DENIAL OF SERVICE ATTACKS

Co-funded by the European Union

ESCAPE. *Preparing healthcare professionals for cyberattacks*
Project No.2023-1-ES01-KA220-VET-000151536

Partners

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS Weser

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

Co-funded by the European Union

FACTSHEET – DENIAL OF SERVICE ATTACKS

1. Definition

It is a malicious attempt to make a computer system, network, or service unavailable by sending too much traffic or asking for too many resources1. Effectiveness is determined by using vulnerable devices.

2. General importance

DoS attacks can block websites, financial platforms, government services, and more, leading to reputational and financial damage. Both defence mechanisms and malicious actors are improving their technical skills, leading to a tug-of-war that implies high damage costs due to the downtime recovery2.

The fact that these attacks can be carried out with little financial resources and technical expertise is concerning because they have serious repercussions. Because the means to execute such attacks are easily accessible, they are among the most prevalent types of cyber aggression.

3. Importance in health and care, and impact in quality of care

Specifically in the health and care sector, Denial of Service (DoS) attacks are critical, as they target the availability of digital systems2. Most of the patient's private information (treatment data, health records, etc.) is saved in electronic platforms, which can make this type of cyber aggression potentially life-threatening. If the attackers are successful, they may disrupt appointment scheduling, delay or prevent access to critical patient data, or even compromise emergency response systems, which could result in treatment delays and additional clinical risk3.

This situation has a significant impact on the quality of care. While in other sectors it may only result in financial damage, in healthcare it can undermine patients' trust in digital health services and even threaten human lives. For these reasons, digital resilience is an essential element in both cybersecurity and maintaining high-quality healthcare delivery5.

4. What can I do as a healthcare professional?

- Know how your company handles downtime so you can switch to manual backup procedures6.
- Report any possible threats immediately to the security team and prioritise effective, essential information storage5.
- Maintain clear and fluent communication with patients to maintain their trust in the healthcare system.
- Take part in cyber training and keep up with how to respond to incidents.

5. More information

5.1 Learning Materials

- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- An infographic on security and cybersecurity devices used in different healthcare settings. (IST-38)
- An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. (IST-39)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview (PRAMMER-33)
- A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia (PRAMMER-34)

5.2 Relevant Videos

This video clearly and simply explains how DoS (Denial of Service) attacks work. It says that a DoS attack tries to make a system unavailable, which is one of the most important parts of cybersecurity, by sending too many requests to servers or networks until they stop responding.

Denial of Service Attacks Explained
https://youtu.be/bDAY-oUP0DQ?si=uaHS8A80SwxLOaGc

5. 3 Relevant Links

This article says that a hacktivist group, thought to be Anonymous, launched multi-stage DDoS attacks against Boston Children's Hospital. These attacks could have affected the hospital's ISP-shared infrastructure and seven other nearby healthcare facilities. The attacks peaked at 28 Gbps and disrupted electronic prescription routing, departmental emails, and access to patient records. Boston Children's Hospital responded by activating its incident response team and utilising DDoS mitigation services.

https://www.radware.com/security/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study/?utm_source=chatgpt.com

According to this article, a broader analysis shows that DDoS attacks on healthcare increased significantly since 2016. Many hospitals were slow to find and respond to attacks, often only finding out about them after a long time had passed. This made people worried about the growing threat.

https://www.healthcareitnews.com/news/denial-service-attacks-healthcare-poised-explode#:~:text=A%20recent%20Neustar%20report%20found,attacks%20than%20its%20global%20counderparts

6. Bibliography

Cloudflare. (s. f.). ¿Qué es un ataque DDoS?

https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/.com

Lella, I., Theocharidou, M., Tsekmezoglou, E., Naydenov, R. S., Ciobanu, C., & Malatras, A. (2022). ENISA Threat Landscape 2022: July 2021 to July 2022. Enisa, 43-49.

https://doi.org/10.2824/764318

Denial of Service (DoS) guidance. (s. f.).

https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

Health. (s. f.). OECD. Recuperado 26 de agosto de 2025, de

https://www.oecd.org/en/topics/chronic-diseases.html

Data privacy and security. (2025). NHS England.

https://digital.nhs.uk/services/networks-and-connectivity-transformation-frontline-capabilities/connectivity-hub/advice-and-guidance/mobile-backup-solutions-for-fixed-healthcare-sites/business-continuity

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.