TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Instructions – Denial-of-service attack

Traficom Research Reports
25/2022

Contents

1 Introduction

1.1 Purpose of the instructions

The purpose of these instructions drawn up by the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency Traficom is to offer advice to organisations in situations in which it is suspected that a denial-of-service attack has occurred or a denial-of-service attack prevents normal operations. The instructions are focused on how to deal with the special characteristics of this type of information security incident. In order to resolve the situation completely, the organisation should maintain the incident response plan it has drawn up in case of information security incidents and follow it.

These instructions offer guidance on a general level on how to act in case of an information security breach and recover from it. It is recommended that the organisation should draw up a separate guide for its own use that takes its technological and operational environment into account in more detail. The project is funded by the National Emergency Supply Agency.

1.2 What does a denial-of-service attack mean?

A denial-of-service attack is an attack in which a malicious actor tries to prevent the use of a network resource or service by disrupting its operation. The attack can be implemented by overloading the targeted service or network traffic with extra traffic or using a vulnerability in the service or network device. Currently most of the denial-of-service attacks are distributed, meaning that the traffic is sent to the target simultaneously from several sources. There is often a botnet controlled by the attacker behind distributed attacks; it consists of several devices connected to the internet that have been hijacked to be used in the attack without the knowledge of the owners of the devices.

Denial-of-service attacks are usually carried out by overloading the target purely due to a large traffic volume, or alternatively by sending the kind of traffic that makes the target device use more memory or computing resources to handle the traffic than normal, in which case the volume of traffic does not need to be especially high. Attacks of this type may not cause abnormal growth in the amount of traffic.

In application layer denial-of-service attacks, the target may be, for instance, a database running behind the application that is overloaded by sending large amounts of queries via the application itself.

Today, a denial-of-service attack does not require any great technical expertise, because such an attack can be purchased affordably as a service over the darknet, for example. Attacks are often used for blackmail, bullying or political harassment (so-called hacktivism), in which case the attack is usually ordered and carried out by different parties.

There are many different ways to execute the attack, but all of them have the same end result. One classic method involves the use of distributed TCP SYN flood attacks, in which a botnet sends large numbers of TCP SYN packages to the target while failing to send ACK packages. This leads to a situation in which the target’s TCP stack fills up with incomplete TCP handshakes, and neither the server nor the device can accept any more new handshake requests. In preparing for an attack, you should focus on combating the most common attack methods.

2 Preparation

Typically, the IT service provider is responsible for correcting any disruptions in telecommunications, which means that quick recovery from a disruption requires a service level agreement (SLA) that obliges the service provider to restore the service level quickly.

In case of a denial-of-service attack, a separate agreement for mitigating the effects in case of an attack may be necessary. The software of the network devices and servers should also be kept up to date, because some denial-of-service attacks exploit the vulnerabilities of software.

In addition to the agreements, duplicating the telecommunications connections as well as potential backup systems must be implemented, depending on how critical the system in question is. In case of a disruption, you should have an operating model ready that guarantees a smooth flow of communication between the company and the service providers as well as a definition of situation management and documentation of the situation. The people involved in correcting the disruption must have clear roles, and the lines of investigation must be clear and appropriate.

Organisations can assess their own readiness by using the Kybermittari (Cybermeter) cyber security evaluation tool of the National Cyber Security Centre Finland, for instance.[1] The National Cyber Security Centre Finland has also published separate instructions for preventing and combating denial-of-service attacks in particular (in Finnish).[2]

2.1 Administrative measures

- Draw up an incident response plan for your organisation in case of a denial-of-service attack.
- Train the personnel on how to act during security incidents such as the ones described in the playbook.
    - Also offer basic training for regular employees, advising them on how to act if a denial-of-service attack cripples the services of the company.
- Find out in advance how you can report an information security breach to the National Cyber Security Centre Finland.[3] Start monitoring the news by the National Cyber Security Centre Finland.[4]
- Review attack scenarios together with the company's management and agree on the practical measures as well as management responsibilities and authority in case of an information security breach.
- Develop[5] an incident response plan and practice it regularly with tabletop exercises, in which responsible persons and interest groups practice the information security incident response process in imaginary scenarios.
- Implement continuous vulnerability and update management.
- Identify the components critical to the business and create and maintain lists of what needs to be protected.
- Specify the necessary access rights carefully based on the needs of the users and the technical functionalities.

