

RSAC[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: PART3-T10

Bringing Down the Empire—The Internet of Medical Things (IoMT)



Axelle Apvrille

Principal Security Researcher
Fortinet / FortiGuard Labs
@cryptax

Aamir Lakhani

Red Team Researcher
Fortinet / FortiGuard Labs
@aamirlakhani

#RSAC

Who are we

Aamir Lakhani

- Senior Researcher
- Red Team Research Lead



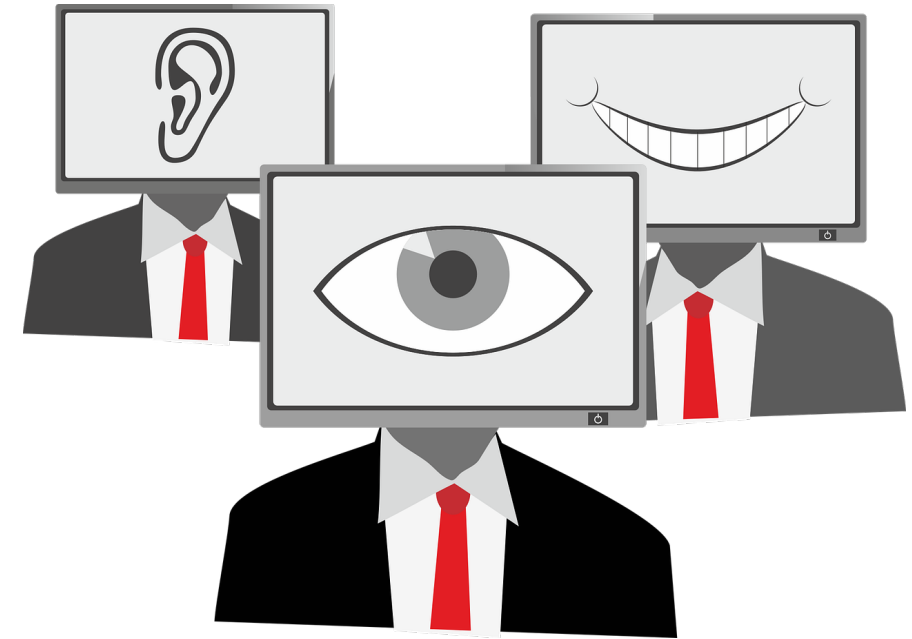
Axelle Apvrille

- Principal Researcher
- Lead researcher for IoT and Healthcare devices



The largest healthcare breaches of 2019

- AMCA DATA BREACH: 25 MILLION PATIENTS, INVESTIGATIONS ONGOING
- DOMINION NATIONAL: 2.96 MILLION PATIENTS
- UW MEDICINE: 973,024 PATIENTS
- WOLVERINE SOLUTIONS GROUP: ESTIMATED 600,000 PATIENTS
- OREGON DEPARTMENT OF HUMAN SERVICES: 645,000 PATIENTS
- COLUMBIA SURGICAL SPECIALIST OF SPOKANE: 400,000 PATIENTS

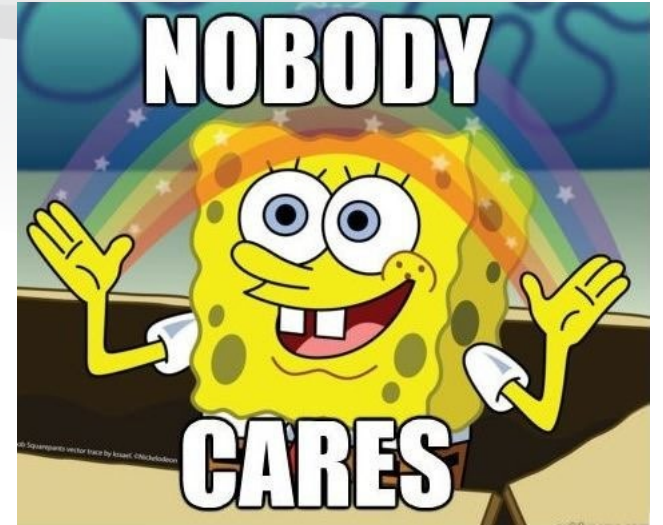


Source: Health IT Security


<https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far>

Medical Devices have vulnerabilities

- CVE 2019-10950
- X-ray devices
- Anesthesia machines
- Emergency responder communication systems
- How many people care?



Medical Databases for Sale



Healthcare Database (210,000 Patients) from Central/Midwest United States
★★★★★ Rating for this product based on number of finalized sales
Seller: [thedarkoverlord](#) (0) 0% Positive feedback
Visit store: thedarkoverlord don't have a store

Finalize Early: No, FE is not required. Shipping Type: **Normal**


Quantity: In stock / 0 sold

Postage Option:

Price: **0 170.00**
BTC 170.0000

[Buy It Now](#)
[Add to favorites](#)
[Send PM to Vendor](#)

Vendor Level 1 Ships From: Worldwide Digital



Healthcare Database (48,000 Patients) from Farmington, Missouri, United States
★★★★★ Rating for this product based on number of finalized sales
Seller: [thedarkoverlord](#) (0) 0% Positive feedback
Visit store: thedarkoverlord don't have a store

Finalize Early: No, FE is not required. Shipping Type: **Normal**


Quantity: In stock / 0 sold

Postage Option:

