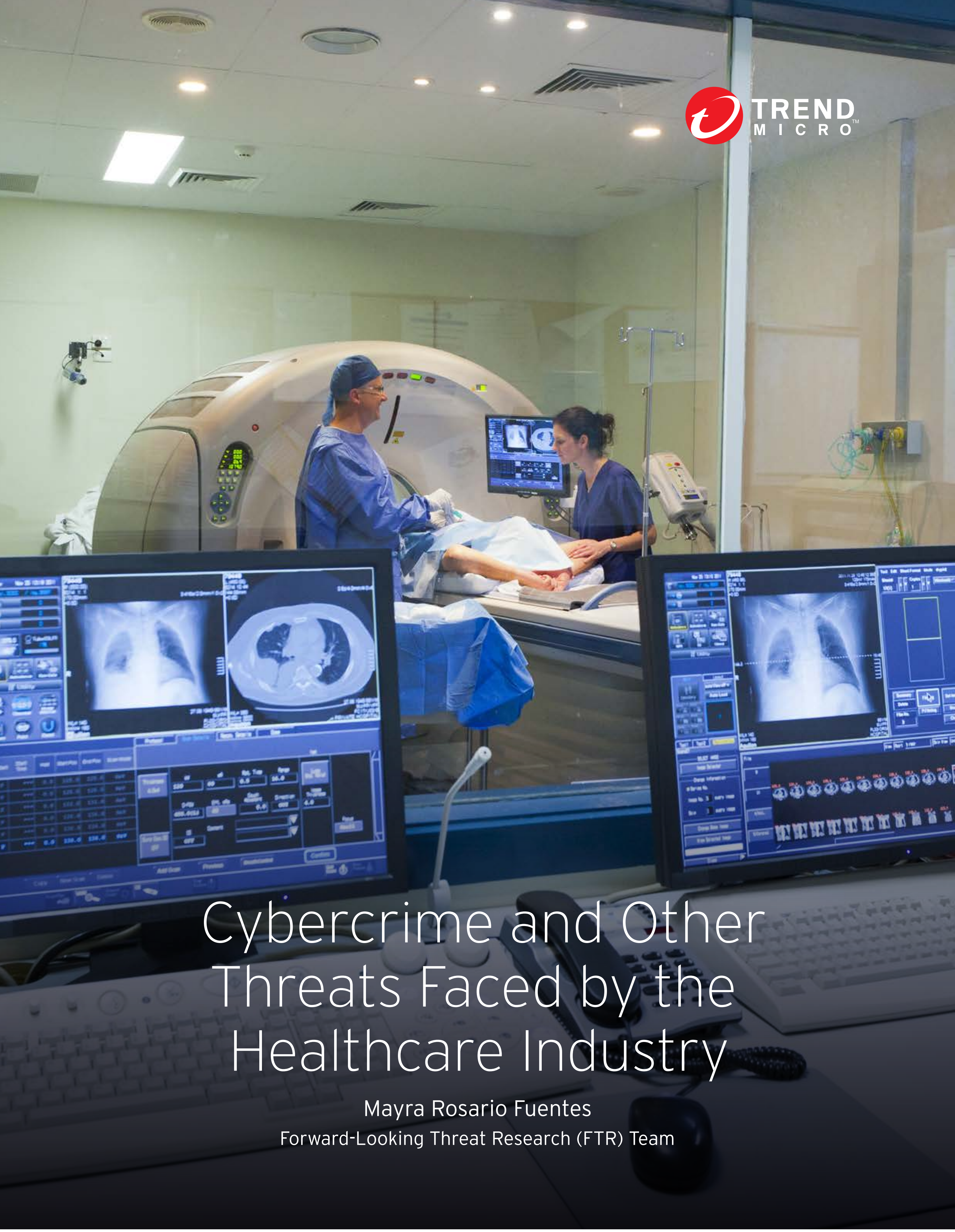


Cybercrime and Other Threats Faced by the Healthcare Industry

Mayra Rosario Fuentes
Forward-Looking Threat Research (FTR) Team

A **TrendLabs** Research Paper

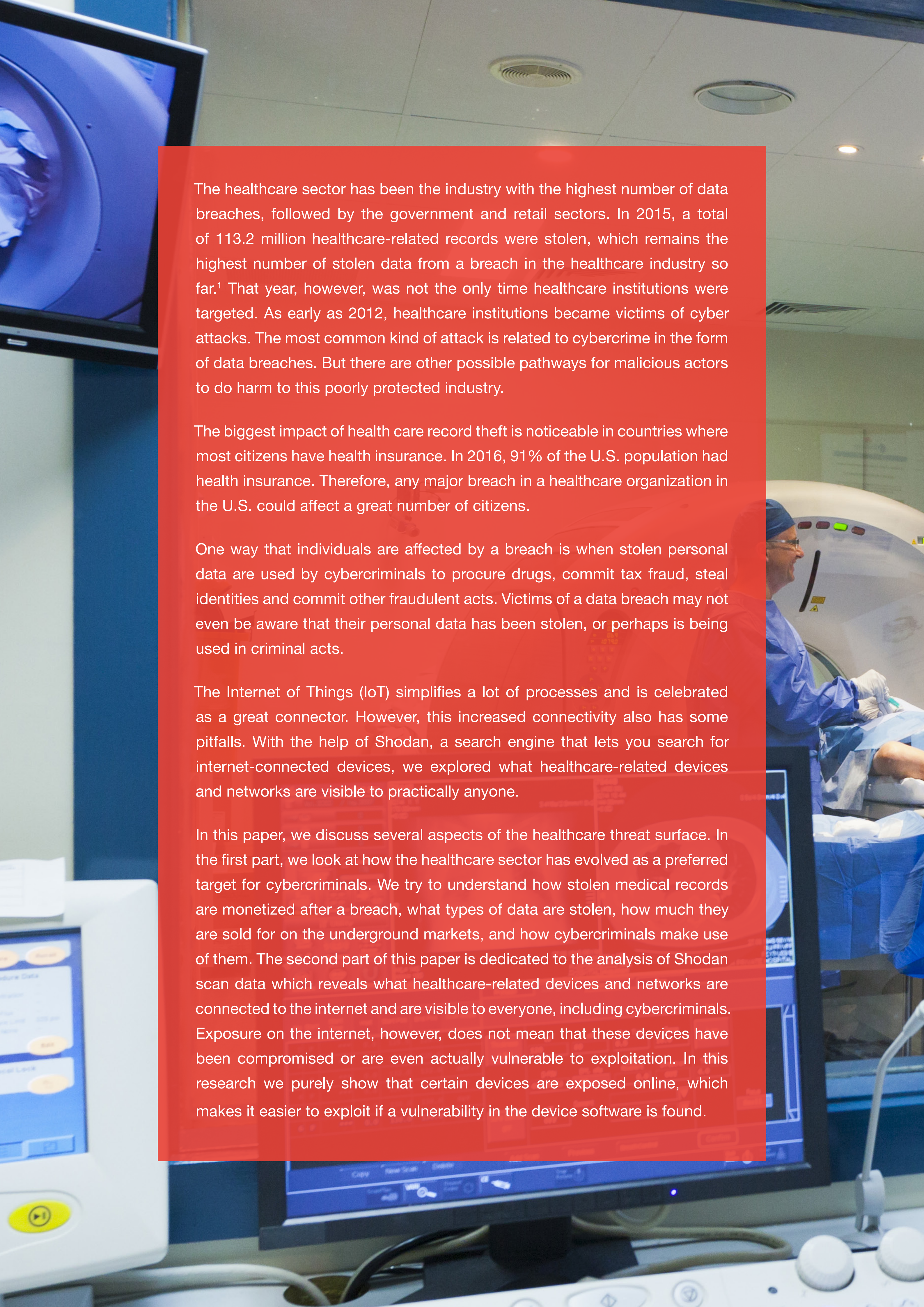
TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents



The healthcare sector has been the industry with the highest number of data breaches, followed by the government and retail sectors. In 2015, a total of 113.2 million healthcare-related records were stolen, which remains the highest number of stolen data from a breach in the healthcare industry so far.[1] That year, however, was not the only time healthcare institutions were targeted. As early as 2012, healthcare institutions became victims of cyber attacks. The most common kind of attack is related to cybercrime in the form of data breaches. But there are other possible pathways for malicious actors to do harm to this poorly protected industry.

The biggest impact of health care record theft is noticeable in countries where most citizens have health insurance. In 2016, 91% of the U.S. population had health insurance. Therefore, any major breach in a healthcare organization in the U.S. could affect a great number of citizens.

One way that individuals are affected by a breach is when stolen personal data are used by cybercriminals to procure drugs, commit tax fraud, steal identities and commit other fraudulent acts. Victims of a data breach may not even be aware that their personal data has been stolen, or perhaps is being used in criminal acts.

The Internet of Things (IoT) simplifies a lot of processes and is celebrated as a great connector. However, this increased connectivity also has some pitfalls. With the help of Shodan, a search engine that lets you search for internet-connected devices, we explored what healthcare-related devices and networks are visible to practically anyone.

In this paper, we discuss several aspects of the healthcare threat surface. In the first part, we look at how the healthcare sector has evolved as a preferred target for cybercriminals. We try to understand how stolen medical records are monetized after a breach, what types of data are stolen, how much they are sold for on the underground markets, and how cybercriminals make use of them. The second part of this paper is dedicated to the analysis of Shodan scan data which reveals what healthcare-related devices and networks are connected to the internet and are visible to everyone, including cybercriminals. Exposure on the internet, however, does not mean that these devices have been compromised or are even actually vulnerable to exploitation. In this research we purely show that certain devices are exposed online, which makes it easier to exploit if a vulnerability in the device software is found.

The Security Issue with Electronic Health Records

An electronic health record (EHR) is a digital version of a patient's medical record. Every EHR contains information about a patient's demographics, insurance information, mailing address, Social Security number, birthdate, notes from prescribing doctor, lifestyle details, medications, vital signs, family medical history, immunization records, laboratory results and even radiology reports among others. Other than medical records, EHRs may also contain billing information such as credit card details and invoices.

An EHR is accessed by EHR management software. In the U.S. programs such as PrognoCIS, NueMD, McKesson, Allscripts, Cerner, Praxis EMR, Athena Health, GE Healthcare, eClinicalWorks, and SRS EHR are used. Internationally, EHR programs such as Allscripts Healthcare Solutions, Inc., Athena Health, Inc. Cerner Corporation, CPSI, Epic Systems, eClinicalWorks, GE Healthcare, Greenway Health LLC, Medical Information Technology, Inc., McKesson Corporation, and NextGen and OpenMRS are utilized.

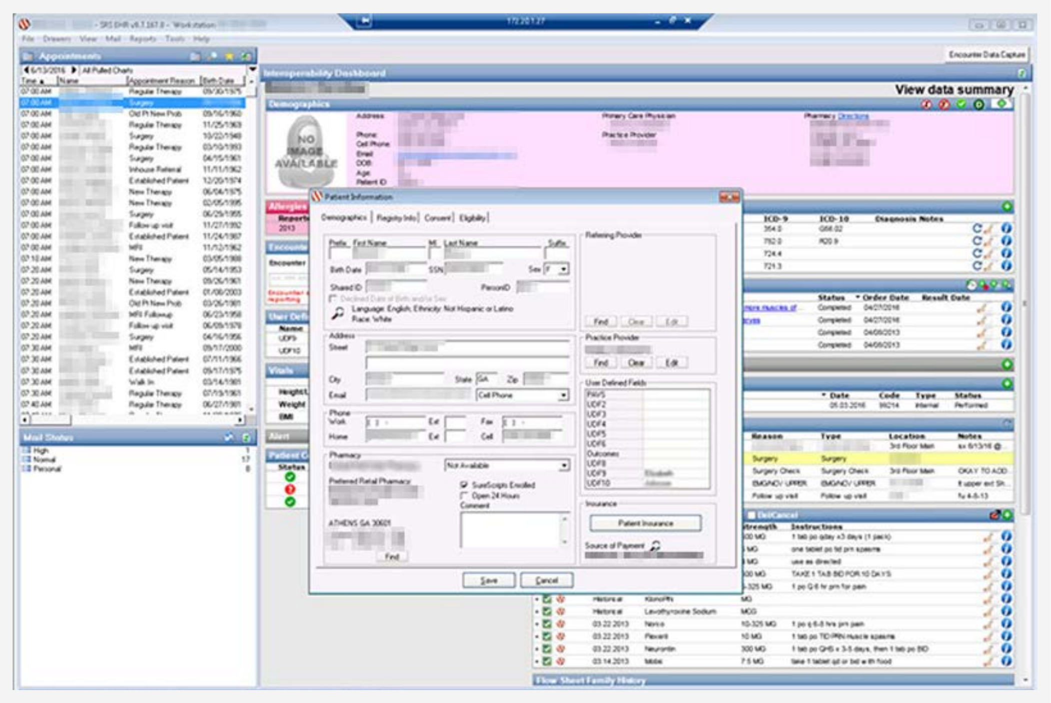
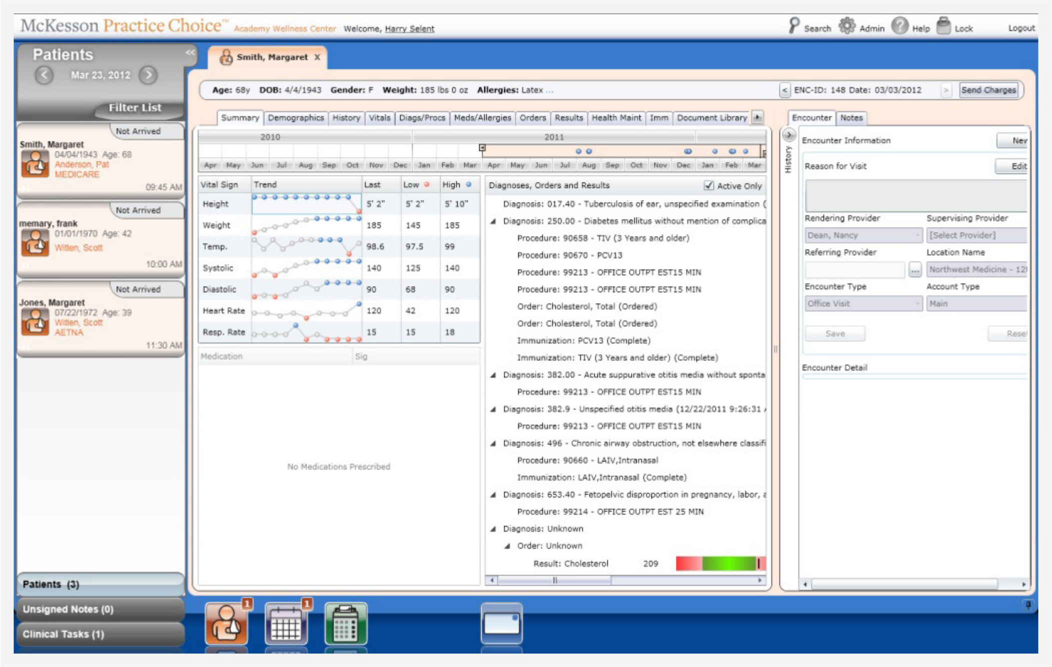


Figure 1. A screenshot of a compromised EHR from a U.S. healthcare facility[2]



Welcome, Harry Selent

Mar 23, 2012

Not Arrived
Smith, Margaret
04/04/1943 Age: 68
Anderson, Pat
MEDICARE
09:45 AM

Not Arrived
memary, frank
01/01/1970 Age: 42
Witlen, Scott
10:00 AM

Not Arrived
Jones, Margaret
07/22/1972 Age: 39
Witlen, Scott
AETNA
11:30 AM

Age: 68y **DOB:** 4/4/1943 **Gender:** F **Weight:** 185 lbs 0 oz **Allergies:** Latex ...

ENC-ID: 148 Date: 03/03/2012

Vital Sign	Trend	Last	Low	High
Height		5' 2"	5' 2"	5' 10"
Weight		185	145	185
Temp.		98.6	97.5	99
Systolic		140	125	140
Diastolic		90	68	90
Heart Rate		120	42	120
Resp. Rate		15	15	18

Medication	Sig
No Medications Prescribed	

Diagnoses, Orders and Results ☑ Active Only

Diagnosis: 017.40 - Tuberculosis of ear, unspecified examination (
Diagnosis: 250.00 - Diabetes mellitus without mention of complica
Procedure: 90658 - TIV (3 Years and older)
Procedure: 90670 - PCV13
Procedure: 99213 - OFFICE OUTPT EST15 MIN
Procedure: 99213 - OFFICE OUTPT EST15 MIN
Order: Cholesterol, Total (Ordered)
Order: Cholesterol, Total (Ordered)
Immunization: PCV13 (Complete)
Immunization: TIV (3 Years and older) (Complete)
Diagnosis: 382.00 - Acute suppurative otitis media without sponta
Procedure: 99213 - OFFICE OUTPT EST15 MIN
Diagnosis: 382.9 - Unspecified otitis media (12/22/2011 9:26:31
Procedure: 99213 - OFFICE OUTPT EST15 MIN
Diagnosis: 496 - Chronic airway obstruction, not elsewhere classifi
Procedure: 90660 - LAIV,Intranasal
Immunization: LAIV,Intranasal (Complete)
Diagnosis: 653.40 - Fetopelvic disproportion in pregnancy, labor, a
Procedure: 99214 - OFFICE OUTPT EST 25 MIN
Diagnosis: Unknown
Order: Unknown
Result: Cholesterol 209

Encounter Information
Reason for Visit
Rendering Provider: Dean, Nancy
Supervising Provider: [Select Provider]
Referring Provider:
Location Name: Northwest Medicine - 12
Encounter Type: Office Visit
Account Type: Main
Encounter Detail

Figure 2. A screenshot of the McKesson EHR software[3]

Given the contents of an EHR and its capacity to hold financial and credit card records, healthcare organizations become targets of cybercriminals who aim to steal personal identifiable information (PII), as well as financial information. But unlike other data breaches, cybercriminals have found more ways to use information from EHRs aside from selling the data in bulk in underground markets. With this in mind, further steps have to be taken to keep health care data secure.

