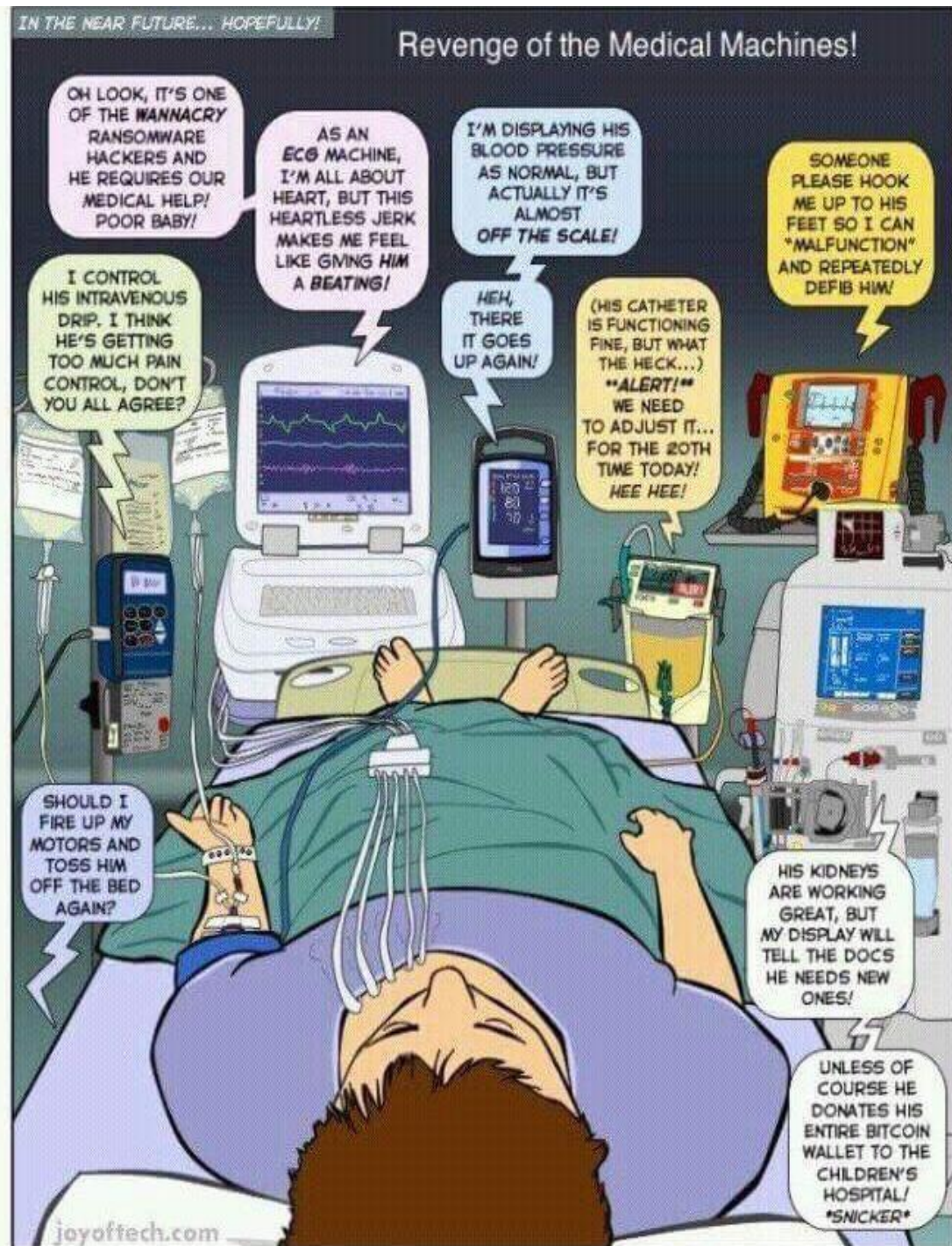




Securing Your Journey
to the Cloud

Healthcare Hacked

Mayra Rosario Fuentes/Numaan Huq
Forward Looking Threat Research (FTR)
Sr. Threat Researcher
mayra_rosario@trendmicro.com



Introduction

❖ Who Am I?

- ❖ Information Assurance (IA) – Booz Allen Hamilton
- ❖ 10 yrs. Cyber Intelligence Officer – US government
- ❖ Principal Intelligence Analyst – Symantec

❖ Interests

- ❖ Healthcare
- ❖ Russian & Arabic underground forums
- ❖ Deep Web
- ❖ Hacktivism
- ❖ Cybercrime



What are we going to cover?



- Overview of what devices are found in hospitals
- Hospital Breaches
- Exposed Medical Systems
- Supply Chain Threats



Devices found in Hospitals



What does an Operating Room look like?



Anesthesia machine **IV pump** Surgical and exam lights **Storage for medical supplies and equipment**
Ventilators Seating for medical staff **Sterilization and cleaning equipment** Disposables **Patient tables**
Robotic technologies **Surgical table and accessories** Air handling systems **Cameras** Stretchers
Lights and booms **Advance imaging equipment** flat screens



What does a Pharmacy look like?



What does a Patient Room look like?

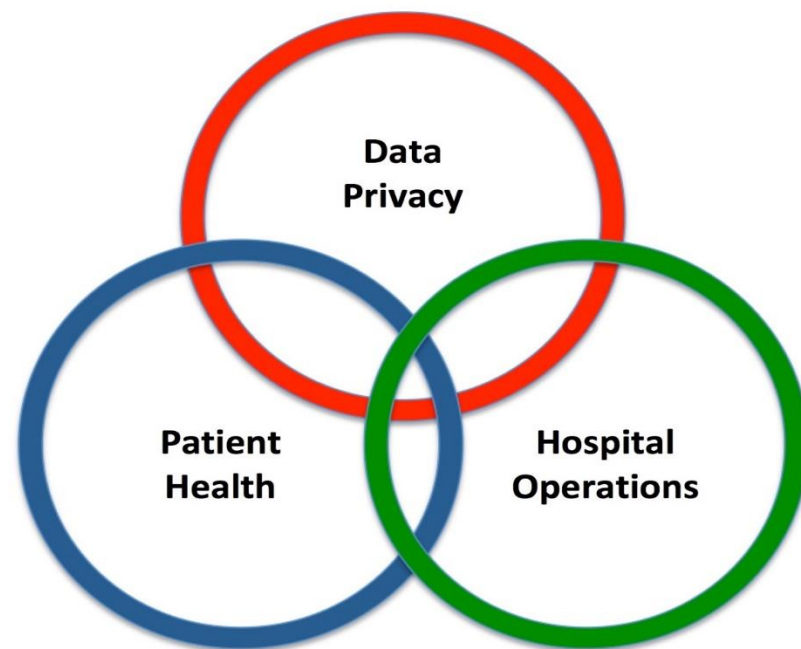


- Bar coding system
- Real-time monitors for vital statistics
- Individual rooms with HVAC controls and lightning systems
- Whiteboards
- Sofa beds
- Wifi availability
- Bed
- Chairs
- TVs
- Phones
- Compact storage space
- Restroom
- Hand washing station



Who is attacking Healthcare?