Price: **0 60.00**
BTC 60.0000

[Buy It Now](#)
[Add to favorites](#)
[Send PM to Vendor](#)

Vendor Level 1 Ships From: Worldwide Digital



Healthcare Insurance Database (9,300,000 Patients) from United States
★★★★★ Rating for this product based on number of finalized sales
Seller: [thedarkoverlord](#) (0) 0% Positive feedback
Visit store: thedarkoverlord don't have a store

Finalize Early: No, FE is not required. Shipping Type: **Normal**


Quantity: In stock / 0 sold

Postage Option:

Price: **0 750.00**
BTC 750.0000

[Buy It Now](#)
[Add to favorites](#)
[Send PM to Vendor](#)

Vendor Level 1 Ships From: Worldwide Digital



Healthcare Database (34,000 Patients) from Bronx, New York, United States
By [thedarkoverlord](#) (100.0%) **Level 1 (14)**

0 20.0000 / BTC 20.0000
In stock.

Postage Option:

[Buy It Now](#)

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

[Favorite](#) [Question](#)

Medical Fraud

- Medical databases contain PII (personally identifiable information)
- Opening credit cards, loans, car leases, cell phone accounts.
- Insurance and billing fraud

The screenshot displays a medical EHR system interface with the following sections:

- Appointments:** A list of appointments for 6/13/2016, including times (e.g., 07:00 AM, 07:30 AM) and reasons (e.g., Surgery, Regular Therapy, MRI).
- Interoperability Dashboard:**
 - Demographics:** Patient information including Address, Phone, Cell Phone, Email, DOB, Age, and Patient ID.
 - Allergies:** Section for listing allergies, with a checkbox for "No Known Drug Allergies".
 - Diagnoses:** Table of active, inactive, and resolved diagnoses with columns for Description, Status, Date, ICD-9, ICD-10, and Diagnosis Notes.
 - Orders/Results:** Table of medical orders and results with columns for Type, Act, Order, Status, Order Date, and Result Date.
 - Smoking Status:** Section for tracking smoking status, including Start Date, Out Date, Packs/day, and Notes.
 - Visit Type:** Table of visit types with columns for Visit Type, Date, Code, Type, and Status.
 - Appointments:** Detailed view of appointments with columns for Date, Time, Reason, Type, Location, and Notes.
 - Rx History:** Table of medication history with columns for Status, Date, Drug, Strength, and Instructions.
 - Family History:** Section for family medical history with checkboxes for Not Relevant and Unknown.
- Mail Status:** Section for managing mail, with checkboxes for High, Normal, and Personal.
- Current encounter:** 6/13/2016 7:30:00 AM.
- Bottom Bar:** Navigation buttons for Anesthesia Consent, Pre Op, Intra Op, Post Op, Information Sheet, MRI/CT, Drug Sheet, and Dictation.

RSA[®]Conference2020

Diabetes

Diabetes

- According to some studies some Asian populations are 63% more likely to get diabetes
- Diabetes is a complicated set of medical conditions that causes abnormalities with blood sugars.
- Diabetes is expensive to treat. Insurance complexities for retired, non-insured, under-insured, and self-insured make it much more difficult.



Let's talk about how medical insurance can help

- Available plans to choose from: 1
- Monthly Premium of plan 810.00
- Medicines covered: Less than 50%
- Medicine cost monthly: \$700 (retailers such as Sam's club give significant discounts under specific conditions)

Step 1 of 1: Confirm your plan choices & enroll [View steps](#)

Confirm your plan choices

You've chosen the plans below. If everything is correct, **confirm plan choices** to continue.

Health plan for [REDACTED] Lakhani

Monthly premium

\$810.88

Including a \$0.00 tax credit

Community Health Choice

[Community Health Choice HMO Bronze 003](#)

Bronze | HMO | Plan ID: 27248TX0010003

✗ Adult Dental
✗ Child Dental

Dental plan for [REDACTED] Lakhani

Monthly premium

\$9.39

Guardian

[Managed DentalGuard TX Essentials 2](#)

HMO | Plan ID: 26250TX0070002

✓ Adult Dental
✓ Child Dental

Cost for Medicine

- Laws and protections are making it more affordable
- Cost for 10ml Vial (all prices are USD)
 - US with insurance \$20
 - US without insurance \$400 (without discounts)
 - AUS \$20
 - India \$2
 - Pakistan \$3

Keep in mind prices and discounts make this difficult to track. These prices are based on me calling several providers in each country.

Darknet Cost of Insulin

- \$2 USD Per 100ML vial
- Price and boxes appear that many are shipped from south Asian countries
- Danger of fakes appears to be minimum.