Healthcare Laws Protecting Data and Users

The Health Information Technology for Economic and Clinical Health (HITECH) Act, under the American Recovery and Reinvestment Act of 2009 (ARRA) made it a federal mandate for healthcare institutions to adopt the use of electronic health records systems to improve health care. This also reduces cost by replacing physical documentation with electronic ones. There was also a series of financial-incentive programs that were established for the implementation, upgrade, maintenance, and smooth operation of EHR technology.

In terms of usage, there were 513,811 health care providers that received payment for participating in the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs in 2016. Between May 2011 and December 2016, more than US$35 billion in Medicare and Medicaid EHR Incentive Program payments were made.[4]

While incentive programs were provided for the use of EHR systems, there was no guidance regarding the security of these EHR systems.[5] On top of that, healthcare facilities lacked the budget, the manpower, and the expertise to manage data breaches caused by evolving cyber threats. Despite Health Insurance Portability and Accountability Act (HIPAA) laws being designed to protect patients against loss, theft or the disclosure of patients' sensitive medical information, there remains a lot of healthcare entities that have not implemented basic safeguards like encrypting data or using a two-factor authentication process, which are risk management tactics that were recommended since 2006. In fact, the HIPAA recommended the use of strong encryption and for Secure Sockets Layer (SSL) to be the minimum requirement for all internet-based systems, including corporate web email systems.[6]

According to a survey by the Healthcare Information and Management System Society (HIMSS), about 68.1% of hospital providers and less than half of medical practice providers encrypt data in transit and are sending protected health information in the clear. As for stationary data, 61.3% of hospitals are encrypting stored data and 48.4% of medical practice providers are encrypting stored data.[7] Without encryption, the data in transit can be captured through eavesdropping, packet sniffing, or through other methods.

The Ponemon Institute's Sixth Annual Benchmark Study on Privacy and Security Health Care Data in May 2016, made the following points:

- About half of all organizations have little or no confidence that they can detect all patient data loss or theft.
- The majority of healthcare organizations still lack sufficient budget for security that will be used to curtail or minimize data breach incidents. A majority also believes that their incident response process has inadequate funding and resources.
- The majority of healthcare organizations have not invested in the technologies necessary to mitigate a data breach, nor have hired enough skilled IT security practitioners.
- The budget for security of most healthcare organizations has declined by 10%, while that of more than half of the organizations have remained static and most healthcare organizations believe they don't have the budget to properly protect data. [8]

Breaches of EHR Software

While there are existing laws that are designed to protect a patient's privacy, like the HIPAA, healthcare facilities still have to enact basic safeguards to protect a patient's information. Unfortunately, a lot of healthcare entities today still do not encrypt data or use a two-factor authentication process. In addition, healthcare institutions also lack the resources, and/ or the expertise, to deal with data breaches and other cyber attacks.

EHRs are targets of cybercriminals since they contain PII that do not expire. For example, Social Security numbers can be used multiple times for malicious intent, making them more valuable compared to other PII. More often than not, cybercriminals target the EHR software and vendors themselves. Attacking cloud-based EHR software vendors can allow cybercriminals access to multiple client databases in a single operation.These databases may be exposed to vulnerabilities such as SQL injections, cross-site scripting and are also exposed via the internet to practically anyone.

Bizmatics, a California-based company offers locally hosted and cloud-based EHR software. Bizmatics produced the PrognoCIS software that was comprised in January 2015 when a malware in their server allowed hackers to gain access to the data. PrognoCIS is an EHR software that includes an online patient portal that allows patients to request appointments, order medicine refills, review their medical records and communicate with the doctor's office. It is believed that 300,000 individuals were affected in this attack alone. [9]

The Bizmatics server contained patients' medical records with information such as names, addresses, dates of birth, insurance information, Social Security numbers, and various types of clinical documentation. At least 17 healthcare facilities were compromised. The clients that reported breaches were the ENT and Allergy Center in Arkansas, North Ottawa Community Health System, Vincent Vein Center Grand Junction P.C., California Health and Longevity Institute, Lafayette Pain Care PC, Eye Associates of Pinellas, Pain Treatment Centers of America, Integrated Health Solutions PC, Illinois Valley Podiatry Group, Complete Family Foot Care, Family Medicine of Weston, HealthCare Consultants, The Vein Doctor, Mark Anthony Quintero M.D. L.L.C. and an undisclosed company represented by the law firm Allen Dell.[10]

Also in 2015, Medical Informatics Engineering suffered from data theft when their web-based EHR software NoMoreClipboard exposed 3.9 million of patient data. The stolen data included patients' names, mailing addresses, email addresses, dates of birth, Social Security numbers, lab results and voice-recorded reports.[11]

Why steal EHR?

EHR data is unique in a way that it includes PII, along with medical, insurance, and financial information. To get a better grasp of an EHR's value, let's compare an EHR breach with a non-EHR breach. In September 2016, Yahoo disclosed a data breach that occurred in 2014 wherein 500 million user accounts were stolen. The PII that were compromised included users' names, emails, telephone numbers, date of birth, hashed passwords, and security questions and answers.[12] While there is a market for PII in the criminal underground, financial information such as those found in EHRs are worth more.

Aside from financial information, an EHR contains PII that cannot be replaced. This poses a big challenge when PII is stolen and peddled in the underground market. By combining portions of PII, cybercriminals are able to unlawfully obtain wares. For example, date of birth, medical insurance ID, and a Social Security number can be combined to acquire medical insurance.

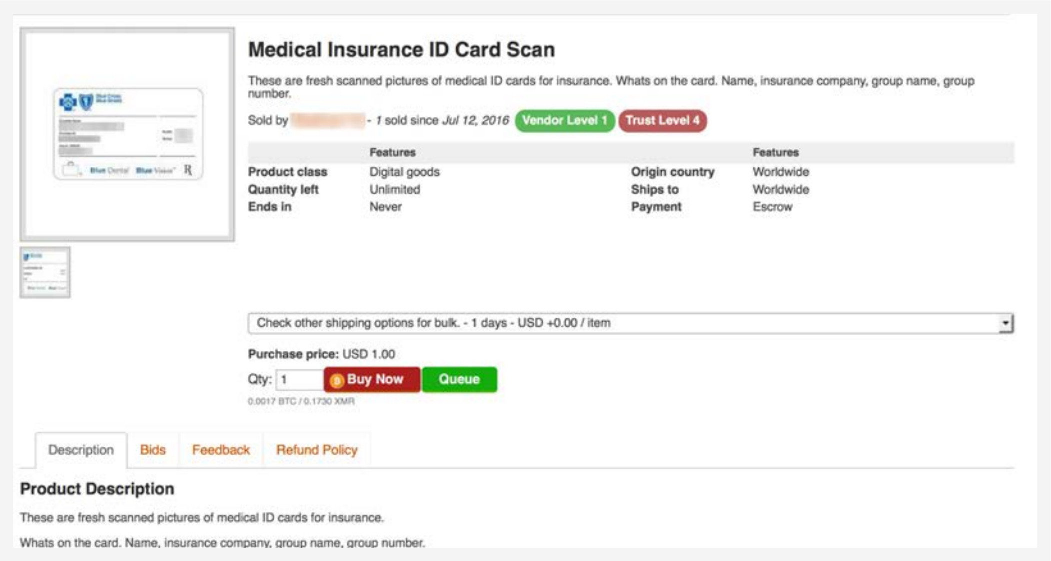
A major reason why cybercriminals can successfully steal EHRs is the lack of safeguards implemented in healthcare institutions with regard to their digital assets. Hospitals and other healthcare organizations may prioritize operations and efficiency of the facility over cybersecurity. Very often hospitals and/or healthcare organizations may not be equipped with the right staff to handle digital threats and basic security methods such as a two-factor authentication or encryption.

Electronic Health Records Traded in the Underground

In the past three years, stealing payment card data became very popular due to the success of point-of-sale (PoS) malware. However, cybercriminals can only use the stolen credit cards before the card expires, is maxed out or cancelled. In contrast, an EHR database containing PII that do not expire—such as Social Security numbers—can be used multiple times for malicious intent. Stolen EHR can be used to acquire prescription drugs, receive medical care, falsify insurance claims, file fraudulent tax returns, open credit accounts, obtain official government-issued documents such as passports, driver's licenses, and even create new identities.

EHRs can be sold as a complete EHR database or the information can be sold in portions. These portions are of course the different PII elements which include Social Security numbers, addresses, etc. Popular Dark Web marketplaces include TheRealDeal, AlphaBay, Valhalla, Apple Market, Python Market, Dream Market and Silk Road. In the following, we have compiled different items that we saw in some underground marketplaces (see figures below).

Medical Insurance ID data



Medical Insurance ID Card Scan

These are fresh scanned pictures of medical ID cards for insurance. Whats on the card. Name, insurance company, group name, group number.

Sold by [redacted] - *1 sold since Jul 12, 2016* Vendor Level 1 Trust Level 4

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Check other shipping options for bulk. - 1 days - USD +0.00 / item

Purchase price: USD 1.00

Qty: 1

0.0017 BTC / 0.1730 XMR

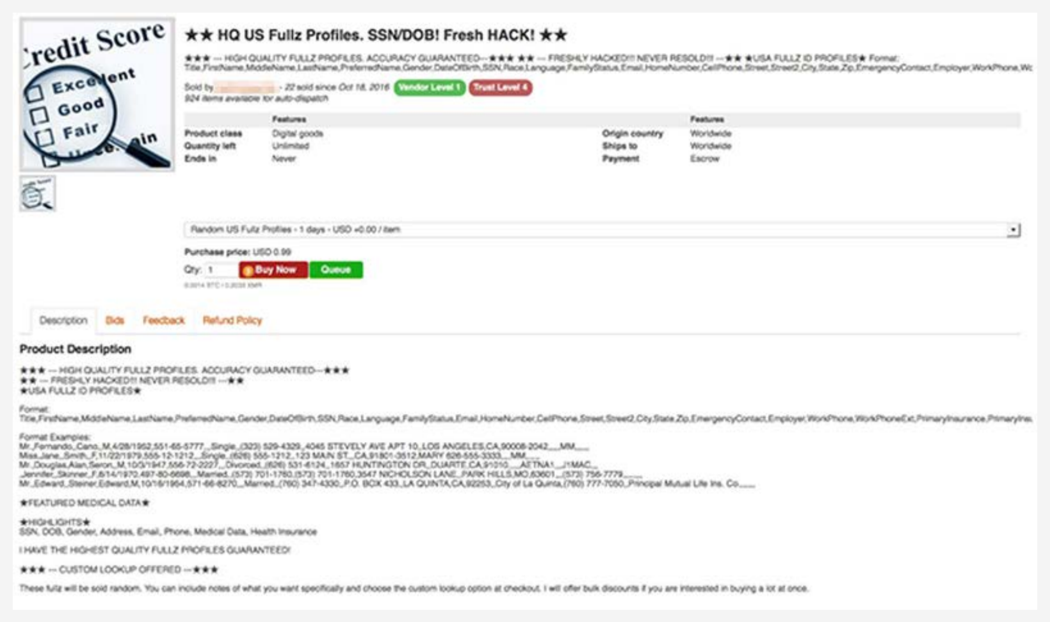
Product Description

These are fresh scanned pictures of medical ID cards for insurance.

Whats on the card. Name, insurance company, group name, group number.

Figure 3. An AlphaBay ad selling medical insurance cards in August 2016

Alphabay vendors are selling medical insurance cards that can be used to receive medical care and order prescription refills through mail orders. Figure 3 shows a threat actor selling stolen medical insurance ID cards for as low as US$1 per ID.



★★ HQ US Fullz Profiles. SSN/DOB! Fresh HACK! ★★

★★★ — HIGH QUALITY FULLZ PROFILES. ACCURACY GUARANTEED—★★★ ★★ — FRESHLY HACKED!!! NEVER RESOLD!!! —★★ ★USA FULLZ ID PROFILES★ Format: Title,FirstName,MiddleName,LastName,PreferredName,Gender,DateOfBirth,SSN,Race,Language,FamilyStatus,Email,HomeNumber,CellPhone,Street,Street2,City,State,Zip,EmergencyContact,Employer,WorkPhone,Wc

Sold by [redacted] - *22 sold since Oct 18, 2016* Vendor Level 1 Trust Level 4
924 items available for auto-dispatch

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Random US Fullz Profiles - 1 days - USD +0.00 / item

Purchase price: USD 0.99

Qty: 1 Buy Now Queue

0.0014 BTC / 0.2038 XMR

Description Bids Feedback Refund Policy

Product Description

★★★ — HIGH QUALITY FULLZ PROFILES. ACCURACY GUARANTEED—★★★
★★ — FRESHLY HACKED!!! NEVER RESOLD!!! —★★
★USA FULLZ ID PROFILES★

Format:
Title,FirstName,MiddleName,LastName,PreferredName,Gender,DateOfBirth,SSN,Race,Language,FamilyStatus,Email,HomeNumber,CellPhone,Street,Street2,City,State,Zip,EmergencyContact,Employer,WorkPhone,WorkPhoneExt,PrimaryInsurance,PrimaryIns

Format Examples:
Mr.,Fernando,,Cano,,M,4/28/1952,551-65-5777,,,Single,,(323) 529-4329,,4045 STEVELY AVE APT 10,,LOS ANGELES,CA,90008-2042,,,,MM,,,,
Miss,Jane,,Smith,,F,11/22/1979,555-12-1212,,,Single,,(626) 555-1212,,123 MAIN ST,,,CA,91801-3512,MARY 626-555-3333,,,MM,,,,
Mr.,Douglas,Alan,Seron,,M,10/3/1947,556-72-2227,,,Divorced,,(626) 531-6124,,1657 HUNTINGTON DR,,DUARTE,CA,91010,,,,AETNA1,,,J1MAC,,
,Jennifer,,Skinner,,F,8/14/1970,497-80-6698,,,Married,,(573) 701-1760,(573) 701-1760,3547 NICHOLSON LANE,,PARK HILLS,MO,63601,,,(573) 756-7779,,,,,
Mr.,Edward,,Steiner,Edward,M,10/16/1964,571-66-8270,,,Married,,(760) 347-4330,,P.O. BOX 433,,LA QUINTA,CA,92253,,City of La Quinta,(760) 777-7050,,Principal Mutual Life Ins. Co.,,,,,

★FEATURED MEDICAL DATA★

★HIGHLIGHTS★
SSN, DOB, Gender, Address, Email,, Phone, Medical Data, Health Insurance

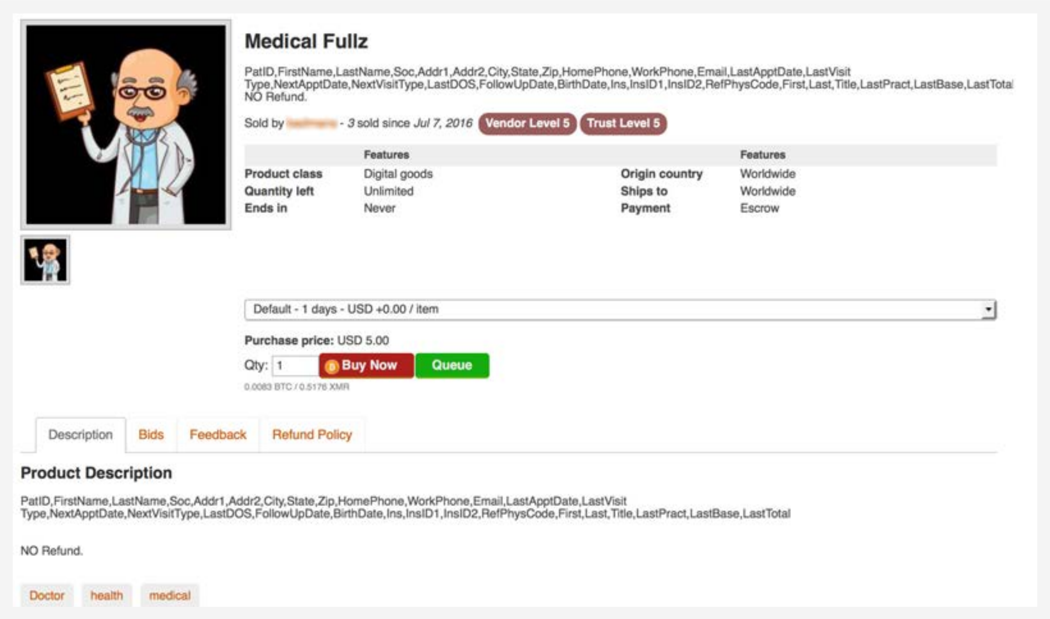
I HAVE THE HIGHEST QUALITY FULLZ PROFILES GUARANTEED!

★★★ — CUSTOM LOOKUP OFFERED —★★★

These fullz will be sold random. You can include notes of what you want specifically and choose the custom lookup option at checkout. I will offer bulk discounts if you are interested in buying a lot at once.

Figure 4. An AplhaBay ad selling full records of U.S. citizens with medical data on 4 November 2016

The figure above shows a hacker selling “full records” of U.S. citizens, which feature specific medical data and the preferred health insurance. Prices start at 99 cents per person but the cybercriminal offers discounts if people buy in bulk.



