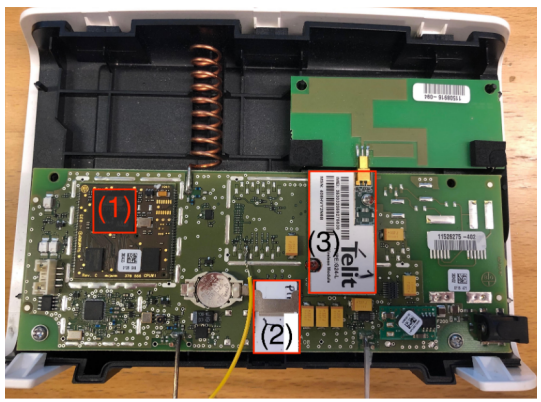
FORTINET

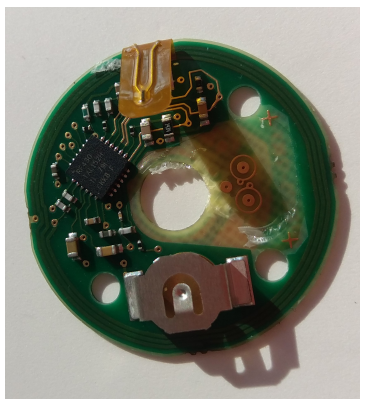
Malware and Cybercrime in Medical IoT

Axelle Apvrille, Fortinet

Copenhagen Cybercrime Conference, September 2020