U-100 Insulin
Syringes - 29G
1cc 1/2" - BX of
100

From: 50 \$ -
Paraphernalia -
physical
Posted by
cryptocurrencys , 19 left

Buy now



1 bag of 10
U-100 Insulin
Syringes - 29G
1cc 1/2"

From: 6 \$ -
Paraphernalia -
physical
Posted by
cryptocurrencys , 200
left

Buy now



Trenbolone
Acetate 100

From: 40 \$ - Steroids
- physical
Posted by
americansteroids , 999
left

Buy now



GHRP-2
MONSTERLAB

From: 169 \$ - Steroids
- physical
Posted by bestgroup ,
100 left

Buy now



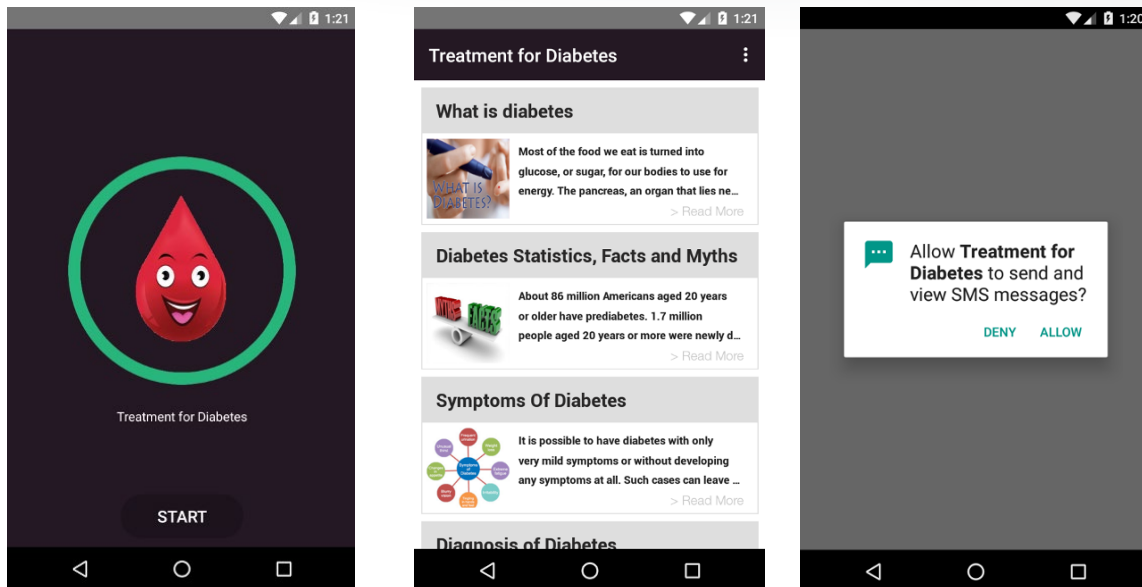
Pregnyl (HCG)
- 5000 iu - SP
Laboratories

From: 32.91 \$ -
Steroids - physical
Posted by

RSA®Conference2020

Medical Malware

Treatment for Diabetes



- Treatment for Diabetes – sounds safe right?
- SMS Short Code
- Country of Origin and Destination unknown
- Premium charge
- Charge unknown

```
protected void onCreate(Bundle savedInstanceState) {
    URL v2;
    if(Build.VERSION.SDK_INT < 23) {
        MainDEV.doSendTheSMS(this); // Old Android, just try to send the SMS
    }
    else if(MainDEV.checkPermission(this, "android.permission.SEND_SMS") == 0) {
        MainDEV.doSendTo5554(this); // If permitted, send SMS
    }
    else {
        String[] permission = new String[]{"android.permission.SEND_SMS"};
        MainDEV.requestPerm(this, permission, 1000);
    }
}
```

Code for managing SMS permission request

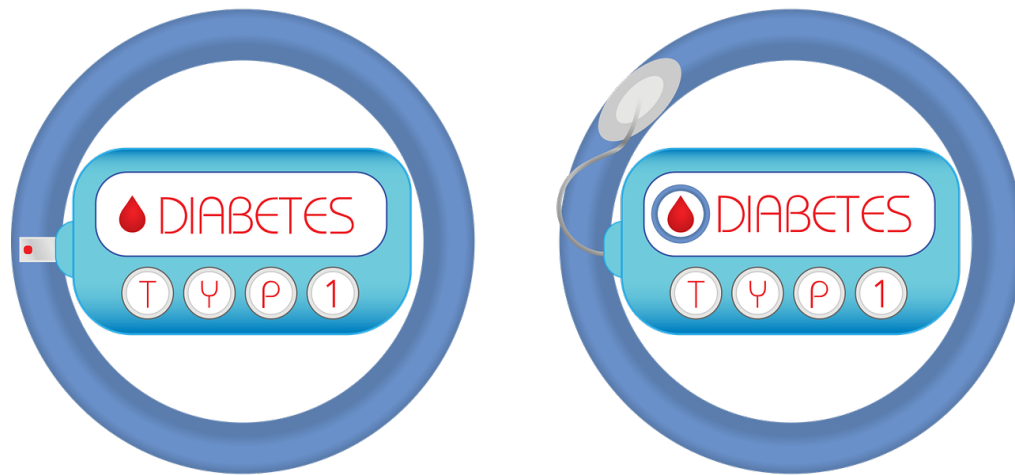
Toll-Fraud

- Toll-fraud like it's 2012!
- Estimates of Toll Fraud have been in the billions
 - I personally find that hard to believe but either way it's more than it should be.

The screenshot shows the SpoofCard website's 'Control Panel'. At the top, the 'SpoofCard' logo is followed by navigation links: HOME, BUY CREDITS, FEATURES, MOBILE APPS, and MEDIA. Below this is a blue header with the text 'Control Panel' and links to DASHBOARD, ADD CREDITS, CALLS, and SMS. The main content area has three tabs: 'Place Your Call', 'SMS', and 'Group Spoof'. The 'SMS' tab is active. It displays a form with two input fields: 'Destination Mobile Number' and 'Caller ID to Display'. The 'Destination Mobile Number' field shows '111-555-1212' with a US flag icon and a note '3 credits per SMS'. The 'Caller ID to Display' field shows 'Bank of America' with a US flag icon and a warning 'Must be a valid Mobile number to be delivered'. At the bottom, a message box states 'Your account has been hacked. Please call 284-111-1111'.