- Nation States
- Script Kiddies
- Cyber Terrorists
- Hacktivists
- Insider Threats
- Criminal Gangs



Ransom Data Theft Disruptive Attacks

How are they attacking the Healthcare industry?

Category	Devices & Systems
Medical Devices	<ul style="list-style-type: none">• Imaging e.g. MRI, CT, X-Ray, Ultrasound, etc.• Infusion pumps• Respiratory ventilators• Anesthesia machines• Heart-Lung machines• Dialysis machines• Robotic surgical tools• Radiotherapy systems• Active & passive monitoring systems
Information Systems	<ul style="list-style-type: none">• EHR/EMR systems• Laboratory information systems• Radiology information systems• Picture Archiving and Communication Systems (PACS)• Mobile health applications
Hospital Operations	<ul style="list-style-type: none">• Work order & staff scheduling systems• Office applications e.g. payroll, email, file servers, databases, etc.• Drug & equipment inventory systems• Hospital paging systems• Building control systems• Barcode scanners & printers• Automated drug dispensers• Pneumatic tube transport system

- Spear phishing
- Distributed Denial of Service (DDoS)
- Vulnerability exploitation
- Privilege Misuse
- Insider Threat
- Data Manipulation
- Malware
 - Ransomware
 - Keyloggers
 - Worms
 - Trojans
 - Rootkits




TheDarkOverlord

- Using TheDarkOverlord Solutions as of Sept 2017
- Summer of 2016 sold Healthcare databases ranging from \$100,000 – \$395,000 USD
- Hacked Netflix and released Orange is the New Black
- Aug 2017 through Oct 2017 hacked multiple healthcare organizations
- Extorts victims in exchange for not releasing the information on Pastebin or download site



TheRealDeal All I want to order ...

Home / Databases / Healthcare Database (48,000 Patients) from Farmington, Missouri, United States



Healthcare Database (48,000 Patients) from Farmington, Missouri, United States

By thedarkoverlord (100.0%) Level 1 (14)

0 10.0000 / BTC 10.0000
In stock.

Postage Option

Escrow Yes, escrow by RealDeal is available.
Class Digital
Ships From Worldwide

Qty: 0

Buy It Now

Favorite Question

Details Feedback Return Policy

Description

This product is a considerably large database in plaintext from a healthcare organization in Farmington, Missouri, United States. It was retrieved from a Microsoft Access database within their internal network using readily available plaintext usernames and passwords.

Format:
Record #,Pat.Act.#,Active,Last Name,First Name,MI,Suf.,Address Line 1,Address Line 2,City,State,Zip,SSN,DOB,Sex,Mar.,Stu.,Email,Home Phone,Work Phone,Cell Phone

Sample:
34441,344416,TRUE,Andrews,Amy,,1166 Newman Lake Rd.,Fredericktown,MO,63645,416043219,2/9/1970,F,D,N.,(573) 783-2800 ,C > - ,C


Statistics:
Total Records Count: 47,864
DOB 1890-1934: 5,650
DOB 1935-1989: 38,136
DOB 1990-1997: 2,783
DOB 1998-2015: 1,295

Ownership of this database will be exclusive and only a single copy will be sold. This has not been leaked anywhere and it has not yet been abused. If you are interested in purchasing this database and would like to make an offer other than what is listed, send a PM. Only serious offer s will be entertained.

Ships To
Worldwide

TheRealDeal All I want to order ...

Home / Databases / Healthcare Database (210,000 Patients) from Oklahoma City, Oklahoma, United States



Healthcare Database (210,000 Patients) from Oklahoma City, Oklahoma, United States

By thedarkoverlord (100.0%) Level 1 (14)

0 25.0000 / BTC 25.0000
In stock.

Postage Option

Escrow Yes, escrow by RealDeal is available.
Class Digital
Ships From Worldwide

Qty: 0

Buy It Now

Favorite Question

Details Feedback Return Policy

Description

This product is a very large database in plaintext from a healthcare organization in the Central/Midwest United States. It was retrieved from a severely misconfigured network using readily available plaintext usernames and passwords.

Format:
SSN,FIRST NAME,MI, LAST NAME,SEX,DOB,ADDRESS

Sample:
128-62-0328,MARLO,0,RIVERA,M,12/17/1977,301 SW 147TH ST OKLAHOMA CITY OK 73170


Statistics:
Total Records Count: 207,572
DOB 1890-1934: 39,412
DOB 1935-1989: 135,387
DOB 1990-1997: 18,396
DOB 1998-2015: 14,377

Ownership of this database will be exclusive and only a single copy will be sold. This has not been leaked anywhere and it has not yet been abused. If you are interested in purchasing this database and would like to make an offer other than what is listed, send a PM. Only serious offer s will be entertained.

Ships To
Worldwide

TheRealDeal All I want to order ...

Home / Databases / Healthcare Organization (24,000 Patients) Fairview, Illinois, United States



Healthcare Organization (24,000 Patients) Fairview, Illinois, United States

By thedarkoverlord (100.0%) Level 1 (14)

0 35.0000 / BTC 35.0000
In stock.

Postage Option

Escrow Yes, escrow by RealDeal is available.
Class Digital
Ships From Worldwide

Qty: 0

Buy It Now

Favorite Question

Details Feedback Return Policy

Description

This product is a fairly large database in plaintext from a healthcare organization in the state of Illinois and the city of Fairview. It was retrieved from an accessible internal network using account credentials that were garnered through the token impersonation of an employee. First stage access was accomplished using RDP 0day.

