of the different open source information concerning DDoS attacks.

This document serves as guideline, help and advice for the Belgian public and private sector to deal with DDoS attacks. The document will not stop a DDoS attack but it will help you being prepared and having response capabilities when an attack happens.

It starts with explaining the different types of DDoS attacks, their impact and their motivation. It will then continue by providing proactive measures to be prepared for an attack and mitigation and reactive measures for surviving and countering an attack.

The proactive and reactive chapters are both preceded by a **summary** chapter.

The summary chapter gives a short overview of recommendations, action points and external references. The chapter following the summary part then contains a more detailed description. If you are in need of quick, **summarized** guidelines then extract the two summary sections.

Note that the references towards Belnet as ISP are only valid if you are *connected via the Belnet network*. If you are **not** connected via the Belnet network then you have to contact your own ISP for the parts of "getting help from your ISP". Similarly, if your organisation is based outside Belgium then contact your own national CSIRT and not CERT.be.

1.2 Actors

1.2.1 CERT.be

CERT.be is the federal cyber emergency team for Belgium.

It is **operated** by Belnet, the Belgian Research and Education Network.

Contact: **Koen Van Impe** <koen.vanimpe @cert.be>
Security Analyst

Thomas Eugene <thomas.eugene @cert.be>
Security Analyst

CERT.be Incident mailbox <cert @cert.be>
+32 2 790 33 85
https://www.cert.be

1.2.2 Belnet

The Belgian Research and Education Network

Contact: Belnet Servicedesk <servicedesk @belnet.be>
+32 790 33 00

1.3 Credits

This document is based on a presentation on DDoS attacks done by CERT.be security analyst Thomas Eugene for the Belnis working group on 8-September 2015.

A big thank you to the valuable input by the CSIRT community in Europe, especially Andrew Cormack.

1.4 Document classification

This document is marked as TLP:WHITE[1] which means it may be distributed without restriction, subject to copyright control.

1.5 Feedback

This is a document in progress. We'd like to receive your feedback or suggestions. Feel free to propose us use-cases to cover in the examples section.

Please send your feedback to **cert@cert.be**

[1] https://www.cert.be/traffic-light-protocol-tlp

2 WHAT IS A DDOS?

DISTRIBUTED DENIAL OF SERVICE

2.1 DoS and DDoS

A **Denial of Service** (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, by temporarily or indefinitely interrupting or suspending services of a host connected to the Internet[2].

It prevents or impairs the authorized use of a system.

The network bandwidth and availability of resources is currently so large for most organizations that a single attacking machine can usually not cause a DoS.

This is the reason why attacks are happening in a coordinated way. The attack is **distributed** across multiple attacking computers, hence **Distributed Denial of Service (DDoS)**. 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.

Typically a DoS attack uses one computer and one Internet connection.

A DDoS uses multiple computers and the Internet connection of each of these computers.

2.2 Reasons for a DDoS

Why do you become the victim of a DDoS?

This can happen for multiple reasons:

- **Blackmail**: someone wants you to pay an amount of money, this is not so much different from the "real-life" racketeering. Blackmail can happen because of extortion but also maybe someone "knows" something (sensitive) about your network that you prefer not to become public;
- **Ideological or hate attacks**: your message or your values don't correspond with the values adhered to by the attackers or someone has an ethical objection to your message. Basically attackers desire to silence you;
- **Competition**: your business is in competition with, or in the way of, the business of the attacker;
- **Politics**: because an individual or group of individuals wants to gets revenge on a state (institute, organisation) or because of political different opinions. These types of attacks can also be nation-state-driven;

[2] https://en.m.wikipedia.org/wiki/Distributed_denial-of-service_attack#Distributed_attack

- **Electronic protest**: someone doesn't agree with a recent decision taken by your organization;

- **Smokescreen**: hide another, often more complex, attack like data-exfiltration, lateral movements or account compromises;

- **Probing**: an attack to test your incident response capabilities. This attack serves as a test to see what your procedures are in case of an incident;

- **Experiment**: someone just learned the "art" of DDoS and wants to test their skills into a real-life example;

- **Prestige or challenge**: someone is bored and wants to show how "skilled" they are. Sometimes group of attackers challenges eachother to point their attention to a specific target;

It is important to realize that almost anyone can launch a DDoS. There are plenty of tools and resources (botnets) available for everyone with a limited skillset but with enough determination (or money - although botnets are not that expensive) to conduct a DDoS attack.

One of the reasons for being a DDoS victim that is often forgotten is that of the **unintentional** DDoS. For example this can be caused by

- A **bug** in the front-end or back-end software, possibly causing endless loops;

- Someone in your organization launched a new campaign or product and your infrastructure isn't properly **scaled** to handle the new load. Similarly, your organization suddenly gets a lot of media-coverage and you experience a big spike of web visits (the Slashdot effect[3]);

- You host a resource (movie, image, document) that is very large, not specifically scaled for the Internet and that suddenly gets accessed a lot of times.

- You can be the victim because of mistaken identity or because of an association (mistaken or not) with the real target.

2.3 Types of DDoS

Basically there are three common categories of DDoS attacks.

1) **Volumetric attacks**;

2) **Traffic attacks**;

3) **Application attack**.

2.3.1 Volumetric attacks

Volumetric attacks happen by overwhelming the available network bandwidth with UDP or ICMP floods, with spoofed-packet floods or through other means.

[3] https://en.wikipedia.org/wiki/Slashdot_effect

The resource of the victim is no longer accessible for proper use. One of the most commonly known volumetric attack type is an **amplification** attack (see 2.3.1.1).

2.3.1.1 Special type of attack : Amplification attacks

An amplification attack is a **volume** based reflection denial of service. The attacker sends a packet to a vulnerable service with a spoofed (fake) source address. This vulnerable service is not the prime target of the attack, but it will reply with a much larger reply towards the spoofed address, which is the real target of the attack.

Note that although maybe not the prime target of the attack, the amplifier –vulnerable service- can also experience a DoS because of the attack.

Amplification attacks can happen because there are still a high number of misconfigured services and servers and not all network administrators implement proper ingress filtering.

The most favoured protocol in use for amplification attacks is DNS (also see the advisory from CERT.be[4] on dealing with DNS amplification attacks) but other protocols (like for example NTP) also provide amplification features.

Amplification attacks almost always use UDP because, by design, UDP is a connection-less protocol. It does not validate the source IP address which makes it fairly easy for attackers to forge this.

2.3.2 Traffic attacks

DDoS Traffic attacks consist of abusing the system resources of a victim.

This type of attack consumes actual server resources, or resources of intermediate communication equipment (firewalls, proxies, load balancers, …).

This attack type can be done in various ways via protocol abuse (for example with a SYN flood), sending a malformed packet (for example Ping of Death) or by sending only parts of packets (fragmented attack, disturbing the capability of the victim to re-assemble the traffic stream).

2.3.3 Application based attacks

This type of attacks focus on the underlying application.

Most often they consist of seemingly legitimate and harmless requests. Their eventual goal is to bring down the service or make the service unusable by exhausting the available resources.

2.4 Timeline of a DDoS

Most DDoS attacks share a fairly similar timeline :

1) Something happens that makes people want to attack you (this can be anything, either under your control or out of your control, also see 2.2) ;

2) Your attacker starts building capacity. This can be in bulk (mostly bandwidth oriented) or towards a specific resource (mostly application oriented);

[4] https://www.cert.be/docs/dns-amplification-attacks-and-open-dns-resolvers

3) The attacker launches the DDoS;

4) The attacker sells you silence or the attacker moves on. You can pay by complying with their demands or with money.

2.5 Capacity building of a DDoS

The majority of the DDoS attacks are done via a botnet, where mostly these botnets are "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 (see 4.6.10).

The malware has an **agent** component that performs the actual attack. Note that most malware has different features where DoS capabilities is often only one of them. The agent that runs on the infected machine gets his commands from a **handler**. This is the module that controls the different agents and tells them what to do.

Owners of infected machines are usually unaware that their machines are infected and contributing to a DDoS attack.

2.6 DD4BC

DD4BC ('DDoS for Bitcoins') is a group of attackers that conduct extortion campaigns threatening with DDoS attacks where you are required to pay in Bitcoins for not being attacked. Their main objective is to gain Bitcoins. DD4BC uses different attack vectors but primarily UDP amplification attacks that comprise Chargen, NTP and SSDP.

