ATTACCHI DENIAL OF SERVICE (ATTACCHI DOS)

Co-funded by the European Union

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

Partner

INSTITUTO DE EDUCACION SECUNDARIA
JAVIERGARCIATELLEZ

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAXXER

eolas

BBS Weser

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

Co-funded by
the European Union

Questo progetto è stato co-finanziato con il supporto della Commissione Europea. Questa pubblicazione [comunicazione] riflette solo le opinioni dell'autore, e la Commissione non può essere ritenuta responsabile per l'uso che possa essere fatto delle informazioni ivi contenute.

CC BY NC

Indice

Co-funded by the European Union

FACTSHEET - ATTACCHI DENIAL OF SERVICE (ATTACCHI DOS)

1. Definizione

Si tratta di un tentativo dannoso di rendere indisponibile un sistema informatico, una rete o un servizio inviando troppo traffico o richiedendo troppe risorse. L'efficacia è determinata dall'utilizzo di dispositivi vulnerabili.

2. Rilevanza generale

Gli attacchi DoS possono bloccare siti web, piattaforme finanziarie, servizi governativi e altro ancora, causando danni reputazionali e finanziari. Sia i meccanismi di difesa che gli autori di attacchi stanno migliorando le proprie competenze tecniche, dando vita a un braccio di ferro che implica elevati costi per i danni dovuti al ripristino in caso di inattività.

Il fatto che questi attacchi possano essere eseguiti con scarse risorse finanziarie e competenze tecniche è preoccupante, perché hanno gravi ripercussioni. Poiché i mezzi per eseguirli sono facilmente accessibili, sono tra le forme di aggressione informatica più diffuse.

3. Importanza nella salute e nell'assistenza e impatto sulla qualità dell'assistenza

In particolare nel settore sanitario e assistenziale, gli attacchi Denial of Service (DoS) sono critici, poiché prendono di mira la disponibilità dei sistemi digitali. La maggior parte delle informazioni private dei pazienti (dati relativi alle cure, cartelle cliniche, ecc.) è salvata su piattaforme elettroniche, il che può rendere questo tipo di aggressione informatica potenzialmente letale. Se gli aggressori hanno successo, possono interrompere la pianificazione degli appuntamenti, ritardare o impedire l'accesso a dati critici dei pazienti o persino compromettere i sistemi di risposta alle emergenze, con conseguenti ritardi nelle cure e ulteriori rischi clinici.

Questa situazione ha un impatto significativo sulla qualità dell'assistenza. Mentre in altri settori può comportare solo danni finanziari, nel settore sanitario può minare la fiducia dei pazienti nei servizi sanitari digitali e persino mettere a repentaglio vite umane. Per questi motivi, la resilienza digitale è un elemento essenziale sia per la sicurezza informatica che per il mantenimento di un'assistenza sanitaria di alta qualità.

4. Cosa posso fare come professionista sanitario?

- Scopri come la tua azienda gestisce i tempi di inattività, così puoi passare a procedure di backup manuali.
- Segnalare immediatamente al team di sicurezza qualsiasi possibile minaccia e dare priorità all'archiviazione efficace ed essenziale delle informazioni.
- Mantenere una comunicazione chiara e fluida con i pazienti per preservare la loro fiducia nel sistema sanitario.
- Partecipa alla formazione informatica e resta aggiornato su come rispondere agli incidenti.

5. Ulteriori informazioni

5.1 Materiali didattici

- 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 Video correlati

Questo video spiega in modo chiaro e semplice come funzionano gli attacchi DoS (Denial of Service). L'obiettivo di un attacco DoS è rendere un sistema non disponibile, uno degli aspetti più importanti della sicurezza informatica, inviando troppe richieste a server o reti finché non smettono di rispondere.

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

5.3 Link rilevanti

Questo articolo afferma che un gruppo di hacktivisti, presumibilmente Anonymous, ha lanciato attacchi DDoS in più fasi contro il Boston Children's Hospital. Questi attacchi avrebbero potuto colpire l'infrastruttura condivisa dall'ISP dell'ospedale e altre sette strutture sanitarie vicine. Gli attacchi hanno raggiunto un picco di 28 Gbps e hanno interrotto l'inoltro delle prescrizioni elettroniche, le email dei reparti e l'accesso alle cartelle cliniche dei pazienti. Il Boston Children's Hospital ha risposto attivando il proprio team di risposta agli incidenti e utilizzando servizi di mitigazione DDoS.
https://www.radware.com/security/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study/?utm_source=chatgpt.com

Secondo questo articolo, un'analisi più ampia mostra che gli attacchi DDoS nel settore sanitario sono aumentati significativamente dal 2016. Molti ospedali sono stati lenti a individuare e rispondere agli attacchi, spesso venendone a conoscenza solo dopo molto tempo. Questo ha fatto sì che le persone si preoccupassero della crescente minaccia.
https://www.healthcareitnews.com/news/denial-service-attacks-healthcare-poised-explode#:~:text=A%20recent%20Neustar%20report%20found,attacks%20than%20its%20global%20counderparts

6. Bibliografia

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

Questo progetto è stato co-finanziato con il supporto della Commissione Europea. Questa pubblicazione [comunicazione] riflette solo le opinioni dell'autore, e la Commissione non può essere ritenuta responsabile per l'uso che possa essere fatto delle informazioni ivi contenute.

CC BY NC