

POLICIA 
NACIONAL

Ingecom IGNITION 
An Exclusive Networks Company



**Ciberseguridad en infraestructuras
hospitalarias y electromedicina**
Javier Modúbar



**IV EDICIÓN CONGRESO SEGURIDAD
DIGITAL Y CIBERINTELIGENCIA**

Agenda

- Visión del riesgo cyber en el Sector Sanitario.
- Caso 1: Peligro de los coches inteligentes.
- Caso 2: DICOM el peligro de las imágenes.
- Caso 3: Lo que no vemos no existe.



Sólo hay **dos tipos de empresas**: Aquellas que han sido hackeadas y aquellas que lo serán. Incluso **están convergiendo en una única categoría**: las compañías que han sido hackeadas y que volveran a serlo de nuevo.”

Fuente: FBI Director Robert Muller, Keynote at RSA Conference 2012.



- Comprender al enemigo y la motivación detrás de un incidente de ciberseguridad o de un ataque dirigido es importante porque puede determinar qué busca un adversario.
- Conocer los motivos puede ayudar a las organizaciones a determinar y priorizar qué proteger y cómo protegerlo.
- Conocer los motivos proporciona una idea de las intenciones de los atacantes y ayuda a las entidades a centrar sus esfuerzos de defensa en el escenario de ataque más probable.

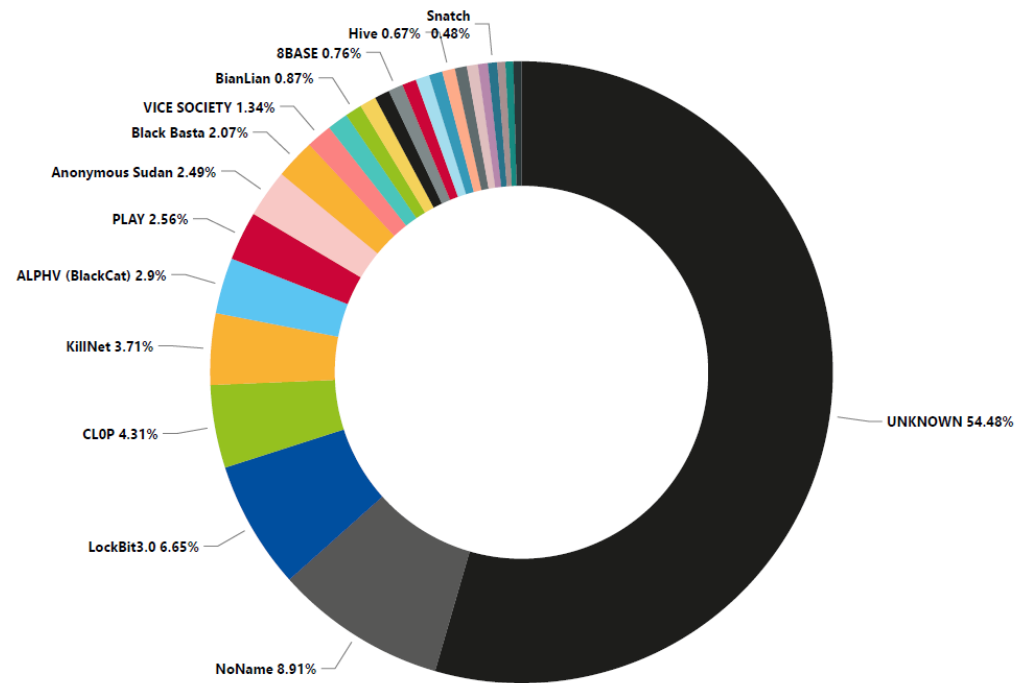


Clasificación de actores de amenazas

- No comprender a los actores de amenazas y cómo operan crea una importante brecha de conocimiento en ciberseguridad o no conocer los activos de uno.
- Analizar las amenazas sin considerar las motivaciones puede conducir a defensas ineficientes o, en algunos casos, a no poder proteger en absoluto.
 - Grupos sponsorizados por estados (APT).
 - Grupo de CyberCriminales.
 - Hacktivistas.
 - Insider.