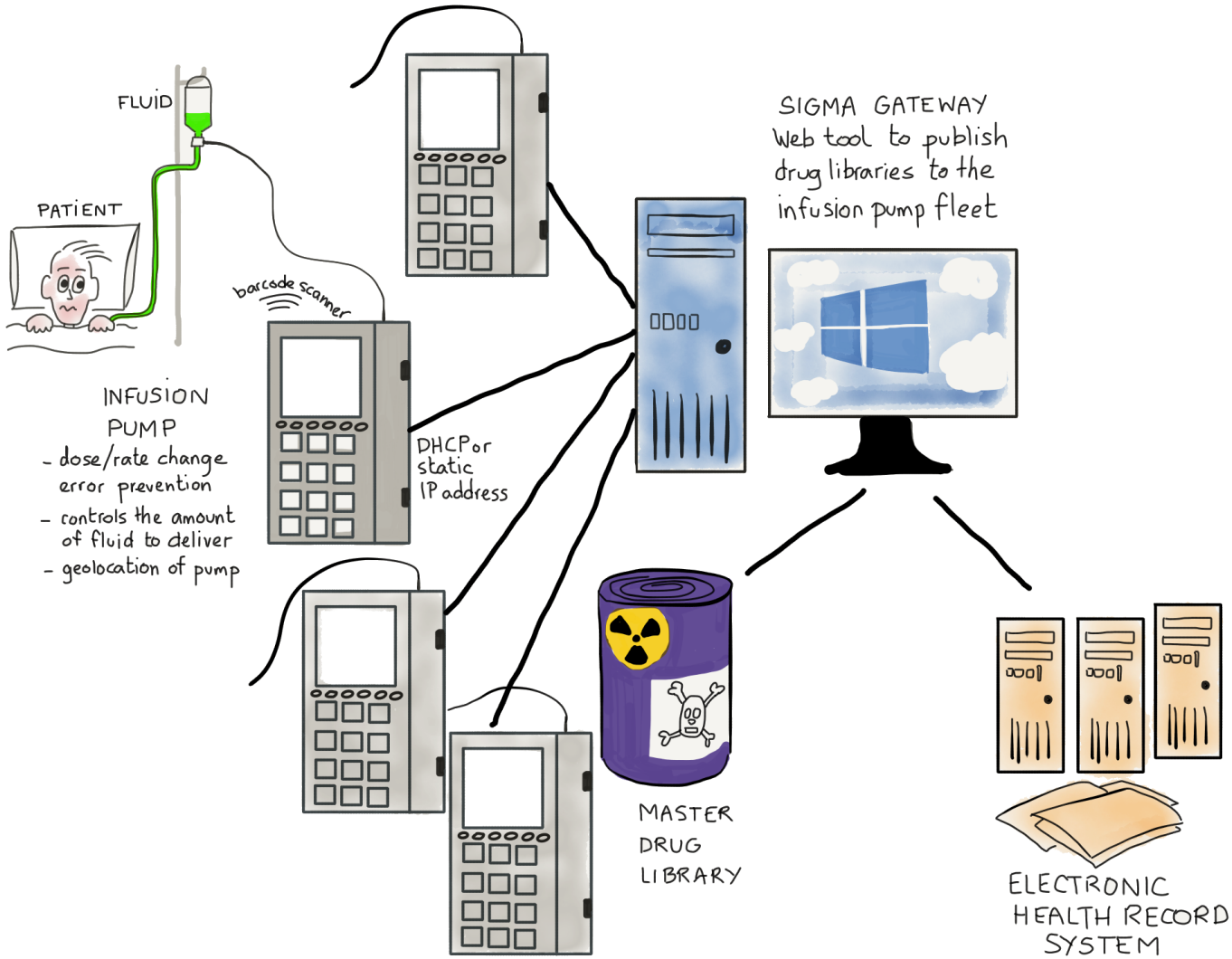
Medical IoT are not *"gadgets"*





They are useful for our **health**

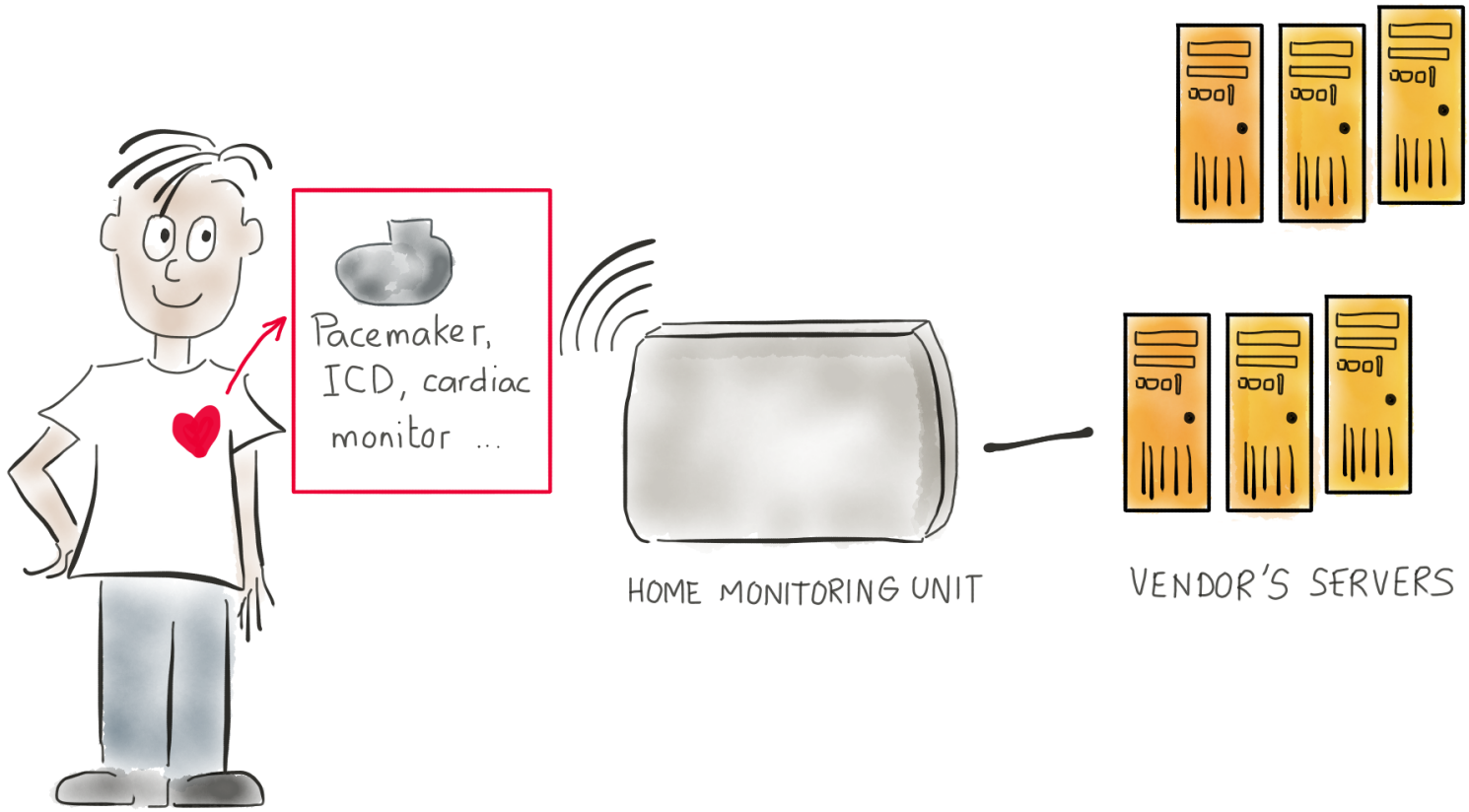
Example: Baxter Spectrum WBM infusion pumps