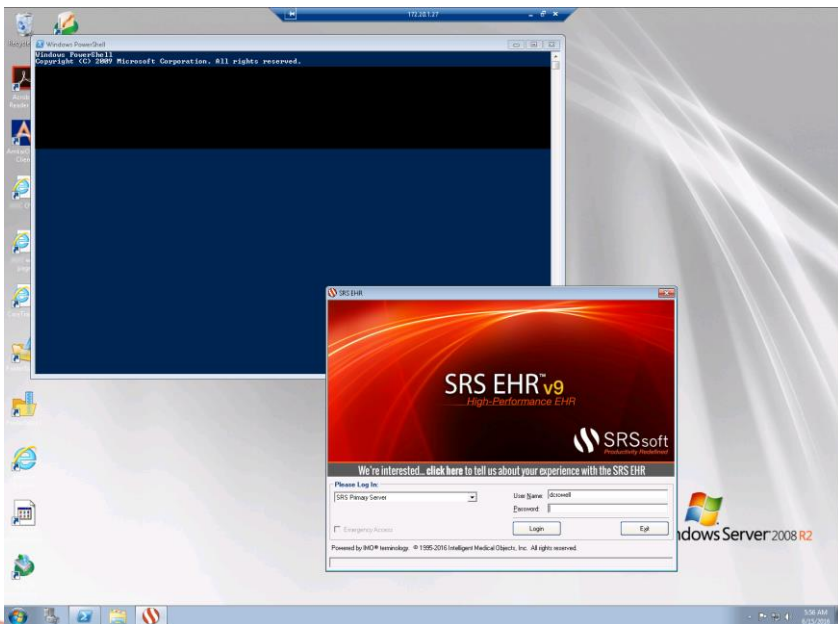
Format:
PatID,FirstName,LastName,Sex,Addr1,Addr2,City,State,Zip,HomePhone,WorkPhone,Email,LastApptDate,LastVisit Type,NextApptDate,NextVisitType,LastDOB,FollowUpDate,BirthDate,Ins,InsID1,InsID2,RefPhysCode,First,Last,Title,LastPract,LastBase,LastTotal

Sample:
"15900","Joseph","Amodi","475-13-9770","1106 Piper Ln","Mascoutah","IL","62258","618-486-5294","618-256-8128","na","09/28/2010","DELFO",,"09/28/2010","05/07/1971","TRIEM","475130770","POET","Charles","Portwood","DC","08","13818","361.6","6312","Steven","Abbink Sr.,"318-68-2970","147 Boskydell Dr.,"Collinsville","IL","62234","618-570-8734","618-228-8630","Frybryd200319818yeh on.com","05/18/2012","DELFO",,"05/30/2012","08/31/2003","TRIEM","318682970","SIMMONS","GREGORY","SIMMONS","MD","JPL","L1846","1785.42","12410","Teresa","Abner","320-46-6217","485 Dartmouth Dr.,"O'Fallon","IL","62269","618-624-6638","618-541-8282","abner1@charter.net","02/18/2016","DELFO",,"02/18/2016","01/16/1949","MCARE","320466217A","DUGAN","Christopher","DPM","EG","A5500","358.29"

Statistics:
Total Records Count: 23,565
File size is 5MB
Insurance Information is available

Ownership of this database will be exclusive and only a single copy will be sold. This has not been leaked anywhere and it has not yet been abused. If you are interested in purchasing this database and would like to make an offer other than what is listed, send a PM. Only serious offer s will be entertained.

Ships To
Worldwide



Patient Summary Form Confirmation Page PCN Number: [REDACTED]

>> Patient Information

Last Name: [REDACTED] First Name: [REDACTED] Sex: M DOB: [REDACTED]
Address: [REDACTED] City: Round Rock State: TX Zip: [REDACTED]
ID#: [REDACTED] Health Plan: [REDACTED] Navigate

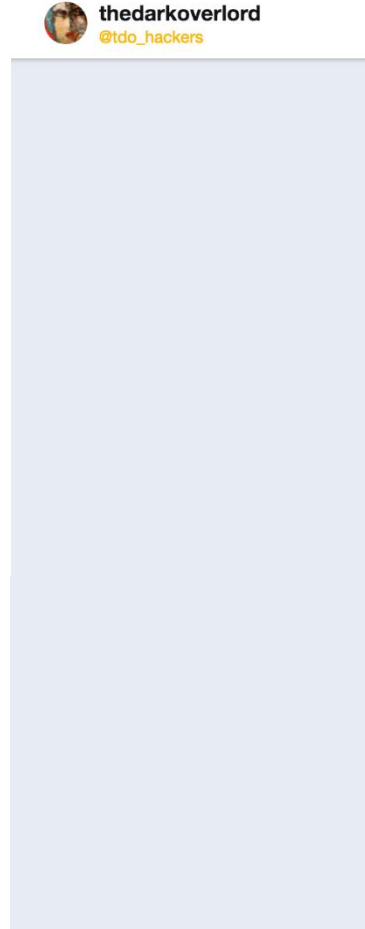
>> Provider Information

Austin Manual Therapy Associates, PT Office Location: 3508 Far West Blvd Ste 240, Austin TX
Credentials: PT

>> Provider Completes This Section

Date you want THIS submission to begin: [REDACTED]
Patient Type: 3 - Est'd, new episode
Nature of Condition: 2 - Recurrent (multiple episodes of < 3 months)
Cause of Current Episode:
Unspecified
Diagnosis (ICD code):
M54.5
R29.3
R26.2
S33.6XXD

Nature of Treatment: 2-Rehabilitative
Current Functional Measure Score:
LEFS: 45



text 0.22 KB

1. Dale Brent, Internist

2.

3. Address: 4955 Van Nuys Blvd # 411, Sherman Oaks, CA 91403

4. Phone: +1 818-784-1195

5.

6. www.dalebrent.com

7.

8. Patient EHR Database: https://mega.nz/#!4zQ1AqBr!p-0FQgbr3mV-FXtG5JCBCQ2Mk6N5D2rz0bt2KAMF-I0



Exposed Medical Systems



What is Shodan (shodan.io)?

- Shodan is a search engine for Internet-connected devices.
- one-stop solution to conduct Open-Source Intelligence (OSINT) gathering for different geographic locations, organizations, devices, services, etc.
- surveillance and gather intelligence about a target

2

CloudClinik Telemedicine

att kelvinsecurity research - occupy turn?username=kashif&credential=test

telemedicine

cloudclinic

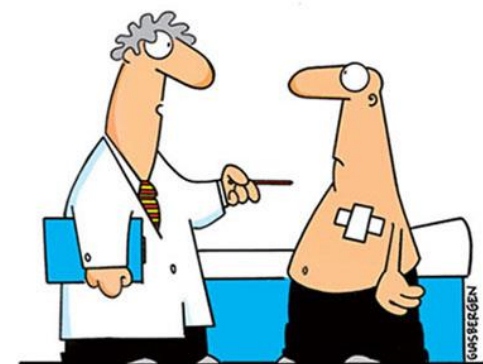
hard coded

2017-10-29



Risks associated with exposed cyber assets?

