Physical Demonstrator of Medical Imaging Unit: Threat Analysis and Protection Strategies in Cybersecurity

Marina Galiano Botella
CSIRT-CV
Valencia, Spain
csirtcv@gva.es

***Abstract*- Cyberattacks on healthcare systems are increasing. For this reason, there is a need to investigate and protect the operation of the technologies involved in healthcare facilities. One of the technologies with the greatest impact on healthcare has been diagnostic imaging. To cover this need for protection, a physical demonstrator of a Medical Imaging Unit has been developed, using the specific technologies of this system. In addition, abuse cases are specifically developed for this system. The purpose of this demonstrator is to help in the training on the operation and use of the technologies of a Medical Imaging Unit, to raise awareness among professionals and organizations, to determine the scope that an attack on the system could have and to generate measures to reduce or mitigate the impact.**

Keywords- health, cybersecurity, radiology, medical imaging.

I. INTRODUCTION

The use of Information Communications Technologies (ICTs) has become essential to meet the challenges faced by the healthcare system. In this sense, the use of some ICT tools such as electronic prescriptions or the Electronic Health Record has meant a great advance in the efficiency and effectiveness of the use of healthcare resources. Another technology that has led to a revolution due to its digitalization is diagnostic imaging.

In recent years, diagnostic imaging has advanced exponentially, becoming the focus of attention of engineers and scientists in order to improve medical imaging [1].

Healthcare systems are increasingly under attack by cybercriminals [2], [3]. Areas of hospitals that use these technologies can sometimes find themselves unprotected due to their rapid advancement and the increasing connectivity of devices to the Internet.

As shown in Fig. 1, during 2022, the healthcare sector was one of the most targeted. There are several reasons why the healthcare sector is targeted by cyberattackers. The first is that the information handled is highly sensitive and therefore offers great value to attackers. The second is the need to require the immediacy of the operation of the entire structure. A hospital cannot stop, since it has patients who need treatment, and whose lives depend on the uninterrupted operation of the hospital facilities. It is for this reason that many hospital systems are subject to computer attacks, such as ransomware (which involves encrypting and rendering computer systems unusable unless a ransom is paid). In such cases, hospital systems are forced to comply with ransom demands in order to continue operating.

A cyberattack on a hospital can have repercussions on the different systems and the usual operations of the facility. The attack can block the systems, making it impossible to access patients' medical records and forcing professionals to make medical reports manually. On the other hand, there are many consequences when the computer system is blocked, such as the cancellation of medical appointments, delays in surgical operations and the loss of electronic documents used by the hospital system such as procedures, among others.

Patient medical records are highly valuable on the dark web due to their comprehensive and sensitive information. This data, including personal, medical, and financial details, is used for identity theft, financial fraud, extortion, and healthcare scams. These records are targeted for their potential in both criminal activities and unauthorized research or commercial use.

In order to understand the scope of cyberattacks on healthcare environments, the objective is to develop a physical demonstrator of a medical environment. The medical environment will seek to represent a typical radiology or medical imaging unit of a hospital. This environment will realistically represent the delivery of medical images from a hospital. In addition, the mock-up of the environment will be