This is a quick and simplified overview of the architecture. It may differ from reality.

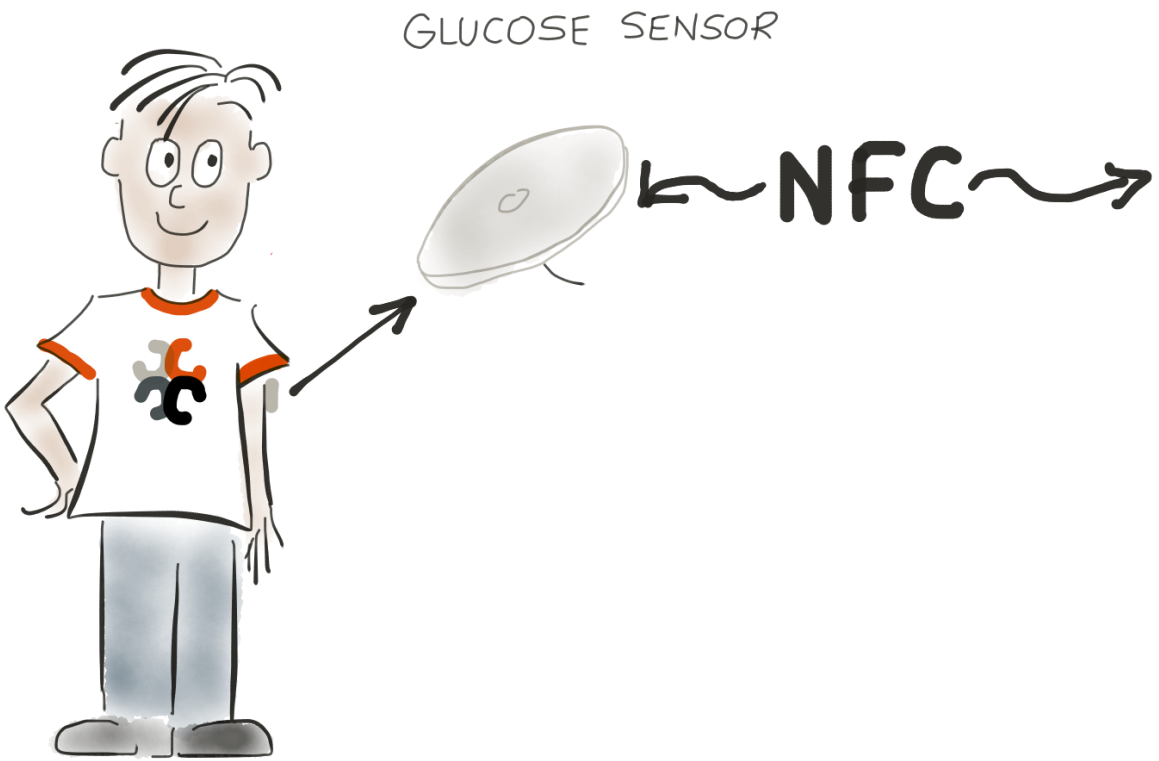
Eases medical staff's work, and reduces error risk