Typically your organization will first receive an e-mail explaining that a low-volume DDoS is taking place, to show that the threat is real. The attackers will provide some details which will allow you to examine your server logs and validate their claim. Following this e-mail the group will demand a ransom to be paid in Bitcoins. If the ransom is not paid the group will conduct a larger (volume) attack.

Note that these e-mails do not always end up with people that are in the position to assess the real scope of the content. It's possible that the extortion demands are sent to generic mailboxes (info@, support@) or that they have been filtered by your spam filter.

The group is aware when victims change their IP addresses to defend themselves.

Next to threatening with DDoS attacks the DD4BC also threatens to publicly embarrass[5] a victim by exposing targeted organizations via social media.

Because extortion is a crime you should file a report with the legal authorities if you face a threat by DD4BC or a similar group. As some organizations have paid the ransom there are copycat hackers that consider this as an easy way to get some quick (Bitcoin) cash.

[5] https://www.stateoftheinternet.com/trends-blogs-september-2015-09-state-of-the-internet-case-study-operation-DD4BC.html

2.7 LOIC

LOIC ("Low Orbit Ion Cannon") is an open source application to be used by a lot of users to launch a DDoS attack against a website.

LOIC is often more associated with hacktivism.

It's a straightforward application with a fairly simple interface. To make it even easier, users that opted to download LOIC can connect the application to a central control (IRC channel) where it gets its instructions automatically.

3 PROACTIVE MEASURES: SHORT SUMMARY

SUMMARY ON PROACTIVE MEASURES

Know your assets

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

Evaluate the risk and importance of your exposed business assets;

- **Prioritize** your business assets;
- Consider a **risk based** approach;
- List sensitive content;
- List critical services;

Have a written down and approved list of **service owners**;

Have up-to-date network and services **diagrams**

Consider filing a complaint with law enforcement if you are the victim of extortion

- Watch out for extortion mails from DD4BC

Contact procedure and details for incident response

Have **internal incident response** capabilities

- Have an **incident response plan;**
- Have an **incident management plan**;
- Define **incident response roles** within your organization;
- Include your management, **communication** and **legal** team in incident response procedures;
- Appoint a **security incident coordinator**;
- Test, review and update your incident response and incident management plans;

Have **out-of-band** communication channels (for example a DSL or 3G connection)

- Setup an emergency telephone, out-of-band e-mail and war-room, make sure people involved in your organization are aware of it

Have **offline** or hardcopies of **contact details** (telephone, e-mail) of your ISP, CERT.be, SOC and most relevant security vendors;

Have hard printed contact details for key departments in your organization

Have an established and tested procedure for reporting a DDoS to your ISP and to your national CERT and know how you can request help;

Make sure your ISP and national CERT know YOU ('vouched'/'valid' contact persons that can report an incident)

Agree on the format for sharing data, have **encrypted** communication channels well established

Know exactly what **your ISP can do and what your ISP can not do** during a DDoS attack (rate-limiting, simple packet filtering to full packet scrubbing)

Setup a meeting with your ISP
be aware that some ISPs can charge for additional services

- Incident reporting CERT.be:
  - cert@cert.be
    - Send an e-mail for testing, whitelist cert@cert.be in your spam filter
  - +32 2 7903385
- Exchange public PGP fingerprints for encrypted messages
- CERT.be keyid: 0x53977C01
- Fedman customers
  Belnet
    - servicedesk@belnet.be
    - +32 2 7903300

Firewalls, IDS, Network filtering, System and Services configuration

Firewalls and IDS provide little extra protection against **volumetric** attacks; some IDS provide limited protection against **anomaly** based application attacks

Block all traffic that is not explicitly permitted (incoming and outgoing)

Filter **RFC1918** (private internets)
Use automated blacklists on applications
Use reverse path verification
Implement BCP-38 / RFC-2827 for proper ingress filtering
Use **bogon prefix filtering** on your edge network

If your ISP provides this service, use **network traffic scrubbing** or traffic shaping

Use a SYN cookie

Rate limit SYN packets

Apply basic resource protection

Use application firewalls but be aware that firewalls provide limited protection
Do not make your services directly accessible (reverse proxy for web apps)

Run regular network, service **scans** (or vulnerability scans);

Prevent open or misconfigured services

Disable open e-mail relays
Disable open recursive DNS servers
Rate limit your authoritative DNS servers
Disable open NTP servers
Disable or filter popular UDP amplification services

Use a properly configured load balancer, reverse proxy and application firewall;

Make sure your load balancer does not become single point of failure

Resize your media material to 'web'-friendly sizes

Host non sensitive media material on **CDNs**
Minify and compress javascript and CSS

Offload some of the dynamic content to static instances

Review the application logic, replace dynamic generated content with static content
Prepare your services to be moved to other networks (DNS changes - **TTL**)

Create single purpose servers

Prevent malware on your network

Patch, firewall, malware protection, host intrusion detection, monitor

Raise user awareness

Users will click, teach them to report to you when they did

- Implement bogon prefix filtering via BGP via Team Cymru
  http://www.team-cymru.org/bogon-reference-bgp.html
- Use **captchas** or challenge response on web forms
- For Apache use mod_reqtimeout and **mod_security**
- Scan for open e-mailrelays with nmap
  nmap --script smtp-open-relay.nse -p 25, 465, 587 -Pn -n my.scan.host
- Scan for open recursive DNS servers with nmap
  nmap --script dns-recursion.nse -p 53 -sU -sV -Pn -n my.scan.host
- Apply the DNS-RRL patch to authoritative DNS servers or use a version that supports it by default
- Lower the TTL for the A-records of critical services
- Use **NMAP** from an IP outside your network (for example a VM at a cloud provider) to regularly scan your public networks for open ports and available systems.
- Use **OpenVAS**, **Nessus** or **Qualys** to scan your assets for vulnerabilities.
- Scan for open NTP servers
  nmap --script ntp-monlist.nse -p 123 -sU -Pn -n my.scan.host
- Consult the matrix from US-CERT on TA14-017A and limit the services with the **highest bandwidth amplification** factor, pay special attention to Chargen, NTP, SSDP, RIPv1 and DNS.
- Setup an internal "I clicked on a link" mailbox where users can report events

Network and system monitoring

Set a **network baseline**

Use netflow

Use nfsen for graphical views on the network volume

Full system and service **logging**

Centralized logging
Make sure not everyone can read the logs
Make the tamper proof, account every access to the logs
Backup the logs
Make sure all system and services are **time-synced**
Analyze / correlate the logs with a SIEM
have access to **raw** log files, not only the aggregated set
Setup retention time of logs and log rotation
Consult your legal department to know how long you can store logs

- Setup netflow with the nfdump and nfsen suite
  - Opt for netflow v9
- Log entries should contain **remote IP**, **timestamp**, resource requested and result of the operation
- Setup OSSIM for centralized logging
- Or collect and process logs with Splunk or the ELK stash

Evidence gathering

Train your evidence gathering skills

Agree with your ISP and CERT.be what evidence you can provide and what type of data they expect

Prefer to stick to flat text files, no Excel files, no PDF files, no screenshots

These closed formats are difficult to impossible to parse

Test raw traffic gathering features on your loadbalancer, proxies or webservers

- Test your 'export to text' or 'export to CSV' feature of your security device
  - If your device is unable to export logs or data to flat text then consider replacing the solution
  - Send a sample of different log files to CERT.be and ask to check if they are usable
    - Update the export field list based on the feedback
- Experiment with your netflow solution
- Gather network traffic data with tcpdump or snoop

  tcpdump -n -I eth0 -s 0 -w dump.pcap "port 80"

  -n : no DNS and service lookups

  -s 0 : full snaplength

  -w : write to file

  optionally use -C to limit the size of the outputfile

Monitor public sources

Continuously scan the internet for threats that might affect your organization

- Use Pystemon to scan dump sites
- Use Hootsuite to scan social networks

Prepare "we are down" services

Setup a status page with an overview of your services and actions being taken by your organization

- Host a temporary blog at a cloud-provider

4 PROACTIVE MEASURES

HOW TO BE READY FOR A DDOS ATTACK?