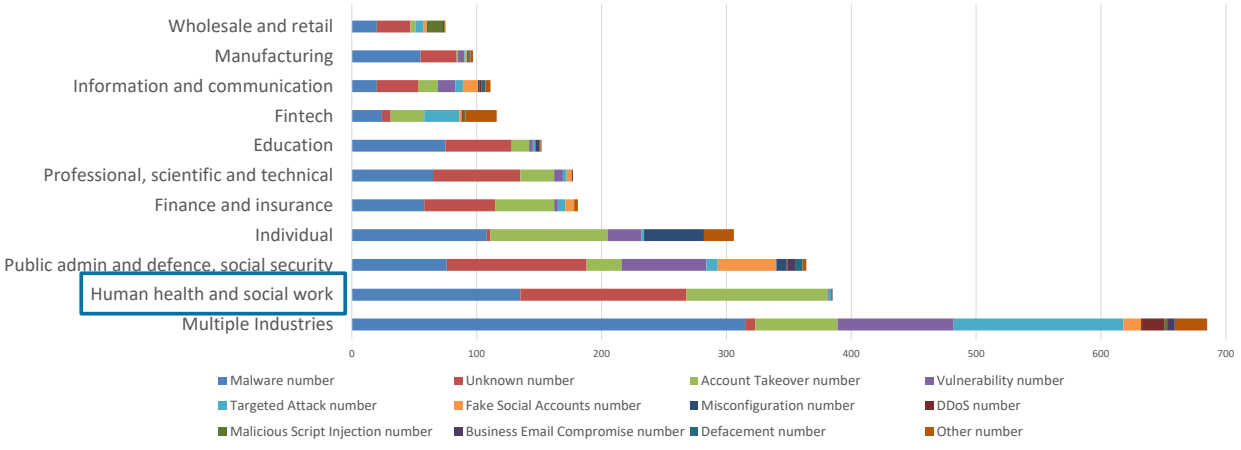

Fig. 1. Attacks by targets breakdowns in 2022 per sector. Data retrieved from [9].

 ISBN: 978-1-68558-089-6

done in such a way that it is as visual as possible when representing different abuse cases or attacks to the medical environment.

The simulation environment aims to investigate and analyze in depth the systems and threats that involve the hospital sector in the area of medical imaging, raise awareness among people and organizations involved in the health sector and test the different systems of the network of the Medical Imaging Unit, being able to determine the scope of the attacks and generate measures to reduce or mitigate the impact. For this purpose, during the project, several abuse cases will be developed, cyberattacks to the environment and its systems, to know the scope of these and use them in future awareness sessions.

The rest of the paper is structured as follows. In Section II, we present the devices that integrate the demonstrator, the defined architecture, and the cases of abuse to be developed. In Section III the results of the cases of abuse developed and launched are presented. Finally, we conclude our work in Section IV highlighting the most relevant aspects of the work performed.

II. MATERIALS AND METHODS

The Medical Imaging Unit environment developed represents 6 medical imaging rooms with 5 different techniques: 2 X-ray rooms, 1 Computerized Tomography (CT), 1 Magnetic Resonance Imaging (MRI), 1 mammography and 1 ultrasound. These imaging techniques are all simulated using PCs with Ubuntu 18.02 OS installed, except for the ultrasound scanner, for which the actual device is physically used, Chison ECO2.

The environment has been designed so that training and demonstrations can be carried out as visually as possible. For this reason, screens have been used to display the images that each modality would be taking in each room, in a simulated way. On the other hand, the modalities of each room have been 3D printed, as well as other decorative objects.

The environment uses the Digital Imaging and Communications in Medicine (DICOM) [4] standard for transmission, storage, retrieval, printing, processing and visualization of medical images and their information. It is used both as a storage format and as a transmission protocol for medical images.

The open source software used for the DICOM server is ORTHANC [5]. This software is used as the Picture Archiving and Communication System (PACS) of the environment. In addition, a PC with OS Windows 10 is used to perform consultations within the network, simulating that of a doctor's or radiologist's health practice. The architecture is shown in Fig. 2.

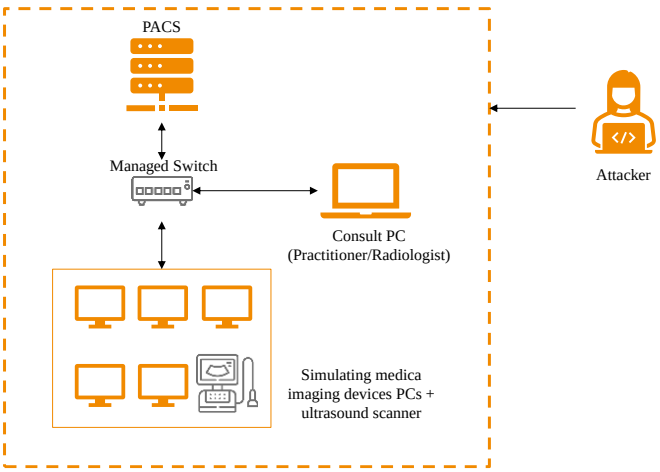

Fig. 2. Medical Imaging Unit environment architecture.

ORTHANC has been configured so that the consultation PC can access the PACS web server and upload and download images, delete patients and other default permissions.

