


# Cybersecurity nel Settore Sanitario Italiano: Esperienze sul Campo e Lezioni Apprese

Lorenzo Bracciale, Giuseppe Bianchi

CNIT Network Assessment, Assurance e Monitoring (NAM LAB)

1



## Cyberthreats on Italian medical landscape

### 2019 – Popular Insulin Pump



- ▶ This wireless RF communication protocol does not properly authentication
- ▶ An attacker can control insulin delivery

### The many Ransomware attacks

L'ATTACCO  
Pubblicati 8,3 GB di dati trafugati  
dall'ASL 1 Abruzzo, attaccata dal  
ransomware Monti

ATTACCO HACKER ASL L'A  
STAMPA: "NO PUBBLICAZI  
18 Maggio 2023 14:12  
L'AQUILA - CROCIACA



- ▶ Verona (2023), L'Aquila(2023), Basilicata (2024), Milano (2023) ...

What is the status of cyber-health of italian NHS?

Lorenzo Bracciale 2

2

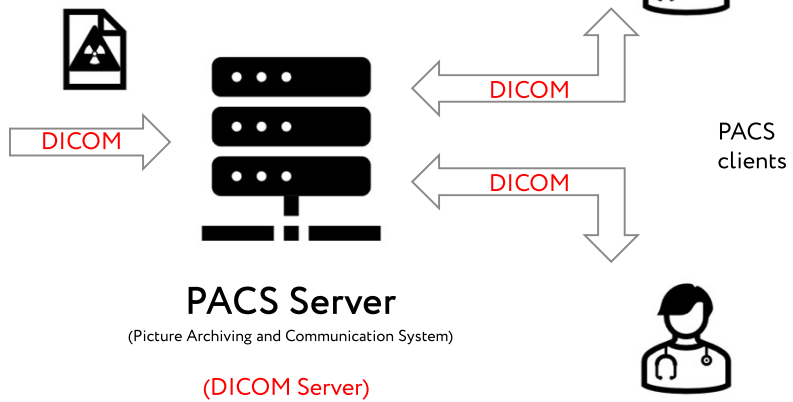
# 1. Exposed PACS

3

## Where your X-Ray goes?



X-ray, MRI, CT



4

SHODAN Maps

country:IT "DICOM Server Response" -tag:"honeypot"

Total Results: 55

Top Services

4242	27
11112	20
104	8

Top Organizations

UNI-Pavia	8
Aruba S.p.A. - Cloud...	6
Fastweb SPA	4
Universita' degli St...	4
Vodafone Italia S.p...	4

Lorenzo Bracciale

5

## What if some of them are left open?

DICOM Query/Retrieve

Retrieved	Name	AE Title	Address	Modality	# In	Date	Time	Source
				MR	783	08/01/24	13:27:02	
				MR	936	08/01/24	11:53:17	
				Cervical	28	10/01/24	12:53:09	
				Cervical	30	10/01/24	13:13:01	
				Cervical	376	10/01/24	13:29:07	
				MR	583	08/01/24	11:32:38	
				Cervical	628	09/01/24	15:56:26	
				Cervical	431	09/01/24	17:16:20	
1				Cervical	5	09/01/24	17:21:00	
2				Se T1 Scn	5	09/01/24	17:21:00	
3				Se T1 Scn	5	09/01/24	17:22:15	
4				Flu T2 Sag	9	09/01/24	17:29:00	
5				Flu T2 Tra	26	09/01/24	17:26:12	
6				3D Hyco T	366	09/01/24	17:43:50	
7				Fast Stone	17	09/01/24	17:49:35	
				MR	579	09/01/24	18:46:16	
				Neuroscop	804	08/01/24	13:46:52	

Realistic example

Lorenzo Bracciale

6



## 2. Medical Cloud Data

7

## Searching open buckets



The screenshot shows the Grayhat Warfare website interface. At the top, there are navigation links for 'Buckets' and 'Shorteners', along with 'Pricing', 'FAQ', and 'Contact Us'. A search bar and 'Login/Register' button are also present. Below the navigation, there are several service cards: 'Files' (2.7bn of 11.9bn), 'Amazon Web Services' (35.9k of 316.7k), 'Azure Blob Storage' (46.7k of 55.2k), 'Digital Ocean Spaces' (7.0k), 'Google Cloud Platform' (36.9k of 78.9k), and 'Last Update' (28 Mar 2024). The main section is titled 'Search Public Buckets' and includes a search form with fields for 'Keywords - Stopwords (start with minus -)', 'Filename Extensions (php, xlsx, docx, pdf)', and checkboxes for 'Full Path' and 'Treat as regex'. There are also 'Additional filters' and 'Random Files' buttons, and a 'Search' button at the bottom right.