[1] https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter
[2] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta_0.pdf

[3] https://www.kyberturvallisuuskeskus.fi/en/report
[4] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news
[5] https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises

- Consider establishing a security operations centre (SOC) or purchasing a similar service. The purpose of the security operations centre is to monitor the network traffic of your company and information security events in the systems.
- Make sure that the agreements with the service providers cover the prevention of denial-of-service attacks.

2.2 Technical measures

- Aim to detect attacks as early as possible by using different kinds of centralised monitoring solutions and make sure that their functionality is also tested regularly. For example, IDS solutions (Intrusion Detection System) detect attacks and often attempt to prevent them automatically.
- Keep the server software up to date and check that the configurations are in accordance with the recommendations. The right configurations can mitigate the impact of denial-of-service attacks.
- Configurations that mitigate the impact of denial-of-service attacks may include features such as limiting the speed of individual connections (rate limiting), extending the TCP connection processing queue (backlog queue), recycling incomplete TCP connections (half-open connection recycling) or implementing SYN cookies. Find out which of these methods are the best suited to your server environment and implement them as needed.
- The National Cyber Security Centre Finland has published a technical guide on how to defend yourself against denial-of-service attacks (in Finnish).[6]

2.3 Preparation and training in practice

One important part of preparation is practicing threat scenarios. By practicing the scenario found in these instructions in advance, an organisation can make sure that it is ready to meet situations like the one described. Training ensures, among other things, that the personnel of the organisation understand what the different parts of the workflow and checklist in the instructions mean and they have the capability to act according to the instructions.

For instance, the scenario in this case could be a situation in which a denial-of-service attack has crippled a critically important information system, preventing the use and operation of the system completely.

What would your organisation do in case of an information security breach like the one described? Practice at least the following steps of this playbook:

- Reporting the security breach and escalating the situation
- Notifying the essential service providers and other interest groups of the situation
- Deploying a backup system
- Final investigation process of the security incident

In connection with all of the steps being practiced, you should think about how the organisation leads the information security breach management, how the internal communications work and who is the person responsible or their deputy at which stage. It is also recommended that you study the materials of the National Cyber Security Centre Finland related to exercises.[7]

[6] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_liite_1_Palvelunestohyokkaysten_tekniikkaa_puolustajille_0.pdf
[7] https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises

3 Detecting an information security breach

A denial-of-service attack is usually detected because services stop working. Comprehensive monitoring may also detect an attack before it affects the availability of services, due to factors such as the rapid increase of network traffic or the consumption of resources on a server. Some denial-of-service attacks may try to cause a malfunction in individual network devices, in which case there may not be major changes visible in the traffic volumes. For this reason, it is important that the operation of individual network devices is within the scope of monitoring.

Report the information security breach to the National Cyber Security Centre Finland.[8] We advise you confidentially and free of charge on how to limit the damage, analyse the incident and take recovery measures. At the same time, you support the national information security situation awareness and make it possible to help and warn other potential victims.