Top actores de ataques



- Clasificación de Motivos:
 - Económicos.
 - Grupos de Ciberdelincuentes.
 - Espionaje.
 - Robo de propiedad Intelectual, datos confidenciales, sensibles (Grupo de ciberdelincuentes esponsorizados por estados)
 - Disrupción.
 - Acciones de carácter geopolítico ((Grupo de ciberdelincuentes esponsorizados por estados o servicios especializados de los estados APT).
 - Hacktivismo.
 - Tienen un carácter ideológico y puede ser realizado por personas individuales o grupo sin un fin económico



IT – (OT / IoT / IoMT)



INDUSTRIAL-SANIDAD

- No Visibilidad de activos.
- Protocolos Proprietarios.
Modbus RTU, EtherNet/IP, Ethernet TCP/IP, Modbus TCP/IP, Profinet, Profibus.
DICOM
- No segmentación.
- Imposibilidad de parcheo muchas veces.
- Fabricantes OT/Sanitarios.



De qué estamos hablando



Dispositivos vitales que se encuentran en los hospitales y que están conectados a una red de IT ya sea por cable o por radio, WIFI o 5G o protocolos de corto alcance como NFC o RFID.



Porque es necesario protegerlos

ALEMANIA

Muere una mujer después de un ataque informático a un hospital de Dusseldorf que no pudo atenderla

IRLANDA >

Un ciberataque obliga a Irlanda a cerrar el sistema informático de la sanidad pública

El bloqueo obliga a cancelar la mayoría de las citas, pero no afecta al plan de vacunación, según el Gobierno

An Illinois hospital is the first health care facility to link its closing to a ransomware attack

A ransomware attack hit SMP Health in 2021 and halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral.



HEALTH TECH

Idaho hospital diverts ambulances, turns to paper charting following cyberattack

By Annie Burky • Jun 1, 2023 04:00pm



Porque es necesario protegerlos

CIBERATAQUES >

Un ciberataque prácticamente paraliza el servicio de al menos tres hospitales catalanes: Moisès Broggi, Dos de Maig y Creu Roja de L'Hospitalet

CIBERDELINCUENCIA

Sacyl aborta un ciberataque dirigido a paralizar la actividad de los hospitales

El personal de informática evita la propagación del 'ransomware', un virus que secuestra datos

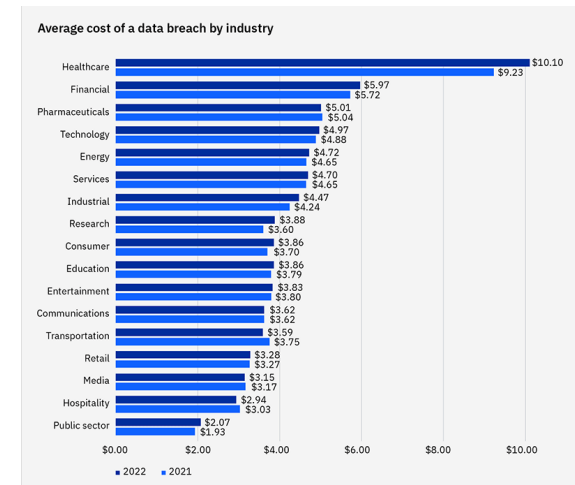
El Hospital Clínic de Barcelona sufre un ciberataque y desprograma visitas y cirugías mientras no se resuelva

Los ciberataques al sector sanitario se disparan un 650%














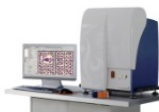




SALUD > Los sistemas llevan cuatro días inutilizados

Torrejón, primer hospital español 'secuestrado' por un virus informático

El Hospital de Torrejón, en Madrid, lleva desde el pasado viernes con sus sistemas informáticos bloqueados por lo que parece ser un virus de tipo 'ransomware'.
