Medical Fullz

PatID,FirstName,LastName,Soc,Addr1,Addr2,City,State,Zip,HomePhone,WorkPhone,Email,LastApptDate,LastVisitType,NextApptDate,NextVisitType,LastDOS,FollowUpDate,BirthDate,Ins,InsID1,InsID2,RefPhysCode,First,Last,Title,LastPract,LastBase,LastTotal
NO Refund.

Sold by [redacted] - *3 sold since Jul 7, 2016* Vendor Level 5 Trust Level 5

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 5.00

Qty: 1 Buy Now Queue

0.0083 BTC / 0.5176 XMR

Description Bids Feedback Refund Policy

Product Description

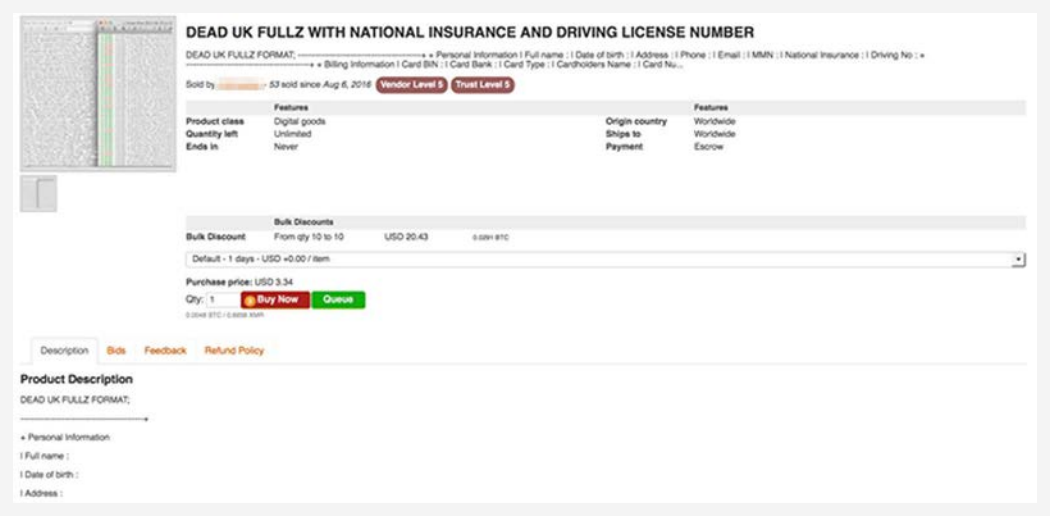
PatID,FirstName,LastName,Soc,Addr1,Addr2,City,State,Zip,HomePhone,WorkPhone,Email,LastApptDate,LastVisitType,NextApptDate,NextVisitType,LastDOS,FollowUpDate,BirthDate,Ins,InsID1,InsID2,RefPhysCode,First,Last,Title,LastPract,LastBase,LastTotal

NO Refund.

Doctor health medical

Figure 5. AlphaBay advertisement for Medical insurance ID

This screenshot shows a hacker selling comprehensive medical profiles on AlphaBay. These profiles were obtained from an EHR database that contained a patient's name, Social Security number, address, date of last visit, date of next appointment, follow-up treatment dates, date of birth, and health insurance ID numbers. Prices per patient information item start at US$5.



DEAD UK FULLZ WITH NATIONAL INSURANCE AND DRIVING LICENSE NUMBER

DEAD UK FULLZ FORMAT; -----------------------------• • Personal Information I Full name : I Date of birth : I Address : I Phone : I Email : I MMN : I National Insurance : I Driving No : • -----------------------------• • Billing Information I Card BIN : I Card Bank : I Card Type : I Cardholders Name : I Card Nu...

Sold by [redacted] - *53 sold since Aug 6, 2016* Vendor Level 5 Trust Level 5

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

	Bulk Discounts		
Bulk Discount	From qty 10 to 10	USD 20.43	0.0291 BTC

Default - 1 days - USD +0.00 / item

Purchase price: USD 3.34

Qty: 1 Buy Now Queue

0.0048 BTC / 0.6058 XMR

Product Description

DEAD UK FULLZ FORMAT;

-----------------------------•

• Personal Information

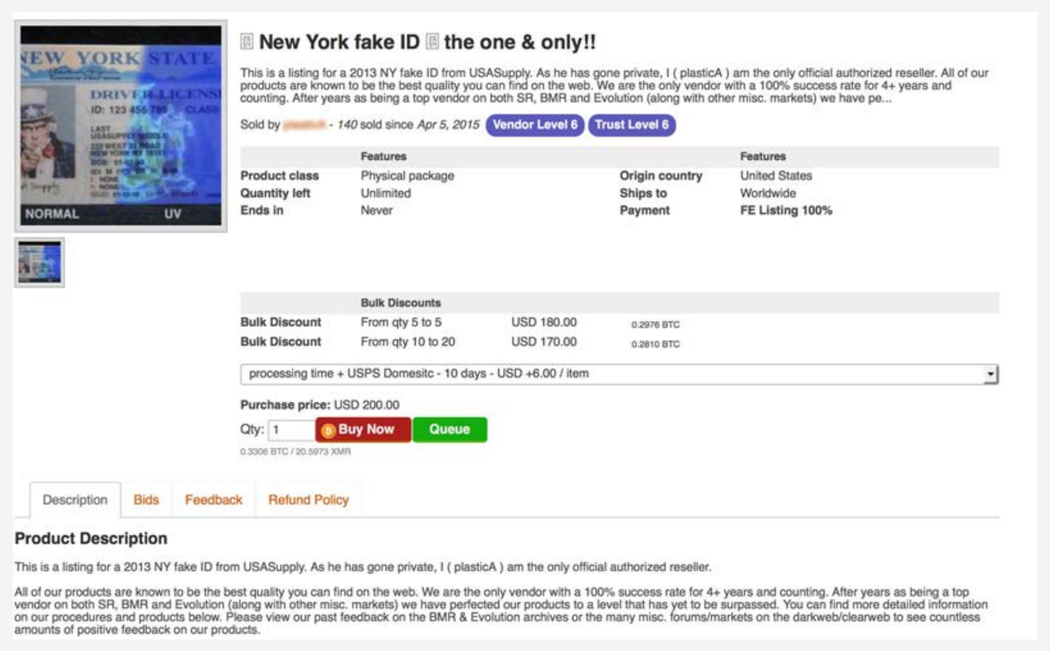
I Full name :

I Date of birth :

I Address :

Figure 6. Alphabay advertisement for UK health insurance ID and driver's license on 4 November 2016

The image above shows a cybercriminal selling United Kingdom health insurance ID numbers along with the corresponding driver's license, and the full name, address, and email of deceased citizens. Prices are US$20.43 per 10 records or US$3.34 for one record.



New York fake ID the one & only!!

This is a listing for a 2013 NY fake ID from USASupply. As he has gone private, I (plasticA) am the only official authorized reseller. All of our products are known to be the best quality you can find on the web. We are the only vendor with a 100% success rate for 4+ years and counting. After years as being a top vendor on both SR, BMR and Evolution (along with other misc. markets) we have pe...

Sold by [redacted] - *140* sold since *Apr 5, 2015* Vendor Level 6 Trust Level 6

	Features		Features
Product class	Physical package	**Origin country**	United States
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	**FE Listing 100%**

	Bulk Discounts		
Bulk Discount	From qty 5 to 5	USD 180.00	0.2976 BTC
Bulk Discount	From qty 10 to 20	USD 170.00	0.2810 BTC

processing time + USPS Domesitc - 10 days - USD +6.00 / item

Purchase price: USD 200.00

Qty: 1 Buy Now Queue

0.3306 BTC / 20.5973 XMR

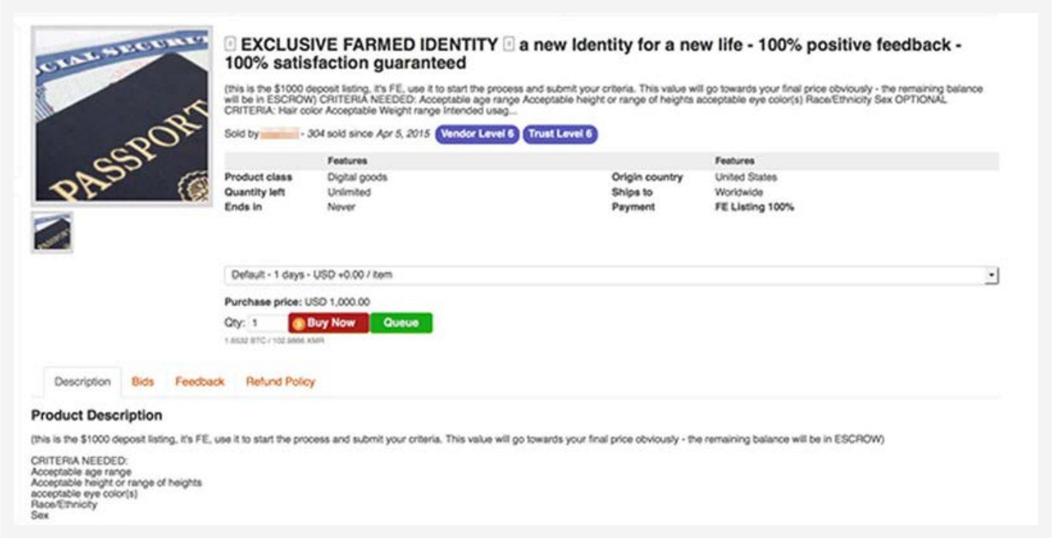
Product Description

This is a listing for a 2013 NY fake ID from USASupply. As he has gone private, I (plasticA) am the only official authorized reseller.

All of our products are known to be the best quality you can find on the web. We are the only vendor with a 100% success rate for 4+ years and counting. After years as being a top vendor on both SR, BMR and Evolution (along with other misc. markets) we have perfected our products to a level that has yet to be surpassed. You can find more detailed information on our procedures and products below. Please view our past feedback on the BMR & Evolution archives or the many misc. forums/markets on the darkweb/clearweb to see countless amounts of positive feedback on our products.

Figure 7. Advertisement for a New York driver's license from AlphaBay marketplace

Figure 7 shows how EHR PII information can be used to obtain official government documents, such as the driver's licenses above for New York City. The hacker sells multiple official government indentification documents such as passports and birth certificates. Prices for driver's licenses start at US$170.



EXCLUSIVE FARMED IDENTITY a new Identity for a new life - 100% positive feedback - 100% satisfaction guaranteed

(this is the $1000 deposit listing, it's FE, use it to start the process and submit your criteria. This value will go towards your final price obviously - the remaining balance will be in ESCROW) CRITERIA NEEDED: Acceptable age range Acceptable height or range of heights acceptable eye color(s) Race/Ethnicity Sex OPTIONAL CRITERIA: Hair color Acceptable Weight range Intended usag...

Sold by [redacted] - 304 sold since Apr 5, 2015 Vendor Level 6 Trust Level 6

	Features		Features
Product class	Digital goods	Origin country	United States
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	FE Listing 100%

Default - 1 days - USD +0.00 / item

Purchase price: USD 1,000.00

Qty: 1

1.8532 BTC / 102.9866 XMR

Product Description

(this is the $1000 deposit listing, it's FE, use it to start the process and submit your criteria. This value will go towards your final price obviously - the remaining balance will be in ESCROW)

CRITERIA NEEDED:
Acceptable age range
Acceptable height or range of heights
acceptable eye color(s)
Race/Ethnicity
Sex

Figure 8. An AlphaBay advertisement that sells new identities using stolen data

Meanwhile, this screenshot above also shows the hacker selling a farmed identity. Farmed identities are created through the use of stolen personal data that includes Social Security numbers, dates of birth, education records, employment records, health insurance, car insurance and passports from individuals that are no longer using the information–which are usually dead people. Once EHRs have been collected, cybercriminals essentially have a database full of stolen information that they can sell at a high price anytime and in any configuration that sells best on the underground market. The minimum price of one farmed identity starts at US$1,000. Cybercriminals can purchase add-ons from the vendors such as birth certificates and passports.

How do Criminals Make Use of Electronic Health Records?

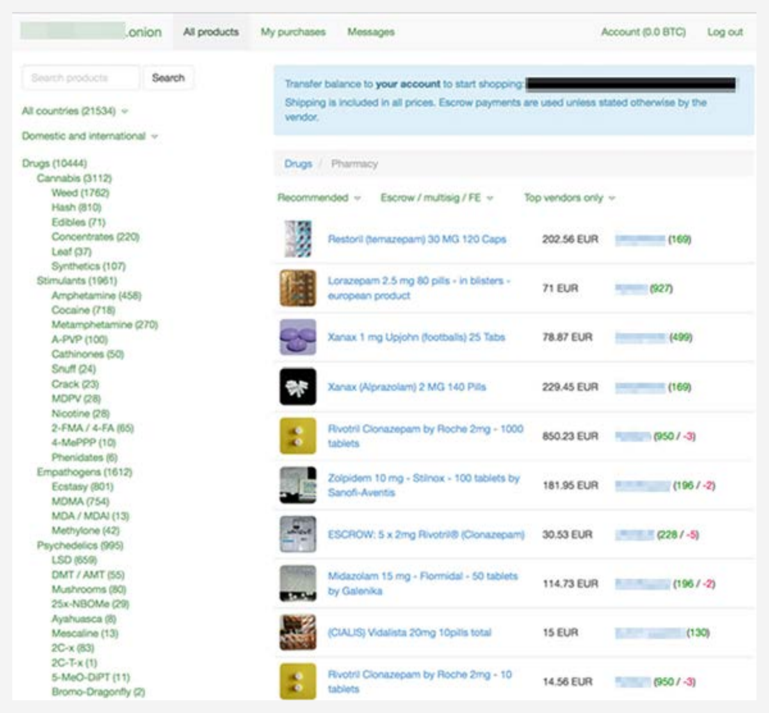
Because of the special nature of the information found in EHRs, cybercriminals are able to offer niche products and services by combining certain data found in an EHR. These products and services are:

- Prescription information that can be used for the procurement of drugs
- Irreplaceable PII, such as Social Security numbers and dates of birth, can be used to create fake identities
- PII such as Social Security numbers and Medicare insurance ID are used to obtain medical insurance
- Birth certificates can be created with stolen medical records and personal data like birthdates
- A combination of Social Security numbers and addresses can help cybercriminals file fraudulent tax returns

Drug Procurement

Purchasing EHR profiles with prescription information can help cybercriminals order prescription drugs through mail-order programs used by the health insurance provider. Later on, these medications can be sold in Dark Web marketplaces for a large profit. By having the medical ID, a cybercriminal can create or update the address on file for the profile they have purchased and then send the medication to their homes by using the credit card information stored on file from the original account holder. Sales of prescription drugs are popular in multiple Dark Web marketplaces.

According to Surescripts, an online software that supports e-prescription, electronic prescribing of controlled substances has increased 7.5 times between 2014 and 2015. Some states, such as New York, created mandates where all prescriptions of controlled substances must be processed through e-prescribing software. The survey found that between 3% and 9% of drug diversions occurred because of forged and/or stolen paper prescription. Over 77% of prescriptions have gone digital last year.[13]



[redacted].onion All products My purchases Messages Account (0.0 BTC) Log out

Search products | Search

All countries (21534)

Domestic and international

Drugs (10444)
- Cannabis (3112)
  - Weed (1762)
  - Hash (810)
  - Edibles (71)
  - Concentrates (220)
  - Leaf (37)
  - Synthetics (107)
- Stimulants (1961)
  - Amphetamine (458)
  - Cocaine (718)
  - Metamphetamine (270)
  - A-PVP (100)
  - Cathinones (50)
  - Snuff (24)
  - Crack (23)
  - MDPV (28)
  - Nicotine (28)
  - 2-FMA / 4-FA (65)
  - 4-MePPP (10)
  - Phenidates (6)
- Empathogens (1612)
  - Ecstasy (801)
  - MDMA (754)
  - MDA / MDAI (13)
  - Methylone (42)
- Psychedelics (995)
  - LSD (659)
  - DMT / AMT (55)
  - Mushrooms (80)
  - 25x-NBOMe (29)
  - Ayahuasca (8)
  - Mescaline (13)
  - 2C-x (83)
  - 2C-T-x (1)
  - 5-MeO-DiPT (11)
  - Bromo-Dragonfly (2)

Transfer balance to **your account** to start shopping: [redacted]
Shipping is included in all prices. Escrow payments are used unless stated otherwise by the vendor.