[8] https://www.kyberturvallisuuskeskus.fi/en/report

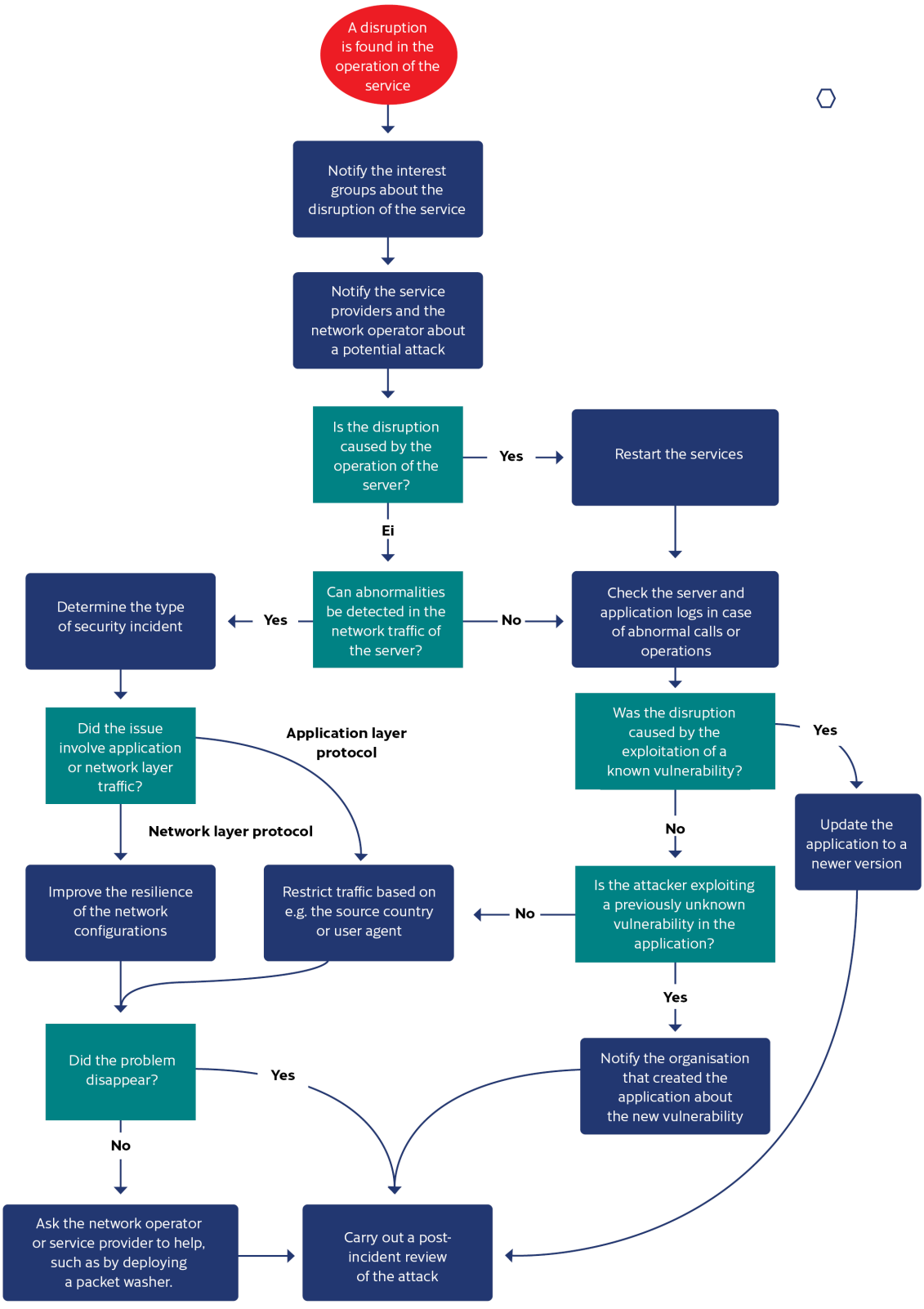
4 Instructions

Use the attached checklist to find measures to help you if you suspect that you have become the target of a denial-of-service attack. The checklist helps your organisation to prioritise and use a phased approach when investigating information security incidents.

4.1 Workflow of an information security breach investigation

The flow chart below describes the right order of measures when investigating the security breach. The flow chart supports the use of the checklist. During the investigation, it is also crucially important to keep an accurate event log of the measures taken. The log should show the measure taken, the timestamp and the party that implemented the measure.

The gathering of potential evidence should also be documented carefully. You should record who gathered the data, what it was, and when and how it was gathered. A carefully drawn up event log makes the investigation as well as the cooperation with the police and information security investigators significantly easier.


A disruption is found in the operation of the service
Notify the interest groups about the disruption of the service
Notify the service providers and the network operator about a potential attack
Is the disruption caused by the operation of the server?
Yes
Restart the services
Ei
Determine the type of security incident
Yes
Can abnormalities be detected in the network traffic of the server?
No
Check the server and application logs in case of abnormal calls or operations
Did the issue involve application or network layer traffic?
Application layer protocol
Network layer protocol
Was the disruption caused by the exploitation of a known vulnerability?
Yes
Update the application to a newer version
No
Improve the resilience of the network configurations
Restrict traffic based on e.g. the source country or user agent
No
Is the attacker exploiting a previously unknown vulnerability in the application?
Yes
Did the problem disappear?
Yes
Notify the organisation that created the application about the new vulnerability
No
Ask the network operator or service provider to help, such as by deploying a packet washer.
Carry out a post-incident review of the attack

4.2 Immediate measures

Goals of the phase	The accuracy and speed of the measures are both important. The goal of the immediate measures is to determine the cause of the telecommunications disruption and start the mitigating or corrective measures as quickly as possible.

