Orange
Cyberdefense

Databreaches in Healthcare

The attractiveness of leaked healthcare data for cybercriminals

Table of Contents

Diana Selck-Paulsson
Threat Research Analyst
Orange Cyberdefense

Co-author: Michael Haugland
Threat Research Analyst
Orange Cyberdefense

Introduction:

The attractiveness of leaked health-care data for cybercriminals

Targeted cyberattacks against various industries have become increasingly common in recent years. The healthcare sector is no exception. In 2015, this reached its peak, especially affecting United States (U.S.) based healthcare companies, with more than 113.27 million records being exposed[1].

The healthcare sector as any other sector is undergoing immense changes towards digitalization. Digital healthcare can empower patients to receive better health services, for example, better tracking over time, timely reminders of screenings and preventative checkups, sharing of medical history cross health providers, etc. There-fore, by digitalizing health data, the data becomes more accessible. The intent of the industry is to increase ac-cessibility for authorized users to increase information sharing and collaboration for better patient care. The side effect of this is an increase in the attack surface because the healthcare sector is not mature enough to secure their assets.

Knowledge and awareness, as well as budget, might not always be sufficient for securing health data and addressing security issues. When we refer to health data, which will be the term moving forward, we under-stand health data as information that describes physical and/or mental health, the provision of health services, such as administrative data (personal identifiable information (PII), financial data), insurance claims data, patient disease registries (registries for collecting clinical data of the population) and clinical trial data for research.

An international problem

The U.S. has implemented a strict healthcare regulation called the Health Information Technology for Economic and Clinical Health Act (HIPAA). Other countries don't operate under such regulations and therefore, even if similar breaches happen worldwide, most statistical data originates from the U.S.

For example, at the beginning of this year, an estimated 2.7 million recorded calls from the Swedish national healthcare service hotline was found publicly accessible due to storage on an entirely unencrypted system. No password or any other sort of authentication was required. The data was stored with a third party called MediCall registered in Thailand. The whole breach included 170,000 hours of sensitive conversations about medical conditions[2].

As this incident shows, more and more third parties are entering the health supply chain and thus increasing the risk of data loss.

There are various reasons why there is an increase or perceived increase in data breaches in healthcare. We say 'perceived' because the actual number of occurrences of breaches was not extensively high, but when breaches occurred, they affected large electronic systems with a large number of compromised health records.

According to a study that collected data on breaches between 2010 and 2017, 2149 breaches were reported to the US Health and Human Services Office for Civil Rights with a total amount of 176.4 million compromised health records[3] .

the risk of digitalization

While the most common media for data loss still seems to be paper and film, the largest share of breached records accounts for information breaches from network servers (ibid.). Therefore digitalization of the industry plays an important role when looking at data breaches in the healthcare sector. Especially, since breaches that concern digital information can remain undetected for a long time period in comparison to a physical medium that contains health data.

The healthcare sector is not the only sector that increases its attack surface through digitalization but the health data they are processing and sharing is, first of all, of very sensitive nature and that makes it crucial for them to protect patients health data. Secondly, health data has many purposes due to the variety of data within one health data record. An attacker can choose to leverage only the PII data, the financial data or the medical history part of this record for a specific purpose, amongst others, fraud, identity theft and/or physical harm. Especially in the latter,

health data cannot be changed regarding medical conditions, social security number, or date of birth - this data is connected to a patient for a lifetime; once compromised, always compromised.

Besides unauthorized access to databases of health data, another cause for an increased attack surface of the healthcare sector is insecure connected medical devices, or IoT medical devices serving as an entry point for attackers.

The medical IoT

Medical devices such as heart rate monitors or insulin pumps were designed to serve a medical purpose. Security features - until now - are often not considered when developing such devices. The devices themselves might not have data storage capabilities but provide an entry point to servers and other network devices that do store sensitive data or provide the opportunity to install malicious software, e.g. ransomware.

The most well-known campaign was WannaCry in 2017, which disrupted and impacted the National Health Service (NHS) hospitals and GP practices in the United Kingdom by disrupting approximately 19,000 appointments and surgeries. This ransomware outbreak cost the NHS almost £100 million[4].

In 2018, a malware dubbed Kwampirs targeted healthcare cooperations in the U.S., Europe, and Asia. The malware seemed to target systems that had the software installed to use and control MRI's and X-ray machines[5].

Only recently, the U.S. based Grays Harbor Community Hospital and Harbor Medical Group were infected, as a consequence medical records, prescriptions, and other functions were down. While direct patient care was not impacted by the attack, patients were asked to bring their prescriptions and other medical histories in physical form so that the staff could access that information. The ransom demanded was $1 million[6].

Additionally, medical devices can be disrupted remotely and cause severe (physical) damage to a patient[7]. While medical devices are playing a significant role when considering vulnerabilities for the healthcare sector, they will not be further explored in this research, the focus will be on compromised health data and what an attacker can do with them.

Hypothesis

Therefore, we would like to explore the question of why health data is so attractive for attackers; and what an attacker can do with stolen health data. In order to explore these questions, we have the following hypothesis:

Hypothesis I: Health data is more attractive to an attacker because it brings more value due to its multitude of information, e.g. financial data, PII, medical history.

Hypothesis II: Stolen health data is sold for a higher price per record on online markets in comparison to other stolen data such as financial data.

Overview of the attack vector:

What has healthcare suffered in the past?

In the past decade, the healthcare sector has experienced over 2,500 data breaches that were reported in the U.S. and thus do not include the dark number of breaches not reported. Records that were either stolen or exposed account for 189,945,874 healthcare records, which stands for more than 59% of the U.S. population[8]. There is a steady increase in occurrences of breaches in the past years, ranking up to 365 breaches in 2018.

"2015 was a record year for healthcare industry data breaches. More patient and health plan member records were exposed or stolen in 2015 than in the previous 6 years combined, and by some distance. More than 113 million records were compromised in 2015 alone, 78.8 million of which were stolen in a single cyber-attack. 2016 saw more healthcare data breaches reported than any other year, and 2017 looks set to be another record-breaker."

Source:
https://www.hipaajournal.com/category/healthcare-cybersecurity/

2015 seemed to have seen a drop in the number of healthcare breaches and 2018 had the all-time high in the number of breaches.

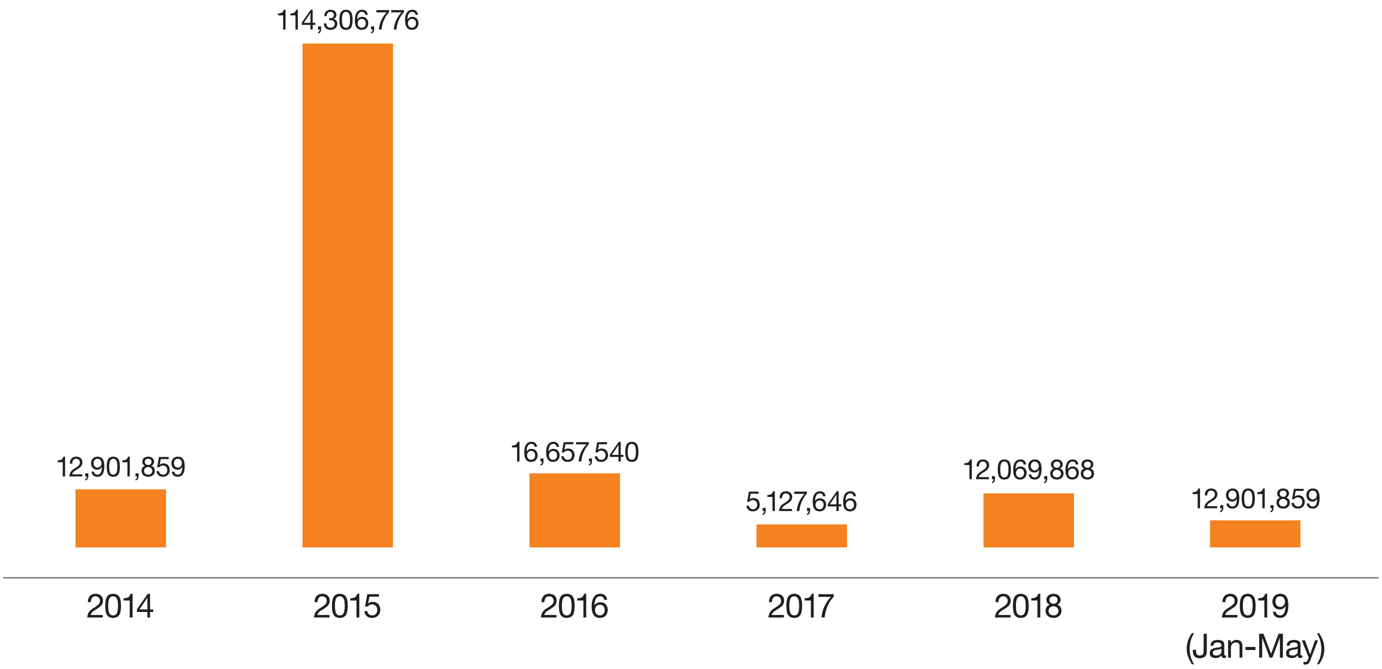
For the first half of 2019, it can be said that April has seen the highest amount of breaches (46), followed closely by May (44). This means that on average in 2019, 37.3 breaches occurred per month, meaning more than one breach has been reported per day[9]. May alone had a 186% increase in the number of exposed health data (1,988,376 healthcare records) in comparison to the month before. And from the beginning of 2019 until May, already more than 6 million pieces of health data were found exposed (ibid.).

However, the number of exposed unencrypted health data has been steadily decreasing over the past years, which shows that some protection mechanisms have been implemented and show effect. June seems to have "normalized" again and shows a breach rate of 30, which translates into one per day.

Nevertheless, the number of health data exposed increased by 73.6% with a total of 3,452,442 healthcare records stolen[10].

Breached healthcare records

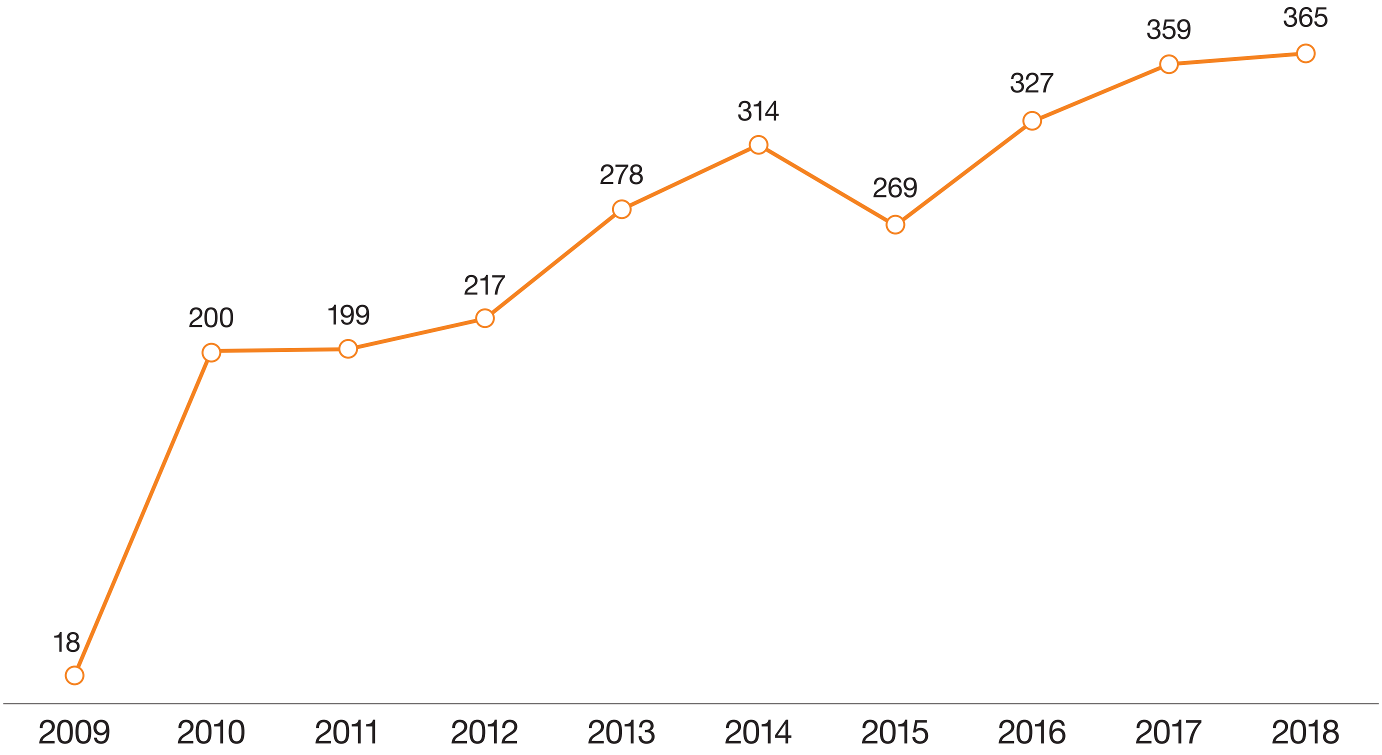
Reported databreaches in the USA



Source: https://www.hipaajournal.com/may-2019-healthcare-data-breach-report/

Number of reported data breaches

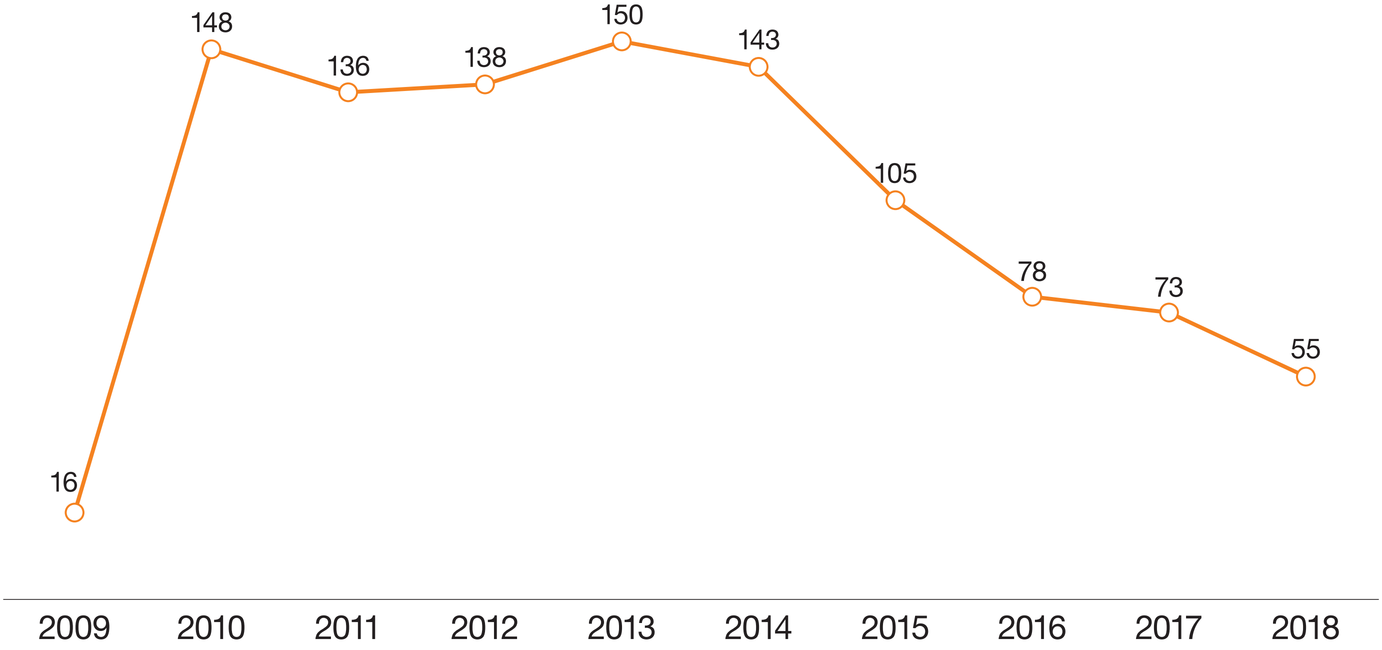
Reported databreaches in the USA



Source: https://www.hipaajournal.com/healthcare-data-breach-statistics/

Theft/loss incidents

Reported databreaches in the USA



Source: https://www.hipaajournal.com/healthcare-data-breach-statistics/

What are the most common causes of health data compromise?