4.1 Dealing with DDoS attacks

Every large organization will have to deal with DDoS attacks, either sooner or later. This means that you have to be prepared to **detect, sustain, mitigate and recover** from the attack.

A few years ago one could just get more bandwidth or more CPU cycles to survive a DDoS attack. Current attacks however have evolved and have become both sophisticated and big. Because of their magnitude getting extra bandwidth or buying extra CPU cycles will do little to nothing to help you sustain an attack conducted by someone with enough motivation or resources at his/her disposal.

Therefore it's necessary to prepare your organization for DDoS attacks. This chapter lists a number of measures, both technical and non-technical, that you should take to limit the impact of a DDoS.

Besides the technical and non-technical measures there are also some legal steps you should take into consideration (6.3.2). Be prepared for these steps.

If you are experiencing an attack and your organization has some public exposure then you'll probably also have to talk to the press (either to respond to questions or to make a public statement). Be ready to have some form of **crisis communication** plan ready.

4.2 Know your assets

4.2.1 Inventory

It might sound obvious but make sure that you know your network, especially know what public services and networks that you have. Make sure you do not forget your off-site (e.g. cloud) services. If your internet connection is down you will not be able to access them.

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 of service owners, people responsible (both technical and non-technical) for all your exposed assets.

4.2.2 Evaluate your assets

You should also evaluate the risk and **importance** for your different services. Prioritize their importance.

In case of a DDoS against a relatively unimportant service you might want to choose to have traffic towards that service dropped at the ISP border routers to save the rest of your internet connection.

4.2.3 Risk based approach

Depending on your type of organization and your business services you can choose for a risk based approach. The resulting actions will then be dependent on the criticality of your (businesses) services.

ENISA has information available that helps you to compare risk management methods and tools (see 8.5)

4.2.4 Inventory sensitive content and critical services

If your services provide sensitive (content, risk, availability) content it's worth to inventory which sensitive content they're providing. Make an overview if you can split the sensitive content from the non-sensitive content.

You should read sensitive as "likely to be attacked" and "important to have available".

4.2.5 Recognize bottlenecks

Map out your network, services and servers to pinpoint possible bottlenecks. Knowing the weak components in your environment helps you to know to which resources you need to pay more attention to.

4.2.6 SANS Critical Security Controls

SANS provides helpful guidelines for achieving this. Both the **SANS Critical Security Control 1, Inventory of Authorized and Unauthorized Devices, and 2, Inventory of Authorized and Unauthorized Software** help you with the different steps on how to achieve this. Have a look at the **solution directory** in the Critical Security Control list for an overview of tools that can help you complying with the controls.

4.3 Contact procedure and details for incident response

When an attack happens you will almost certainl need to call for help from other parties.

Make sure that you do not solely rely on digital access for your contact procedure. In case of an attack the access to your contact database or telephone system (VoIP) might be limited. To deal with these kind of situations it's best to rely on a couple of hardcopies or offline copies of your most important contact details (key players in your management, legal department, communication department, your ISP, your national CERT, your SOC and possibly your security vendors).

Double check whether you have these out-of-band contact details. In cause of an attack it's very likely you will **not be able to e-mail** people!

Have an office room (war room) where people can work together on the incident. Having people sit together and work on the incident makes internal communication and coordination faster and less prone to errors.

Don't wait for an incident to appoint roles and responsibilities for incident response. Building an entire incident response team is out of scope of this document (see 8.4 for more info) but at least laying out out some groundwork for an incident response plan and an incident management plan is necessary.

A good incident response plan can make the difference between a security incident and a security crisis. Remember that it takes time and experience to build up the necessary expertise to be able to efficiently handle cyber security incidents.

Have your incident response plan **reviewed** regularly and have it **updated** frequently.

Appoint someone to **coordinate** this and take the lead and include both your communication and legal team in the incident plans. Communication people can help you dealing with the press and bringing the story correctly. The legal department in its turn can assist with filing complaints with legal authorities.

You should at least have some well-established crisis handling procedures and a containment strategy. It should be noted that computer people tend to only rely on e-mail for communication. In case of a DDoS e-mail communication might become cumbersome or slow so make sure you have other ways of reaching out to your contacts.

4.3.1 What do you report to your ISP, national CERT, SOC or security vendor?

Your ISP needs to be your best friend during a DDoS attack. They can help you with filtering incoming traffic and rate limiting traffic on their edge-routers.

The Belgian national CERT, CERT.be, can help you reach out to other parties involved. Through their international contacts and collaboration the CERT can assist your ISP in establishing proper contacts with other network owners and dealing with the attack. Depending on the nature of data that you want to share you might want to use an encrypted communication channel. To this purpose most CERTs use GPG[9], it is advised to exchange your public keys and verify fingerprints to allow for proper encrypted communication.

Prepare a contact procedure with your ISP and CERT.be so that you know how to report a DDoS incident to them and ask them for help. Make sure you test the contact procedure regularly.

Make sure that your ISP knows you as well. In case of an incident you don't want to go through the trouble of getting someone approved as a valid contact person to report issues to your ISP.

It is a good idea to ask your ISP what kind of protection measures they can put in place. Some ISPs can only apply limited packet-filtering where others can do full packet scrubbing.

Things you need to report are:

- affected networks (subnets, individual IPs, …)
- service (e.g. http) oriented or volume oriented
- start date
- what do you expect them to do (rate limit, filter, monitor, expand bandwidth?)
- packet capture samples (see 4.7.1)

4.3.2 What if you are part of the problem?

Instead of being the victim of an attack you might also be **part of the problem** (for example with amplification attacks, see 2.3.1.1) by participating to a DDoS attack.

To prevent, or at least limit, this problem you should apply filtering and proper system and service configuration (also see 4.6).

[9] https://www.gnupg.org/

Your national CERT (and to a lesser extend your ISP) can help you when you are unwillingly participating to a DDoS attack.

You will have to report the same information as when you are the victim of an attack. Similarily, make sure that you have a good understanding of how to report incidents to your CERT and ISP.

4.3.3 SANS Critical Security Controls

The SANS Critical Security Control 18, Incident Response and Management provides helpful guidelines for achieving this.

4.4 Firewalls and IDS

Firewalls only provide a limited protection against DDoS attacks. What's more, by exhausting the available resources on a firewall the attackers can prevent your network from accepting any incoming or outgoing packets. Additionally firewalls only act as a gateway and as such they can also become a bottleneck (by an attacker flooding the available connection tables). If your firewall allows web traffic (http) and the attacker targets the webserver then the firewall lets the traffic towards the webserver pass through.

Most of the DDoS attacks of today use valid packets, as such, an anomaly based detection solution as IDS or IPS is not very effective against a DDoS attack.

It is advisable to review if your network is well enough separated. Differentiate between public, private and semi-private services and have proper boundary protections between them. Also make sure that you have up-to-date physical and logical architecture schemas.

4.5 Network filtering

Note that some of the network mitigation techniques, described below, will not protect you against the more sophisticated attacks. They will almost certainly not protect you against large and longstanding volumetric attacks. This doesn't make these measures obsolete as the minimal effort needed to implement them still offers an extra layer of defense. Ideally you redirect your traffic through high-capacity networks that employ "traffic scrubbing" filters, but this might not be possible for every organization (or service type).

4.5.1 Network filtering

It is a good security practice to configure your network perimeter to deny all **incoming** and **outgoing** traffic that is not explicitly permitted.

You should apply the best practices mentioned in BCP-38 (or RFC 2827) for proper ingress network filtering. Block traffic that is often used within DDoS attacks (for example 'echo').

Rate limit the incoming ICMP traffic or certain UDP traffic that is not used within your organization. Only accept outgoing source addresses from your own range and drop incoming packets that have a source address in your range.

Rate limit outgoing ICMP and UDP to prevent the harm your network could cause in case a service on your network is abused as amplifier.

4.5.2 Application black lists

Sometimes it can make sense to prevent access to your applications from known "bad" IPs. Use automated blacklists to achieve this. Make sure that these lists are **automatically** updated.

4.5.3 Implement bogon block list

Bogon prefixes are routes that should never be seen (e.g. unallocated IP ranges, private address space, …). Although DDoS attacks can consists of other traffic sources, a lot of the attacks contain traffic that has a spoofed source in a bogon prefix.