Source: The Threat of Toll Fraud
<https://www.nojitter.com/security/threat-toll-fraud-persists>

How home glucose monitors work



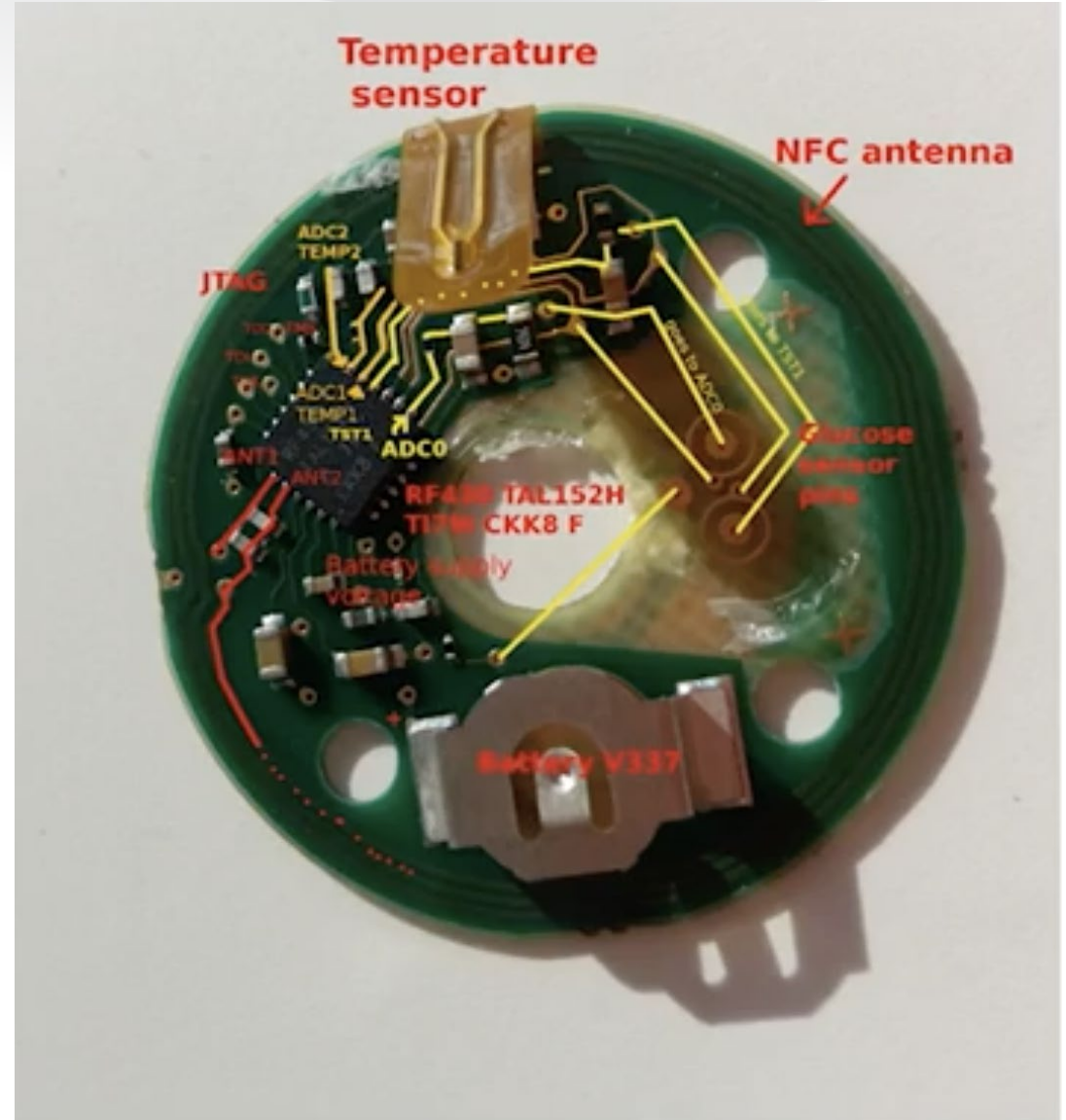
Smart sensors

- Smart sensors let you monitor glucose levels
- You don't need to keep pricking yourself
- Take one normal reading
- Attach smart sensor to your body
- Sensor expires in 14 days. Users need to buy a new sensor every 14 days