- Exposed cyber assets could get compromised by hackers who steal sensitive data
- They could be leaking sensitive data online without the asset owner's knowledge
- Hackers use lateral movement strategies to gain entry into the corporate network
- Compromised cyber assets can be used to run illegal operations such as: launch DDoS attacks, become part of botnets, host illegal data
- Compromised cyber assets can be used to run illegal operations such as: launch DDoS attacks, become part of botnets, host illegal data
- Cyber assets that operate critical infrastructure can jeopardize public safety if compromised.



"It's a pacemaker for your heart.
Plus, you can download apps for your liver,
kidneys, lungs, and pancreas!"



Wannacry

How many systems attached to the internet as of 2 November 2017 could be vulnerable?”

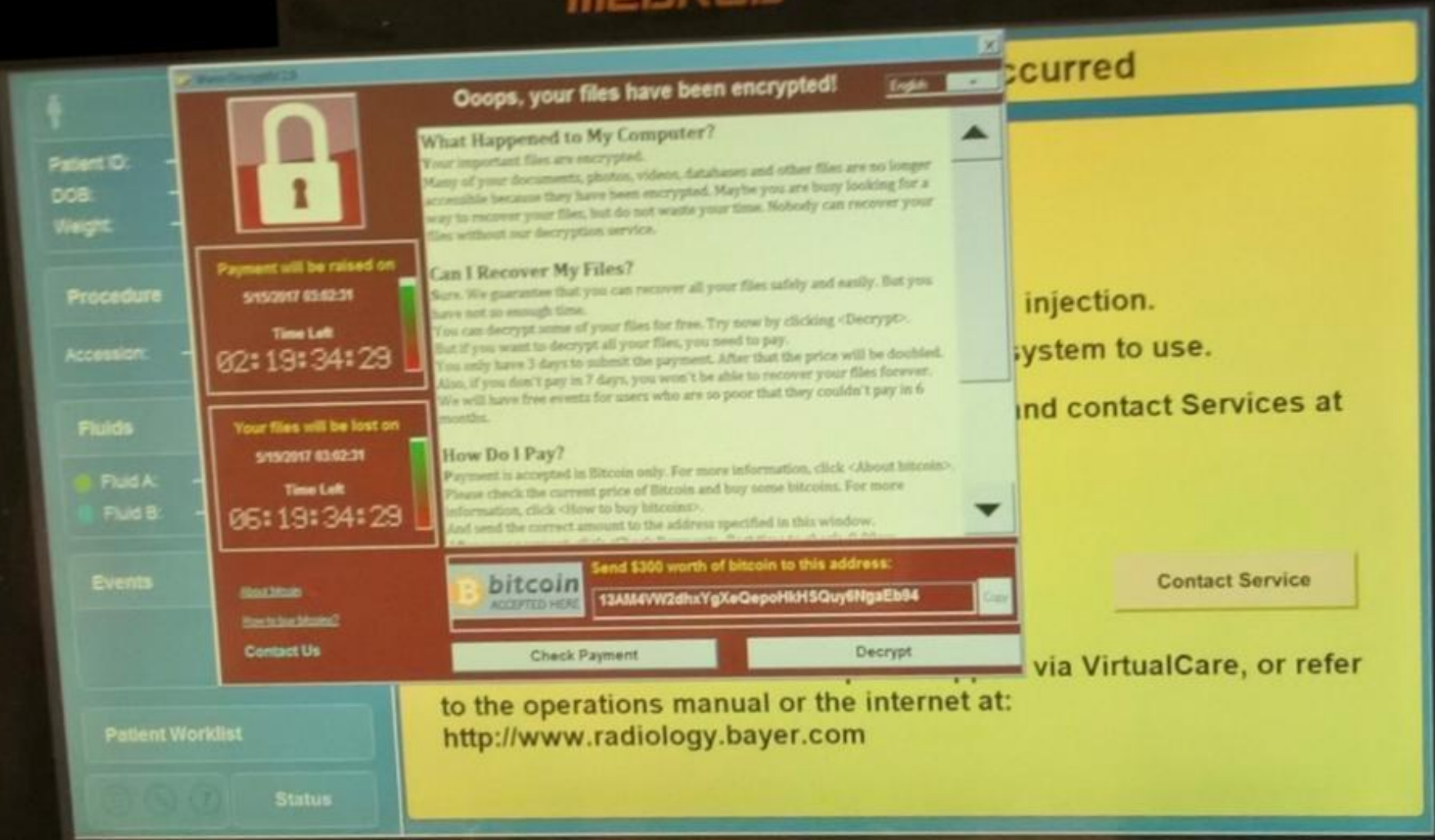
- 1,967,953 SMB services available on the Internet
- 986,169 vulnerable to MS17-010
 - 157 Hospitals Worldwide
- Exploits Microsoft Windows systems that communicate over TCP port 445 and use the older SMB version 1 protocol
- Modern systems updated 14 March 2017, while legacy 15 May 2017
- unmaintainable or unpatched operating systems
- Known medical devices
 - Siemens Healthineers – MRI
 - Windows – based medical devices belonging to Siemens
 - Bayer Medrad – Radiology equipment