You or your ISP should apply bogon prefix filtering[10]. If you apply bogon prefix filtering then it is very important that the block list is **automatically** updated, ideally you accomplish this via setting up a peering session.

4.5.4 Traffic shaping

Traffic shaping is manipulating and prioritizing network traffic. It's also called Quality of Service (QoS) or bandwidth management. If your network gear supports this you can delay the flow of less important traffic and prioritize the flow of other preferred network streams.

Be aware that traffic shaping / QoS can make the attack worse under certain conditions. Also, it doesn't help in protecting you against volumetric attacks or when the attackers use the high-priority traffic as an attack vector.

4.5.5 Network scrubbing

Redirect traffic towards your network through high-capacity networks that employ traffic scrubbing filters.

A couple of these high-capacity network solutions are listed in 8.10. Be aware that redirecting your traffic through these services can require you to change your DNS settings (the TTL, see 4.6.9).

4.5.6 Use a SYN Cookie

A SYN cookie is a specific choice of initial TCP sequence number. It can protect you against a SYN flood (in which the attacker only sends SYN packets, thereby filling the buffer at the receiving end). Instead of holding a table with all valid SYN/SYN-ACK sequences the server calculates the TCP sequence number. On receipt of the ACK from the client, the TCP sequence number is checked against the function to determine if this is a legitimate reply.

Implementing SYN cookie on the server that provides the resource that needs to be protected is a bad idea as calculating the cookie has a CPU impact. Ideally you enable this feature on a load balancer or protection device in front of your resource.

4.5.7 Rate limit the number of SYN packets

Rate limiting the number of SYN packets is another, more crude, way to protect your resources from a SYN flood.

Note that you'll have to be careful to not drop legitimate SYN packets. As such you first have to sample the "regular" number of SYN packets and then adjust your filters accordingly.

Be aware that this can also block legitimate large-scale proxies.

[10] http://www.team-cymru.org/bogon-reference.html

4.5.8 Filter incoming RFC-1918 addresses

The RFC-1918[11] address space is used for private Internets. These addresses should not enter your network via a public interface.

4.5.9 Use reverse path verification

Configure your network devices to only accept packets that have a route that points back to the same interface. Otherwise drop the packet. Large-scale networks with asynchronous routes might have to skip this method.

4.5.10SANS Critical Security Controls

The SANS Critical Security Control 10, Secure Configurations for Network Devices such as Firewalls, Routers, and Switches, the Control 11, Limitation and Control of Network Ports, Protocols, Services and the Control 13, Boundary Defense and the Control 19, Secure Network Engineering provide helpful guidelines for achieving this.

4.6 Proper system and service configuration

4.6.1 Updates and patching

The system and services that you expose should, in line with the patching policies and procedures of your organisation, be kept up to date. Patching is not only important for running reliable services but also for keeping them safe from abuse. Make sure that you are subscribed to the announcements from your server and service providers to get the latest updates that fix security (and other) problems.

4.6.2 Management interface

It is best practice to not manage the assets via the same communication by which your expose the service. For example if you run a public DNS server on IP 1.2.3.4 you should not do the remote management via that same IP but via another interface and IP (the 'management interface').

4.6.3 Vulnerability scanning

Scan your systems regularly for vulnerabilities. There are a number of services available that allow you to automatically scan your systems and services for vulnerabilities. Do the vulnerability scanning in coordination with your asset management (see 4.2).

4.6.4 Basic resource exhaustion protection

Configure your services properly so that attackers do not easily abuse them. Simple measures can already get you very far

- protect sign-up forms with a captcha or use challenge-response
- use application firewalls (for example for Apache you can use mod_reqtimeout, and mod_security), note that application firewalls do not provide protection against volumetric attacks
- resize your web material to reasonable formats (web-page images do not always need to be in full-color high resolution)
- use CDN[12] to host non-sensitive material (also see 4.6.9 and see 8.10)

[11] RFC1918 - http://www.ietf.org/rfc/rfc1918.txt

[12] CDN : Content Delivery Network
https://en.wikipedia.org/wiki/Content_delivery_network

An easy way to save on available resources is to separate your dynamic and static content to different servers. Separating your services, between dynamic and static services, allows you to do more fine-grained server-resource dimensioning. This of course requires you to have a good understanding of how your services are mapped out on your servers and network.

Reviewing your application logic can also help. Reverting to more static content will not only save you on processing power, it can also save bandwidth and will definitely get you a more responsive service.

Also note that there are a number of solutions available that reduce the size (and thus the required resources) of JavaScript and CSS files.

4.6.5 Load balancers and reverse proxies

You can add an additional layer of protection to your web resources by adding a load balancer or reverse proxy.

4.6.6 Prevent "open" services

You might be offering services that can be used by anyone on the Internet but that does not mean you should leave them uncontrolled. For example:

- prevent open Windows shares
- prevent open mail relays
- disable or restrict UDP services that can be used for amplification attacks
- prevent to run an open resolver
- configure your authoritative DNS servers to use RRL[13]

4.6.7 Create single purpose servers

If you run a **really critical** application or service, you should have (one or more) dedicated servers. This also makes it easier to move the application around in case of an incident.

4.6.8 Special attention to amplification vulnerable services

A lot of UDP services are abused for amplification attacks, because UDP is a connection-less protocol that does not validate the source IP address. As such it's fairly easy for an attacker to fake the source address. When many UDP packets have their source IP address forged to a single address, the server responds to that victim, creating a reflected Denial of Service (DoS) Attack.

The US-CERT published a list of UDP services that have the highest amplification rate (see 8.8). If you run any of these services it is strongly suggested to properly firewall or rate limit the service. Pay special attention to Chargen, NTP, SSDP, RIPv1 and DNS.

4.6.9 DNS TTL

One of the mitigation measures against an application attack is to move your service to another network. In most cases this will involve changing the IP address.

If you use a TTL of for example 24 hours then changing the IP address will still make your service unavailable for your users for a long timeframe.

[13] Response Rate Limiting in the Domain Name System (DNS RRL) : http://www.redbarn.org/dns/ratelimits

One option is to lower the TTL to for example 5 minutes. This will allow you to anticipate on an attack and conduct swift DNS changes.

Lower TTLs involve more DNS lookups (hence more DNS resource usage). You should check with your DNS provider if this poses any issues. You do not want to DoS yourself with to many DNS lookups! Also more DNS queries increase the chance of having cache poisoning (more frequent lookups that can be targeted).

Also be informed that some ISPs do not fully honor the TTL setting, they set their own cache setting, completely ignoring your provided TTL.

4.6.10 Prevent malware on your network

It's obvious that having a clean network not only increases the good functioning of your business resources but it also has other different advantages:

- your resources are not wasted to non-business processes
- your organization does not participate in malicious and possible illegal activities

Although it will not directly prevent a DDoS attack it prevents you from being part of the problem (preventing an outbound DoS). As such you should apply all the common advices for protecting your network.

So make sure that you properly update (regular patching) and firewall your machines (including workstations to make lateral movements more difficult), run malware protection measures and ideally a host intrusion system on your systems.

4.6.11 User awareness

Additionally you should continuously **raise awareness** amongst your users. Remember that in the end, no matter how much awareness you try to raise, you cannot prevent them from doing something wrong (clicking an attachment, entering user credentials on a phishing site).

The key is to make them **report** an issue when they feel something is suspicious. Ideally you set up an internal "report a security problem" mailbox. Make sure this mailbox is different to the normal "report an IT problem" mailbox.

4.6.12 SANS Critical Security Controls

The SANS Critical Security Control 3, Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, Control 4, Continuous Vulnerability Assessment and Remediation, Control 5, Malware Defenses, Control 11, Limitation and Control of Network Ports, Protocols, and Service and Control 12, Controlled Use of Administrative Privileges provides helpful guidelines for achieving this.

4.7 Network and system monitoring

4.7.1 Network baseline

You should do proper network monitoring to make sure that you have a baseline of what is normal network traffic. By having a baseline it's easier to detect what is abnormal traffic.

4.7.2 Netflow

Netflow data is network traffic data with the source and destination addresses, the source and destination ports and the amount of traffic transferred. It does not contain the actual data being transferred.