Que nos deberíamos encontrar en una red médica IoMT

<p>11 Devices</p>  <p>1 Model 0 High Risk</p>	<p>73 Devices</p>  <p>2 Models 0 High Risk</p>	<p>66 Devices</p>  <p>1 Model 0 High Risk</p>	<p>8 Devices</p>  <p>2 Models 0 High Risk</p>	<p>4 Devices</p>  <p>1 Model 0 High Risk</p>	<p>2 Devices</p>  <p>1 Model 2 High Risk</p>
<p>C-Arm</p> <p>4 Devices</p>  <p>2 Models 0 High Risk</p>	<p>Central Station</p> <p>65 Devices</p>  <p>2 Models 0 High Risk</p>	<p>Chemistry Analyzer</p> <p>2 Devices</p>  <p>1 Model 0 High Risk</p>	<p>Computed Tomography</p> <p>5 Devices</p>  <p>4 Models 4 High Risk</p>	<p>Defibrillator</p> <p>21 Devices</p>  <p>2 Models 13 High Risk</p>	<p>Densitometer</p> <p>3 Devices</p>  <p>1 Model 0 High Risk</p>
<p>Diagnostic Workstation</p> <p>5 Devices</p>  <p>1 Model 0 High Risk</p>	<p>Digital Cell Morphology</p> <p>5 Devices</p>  <p>1 Model 0 High Risk</p>	<p>ECG</p> <p>63 Devices</p>  <p>2 Models 0 High Risk</p>	<p>Fecal Analyzer</p> <p>4 Devices</p>  <p>1 Model 0 High Risk</p>	<p>Glucose Meter</p> <p>265 Devices</p>  <p>1 Model 0 High Risk</p>	<p>Hematology Analyzer</p> <p>4 Devices</p>  <p>2 Models 0 High Risk</p>



Que nos encontramos:

<p>Printer 107 Devices</p>  <p>57 Models 36 High Risk</p>	<p>RTLS 309 Devices</p>  <p>3 Models 0 High Risk</p>	<p>RTU 95 Devices</p>  <p>1 Model 0 High Risk</p>	<p>Robotic Surgery System 3 Devices</p>  <p>2 Models 0 High Risk</p>	<p>Room Monitor 5 Devices</p>  <p>1 Model 0 High Risk</p>	<p>Router 4 Devices</p>  <p>2 Models 0 High Risk</p>	<p>Security Camera 26 Devices</p>  <p>11 Models 3 High Risk</p>
<p>Serial-to-Ethernet 8 Devices</p>  <p>0 Models 0 High Risk</p>	<p>Server 100 Devices</p>  <p>2 Models 0 High Risk</p>	<p>Smartphone 8,556 Devices</p>  <p>47 Models 104 High Risk</p>	<p>Tablet 315 Devices</p>  <p>6 Models 2 High Risk</p>	<p>Telemedicine 2 Devices</p>  <p>1 Model 0 High Risk</p>	<p>Telemetry Monitor 147 Devices</p>  <p>5 Models 0 High Risk</p>	<p>Temperature Sensor 14 Devices</p>  <p>2 Models 0 High Risk</p>
<p>Time Clock 15 Devices</p>  <p>1 Model 7 High Risk</p>	<p>UPS 7 Devices</p>  <p>2 Models 0 High Risk</p>	<p>Ultrasound 33 Devices</p>  <p>4 Models 4 High Risk</p>	<p>Vending Machine 1 Device</p>  <p>1 Model 0 High Risk</p>	<p>Ventilator 117 Devices</p>  <p>3 Models 0 High Risk</p>	<p>Video Conference 5 Devices</p>  <p>3 Models 0 High Risk</p>	<p>Vital Signs Monitor 333 Devices</p>  <p>1 Model 0 High Risk</p>



Caso 1: Presente.....




Más de 1.5 Millones de Teslas vendidos en 2022.

Más de 1.8 Millones de Teslas vendidos en 2023.

Fuente: <https://es.statista.com/estadisticas/609704/ventas-de-vehiculos-de-la-marca-tesla-en-el-mundo/>

Caso1: Tesla conectado a red Hospitalaria.




Device Information | Risk & Alerts | Vulnerabilities | Communication Map | Utilization | History




● Tesla | Tesla
RISK SCORE: MEDIUM (43.2)

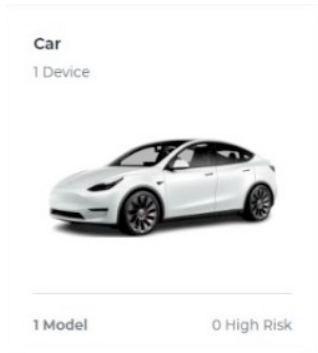
+ Add Note | + Add Labels | + Add Assignees | + Upload Device Security Files