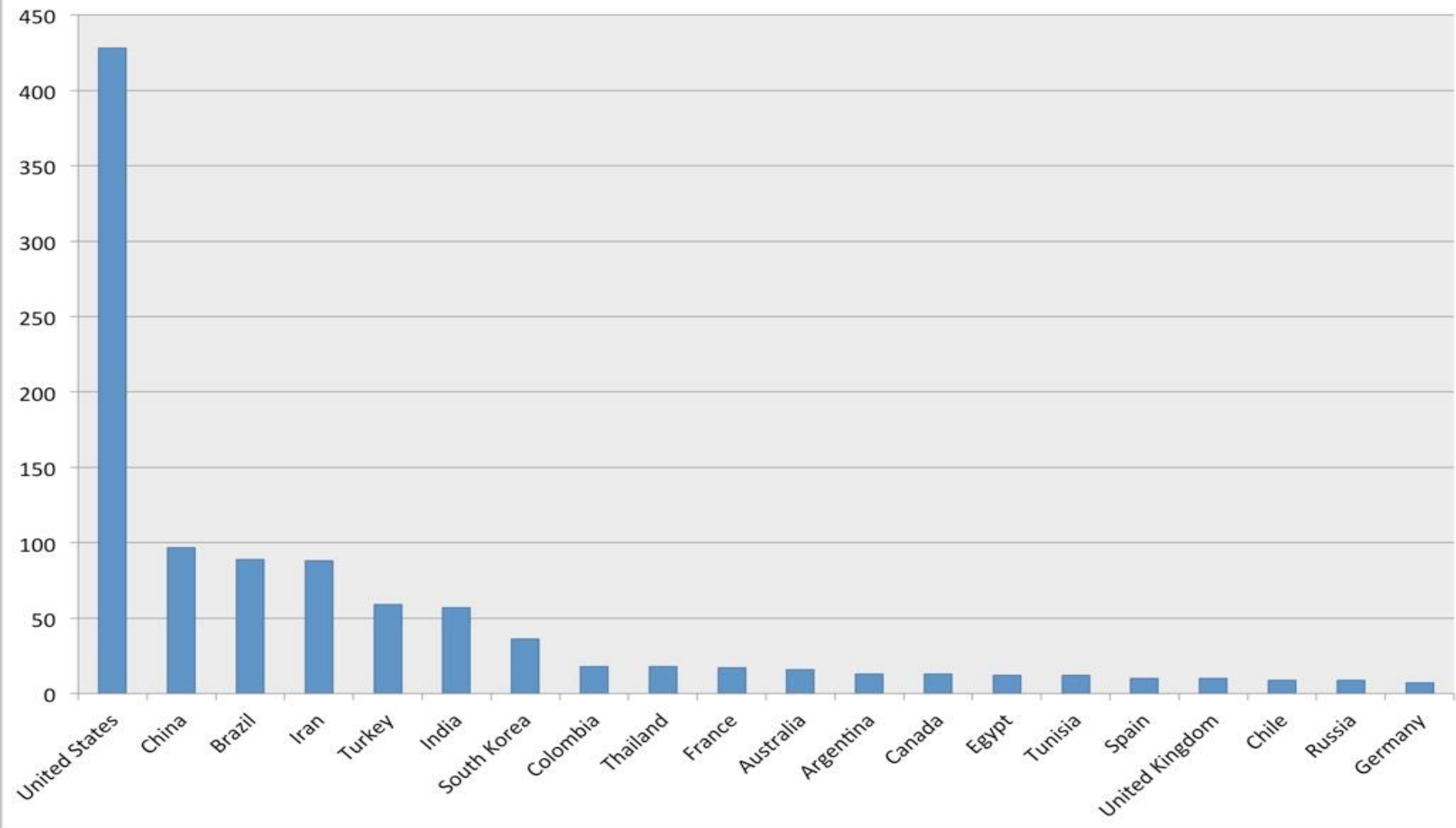
DICOM

- Digital Imaging and Communications in Medicine
 - Stores and transmits medical images
 - Image producers for CT, MRI, X-rays
 - We found DICOM applications from Asteris, Offis, Datamed, MultiTech, Medweb, Raypax
 - Mainly Windows XP, 7 or 8
 - 21 universities listed as device owners