Netflow allows you to have an overview of the traffic entering and leaving your network. You can configure it to log every packet or only sample traffic (for example 1 out of every 100 packets). Netflow is available[14] on most routers. It is an ideal tool to fingerprint traffic patterns.

4.7.3 Graphical network stats

Netflow data provides you the raw network headers. Some netflow implementations (like for example nfsen) will give you a graphical representation of the traffic volume. Having graphs is necessary to quickly visually detect spikes in the traffic volume.

4.7.4 System and application logs

Ensure that your system and services do proper logging with all the necessary details for investigation. Your log entries should at least contain a full time stamp, the remote IP address, possible remote user identification data (user name, version and type of a client application) and the result of the request (a successful access, a failure).

Make sure that your system has enough storage space for the generated logs. Note that prior to a DDoS attack the attacker could have already done some reconnaissance. It's important to have logs for as long as technically and legally possible. If your system for processing logs does not have enough storage space you can transfer some of the older logs to other storage systems.

Take special care with access restrictions and possible tampering of logs.

4.7.5 Central Logger and Log management

Ideally you store the logs in one central place and store them in a central logger.

A central logger is not the same as a SIEM (Security information and event management).

Having all the logs centralized in a SIEM allows you to correlate different events from different machines. But it also introduces the possibility that you can miss important log-entries because they were hidden as a result of the correlation. If you are going to rely on a SIEM then verify that it is getting the necessary logs and that correlation of log events does not hide important data that can be of use during an investigation. Make sure that you have a system in place that allows you to get access to all the raw full logs and not only the aggregated, downsized logs.

Note that some attacks can prevent your systems from properly logging to a central logger. Use a dedicated network for logging.

4.7.6 Time synchronisation

Make sure that your network equipment, servers and services are **time-synced**. Having different time shifts makes it very difficult to reconstruct an event afterwards.

4.7.7 SANS Critical Security Controls

The SANS Critical Security Control 14, Maintenance, Monitoring, and Analysis of Audit Logs provides helpful guidelines for achieving this.

[14] It was initially introduced on Cisco routers but is now available on most routers. There is also a Linux daemon that can export netflow data of the network traffic being seen.

4.8 Evidence gathering

In order to help your ISP, your national CERT, SOC or security vendor to identify the type of attack and fingerprint its characteristics you need some evidence.

It's a good thing to prepare and test your evidence-gathering infrastructure prior to an attack. Consult and talk with your ISP and CERT to check on what they need and what you can provide. It doesn't make sense to send a large bulk of log files in a closed format if your ISP or CERT is unable to parse it. In most cases having the log formats in flat text files with well-defined fields is the easiest way for an ISP or CERT to parse the data.

Depending on the type attack you'll have to focus more on application level data or network level data. Make sure that there are no time skews in your evidence, we can't stress enough the importance of having your devices time synced properly (4.7.6).

If you suffer from an application attack then the application logs (see 4.7.3 and 4.7.5) are more important.

4.8.1 Traffic flows

As mentioned in 4.7.2 netflow is an ideal tool to get a basic overview of your traffic flows. Make sure you know how to use the netflow tool to extract the network traffic patterns from during an attack.

4.8.2 Raw traffic capturing

Raw traffic captures (with tcpdump or snoop) provide an ideal source to obtain more information on the exact attack traffic pattern. Some commercial brand firewalls also allow you to capture a (limited) set of packets. It is advised to store the captured data in a standard format such as PCAP.

Note that in most cases, especially during volumetric attacks, it can become impossible to capture the packets.

If for example an attack is towards your webserver you can do raw traffic gathering on your load balancers, your proxies or on your webservers. Use proper traffic filters to only capture the traffic that you need. Ideally you write the traffic to a file and not to the console display.

4.8.3 SANS Critical Security Controls

The SANS Critical Security Control 14, Maintenance, Monitoring, and Analysis of Audit Logs provides helpful guidelines for achieving this.

4.9 Monitor public sources

Some attacks are "pre"-announced on public networks, primarily social networks and dumpsites. It is worth investing in a couple of tools that monitor your organization name or products on these networks. Be careful though not to react in panic with every announcement. One of the goals of the attackers is to abuse your resources. If they can make you go in panic mode by merely posting one message announcing an attack then they have achieved their goal, without actually sending one packet to your environment.

4.9.1 Monitor dump sites

Sites like pastebin.com can be monitored with a tool called **Pystemon**, to be found on Github (https://github.com/cvandeplas/pystemon).

4.9.2 Monitor social websites

There's a plethora of tools available to monitor social websites. For example **Hootsuite** and **Social Mention** allow you to monitor different social networks for your brand name

4.10 Prepare "We are down" services

In the event that you have to deal with a DDoS attack that cripples your services you might want to inform your users of the downtime. It's a good thing to have a couple of services (web blog, status page, …) available that inform your users of the current status.

Make sure that these services consume little resources (static page), preferably are hosted off-site and that you have the mechanisms in place (e.g. DNS changes) to redirect your users towards these services. Since you won't be using them, don't forget to routinely check these pages, update them and patch them.

Be aware that, in case they are off-site, you should be able to communicate with them so prepare out-of-band connection measures.

5 REACTIVE MEASURES: SHORT SUMMARY

SUMMARY ON REACTIVE MEASURES

Verify and fingerprint

Look at your network / bandwidth graph to spot spikes

Define: the **timeframe**
the **network protocols** being used
the **source** networks and **destination** (you) networks/resources
get a list of top talkers
packet details
packet content

Analyze if the attack is **targeted** towards your entire network, a list of machines or services, one specific machine or service

If it is service or system oriented use your SIEM or **central logger** and match the list of external **top talkers** with your logs.
Define if there are a lot of rejected or error requests.

Match attacked assets on your network with critical services

- Use MRTG
- Netflow queries : aggregate on source and destination (address and port)
- Netflow queries : use number of flows, packets per second, bits per second
- **CERT.be** has netflow data (sampled 1/100) for Belnet and Fedman customers
- **CERT.be** can analyze flat-text logfiles for most common services

Escalate and start incident response procedure

List service **impact**

Evaluate legal actions

Double check your logging features

Setup a war room for incident response
Have contact details accessible

Be aware that DDoS can be a **smokescreen** for other attacks

Involve legal and communication department

Follow internal procedures during an incident

Take note of every action

- Do you have access to important contact details?
- Follow incident management plan
- Log every action
  - timestamp
  - the user who did the action
  - the expected result
  - the actual result
  - where the action took place

who approved the action

Mitigate application attack

Isolate the service
- Move to dedicated instance
- Disable the service, if possible according to your business needs

Strip down the service

- Move to cloud provider - **CDN**
  - Use Akamai, Cloudflare, etc.
- Minimize and compress CSS and JavaScript
- Split static and dynamic content

Evidence gathering

Export to flat text files
- Netflow data
- Application logs

Screenshots of network traffic graphs

Tcpdump output

Belnet and CERT.be (for volumetric attacks)

Fingerprint the attack

Inform the Belnet servicedesk

Report to CERT.be

CERT.be can provide input to Belnet network team based on netflow data

CERT.be can analyze application logs

- Verify traffic volume on Belnet Monitor
- ACLs on the edge routers of Belnet
  - Filter networks and ports
- CERT.be has **netflow** for Belnet customers
  - help with fingerprinting
  - provide feedback to Belnet networking team
- Send log samples to CERT.be
- Send traffic samples to CERT.be

6 REACTIVE MEASURES

HOW TO REACT WHEN YOU ARE THE VICTIM OF A DDOS?

6.1 A confirmed DDoS

So based on your **network baseline**, users reporting problems and central syslogger analysis you have confirmed that you are the victim of a DDoS attack.

Before jumping to conclusions and think that you are experiencing a DDoS attack it is necessary to check if a resource is only unavailable to you or also unavailable for everyone. There are a number of online resources that allow you to check if something is down, only for you or for everyone:

- http://www.isup.me/
- http://www.justdownforme.com/

When this happens: stay calm and accept it. By not getting into panic mode one can use more judgment to react to this attack. Also be prepared to accept that some DDoS attacks can only be solved by sitting it out.

The next steps, verifying the attack and fingerprinting the attack will happen in a recursive way, allowing you to get more details and providing more confirmation that the attack is still ongoing.