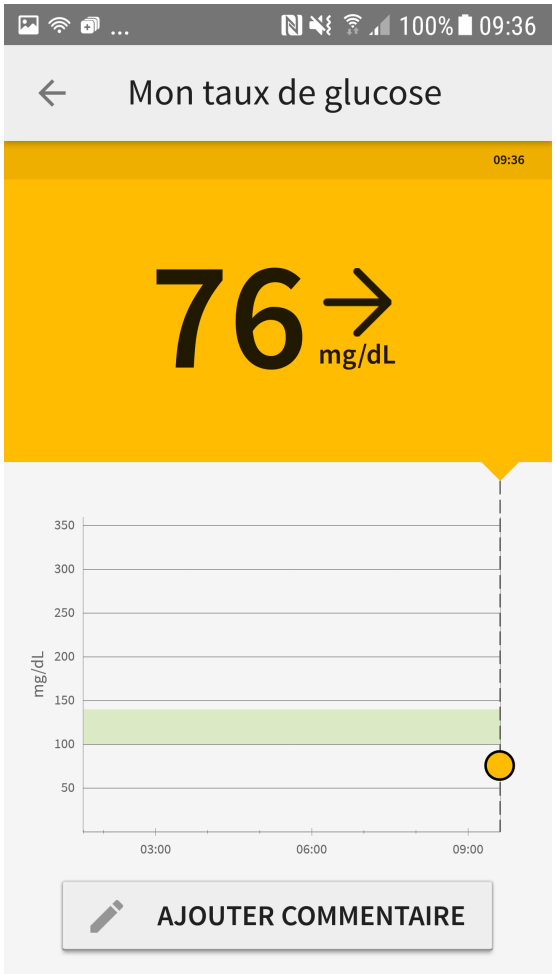
Example: Biotronik Cardio Messenger



Eases patient's life: reduces the number of visits to their practitioners. Data from pacemaker/ICD is uploaded to the vendor's servers, where practitioners can access them remotely.

Example: FreeStyle Libre glucose sensor

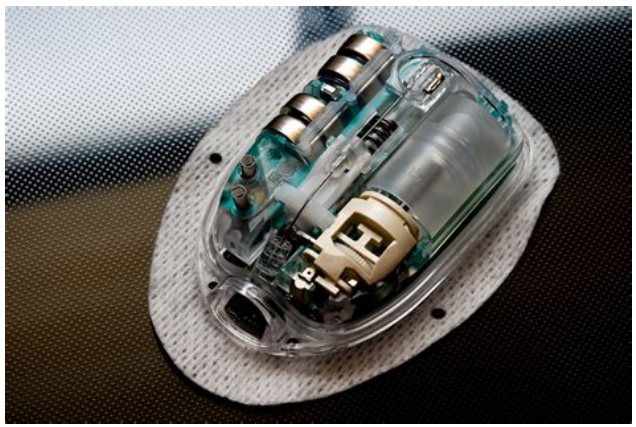




Eases patient's life: reduces the number of daily blood glucose samples.