Phase	Purpose	Measures
Check the status of the servers in the service targeted by the disruption	The aim is to determine the cause of the disruption as accurately as possible. For instance, if there is a problem on a website, it may have been caused by a malfunction of one of the site's background servers. A denial-of-service attack may also cause one of the background applications to crash.	Ask the application server administrator to check the status of the application, the logs and the use of the server's resources. If there are any background services such as databases linked to the application, they should also be inspected separately.
Check the traffic of the service involved in the disruption in case of incidents and identify the type of attack	In many cases, a denial-of-service attack manifests in a clear growth of traffic volume. For this reason, the growth of traffic volume combined with the service not working may be a sign of a denial-of-service attack. It is also important to identify the type of denial-of-service attack to make combating it easier.	Check if the application logs have more received queries than normal, and where the queries have come from. A sudden increase in queries from foreign IP addresses, for instance, may be a sign of a denial-of-service attack. Today, most of the denial-of-service attacks are carried out by using the TCP SYN flood attack method. These attacks are more difficult to detect, because they are not visible in the network server logs. They can be detected in real time in the TCP connection list of the servers, however, based on the number of 'SYN RECV' rows being larger than normal. An application layer attack usually manifests as unusual HTTP queries in the web server log, or alternatively as an exceptionally large number of normal queries. This attack is the easiest to carry out technologically, but it also causes the least damage to the target. An amplified DNS attack is also visible as an increased number of HTTP queries in the log, but it causes much more damage compared to a normal application layer HTTP attack. The attacker implements it by sending several name servers DNS queries, in which the sender's address has been spoofed so that it appears to come from the organisation targeted in the attack. In that case, the servers return the response to the target of the attack, overloading it. You can identify the attack in logs based on HTTP responses that do not have a corresponding query.

Contact your IT/ICT service provider	Often a part of the organisation's IT infrastructure has been outsourced to a service provider. The harmful traffic almost always passes through the service provider's network, in which case the service provider is able to filter traffic if agreements on the issue have been drawn up in advance.	Report the incident to your IT or ICT service provider, depending on which service is the target of the attack. If the attack is volumetric, meaning that it is based on a large traffic volume, the service provider can help with stopping the attack by restricting the traffic to and from the service with a packet washer.
Notify the partners in cooperation and interest groups that may be affected by the incident about the information security breach	The security breach may cause the partners, customers and service providers risks or problems with the availability of services.	Notify the contact persons in case of crisis situations of different interest groups about the incident if you believe that it may affect the availability of their services. Also communicate about the incident internally, especially if the attack limits the availability of internal services, too.
Evaluate whether you need external help to handle the security breach or not	The organisation may need help with technical measures, managing the security breach and organising measures. If the necessary expertise is not available within the organisation itself or from the IT service providers used, you should consider getting external help.	Technical measures to handle the security breach may require external expertise. Such measures may include collecting identification information and investigating the threat based on it. The National Cyber Security Centre Finland can help organisations especially during the first response to the incident as well as by offering additional information on similar cases in Finland and abroad. You can find Finnish service providers in the resources listed in the footnote.[9]
Report the information security breach to the authorities	Report the security breach to the authorities. The organisation may have an obligation to report the security breach based on regulations or the cyber insurance.	File a report of an offence about the incident with the police.[10] Also notify the National Cyber Security Centre Finland[11] of the incident to maintain situation awareness and get help. The infrastructure operators and service providers critical to the security of supply must notify the authorities of any information security incidents in their networks and information systems.[12]

[9] https://dfir.fi/
https://www.fisc.fi/fi/about-us
https://www.hansel.fi/yhteishankinnat/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/ (in Finnish)

[10] https://poliisi.fi/en/report-a-crime

[11] https://www.kyberturvallisuuskeskus.fi/en/report

[12] https://www.kyberturvallisuuskeskus.fi/en/services/report-security-incident-nis-notification-obligation

4.3 Investigating an information security breach

Goals of the phase	The goal of investigating the security breach is to find out how the attack caused the disruption in the service and determine in this way how to protect the organisation from similar attacks in the future.