At first you might consider the traffic as a nuisance, while later you might have to escalate the event and redefine it to an incident, based on what you learn from the attack pattern and the impact that it has on your services.

6.2 Verify and Fingerprint the attack

Before going into incident mode it is important to verify that an attack is actually taking place. Use your network monitoring tools and the system and application logs from your central syslogger to analyze if the attack is real. Make sure to exclude any unintentional attacks by verifying the logs. Be aware that if you use a SIEM instead of a central syslogger it can give you a limited view on what is happening (because of reduced log information).

Compare the traffic that you currently observe with the traffic pattern that you learned previously from the network baseline. The graphical view on the network traffic volume can be very helpful in this type of situations.

This same process will also help you determine if this consists of a traffic attack, a volumetric attack or an application attack. You'll need netflow data to determine this.

Basically what you have to do in a first round is to answer the following questions:

- determine the timeframe of the attack (what was the start point, is the attack still ongoing?)
- what network protocols are used (TCP, UDP, ICMP, IPv4 or IPv6, …)
- what are the sources and destinations (network location)
- packet details (size, which flags are set, source port and destination ports)
- packet content (type of request)

6.2.1 Netflow

Netflow is the ideal tool to do a high level analysis of the network attack pattern as it can show you what protocols are used, the sources of the attack and the target of the attack.

Ideally you have a tool in place that continuously monitors your network traffic and provides both a data view and a graphical view. A DDoS should show a spike in the monitored traffic. Focus your netflow queries around that timeframe.

Once you have isolated the timeframe you can run different queries. Use queries that focus on number of flows, number of packets, number of bits, number of packets per second or number of bits per second.

Use the different netflow queries with aggregation on source address, source port, destination address and destination port. For example by running a query that aggregates on destination address you can find out if the attack is towards different assets in your network or only against one host. A next aggregation query (on destination port) can reveal if the traffic is aimed towards one specific service.

By looking at number of flows and number of packets you can determine if it is normal traffic or traffic that tries to exhaust your resources. Also use netflow to verify if the attacked host(s) sends replies. This reveals if it consists of established communication flows or not. Based on the different netflow queries you should be able to tell if this is either a traffic / application attack or a volumetric attack.

Use netflow to build a list of

- top talkers (remote and local)
- protocols used
- top ports (source and destination)
- package length, package flags

6.2.2 Netflow at CERT.be

CERT.be has netflow data for a number of Belnet (and Federal government) customers. This netflow data is sampled though and does not provide as much details as having your own netflow solution.

6.2.3 Application logs

If you conclude that this is an application attack then you have to analyze the application logs and look for anomalies.

Use the list of remote top talkers to extract the relevant log lines for one of the attackers. Next verify if these log lines contain accepted requests, reject requests or errors. Accepted requests are requests that look fairly “normal”, they can be done by

almost everyone and are in line with normal interaction with the service. Rejected requests are also in line with normal interaction with the service but contain some sort of error. Errors are requests that have nothing to do with the provided application.

For example if you run an application via Drupal. An accepted request is a 200 HTTP status for getting a Drupal web page. A 403 HTTP status in turn corresponds with a rejected request to access an ACL protected area. A 404 HTTP status corresponds with an error request, for example a request to access a resource that only exists in Wordpress sites.

6.2.4 Matching with your sensitive content and critical services

Based on the information that you gathered from netflow and the different logs you can now verify how much impact this attack has on your organization. Use the knowledge of your assets and priority of the different services (and content) to assess if the impact is critical or if it can be ignored (or monitored with a lower priority).

6.3 Escalate to an incident

Escalating the attack to an incident means starting your incident response procedure, both internally and for actions with your partners. There is no “one-rule-fits-it-all” to make the difference between what is an event (albeit annoying and disturbing) and when it becomes an incident.

The following are actions that should be taken into account when escalating an event to an incident.

6.3.1 Determine the service impact

By fingerprinting of the attack and matching this with your critical services you were able to deduct the nature of the attack.

You should identify, log and note the impact the attack has on your services. Do this both from an internal point of view and “from the outside”.

This verification process should also include the input from the risk based approach (see 4.2.3).

If the attack prevents a service from working properly you should inform the service owner and your management. Additional controls might be in place but this depends on your BCP[15] and incident management plan.

6.3.2 Legal actions

Besides the technical and non-technical measures there are also some legal steps you should take into consideration. Especially if you are the victim of extortion (for example DD4BC 2.6) you should file a complaint with the legal authorities.

Consult with your management and legal team to setup proper procedures.

6.3.3 Verify logging

During the escalation process you should verify that all your logging (central logger or SIEM) and alerting procedures are still working properly. You don’t want to end up dealing with an incident and then finding out you have no appropriate logging or investigation material.

[15] business continuity plan

6.3.4 Smokescreen

Realize that a DDoS attack can merely be a smokescreen to hide another attack. Because you go into incident mode your staff will be focused on dealing with the attack. Other events might go unnoticed or get less attention.

The DDoS can mask the attempts from attackers to gain access to other parts of your network or exfiltrate your company data. Because of this it remains important to keep on following your normal procedures during an attack.

6.3.5 When is the incident, DDoS attack finished?

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. They can make you believe that the attack has stopped, hoping you let your guard down and then re-launch a new, more powerful, attack.

6.4 Setup a war room for incident response

Make sure that all people get together in one place for easier collaboration and communication so setup a war room. Ensure the availability of out-of-band communication (see 4.3) lines and all the necessary contact details in this office place.

Assign somoneto to take the lead for incident response managing the actions. Make sure that everyone knows how to contact (telephone, e-mail, office location) the lead.

Setup liaisons with your communication and legal department and inform management.

Note that your communication team deals with your “outside” communication. Define “outside” as “outside your IT environment”. You will have to provide your communication team the input on **what** happened so that they can have a streamlined communication process with management, the press, stakeholders and the other company departments. Also see 8.4 and 8.5.

6.5 Contact your ISP and CERT.be

The data that you have collected during the fingerprinting process and later on during the evidence gathering can help you determine if you can mitigate the attack internally or if you need assistance from your ISP or CERT.be

The collected data and fingerprint is needed to report the incident to your ISP and CERT.be and request actions. Because of this it is important to be as detailed as possible.

If you contact your ISP you should at least provide:

- the **traffic fingerprint** observed so far
- the timestamp, when did it started, is it still ongoing
- the impact on your services
- what would you like them to do

Backup your claim to the ISP and CERT.be by providing traffic captures, sample netflow and application logs.

If you contact your ISP and only mention that you are under attack without further details their mitigation actions might be limited. Or they could take the wrong actions and make things even worse. If you can specify what you observed they can more easily apply effective filters or rate limit certain traffic.

6.6 Procedures

6.6.1 Follow the internal procedures

It is important to stress that, even during an incident, you have to follow the normal internal procedures. Do not let the crisis allow anyone to overrun your own security protocols and policies.

6.6.2 Log the actions

Evenly important as adhering to the existing procedures is to keep notes of all the actions being taken, by whom, for what reason and what was the expected outcome. Eventually you should have a complete log of the different actions being taken during the incident.

This log should contain the timestamp, the user who did the action, the expected result and the actual result, where the action took place and who approved the action.

Do not let anyone apply a measure that cannot be tracked afterwards.

This log will help you to reconstruct the entire timeline afterwards and it will also be a big help for doing the "**lessons learned**" phase afterwards.

Do not be limited to "digital log taking". Sometimes it's far easier to write the actions in a notebook.

6.7 Mitigating an application attack

6.7.1 Isolate the service

If the attacked service is on a server that also provides other services you can move the attacked service to another machine.

You can either move it to

- a more powerful virtual machine in your infrastructure
- a more powerful physical machine in your infrastructure
- a **cloud hosting provider** (**CDN**), depending on the sensitivity of the hosted content

Even if you host sensitive content you can still use an external cloud-hosting provider by splitting the sensitive (hosted locally) and non-sensitive content (hosted in the cloud).

Note that moving your service to another host or network most likely involves changing the DNS records. Make sure you have lowered the DNS TTL settings (4.6.9) as a preventive measure otherwise the impact for your customers can be longer than expected.