In order to develop abuse cases in the Medical Imaging Unit physical demonstrator, the use of DICOM within the environment has been understood. The use of C-ECHO, C-STORE, C-MOVE, C-FIND and C-RETRIEVE has been studied in depth [6]. A specific configuration was performed in the environment when performing the abuse cases. The server configuration allowed C-ECHO, C-FIND and C-STORE from all devices within the network, while C-MOVE and C-RETRIEVE were only allowed for the specific asset simulating the radiography consultation equipment.

The abuse cases are developed in Python 3 using mostly the *pydicom* library for working with images in DICOM format [7]. The abuse cases should be launched from the radiologist's consulting PC, simulating that one of the radiologists' PCs has been compromised. However, depending on the network topology, these abuse cases could be launched from any network access point.

The proposed abuse cases are:

A. Convert an image to DICOM

The objective of the attack is to convert jpeg or png files into DICOM files so that a medical image can be replaced by the desired image and uploaded to PACS. There are multiple programs and libraries that can convert an image from a specific format to DICOM. In this case, the *Python-GDCM* library has been used [8].

B. Steganography in DICOM

The goal of the attack is to embed a message in a DICOM file in a hidden way so that it can be used as a means of communication between cyber attackers. For steganography of messages in a DICOM image, we focus on its metadata. DICOM has its own function which is to create private blocks to store patient information that has not been matched to any of the base fields of the DICOM metadata. Therefore, several private blocks are created, and the text is encrypted using Base64. The size of the image is not a limiting factor as these images are usually around 5MB in size.

C. Modify metadata

The objective of the attack is to acquire the image from the PACS, modify the metadata and replace it in the PACS. In this case, the original metadata is changed to that of another patient, potentially creating confusion for clinicians reviewing the patient, modality or clinician who performed the assessment.

D. DICOM image modification

The objective of the attack is to obtain a medical image from the PACS and modify the DICOM image by varying the pixels in such a way that it cannot be readable. In this way, we can darken the image or create areas with more brightness that may look like pathologies. We can also modify the image with another image, leaving the original metadata but completely modifying the image.

 ISBN: 978-1-68558-089-6

E. Exfiltration of information

The aim of the attack is to extract the medical images available in PACS in order to modify them and delete the original ones. In this way, the saved images of patients would not correspond to the original ones. In addition, these images are connected to patient data, and private health data can be obtained.

F. Export metadata

The aim of the attack is to obtain confidential patient information. To do this, all this data is stored in a local file.

The abuse cases are compiled into a single script that can be launched automatically, making it unnecessary for the attacker's technical knowledge to compromise hospital patient data.

III. RESULTS

The medical environment has been built taking into account that it must be a mobile unit, compact and easy to move without losing sight of the functionality of the environment, represented in a single module and with the capacity to integrate new modules. The visualization of the environment is shown in Fig. 3.

Therefore, the training and execution of attacks in the environment are more visual. In addition, when investigating the operation of the DICOM standard, tests can be performed without having to consider that the system shutdown may be critical or that the safety of any patient dependent on the operation of the devices may be involved.

The results obtained with the developed abuse cases are shown and discussed below.

A. Convert an image to DICOM

The image conversion is successful, but the DICOM file gets a unique identifier (UID) related to JPEG. When uploading the file to the DICOM server, the configuration of the server must be taken into account, since if it is not in promiscuous mode or does not accept these UIDs or image types, the upload may be rejected. Another alternative proposed is to modify the UID of the image created, pretending that it has been obtained from one of the modalities of the Medical Imaging Unit. This case of abuse is the beginning of most of the more developed cases, being essential in some occasions.

B. Steganography in DICOM

The private blocks have been created correctly and the Base64 encrypted message has been successfully included. The image has hardly suffered any variation in the image size as estimated, and in addition, the encrypted message is well camouflaged as there are several fields with numbers in the metadata that doctors do not usually check. On the other hand, more robust encryption could be used for future iterations or other steganography methods could be sought where the patient's image is involved instead of the metadata itself. These types of communications have been used by advanced persistent threat (APT) groups in social networks or other environments. They are not currently known to be used in healthcare settings, but it is a starting point to consider monitoring.

C. Modify metadata

Patient data can be changed for images previously downloaded from PACS. This may have an impact on the study not being found in common searches if the main search fields such as patient name or patient ID number have been modified.