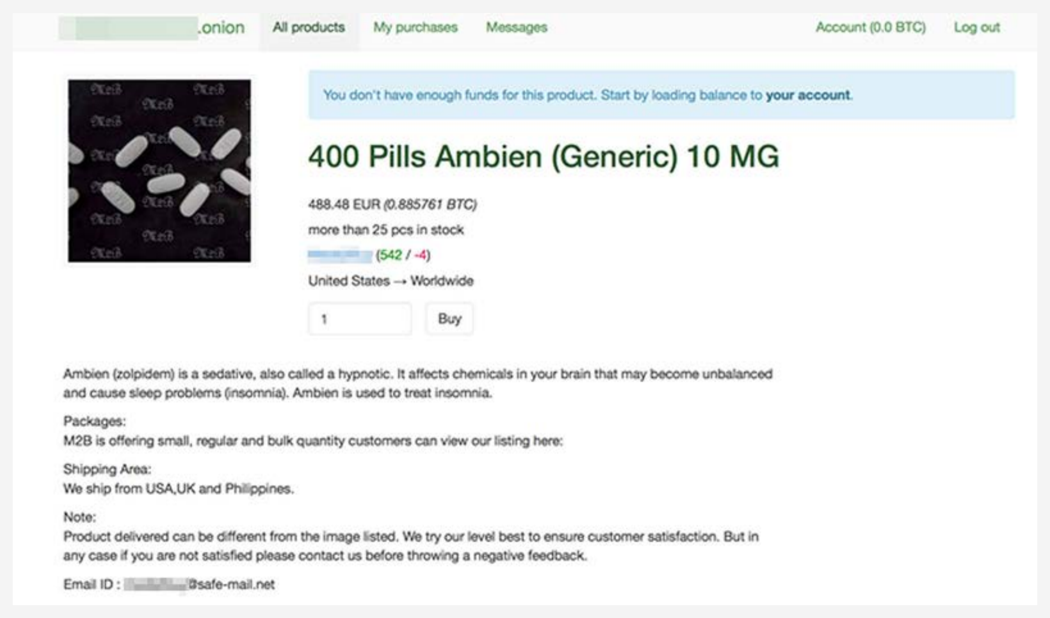
Drugs / Pharmacy

Recommended Escrow / multisig / FE Top vendors only

Restoril (temazepam) 30 MG 120 Caps	202.56 EUR	[redacted] (169)
Lorazepam 2.5 mg 80 pills - in blisters - european product	71 EUR	[redacted] (927)
Xanax 1 mg Upjohn (footballs) 25 Tabs	78.87 EUR	[redacted] (499)
Xanax (Alprazolam) 2 MG 140 Pills	229.45 EUR	[redacted] (169)
Rivotril Clonazepam by Roche 2mg - 1000 tablets	850.23 EUR	[redacted] (950 / -3)
Zolpidem 10 mg - Stilnox - 100 tablets by Sanofi-Aventis	181.95 EUR	[redacted] (196 / -2)
ESCROW: 5 x 2mg Rivotril® (Clonazepam)	30.53 EUR	[redacted] (228 / -5)
Midazolam 15 mg - Flormidal - 50 tablets by Galenika	114.73 EUR	[redacted] (196 / -2)
(CIALIS) Vidalista 20mg 10pills total	15 EUR	[redacted] (130)
Rivotril Clonazepam by Roche 2mg - 10 tablets	14.56 EUR	[redacted] (950 / -3)

Figure 9. Drug Enforcement Administration (DEA)-controlled drugs sold on Valhalla on 19 September 2016

Figure 9 shows Valhalla's section of medications that are available for purchase. This section includes controlled substances such as the anti-anxiety medications Xanax and Klonopin.



[redacted].onion All products My purchases Messages Account (0.0 BTC) Log out

You don't have enough funds for this product. Start by loading balance to **your account**.

400 Pills Ambien (Generic) 10 MG

488.48 EUR *(0.885761 BTC)*

more than 25 pcs in stock

[redacted] (542 / -4)

United States → Worldwide

1 Buy

Ambien (zolpidem) is a sedative, also called a hypnotic. It affects chemicals in your brain that may become unbalanced and cause sleep problems (insomnia). Ambien is used to treat insomnia.

Packages:
M2B is offering small, regular and bulk quantity customers can view our listing here:

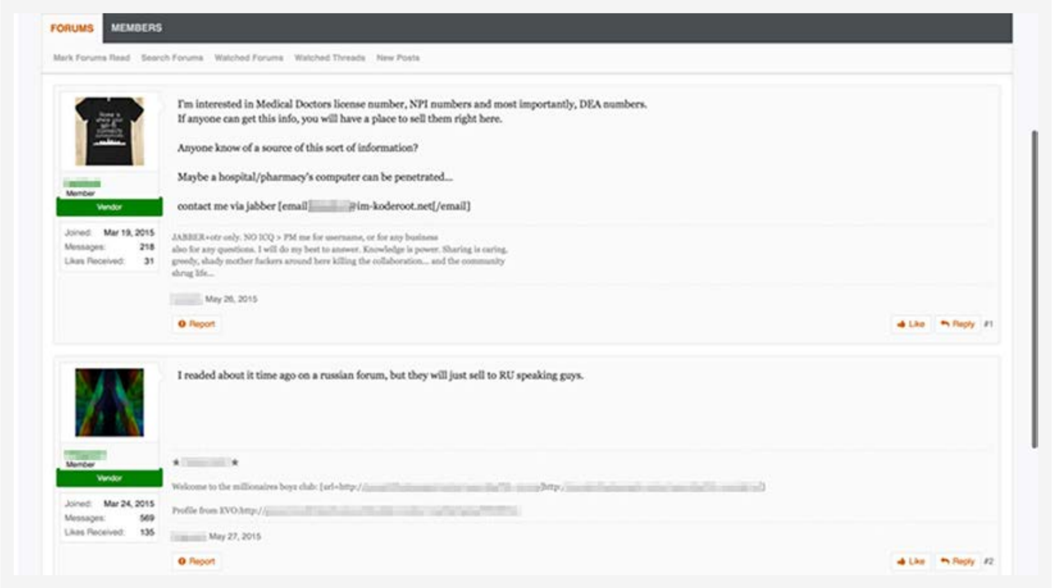
Shipping Area:
We ship from USA,UK and Philippines.

Note:
Product delivered can be different from the image listed. We try our level best to ensure customer satisfaction. But in any case if you are not satisfied please contact us before throwing a negative feedback.

Email ID : [redacted]@safe-mail.net

Figure 10. Advertisement for Ambien medication on Vahalla

Figure 10 is an advertisement for Ambien, a controlled medication that is usually prescribed to help people with sleep disorders. Ambien is also known to be abused by many users. The number of Ambien-related emergency visits in the U.S. has gone up according to a report from the Substance Abuse and Mental Health Services Administration (SAMHSA). It is estimated that between 2006 and 2011, 38 million Ambien prescriptions were written. A survey also revealed that there were more than half a million people in the U.S. who abused Ambien.[14]



[redacted]

I'm interested in Medical Doctors license number, NPI numbers and most importantly, DEA numbers.
If anyone can get this info, you will have a place to sell them right here.

Anyone know of a source of this sort of information?

Maybe a hospital/pharmacy's computer can be penetrated...

contact me via jabber [email][redacted]@im-koderoot.net[/email]

JABBER+otr only. NO ICQ > PM me for username, or for any business
also for any questions. I will do my best to answer. Knowledge is power. Sharing is caring.
greedy, shady mother fuckers around here killing the collaboration... and the community
shrug life...

[redacted] May 26, 2015

[redacted]

I readed about it time ago on a russian forum, but they will just sell to RU speaking guys.

★ [redacted] ★

Welcome to the millionaires boys club: [url=http://[redacted]]http://[redacted]]

Profile from EVO:http://[redacted]

[redacted] May 27, 2015

Figure 11. AlphaBay forum discussion asking for DEA numbers in order to obtain fraudulent prescription

In the figure above, a user can be seen asking members of AlphaBay for DEA numbers in order to obtain fraudulent prescriptions. Fraudulent prescriptions can be used to resell drugs on the Dark Web or for personal drug use.

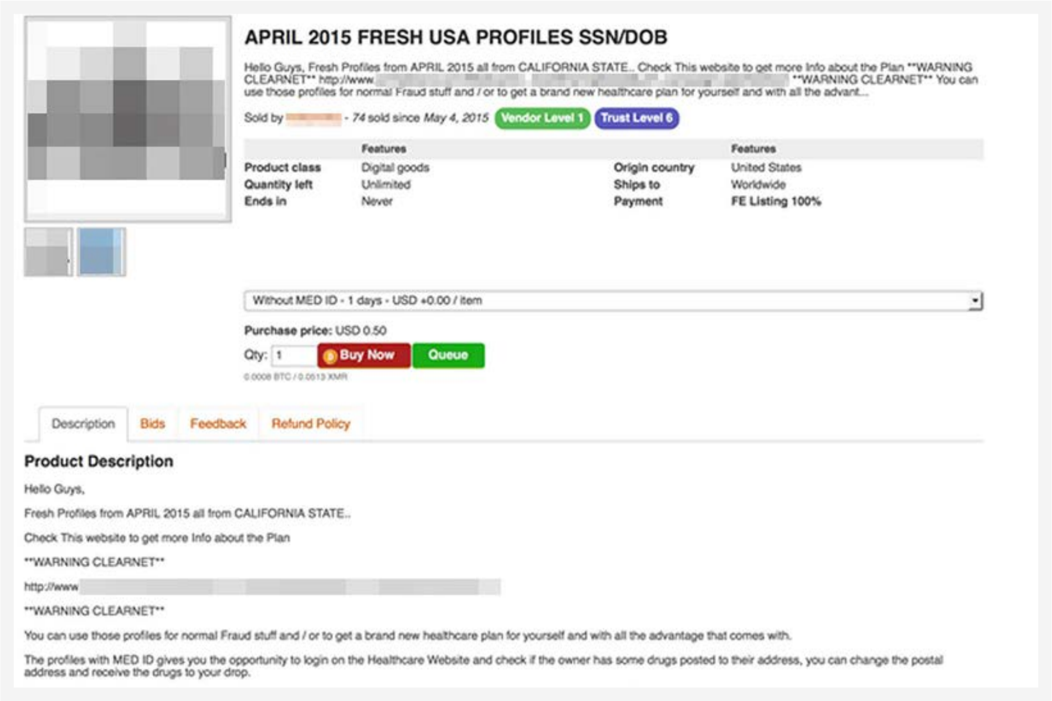
Identity Theft

A study by the Ponemon Institute in 2014 identified 500,000 as the number of victims of medical identity fraud. In 2015 those numbers rose to 22%, without adding the Anthem breach. In terms of resolving fraud issues, credit cards breaches have financial lability limited to US$50 per card. In the health industry, however, 65% of victims of medical identity theft had to pay an average of US$13,500 to resolve the crime–with costs covering the services of creditors and legal counsel. Credit cards can be easily cancelled and replaced but health care data such as Social Security numbers, and birthdates, are permanent–which means the data will live forever and that cybercriminals may reuse such information for a variety of purposes.[15]

According to the Consumer Financial Protection Bureau, roughly half of all collection accounts on credit reports are due to medical debt, which can be incurred by the other person using the stolen identity. A single collection debt account can make a credit score drop 50 to 100 points.[16] Credit bureaus will wait 180 days before adding medical debt to your report[17] but unlike credit card crimes medical identity theft can take more than three months after a crime has been committed to be reported and 30% will never know they are victims.

When a victim's medical ID is used by another person to receive health services, the EHR is also modified–sometimes affecting critical information such as a person's blood type, list of known allergies, and current medications. Detecting medical identity theft is not as easy as detecting credit card crimes. As a result, about 20% of victims received the wrong diagnosis or perhaps proper care was delayed because their EHR information was used and altered.[18]

Medical Insurance



APRIL 2015 FRESH USA PROFILES SSN/DOB

Hello Guys, Fresh Profiles from APRIL 2015 all from CALIFORNIA STATE.. Check This website to get more Info about the Plan **WARNING CLEARNET** http://www[redacted] **WARNING CLEARNET** You can use those profiles for normal Fraud stuff and / or to get a brand new healthcare plan for yourself and with all the advant...

Sold by [redacted] - *74 sold since May 4, 2015* Vendor Level 1 Trust Level 6

	Features		Features
Product class	Digital goods	**Origin country**	United States
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	**FE Listing 100%**

Without MED ID - 1 days - USD +0.00 / item

Purchase price: USD 0.50

Qty: 1

0.0008 BTC / 0.0513 XMR

Product Description

Hello Guys,

Fresh Profiles from APRIL 2015 all from CALIFORNIA STATE..

Check This website to get more Info about the Plan

WARNING CLEARNET

http://www[redacted]

WARNING CLEARNET

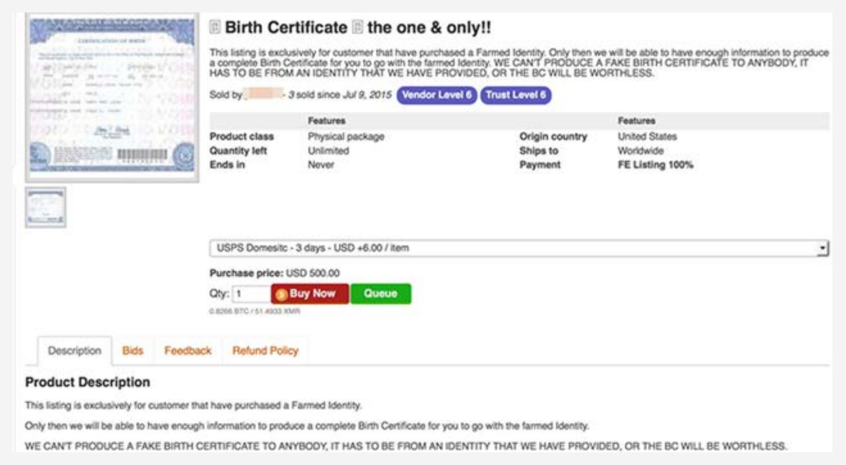
You can use those profiles for normal Fraud stuff and / or to get a brand new healthcare plan for yourself and with all the advantage that comes with.

The profiles with MED ID gives you the opportunity to login on the Healthcare Website and check if the owner has some drugs posted to their address, you can change the postal address and receive the drugs to your drop.

Figure 12. An Alphabay advertisement for California State Medicare Insurance Cards

In Figure 12, a hacker is seen selling individual profiles that contain Social Security numbers, dates of birth, and Medicare insurance ID numbers that can be used to obtain medical insurance. The hacker also happens to sell the profiles that have approved prescriptions in Los Angeles, California. Even though the information is from 2015, the vendor assures buyers that the medical information is still active. At only 50 cents per profile, cybercriminals can buy multiple profiles and perform several test purchases.

Birth Certificates



Birth Certificate the one & only!!

This listing is exclusively for customer that have purchased a Farmed Identity. Only then we will be able to have enough information to produce a complete Birth Certificate for you to go with the farmed Identity. WE CAN'T PRODUCE A FAKE BIRTH CERTIFICATE TO ANYBODY, IT HAS TO BE FROM AN IDENTITY THAT WE HAVE PROVIDED, OR THE BC WILL BE WORTHLESS.

Sold by [redacted] - 3 sold since *Jul 9, 2015* Vendor Level 6 Trust Level 6

	Features		Features
Product class	Physical package	Origin country	United States
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	FE Listing 100%

USPS Domesitc - 3 days - USD +6.00 / item

Purchase price: USD 500.00

Qty: 1 Buy Now Queue

0.8266 BTC / 51.4933 XMR

Product Description

This listing is exclusively for customer that have purchased a Farmed Identity.

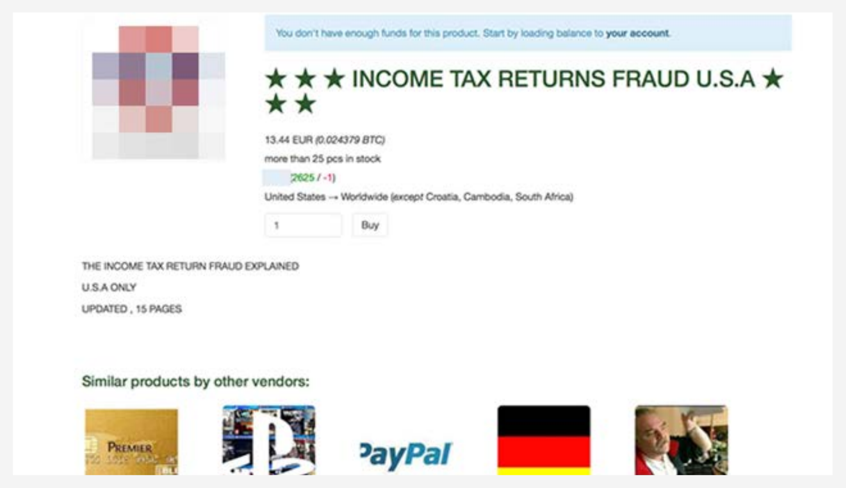
Only then we will be able to have enough information to produce a complete Birth Certificate for you to go with the farmed Identity.

WE CAN'T PRODUCE A FAKE BIRTH CERTIFICATE TO ANYBODY, IT HAS TO BE FROM AN IDENTITY THAT WE HAVE PROVIDED, OR THE BC WILL BE WORTHLESS.

Figure 13. An AlphaBay advertisement for birth certificates found on 15 September 2016

Using data stolen from medical records, birthdates can be obtained and sold individually to obtain a copy of a real birth certificate. In the above figure, we can see an advertisement for birth certificates starting at US$500 per person.

Fraudulent Tax Returns



You don't have enough funds for this product. Start by loading balance to **your account**.