6.7.2 Strip down the service

Based on an earlier analysis of the application logic it might be possible to strip down a service to its bare minimum. For web applications for example using low-res images and compress and minify the CSS and JavaScript files can already reduce the traffic load. Hosting the images, CSS and JavaScript on other servers could also temporarily help with mitigating the problem.

Take note though that if your service is an HTTPS application that you do no start mixing HTTP and HTTPS content. Having “mixed” content should raise suspicion amongst your users. On the other hand it can be a good trade-off instead of losing the service entirely.

You can also replace dynamic generated contact with static content. This will be dependant on the type of service that you provide. Instead of for example having your application doing regular requests to its back-end you can –temporarily- provide it with a static reply.

6.7.3 Protect an SSL service

If you run an SSL enabled application you can consider offloading the SSL from the original infrastructure. Once offloaded it can be possible to inspect the traffic and possibly mitigate against attack traffic. Be careful that you are not moving the problem from one place to another place. Note that because you remove the encryption you’ll have to make sure that this is in compliance with regulations and your user policy.

6.7.4 Avoid remote management

Most assets are now managed remotely. You should have an out-of-band solution to keep management access to your assets but in some cases even this access might fail.

As a last result you can ask your datacenter provider if you can host staff at their premises to access your assets via the console. Because console access is not designed to be used for long-time debugging, dealing with the attack via this way can be a slow and painful process.

6.8 Evidence gathering

Regardless if you want to report the incident to your ISP, to CERT.be, to the legal authorities or to any other partner you’ll have to come up with some form of evidence. You can provide evidence on a flow level, network level and application level. Ideally you can come up with all of these.

Verify the recommendations set in the previous chapter 4.8 to gather raw traffic captures and export your netflow and application logs.

Together with your earlier gathered fingerprint details you should report the

- flat text exported netflow data
- maybe some screenshots of the network graphs to illustrate the network traffic peaks
- flat text export of the application logs
- a representative network capture (pcap)

We can't stress it enough that the time settings of the machines that you use are all time synced, make sure that there are no time skews (see 4.7.6).

6.9 How can your ISP and national CERT help?

If you suffer from a volumetric attack then your ISP is often the only one who can help you. Your ISP can also provide help when you suffer from a traffic or application attack if you are unable to apply proper mitigation techniques.

You, as a victim, will probably have little to no defense measures to take against a volumetric attack.

ISPs can help their customers in different ways and you should absolutely inquire with the network team of your ISP what type of protection service that they provide you (see 4.3.1). Preferably you do this before an attack happens.

The basic protection measures will consist of

- Filtering or rate-limiting incoming packets (blocking) for a specific host or network

- filtering or rate-limiting incoming packets (blocking) for a specific service

Most ISPs will also be able to apply rate-limiting protection measures. Rate limiting can help with protection against volumetric attacks but might not be the ideal solution to protect applications.

It is likely that if you rate limit for example the number of incoming SSDP or UDP-Quake packets that you will experience little to no side-effects. So this can protect you if you suffer from this type of amplification attack. However if the traffic is oriented towards your application (for example resource exhaustion) then rate-limiting traffic towards your application will have the desired effect, but from an attacker point of view: Your service is no longer fully available.

Some ISPs provide you with traffic shaping (or Quality of Service) where certain network traffic gets a higher priority.

Certain responses (particularly to volume attacks) involve sacrificing (completely blocking) an attacked service in order to protect the other parts of your network.

Some ISPs provide you with high-bandwidth network scrubbing services. You can compare this service with a car-wash for network packets. All the unwanted traffic during an application attack or traffic attack can be cleaned up and then again redirected to your network. Using these scrubbing services can require you to change the DNS settings (also see 4.6.9 and TTL). A similar approach is having your traffic redirected to a high-bandwidth provider as listed in 8.10.

Your national CERT will rarely be in the position to apply network filters themselves but they can help you with analyzing the attack pattern and building a fingerprint. Also because most national CERTs have good international contacts they can coordinate the request to ISPs (in other countries) to take actions against an ongoing attack.

Note that if you are going to file a complaint with the legal authorities you might have to go through your local police to have them coordinate the actions. Because of legal boundaries this process might not be as fast as desired.

Because national CERTs exchange information on current attack trends they can also assist you in dealing with more advanced attacks and verify if certain attack patterns were observed on other networks in other countries.

6.9.1 How can Belnet help?

If Belnet is your ISP then it can help you with both rate limiting and filtering network traffic. Belnet does not provide traffic shaping and traffic scrubbing at the time of writing.

Note that any filtering measures put in place by Belnet are only **temporarily**. You should not consider Belnet filtering as a replacement for your local firewall or security devices.

6.9.2 How can CERT.be help?

CERT.be is part of Belnet. If Belnet is your ISP then CERT.be is in a unique position to coordinate the mitigation actions with the Belnet network department.

If Belnet is your ISP then CERT.be can also analyze part of the attacking network traffic via its own netflow sensor (see 6.2.2). Note that the netflow data is sampled so for a full detailed view you'll still have to rely on your own infrastructure.

CERT.be can help you defining the exact, adequate fingerprint to deal with the attack and provide this information in a direct communication with the Belnet network team.

CERT.be works closely within the circle of European national and government CERTs[16][17]. CERT.be also has a good working relationship with a number of teams outside[18] of Europe (both national, governmental and commercial CERTs).

The CERT.be employees are also very active within different security groups. With all this information CERT.be is able to verify if your attack was also observed at other locations (maybe against an organization in the same sector in another country) and what tools or processes might have caused this attack.

If you notice that the bulk of an attack originates from an ISP outside Belgium then CERT.be may be able to get to that ISP via its relations with the CERTs in the originating country.

[16] EGC : European Governmental CERTs

[17] TF-CSIRT : Trusted CERTs within Europe

[18] FIRST : Forum of Incident Response Teams

7 EXAMPLES

SOME REAL-LIFE EXAMPLES

7.1 Volumetric attack, UDP amplification attack

7.1.1 Intake

You are a customer of Belnet and you have reported a slow internet to the Belnet servicedesk. You requested help.

All of your Internet connection is suddenly getting very slow. No-one at your organization is able to get “out” on the Internet and no-one from the outside is able to reach your webserver. Your network graphs show a spike in traffic since 30’. Instead of the regular 20Mbs you are now suddenly getting 750Mbs. You do not have a netflow solution and you do not have the technical expertise to do network captures.

You ask Belnet to cooperate with CERT.be.

In close communication with you as the customer, Belnet will report to CERT.be that :

- That you are a Belnet customer with acronym “ALPHAPAPA”
- That your public networks are 193.191.x1.1/25 and 193.191.x2.1/26
- That you observed the beginning of the attack, based on your network graphs, some 30’ ago

7.1.2 Analysis

CERT.be will then use its netflow sensor and examine all the traffic going to and coming from the networks 193.191.x1.1/25 and 193.191.x2.1/26. CERT.be will then query for the top network flows, aggregate on destination address and aggregate on destination port. The last query will show a high amount of individual short flows towards SNMP up/161 and Chargen up/19.

The queries show that there a high number of different source networks involved. Combined with the UDP-protocol these source addresses are very likely spoofed.

CERT.be will report this information to you and to Belnet.

CERT.be proposes to you to filter all traffic towards udp/19 and udp/161 coming from outside your network.

7.1.3 Actions

You report to Belnet and CERT.be that you use SNMP to monitor your services.

This does not pose a problem because Belnet will only filter traffic that is coming from outside the Belnet network. Your SNMP requests have an IP address within the Belnet range.

Belnet applies the network filters and activates network counters to check if the attack is still ongoing. Once the counters no longer increase the network filters will be removed.

7.1.4 Lessons learned

Once the attack has been dealt with CERT.be, Belnet and you should have a lessons learned meeting.