DEVICE INFORMATION

Device IDs	IP  10.10.40.106 (Last known IP)	MAC 90:3A:E6:2D:EF:92	MAC OUI Parrot Sa	DEVICE ID FTIRHPM	CATEGORY IoT
	SUB CATEGORY General IoT	MANUFACTURER Tesla	TYPE Car	MODEL Tesla	MACHINE TYPE Physical
Versions & Names	OS Linux	OS NAME Linux 	DHCP FINGERPRINT udhcp 1.20.2		
Network	NETWORK Corporate	NETWORK SCOPE Default	VLAN Unknown	CONNECTION TYPE Ethernet 	IP ASSIGNMENT DHCP
	FIRST SEEN 11/05/2023, 12:39 pm	LAST SEEN 01/06/2023, 6:22 pm			
Network Security	AUTHENTICATION USER 903ae62def92				
Location	COLLECTION INTERFACES enp1s0f1@cun-main-collection-1, ...				

 Ayuda

Caso1: Tesla conectado a red Hospitalaria.



VULNERABILITIES

Showing 1 Vulnerabilities / 1 CVEs

Sorted by VULNERABILITY SEVERITY ASC

Export

VULNERABILITY NAME	VULNERABILITY TYPE	CVEs	CVSS V3 BASE SCORE	DESCRIPTION	MANUFACTURER REMEDIATION INFO	VULNERABILITY RELEVANCE	VULNERABILITY PRIORITY GROUP
CVE-2022-3602	Application	CVE-2022-3602	High (7.5)	A buffer overrun certificate verify constraint check	N/A	Potentially Relevant	Priority Group 1

About

Detects attempts at exploitation of CVE-2022-3602, a remote code execution vulnerability in OpenSSL v 3.0.0 through v.3.0.6

CVE-2022-3602 es una falla de seguridad que produce un desbordamiento arbitrario de búfer de la pila de 4 bytes que podría desencadenar bloqueos o provocar la ejecución remota de código (RCE)

Fuente: <https://nvd.nist.gov/vuln/detail/CVE-2022-3602>

Caso1: Tesla conectado a red Hospitalaria.



Los coches de Tesla entran dentro de lo que conocemos como **“coches conectados”**. Estos vehículos cuentan con una **conexión permanente a Internet**, la cual se realiza a través de la **misma red de datos que utilizamos en nuestros móviles**

Fuente: <https://www.adslzone.net/2018/01/29/como-funciona-internet-tesla/>

Caso 1: Futuro.... pero ya!!!!

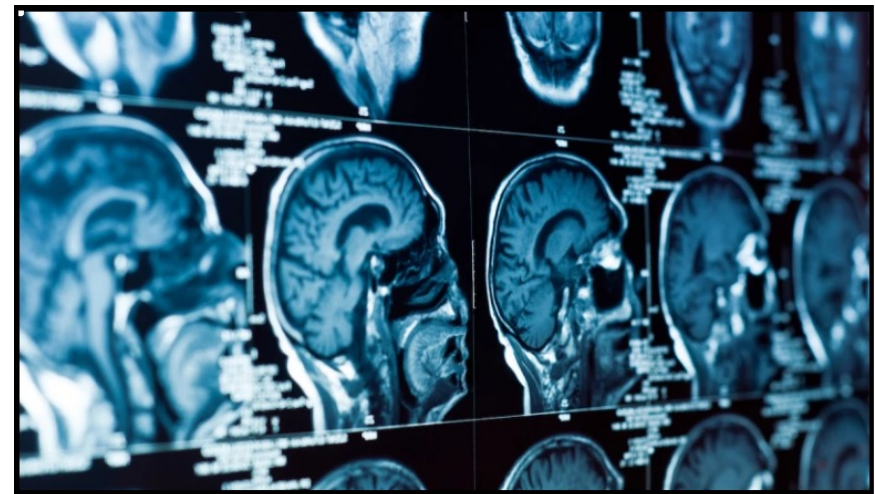
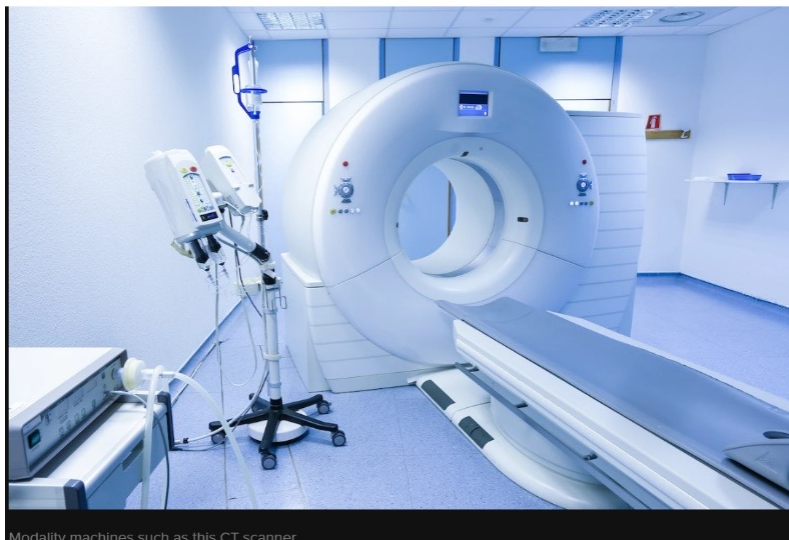