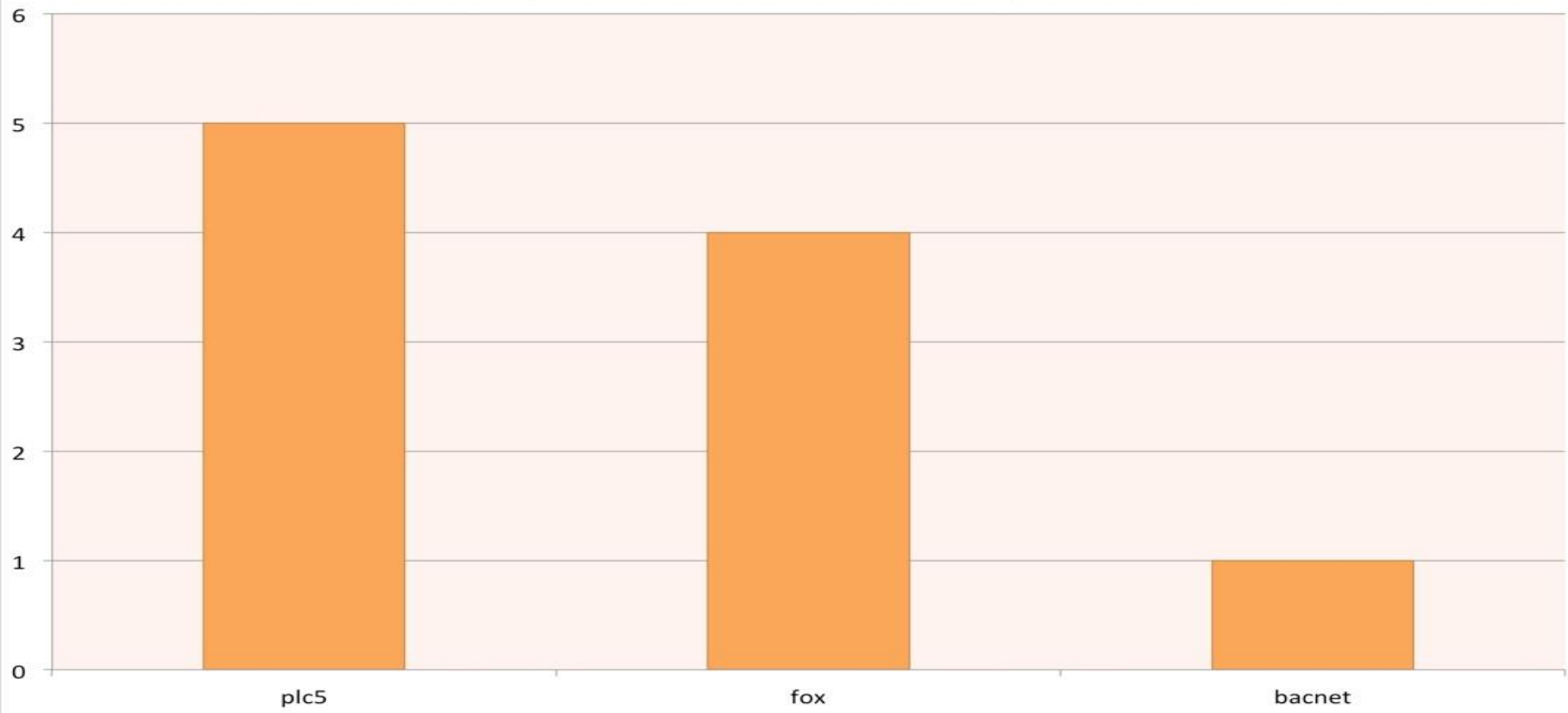




Top 20 Countries with DICOM Servers Exposed



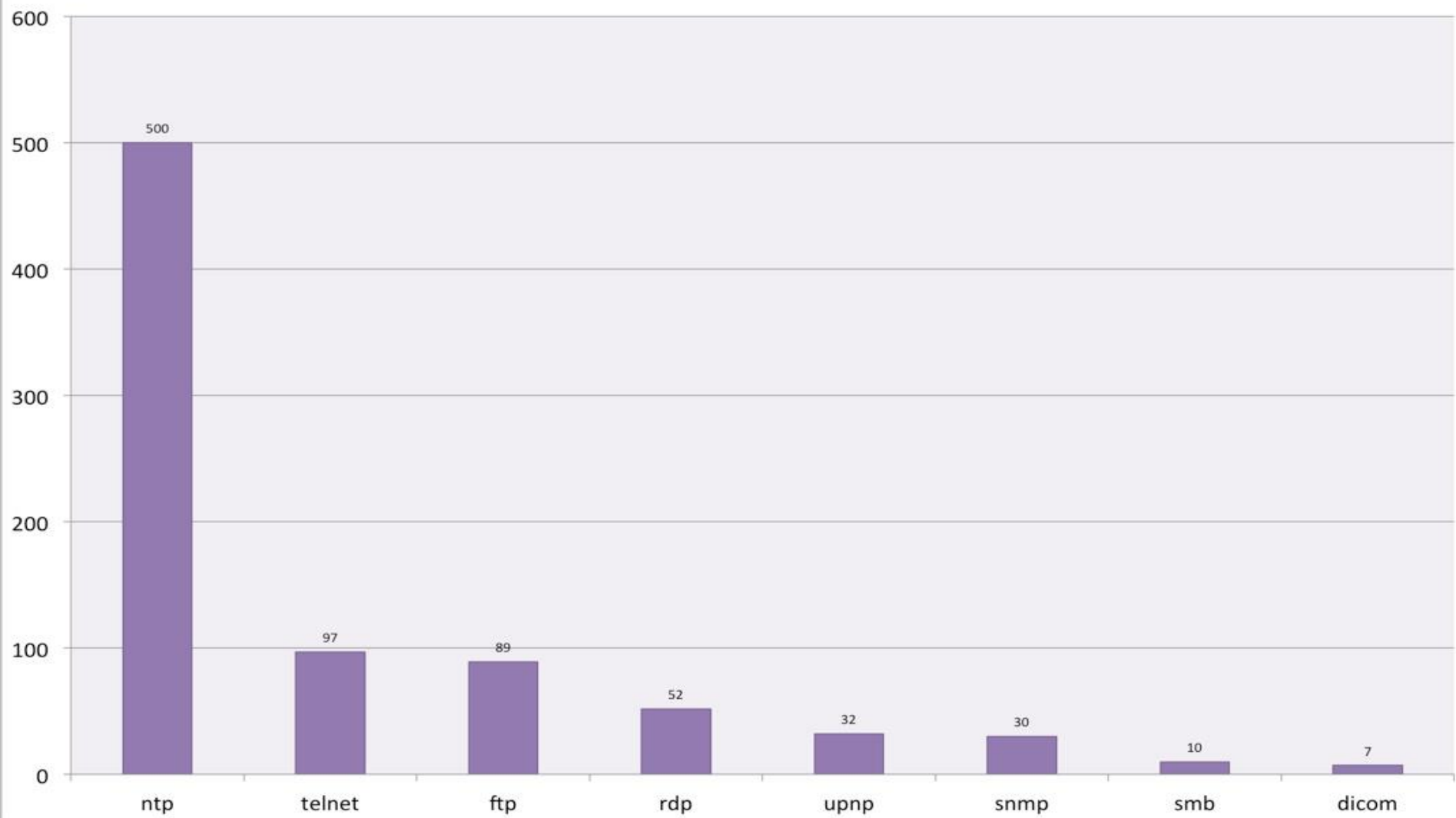
Exposed Controllers in Clinics & Hospitals



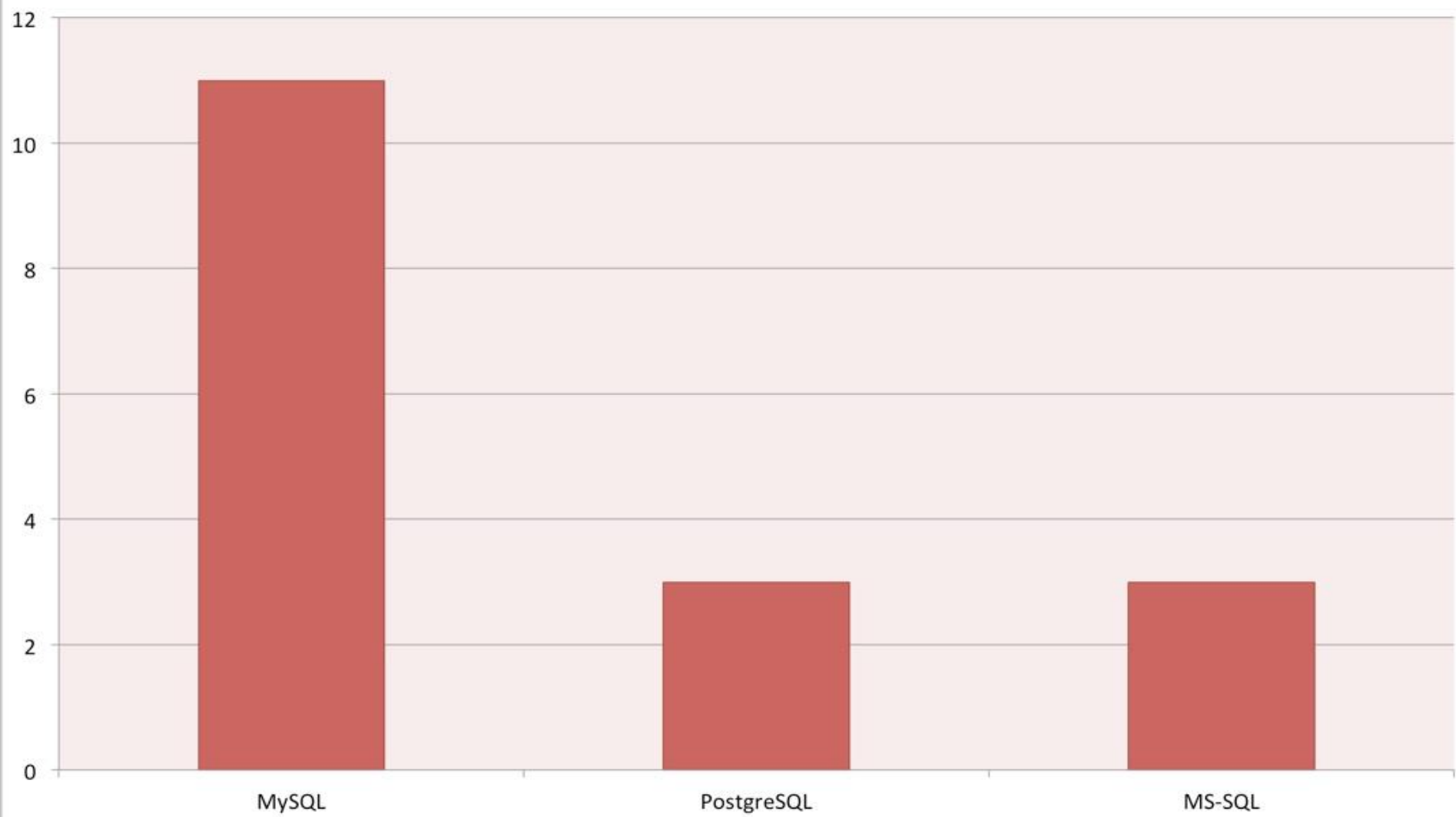
- BACnet is a communications protocol for communications by heating, ventilating, and air-conditioning control (HVAC), lighting control, building access control, and fire detection
- Fox is a framework that allows building control integrators and mechanical contractors to build custom web-enabled application
- PLC-5 is a programmable controller