In 2018, the most frequent cause of exposed health data was hacking/IT incidents. Looking back to the past years, there has been an increase recorded and that is in part due to an actual increase in malicious activity, but also due to improvements in detection capabilities and reporting of incidents for the industry as a whole. This needs to be acknowledged when claiming that there is an overall increase in breaches. Incidents of unauthorized access (internal or external) can be detected faster as well as the installation of malicious software such as ransomware than was the case a decade ago.

According to the 2019 Data Breach Investigations Report from Verizon, the healthcare sector is listed as number two when considering data breaches. 16% of breaches were recorded in the public sector, closely followed by 15% of breaches in healthcare and 10% in the finance sector. The top 3 patterns for causes of health data leakage are miscellaneous errors (number one), privilege misuse (number two) and hacking/web applications.

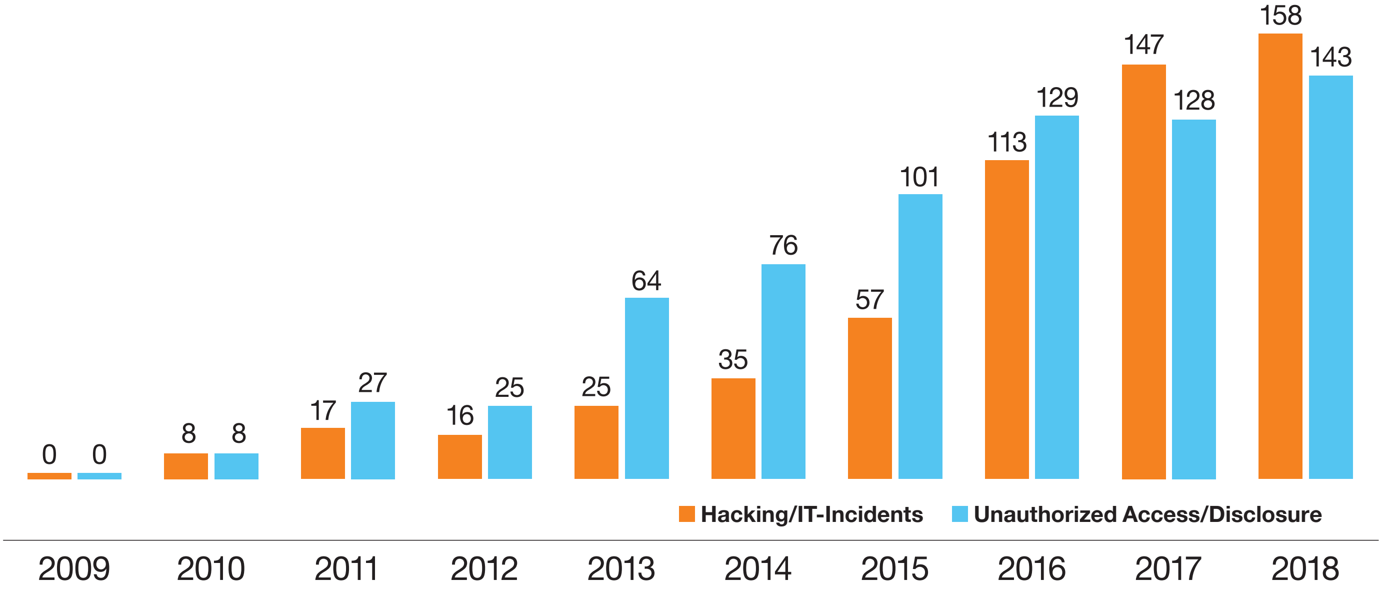
This is interesting because some say that the healthcare industry is one of the few that struggles with experiencing more insider threats than threats from the outside.

This then means that accessing health data has no real threshold since they already have access to relevant systems. Often the healthcare sector is able to detect hacking incidents from external parties quicker than detecting insider threats, which can take up to several years between detection and the actual breach.

Another common error that the healthcare sector experiences is that sensitive patient data is sent to the wrong recipient (wrong patient, wrong department internally, wrong insurance recipient, etc.) which explains the number one cause mentioned above - miscellaneous error. This often still happens commonly in paper form as well as electronic transmission[12].

Common causes of compromise

Hacking/IT-incidents and unauthorized access/disclosure



Source: https://www.hipaajournal.com/healthcare-data-breach-statistics/

Social engineering

Additionally, healthcare, as other industries, is vulnerable to social engineering (number four cause), for example in the form of phishing emails. Ransomware, information theft, and spear-phishing had already become the root cause of a large issue for the healthcare sector back in 2016, according to the report from Trend Micro[13].

And this trend continues until and throughout 2019. Ransomware incidents account for 70% of all registered malware outbreaks in the sector for the second year running[14].

Examples

Examples for theft[15]:

- Theft committed by outsiders or unknown parties
- Theft committed by former or current employees

Examples for unauthorized access:

- Employee disclosing PHI through mailing mistakes (e.g. wrong recipients; sensitive information showing through envelope windows)
- Employee taking PHI home or forwarding PHI to personal accounts or devices
- Employee accessing PHI without authorization
- Employee disclosing PHI through email mistakes (eg, wrong recipients, cc instead of bcc, unencrypted content)
- Other accidental disclosure of PHI by employees

Examples for hacking or IT-incidents (technical intrusions to an entity's server or computers):

- Entity accidentally exposing PHI through Internet
- Malware or virus
- Employee clicking phishing emails
- Hackers using employees' login and password

Error

- Loss (losing equipment or paper records)
- Entity losing or misplacing unencrypted equipment (eg, laptop computer)
- A business associate or mail carrier losing PHI in transportation
- Entity losing or misplacing paper records
- Improper disposal (electronic media not appropriately cleared or purged or paper records not appropriately shredded or destroyed)

Why is the healthcare vertical such an attractive target?

Financial Motivation

One of the main drivers for cybercriminal activity is financial gain. This applies to health data as well, especially since administrative data - which is part of health data - includes financial data. It is possible that this could be the sole motivation for targeting health data – the financial segment of a full medical record. This can easily be monetized as tradable goods in market listings in the "underground"[16].

Many reports refer to underground markets, which means that often stolen data is sold on the darknet or deep web where anonymity is higher than on the normal web.

There is a variety of sources that claim that health data is up to ten times more valuable for selling than other stolen data such as credit card information[17].

The actual value of one single health data record can be "hundreds and thousands of U.S. dollars according to Forbes[18]; or up to $50 for a medical record in comparison to credit card information for $1.50 or a social security number for $3[19].

Some medical records are sold for up to $60 each[20] (approx. bitcoin equivalent); or full medical records including date of birth, place of birth, credit card details, social security number, address, and emails are offered for up to $1,000[21] or "health information and medical records are estimated at $82.90 a piece for U.S. consumers, while a social security number is worth $55.70. Payment details, physical location information, home address, marital status, as well as the name and gender information are pegged at $45.10, $38.40, $17.90, $6.10 and $2.90", respectively
according to Trend Micro[22].

While most of the sources differ in the actual value of a health data record sold on the darknet marketplaces, they all agree that medical records typically are worth more than financial data on the markets. The main reason being that health data cannot easily be blocked and changed as, for instance, credit card information.

Secondly, banks have taken some precautions over the years, and are faster in their response towards theft, while the healthcare sector is in the middle of digital transformation and will most likely need more time to set up detection and response capabilities.

Once they are capable of reacting fast(-er) towards breaches and stolen health data, the value of stolen health data might lower, at least for the part that can be "disabled" and not further leveraged by an attacker. For demographic data, clinical data and family history, that part cannot be changed and remains leaked for a lifetime. Which means a part of a health data record will always be attractive to an attacker, depending on the purpose of leveraging this part of a record, which cannot be changed but harvested by committing fraud and/or even physical harm.

Identity theft to commit fraud

Because health data is so rich in information about an individual that is included in one single record, an attacker can easily use this data to commit identity theft. With a victim's family history, demographic data, insurance information, medications, a lot can be done to pretend to be someone else. But for what purpose? By far the most common motivation is a direct monetary gain for the perpetrator. A fraudster can either choose to just use PII data to apply for loans, credit cards, tax returns or even apply to open a new bank account or the stolen identity could be used to leverage the healthcare service.

This means patient information could be used to fraud insurances and receive payments of treatments and prescribed medications that the fraudster did not actually receive. Meanwhile the actual patient and thus victim of identity theft might experience issues claiming payment due to the fact that the payments might have already been issued to the wrong "patient". Or on the other side, a patient receives notification of an invoice for a surgery the actual patient has not received.

Using a patient's prescriptions is another opportunity that can either serve for someone's own drug consumption or it can be for the purpose of drug diversion, which means someone is then selling the prescribed controlled substance on the darknet marketplaces. The same can be applied for medical equipment acquired through a patient's prescription.

Identity theft is such a broad field, many other illegal activities can be done with one's identity, above only a few are mentioned.

Physical harm / targeted assassination /blackmail & extortion

Gaining access to someone's health data can provide a good opportunity to gain access to their health conditions such as allergies, medication and other dependencies on modern medical interventions.

Last July, a targeted attack took place aiming to gain access to the health data of Singapore's prime minister. SingHealth, the largest healthcare group in Singapore, noted a massive data breach of 1.5 million patient records from patients who visited SingHealth clinics between May 2015 and July 2018. One particular health record of interest seemed to be the one of Singapore's prime minister Lee Hsien Loong, which contained information about his medication. It was later concluded that the attack seemed well-planned, sophisticated and targeted, even potentially nation-state sponsored[23].

Another opportunity to cause physical harm towards a specific individual is to alter the victim's medical record by adding false information or removing an entry stating that the patient is allergic to penicillin. This could have life-threatening consequences for the patient.

Additionally, depending on the nature and origin of the stolen medical data, it can be used for blackmail and extortion purposes[24].

One example that has been present in the media is the activities from the hacker group known as "The Dark Overlord" (TDO). The threat actor has been active since 2016 and has targeted different healthcare areas including plastic surgery clinics attempting to blackmail its victim including photographs of before, during and after the plastic surgery to extort money, which the healthcare provider did not pay.

> **“We're going to pitch it all up for everyone to nab. The entire patient list with corresponding photos. The world has never seen a medical dump of a plastic surgeon to such degree.”**
>
> TDO, 2017
> https://www.thedailybeast.com/hackers-steal-photos-from-plastic-surgeon-to-the-stars-claim-they-include-royals

Consequently, TDO put the files up for sale on a darknet forum afterwards, which means that even though the clinic has chosen not to pay, the patient data will be sold and can be individually leveraged by contacting the actual victims and trying to blackmail them instead[25].

Sensitive information such as a diagnosis of a patient, be it a history of plastic surgery or mental health challenges, medical blackmail becomes an incentive for an attacker that is motivated by financial gain or harm-inflicting intentions to ruin the victim's reputation.

Besides breached health data, medical devices can inflict harm when taken over by an attacker, preventing healthcare providers from treating their patients. Attackers know that medical devices most often don't contain any health data but they are an easy first target when trying to interrupt a service or treatment and thus inflict physical harm. Especially in comparison to accessing network devices that might be more secure than medical devices.

This, however, is noteworthy when considering motivations and the end goal of an attack, but it is not the focus of this research and will therefore not be further explored.

Data collection:

Diving into the darknet looking for health dumps

In an attempt to validate the claim that health data is more attractive to an attacker because of its multi-purpose nature, we went to different darknet marketplaces and forums to observe what the value of current listings is, especially in comparison to other breached data such as financial data or PII; how common is breached health data really and what is the conversation around usability for an attacker?

What we knew before was that it might be difficult to find listings relevant to this research. Marketplaces on the darknet can in some cases not easily be found or accessed, and thus finding them might be time-consuming and dependent on the market accessibility. By market accessibility, we mean that some markets require just a simple registration of email and password, while others are invite-only or require a minimum of certain actions to be accepted or enabled to enter.

Therefore, we have only focused on marketplaces that could be entered by a simple registration and could be found through the site https://dark.fail or markets that were mentioned in a forum thread. Consequently, this is a limitation that we acknowledge, we were also very dependent on the availability of those marketplaces at times, marketplaces we intended to visit were simply offline and thus not available for data collection. Again, this was a matter of time, because those markets would be online again to a later time.

The initial phase to find market listings were mostly going through online sources such as Google searches, Reddit threads, hidden wiki-links, dark.fail links and reaching out to other researchers. The most successful rates in accessing marketplaces we experienced through the dark.fail list or forum references.

