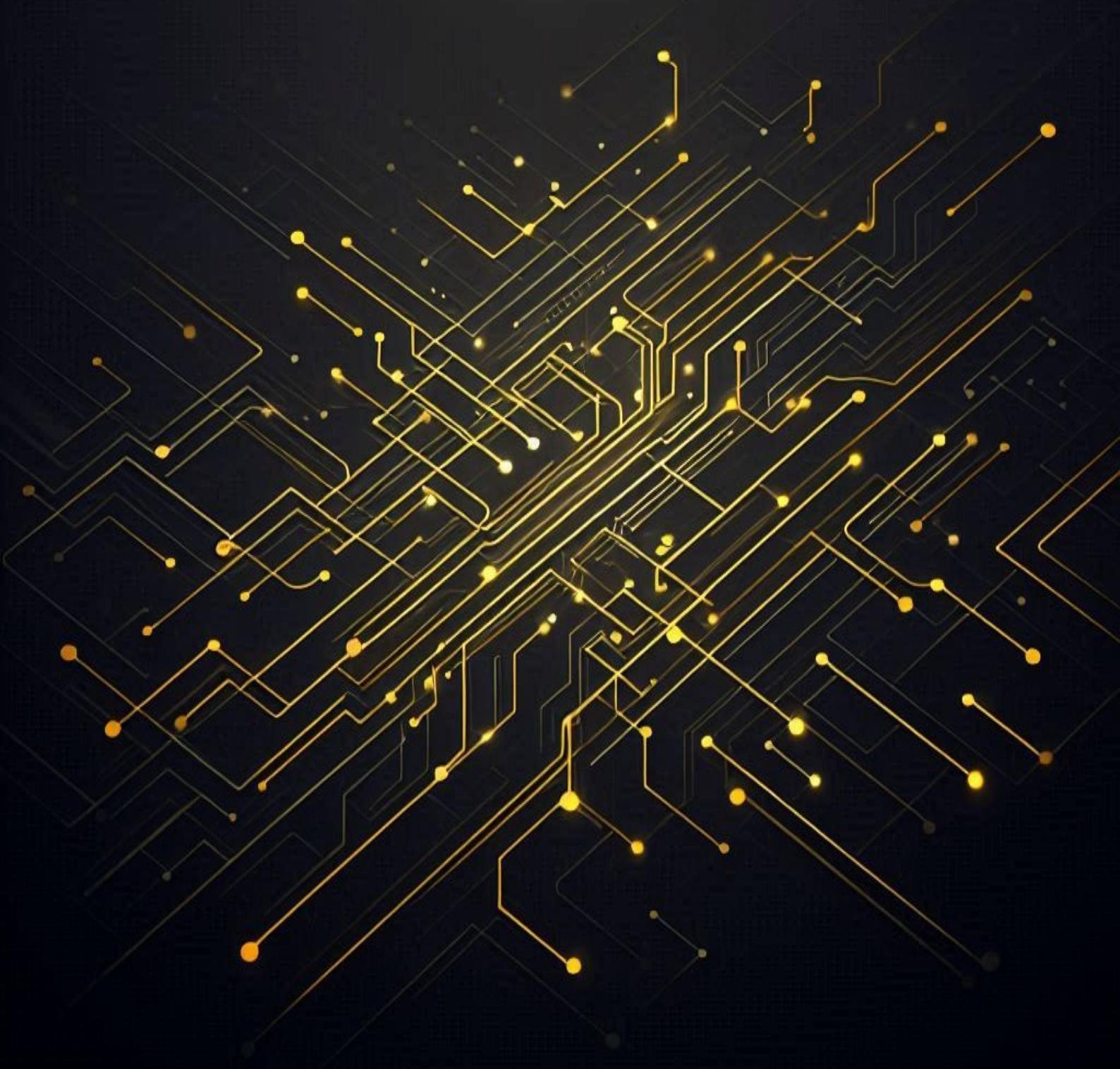


Ampliación de amenazas y análisis de ataques al Internet de las Cosas (IoT)



ENUNCIADO:

Tarea: Ampliación de amenazas y análisis de ataques al Internet de las Cosas (IoT)

Parte 2: Investigación de ataques al Internet de las Cosas (IoT)

Realiza una investigación sobre ataques recientes a dispositivos del Internet de las Cosas (IoT). **Encuentra noticias actuales que detallen incidentes de seguridad, brechas de privacidad o vulnerabilidades en dispositivos conectados como cámaras de seguridad, electrodomésticos inteligentes, automóviles conectados, etc.**

- Noticias y análisis: Describe los ataques más recientes, explica sus causas y consecuencias, y cómo afectan la seguridad del IoT.

Ataque hospital de Londres

<https://cnnespanol.cnn.com/2024/06/05/ciberataque-ransomware-interrumpio-atencion-pacientes-hospitales-londres-cancelaron-operaciones-trax>

El reciente ciberataque mediante ransomware que afectó a los hospitales de Londres interrumpió servicios médicos cruciales, cancelando operaciones y citas importantes, especialmente aquellas que dependían de transfusiones de sangre. El ataque se dirigió a Synnovis, una compañía que provee servicios de laboratorio para el NHS (Sistema Nacional de Salud), afectando el análisis de sangre y otros procedimientos vitales. Este incidente resalta la vulnerabilidad de los sistemas de salud ante las amenazas cibernéticas.

Causas

Los ataques de ransomware, como este, buscan extorsionar a las instituciones, en este caso paralizando sistemas críticos de salud para obtener rescates. La creciente digitalización de los servicios médicos y la falta de ciberseguridad adecuada en algunas áreas ha facilitado que los ciberdelincuentes aprovechen las debilidades de los sistemas de datos.

Consecuencias

Además de la interrupción de servicios médicos, se genera un gran riesgo para la privacidad de los pacientes, ya que los atacantes suelen filtrar datos sensibles. En el pasado, ha habido casos de muertes debido a retrasos médicos causados por ciberataques. A largo plazo, esto puede llevar a un mayor enfoque en la ciberseguridad médica y la implementación de medidas más estrictas.

Este ataque subraya la importancia de reforzar la seguridad en el Internet de las Cosas (IoT), ya que muchos dispositivos médicos están conectados a la red. Si no se mejora la protección, el IoT seguirá siendo un objetivo vulnerable que podría comprometer la seguridad y privacidad de los pacientes,

Ataque a la DGT

<https://www.motorpasion.com/seguridad/dgt-ha-sufrido-ciberataque-datos-personales-34-millones-conductores-sus-coches-podrian-ser-revelados>

La Dirección General de Tráfico (DGT) ha sido víctima de un ciberataque en el que se han comprometido los datos personales de 34 millones de conductores en España. Entre la información expuesta están las matrículas, modelos de coches y los datos de los titulares.

Causas

El ataque probablemente se aprovechó de vulnerabilidades en los sistemas de seguridad de la DGT. La creciente digitalización sin suficientes medidas de ciberseguridad hace que instituciones como la DGT sean objetivos fáciles para hackers.

Consecuencias

Los datos filtrados pueden ser utilizados para fraudes, suplantación de identidad o venta en mercados ilegales. Esto compromete la seguridad personal de los afectados, generando riesgo de robo o uso indebido de información.

Ataque para acceder a las cámaras de los usuarios

https://www.lespanol.com/sociedad/20240417/ciberataque-iniciado-cartagena-afecta-pareja-manteniendo-sexo-ayuntamientos-empresas/848415223_0.html

Un ciberataque iniciado en Cartagena ha afectado tanto a personas particulares, incluyendo a una pareja que fue grabada en un momento íntimo, como a ayuntamientos y empresas.

Causas

El ataque explotó vulnerabilidades en correos electrónicos y cámaras de seguridad. Los hackers accedieron a credenciales compartidas en diferentes plataformas, exponiendo datos y videos privados.

Consecuencias

Más de 200 personas podrían estar afectadas. Los datos robados podrían ser vendidos o utilizados para extorsión, afectando tanto a ciudadanos como a entidades públicas y privadas.