More medical IoT

Medtronic Evera ICD (Implantable Cardioverter Defibrillator) - **Critical**



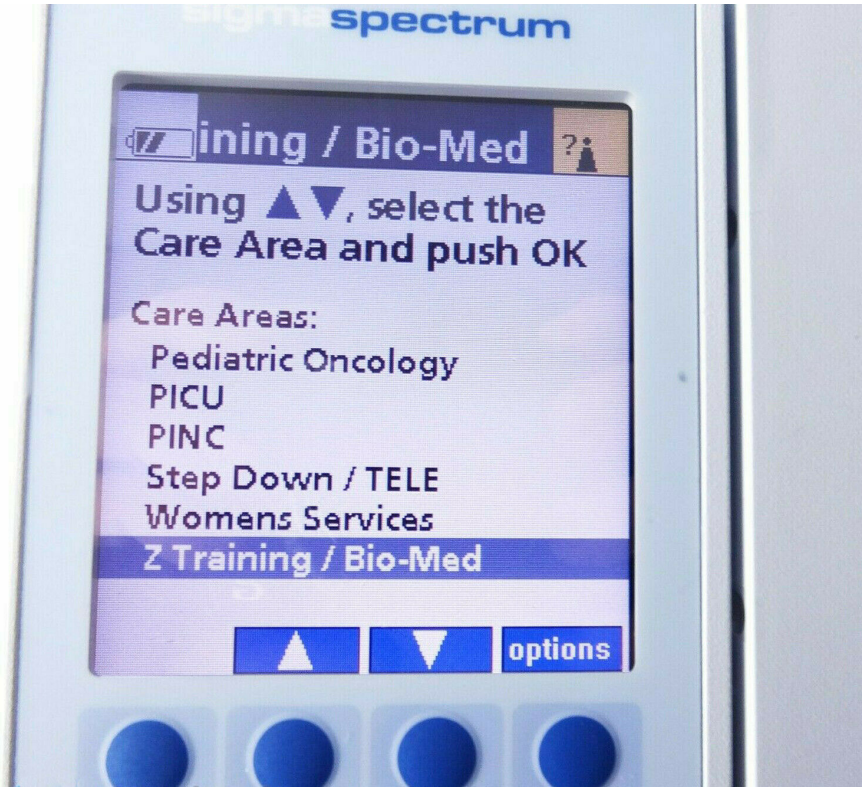
Insulet Omnipod (Insulin pump) - **Useful / Critical**

Glowcap (Connected pill bottle) - **Useful**

All medical devices (or nearly all) have vulnerabilities...

Baxter Sigma Spectrum Infusion Pumps

- CVE-2020-12039, CVE-2020-12040, CVE-2020-12041, CVE-2020-12043 ...
- Access sensitive data, change system configuration
- Product Security Bulletin, June 2020
- HIPAA Journal Advisory