Police line, do not cross

Another limitation we found was that a majority of published research efforts and blog posts on the topic were outdated due to extensive law enforcement activities in the first half of 2019 that shut down many referenced marketplaces.

For example, DreamMarket was referenced a lot, when trying to find the marketplace, we found that it was closed, most likely an exit scam by its operators, just one month prior to our data collection phase[27].

While the Wallstreet Market was shut down in May 2019 by law enforcement one month after DreamMarket shut down[28].

Another - one of the oldest marketplaces - was just taken down when we started with the data collection, known under the name Valhalla or the Finnish name Silkkitie[29].

The DeepDotWeb was also taken over by a joint effort of law enforcement agencies in May 2019[30]. During the research period, the Nightmare market has also done an exit scam, according to some forum threads and was unavailable since July 2019.

This meant that there were limited marketplaces available, combined with the uncertainty of where the major vendors would move to after the shutdowns. This made data collection more difficult than anticipated. Not just because of the limited number of marketplaces but also the number of listings we would actually find after such an interruption in the darknet marketplaces.

During a period of three months, we visited nine marketplaces and five paste sites and forums. The marketplaces we visited were:

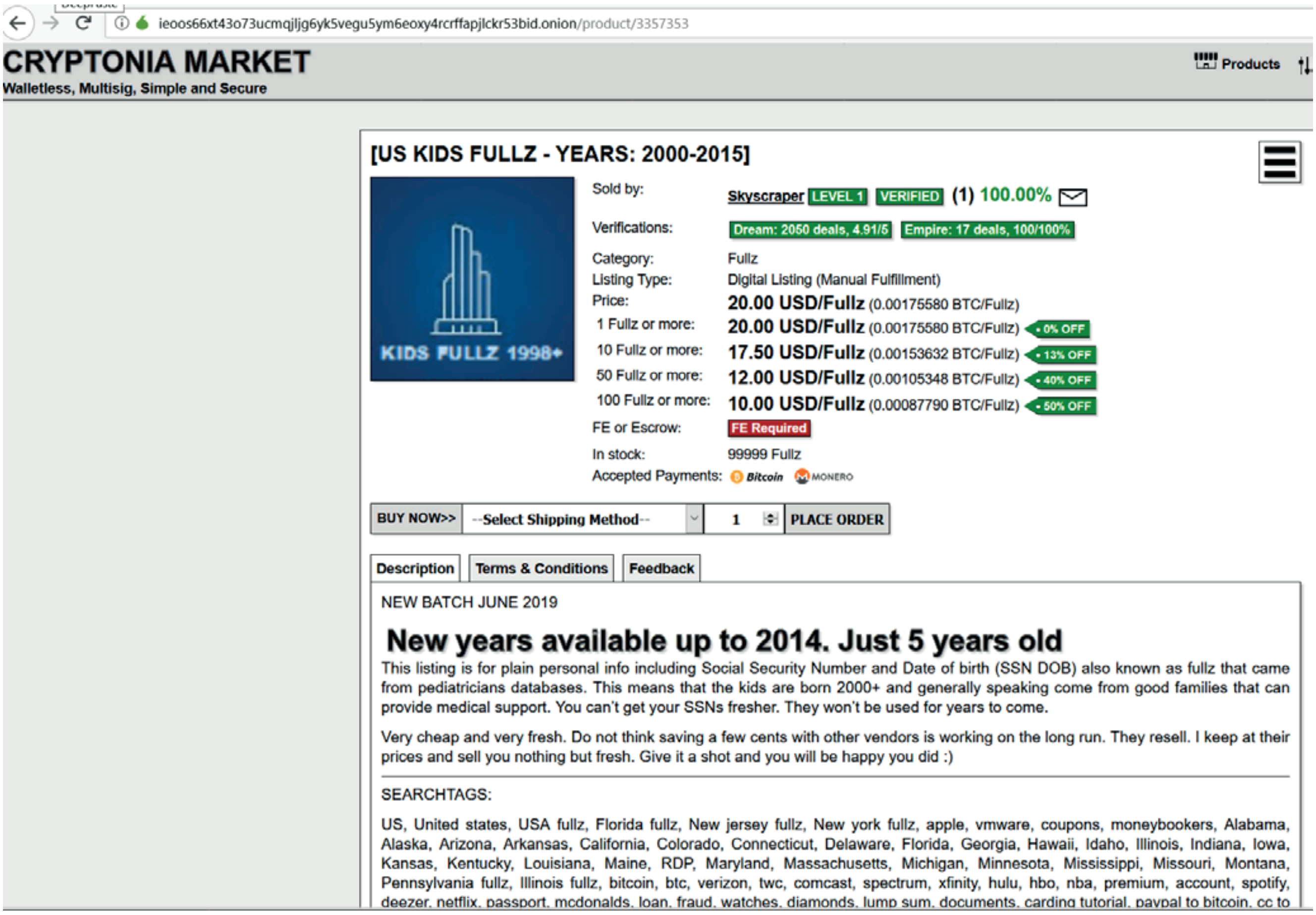
- Empire Market (last checked in August 2019)
- Cryptonia Market (last checked in August 2019)
- Berlusconi Market (last checked in August 2019)
- Nightmare Market (last checked in July 2019)
- The Majestic Garden (last checked in July 2019)
- Tochka (last checked in July 2019)
- Genesis Market (last checked in August 2019)
- Hydra (last checked in August 2019)
- Apollon Market (last checked in August 2019)

Whereas the Empire Market and the Cryptonia Market were the most relevant places for our research since we found health-related listings at those marketplaces We either searched through categories of listings such as fraud, dumps, databases, data and scans or searched for keywords such as Med Fullz, Medical Fullz, health data, health records, patient records PHI, EHR, Hospital, Pediatric, Pediatriciankids/kids or healthcare fraud package.

"Fullz" or "Fulls" are often part of the title or keywords to find breached data and basically means that a listing includes the full package of something, be it a full record including PII such as first name, last name, email, address, phone number and social security number; or financial information such as credit card number, cardholder and expiration date. Both examples can be referred to as "fullz".

Cryptonia Market

#1 Kids medical Fullz from pediatrician databases



ieoos66xt43o73ucmqjljg6yk5vegu5ym6eoxy4rcrffapjlckr53bid.onion/product/3357353

CRYPTONIA MARKET
Walletless, Multisig, Simple and Secure

[US KIDS FULLZ - YEARS: 2000-2015]

Sold by:	Skyscraper LEVEL 1 VERIFIED (1) 100.00%
Verifications:	Dream: 2050 deals, 4.91/5 Empire: 17 deals, 100/100%
Category:	Fullz
Listing Type:	Digital Listing (Manual Fulfillment)
Price:	20.00 USD/Fullz (0.00175580 BTC/Fullz)
1 Fullz or more:	20.00 USD/Fullz (0.00175580 BTC/Fullz) 0% OFF
10 Fullz or more:	17.50 USD/Fullz (0.00153632 BTC/Fullz) 13% OFF
50 Fullz or more:	12.00 USD/Fullz (0.00105348 BTC/Fullz) 40% OFF
100 Fullz or more:	10.00 USD/Fullz (0.00087790 BTC/Fullz) 50% OFF
FE or Escrow:	FE Required
In stock:	99999 Fullz
Accepted Payments:	Bitcoin MONERO

NEW BATCH JUNE 2019

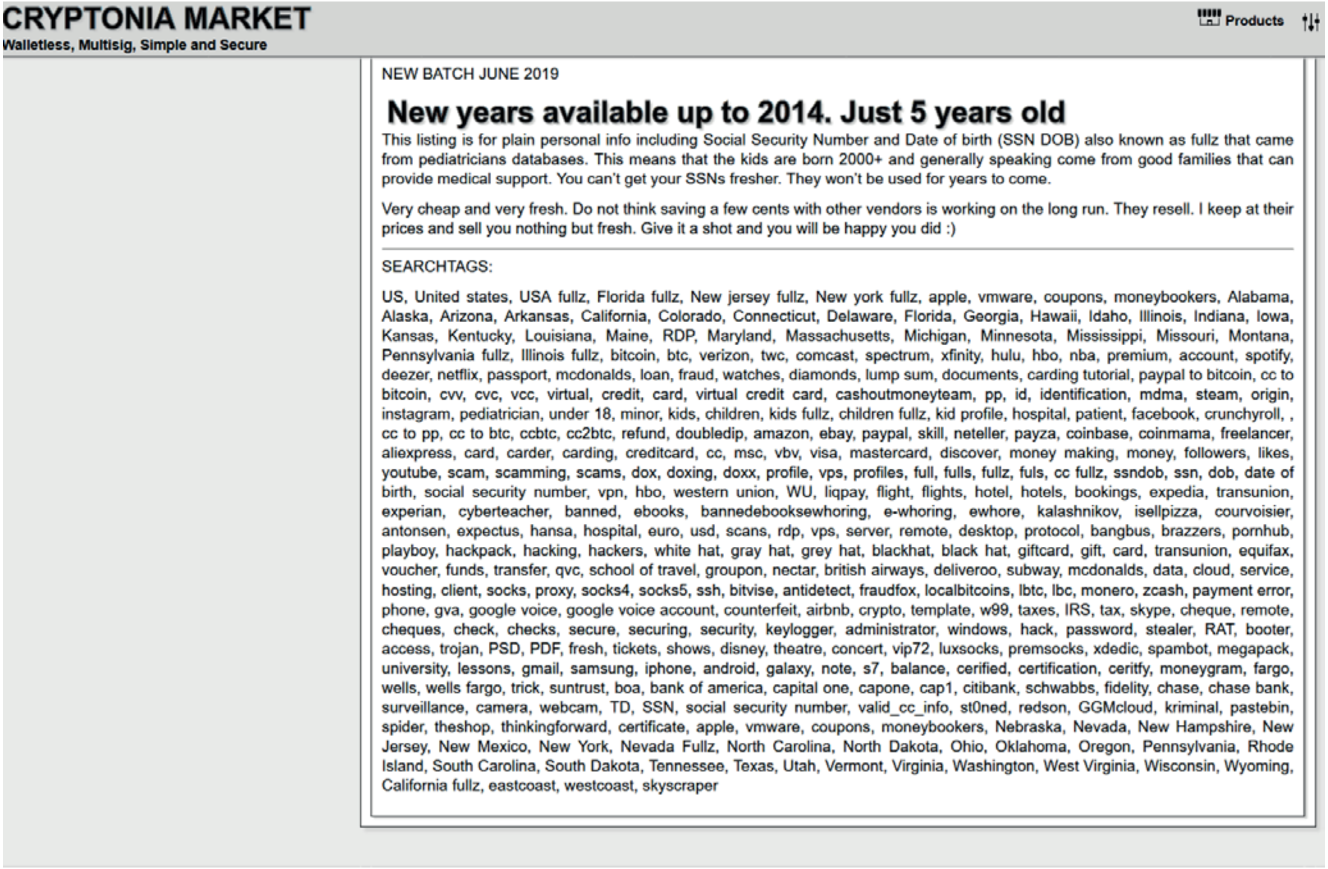
New years available up to 2014. Just 5 years old

This listing is for plain personal info including Social Security Number and Date of birth (SSN DOB) also known as fullz that came from pediatricians databases. This means that the kids are born 2000+ and generally speaking come from good families that can provide medical support. You can't get your SSNs fresher. They won't be used for years to come.

Very cheap and very fresh. Do not think saving a few cents with other vendors is working on the long run. They resell. I keep at their prices and sell you nothing but fresh. Give it a shot and you will be happy you did :)

SEARCHTAGS:

US, United states, USA fullz, Florida fullz, New jersey fullz, New york fullz, apple, vmware, coupons, moneybookers, Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, RDP, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Pennsylvania fullz, Illinois fullz, bitcoin, btc, verizon, twc, comcast, spectrum, xfinity, hulu, hbo, nba, premium, account, spotify, deezer, netflix, passport, mcdonalds, loan, fraud, watches, diamonds, lump sum, documents, carding tutorial, paypal to bitcoin, cc to



CRYPTONIA MARKET
Walletless, Multisig, Simple and Secure

NEW BATCH JUNE 2019

New years available up to 2014. Just 5 years old

This listing is for plain personal info including Social Security Number and Date of birth (SSN DOB) also known as fullz that came from pediatricians databases. This means that the kids are born 2000+ and generally speaking come from good families that can provide medical support. You can't get your SSNs fresher. They won't be used for years to come.

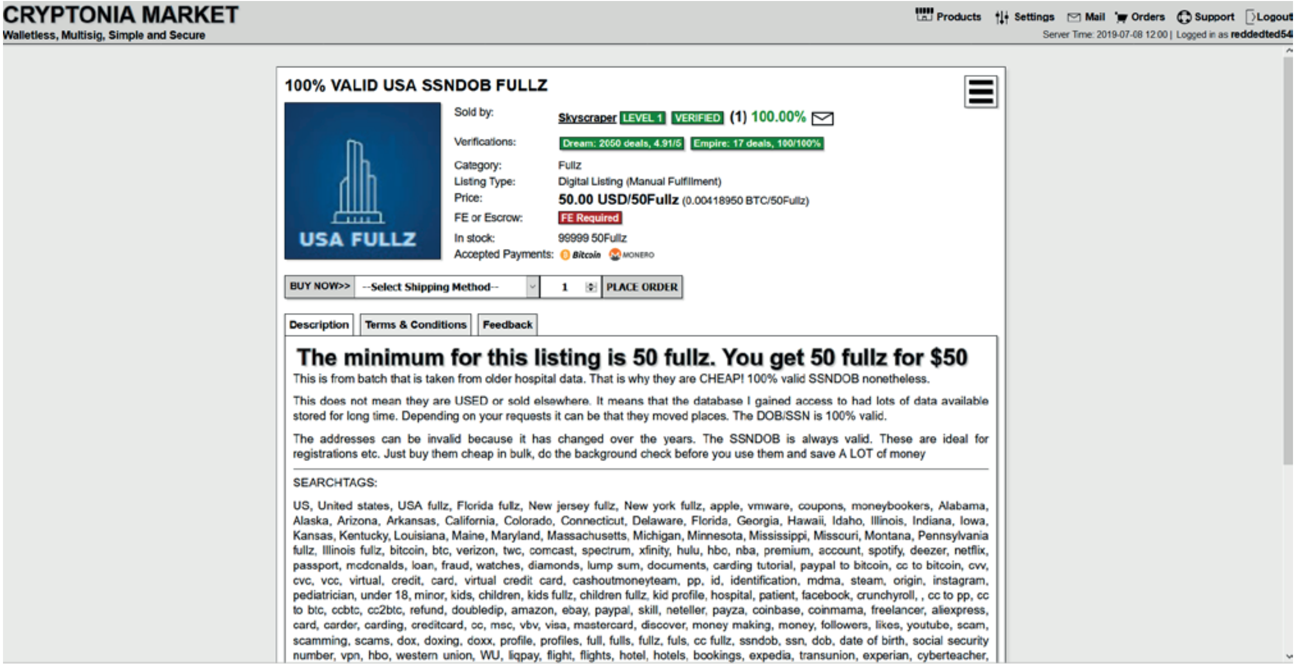
Very cheap and very fresh. Do not think saving a few cents with other vendors is working on the long run. They resell. I keep at their prices and sell you nothing but fresh. Give it a shot and you will be happy you did :)

SEARCHTAGS:

US, United states, USA fullz, Florida fullz, New jersey fullz, New york fullz, apple, vmware, coupons, moneybookers, Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, RDP, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Pennsylvania fullz, Illinois fullz, bitcoin, btc, verizon, twc, comcast, spectrum, xfinity, hulu, hbo, nba, premium, account, spotify, deezer, netflix, passport, mcdonalds, loan, fraud, watches, diamonds, lump sum, documents, carding tutorial, paypal to bitcoin, cc to

bitcoin, cvv, cvc, vcc, virtual, credit, card, virtual credit card, cashoutmoneyteam, pp, id, identification, mdma, steam, origin, instagram, pediatrician, under 18, minor, kids, children, kids fullz, children fullz, kid profile, hospital, patient, facebook, crunchyroll, , cc to pp, cc to btc, ccbtc, cc2btc, refund, doubledip, amazon, ebay, paypal, skill, neteller, payza, coinbase, coinmama, freelancer, aliexpress, card, carder, carding, creditcard, cc, msc, vbv, visa, mastercard, discover, money making, money, followers, likes, youtube, scam, scamming, scams, dox, doxing, doxx, profile, vps, profiles, full, fulls, fullz, fuls, cc fullz, ssndob, ssn, dob, date of birth, social security number, vpn, hbo, western union, WU, liqpay, flight, flights, hotel, hotels, bookings, expedia, transunion, experian, cyberteacher, banned, ebooks, bannedebooksewhoring, e-whoring, ewhore, kalashnikov, isellpizza, courvoisier, antonsen, expectus, hansa, hospital, euro, usd, scans, rdp, vps, server, remote, desktop, protocol, bangbus, brazzers, pornhub, playboy, hackpack, hacking, hackers, white hat, gray hat, grey hat, blackhat, black hat, giftcard, gift, card, transunion, equifax, voucher, funds, transfer, qvc, school of travel, groupon, nectar, british airways, deliveroo, subway, mcdonalds, data, cloud, service, hosting, client, socks, proxy, socks4, socks5, ssh, bitvise, antidetect, fraudfox, localbitcoins, lbtc, lbc, monero, zcash, payment error, phone, gva, google voice, google voice account, counterfeit, airbnb, crypto, template, w99, taxes, IRS, tax, skype, cheque, remote, cheques, check, checks, secure, securing, security, keylogger, administrator, windows, hack, password, stealer, RAT, booter, access, trojan, PSD, PDF, fresh, tickets, shows, disney, theatre, concert, vip72, luxsocks, premsocks, xdedic, spambot, megapack, university, lessons, gmail, samsung, iphone, android, galaxy, note, s7, balance, cerified, certification, ceritfy, moneygram, fargo, wells, wells fargo, trick, suntrust, boa, bank of america, capital one, capone, cap1, citibank, schwabbs, fidelity, chase, chase bank, surveillance, camera, webcam, TD, SSN, social security number, valid_cc_info, st0ned, redson, GGMcloud, kriminal, pastebin, spider, theshop, thinkingforward, certificate, apple, vmware, coupons, moneybookers, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, Nevada Fullz, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming, California fullz, eastcoast, westcoast, skyscraper

#2 Partial data from hospital data - only includes SSNDOB (Social Security Number Date of Birth)



Server Time: 2019-07-08 12:00 | Logged in as reddedted54

100% VALID USA SSNDOB FULLZ

Sold by:	Skyscraper LEVEL 1 VERIFIED (1) 100.00%
Verifications:	Dream: 2050 deals, 4.91/5 Empire: 17 deals, 100/100%
Category:	Fullz
Listing Type:	Digital Listing (Manual Fulfillment)
Price:	50.00 USD/50Fullz (0.00418950 BTC/50Fullz)
FE or Escrow:	FE Required
In stock:	99999 50Fullz
Accepted Payments:	Bitcoin MONERO

The minimum for this listing is 50 fullz. You get 50 fullz for $50

This is from batch that is taken from older hospital data. That is why they are CHEAP! 100% valid SSNDOB nonetheless.

This does not mean they are USED or sold elsewhere. It means that the database I gained access to had lots of data available stored for long time. Depending on your requests it can be that they moved places. The DOB/SSN is 100% valid.

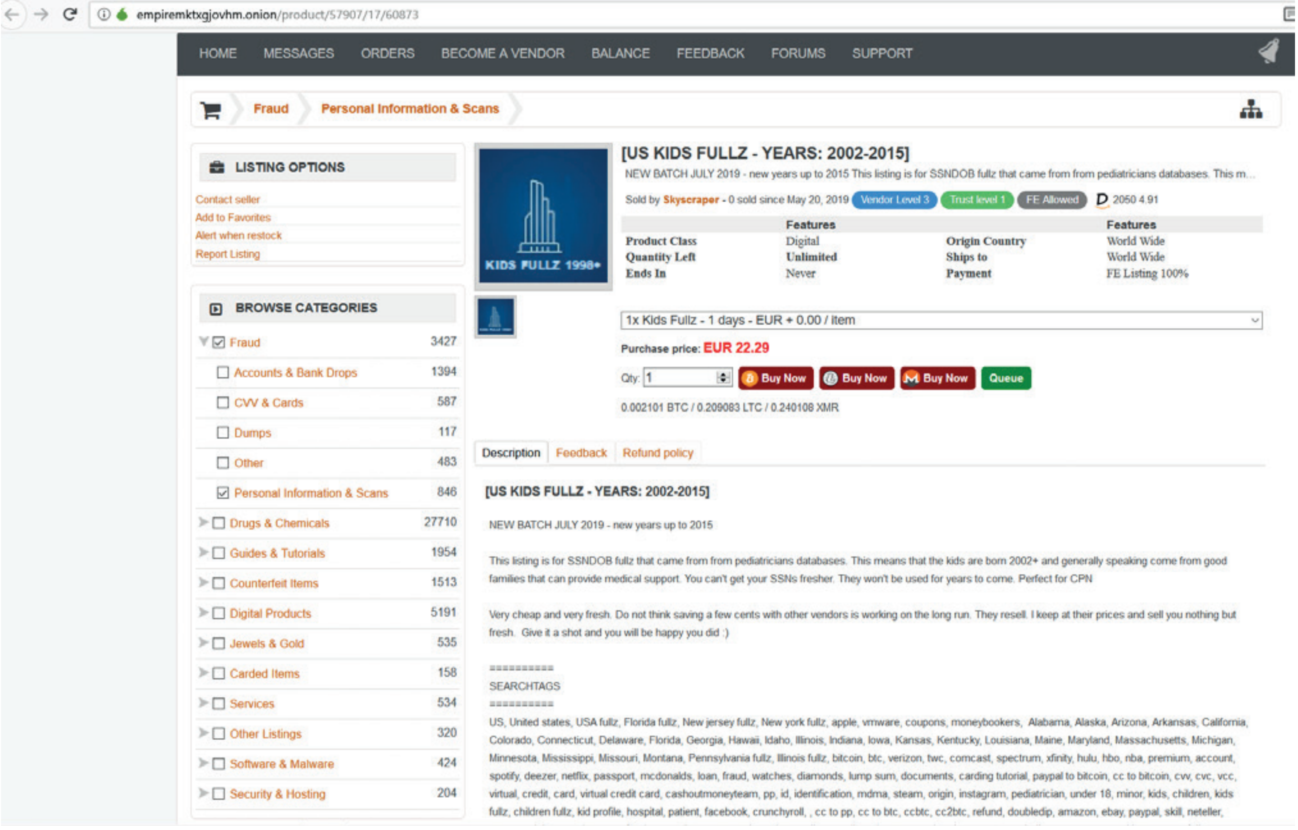
The addresses can be invalid because it has changed over the years. The SSNDOB is always valid. These are ideal for registrations etc. Just buy them cheap in bulk, do the background check before you use them and save A LOT of money

SEARCHTAGS:

US, United states, USA fullz, Florida fullz, New jersey fullz, New york fullz, apple, vmware, coupons, moneybookers, Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Pennsylvania fullz, Illinois fullz, bitcoin, btc, verizon, twc, comcast, spectrum, xfinity, hulu, hbo, nba, premium, account, spotify, deezer, netflix, passport, mcdonalds, loan, fraud, watches, diamonds, lump sum, documents, carding tutorial, paypal to bitcoin, cc to bitcoin, cvv, cvc, vcc, virtual, credit, card, virtual credit card, cashoutmoneyteam, pp, id, identification, mdma, steam, origin, instagram, pediatrician, under 18, minor, kids, children, kids fullz, children fullz, kid profile, hospital, patient, facebook, crunchyroll, , cc to pp, cc to btc, ccbtc, cc2btc, refund, doubledip, amazon, ebay, paypal, skill, neteller, payza, coinbase, coinmama, freelancer, aliexpress, card, carder, carding, creditcard, cc, msc, vbv, visa, mastercard, discover, money making, money, followers, likes, youtube, scam, scamming, scams, dox, doxing, doxx, profile, profiles, full, fulls, fullz, fuls, cc fullz, ssndob, ssn, dob, date of birth, social security number, vpn, hbo, western union, WU, liqpay, flight, flights, hotel, hotels, bookings, expedia, transunion, experian, cyberteacher,

Empire Market

#1 Kidz Fullz



empiremktxgjovhm.onion/product/57907/17/60873

☑ Fraud	3427
☐ Accounts & Bank Drops	1394
☐ CVV & Cards	587
☐ Dumps	117
☐ Other	483
☑ Personal Information & Scans	846
☐ Drugs & Chemicals	27710
☐ Guides & Tutorials	1954
☐ Counterfeit Items	1513
☐ Digital Products	5191
☐ Jewels & Gold	535
☐ Carded Items	158
☐ Services	534
☐ Other Listings	320
☐ Software & Malware	424
☐ Security & Hosting	204

[US KIDS FULLZ - YEARS: 2002-2015]

NEW BATCH JULY 2019 - new years up to 2015 This listing is for SSNDOB fullz that came from from pediatricians databases. This m...

Sold by Skyscraper - 0 sold since May 20, 2019 Vendor Level 3 Trust level 1 FE Allowed D 2050 4.91

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	FE Listing 100%

1x Kids Fullz - 1 days - EUR + 0.00 / item

Purchase price: EUR 22.29

Qty: 1

0.002101 BTC / 0.209083 LTC / 0.240108 XMR

[US KIDS FULLZ - YEARS: 2002-2015]

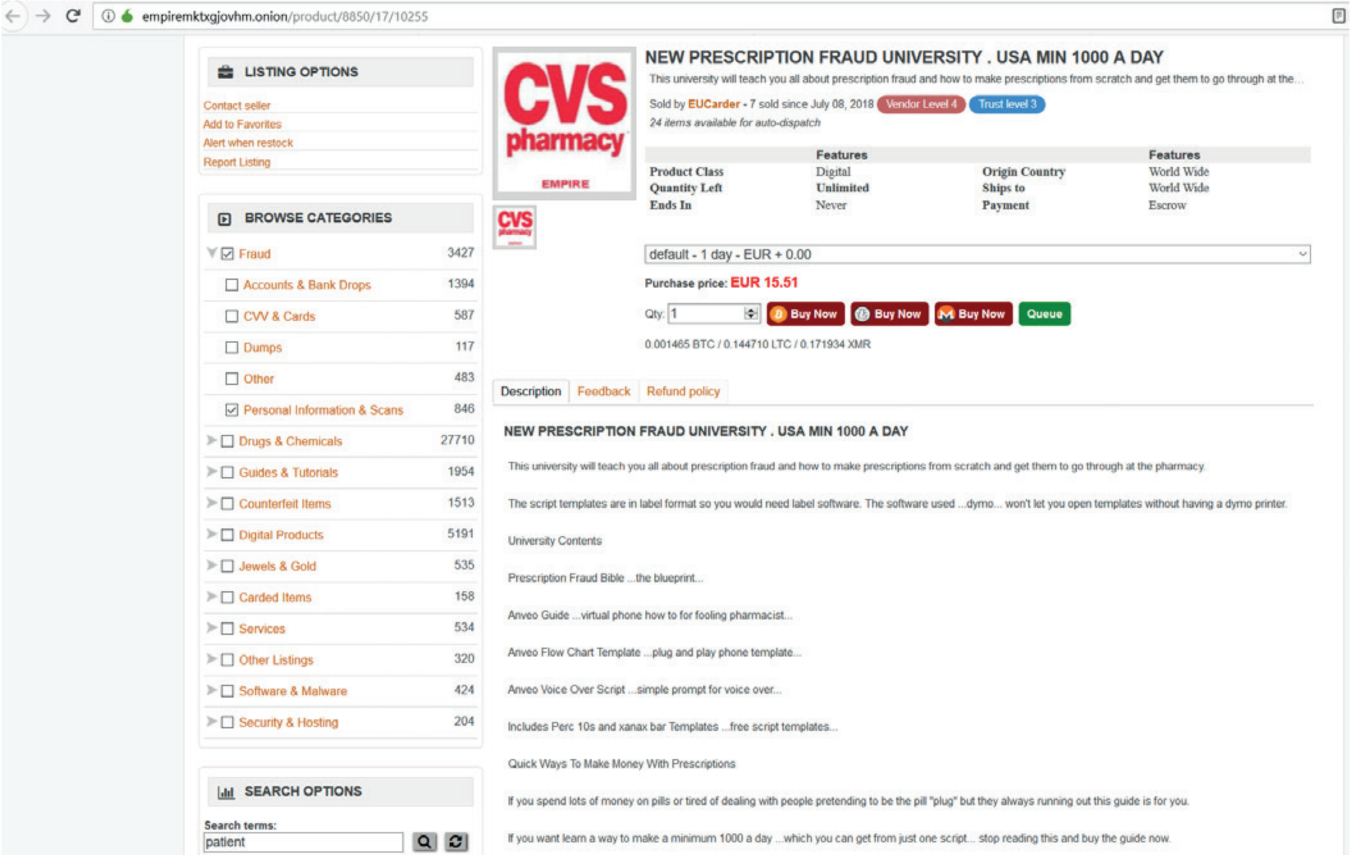
NEW BATCH JULY 2019 - new years up to 2015

This listing is for SSNDOB fullz that came from from pediatricians databases. This means that the kids are born 2002+ and generally speaking come from good families that can provide medical support. You can't get your SSNs fresher. They won't be used for years to come. Perfect for CPN

Very cheap and very fresh. Do not think saving a few cents with other vendors is working on the long run. They resell. I keep at their prices and sell you nothing but fresh. Give it a shot and you will be happy you did :)

==========
SEARCHTAGS
==========
US, United states, USA fullz, Florida fullz, New jersey fullz, New york fullz, apple, vmware, coupons, moneybookers, Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Pennsylvania fullz, Illinois fullz, bitcoin, btc, verizon, twc, comcast, spectrum, xfinity, hulu, hbo, nba, premium, account, spotify, deezer, netflix, passport, mcdonalds, loan, fraud, watches, diamonds, lump sum, documents, carding tutorial, paypal to bitcoin, cc to bitcoin, cvv, cvc, vcc, virtual, credit, card, virtual credit card, cashoutmoneyteam, pp, id, identification, mdma, steam, origin, instagram, pediatrician, under 18, minor, kids, children, kids fullz, children fullz, kid profile, hospital, patient, facebook, crunchyroll, , cc to pp, cc to btc, ccbtc, cc2btc, refund, doubledip, amazon, ebay, paypal, skill, neteller,

#2 Prescription Fraud Course



BROWSE CATEGORIES

☑ Fraud	3427
□ Accounts & Bank Drops	1394
□ CVV & Cards	587
□ Dumps	117
□ Other	483
☑ Personal Information & Scans	846
□ Drugs & Chemicals	27710
□ Guides & Tutorials	1954
□ Counterfeit Items	1513
□ Digital Products	5191
□ Jewels & Gold	535
□ Carded Items	158
□ Services	534
□ Other Listings	320
□ Software & Malware	424
□ Security & Hosting	204

Search terms: patient

NEW PRESCRIPTION FRAUD UNIVERSITY . USA MIN 1000 A DAY

This university will teach you all about prescription fraud and how to make prescriptions from scratch and get them to go through at the...

Sold by EUCarder - 7 sold since July 08, 2018 Vendor Level 4 Trust level 3

24 items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - EUR + 0.00

Purchase price: EUR 15.51

Qty: 1

0.001465 BTC / 0.144710 LTC / 0.171934 XMR

NEW PRESCRIPTION FRAUD UNIVERSITY . USA MIN 1000 A DAY

This university will teach you all about prescription fraud and how to make prescriptions from scratch and get them to go through at the pharmacy.

The script templates are in label format so you would need label software. The software used ...dymo... won't let you open templates without having a dymo printer.

University Contents

Prescription Fraud Bible ...the blueprint...

Anveo Guide ...virtual phone how to for fooling pharmacist...

Anveo Flow Chart Template ...plug and play phone template...

Anveo Voice Over Script ...simple prompt for voice over...

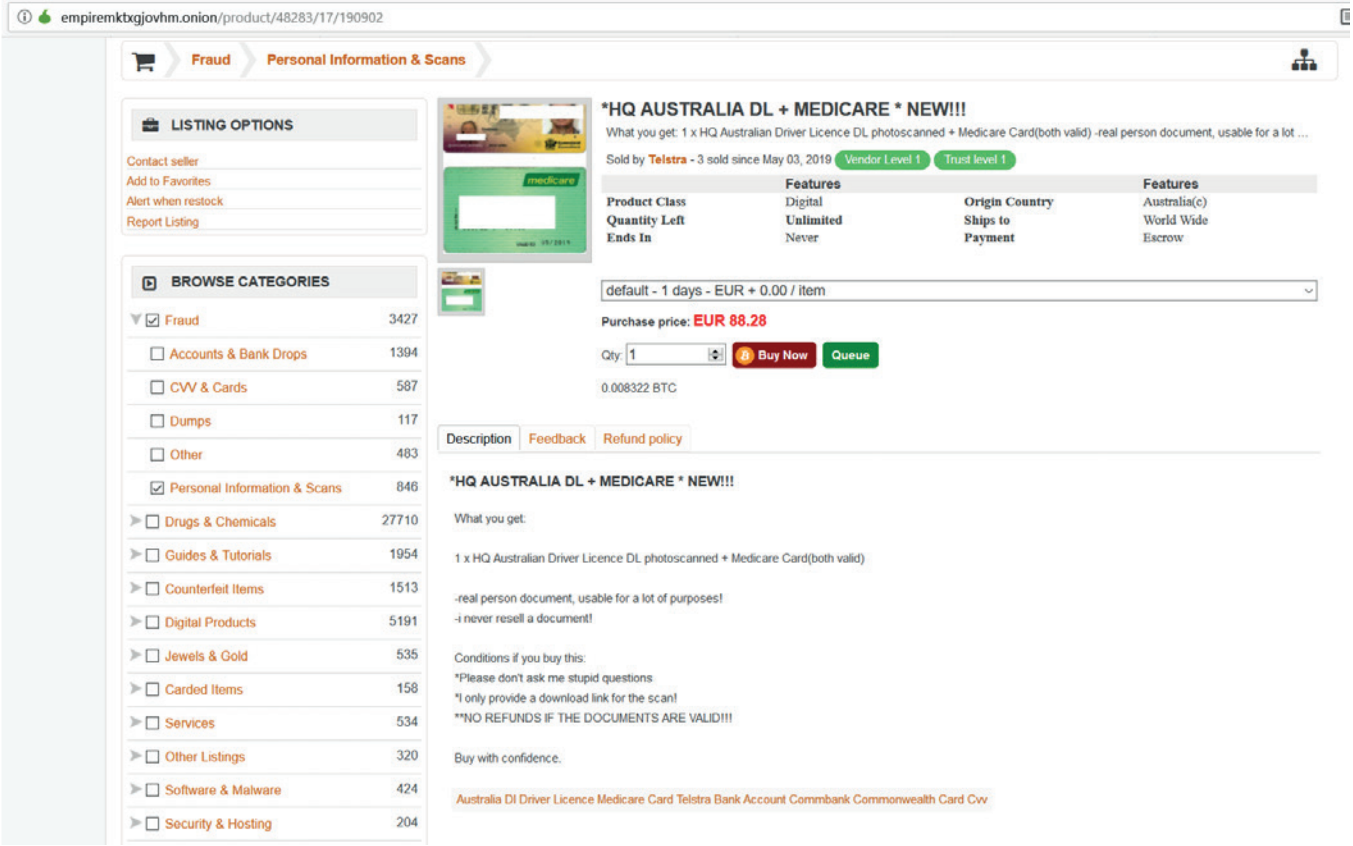
Includes Perc 10s and xanax bar Templates ...free script templates...

Quick Ways To Make Money With Prescriptions

If you spend lots of money on pills or tired of dealing with people pretending to be the pill "plug" but they always running out this guide is for you.

If you want learn a way to make a minimum 1000 a day ...which you can get from just one script... stop reading this and buy the guide now.

#3 Medicare Card (Australia)



BROWSE CATEGORIES

☑ Fraud	3427
□ Accounts & Bank Drops	1394
□ CVV & Cards	587
□ Dumps	117
□ Other	483
☑ Personal Information & Scans	846
□ Drugs & Chemicals	27710
□ Guides & Tutorials	1954
□ Counterfeit Items	1513
□ Digital Products	5191
□ Jewels & Gold	535
□ Carded Items	158
□ Services	534
□ Other Listings	320
□ Software & Malware	424
□ Security & Hosting	204

***HQ AUSTRALIA DL + MEDICARE * NEW!!!**

What you get: 1 x HQ Australian Driver Licence DL photoscanned + Medicare Card(both valid) -real person document, usable for a lot ...

Sold by Telstra - 3 sold since May 03, 2019 Vendor Level 1 Trust level 1

	Features		Features
Product Class	Digital	Origin Country	Australia(c)
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 days - EUR + 0.00 / item

Purchase price: EUR 88.28

Qty: 1

0.008322 BTC

***HQ AUSTRALIA DL + MEDICARE * NEW!!!**

What you get:

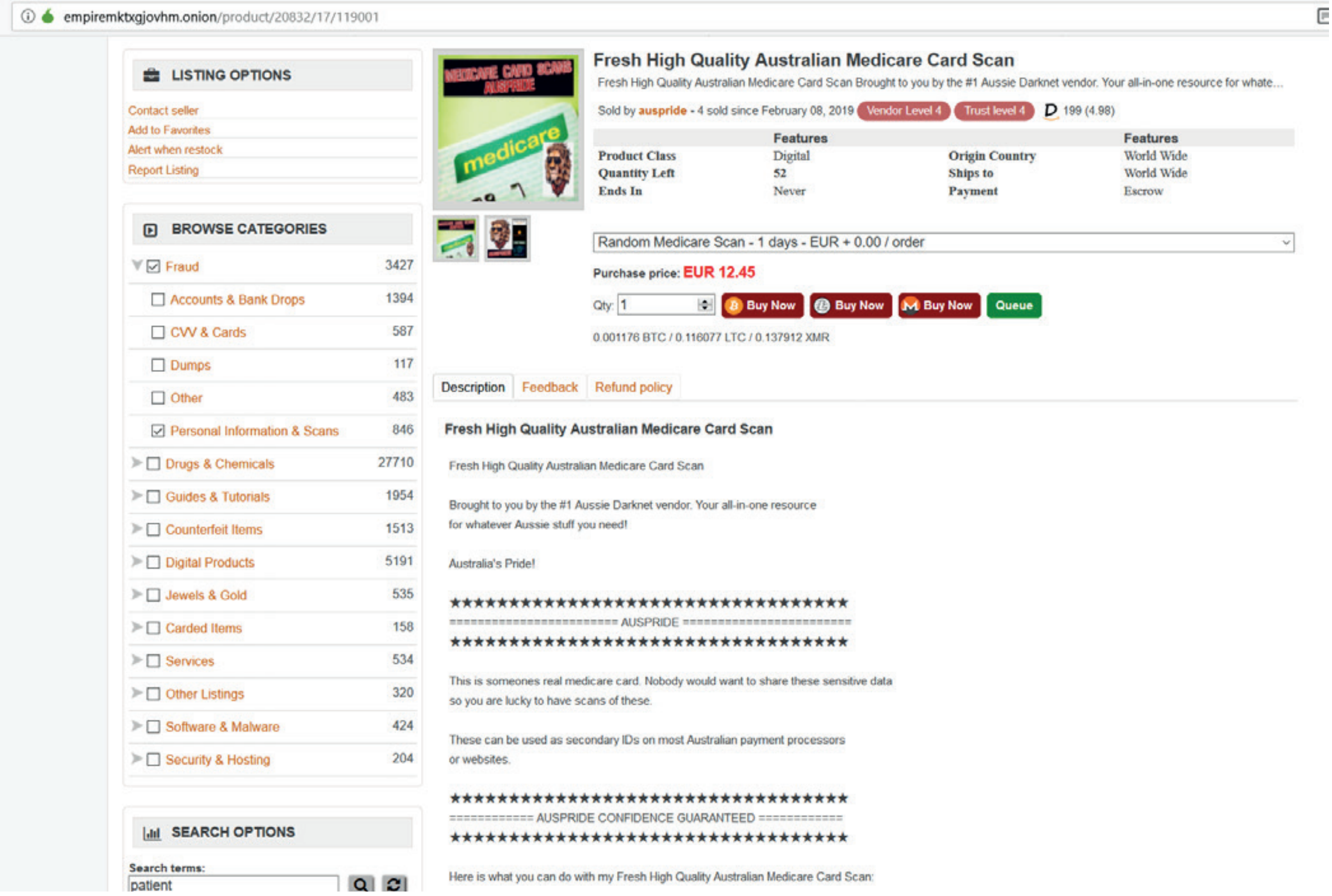
1 x HQ Australian Driver Licence DL photoscanned + Medicare Card(both valid)

-real person document, usable for a lot of purposes!
-i never resell a document!

Conditions if you buy this:
*Please don't ask me stupid questions
*I only provide a download link for the scan!
**NO REFUNDS IF THE DOCUMENTS ARE VALID!!!

Buy with confidence.

Australia Dl Driver Licence Medicare Card Telstra Bank Account Commbank Commonwealth Card Cvv



empiremktxgjovhm.onion/product/20832/17/119001

LISTING OPTIONS

Contact seller
Add to Favorites
Alert when restock
Report Listing

BROWSE CATEGORIES

☑ Fraud	3427
□ Accounts & Bank Drops	1394
□ CVV & Cards	587
□ Dumps	117
□ Other	483
☑ Personal Information & Scans	846
□ Drugs & Chemicals	27710
□ Guides & Tutorials	1954
□ Counterfeit Items	1513
□ Digital Products	5191
□ Jewels & Gold	535
□ Carded Items	158
□ Services	534
□ Other Listings	320
□ Software & Malware	424
□ Security & Hosting	204

SEARCH OPTIONS

Search terms: patient

Fresh High Quality Australian Medicare Card Scan

Fresh High Quality Australian Medicare Card Scan Brought to you by the #1 Aussie Darknet vendor. Your all-in-one resource for whate...

Sold by auspride - 4 sold since February 08, 2019 Vendor Level 4 Trust level 4 D 199 (4.98)

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	52	Ships to	World Wide
Ends In	Never	Payment	Escrow

Random Medicare Scan - 1 days - EUR + 0.00 / order

Purchase price: EUR 12.45

Qty: 1 Buy Now Buy Now Buy Now Queue

0.001176 BTC / 0.116077 LTC / 0.137912 XMR

Description Feedback Refund policy

Fresh High Quality Australian Medicare Card Scan

Fresh High Quality Australian Medicare Card Scan

Brought to you by the #1 Aussie Darknet vendor. Your all-in-one resource
for whatever Aussie stuff you need!

Australia's Pride!

★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★
======================== AUSPRIDE ========================
★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★

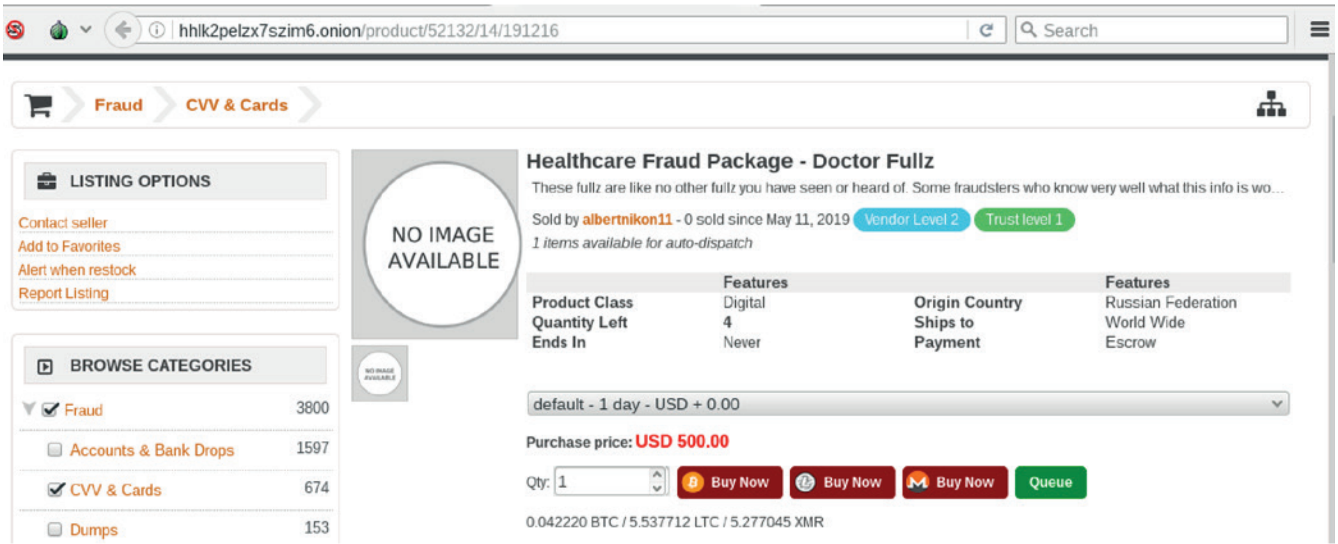
This is someones real medicare card. Nobody would want to share these sensitive data
so you are lucky to have scans of these.

These can be used as secondary IDs on most Australian payment processors
or websites.

★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★
============ AUSPRIDE CONFIDENCE GUARANTEED ============
★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★

Here is what you can do with my Fresh High Quality Australian Medicare Card Scan:

#4 Healthcare Fraud Package



hhlk2pelzx7szim6.onion/product/52132/14/191216

Fraud > CVV & Cards

LISTING OPTIONS

Contact seller
Add to Favorites
Alert when restock
Report Listing

BROWSE CATEGORIES

☑ Fraud	3800
□ Accounts & Bank Drops	1597
☑ CVV & Cards	674
□ Dumps	153

Healthcare Fraud Package - Doctor Fullz

These fullz are like no other fullz you have seen or heard of. Some fraudsters who know very well what this info is wo...

Sold by albertnikon11 - 0 sold since May 11, 2019 Vendor Level 2 Trust level 1

1 items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	Russian Federation
Quantity Left	4	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: USD 500.00

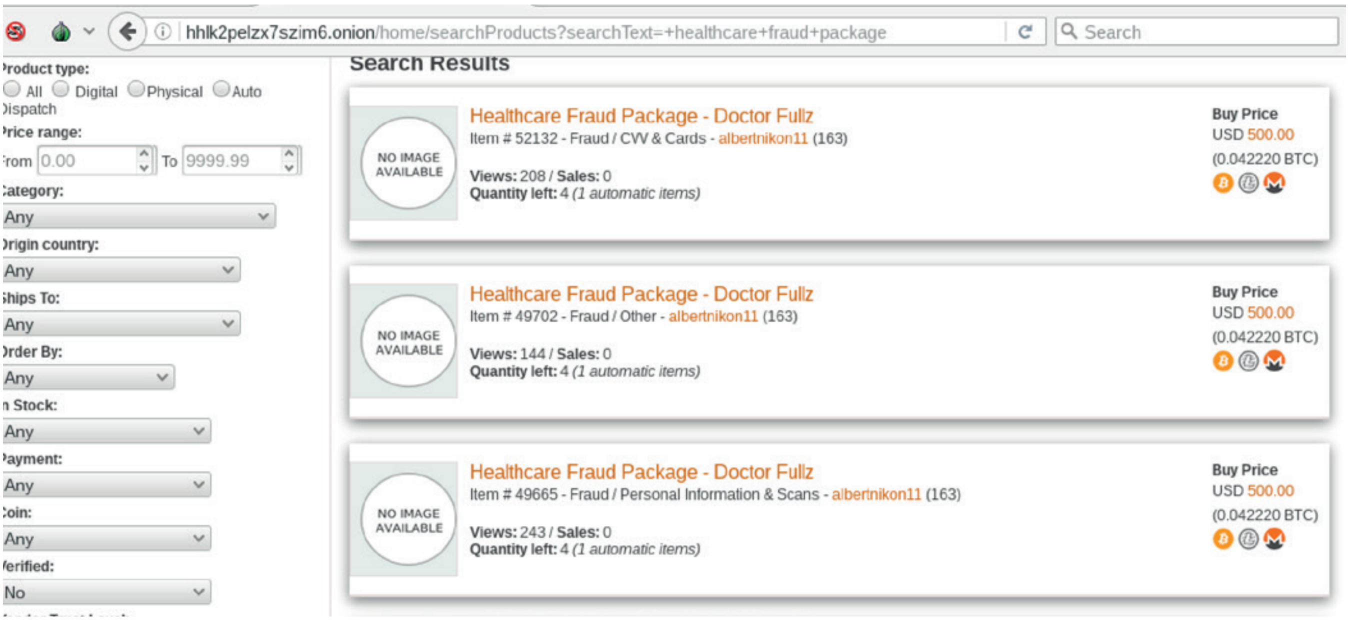
Qty: 1 Buy Now Buy Now Buy Now Queue

0.042220 BTC / 5.537712 LTC / 5.277045 XMR

Using just 1 doctor identity you can make hundreds of thousands of dollars in just a few months, if you are skilled at this and have experience you can easily make over $1,000,000 in a year.

This listing is for a pack with the following documents (High Quality Color Scans):
Bachelor Diploma
Bachelor Medical Technology
Resume
Malpractice Insurance Document
Medical Diploma & Board Recommendations
Medical Doctor License
DEA License
Medical Technologist Certification (ASCP)
New Mexico MD License
Driving License Scan
Passport Scan

If you have any questions about the info freshness, quality, etc contact me. I have a limited supply but I can get bulk amounts if you are looking for them in bulk.



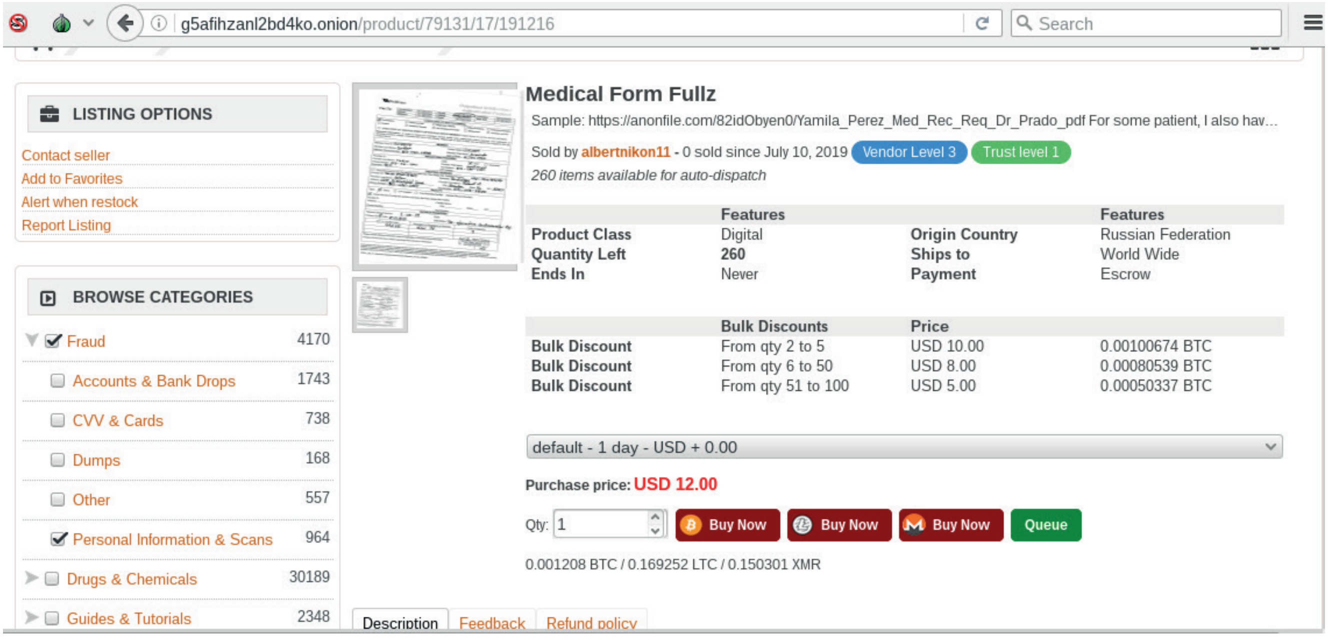
hhlk2pelzx7szim6.onion/home/searchProducts?searchText=+healthcare+fraud+package

roduct type:
○ All ○ Digital ○ Physical ○ Auto
ispatch
rice range:
rom 0.00 To 9999.99
ategory: Any
rigin country: Any
hips To: Any
rder By: Any
n Stock: Any
ayment: Any
oin: Any
erified: No

Search Results

NO IMAGE AVAILABLE	Healthcare Fraud Package - Doctor Fullz Item # 52132 - Fraud / CVV & Cards - albertnikon11 (163) Views: 208 / Sales: 0 Quantity left: 4 *(1 automatic items)*	Buy Price USD 500.00 (0.042220 BTC)
NO IMAGE AVAILABLE	Healthcare Fraud Package - Doctor Fullz Item # 49702 - Fraud / Other - albertnikon11 (163) Views: 144 / Sales: 0 Quantity left: 4 *(1 automatic items)*	Buy Price USD 500.00 (0.042220 BTC)
NO IMAGE AVAILABLE	Healthcare Fraud Package - Doctor Fullz Item # 49665 - Fraud / Personal Information & Scans - albertnikon11 (163) Views: 243 / Sales: 0 Quantity left: 4 *(1 automatic items)*	Buy Price USD 500.00 (0.042220 BTC)

#5 Medical Form Fullz



g5afihzanl2bd4ko.onion/product/79131/17/191216

LISTING OPTIONS
- Contact seller
- Add to Favorites
- Alert when restock
- Report Listing

BROWSE CATEGORIES

☑ Fraud	4170
□ Accounts & Bank Drops	1743
□ CVV & Cards	738
□ Dumps	168
□ Other	557
☑ Personal Information & Scans	964
□ Drugs & Chemicals	30189
□ Guides & Tutorials	2348

Medical Form Fullz

Sample: https://anonfile.com/82idObyen0/Yamila_Perez_Med_Rec_Req_Dr_Prado_pdf For some patient, I also hav...

Sold by albertnikon11 - 0 sold since July 10, 2019 Vendor Level 3 Trust level 1

260 items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	Russian Federation
Quantity Left	260	Ships to	World Wide
Ends In	Never	Payment	Escrow

	Bulk Discounts	Price	
Bulk Discount	From qty 2 to 5	USD 10.00	0.00100674 BTC
Bulk Discount	From qty 6 to 50	USD 8.00	0.00080539 BTC
Bulk Discount	From qty 51 to 100	USD 5.00	0.00050337 BTC

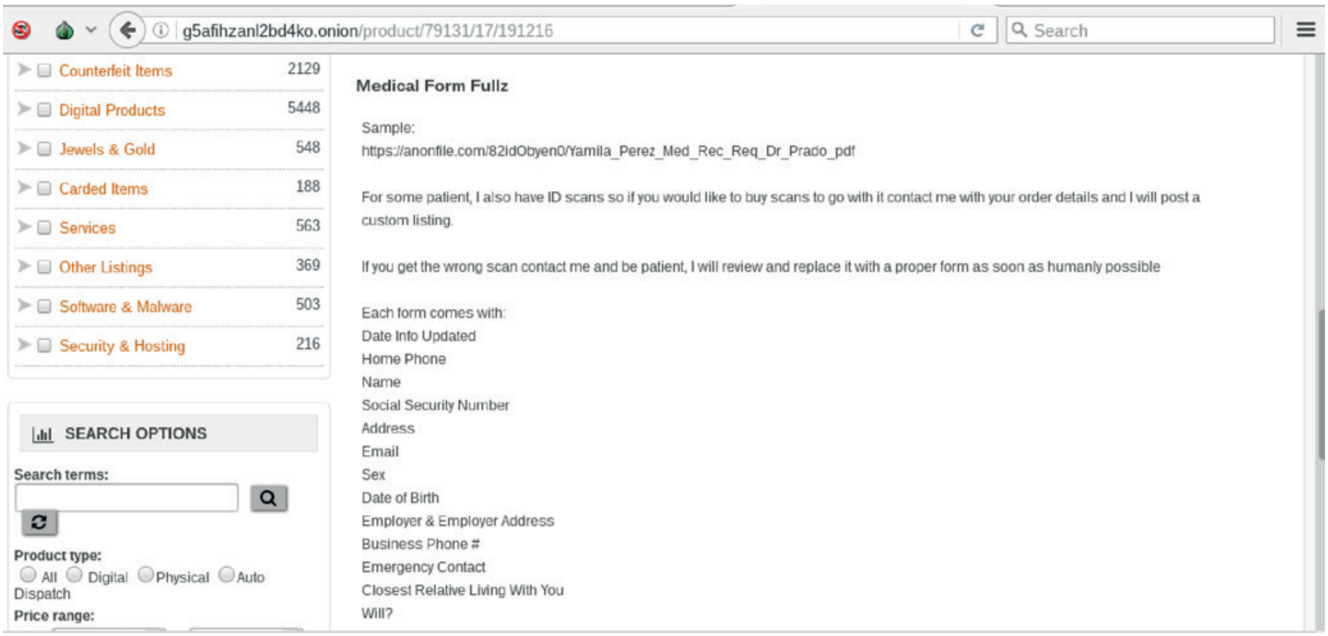
default - 1 day - USD + 0.00

Purchase price: USD 12.00

Qty: 1 Buy Now Buy Now Buy Now Queue

0.001208 BTC / 0.169252 LTC / 0.150301 XMR

Description Feedback Refund policy



g5afihzanl2bd4ko.onion/product/79131/17/191216

□ Counterfeit Items	2129
□ Digital Products	5448
□ Jewels & Gold	548
□ Carded Items	188
□ Services	563
□ Other Listings	369
□ Software & Malware	503
□ Security & Hosting	216