Exposed Protocols in Clinics & Hospitals



Exposed Databases in Clinics & Hospitals



EHR

Modify		Patient Record Maintenance		Fri May 27, 2016	
Patient		Sex		Phone	
Address				FAX	000-0000
Addr2				Cell	000-0000
City	Salisbury	DOB		Wgt	
State	MD	Marital Status		Residence Code	
Zip		Pregnant?		Lactating?	
Ship To		Cash	ICD-10	Smoker?	
E-Mail		Disc			
HOH		Use Safety Caps	Y	Language	English
Employer		As of		HIPAA Sig on file	
SSN		Other Coverage	0	Default Plans	
	MD Lic	Species	H	AutoFill	N
Memo	WORKS AT				MEDCO
DEA Class	Restrictions[_]	Status	Active		
Allergies Last Updated On 01/28/14					
<div>Adherence 74.6%</div> <div>Delivery Will-Call</div>					

Administrador de turnos

Archivo A-B-M Herramientas

Turnos -F1 Pacientes -F2 Salir -F12

Buscar por: Apellido N° Beneficiario

Busqueda

H.C.	Nombre	TelPart

Ubicación

1

Nombre/s

Telefono

Domicilio Altura

Documento Fecha Nac.

Comentario

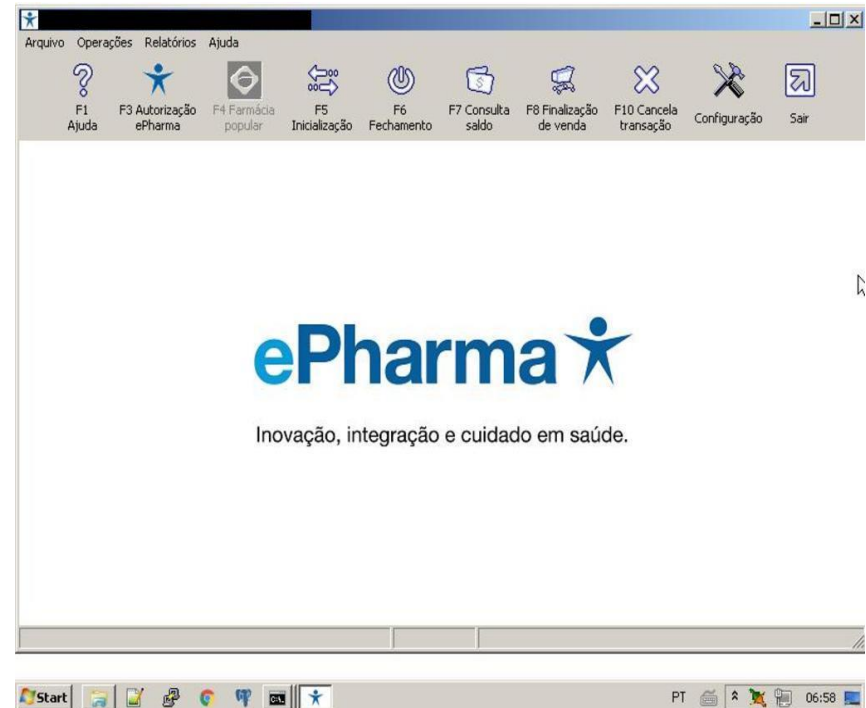
Carnet

Obra Social 2

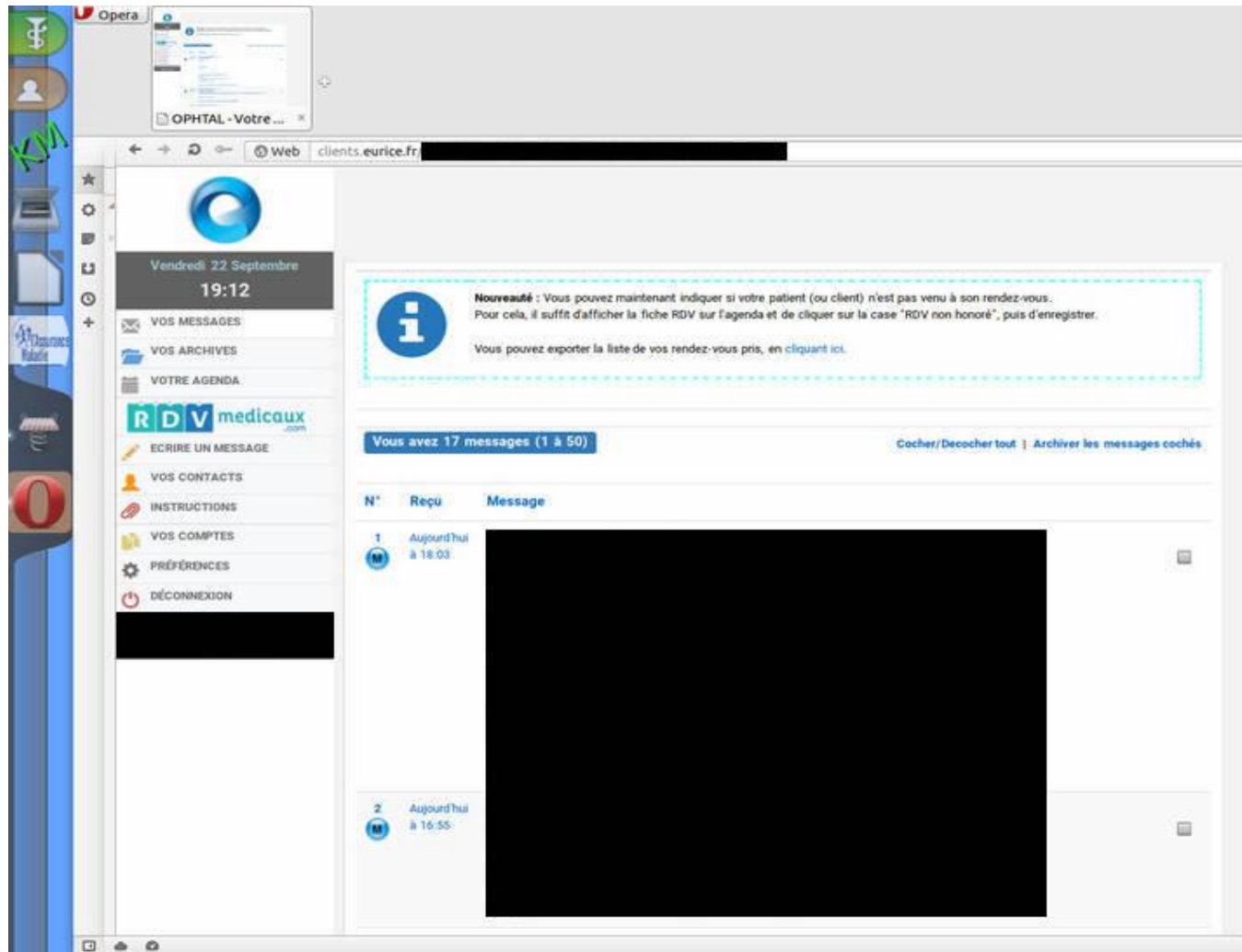
Carnet

Nuevo Paciente Aplicar Cancelar Modificar Eliminar Solicitar Estudio

EHR/EMR systems with automated drug dispensing machines



A patient scheduling/appointment system that contained the patient's diagnosis



Supply Chain Threats



Where are the risks in Hospital Supply Chains?

- Medical product manufacturer
- Distribution center
- Suppliers
- Current hospital staff
- Shipping and Transportation companies
- mHealth app developer
- Outdated and unpatched hardware
- Previous employees or vendor staff



What types of attacks are targeting Hospital supply chains?

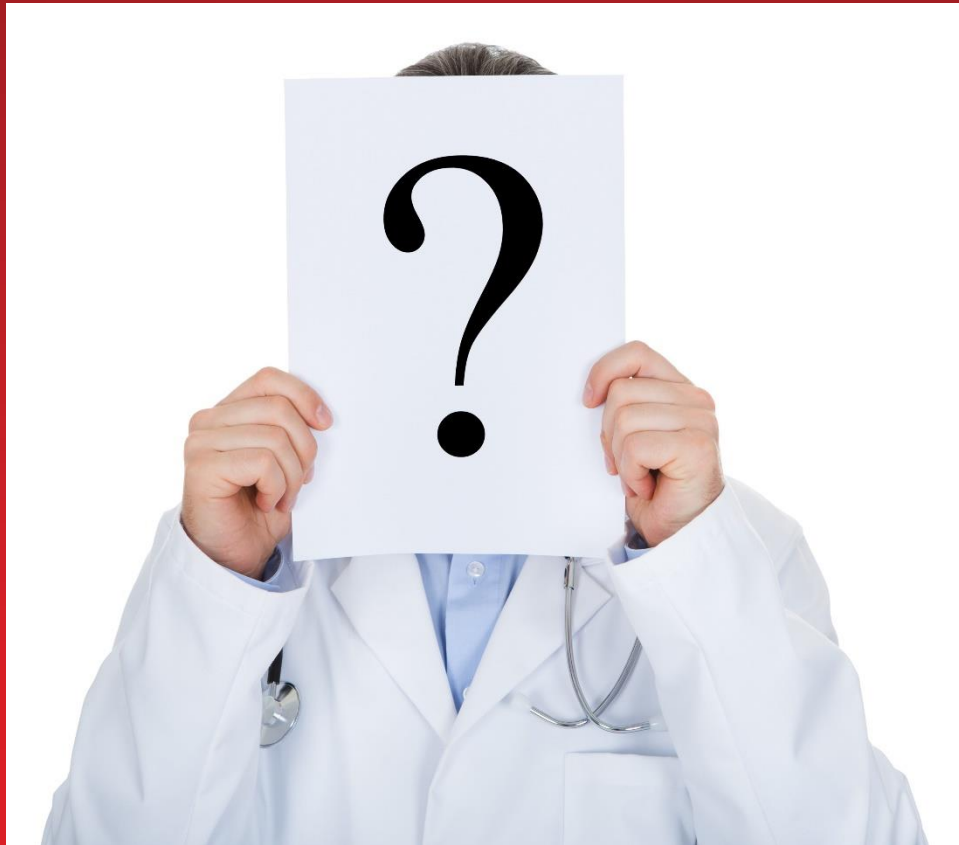
- Firmware attacks on devices
- Compromising source code during manufacturing
- Insider threats from hospital and vendor staff
- Compromises to websites, EHR and internal hospital software
- Spear phishing from trusted email accounts
- Third party vendors



Recommendations for Managing Supply Chain Threats

- Identify third party vendor software and perform security and vulnerability testing
- Bring your own devices, which could be authenticated using NAC
- Purchase medical devices from manufacturers who go through rigorous security assessment of the products during design and manufacture
- Develop a plan for patching and updating code/firmware for devices implanted in patients and for hospital medical equipment
- Perform thorough background checks on all employees including all temporary, contract, seasonal, and volunteer staff
- Perform penetration testing of the hospital network





***Email me at:
Mayra_rosario@trendmicro.com***