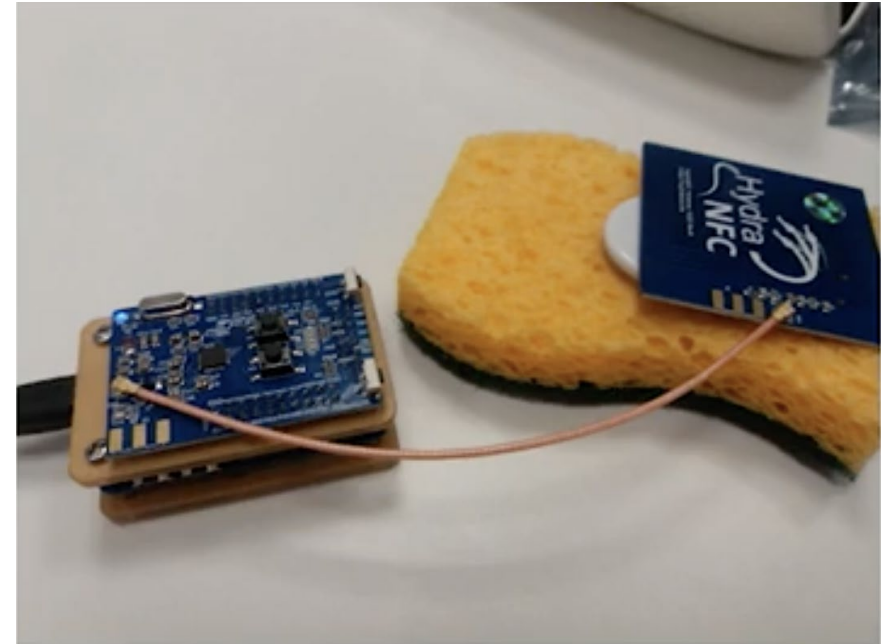
Analyzing the Sensor

- Custom chips
- Low Powered consumption
- Is there an attack service?



Analyzing Smart Sensor

- Sensor uses NFC with the smartphone
- ISO 15693
- **Anyone can read: no authentication required**
- Used sponge to replace arm
- Sponge has hot water and sugar



Memory Dump

- After weeks of reverse engineering Axelle was able to dump the memory of the sensor
- We discovered records are stored in 6-bytes
- Limited memory on the sensor
- We were able to reverse many commands of the memory including wear time
- 37 HEX or 110111
- $(37)_{16} = (3 \times 16^1) + (7 \times 16^0) = (55)_{10}$
- 55 minutes

```
Block 00 F4 18 B0 32 03 01 02 08
Block 01 00 00 00 00 00 00 00 00
Block 02 00 00 00 00 00 00 00 00
Block 03 E6 20 06 03 D2 02 C8 84
Block 04 A1 00 D0 02 C8 78 A1 00
Block 05 D0 02 C8 74 A1 00 D0 02
Block 06 C8 6C A1 00 CF 02 C8 6C
Block 07 61 00 CF 02 88 76 61 00
Block 08 E0 02 C8 A0 61 00 DE 02
.....
Block 0F C8 90 A1 00 1E 03 C8 68
Block 10 62 00 EC 02 C8 E8 61 00
Block 11 D7 02 C8 94 61 00 00 00
.....
Block 27 00 00 00 00 37 00 00 00
Block 28 BA 32 00 01 BA 32 00 01
```

The Mobile App – Firebase Analytics Logs and SDKs

```
05-24 08:20:11.384 V/FA      (13108): Event recorded:
↳ Event{appId='com.*****', name='screen_view(_vs)',
↳ params=Bundle[{firebase_event_origin(_o)=auto,
↳ firebase_previous_class(_pc)=SplashActivity,
↳ firebase_previous_id(_pi)=-3985357911052850480,
↳ firebase_screen_class(_sc)=HomeActivity,
↳ firebase_screen_id(_si)=-3985357911052850479}]}
05-24 08:20:11.436 D/FA      (17498): Logging event (FE):
↳ SYS_UNEXPECTED, Bundle[{firebase_event_origin(_o)=app,
↳ firebase_screen_class(_sc)=HomeActivity,
↳ firebase_screen_id(_si)=-3985357911052850479}]
05-24 08:20:11.526 D/FA      (17498): Logging event (FE):
↳ user_engagement(_e), Bundle[{firebase_event_origin(_o)=auto,
↳ engagement_time_msec(_et)=290,
↳ firebase_screen_class(_sc)=HomeActivity,
↳ firebase_screen_id(_si)=-3985357911052850479}]
```

Hardware Vulnerabilities Discovered by Fortinet



Hardware 



Event tracking in the mobile app



Sensor vulnerability currently under discussion



Reading the sensor

- Hardware: Anyone can read the sensor. (2) We found a vulnerability we disclosed.

Event Tracking in the App

Do Cybercriminals Care?