SEARCH OPTIONS

Search terms:

Product type:
○ All ○ Digital ○ Physical ○ Auto
Dispatch
Price range:

Medical Form Fullz

Sample:
https://anonfile.com/82idObyen0/Yamila_Perez_Med_Rec_Req_Dr_Prado_pdf

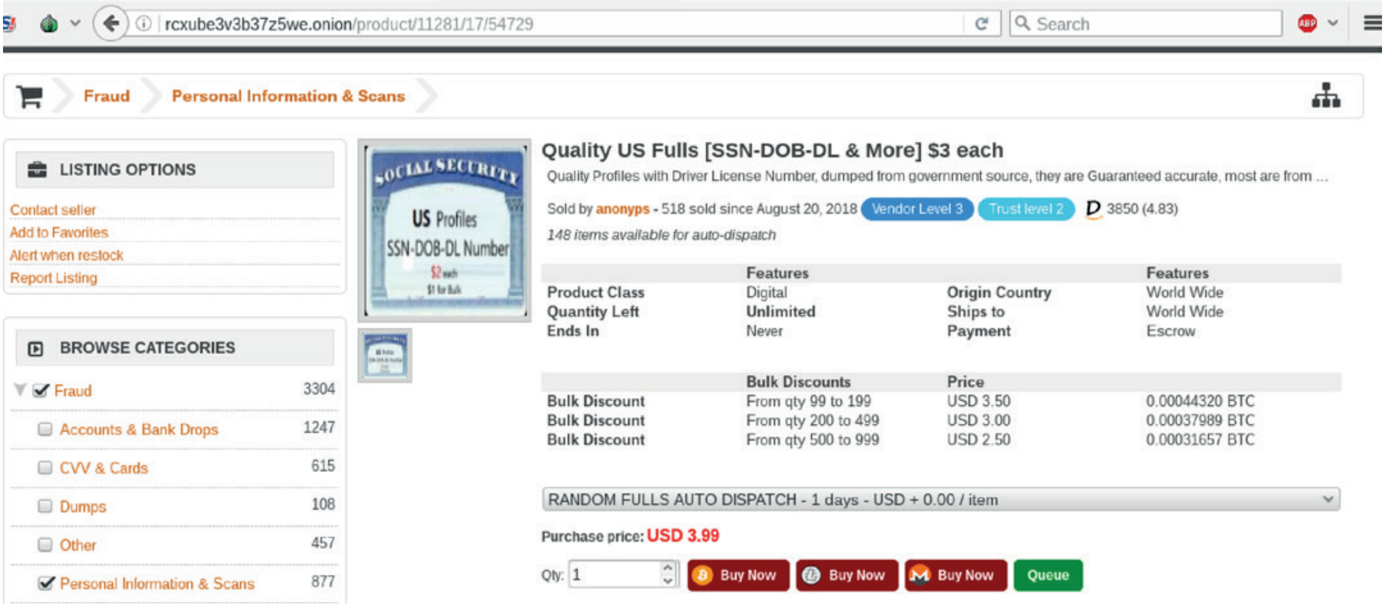
For some patient, I also have ID scans so if you would like to buy scans to go with it contact me with your order details and I will post a custom listing.

If you get the wrong scan contact me and be patient, I will review and replace it with a proper form as soon as humanly possible

Each form comes with:
Date Info Updated
Home Phone
Name
Social Security Number
Address
Email
Sex
Date of Birth
Employer & Employer Address
Business Phone #
Emergency Contact
Closest Relative Living With You
Will?

Examples for non-healthcare related listings

#1 Empire Market: US Fulls



rcxube3v3b37z5we.onion/product/11281/17/54729

Fraud > Personal Information & Scans

LISTING OPTIONS

Contact seller
Add to Favorites
Alert when restock
Report Listing

BROWSE CATEGORIES

☑ Fraud	3304
□ Accounts & Bank Drops	1247
□ CVV & Cards	615
□ Dumps	108
□ Other	457
☑ Personal Information & Scans	877

Quality US Fulls [SSN-DOB-DL & More] $3 each

Quality Profiles with Driver License Number, dumped from government source, they are Guaranteed accurate, most are from ...

Sold by anonyps - 518 sold since August 20, 2018 Vendor Level 3 Trust level 2 D 3850 (4.83)

148 items available for auto-dispatch

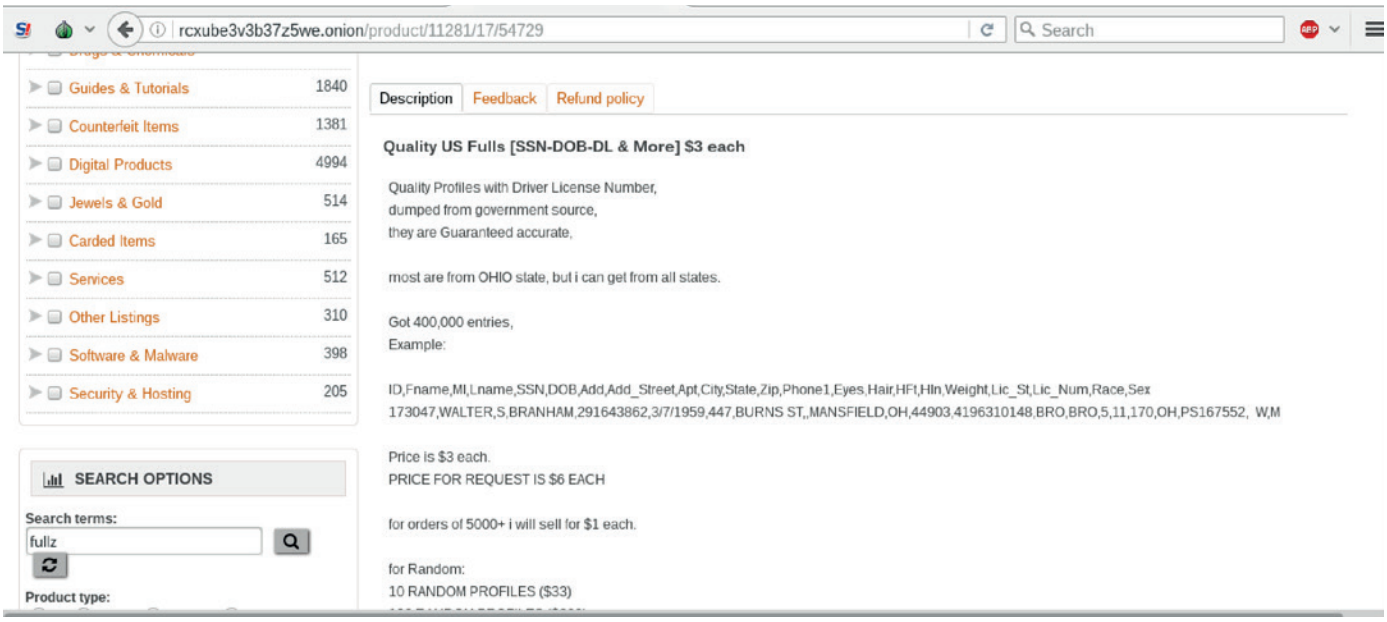
	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

	Bulk Discounts	Price	
Bulk Discount	From qty 99 to 199	USD 3.50	0.00044320 BTC
Bulk Discount	From qty 200 to 499	USD 3.00	0.00037989 BTC
Bulk Discount	From qty 500 to 999	USD 2.50	0.00031657 BTC

RANDOM FULLS AUTO DISPATCH - 1 days - USD + 0.00 / item

Purchase price: USD 3.99

Qty: 1



rcxube3v3b37z5we.onion/product/11281/17/54729

□ Guides & Tutorials	1840
□ Counterfeit Items	1381
□ Digital Products	4994
□ Jewels & Gold	514
□ Carded Items	165
□ Services	512
□ Other Listings	310
□ Software & Malware	398
□ Security & Hosting	205

SEARCH OPTIONS

Search terms: fullz

Product type:

Quality US Fulls [SSN-DOB-DL & More] $3 each

Quality Profiles with Driver License Number,
dumped from government source,
they are Guaranteed accurate,

most are from OHIO state, but i can get from all states.

Got 400,000 entries,
Example:

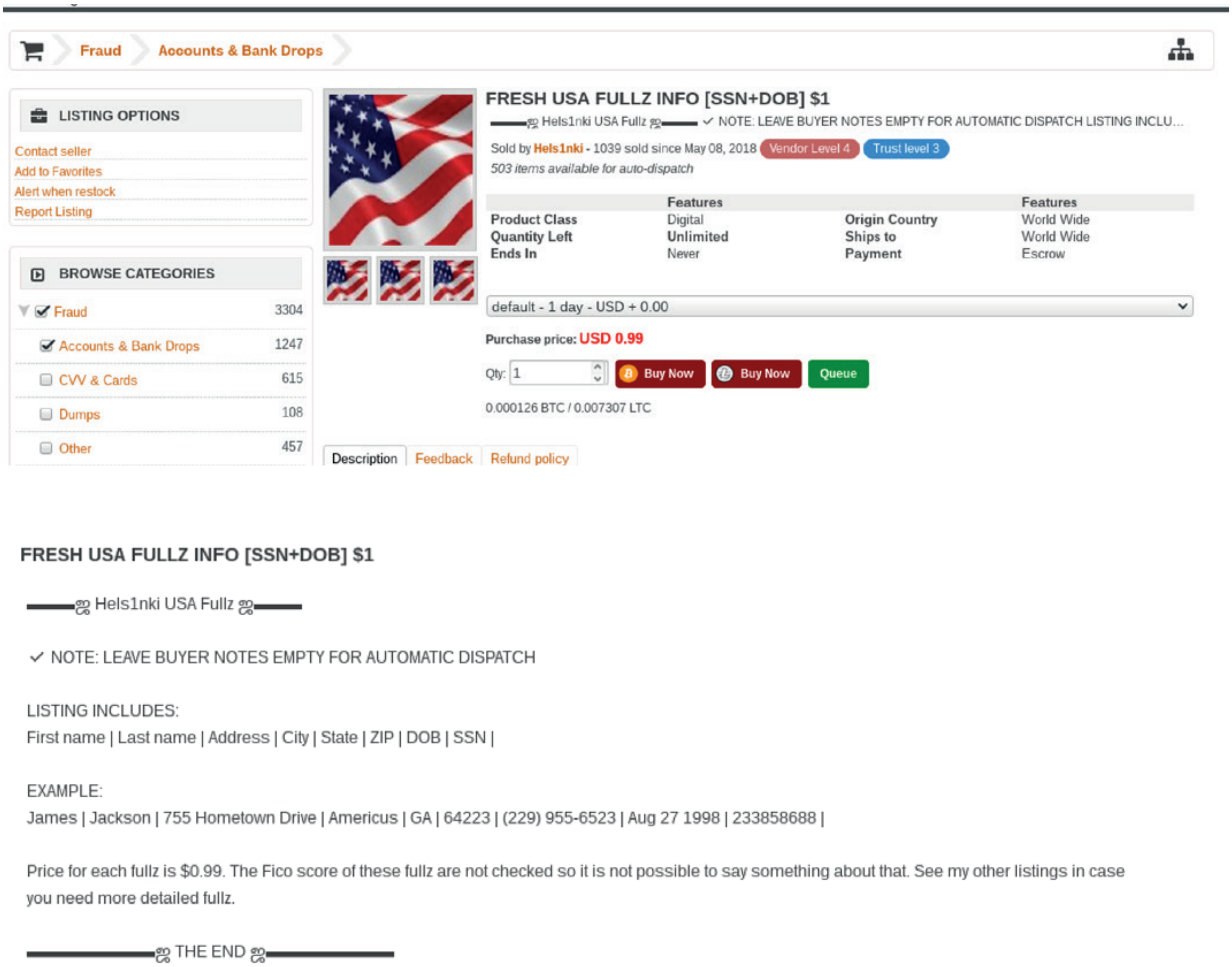
```
ID,Fname,MI,Lname,SSN,DOB,Add,Add_Street,Apt,City,State,Zip,Phone1,Eyes,Hair,HFt,HIn,Weight,Lic_St,Lic_Num,Race,Sex
173047,WALTER,S,BRANHAM,291643862,3/7/1959,447,BURNS ST,,MANSFIELD,OH,44903,4196310148,BRO,BRO,5,11,170,OH,PS167552,  W,M
```

Price is $3 each.
PRICE FOR REQUEST IS $6 EACH

for orders of 5000+ i will sell for $1 each.

for Random:
10 RANDOM PROFILES ($33)

#2 Fresh USA FULLZ



FRESH USA FULLZ INFO [SSN+DOB] $1

━━━━ஐ Hels1nki USA Fullz ஐ━━━━ ✓ NOTE: LEAVE BUYER NOTES EMPTY FOR AUTOMATIC DISPATCH LISTING INCLU...

Sold by **Hels1nki** - 1039 sold since May 08, 2018 Vendor Level 4 Trust level 3

503 items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: USD 0.99

Qty: 1

0.000126 BTC / 0.007307 LTC

FRESH USA FULLZ INFO [SSN+DOB] $1

━━━━ஐ Hels1nki USA Fullz ஐ━━━━

✓ NOTE: LEAVE BUYER NOTES EMPTY FOR AUTOMATIC DISPATCH

LISTING INCLUDES:
First name | Last name | Address | City | State | ZIP | DOB | SSN |

EXAMPLE:
James | Jackson | 755 Hometown Drive | Americus | GA | 64223 | (229) 955-6523 | Aug 27 1998 | 233858688 |

Price for each fullz is $0.99. The Fico score of these fullz are not checked so it is not possible to say something about that. See my other listings in case you need more detailed fullz.