D. DICOM image modification

Image modification using pixels can cause initial chaos for the radiologists who have to treat that image or for the physician who receives it this way post image processing. However, it could be easily reversible for a skilled technician. On the other hand, medical images could be exchanged between patients, leading to misdiagnosis by medical staff. However, the rise of AI also makes it increasingly difficult to distinguish real medical images from those generated by an algorithm. An example of substitution in the Medical Imaging Unit is shown in Fig. 4. This is one of the cases of abuse with the greatest impact both because of its visual nature and because it could lead to a real diagnosis, since the patient could be diagnosed with a pathology that he/she does not suffer from or even not be diagnosed with one that he/she does suffer from, putting his/her life at risk.

E. Exfiltration of information

This case of abuse is only possible if the compromised machine requesting it has permission to obtain such images, as is the case with a radiology station. However, proper network segmentation, or monitoring of strange or abundant requests, can help prevent this type of attack in a hospital environment. Cyberattackers sometimes get this information from patients along with their medical images in order to sell them on the

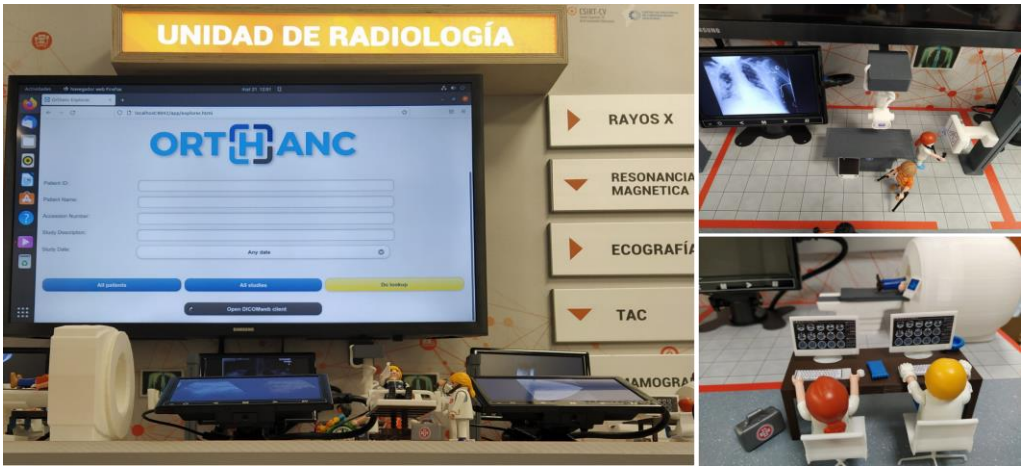

Fig. 3. Medical Imaging Unit Representation.

dark web. Proper segmentation, permissions management and monitoring of the DICOM standard could help prevent and detect this type of attack.

F. Export metadata

In the Medical Imaging Unit, this case could be executed from any point in the network since the only thing obtained was the patient data and not the image itself. An expert attacker could obtain them despite being a complex protocol. Segmentation and configuration of permissions on each device is essential to prevent this type of attack. In addition, monitoring the requests helps to detect them.

In many cases, the measures that are implemented or advised in hospital environments for the prevention and detection of these attacks are usually technical. Some of these countermeasures are:

- Use strong passwords.
- Encrypt DICOM communications.
- Perform periodic audits on medical network.
- Monitor DICOM requests and accesses through web interface.
- Network segmentation.
- Implement security measures as firewalls.

However, not all of them must be of this technical nature. It is crucial for cyberattack prevention to involve all staff and raise their awareness of cybersecurity. These countermeasures are based on awareness and training in cybersecurity, and of course, targeting this education to the healthcare sector. Raising awareness of the hospital's internal processes and the repercussions that misuse of systems can bring is indispensable. It is also very important to create security procedures to help implement these cybersecurity practices.

The development and construction of the Medical Imaging Unit, in addition to the creation of the abuse cases, helps to conduct more visual training sessions that reinforce this message.

The creation of the abuse cases has helped to gain a deeper understanding of the risks that can exist in a hospital, so that once they are known, they can be mitigated.

IV. CONCLUSIONS

The developed Medical Imaging Unit environment helps the different teams involved in cybersecurity to improve their knowledge of healthcare environments, as well as to test in a real simulated environment using the developed abuse cases. Attack teams can identify vulnerabilities and exploit them without risk of causing harm to either facilities or patients, while defense teams can monitor such actions. The execution of the abuse cases assists in the threat analysis of an attacker compromising an in-network system in a hospital with access to medical images of a hospital's patients. Finally, these abuse cases can be used in conferences, lectures, and trainings for cybersecurity awareness in healthcare environments, as well as to teach new professionals how to defend and attack such facilities for ethical purposes.