Medical Malware is Everywhere

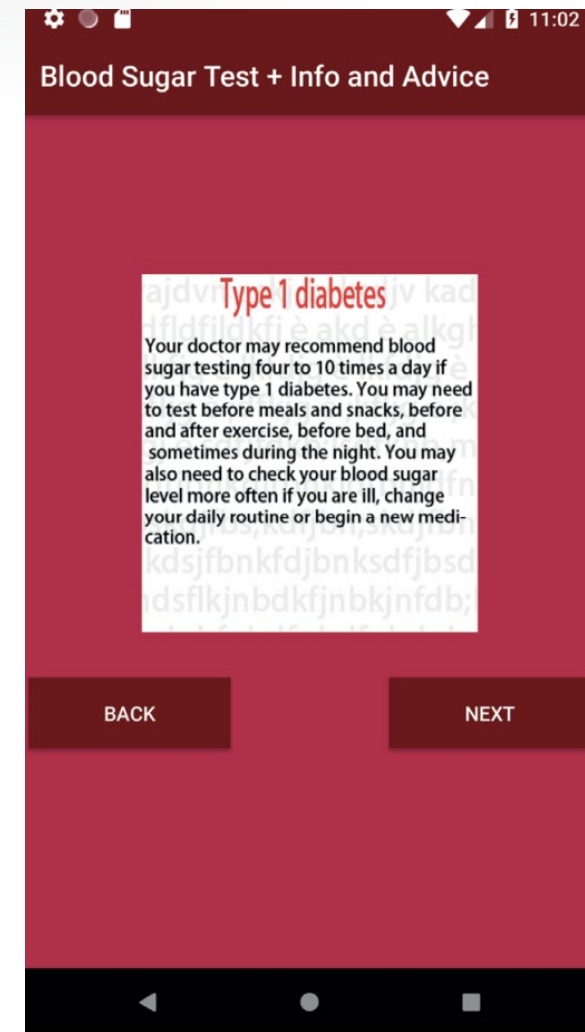
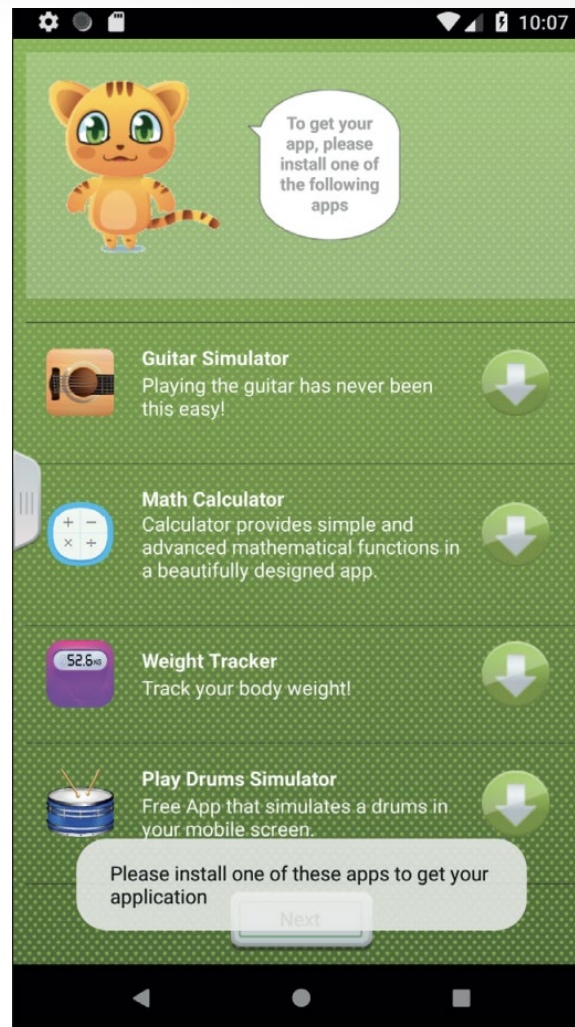
- Malware
- Ransomware Advice and Kits
- Attacks against medical equipment.

| | | | |
|---|----------|--------|---------|
| Apr 28, 2018 8:21:31 AM - Android | | | |
| Signs of Diabetes (com.appman.signsofdiabetes) | Detected | Adware | AirPush |
| 56dda03b5326e9435e56c60378e0bb5ce51ed8a7989a54c9301b858881c7cd13 | | | |
| Apr 22, 2018 3:41:50 PM - Android | | | |
| Signs of Diabetes (com.appman.signsofdiabetes) | Detected | Adware | AirPush |
| 26512a86db403978eabe968f61fcc097d3b25c5e08030e1d5d9bdb168029f938 | | | |
| Apr 21, 2018 3:34:23 PM - Android | | | |
| Signs of Diabetes (com.appman.signsofdiabetes) | Detected | Adware | AirPush |
| 91d9cedae0314f78ea5984cb324cd5a291d0f45c7127b42547999362fc46166e | | | |
| Apr 21, 2018 2:06:11 AM - Android | | | |
| Signs of Diabetes (com.appman.signsofdiabetes) | Detected | | |
| dbae98098f5479a2a91215ea728f44ca0c30bcf2085563f0cec83b48f3cf33af | | | |
| Apr 16, 2018 3:08:10 AM - Android | | | |
| Diabetes Destroyer (com.wDiabetesDestroyer) | Detected | | |
| 67b73d4cc8f1433eec2b7db3143800fd3c86e8180058228a587295ed5f0fa56f | | | |
| Mar 22, 2018 1:37:21 PM - Meyers Norma | | | |
| Diabetes - Glucose Diary 2.0.02 (fulledition.com.szyk.diabetes) | Detected | | |
| a18a5594558e08472df75f6ae2cc2c61f1897f0a97df7f38abba3827191b86e | | | |
| Dec 27, 2017 1:49:07 AM - ASDD | | | |
| Diabetic App.Guía Diabetes (com.mobincube.diabetic_appguia_diabetes.sc_HYLBUTU) | Detected | | |
| 013fb909ef58c0f6050ac4863a7631fdd2fe4acb75da0a66990cbb464f861625 | | | |
| May 6, 2017 1:24:12 PM - Mobimento Mobile | | | |
| DIABETES VIDA SANA (com.mobincube.consejos_de_salud.sc_3JGERJ) | Detected | | |
| efc283cdedb0540ac615d096f1aabcecc62e72256afc3cdf32f5ab3ffd0951b3 | | | |
| Mar 17, 2017 5:23:47 PM - Mobimento Mobile | | | |
| Diabetes Ke Upay (com.desitoteapp.DiabetesKeUpay) | Detected | Adware | |
| 7c9d3e75af3a46f6cccbcbadca538cd3e79383d516aca84e939de51e10ea7b87 | | | |