8

# Searching for "medical report"

Results for "referto"



Save & notify | See corresponding API Call

Showing 1 - 20 out of 87 results

Premium users using this query see 142 more results. More info here.

#	Bucket	Container	Size	La
1	amazonaws.com		29.44kB	28
2	digitaloceanspaces.com	chat/attachments	1.64kB	10
3	digitaloceanspaces.com	chat/attachments	194.58kB	31
4	digitaloceanspaces.com	chat/attachments	164.17kB	31
5	digitaloceanspaces.com	chat/attachments	504.30kB	09
6	digitaloceanspaces.com	chat/attachments	31.29kB	16
7	digitaloceanspaces.com	chat/attachments	708.26kB	17



Lorenzo Bracciale

9

9

# Exposed medical report: example

LABORATORIO DI ANALISI CLINICHE

VIA G. POLIGNANO A MARE -

Nr. 7 ASL:ASL BA s.s.l. Bari 4

Data Nascita: Sig.

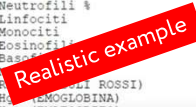
(ASL BA ) Pag. 1

Descrizione esame ESITO Data\* di misura Valori di riferimento

Profilo Analitico: Ematologia

EMOCROMO

WBC (GLOBULI BIANCHI)		R/μL	(4.0 - 11.0)
Linfociti %		%	(20.0 - 45.0)
Monociti %		%	(0.0 - 10.0)
Eosinofili %		%	(0.0 - 6.0)
Basofili %		%	(0.0 - 1.0)
Neutrofili %	7	%	(40.0 - 75.0)
Linfociti		R/μL	(1.5 - 4.0)
Monociti		R/μL	(0.0 - 0.8)
Eosinofili		R/μL	(0.0 - 0.4)
Basofili		R/μL	(0.0 - 0.1)
Emoglobina (Hb) (GLOBULI ROSSI)	2	M/μL	(4.50 - 6.50)
Hematocrito (Hct) (EMOGLOBINA)	1	g/dL	(13.0 - 18.0)
Hemoglobina (Hb) (EMATOCRITO)	1	%	(40.0 - 50.0)



Lorenzo Bracciale

10

10

# Searching for DICOM files



One million?????!!!

All files

★ Save & notify ▾ See corresponding API Call 🔊

Showing 1 - 20 out of 100000 results

Premium users using this query see 900000 more results. More info here.

#	Bucket	Filename	Container	Size	Last Modified
1	core.windows.net	wGp5PUvPpFA.dcm	documents	11.71MB	13-11-2019 18:57:34
2	core.windows.net	p5lWpmTxPaw.dcm	documents	11.71MB	27-11-2019 10:53:31
3	blob.core.windows.net	No5K8Gv3hgQ.dcm	documents	11.71MB	27-11-2019 10:59:32
4	blob.core.windows.net	ghylwXQwCgw.dcm	documents	11.71MB	27-11-2019 11:06:31
5	googleapis.com	r-930b-6bb4ade86a2c.dcm		4.57MB	09-06-2020 20:01:29