8 EXTERNAL RESOURCES

8.1 Resources for proactive measures

Security Control 1 : Inventory of Authorized and Unauthorized Devices
https://www.sans.org/critical-security-controls/control/1
https://www.sans.org/critical-security-controls/vendor-solutions/control/1

Security Control 2 : Inventory of Authorized and Unauthorized Software
https://www.sans.org/critical-security-controls/control/2
https://www.sans.org/critical-security-controls/vendor-solutions/control/2

Security Control 3 : Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
https://www.sans.org/critical-security-controls/control/3
https://www.sans.org/critical-security-controls/vendor-solutions/control/3

Security Control 4 : Continuous Vulnerability Assessment and Remediation
https://www.sans.org/critical-security-controls/control/4
https://www.sans.org/critical-security-controls/vendor-solutions/control/4

Security Control 5 : Malware Defenses
https://www.sans.org/critical-security-controls/control/5
https://www.sans.org/critical-security-controls/vendor-solutions/control/5

Security Control 10 : Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
https://www.sans.org/critical-security-controls/control/10
https://www.sans.org/critical-security-controls/vendor-solutions/control/10

Security Control 11 : Limitation and Control of Network Ports, Protocols, Services and the Control
https://www.sans.org/critical-security-controls/control/11
https://www.sans.org/critical-security-controls/vendor-solutions/control/11

Security Control 12 : Controlled Use of Administrative Privileges
https://www.sans.org/critical-security-controls/control/12
https://www.sans.org/critical-security-controls/vendor-solutions/control/12

Security Control 13 : Boundary Defense and the Control
https://www.sans.org/critical-security-controls/control/13
https://www.sans.org/critical-security-controls/vendor-solutions/control/13

Security Control 14 : Maintenance, Monitoring, and Analysis of Audit Logs
https://www.sans.org/critical-security-controls/control/14
https://www.sans.org/critical-security-controls/vendor-solutions/control/14

Security Control 18 : Incident Response and Management
https://www.sans.org/critical-security-controls/control/18
https://www.sans.org/critical-security-controls/vendor-solutions/control/18

Security Control 19 : Secure Network Engineering
https://www.sans.org/critical-security-controls/control/19
https://www.sans.org/critical-security-controls/vendor-solutions/control/19

NFDUMP / NFSEN
http://nfdump.sourceforge.net/
http://sourceforge.net/projects/nfsen/

OSSIM
http://www.alienvault.com/

Splunk
http://www.splunk.com/

ELK – Elasticsearch, Logstash, Kibana
https://www.elastic.co/

Cisco - Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks
http://www.cisco.com/c/en/us/support/docs/security-vpn/kerberos/13634-newsflash.html

TCP SYN Cookies – DDoS defense
http://etherealmind.com/tcp-syn-cookies-ddos-defence/

tcpdump
http://www.tcpdump.org/

tcpdump cheat sheet
http://packetlife.net/blog/2008/oct/18/cheat-sheets-tcpdump-and-wireshark/

snoop
http://docs.oracle.com/cd/E23824_01/html/821-1453/gexkw.html

Pystemon
https://github.com/cvandeplas/pystemon

Hootsuite
https://hootsuite.com/

CSS Minifier
http://cssminifier.com/

JS Compress
http://jscompress.com/

Team Cymru Bogon Prefixes
http://www.team-cymru.org/bogon-reference.html
http://www.team-cymru.org/bogon-reference-bgp.html

UDP-Based Amplification Attacks
https://www.us-cert.gov/ncas/alerts/TA14-017A

DNS amplification attacks and open DNS resolvers
https://www.cert.be/docs/dns-amplification-attacks-and-open-dns-resolvers

DNS-RRL,DNS Ratelimiting
http://www.redbarn.org/dns/ratelimits

Mod_Security
https://www.modsecurity.org/

NMAP Cheat Sheet
http://pen-testing.sans.org/blog/2013/10/08/nmap-cheat-sheet-1-0

OpenVAS
http://www.openvas.org/

NIST 800-3 : Establishing a Computer Security Incident Response Capability
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

GPG Userguides
https://www.gnupg.org/documentation/guides.html

MIT GPG Public Server
https://pgp.mit.edu/

8.2 Resources for reactive measures

Verify that you are experiencing an attack
http://www.isup.me/
http://www.justdownforme.com/

Netflow for incident detection
https://www.first.org/global/practices/Netflow.pdfHootsuite

MRTG
https://oss.oetiker.ch/mrtg/doc/mrtg.en.html

Belnet Monitoring
https://monitor.belnet.be

8.3 DDoS Guidance

DDoS Mitigation by CIRCL
https://www.circl.lu/pub/dfak/DDoSMitigation/#the-digital-first-aid-kit

8.4 Incident Response

NIST 800-3 : Establishing a Computer Security Incident Response Capability
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

ENISA material
https://www.enisa.europa.eu/activities/risk-management/current-risk/bcm-resilience/bc-plan/incident-response-plan
https://www.enisa.europa.eu/activities/risk-management/current-risk/bcm-resilience/bc-plan/incident-management-plan
https://www.enisa.europa.eu/activities/cert/support/guide

A step-by-step approach on how to setup a CSIRT
https://www.enisa.europa.eu/activities/cert/support/guide

Create a CSIRT by CERT/CC
http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm?

SANS Building an Incident Response Program To Suit Your Business
https://www.sans.org/reading-room/whitepapers/incident/building-incident-response-program-suit-business-627

8.5 Risk Management

ENISA Risk Management
https://www.enisa.europa.eu/activities/risk-management

ENISA Comparison of Risk Management Methods and Tools
https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/comparison/comparison.html

Report on Cyber Crisis Cooperation and Management
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study

8.6 SANS Critical Security Controls

List of Critical Security Controls
https://www.sans.org/critical-security-controls/controls

List of solutions for achieving the Critical Security Controls
https://www.sans.org/critical-security-controls/vendor-solutions

8.7 Network related

Cisco - Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks
http://www.cisco.com/c/en/us/support/docs/security-vpn/kerberos/13634-newsflash.html

TCP SYN Cookies - DDoS defense
http://etherealmind.com/tcp-syn-cookies-ddos-defence/

The Bogon Reference
http://www.team-cymru.org/bogon-reference.html

8.8 Services related

DNS amplification attacks and open DNS resolvers
https://www.cert.be/docs/dns-amplification-attacks-and-open-dns-resolvers

UDP-Based Amplification Attacks
https://www.us-cert.gov/ncas/alerts/TA14-017A

8.9 Useful RFCs

The RFCs can be found at http://www.ietf.org/rfc/

RFC1918 - Address Allocation for Private Internets
http://www.ietf.org/rfc/rfc1918.txt

RFC2827 - BCP38 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
https://www.ietf.org/rfc/rfc2827.txt

8.10 Commercial Solutions

This is only a limited overview of commercial solutions available to deal with DDoS. None of the solutions here are endorsed by CERT.be and neither does it mean that when a solution is not listed here that CERT.be advocates against the use of this solution.

There have been comparisons between the different available solutions. But as with all the "test" comparisons you should translate the results to your network environment.

See for example :

- http://ddos-protection-services-review.toptenreviews.com/
- http://www.net-security.org/secworld.php?id=13446

8.10.1 Cloudflare

CloudFlare's advanced DDoS protection, provisioned as a service at the network edge, matches the sophistication and scale of such threats, and can be used to mitigate DDoS attacks of all forms and sizes including those that target the UDP and ICMP protocols, as well as SYN/ACK, DNS amplification and Layer 7 attacks.

See : https://www.cloudflare.com/ddos

8.10.2 Arbor

Arbor has been protecting the world's largest and most demanding networks from DDoS attacks for more than a decade. Arbor strongly believes that the best way to protect your resources from modern DDoS attacks is through a multi-layer deployment of purpose-built DDoS mitigation solutions.

See : http://www.arbornetworks.com/ddos-attacks

8.10.3 Akamai

Akamai's DDoS protection service is said to be designed to stop even the largest, strongest DDoS attacks.

See : https://www.akamai.com/us/en/solutions/products/cloud-security/ddos-protection-service.jsp

8.10.4Prolexic

Prolexic, now a part of Akamai is the world's largest and most trusted distributed denial of service (DDoS) mitigation service provider. They claim to block the biggest and most complex DoS and DDoS denial of service attacks that often overwhelm other vendors.

See : http://www.prolexic.com/

8.11 War stories

Large Scale DDoS Attack on github.com
https://github.com/blog/1981-large-scale-ddos-attack-on-github-com

Technical Details Behind a 400Gbps NTP Amplification DDoS Attack
https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

DDoS Packet Forensics: Take me to the hex!
https://blog.cloudflare.com/ddos-packet-forensics-take-me-to-the-hex/