Malware Smart Apps

- How Long Do I have to Live?
- All data leaked to remote server
- Program prevents accessing diabetes application unless you download sponsored adware
- Advice with ads and tracks everything: Installed Apps, IP, GPS

The screenshot shows a mobile app titled "How long will I live?". It features a form with several dropdown menus and text input fields. The instructions at the top say: "Fill in the following form then click the button labeled 'Calculate Life Expectancy'. (We will try to guess the values you leave blank. So leave them blank if you think our guessing is better than yours. :-)". The form includes fields for "I am a" (planning marriage), "white", "male", "who", "smokes 4 cigarettes per day", "I am 0 years old", "I sometimes wear a seat belt during the 10 thousand miles per year I travel in a car", "I exercise 20 minutes per week", and "My home has never been checked for radon".



Latest Downloads from the Darknet

Lantus Solostar - Insulin - 100IU 10x3ml - Sanofi + Add Listing



Sold by pharmamed 2 5.00 ★ Trust Level 1

| FEATURES | | | |
|---------------|------------------|---------------|-----------|
| Product class | Physical Package | Quantity left | Unlimited |
| Ships from | European Union | | |
| Ships to | WorldWide | | |
| Views | 12 | Visibility | Public |
| Ends In | Never | Payment | Escrow |

Unit price: USD 149.60 0.01768093 BTC


Europe 3 Days - USD +11.51 / item

Buy Now

Maximum Quantity: Unlimited

| Feedback | Buyer/Price | Date/Time | Rating |
|---|-------------|-----------|--------|
| This product doesn't currently have any feedback. | | | |

Humalog KwikPen - Insulin - 100IUx5x3ml - Lilly + Add Listing



Sold by pharmamed 2 5.00 ★ Trust Level 1

| FEATURES | | | |
|---------------|------------------|---------------|-----------|
| Product class | Physical Package | Quantity left | Unlimited |
| Ships from | European Union | | |
| Ships to | WorldWide | | |
| Views | 13 | Visibility | Public |
| Ends In | Never | Payment | Escrow |

Unit price: USD 92.06 0.01088057 BTC

Europe 3 Days - USD +11.51 / item

Buy Now

Maximum Quantity: Unlimited

| Feedback | Buyer/Price | Date/Time | Rating |
|---|-------------|-----------|--------|
| This product doesn't currently have any feedback. | | | |

ProCrim Prresents= Metformin 500mg Pharm grade



฿0.00287

\$10.4

Vendor

[White_Girl_Wasted](#) (390) (4.64★)

Ships to

Worldwide, Canada

Ships from

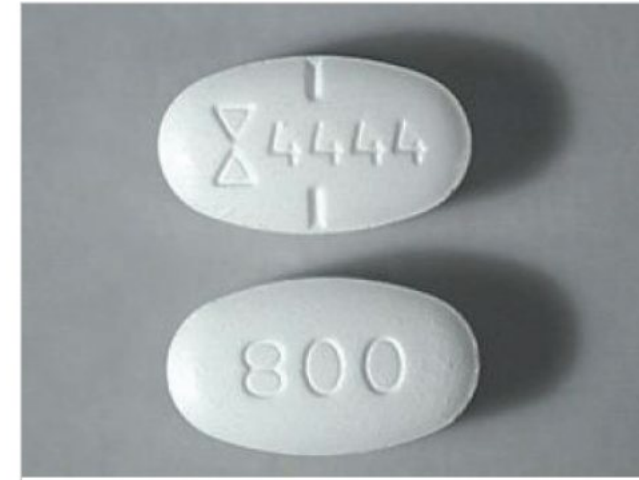
Gotham City

Escrow

Yes

[View offer](#)

5 - 800mg Gabapentin Pills TEVA



฿0.00673

\$24.388

Vendor

[fatassgbs123](#) (720) (4.85★)

Ships to

United States, United

States

Ships from

United States

Escrow

Yes

[View offer](#)

Insurance Fraud

- Multiple health insurance cards and IDs being sold
- Average rate is \$500
- Walk into any doctor's office or pharmacy and show them a medical insurance card and ID
- We are not showing specific items for sale because they all appear to be stolen.
- Major US insurance companies were at risk