California aprueba servicios de taxi sin conductor, el principio del fin de la conducción- (2023)

Múltiples dispositivos con conexión a Internet.



Caso 2: Hackeo a protocolo DICOM



Caso 2: Hackeo a protocolo DICOM



A hacking incident involving data theft from a prominent provider of medical imaging services in Massachusetts has affected 2 million individuals, making it the largest health data breach reported to federal regulators so far this year.

Fuente: [Hack of Medical Imaging Provider Affects Data of 2 Million \(govinfosecurity.com\)](https://www.govinfosecurity.com)



Caso 2: Hackeo a protocolo DICOM

- ¿Alguna vez te han hecho una tomografía computarizada?
- ¿Qué tal una resonancia magnética o una ecografía?

Además de ser herramientas de diagnóstico críticas que proporcionan imágenes detalladas de nuestros órganos y huesos, esos escaneos tienen otra cosa en común: se comunican mediante el protocolo estándar **DICOM**.

Fuente: <https://claroty.com/team82>



DICOM (Digital Imaging and Communications in Medicine)

DICOM es el protocolo de red estándar y formato de datos para el almacenamiento y transferencia de imágenes médicas y datos de pacientes.

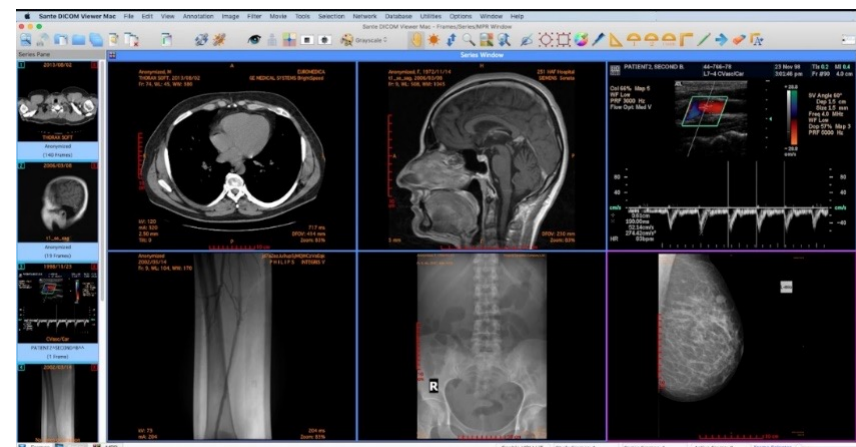
El estándar DICOM, utilizado en hospitales, clínicas y centros de radiología de todo el mundo, garantiza que los equipos de imágenes médicas puedan compartir, almacenar, transmitir, procesar y mostrar imágenes de modalidad médica de manera adecuada, independientemente del fabricante o la tecnología patentada involucrada

Dentro las imágenes médicas tomadas por las máquinas, junto con metadatos como información sobre el paciente (como nombre, sexo, edad, etc.), la prueba realizada (es decir, una exploración abdominal.), metadatos sobre el estudio (fecha del procedimiento) y más.