Phase	Purpose	Measures
Identify the targets of the attack	It is important to identify which part of the infrastructure was targeted by the denial-of-service attack. For example, in case of a network service, it is essential to find out if the attack focused directly on a website server or the network devices connected to it, for instance.	Check the log data of the server that was targeted in the attack. If it is a website server, the attack may be visible as an increased number of handshakes in the log. If there has been a TCP SYN flood attack or another lower level protocol attack, the investigation may be difficult without the help of the IT service provider.
Determine the type of attack	It is important to determine the type of attack so that the service can be protected better in the future. It may involve an application layer attack, such as HTTP, or a network layer protocol attack, such as TCP, or the attacker may have exploited a software vulnerability in the target.	If the attack was carried out by exploiting a vulnerability in the target, the target system must be updated to remove the vulnerability. If an application that the organisation has ordered from a third party is involved, the party that provided the application should be contacted to correct the vulnerability. In volumetric attacks, the most effective defence is traffic filtering by the IT or ICT service provider, which requires a separate agreement with the service provider. You can try to combat application layer protocol attacks independently, such as by restricting handshakes based on the IP address, domain name, the browser's user agent or the geolocation of the IP.
Save all logs related to the incident for later investigation	The aim of collecting and storing evidence is to guarantee a high-quality investigation after the incident so that the root causes of the incident can be determined. Evidence may be needed in connection with filing a report of an offence and for legal proceedings.	Save all log files with information relevant to the investigation of the security breach on a hard drive isolated from the network.

4.4 Recovery

Goals of the phase	Denial-of-service attacks last for less than 15 minutes on average, but sometimes they may drag on for several hours. The operation of the services is usually restored automatically after the attack.

Phase	Purpose	Measures
Check the different parts of the targeted service in case of a malfunction	The denial-of-service attack may have caused a malfunction in the targeted server or network device, which means that it is good to check that the servers and the applications that run on them operate normally.	Check the status of the targeted servers and network devices. Also check that the applications function normally.
Check that the software and configuration of servers are up to date	The denial-of-service attack may have exploited a vulnerability in an application or a server, which is why it is good to check that the server's updates are up to date.	Review the application versions of the server targeted in the attack and update them to a newer version, if necessary. Based on the application's logs, find out what kind of calls the application has received to determine which calls may have been used as a part of the attack.

5 Post-incident review of an information security breach

When the crisis is over and business operations have returned to normal, it is important to start the post-incident review of the attack and learn as much as possible about what happened for the future. At the same time, crisis management systems should be updated based on the observations made. The organisation may become a victim of a similar attack again, if the root causes of the incident cannot be determined and no lessons are learned from it.

During the post-incident review, the activities during the crisis are studied: what measures were done well, what could have been done better, and how the plans and the security level could be improved. A report should be drawn up on the post-incident review that examines at least the following questions in addition to the course of the events:

- Root causes of the incident:
    - What technical or functional weaknesses led to the situation?
- Effectiveness of the organisation's own protection:
    - Were the controls used to detect attacks sufficient?
    - Did the attacker's actions raise any alarms?
    - What was the reaction to the alarms like? Was the information about alarms transmitted to the right responsible persons?
- Actions during the crisis:
    - Was the crisis plan followed? How usable was it?
    - Were the responsibilities of the crisis management team assigned to the right people?
    - How successful was limiting the scope of the attack and removing the attacker?
    - How successful were the communications of the crisis management team? How were the interest groups taken into account?
- Recovery:
    - How did the recovery of critical information and services go?
- Post-incident review:
    - Have the course of events and the investigation work been documented?
    - Was the technical investigation of the incident sufficient? Has it been possible to submit sufficient data on the attack for the use of the authorities, for example?
    - Evaluate the actions of the service providers. Were the response time and the services that were agreed upon sufficient for the investigation of the incident?

The organisation should update its own incident response plan and more detailed playbooks designed for combating different types of security incidents after the fact. Practicing different scenarios at regular intervals is also recommended to ensure that you can benefit from them in crisis situations.

The National Cyber Security Centre Finland hopes that the companies and organisations share the most important lessons they have learned from the incident with the Centre, too. With incident reports, the National Cyber Security Centre Finland can help other organisations in Finland as well as internationally to investigate similar cases. The lessons learned from recovery help with developing the preparedness of all organisations.

Finnish Transport and Communications Agency
Traficom
National Cyber Security Centre Finland
PO Box 320, FI-00059 TRAFICOM
tel. +358 29 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-817-1

NATIONAL EMERGENCY SUPPLY AGENCY

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre