RANSOMWARE

Co-funded by
the European Union

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

Socios

ESCAPE. Preparación de profesionales sanitarios ante ciberataques. Proyecto n.° 2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente la opinión del autor, y la Comisión no se responsabiliza del uso que pueda hacerse de la información que contiene.

Tabla de contenido

Co-funded by the European Union

FACTSHEET – RANSOMWARE

1. Definición

Es un tipo de malware que cifra archivos y los hace inaccesibles. Para restaurarlos, los atacantes exigen un rescate a cambio de descifrarlos. Algunas acciones pueden incluir el bloqueo total del equipo, el robo de datos, el cifrado o la eliminación, o la amenaza de filtrar toda la información robada.

2. Importancia general

El ransomware causa graves interrupciones operativas al provocar tiempos de inactividad, pérdidas financieras, daños a la reputación e insatisfacción del cliente, entre otros. Se trata de un ciberdelito lucrativo que pone en peligro la vida de los pacientes. Además, el coste global del ransomware es enorme y puede paralizar operaciones críticas en la fabricación, las cadenas de suministro, la distribución de energía o los servicios públicos.

Los atacantes han mejorado sus métodos utilizando la doble y triple extorsión: no sólo cifran los datos, sino que también amenazan con filtrarlos o atacar a sus socios3.

3. Importancia en el ámbito de la salud e impacto en la calidad de los cuidados

La atención médica depende principalmente de sistemas digitales para los registros, diagnósticos y tratamientos de los pacientes. El ransomware puede incapacitar las plataformas de atención médica, lo que provoca consecuencias trágicas como un aumento de casos de emergencia[2] (incluidos accidentes cerebrovasculares y paros cardíacos), retrasos en los resultados de laboratorio y la suspensión de diagnósticos y tratamientos.

Fuentes como Microsoft4 citan las siguientes consecuencias de los ataques de ransomware ocurridos en cuatro hospitales, dos atacados y dos no atacados:

Aumento de casos de ictus.
Aumento de paros cardíacos.
Disminución de la supervivencia con resultados neurológicos favorables.
Aumenta llegada de ambulancias.
El volumen de pacientes aumenta.
Interrupciones adicionales en la atención,

Esto afecta directamente la calidad de la atención. Las cancelaciones de tratamientos y procedimientos, junto con la reducción del acceso a datos críticos de los pacientes, son algunos ejemplos. Además, los flujos de trabajo manuales y en papel son propensos a errores, menos seguros y aumentan el estrés del personal.

Los incidentes reales demuestran que el ransomware puede aumentar las tasas de mortalidad hospitalaria en las zonas afectadas por ataques6.

4. ¿Qué puedo hacer como profesional sanitario?

Tome medidas preventivas como usar contraseñas seguras, mantener el software actualizado, habilitar la autenticación de dos factores, etc.

Evite compartir detalles de inicio de sesión en dispositivos no seguros y tenga cuidado al compartir información confidencial entre colegas.

Esté alerta a las amenazas cibernéticas (correos electrónicos de phishing, enlaces sospechosos) e informe inmediatamente cualquier irregularidad.

- Participe en la capacitación cibernética y manténgase actualizado sobre cómo responder ante incidentes.

5. Más información

5.1 Materiales de aprendizaje

- Cybersecurity for your sector (JGT-1)
- Sequential videos for general topics about cybersecurity (JGT-2)
- Web seminars about key aspects of cibersecurity (JGT-3)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- Interactive learning environment to develop cybersecurity skills. Requires national identification (JGT-9)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. (IST-39)
- Educational project on safe and responsible digital use. (IST-41)
- 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 Vídeos relevantes

Este vídeo explica qué son los ataques de ransomware, cómo comienzan, cómo afectan a las empresas, cuánto cuestan, qué industrias corren mayor riesgo y qué medidas se pueden tomar para evitarlos.

What a Real Ransomware Attack Looks Like
https://youtu.be/jl8K0VJraX4?si=XQBMPv4PAOAWwpVB

El siguiente vídeo nos muestra formas reales en que las personas pueden protegerse del ransomware.

Protecting Yourself from Ransomware
https://youtu.be/eizn9TC68E8?si=iMeXQ_AZAs0_lFzb

5. 3 Enlaces relevantes

This article talks about a real-life case in which a ransomware attack caused St. Margaret's Health, a small, rural health system in Illinois, to go into a downward financial spiral. The attack made it impossible for the 44-bed Spring Valley hospital to recover after weeks of being down, so it had to close for good.

https://www.hipaajournal.com/ransomware-attack-key-factor-in-decision-to-close-rural-illinois-hospital/

According to the article, UC San Diego Health reported a phishing attack that took place between January 9 and 22, 2024. This attack compromised the email accounts of two employees, putting sensitive patient information at risk for 1,642 people.

https://www.hipaajournal.com/march-13-2023-healthcare-data-breaches/

The article talks about how a ransomware attack on Ascension Health in May 2024 messed up operations across its hospital network, forcing manual patient record-keeping, ambulance diversions, and clinical delays. In the end, about 5.6 million patient records were compromised.

https://www.hipaajournal.com/ascension-cyberattack-2024/#:~:text=The%20May%202024%20ransomware%20attack,paper%20to%20record%20patient%20information.

The Change Healthcare ransomware attack shows how weak the U.S. healthcare system is overall. It caused huge financial losses, made it hard for providers to do their jobs, and showed how badly the whole sector needs to be more cyber-resilient.

https://www.csoonline.com/article/3484304/the-cyber-assault-on-healthcare-what-the-change-healthcare-breach-reveals.html

6. Bibliografía

National Cyber Security Centre. (s. f.). A guide to ransomware.

https://www.ncsc.gov.uk/ransomware/home

Reed, J. (2025, 31 marzo). When ransomware kills attacks on healthcare facilities. IBM.

https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities?utm_source=chatgpt.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

US healthcare at risk: Strengthening resiliency against ransomware attacks. (s. f.). Microsoft Security. Recuperado 1 de agosto de 2025, de

https://www.microsoft.com/en-us/security/security-insider/threat-landscape/us-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks?utm_source=chatgpt.com

Burgess, M. (2024, 24 June). Red tape is making hospital ransomware attacks worse. WIRED.

https://www.wired.com/story/ransomware-health-care-assurance-letters/?utm_source=chatgp.com

Freed, A. M. (2025, 27 febrero). Top Factors that Put Healthcare Sector at Risk from Ransomware Attacks. Halcyon.

https://www.halcyon.ai/blog/top-factors-that-put-healthcare-sector-at-risk-from-ransomware-attacks?utm_source=chatgpt.com

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.

ESCAPE. Preparación de profesionales sanitarios ante ciberataques. Proyecto n.° 2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente la opinión del autor, y la Comisión no se responsabiliza del uso que pueda hacerse de la información que contiene.