Lorenzo Bracciale

11

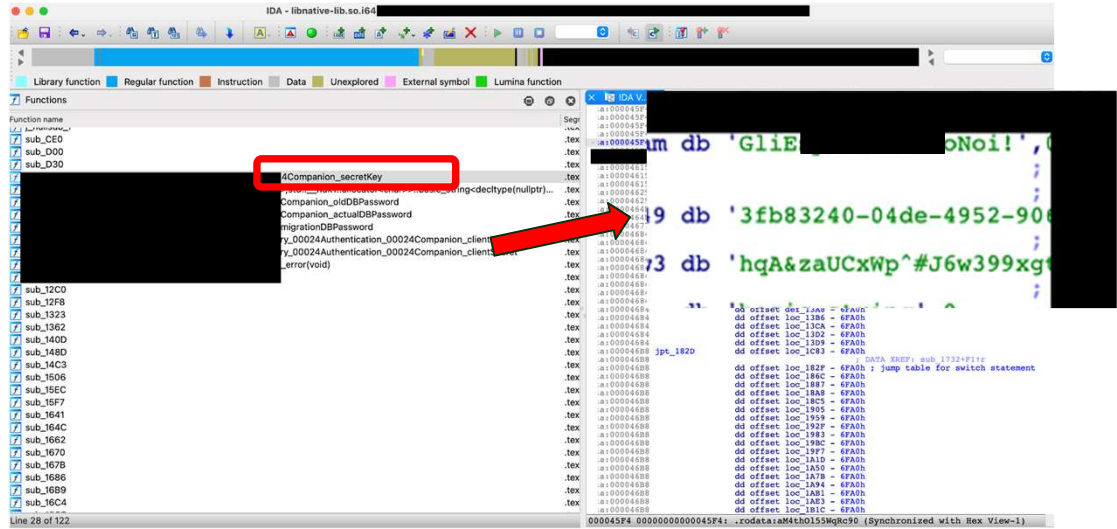
11

## 3. Medical Mobile Applications

12

12

# Hard-coded credentials



Lorenzo Bracciale

13

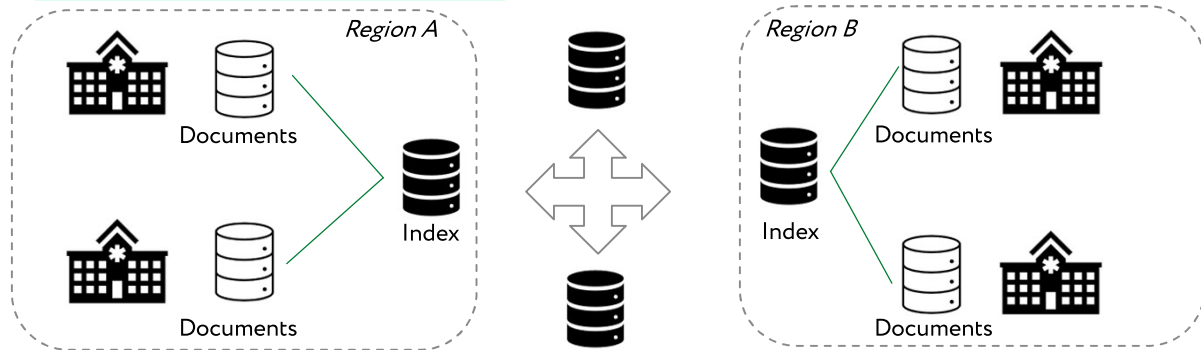
13

## 4. Electronic Health Records: A Tale of a Vulnerability

14

14

## Italian Electronic Health Record (EHR/FSE)



- ▶ Contains all YOUR medical records (and data). It is enabled by DEFAULT.
- ▶ A wide access control policy: doctors, hospitals, ASL, pharmacies
- ▶ 20 different implementation for (almost) the same service (!)
- ▶ Technical changes + rush: a perfect explosive cocktail!
  - ▶ Next Generation EU (PNRR): target 85% of Patient Summary data by 2025 (Mission 6).
  - ▶ FSE 2.0 (new architecture).

Lorenzo Bracciale

15

15

## User Data in EHR



*Ministero della Salute*



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri

### INTRODUZIONE

#### Definizione di Taccuino

Il DPCM 178/2015 definisce all'Art. 4 il "Taccuino personale dell'assistito" come sezione riservata del FSE all'interno della quale è permesso all'assistito di inserire dati e documenti personali relativi ai propri percorsi di cura, anche effettuati presso strutture al di fuori del SSN, precisando che i dati e i documenti inseriti nel taccuino sono informazioni non certificate e devono essere distinguibili da quelli inseriti dagli altri soggetti che concorrono all'alimentazione del FSE (definiti all'articolo 12 del medesimo Decreto).

Si tratta quindi di una sezione del FSE con caratteristiche profondamente differenti dalle altre, che debbono essere considerate nell'analisi dei contenuti informativi ed anche, in prospettiva, nella realizzazione dei servizi e nell'utilizzo delle informazioni ivi contenute.

Lorenzo Bracciale

16

16



# FSE – User Data



The screenshot shows the 'Elenco Documenti Caricati' page in the SALUTE LAZIO system. A red arrow points to the document list area. The interface includes a navigation menu, user profile, document upload options, and a calendar for June 2023. A sidebar on the right contains various notification and communication widgets.


17

# FSE – (distributed) Stored XSS




The screenshot shows a security warning dialog box over the SALUTE LAZIO interface. The warning message reads: 'www.salutelazio.it says Questo non e' sicuro'. A red arrow points to this message. Below the warning, a simple smiley face is visible on the page. A red box at the bottom of the slide contains the text: 'Serious Issue: spear fishing, massive data exfiltration, actions on behalf of the doctos, account takeover by password change?'.

18



## Aftermath

Responsible disclosure
Notification about a fix



7+ months

June 20, 2023
January 26, 2024

- ▶ **7 months vs 15 days** for "decisive interventions" (recent cybersecurity bill) – 12 march 2024
- ▶ Closed case? two major remaining concerns on our side
  - ▶ What about the 19 remaining ITA regions? All unaffected?
  - ▶ Is the fix robust?

12 marzo 2024

### Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici

In dettaglio, il **comma 1** prevede che l'Agenzia per la cybersicurezza nazionale (ACN) possa segnalare, ad una serie di soggetti pubblici o che forniscono servizi pubblici, **specifiche vulnerabilità cui essi risultano potenzialmente esposti**; inoltre prevede che i destinatari di tali segnalazioni devono provvedere senza ritardo, e comunque non oltre **15 giorni** dalla comunicazione, all'adozione degli **interventi risolutivi** indicati dalla stessa Agenzia.

Lorenzo Bracci

19



# TOR VERGATA

UNIVERSITÀ DEGLI STUDI DI ROMA

## Discussion & Suggestions

20

# Suggestions

## 1. Use recognisance tools to do active monitoring

Lorenzo Bracciale

21

21

### List of items purchased by Public Administration

oggetto_gara	oggetto_principale_contratto	importo_complessivo_gara	data_publicazione	data_scadenza_offerta	cf_amministrazione_appaltante	denominazione_amministrazione_appaltante
LAVORI DI SOSSIMA URGENZA RISANAMENTO CONSERVATIVO E BIRKOLIZIA LAVORI		1989970	27/09/2018	27/09/2018	805540799	AZIENDA SANITARIA PROVINCIALE DI CATANZARO
ACQUISTO FARMACO MODITE DEPOT DITTA BRISTOL MYERS SQUIBB SRL FORNITURE		7210,0	25/09/2018	09/10/2018	96024110635	ASL NAPOLI 2 NORD
ACQUISTO MONITOR		2000,0	28/09/2018	28/09/2018	763810587	FONDAZIONE ENASARCO
ACQUISIZIONE GARBA REGIONALE DRI 2ª EDIZIONE LOTTO 5 OCCHIALI AD ASTINE FORNITURE		6534,0	20/09/2018	20/09/2018	962051110	AZIENDA UNITA' SANITARIA LOCALE N. 5 SPEZZINO
AFFIDAMENTO FORNITURA PRODOTTI DI PULIZIA PER LASILO NIDO COMUNI FORNITURE		1000,0	14/09/2018	29/09/2018	627980827	COMUNE LERCARA FRIDDI
NOLOGGIO QUADRIMENSALE DI VEICOLI SENZA CONDUCENTE DA ASSEGNARE FORNITURE		34392,0	27/09/2018	27/09/2018	225930156	COMUNE DI SESTO SAN GIOVANNI
STAGE A DURINDO 18-19		1235000	20/09/2018	20/10/2018	9702000515	ISTITUTO TECNICO STATALE PER IL TURISMO ARTEMISIA GENTILESCHI
PROCEDURA RISTRETTA PER LA FORNITURA DI DEFLUSSORI - REGOLATORI D FORNITURE		577400,0	07/09/2018	09/08/2021	2101050546	AZIENDA OSPEDALIERA DI PERUGIA SANTA MARIA DELLA MISERICORDIA
MANUTENZIONE HARDWARE IBM SEDE CENTRALE (GARANZIA SUL SERVIZIO) SERVIZI		112000,0	17/09/2018	02/10/2018	8094380586	CONSIGLIO NAZIONALE DELLE RICERCHE
SERVIZIO DI BUSINESS INFORMATION PER LA VALUTAZIONE DELLA POSIZIONE SERVIZI		250000,0	10/09/2018	17/09/2018	617991028	ENEL ITALIA SPA
SERVIZIO DI PULIZIA ORDINARIA C/O LOCALI E LORO PERTINENZE SERVIZI		81402,0	14/09/2018	24/09/2018	193460680	COMUNE DI MONTESILVANO
PIANO DI INTERVENTO TRIENNALE DI NOLOGGIO MEZZI OPERATIVI PER LA S SERVIZI		300000,0	27/09/2018	21/11/2018	107990812	CITTA' METROPOLITANA DI TORINO
FORNITURA DI DISPOSITIVI PER STOMIE CATEREER SONDE VESICALI E ALTR FORNITURE		159158,68	11/09/2018	11/09/2018	166159091	AZIENDA SANITARIA PROVINCIALE DI SIRACUSA

Struttura ▼ Acquisito Dispositivo SPA

1. UNITA SANITARIA LOCALE ROMA MANUTENZIONE ED ASSISTENZA TECNICA ANGIOGRAFO INNOVA 2000 01/012014-30/04/2014 innova 2000 firmware BERICA

### CVEs of medical devices

1. EXECUTIVE SUMMARY
- CVSS v3 9.8
  - ATTENTION: Exploitable remotely/low skill level to exploit
  - Vendor: GE Healthcare
  - Equipment: GE Imaging and Ultrasound Products
  - Vulnerabilities: Unprotected Transport of Credentials, Exposure of Sensitive System Information to an Unauthorized Control Sphere



Maps of purchases of vulnerable medical devices

<https://www.nature.com/articles/s41598-023-45927-1> Lorenzo Bracciale

22

22

## Suggestions

1. Use recognisance tools to do active monitoring
2. Move from a prescriptive to supportive approach

## Do not dump the cyber sec problem on healthcare facilities



## Suggestions

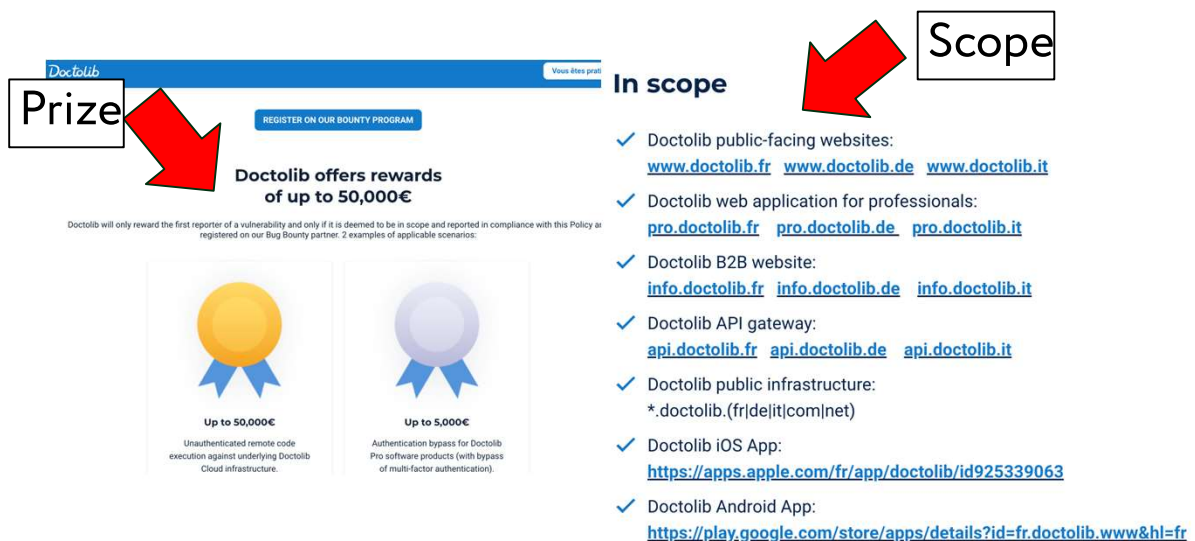
1. Use recognisance tools to do active monitoring
2. Move from a prescriptive to supportive approach
3. Use the community: bug bounty, open policies for bug reporting ecc.