★ ★ ★ INCOME TAX RETURNS FRAUD U.S.A ★ ★ ★

13.44 EUR *(0.024379 BTC)*

more than 25 pcs in stock

[redacted]2625 / -1)

United States → Worldwide (except Croatia, Cambodia, South Africa)

1 Buy

THE INCOME TAX RETURN FRAUD EXPLAINED

U.S.A ONLY

UPDATED , 15 PAGES

Similar products by other vendors:

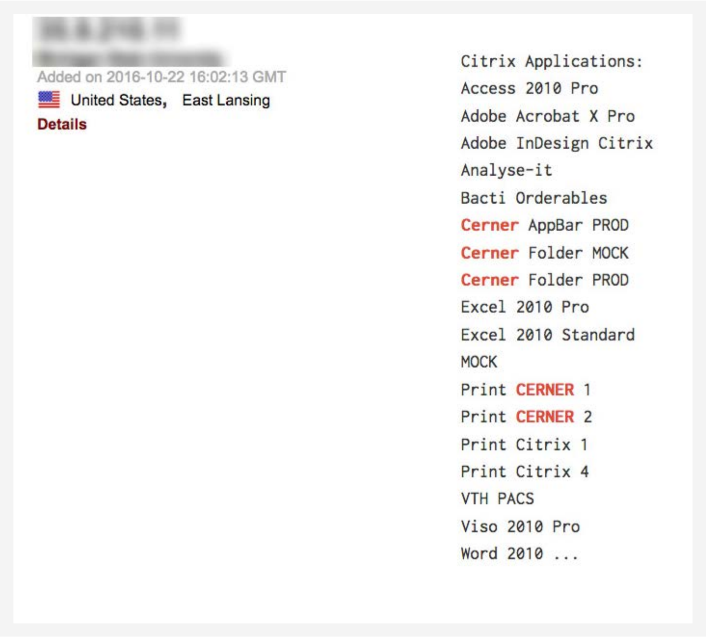
Figure 14. An advertisement found in Valhalla offering services to commit income tax fraud

In the last two years the number of cybercriminals committing tax fraud, through the use of stolen personal data found in EHRs, increased.[19] As a result, Turbo Tax–a program used for filing taxes in the U.S.–had to temporarily suspend state tax filings to investigate the increasing number of fraud cases. The image above shows the vendor selling 25 income tax returns at US$15 per tax return.

Exposed Healthcare Systems

Internet-connected devices revealing EHR systems

For this research, we conducted queries on Shodan, a search engine that indexes internet-connected devices. Search results revealed EHR systems, healthcare facilities, medical equipment, and networks that are vulnerable to cybercriminals. As part of the process, Shodan gathers the banner that displays the current services running on the device. Sometimes these banners can provide version numbers of the software running on a device. The banner also displays meta-data such as operating systems, system file structures, folders, IP addresses, geographical locations, hostnames and more.[20]



[redacted]

Added on 2016-10-22 16:02:13 GMT

United States, East Lansing

Details

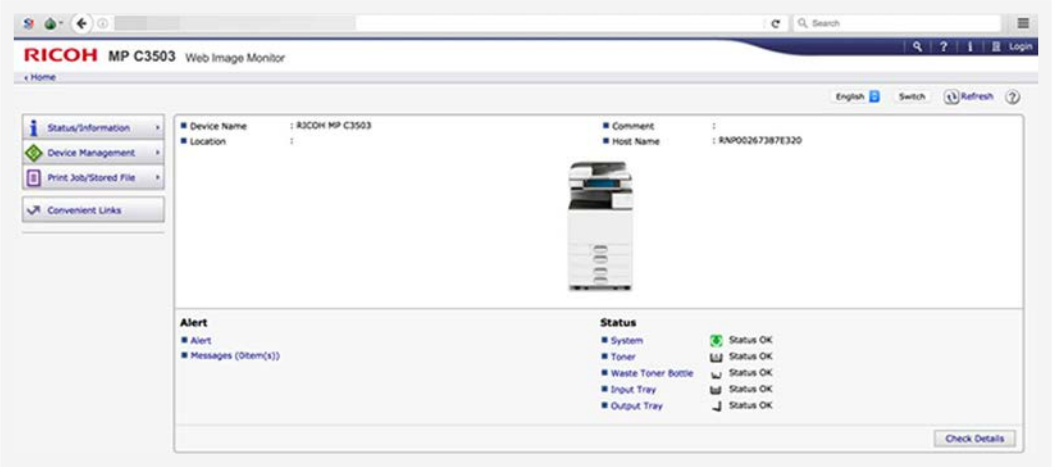
```
Citrix Applications:
Access 2010 Pro
Adobe Acrobat X Pro
Adobe InDesign Citrix
Analyse-it
Bacti Orderables
Cerner AppBar PROD
Cerner Folder MOCK
Cerner Folder PROD
Excel 2010 Pro
Excel 2010 Standard
MOCK
Print CERNER 1
Print CERNER 2
Print Citrix 1
Print Citrix 4
VTH PACS
Viso 2010 Pro
Word 2010 ...
```

Figure 15. A search on Shodan for the Cerner EHR software displays the version numbers, folders, and the software running on the devices as of 24 October 2016.

Shodan allows searches that target doctors with specializations like dermatologists and oncologists. Shodan is also able to search by services or programs running on target computers, EHR vendors, and VPNs. Searches of connected printers and webcams can also be conducted. To log in and make use of these printers and/or webcams, cybercriminals may use websites such as Datarecovery.com and Defaultpasswords.com to see if default passwords were never changed. Hundreds of applications are known to be deployed with default passwords, and are not always changed before they are plugged into a network.

Unsecured Devices

Having unsecured IoT devices in both healthcare institutions, as well as offices of EHR developers, can leave devices vulnerable to attacks. Exploitation of the Universal Plug and Play Protocol (UPnP) can give cybercriminals access to these devices. In turn, attackers may change the configuration of these devices in a way that lets them collect information. These unsecured devices can also be used as a gateway for cybercriminals to break into their target's network.[21]



- Device Name : RICOH MP C3503
- Location :
- Comment :
- Host Name : RNP00267387E320

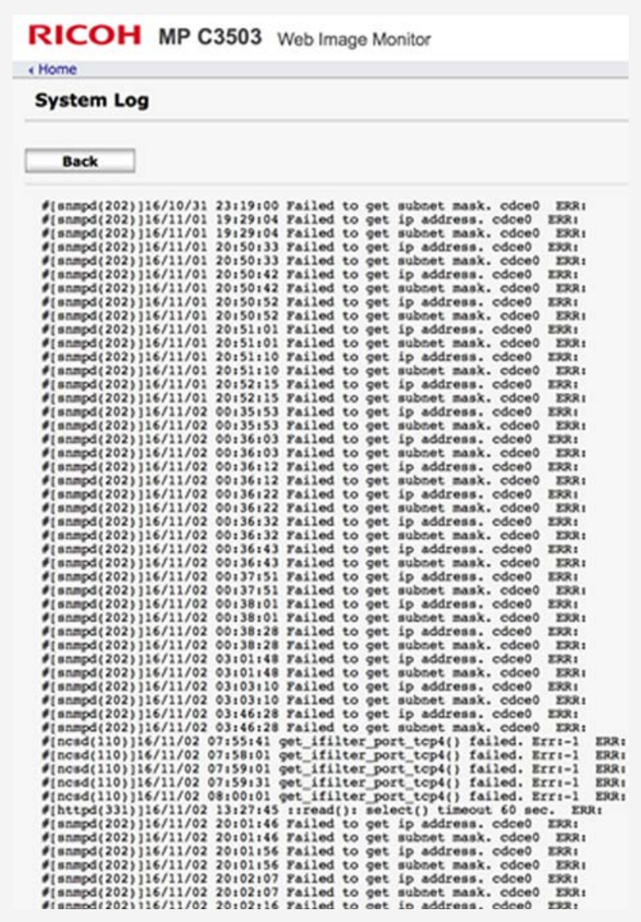
Alert

- Alert
- Messages (0item(s))

Status

- System Status OK
- Toner Status OK
- Waste Toner Bottle Status OK
- Input Tray Status OK
- Output Tray Status OK

Figure 16. Unsecured Ricoh printer being used at a healthcare organization



RICOH MP C3503 Web Image Monitor

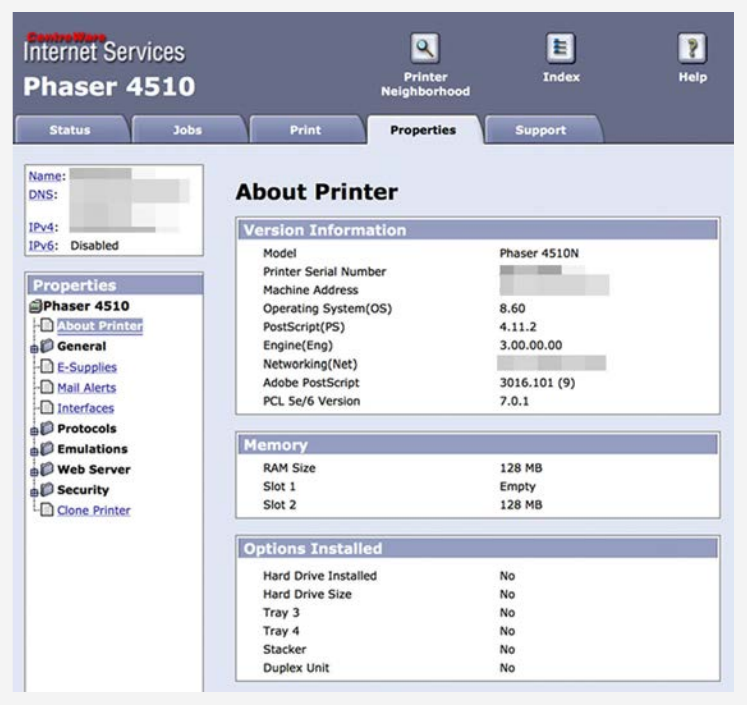
‹ Home

System Log

Back

```
#[snmpd(202)]16/10/31 23:19:00 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/01 19:29:04 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/01 19:29:04 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/01 20:50:33 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/01 20:50:33 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/01 20:50:42 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/01 20:50:42 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/01 20:50:52 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/01 20:50:52 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/01 20:51:01 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/01 20:51:01 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/01 20:51:10 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/01 20:51:10 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/01 20:52:15 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/01 20:52:15 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 00:35:53 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 00:35:53 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:03 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:03 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:12 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:12 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:22 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:22 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:32 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:32 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:43 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 00:36:43 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 00:37:51 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 00:37:51 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 00:38:01 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 00:38:01 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 00:38:28 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 00:38:28 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 03:01:48 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 03:01:48 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 03:03:10 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 03:03:10 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 03:46:28 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 03:46:28 Failed to get subnet mask. cdce0  ERR:
#[ncsd(110)]16/11/02 07:55:41 get_ifilter_port_tcp4() failed. Err:-1  ERR:
#[ncsd(110)]16/11/02 07:58:01 get_ifilter_port_tcp4() failed. Err:-1  ERR:
#[ncsd(110)]16/11/02 07:59:01 get_ifilter_port_tcp4() failed. Err:-1  ERR:
#[ncsd(110)]16/11/02 07:59:31 get_ifilter_port_tcp4() failed. Err:-1  ERR:
#[ncsd(110)]16/11/02 08:00:01 get_ifilter_port_tcp4() failed. Err:-1  ERR:
#[httpd(331)]16/11/02 13:27:45 ::read(): select() timeout 60 sec.  ERR:
#[snmpd(202)]16/11/02 20:01:46 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 20:01:46 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 20:01:56 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 20:01:56 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 20:02:07 Failed to get ip address. cdce0  ERR:
#[snmpd(202)]16/11/02 20:02:07 Failed to get subnet mask. cdce0  ERR:
#[snmpd(202)]16/11/02 20:02:16 Failed to get ip address. cdce0  ERR:
```

Figure 17. A screenshot of the system log and network information from an exposed Ricoh Printer



Name: [redacted]
DNS: [redacted]
IPv4: [redacted]
IPv6: Disabled

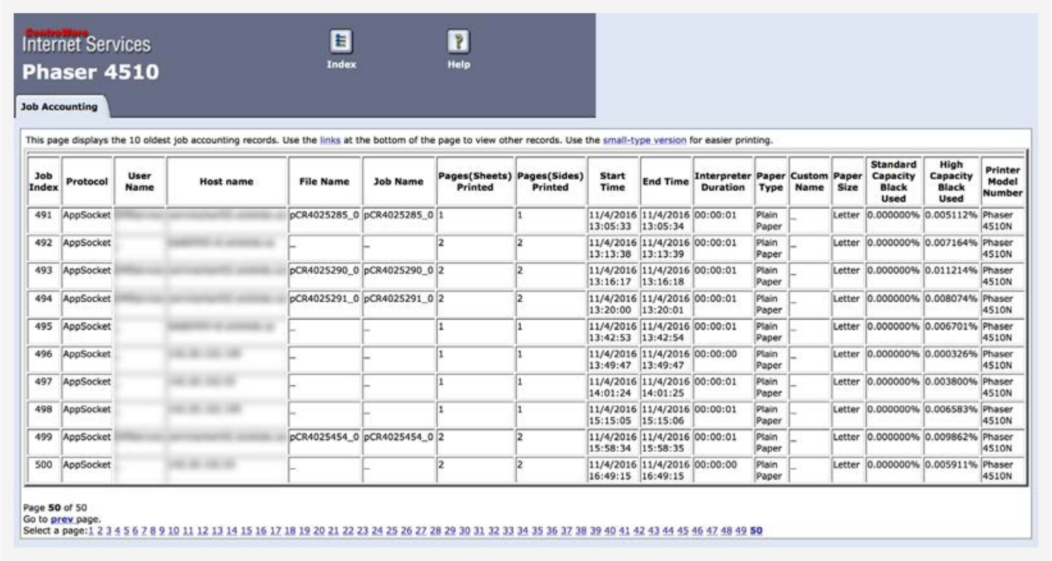
About Printer

Version Information	
Model	Phaser 4510N
Printer Serial Number	[redacted]
Machine Address	[redacted]
Operating System(OS)	8.60
PostScript(PS)	4.11.2
Engine(Eng)	3.00.00.00
Networking(Net)	[redacted]
Adobe PostScript	3016.101 (9)
PCL 5e/6 Version	7.0.1

Memory	
RAM Size	128 MB
Slot 1	Empty
Slot 2	128 MB

Options Installed	
Hard Drive Installed	No
Hard Drive Size	No
Tray 3	No
Tray 4	No
Stacker	No
Duplex Unit	No

Figure 18. A printer’s control panel of a hospital

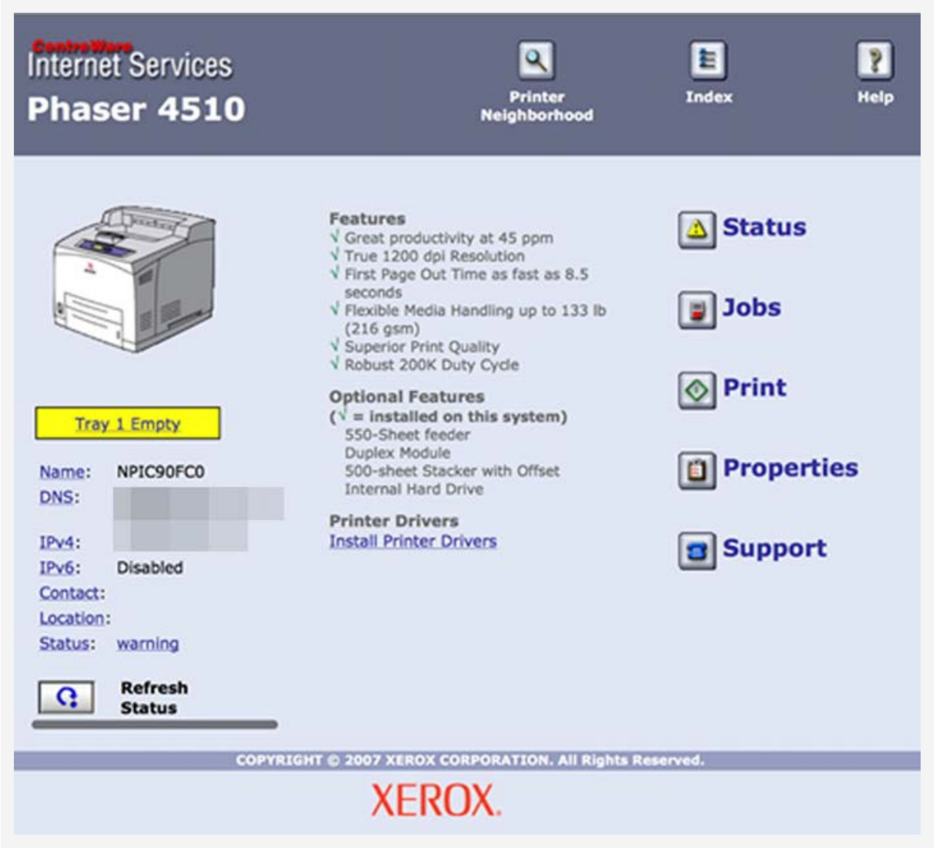


This page displays the 10 oldest job accounting records. Use the links at the bottom of the page to view other records. Use the small-type version for easier printing.