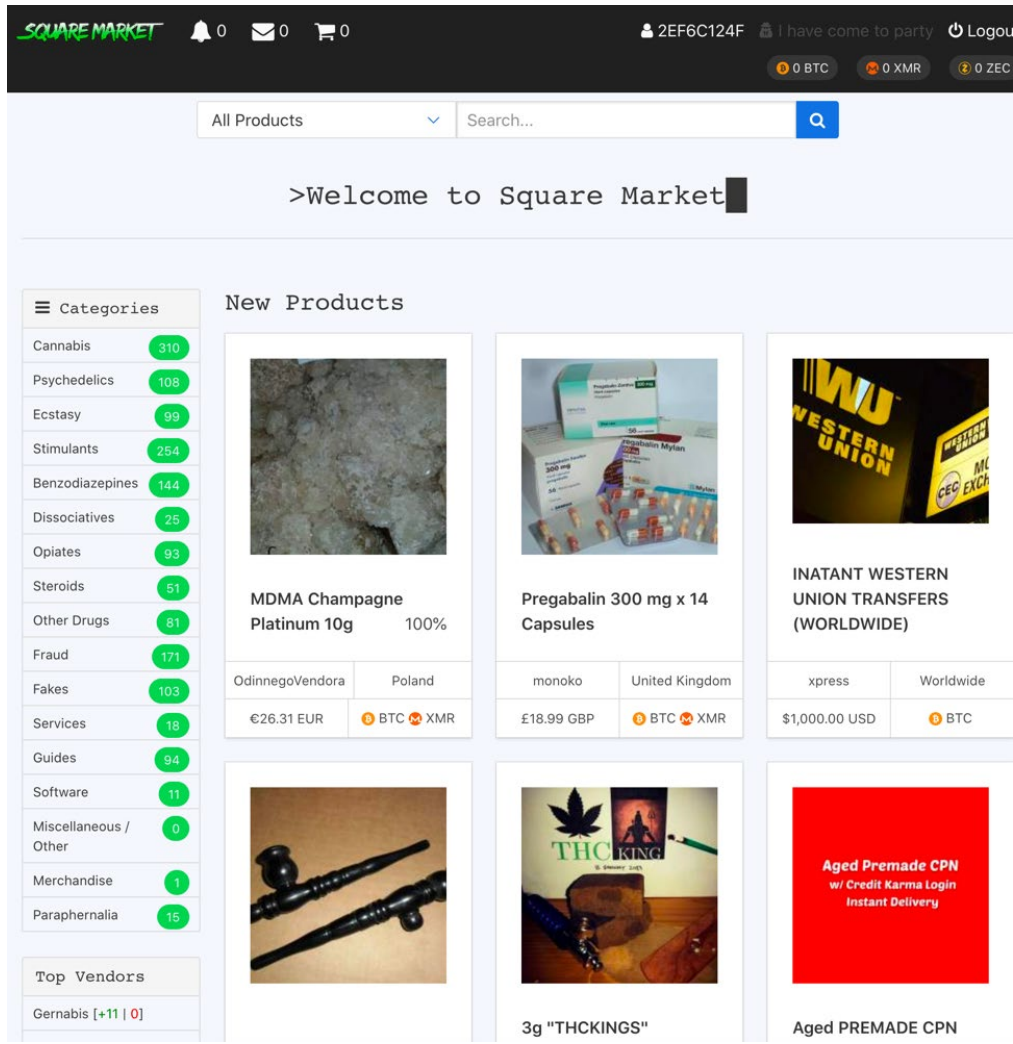
Take the Day Off

- Doctor's notes are cheap \$1 - \$10
- Take the day off
- Some provide verification from call centers



The screenshot shows a marketplace listing for a product titled "★★ DOCTORS NOTES PACK ★★". The price is listed as 4.28 EUR (\$ 0.000478). The item is marked as "In stock". The seller is "BigDawgScott" with a rating of [11] - [0]. The class is "Digital" and the escrow type is "Full escrow". It notes "0 items sold since 2019-04-17 18:38:03". On the right, there are buttons for "Favorite", "Question", and "Report". Below these, a "Quantity" dropdown is set to "1". There are radio button options for "Litecoin (LTC)", "Bitcoin (BTC)", "Monero (XMR)", and "Multisig COMING SOON". A red "Buy Now" button is at the bottom of the purchase options. At the bottom of the listing, there are tabs for "Details", "Terms & Conditions", and "Feedback". The "Details" tab is active, showing a placeholder image and the text "Need the day off work/school?". Below this, it says "This pack has a HUGE variety of signed doctors notes."

The Darknet Market today



- There used to be 2-5 large markets with thousands of items for sale
- Now: Multiple market (15 – 30)
- Hundreds of items for sale

RSAConference2020

What we have learned

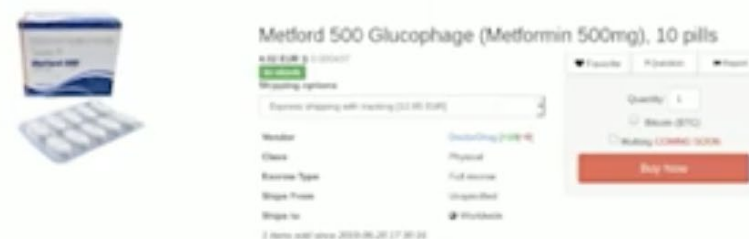
What we learned

- Cybercriminals don't care if you have had medical problems.
- They will use whatever advantage they can to make money
- You can buy cheap medicine from the Darknet
- There are risks involved



Risks in buying from Darknet

- Side effects
- Wrong medicine
- Wrong package



Berlusconi Market, July 2019



Pregabalin, in a box, on Tochka - July 2019



Dream Market, Jan 2019. Beware side effects: suicide, cancer, abuse, addiction...



Pregabalin powder, on Agarthia - July 2019. Risks?!

Smartphone Apps

- Smartphone applications are vulnerable to lots of attacks
- People will tolerate dangerous adware and spyware when they need the information urgently
- SMS and Toll-Fraud is still an attack service
- We are lucky – It could have been much worse.

A big thank you

- Tons of people told us their stories about many aspects for this talk.
 - People buying from Darknet
 - People with health issues
 - People with insurance issues
- Axelle, we missed you!
- Lots of people helped us out with technical and non-technical pieces
- Check out the Fortinet blog for updates and more research