DICOM Viewer

- Los visores DICOM son el cliente que utilizan los profesionales médicos para analizar y examinar los resultados de las pruebas. Estos visores DICOM normalmente reciben o recuperan una muestra DICOM y muestran las imágenes y metadatos que guarda.



PACS

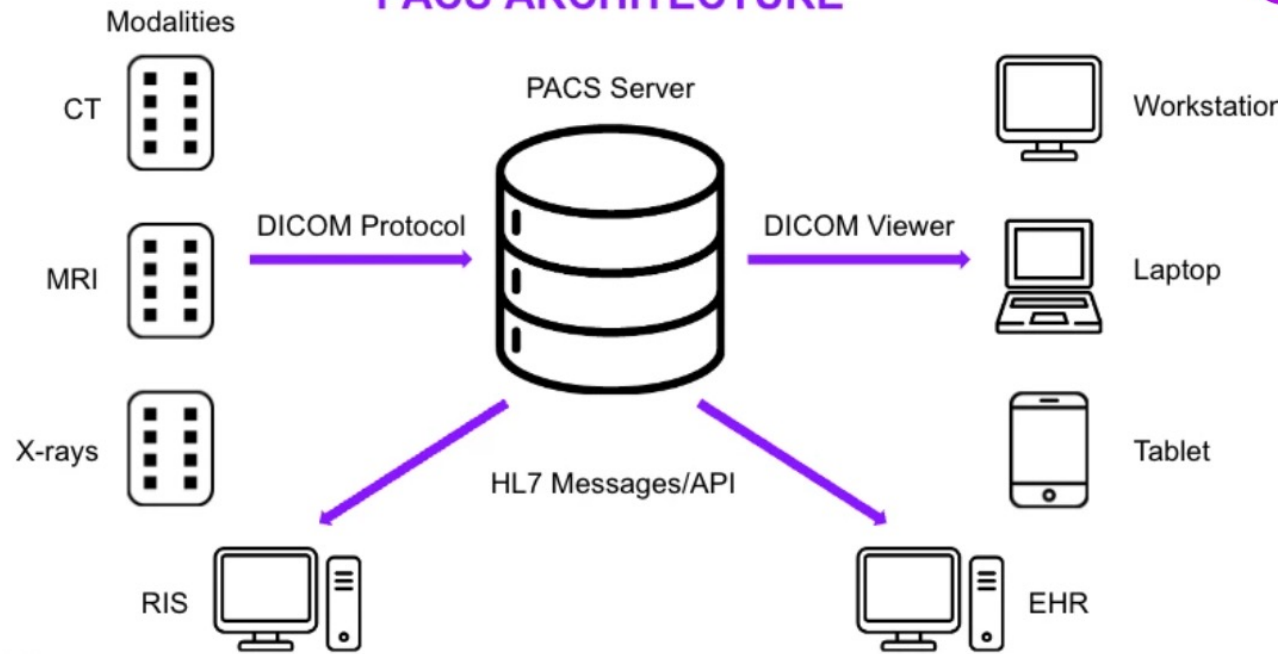
- En los hospitales modernos se utiliza una solución basada en red conocida como máquina del sistema de comunicación y archivo de imágenes (PACS).
- PACS actúa como una base de datos de estudios DICOM, lo que permite a los profesionales médicos conectarse a ella mediante un visor y buscar los estudios que elijan. En cierto sentido, el servidor PACS conecta las máquinas de modalidad que realizan los estudios a los visores DICOM, archivando las pruebas para su uso posterior.
- PACS contiene información de identificación personal (PII) confidencial.