Job Index	Protocol	User Name	Host name	File Name	Job Name	Pages(Sheets) Printed	Pages(Sides) Printed	Start Time	End Time	Interpreter Duration	Paper Type	Custom Name	Paper Size	Standard Capacity Black Used	High Capacity Black Used	Printer Model Number
491	AppSocket	[redacted]	[redacted]	pCR4025285_0	pCR4025285_0	1	1	11/4/2016 13:05:33	11/4/2016 13:05:34	00:00:01	Plain Paper	_	Letter	0.000000%	0.005112%	Phaser 4510N
492	AppSocket		[redacted]	_	_	2	2	11/4/2016 13:13:38	11/4/2016 13:13:39	00:00:01	Plain Paper	_	Letter	0.000000%	0.007164%	Phaser 4510N
493	AppSocket	[redacted]	[redacted]	pCR4025290_0	pCR4025290_0	2	2	11/4/2016 13:16:17	11/4/2016 13:16:18	00:00:01	Plain Paper	_	Letter	0.000000%	0.011214%	Phaser 4510N
494	AppSocket	[redacted]	[redacted]	pCR4025291_0	pCR4025291_0	2	2	11/4/2016 13:20:00	11/4/2016 13:20:01	00:00:01	Plain Paper	_	Letter	0.000000%	0.008074%	Phaser 4510N
495	AppSocket		[redacted]	_	_	1	1	11/4/2016 13:42:53	11/4/2016 13:42:54	00:00:01	Plain Paper	_	Letter	0.000000%	0.006701%	Phaser 4510N
496	AppSocket		[redacted]	_	_	1	1	11/4/2016 13:49:47	11/4/2016 13:49:47	00:00:00	Plain Paper	_	Letter	0.000000%	0.000326%	Phaser 4510N
497	AppSocket		[redacted]	_	_	1	1	11/4/2016 14:01:24	11/4/2016 14:01:25	00:00:01	Plain Paper	_	Letter	0.000000%	0.003800%	Phaser 4510N
498	AppSocket		[redacted]	_	_	1	1	11/4/2016 15:15:05	11/4/2016 15:15:06	00:00:01	Plain Paper	_	Letter	0.000000%	0.006583%	Phaser 4510N
499	AppSocket	[redacted]	[redacted]	pCR4025454_0	pCR4025454_0	2	2	11/4/2016 15:58:34	11/4/2016 15:58:35	00:00:01	Plain Paper	_	Letter	0.000000%	0.009862%	Phaser 4510N
500	AppSocket		[redacted]	_	_	2	2	11/4/2016 16:49:15	11/4/2016 16:49:15	00:00:00	Plain Paper	_	Letter	0.000000%	0.005911%	Phaser 4510N

Page **50** of 50
Go to prev page.
Select a page:1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 **50**

Figure 19. A screenshot showing a printer’s history used at a healthcare organization



Name: NPIC90FC0
DNS: [redacted]
IPv4: [redacted]
IPv6: Disabled
Contact:
Location:
Status: warning

Features
√ Great productivity at 45 ppm
√ True 1200 dpi Resolution
√ First Page Out Time as fast as 8.5 seconds
√ Flexible Media Handling up to 133 lb (216 gsm)
√ Superior Print Quality
√ Robust 200K Duty Cycle

Optional Features
(√ = installed on this system)
550-Sheet feeder
Duplex Module
500-sheet Stacker with Offset
Internal Hard Drive

Printer Drivers
Install Printer Drivers

COPYRIGHT © 2007 XEROX CORPORATION. All Rights Reserved.

Figure 20. Printer specifications used at a healthcare organization

Remote Desktop Protocols

When administrators have log-in names as their real names in remote desktop protocols (RDP), malicious actors may resort to social engineering tactics to trick the target into giving information about their password. Attackers may also go through the target's social network accounts to guess the password.

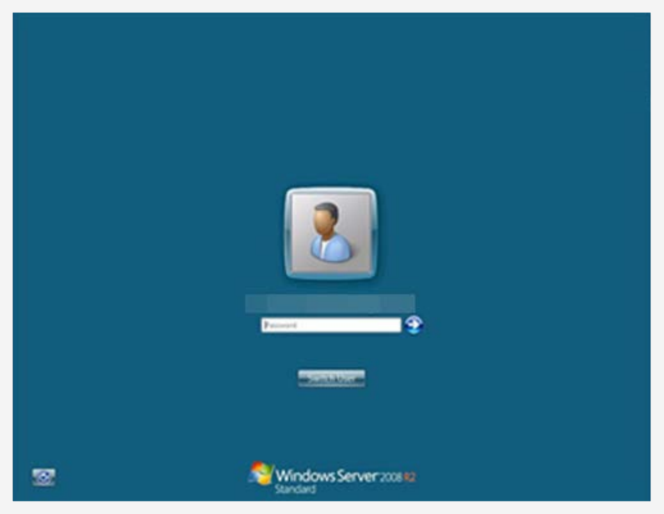


Figure 21. RDP of a healthcare organization

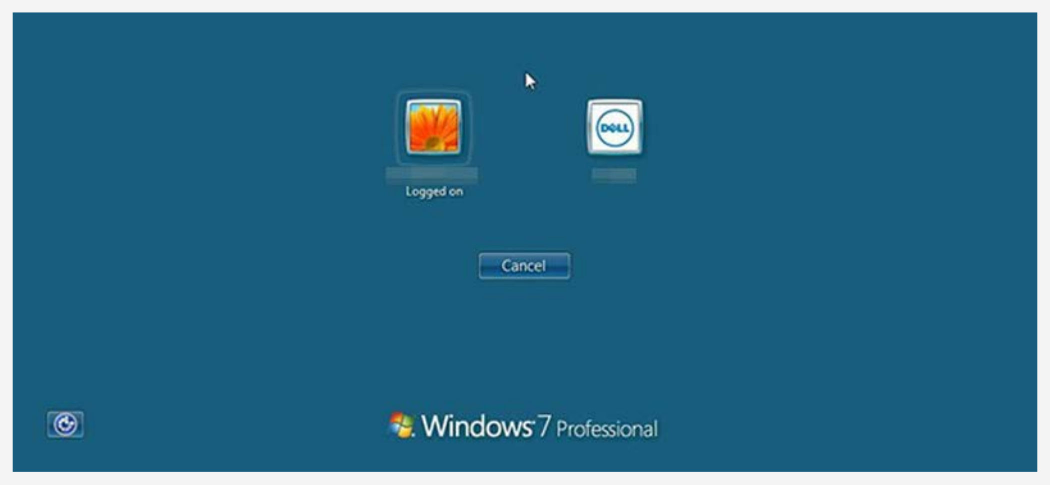
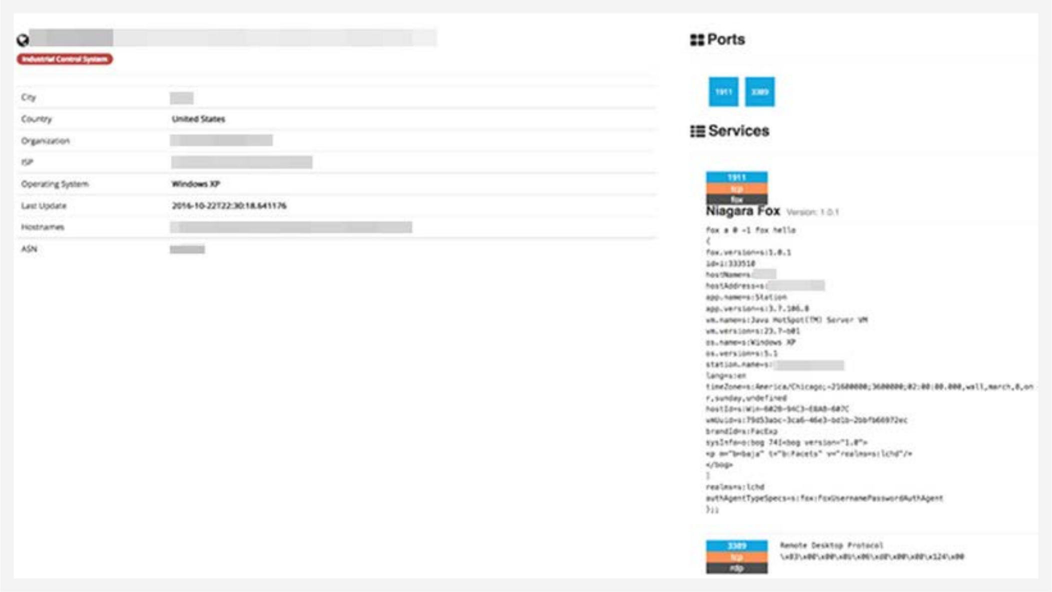


Figure 22. RDP for a healthcare organization

Industrial Control Systems

Healthcare organizations that use Industrial Control Systems (ICS) to run its facilities are exposed to some pitfalls. This includes an ICS running on legacy systems such as Windows® XP. Cybercriminals may also break into an ICS system by acquiring log-in credentials.



[redacted]

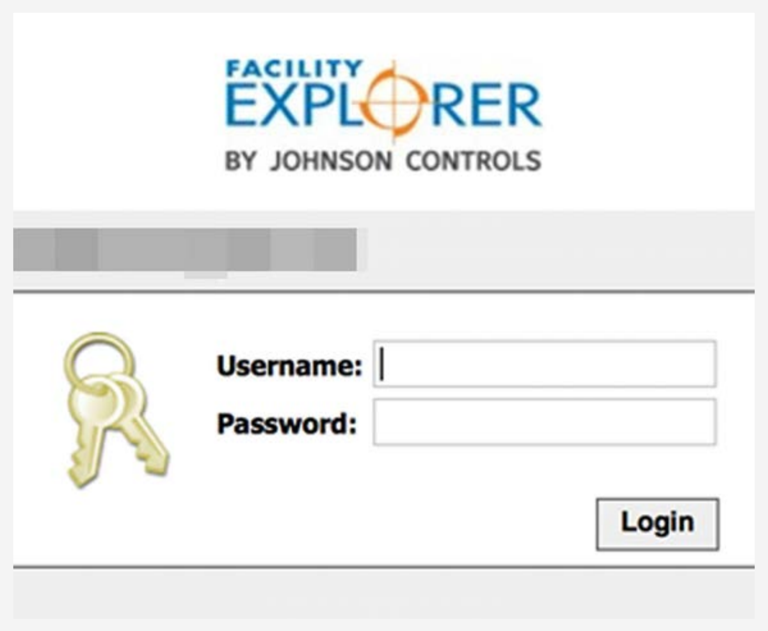
City	[redacted]
Country	United States
Organization	[redacted]
ISP	[redacted]
Operating System	Windows XP
Last Update	2016-10-22T22:30:18.641176
Hostnames	[redacted]
ASN	[redacted]

Niagara Fox Version: 1.0.1

```
fox a 0 -1 fox hello
{
fox.version=s:1.0.1
id=i:333510
hostName=s:[redacted]
hostAddress=s:[redacted]
app.name=s:Station
app.version=s:3.7.106.8
vm.name=s:Java HotSpot(TM) Server VM
vm.version=s:23.7-b01
os.name=s:Windows XP
os.version=s:5.1
station.name=s:[redacted]
lang=s:en
timeZone=s:America/Chicago;-21600000;3600000;02:00:00.000,wall,march,8,on
r,sunday,undefined
hostId=s:Win-6020-94C3-E8A8-607C
vmUuid=s:79d53abc-3ca6-46e3-bd1b-2bbfb66972ec
brandId=s:FacExp
sysInfo=o:bog 741<bog version="1.0">
<p m="b=baja" t="b:Facets" v="realms=s:lchd"/>
</bog>
}
realms=s:lchd
authAgentTypeSpecs=s:fox:FoxUsernamePasswordAuthAgent
};;
```

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

Figure 23. A screenshot showing that a healthcare organization's ICS is running on Windows XP

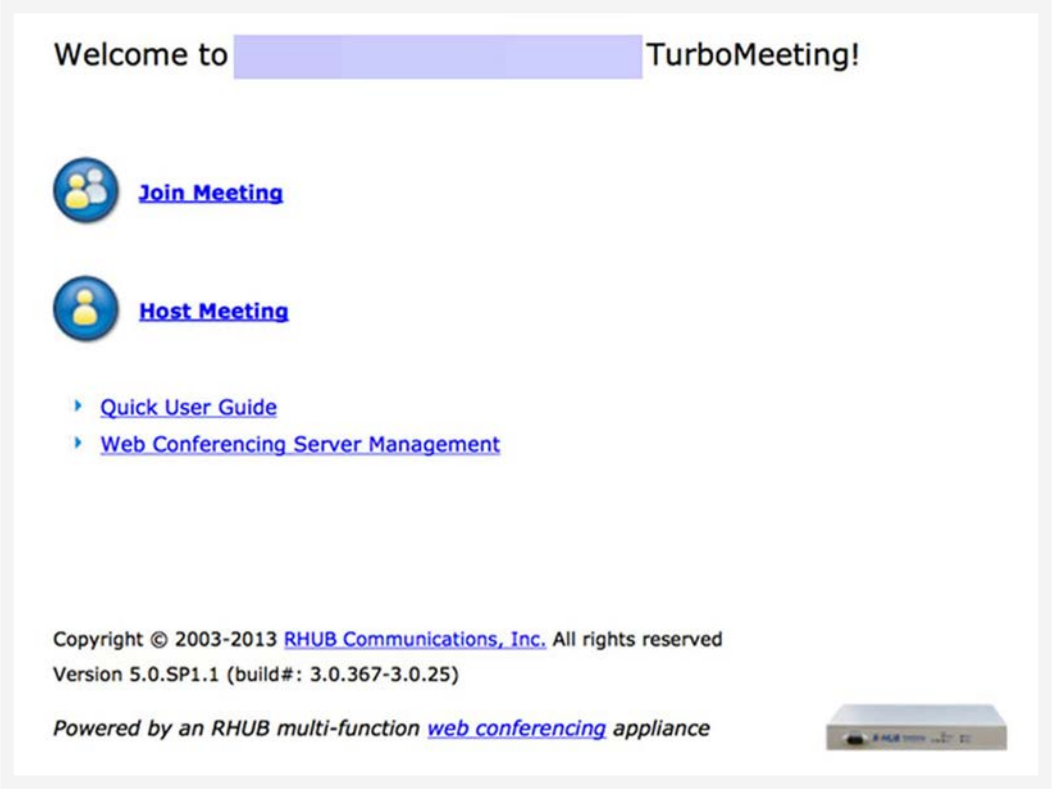


[redacted]

Figure 24. Healthcare Organization's Server ICS login

Communication Tools and Other Online Vulnerabilities

Attackers are constantly on the lookout for ways to break into their target's database. Meanwhile healthcare institutions or EHR software companies may host meetings using third party software; there are still a lot of organizations that use their own websites to host and join meetings. However, if these meetings use a default password, hackers can access these meetings too. Since most systems do not vet if the person listed is who they are, the host of the meeting may not notice if there are unauthorized people listening to their calls.



Welcome to [redacted] TurboMeeting!

Join Meeting

Host Meeting

- Quick User Guide
- Web Conferencing Server Management

Copyright © 2003-2013 RHUB Communications, Inc. All rights reserved

Version 5.0.SP1.1 (build#: 3.0.367-3.0.25)

Powered by an RHUB multi-function web conferencing appliance

Figure 25. Exposed web conference meeting site that allows other users to host meetings at a healthcare organization

For meetings that utilize conferencing systems, attackers can turn those exposed systems or equipment into video-surveillance units. Then hackers can use them to snoop for information, record video conferences, or even privately or publicly broadcast a meeting.

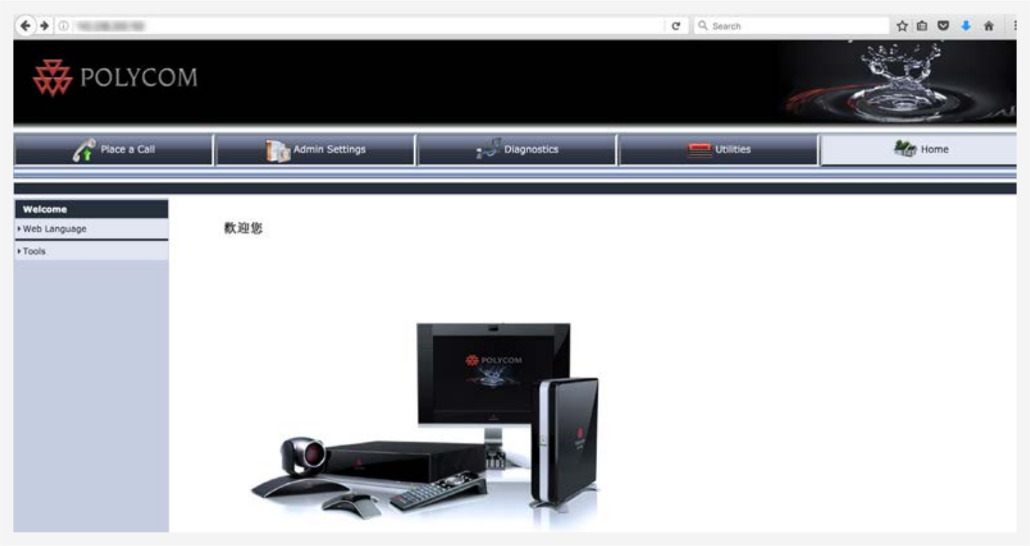
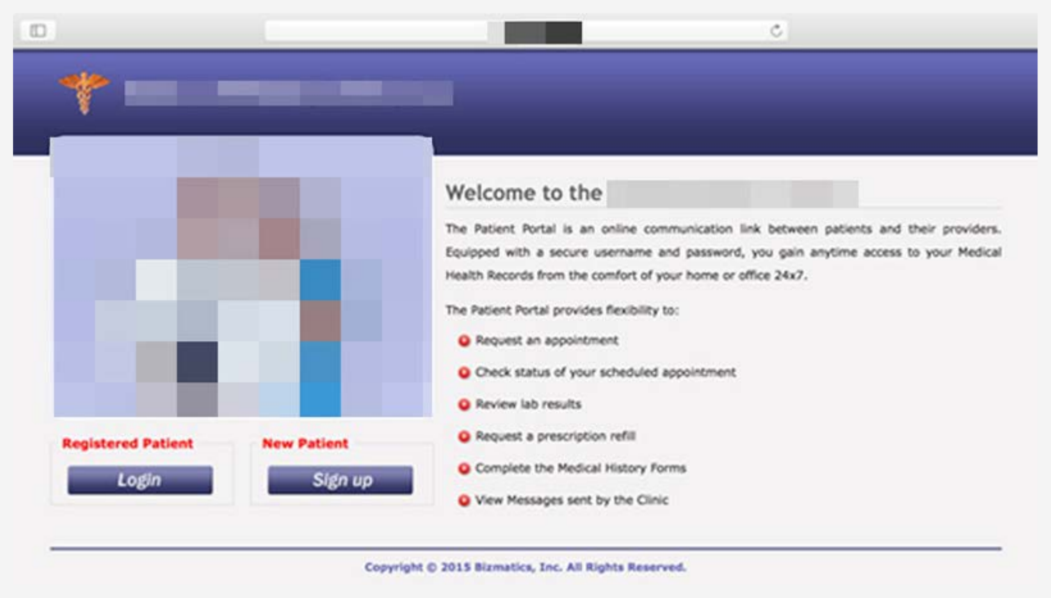


Figure 26. Exposed Polycom conference video from a healthcare organization

Some EHRs can be accessed through the IP address of the vendor. Hackers can use brute force attacks against the log-in credentials to break into the system. Sites that store or give access to EHR should ideally be accessible through an internal network or VPN.