REFERENCES

[1] M. Desco and J. J. Vaquero, ‘Más de un siglo de imagen médica’ [in English: Over a century of medical imaging], Arbor, vol. CLXXVII, no. 698, pp. 337–364, Feb. 2004, doi: 10.3989/arbor.2004.i698.611.

[2] ‘Ciberataque al hospital Clínic de Barcelona | Hospital Clínic Barcelona’ [in English: Cyberattack to Barcelona’s Hospital Clinic], Clínic Barcelona. https://www.clinicbarcelona.org/prensa/ultima-hora/ciberataque-al-hospital-clinic-de-barcelona (accessed Mar. 23, 2023).

[3] E. Press, ‘Lockbit se disculpa por el ataque de ransomware a un hospital infantil y ofrece la herramienta para liberar los sistemas’ [in English: Lockbit apologises for ransomware attack on children's hospital, offers tool to free systems], Jan. 03, 2023. https://www.europapress.es/portaltic/ciberseguridad/noticia-lockbit-disculpa-ataque-ransomware-hospital-infantil-ofrece-herramienta-liberar-sistemas-20230103122550.html (accessed Mar. 23, 2023).

[4] ‘DICOM’. https://www.dicomstandard.org/ (accessed Feb. 28, 2022).

[5] ‘Orthanc - DICOM Server’. https://www.orthanc-server.com/ (accessed Mar. 23, 2023).

[6] ‘9.3 Protocol’, https://dicom.nema.org/dicom/2013/output/chtml/part07/sect_9.3.html, (accessed Mar. 23, 2023).

[7] ‘Pydicom |’, https://pydicom.github.io/ (accessed Sep. 01, 2023).

[8] ‘python-gdcm: Grassroots DICOM runtime libraries’, 2023, [MacOS, Microsoft: Windows, POSIX, Unix]. Available: https://github.com/tfmoraes/python-gdcm/ (accessed Sep. 01, 2023).

[9] ‘2022 Cyber Attacks Statistics – HACKMAGEDDON’, [Online]. Available: https://www.hackmageddon.com/2023/01/24/2022-cyber-attacks-statistics/ (accessed Nov. 06, 2023).

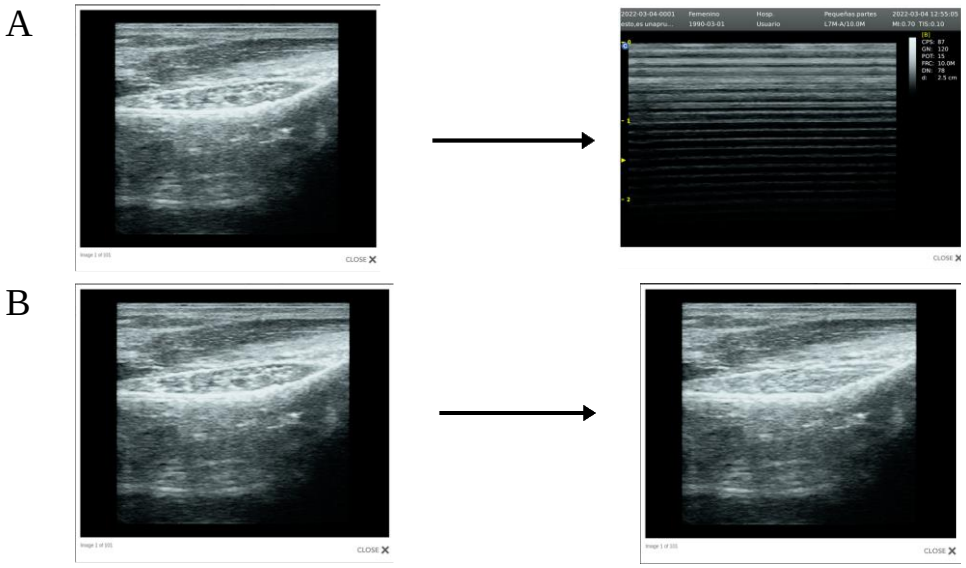

Fig. 4. Modification of a medical image. A. Image changed. B. Image modified by AI.