Lorenzo Bracciale

25

25



## Best Practice: Doctolib (300k HCPs)



**Prize**

Doctolib offers rewards of up to 50,000€

Doctolib will only reward the first reporter of a vulnerability and only if it is deemed to be in scope and reported in compliance with this Policy as registered on our Bug Bounty partner. 2 examples of applicable scenarios:


-  **Up to 50,000€**  
Unauthenticated remote code execution against underlying Doctolib Cloud infrastructure.
-  **Up to 5,000€**  
Authentication bypass for Doctolib Pro software products (with bypass of multi-factor authentication).

**In scope**


- ✓ Doctolib public-facing websites: [www.doctolib.fr](http://www.doctolib.fr) [www.doctolib.de](http://www.doctolib.de) [www.doctolib.it](http://www.doctolib.it)
- ✓ Doctolib web application for professionals: [pro.doctolib.fr](http://pro.doctolib.fr) [pro.doctolib.de](http://pro.doctolib.de) [pro.doctolib.it](http://pro.doctolib.it)
- ✓ Doctolib B2B website: [info.doctolib.fr](http://info.doctolib.fr) [info.doctolib.de](http://info.doctolib.de) [info.doctolib.it](http://info.doctolib.it)
- ✓ Doctolib API gateway: [api.doctolib.fr](http://api.doctolib.fr) [api.doctolib.de](http://api.doctolib.de) [api.doctolib.it](http://api.doctolib.it)
- ✓ Doctolib public infrastructure: \*.doctolib.(fr|de|it|com|net)
- ✓ Doctolib iOS App: <https://apps.apple.com/fr/app/doctolib/id925339063>
- ✓ Doctolib Android App: <https://play.google.com/store/apps/details?id=fr.doctolib.www&hl=fr>

**Scope**

26



## Best Practice - WHO



Prize

### Vulnerability Hall of Fame

WHO is committed to protecting the privacy and security of its people, processes, and IT solutions. Our Vulnerability Hall of Fame is intended to minimize the risk and impact of cybersecurity vulnerabilities that hackers seek to exploit for malicious purposes.

**WHO responsible disclosure and reporter acknowledgment policy**

To continuously improve the protection of information technology and digital assets, we encourage the public to assist our efforts by disclosing cybersecurity vulnerabilities in WHO publicly accessible information systems.

**What to report to WHO (qualifying vulnerabilities)**

Technical details of cybersecurity vulnerabilities associated with publicly accessible WHO digital assets. We are open to accepting any valid in-scope vulnerability, but we are especially interested in the following vulnerabilities:

- OS Shell Execution (Remote Code Execution, Code Injection, OS Command Injection);
- SQL Injection (Inband SQLi, Blind SQLi);
- Server-Side Request Forgery (Unrestricted SSRF, Content-Restricted SSRF, Error-based SSRF (true/false), Blind SSRF);

**Related**

Cyber security

**News**

6 February 2024 | Departmental news  
**WHO reports outline responses to cyber-attacks on health care and the rise of disinformati...**

23 April 2020 | News release  
**WHO reports fivefold increase in cyber attacks, urges vigilance**

Scope

Prize

27



# TOR VERGATA

UNIVERSITÀ DEGLI STUDI DI ROMA



Lorenzo Bracciale

28