Welcome to the

The Patient Portal is an online communication link between patients and their providers. Equipped with a secure username and password, you gain anytime access to your Medical Health Records from the comfort of your home or office 24x7.

The Patient Portal provides flexibility to:

- Request an appointment
- Check status of your scheduled appointment
- Review lab results
- Request a prescription refill
- Complete the Medical History Forms
- View Messages sent by the Clinic

Copyright © 2015 Bizmatics, Inc. All Rights Reserved.

Figure 27. PrognoCIS exposing the EHR system’s log-in page

Exposed U.S. Hospitals

Shodan U.S. scan data for February 2017 contains a total of 123,098,618 records, with 36,116 records being related to healthcare. Out of the 36,116 healthcare-related records, 6,502 originated from the top 10 U.S. cities with exposed healthcare facilities. The data also showed that 14,327 healthcare facilities had SSL certificates that were up-to-date while 1,067 were expired.

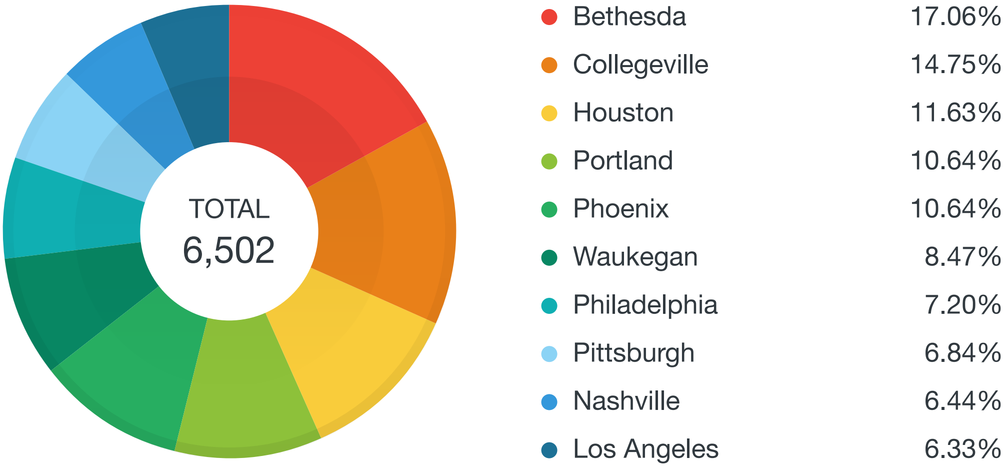


Figure 28. Top cities in the U.S. with exposed healthcare facilities

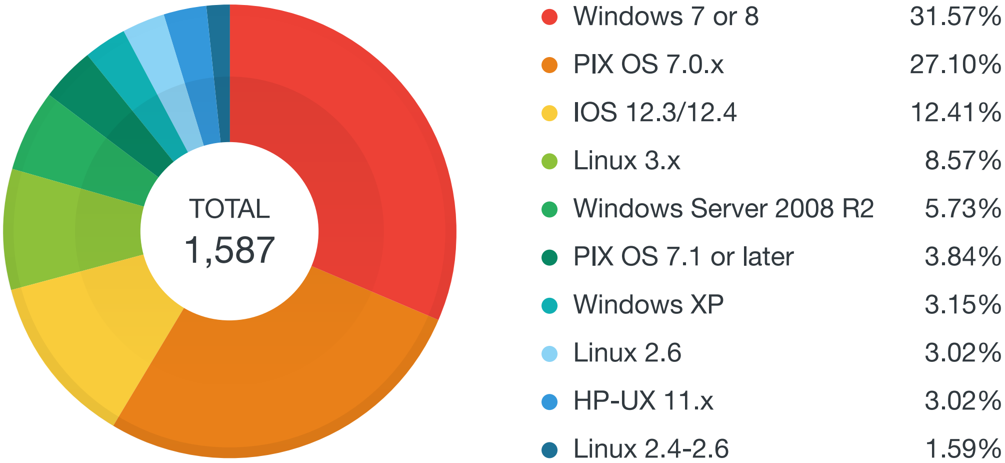


Figure 29. Top operating systems used in exposed U.S. healthcare institutions

Exposed Global Hospitals

As of February 2017, global data from Shodan contains a total of 240,933,715 records. Out of those records, 101,394 are healthcare-related.

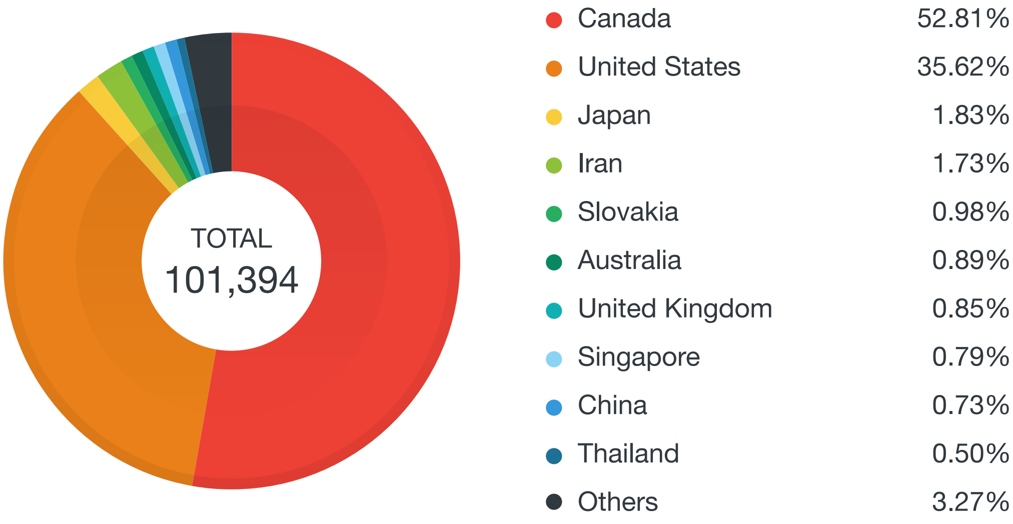


Figure 30. Countries with the highest number of exposed healthcare organizations

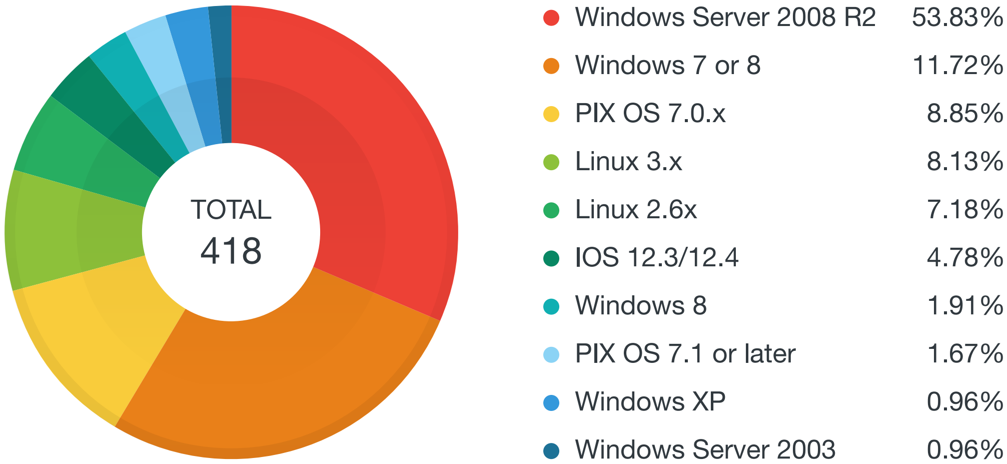


Figure 31. Top exposed operating systems globally

Microsoft ended support for Windows XP two years ago and yet there are still several hospitals using Windows XP. These hospitals are at risk of attacks exploiting currently existing vulnerabilities. Since Windows XP will no longer receive any update, networks using this OS are at risk of being attacked by malicious actors.

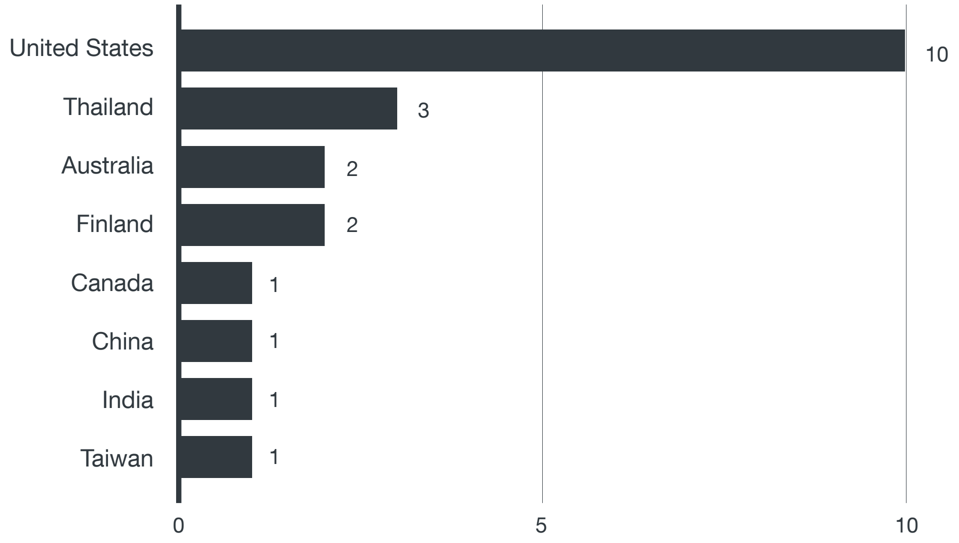


Figure 32. Countries with the highest number of devices affected by the Heartbleed vulnerability (CVE 2014-0160)

Although it has been two years since the discovery of a major vulnerability called Heartbleed, there are still numerous devices that remain unpatched. The U.S. had the highest number of devices that were affected by Heartbleed.

The Heartbleed bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows an attacker to read the memory of systems using certain versions of OpenSSL, potentially allowing attackers to access usernames, passwords, or even the secret cryptographic keys of the server used for SSL. Obtaining these keys would allow malicious actors to observe all types of communication in a system, thus allowing further exploits to take place.[22]

Conclusion

Healthcare organizations are still a prime target for cybercriminals. In this paper we have taken a closer look at the reason behind this and in what ways healthcare organizations are vulnerable. In our research we singled out two main areas: 1) the fate of stolen documents after a data breach and 2) a new dimension of attacks that could be brought about via exposed devices that are internet-connected and can be theoretically exploited by anyone ill-minded on the internet.

EHRs are being peddled in the cyber underground, often sold either in bulk or in portions. The information held in these EHRs can be used to obtain illegal products such as prescription drugs, fake identities, or create fake documents such as fraudulent tax returns. Using the Shodan search engine, we also explored which internet-connected devices can be easily found online by anyone. Cybercriminals may use these devices to break into existing networks of EHR vendors and healthcare systems.

EHR software holds invaluable patient data that should be kept private at all costs. Providers must focus on securing their products and systems, which includes the EHRs that they store. To do this, healthcare providers must take stock of all IoT devices connected to the network and make sure that these devices are patched and are no longer using the default password. Vendors of EHR software need to provide strong encryption for stored data in order to reduce the impact of data breaches. As for accessing data remotely, healthcare institutions must improve their authentication processes to avoid any unauthorized access.

Healthcare institutions using EHR software should actively secure EHRs. This can be done by educating staff members, who access EHRs, on the basics of cybersecurity and risk management. These institutions may also seek assistance from security companies to protect data stored within their facilities. Having a robust network security may also lessen the chances of attackers using the institution's own network as a gateway into the EHR provider's network.

Appendix

Data Breaches in the Healthcare Sector

We have mentioned how prominent data breaches are in the healthcare sector, how they affect the people when their EHRs are stolen, and how cybercriminals are going after EHR for its high value. To properly describe the situation of the healthcare sector in terms of cybersecurity, it is also important to know the frequency of attacks targeting the sector, the magnitude of a large-scale attack, as well as various cases of a data breaches outside the U.S.

All healthcare data breaches in this paper were collected from the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights Breach Notification.[1] Only breaches that involved patient health data affecting 500 or more individuals are reported due to the Health Information Technology for Economic and Clinical Health Act (HITECH). HHS identifies breaches by several methods. It also identifies if the breach was caused by loss, theft, unknown sources, unauthorized access/disclosure, hacking/IT incident, improper disposal and other. The data collected in this report is from January 2012 to September 2016. Some reports of breaches may be missing as detection and notification to HHS may take several months.

According to Verizon's 2016 Data Breach Investigations Report (DBIR) the time to identify and respond to a breach incident has gotten worse since 2014. Attackers are getting quicker at compromising their victims yet detection and discovery of the breach are lagging behind several months. Most companies depend on third parties to detect breaches.[23] It is estimated that cyber attacks against hospitals, clinics and doctors cost the U.S. healthcare industry more than US$6 billion a year, with an average data breach costing a hospital US$2.1 million. [1]

Notable 2016 U.S. Breaches

From October 2009 to December 2016, the Office for Civil Rights logged 1,798 data breach incidents involving healthcare organizations. As of December 2016, the breach reporting includes:

- 480 Unauthorized Access/Disclosure
- 266 Hacking/IT
- 795 Theft
- 154 Loss
- 63 Improper disposal [1]

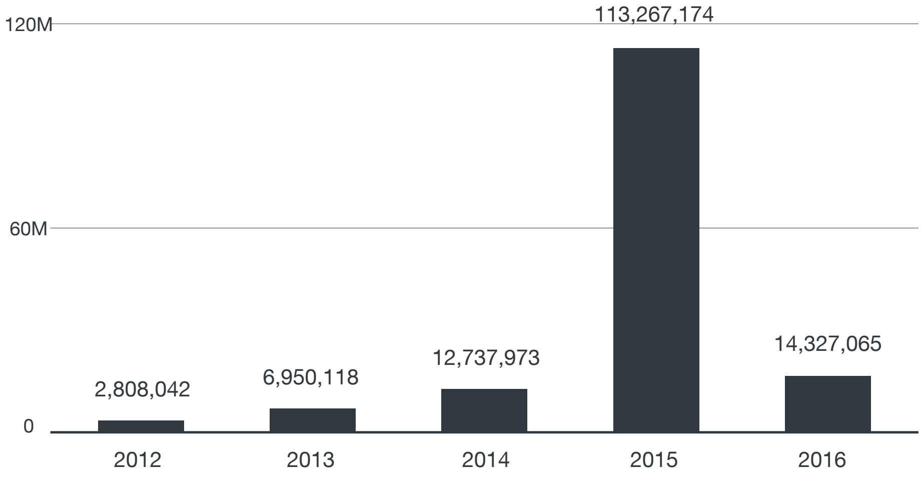


Figure 33. Health data breach incident disclosures from 2010 to 2016 according to the HHS Breach Notification data[1]

The image above shows that the total number of reported stolen EHRs per year has been steadily increasing since 2012. The year 2015 showed a significant increase as three of the top U.S. healthcare insurance providers were compromised (Excellus Health Plan, Premera Blue Cross, and Anthem). The breaches included information such as Social Security numbers, financial records, passwords, and credit card credentials.