Fuente: <https://www.hipaajournal.com/>



ARQUITECTURA

PACS ARCHITECTURE



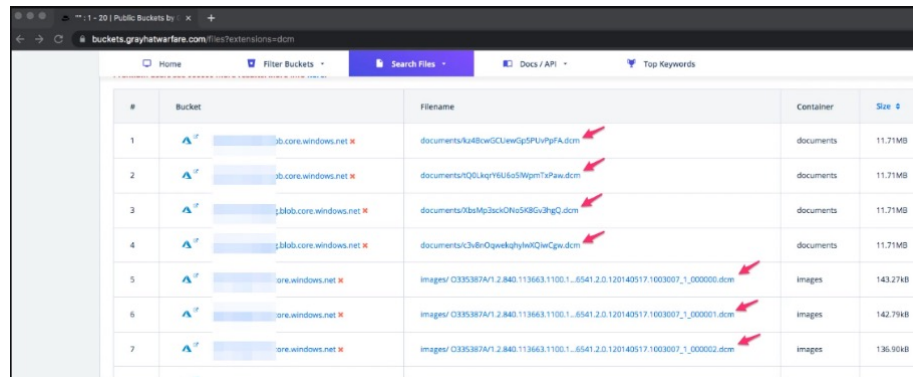
Representación de elementos DICOM

- Para comprender la superficie de ataque y el riesgo de las aplicaciones y dispositivos DICOM, debemos comprender cómo se estructuran e interpretan los elementos de datos en DICOM.
- Cada elemento de un estudio DICOM se compone
 - 1.-Una etiqueta
 - 2.-Una representación de valor (VR)
 - 3.- Datos en sí.



Seguridad en el Estándar DICOM

- Los servidores DICOM rara vez utilizan un protocolo de cifrado para su tráfico y, en cambio, envían información confidencial en formato plano.
 - Usar TLS sobre DICOM (Evitará este problema).
- Cloud.
 - Miles de ficheros accesibles para cualquiera que contienen millones de archivos DICOM expuestos que están al alcance de los cibercriminales con sufijo DICOM (.dcm).



#	Bucket	Filename	Container	Size
1	...b.core.windows.net	documents/kz48owGCLewQpSPUvPpFA.dcm	documents	11.71MB
2	...b.core.windows.net	documents!QQLkqrY6U6oS5WpmTspaw.dcm	documents	11.71MB
3	...blob.core.windows.net	documents!9baMp3acki0Nz5K8Gv3hgQ.dcm	documents	11.71MB
4	...blob.core.windows.net	documents!Ch8rQgvek4yhWQwCpW.dcm	documents	11.71MB
5	...ore.windows.net	images/!C335387A/1.2840.113663.1100.1..6541.2.0.120140517.1003007_1_000000.dcm	images	143.27KB
6	...ore.windows.net	images/!C335387A/1.2840.113663.1100.1..6541.2.0.120140517.1003007_1_000001.dcm	images	142.79KB
7	...ore.windows.net	images/!C335387A/1.2840.113663.1100.1..6541.2.0.120140517.1003007_1_000002.dcm	images	136.90KB

Utilidad: <https://buckets.grayhatwarfare.com/>



Seguridad en el Estándar DICOM

- Servidores PACS con acceso a Internet que debido a una mala configuración pueden dar acceso a información confidencial, existen actualmente más de 4000 servidores que almacenan datos confidenciales en formato DICOM expuestos.

```
SUVIDHA CABLE NET          DICOM Server Response
India, Mumbai              \x02\x00\x00\x00\x00\xb3\x00\x01\x00\x00ANY-SCP
medical

Gamma Telecom Limited      DICOM Server Response
United Kingdom, Edinburgh \x02\x00\x00\x00\x00\xb8\x00\x01\x00\x00ANY-SCP
medical

customer.sl.net.com.au    DICOM Server Response
SLNET Internet Services   \x02\x00\x00\x00\x00\xb8\x00\x01\x00\x00ANY-SCP
Australia, Melbourne
medical

135.97.140.34.bc.googleusercontent.com
Google LLC                 DICOM Server Response
                           \x02\x00\x00\x00\x00\xb8\x00\x01\x00\x00ANY-SCP

Shodan results showing DICOM servers that expose their services to the Internet.
```

Fuente: <https://www.shodan.io/>



Seguridad en el Estándar DICOM

- Vulnerabilidades sobre DICOM.

- Aplicaciones Médicas.

- MedDream
 - CVE-2023-40150
CVSS 9.8
 - Orthanc PACS.
 - Otras.