━━━━━━━━ஐ THE END ஐ━━━━━━━━

Findings

This research is in no way meant to be representative and only serves to give some insights and "reality check" towards the assumptions we raised earlier in form of our hypotheses and also to provide a picture on how frequent health data is traded on the dark markets.

Additionally, we wanted to check what the references such as underground markets and darknet markets used by the industry actually mean, without just blindly repeating what others have said. One particular phenomenon we noticed when gathering existing knowledge and research on the topic was that everyone seemed to just refer to each other by describing how health data is sold in the underground or on darknet/dark web/deep web forum and markets.

But it was rather difficult to find concrete references on where exactly, which markets, for how much, etc.

Therefore, we wanted to advocate a very transparent approach, showing what we have found, when and what the actual state of trade is (always put in context to our limitations of access).

In the following overview, we provide listings we came across that we deemed as relevant to this research.

Darknet Marketplace	Listing	Price/Unit
Cryptonia	**Kidz Fullz** ▪ SSN DOB	$20/1 (USD)
Cryptonia	**Partial data from Hospital breach** ▪ SSN DOB	$50/50 (USD)
Empire	**Kidz Medical Fullz** ▪ SSN DOB	$24/1 (converted to USD)
Empire	**Prescription Fraud Course** ▪ script templates ▪ how to fool pharmacist guide ▪ quick ways to make money guide	$16.97/1 (converted to USD)
Empire	**Medicare Card (Australia)** ▪ 1x HQ Australian Driver License DL photo scanned ▪ Medicare Card ▪ both valid	$97.84/1 (converted to USD)
Empire	**Healthcare Fraud Package** ▪ Bachelor Diploma ▪ Bachelor Medical Technology ▪ Resume ▪ Malpractice Insurance Document ▪ Medical Diploma & Board Recommendation ▪ DEA License ▪ Medical Technologist Certification (ASCP) ▪ New Mexico MD License ▪ Driving License Scan ▪ Passport Scan	$500/1
Empire	**Medical Form Fullz** ▪ Date Info updated ▪ Home Phone ▪ Name ▪ Social Security Number ▪ Address ▪ Email ▪ Sex ▪ Employer & Employer Address ▪ Business Phone ▪ Emergency Contact ▪ Closest Relative Living with you ▪ Will ▪ for some patients, ID scans available	$12/1

Findings - Hypothesis I:

Health data is more attractive to an attacker because it brings more value due to its multitude of information, e.g. financial data, PII, medical history

When looking at our first assumption, based on our findings it was rather hard to confirm or refute if health data is more attractive. This is partly due to the fact that health data was not as present as the amount of pure financial and PII records. One reason could be the recent shutdown of marketplaces since some sources had referenced to markets that had just been taken down when we started our research. This was evident by looking at one seller.

This seller had about 17 listings on the Empire Market, at the time of data collection, and 2050 listings on the DreamMarket. The seller seemed to deal exclusively in fullz and fraud-related data and, as it seemed, might have just recently moved to the Empire Market after the DreamMarket shut down. Another aspect is that not all listings might be labeled as originating from healthcare breaches. We have found some listings where the seller stated that those were taken from healthcare databases and sold more cheaply since it was only the financial or PII part of it that was sold.

Generally, we still agree that health data, when sold as a whole, is more attractive and can be used and therefore sold for different purposes, depending what a buyer is looking for and what motivation is behind the buy.

Findings - Hypothesis II:

Stolen health data is sold for a higher price per record on online markets in comparison to other stolen data such as financial data

Based on what listings we were able to find; we can confirm that healthcare-related listings were sold more expensive than "just" financial data or PII. The listing that we found that sold data such as SSN DOB from a healthcare dump was in line with the value between $1 to $3.99 for a normal record not related to healthcare data (see "Partial data from Hospital breach" in Table 2).

This could be due to the variety of purposes health data can be used for, e.g. insurance fraud, prescription fraud, drug diversion or identity theft. And also, that health data has a long shelf life since it might take time until detection and if detected most of the leaked data can still not be changed since it is data that stays lifelong.

All of this makes health data more valuable to a potential buyer. Also, demand can influence the price, while the marketplaces are full of financial data and PII fullz, health data is not as present, and this impacts the price.

Additional Findings

Interestingly, while looking for health data that would more or less focus on leaked patient data and all that comes with it, we found other healthcare-related data being sold on the marketplaces that we did not consider beforehand.

One example was that we came across one data dump that sold children's data which came from a breached pediatrician's database. We came across two listings from the same seller but at two different marketplaces (Empire and Cryptonia), one included information of children born in the years 2000+ and the other included children born in the years 2002+.

The listing "only" included SSN DOB data, but the seller argued that these are especially valuable since those will not be used for years. What he or she means by that is that until the child has grown and starts registering at public entities such as the bank, insurance claims, etc., it might take years and consequently, those SSN can be used for various types of frauds for a long time with low risk of detection.

The seller even recommends that the record is perfect for "CPN", which stands for Credit Profile Number. How this could be leveraged by a buyer is that the PII data can be used to create a good CPN score, which will enable that person to buy goods and services with a good (but fake) credit score. The CPN can also replace SSN in some cases when applying for credit[31], which means this sort of identity theft can remain undetected even longer than when using a victim's SSN. The CPN is used in the United States, and therefore can only be applied there.

In comparison to actual health data, the value of one "Kidz Fullz" record was $20, which is less than one might expect for health-related data but more than a normal SSN DOB listing. This is probably due to the reason just mentioned before, those records also have a longer shelf-life due to the age of the victim and lower risk of detection.

A strange doctor

Another interesting finding was the "Healthcare Fraud Package - Doctors Fullz" listing. While we had our focus on patient data, we did not consider that doctors might also be a lucrative victim for insurance fraud. In this case, the seller underlined the lucrativeness by stating: "Using just one doctor identity you can make hundreds of thousands of dollars in just a few months, if you are skilled at this and have experience you can easily make over $1,000,000 in a year." This kind of fraud depends heavily on the country since not all healthcare systems work the same and insurance claims from a doctor might be unique to one country's procedure, in this case, the U.S.

The doctors fullz was the most expensive listing and also the most comprehensive, including many documents that would support the identity claim of the fraudster.

Based on each country's healthcare system, medical fraud opportunities vary and provide either very good possibilities to fraud for example insurances or turn out to be more difficult. Especially, in the U.S. and Australia, fraud seemed to be easier based on stolen health data.

This was also evident based on the listing on Medicare cards, which was the second most expensive listing we found, with a sales value of $97.84 per record.

Additionally, one of the listings, the Medical Form Fullz listing, seemed to be scans from faxes. This supports the current state of the healthcare sector that data loss is still caused by loss of an analog medium such as a paper form. Here, speculations could be made to how this data was breached. It could be that the forms were not disposed correctly and someone else gained access to them. It could also be that an insider collected those and scanned them with the intention to sell them online. Or, that through a compromised email account the scans were sent to a printer/fax machine and the forms were leaked. Several possibilities exist how the seller might have come to the possession of those medical forms.

Conclusion

Dark Figures

There is no doubt that healthcare data is being sold and traded in underground circles. Due to the volatile nature of the darknet and presumably, limited visibility, it's hard to judge exactly how widespread the activity is.

As we have shown, our biggest limitation was access to marketplaces due to above-mentioned reason. Nevertheless, we can definitely see why someone is attracted to buy medical fullz because possibilities of leveraging health data are extensive and can serve several purposes to defraud or harm a victim.

The healthcare sector is especially an interesting one and will remain an attractive target due to its immaturity for security while simultaneously being in the middle of digital transformation.

The latter might then increase the usage of third-party providers, supporting the industry moving towards digitalization and offering services such as data storage of patient data or the implementation of medical IoTs.

This increases the attack surface for an attacker while at the same time healthcare personnel is not trained or equipped enough to secure its assets. Especially doctors seem to be a lucrative target in certain countries where the healthcare system can be easily defrauded through false insurance claims.

Recommendations
to the healthcare sector

- **Patch, patch, and patch. Practice good cyber hygiene and update systems within a reasonable time to address known vulnerabilities.**
- **Offer cyber awareness training to healthcare personnel. Healthcare service providers are not just offering medical care anymore but are also storing a vast amount of sensitive data.**
- **Practice network security through network segmentation including segmenting applications, user and data. This will help to isolate and identify threats as well as applying policies and control mechanisms to certain segments.**
- **Use threat intelligence and automatization to combat limited time vs. required actions such as identifying vulnerable systems, identifying threats and mitigate risks.**
- **There is not a one-size-fits-all solution to infrastructure security. Different motivations (financial gain vs. physical harm) need to be addressed with different strategies.**
- **Recommendations for future research, for example, to look at the service providers that offer financial rewards for patient records.**

Literature & Sources

Articles / Blog posts

Healthcare industry steps up security as cyber-attacks increase.pdf
(source: Medical Laboratory Observer, 2017, Vol.49(11), p.56(1))

financial consequences of cyber-attacks leading to data breaches in healthcare sector.pdf
(source: Coper-nican Journal of Finance and Accounting, 2017, Vol.6(3), pp.63-73)

Comparing crypto markets for drugs. A characterization of sellers and buyers over time.pdf
(source: Inter-national Journal of Drug policy, Volume 56, June 2018, Pages 176-186)

https://www.deepdotweb.com/dark-net-market-comparison-chart/

https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records

https://www.hcinnovationgroup.com/cybersecurity/article/13030570/what-can-the-industry-learn-from-recent-highprofile--cyber-attacks

https://healthitsecurity.com/news/healthcare-industry-worst-in-stopping-insider-data-breaches

https://www.alpinesecurity.com/blog/most-dangerous-hacked-medical-devices

https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#580aabda50cf

https://www.darkowl.com/blog/2018/thedarkoverlord-selling-new-patient-data

https://www.deepdotweb.com/marketplace-directory/listing/therealdeal-market

https://www.darkowl.com/blog/2019/russians-on-the-darknet-marketplaces-amp-forums

https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/

goodman_2.pdf (Last accessed on 2019/04/25; 08:49 CET;
retrieved from: http://www.ehcca.com/presentations/HIPAA24/goodman_2.pdf)

https://www.csoonline.com/article/3189869/healthcare-records-for-sale-on-dark-web.html

https://www.hipaajournal.com/category/healthcare-cybersecurity/

Reports

https://www.verizon.com/about/news/ransomware-still-top-cybersecurity-threat-warns-verizon-2018-data-breach-investigations-report

2019 Breach Barometer Annual Report.pdf

TV_Value_of_Data_Report_Final_PDF.pdf

IntSights_Chronic_Cyber_Pain_Healthcare-Final.pdf

SSC-2019-Healthcare-Report.pdf

Research letter: Jiang J, Bai G. Evaluation of Causes of Protected Health Information Breaches. JAMA Intern Med. Published online November 19, 2018179(2):265–267. doi:10.1001/jamainternmed.2018.5295
(accessed last: 2019-08-20, 11:59) https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2715158

Research letter: McCoy TH, Perlis RH. Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-2017. JAMA. 2018;320(12):1282–1284. doi:10.1001/jama.2018.9222
(accessed last: 2019-08-22, 16:22) https://jamanetwork.com/journals/jama/fullarticle/2703327

Sources

[1] https://www.hipaajournal.com/healthcare-data-breach-statistics/

[2] https://www.bbc.com/news/technology-47292887; https://www.databreaches.net/healthcare-hotline-millions-of-medical-advice-calls-exposed-in-sweden/

[3] McCoy TH, Perlis RH, 2018

[4] https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/

[5] https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

[6] https://healthitsecurity.com/news/hackers-demand-1m-in-grays-harbor-ransomware-attack

[7] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

[8] https://www.hipaajournal.com/healthcare-data-breach-statistics

[9] https://www.hipaajournal.com/may-2019-healthcare-data-breach-report/

[10] https://www.hipaajournal.com/june-2019-healthcare-data-breach-report/

[11] source: Protenus report (https://www.protenus.com/breach-barometer-report)

[12] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[13] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records

[14] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[15] JAMA Intern Med. 2019; 179(2):265-267. doi: 10.1001/jamainternmed.2018.5295, p. 266

[16] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records

[17] https://techcrunch.com/2018/08/09/the-healthcare-industry-is-in-a-world-of-cybersecurity-hurt/).

[18] https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#9d5447150cf1

[19] http://www.ehcca.com/presentations/HIPAA24/goodman_2.pdf#page=22

[20] https://www.fastcompany.com/3061543/on-the-dark-web-medical-records-are-a-hot-commodity

[21] https://www.msn.com/en-us/news/technology/hackers-are-stealing-medical-records-%E2%80%93-and-selling-them-on-the-dark-web/ar-BBTA1YG

[22] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records

[23] https://www.hcinnovationgroup.com/cybersecurity/article/13030570/what-can-the-industry-learn-from-recent-highprofile-healthcare-cyber-attacks

[24] https://www.fastcompany.com/3061543/on-the-dark-web-medical-records-are-a-hot-commodity

[25] https://www.spamfighter.com/News-22079-AZ-Plastic-Surgery-Center-refused-to-give-extortion-to-TDO.htm

[26] https://www.thedailybeast.com/hackers-steal-photos-from-plastic-surgeon-to-the-stars-claim-they-include-royals

[27] https://www.zdnet.com/article/top-dark-web-marketplace-will-shut-down-next-month/

[28] https://www.theverge.com/2019/5/3/18528211/wall-street-market-silkkitie-valhalla-dark-web-takedown-police-germany

[29] https://bitcoinmagazine.com/articles/major-darknet-marketplace-wall-street-market-shuttered-law-enforcement

[30] https://techcrunch.com/2019/05/07/deep-dot-web-arrests

[31] https://www.fraudbeat.com/synthetic-fraud/

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to protect freedom and build a safer digital society.

We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats. With a 25+ year track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. It is our people that make us different.

We are proud of our high-end security research unit, thanks to which we publish regularly white papers, articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured at industry conferences including, Infosec, Manchester DTX, RSA, BlackHat and DefCon.