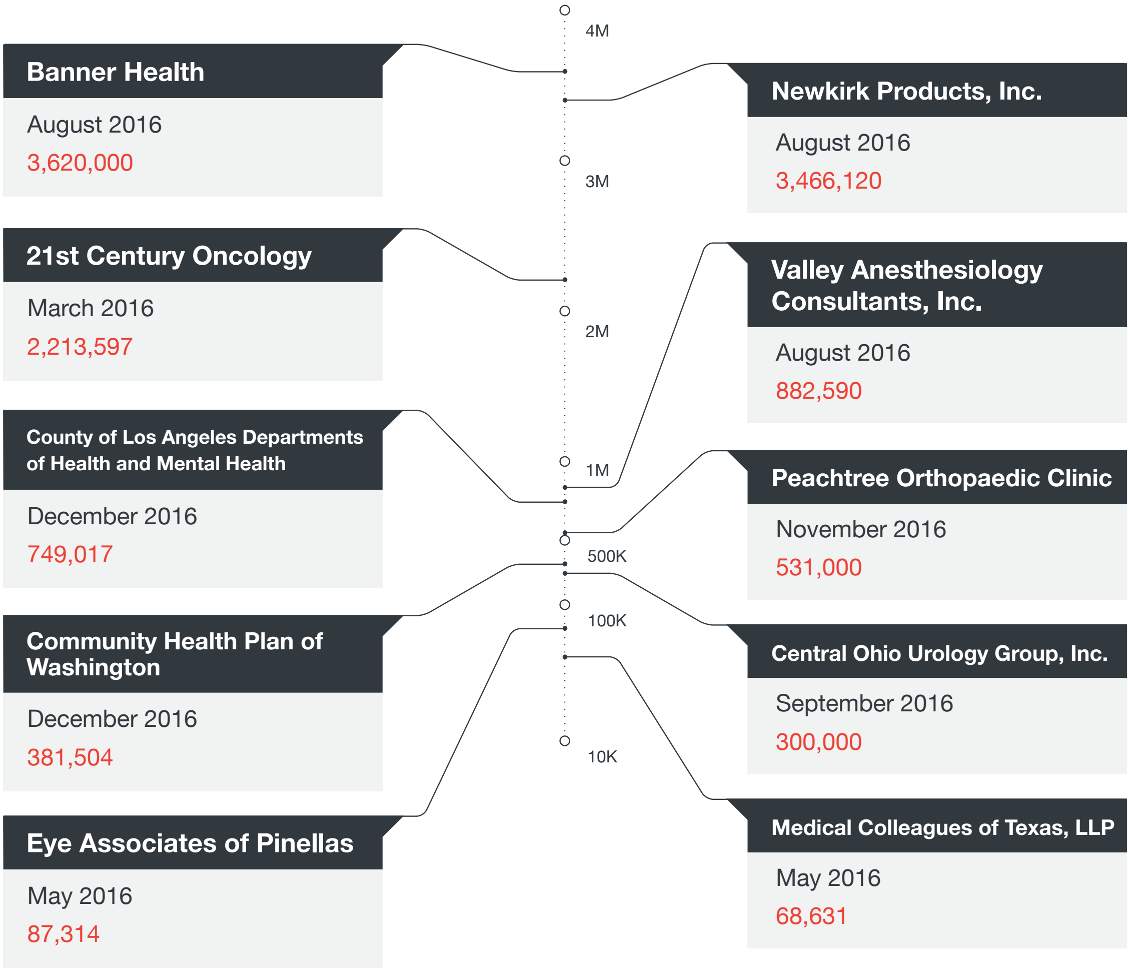


Figure 34. Top 10 data breaches according to the HHS Breach Notification data due to hacking incidents by a cybercriminal from January through December 2016. [1]

**Date referred to by Central Ohio Urology Group, Inc, Peachtree Orthopaedic Clinic, and Community Health Plan of Washington refers to the date of disclosure. Date of actual breach is still under investigation or has yet to be disclosed.*

1. In July 2016 Banner Health discovered a cybercriminal trying to gain unauthorized access to their computer systems. These systems contained payment card data and patient information of 3.6 million individuals. The payment information included cardholder name, card number, card expiration date, and verification code. While the exposed patient data included names, birthdates, addresses, physicians' names, dates of service, claims information, health insurance information and Social Security numbers.[24]

2. Newkirk Products Inc., which issues insurance cards including those to Blue Cross Blue Shield, experienced a breach to their server that contained health plan information of 3.4 million individuals.[25]

3. 21st Century Oncology Holdings in Florida reported a breach that affected 2.2 million patients in 145 of its cancer treatment centers in the U.S. and 36 more in Latin America. The breach included names, Social Security numbers, physicians' names, along with treatment and insurance details.[26]

4. Valley Anesthesiology and Pain Consultants in Arizona (VAPC) identified a third party that gained unauthorized access to their systems; which included bank information, patients' names, limited clinical information, name of health insurer, insurance identification numbers, professional license numbers, DEA numbers, National Provider Identifiers (NPIs) and Social Security numbers of 882,590 individuals.[27]

5. In May 2016, 108 Los Angeles County Department of Health and Department of Mental Health employees fell for phishing emails. This resulted in the theft of over 700,000 EHR which included first and last names, birthdates, Social Security numbers, license or state identification numbers, payment information, financial data, medical insurance information, treatment history, and many more.[28]

6. Peachtree Orthopaedic Clinic in Atlanta disclosed that its network had been compromised. According to the clinic, patients prior to July 2014 were affected by this. The information stolen includes patient names, addresses, email addresses, dates of birth, treatment codes, prescription records, and Social Security numbers.[29]

7. An anonymous caller reached out to Community Health Plan of Washington (CHPW) explaining that there was a vulnerability in the institution's technical services provider. After hiring a forensic investigator, CHPW discovered that records of current and former patients had been exposed. The investigation confirmed that hackers got access to names, addresses, birthdates, Social Security numbers, as well as other health-related information.[30]

8. A Ukrainian hacktivist group posted 223GB worth of data stolen from Central Ohio Urology Group on a public drive. The data contained text files, .zip files, video files, PDF, photos and other files. Aside from EHR, the leaked data included network design, detailed communication flow, as well as log-in details to various servers.[31]

9. Eye Associates of Pinellas was breached through their EHR management software PrognoCIS and is part of a larger breach of the company Bizmatics, which occurred in 2015 and affected 87,314 individuals. The U.S. HHS Breach Notification website added this as an incident that took place in 2016.[26]

10. Medical Colleagues of Texas (MCT), LLP in Katy, Texas, disclosed that cybercriminals gained access to its computer network and accessed 68,631 records that included the names, addresses, Social Security numbers, and health insurance information of its patients and employees. MCT is working to implement a two-factor authentication system for the remote access of EHRs.[26]

Notable 2016 International Breaches

UK

The Information Commissioner's Office (ICO) is responsible for data governance in the United Kingdom. Therefore, all types of breaches are reported to that specific agency. In the first quarter of 2016, 232 healthcare-related breaches had already occurred and made the healthcare sector the industry with the highest number of data breaches.

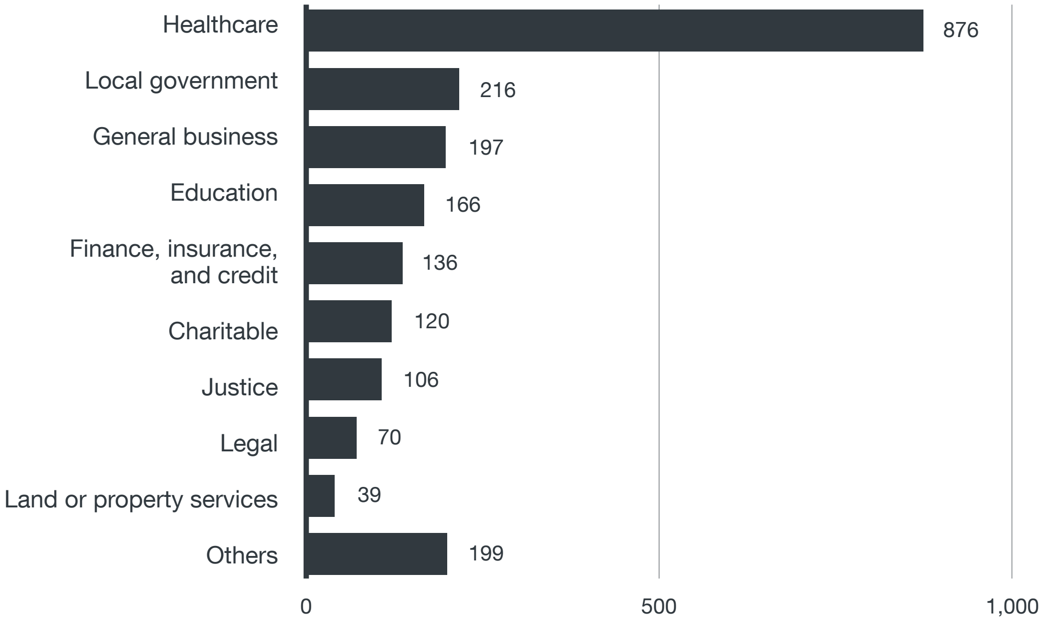


Figure 35. Data breaches in the U.K. recorded in 2016 [32]

Australia

In September 2016, the Health Minister of Australia disclosed 3 million patient data that had been breached when a vulnerability to the Medicare system was discovered. Decrypting the stolen data gave cybercriminals access to doctor's prescriptions and patients' PII.[33]

Canada

North Ottawa Community Health System patient information was breached through their EHR vendor Bizmatics in June 2016. The breach is part of a larger breach that took place against Bizmatics in 2016. In total, there were 20,000 files of patient data including name, address, health insurance information, last four digits of a credit card number and Social Security numbers that were breached.[34]

Hong Kong

In July 2016, 17,000 personal and clinical files from the Department of Health's Immunization Records System were accessed. The data compromised includes family health history, dental services, and school records. The breach was discovered when suspicious files were identified on the EHR vendor's server.[35]

China

A hacker uploaded 6,000 videos of newborn babies to a video-sharing website. The videos were recorded from the Anhui Women and Children Health Hospital in Hefei, China. Parent information was not compromised in the breach.[36]

United Arab Emirates

A threat actor hacked the Al Zahra Private Medical Centre in September 2016. The hacker posted the compromised data on Pastebin, which included sample data of medical history, insurance, telephone number, email addresses, address, names, and nationality.[37]

References

1. U.S. Department of Health and Human Services. (n.d.). *U.S. Department of Health and Human Services Office for Civil Rights*. “Breaches Affecting 500 or More Individuals.” Last accessed on 3 October 2016, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

2. Deepdotweb. (26 June 2016). *Deepdotweb*. “655,000 Healthcare Records (Patients) Being Sold.” Last accessed on 28 January 2017, https://www.deepdotweb.com/2016/06/26/655000-healthcare-records-patients-being-sold/.

3. Cathy Reisenwitz. (30 April 2015). *Capterra Medical Software Blog*. “EMR Software Comparison: 5 Popular Choices.” Last accessed on 28 January 2017, http://blog.capterra.com/emr-software-comparison/.

4. Centers for Medicare and Medicaid Services. (30 January 2017). *Centers for Medicare & Medicaid Services*. “Data and Program Reports.” Last accessed on 31 January 2017, https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/dataandreports.html.

5. HealthIT.gov. (12 May 2016). *Health IT Legislation and Regulations*. “Health IT Legislation.” Last accessed on 28 January 2017, https://www.healthit.gov/policy-researchers-implementers/health-it-legislation.

6. U.S. Department of Health and Human Resources. (28 December 2006). *U.S. Department of Health & Human Services*. “HIPAA Security Guidance.” Last accessed on 28 January 2017, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf.

7. Healthcare Information and Management Systems Society. (19 August 2016). *Healthcare Information and Management Systems Society*. “2016 HIMSS Cybersecurity Survey.” Last accessed on 28 January 2017, http://www.himss.org/sites/himssorg/files/2016-cybersecurity-report.pdf.

8. Ponemon Institute. (11 May 2016). *ID Experts*. “Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data.” Last accessed on 28 January 2017, https://www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents?utm_source=Referral&utm_medium=press%20release&utm_campaign=Ponemon%202016.

9. Dissent. (28 June 2016). *DataBreaches*. “264,000 and counting: Hack of EHR/EMR Vendor Leaves Clients Scrambling.” Last assessed on 28 January 2017, https://www.databreaches.net/264000-and-counting-hack-of-ehremr-vendor-leaves-clients-scrambling/.

10. Health Insurance Portability and Accountability Act Journal. (24 June 2016). *HIPAA Journal*. “Bizmatics Data Breach Victim Count Rises to Almost 177,000.” Last accessed on 28 January 2017, http://www.hipaajournal.com/bizmatics-data-breach-victim-count-rises-almost-177000-3483/.

11. Harriet Cohen. (2 October 2016). *Digital Guardian*.“June 2015: The Month of the Breach?” Last accessed on 28 January 2017, https://digitalguardian.com/blog/june-2015-month-breach.

12. Mark Fahey. (22 September 2016). *CNBC*. “Yahoo Data Breach Among the Biggest in History.” Last accessed on 26 January 2017, http://www.cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-in-history.html.

13. David Pittman. (17 August 2016). *Politico*. “E-prescribing Controlled Substances Skyrockets.” Last accessed on 28 January 2017, http://www.politico.com/tipsheets/morning-ehealth/2016/08/e-prescribing-controlled-substances-skyrockets-215922.

14. Addition Center. (18 December 2015). *Addiction Center*. ”Ambien Addition and Abuse.” Last accessed on 28 January 2017, https://www.addictioncenter.com/sleeping-pills/ambien/.

15. Ponemon Institute (23 February 2015). *Medical Identity Fraud Alliance*. “Fifth Annual Study on Medical Identity Theft.” Last accessed on 28 January 2017, http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

16. Gerri Detweiler. (8 December 2016). *Credit*. "How Medical Debt Can Impact Your Credit Score." Last accessed on 28 January 2017, https://www.credit.com/credit-scores/how-medical-debt-can-impact-your-credit-score/.

17. Kara Brandeisky. (9 March 2015). *Time*. "It Just Got Harder for Debt Collectors to Destroy Your Credit." Last accessed on 28 January 2017, http://time.com/money/3737140/credit-score-medical-debt/.

18. Michelle Andrews. (25 August 2016). *Consumer Reports*. "The Rise of Medical Identity Theft." Last accessed on 28 January 2017, http://www.consumerreports.org/medical-identity-theft/medical-identity-theft/.

19. Internal Revenue Services. (18 February 2016). *Internal Revenue Service*. "Consumers Warned of New Surge in IRS E-mail Schemes During 2016 Tax Season; Tax Industry Also Targeted." Last accessed on 2 February 2017, https://www.irs.gov/uac/newsroom/consumers-warned-of-new-surge-in-irs-email-schemes-during-2016-tax-season-tax-industry-also-targeted.

20. John Matherly. (26 December 2016). *Leanpub*. "Complete Guide to Shodan." Last accessed on 1 February 2017, https://leanpub.com/shodan.

21. The U.S. Federal Bureau of Investigation. (10 September 2015). *Internet Crime Complaint Center*. "Internet of Things Poses Opportunities for Cyber Crime." Last accessed on28 January 2017, https://www.ic3.gov/media/2015/150910.aspx.

22. Pawan Kinger. (8 April 2016).*TrendLabs Security Intelligence Blog*. "Skipping a Heartbeat: The Analysis of the Heartbleed OpenSSL Vulnerability." Last accessed on 10 February 2017, http://blog.trendmicro.com/trendlabs-security-intelligence/skipping-a-heartbeat-the-analysis-of-the-heartbleed-openssl-vulnerability/.

23. Verizon. (19 May 2016). *Verizon Enterprise*. "2016 Data Breach Investigations Report." Last accessed on 28 January 2017, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

24. Banner Health. (3 August 2016). *Banner Health*. "Banner Health Identifies Cyber Attack." Last accessed on 28 January 2017, https://www.bannerhealth.com/news/2016/08/banner-health-identifies-cyber-attack#.

25. Marianne Kolbasuk McGee. (25 August 2016). *Careers Infosecurity*. "Healthcare Hacker Attack Victim Tally Soaring." Last accessed on 28 January 2017, http://www.careersinfosecurity.com/healthcare-hacker-attack-victim-tally-soaring-a-9361.

26. Trend Micro (30 May 2016). *Trend Micro Security News*. "Latest Data Breaches Put Spotlight on U.S. Hospitals." Last accessed on 28 January 2017, http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/latest-data-breaches-put-spotlight-on-u-s-hospitals.

27. Valley Anesthesiology and Pain Consultants. (12 August 2016) PR Newswire. "Valley Anesthesiology and Pain Consultants Identifies and Addresses Information Security Incident." Last accessed 28 January 2017, http://www.prnewswire.com/news-releases/valley-anesthesiology-and-pain-consultants-identifies-and-addresses-information-security-incident-300312986.html.

28. Kevin Townsend (19 December 2016). *Security Week*. "Los Angeles County Notifies 756,000 of Data Breach." Last accessed on 10 February 2017, http://www.securityweek.com/los-angeles-county-notifies-756000-data-breach.

29. Dissent. (13 October 2016). *DataBreaches*. "Peachtree Orthopedic Clinic Notifies Patients of Hack." Last accessed on 10 February 2017, https://www.databreaches.net/peachtree-orthopedic-clinic-notifies-patients-of-hack/.

30. Jessica Davis. (21 December 2016). *Healthcare IT News*. "Breach at Community Health Plan of Washington affects nearly 400,000 members." Last accessed on 10 February 2017, http://www.healthcareitnews.com/news/breach-community-health-plan-washington-affects-nearly-400000-members.

31. Waqas. (3 August 2016) *Hackread*. "Central Ohio Urology Group Hacked; 223GB of Crucial Data Leaked." Last accessed on 10 February 2017, https://www.hackread.com/central-ohio-urology-group-hacked/.

32. Information Commissioner's Office. (3 February 2017). *Information Commissioner's Office*. "Data Security Incident Trends." Last accessed on 9 February 2017, https://ico.org.uk/action-weve-taken/data-security-incident-trends/.

33. Raina Spooner and Noel Towell. (29 September 2016). *The Sydney Morning Herald*. "Fears That Patients' Personal Medical Information Has Been Leaked in Medicare Data Breach." Last accessed on 28 January 2017, http://www.smh.com.au/national/public-service/privacy-watchdog-called-after-health-department-data-breach-20160929-grr2m1.html.

34. Krystle Wagner. (10 June 2016). *Grand Haven Tribune*. "NOCHS Takes Precautions Following Possible Breach." Last accessed on 28 January 2017, http://www.grandhaventribune.com/Health-Care/2016/06/10/No-evidence-patient-information-breached-NOCHS-takes-precautions.

35. Phoenix Un. (21 July 2016). *The Standard*. "Privacy Concerns After Health Hack." Last accessed on 28 January 2017, http://www.thestandard.com.hk/section-news.php?id=171825.

36. Fan Yiying. (12 July 2016). *Sixth Tone*. "Hospital Hackers Steal Thousands of Newborn Baby Videos." Last accessed on 28 January 2017, http://www.sixthtone.com/news/hospital-hackers-steal-thousands-newborn-baby-videos.

37. Dissent. (5 September 2016). *DataBreaches.* "UAE: Al Zahra Private Medical Centre Hacked." Last accessed on 28 January 2017, https://www.databreaches.net/uae-al-zahra-private-medical-centre-hacked/.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey
to the Cloud

www.trendmicro.com