<https://claroty.com/team82/disclosure-dashboard/cve-2023-40150>

- Librerías/SDKs

- DCMTK
 - CVE-2022-2121
 - CVE-2022-2120
 - CVE-2022-2119
 - Dcm4chee, Pynetdicom, go-dicom

<https://claroty.com/team82/disclosure-dashboard/cve-2022-2121>

<https://claroty.com/team82/disclosure-dashboard/cve-2022-2120>

<https://claroty.com/team82/disclosure-dashboard/cve-2022-2119>

Fuente: <https://dicom.offis.de/dcmtk.php.en>



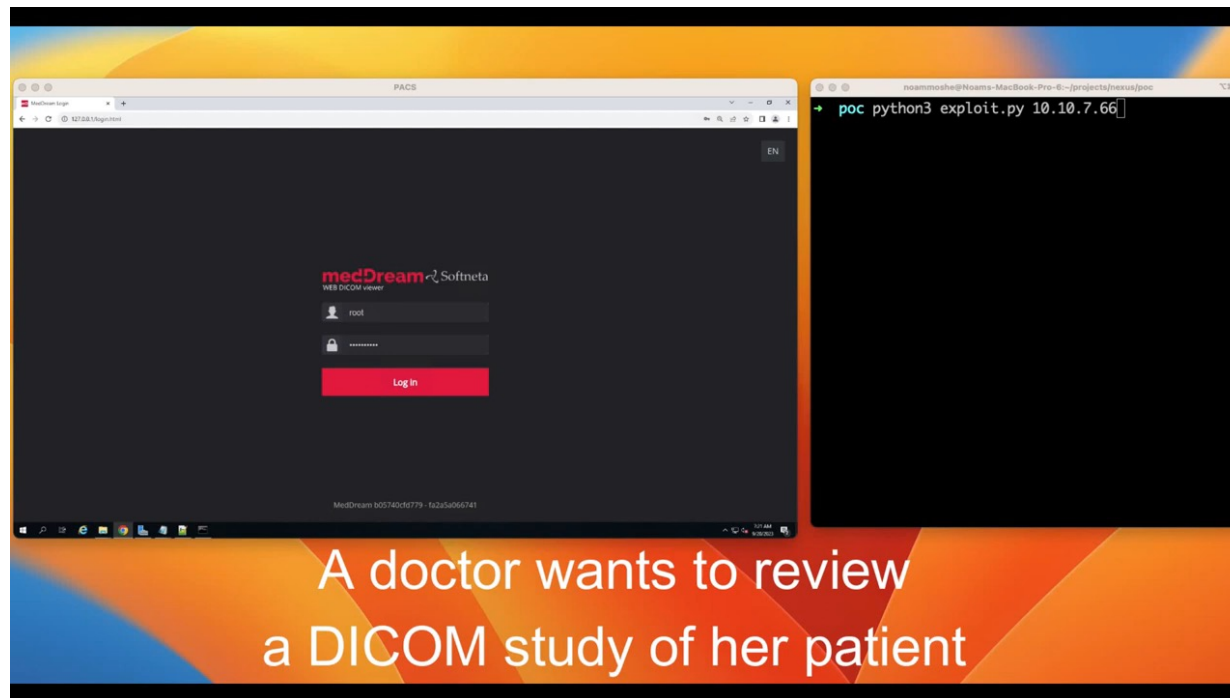
DICOM Attack

- Fase I: Definición
 - Una persona embarazada se somete a una prueba de ultrasonido, lo que permite a los médicos ver y evaluar la salud del feto.
 - El técnico de ultrasonido toma imágenes para que el médico realice su chequeo. Se crea un estudio DICOM que organiza toda la prueba en estudio, incluidas las imágenes, junto con la información del paciente y los metadatos generales. Luego, este estudio se almacena en una máquina PACS, lo que permite al médico conectarse con su visor y realizar el chequeo.
- Fase 2: Ataque.
 - Se ataca la máquina PACS para filtrar toda la base datos.
 - Al obtener el control total de la máquina PACS, los atacantes alteran algunos de los estudios DICOM, específicamente la prueba de ultrasonido de la persona embarazada. Los atacantes alteran las imágenes que tomó el técnico de ultrasonido y optan por agregar otro feto a la prueba de la mujer y obligan al médico a pensar que la persona embarazada tiene un par de gemelos. (CVE-2023-40150.)

<https://www.youtube.com/watch?v=xAPPRxk4MCE&t=10s>



DICOM Attack



Caso 3: Demo:





¡Muchas Gracias!

Javier Modúbar
jmodubar@ingecom.net

Ingecom IGNITION 
An Exclusive Networks Company