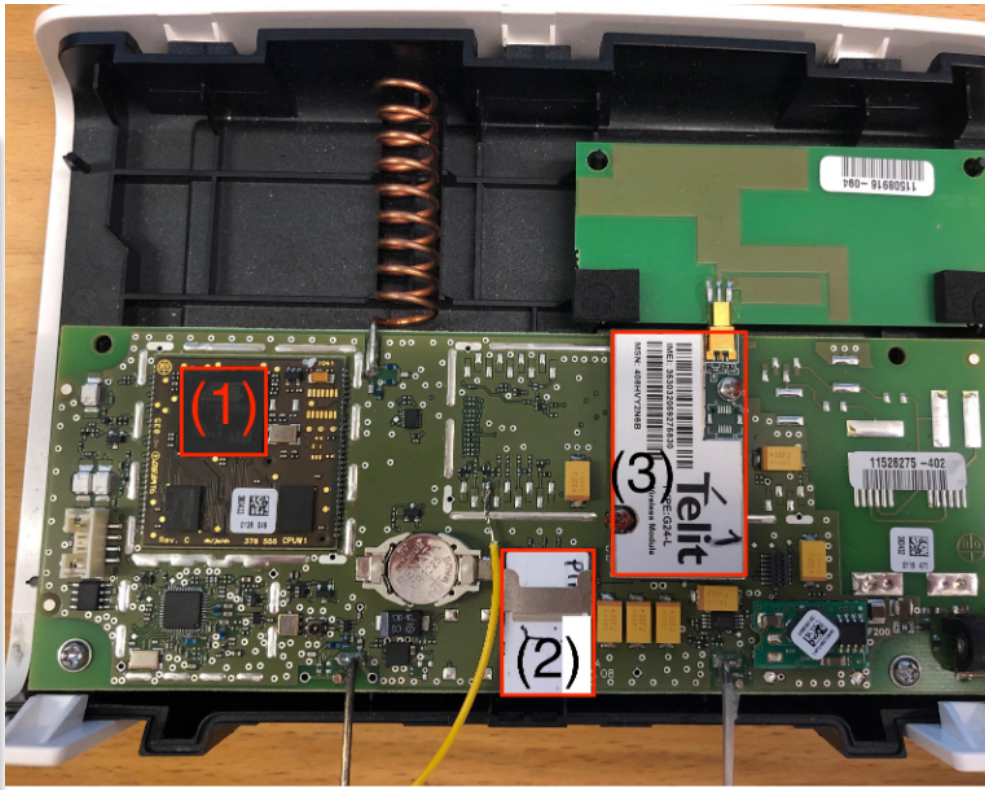


Picture is for illustration purposes, found on the web, and may differ from the exact model which is vulnerable.

All medical devices (or nearly all) have vulnerabilities...

Biotronik CardioMessenger II

- CVE-2019-18246, CVE-2019-18248, CVE-2019-18252...
- Sensitive data theft
- No longer on the market
- Master thesis of Guillaume Bour (CISA) and Blog post
- Biotronik Cybersecurity statement

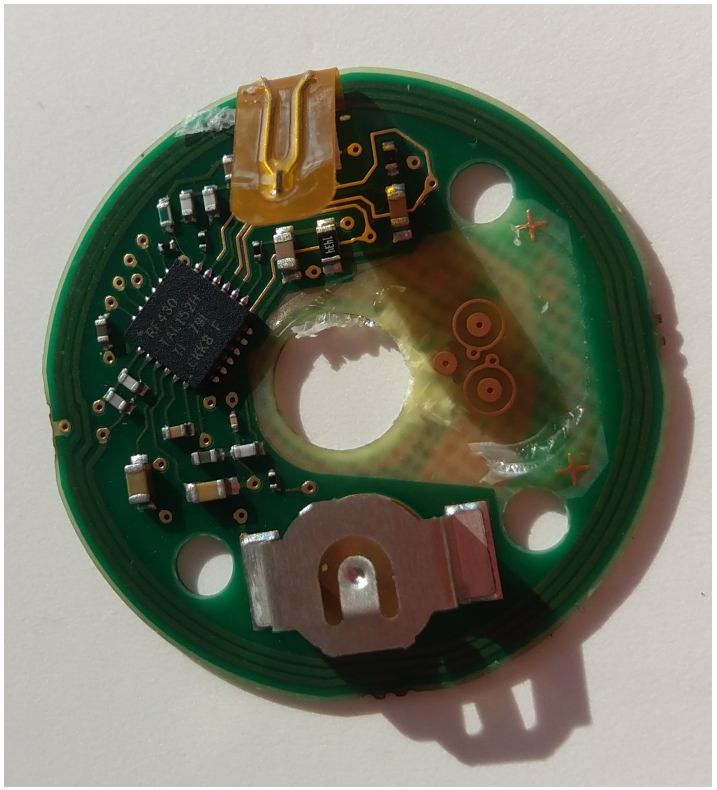


Board of a Cardio Messenger 2-S
Source: Master thesis of Anniken Wium Lie

All medical devices (or nearly all) have vulnerabilities...

Abbott FreeStyle Libre

- CVE-2020-8997, FG-VD-20-028
- Reset of expired sensor, eavesdropping glucose level, and in more demanding situations: modification of glucose levels, activation time change...
- Research done in collaboration with **Travis Goodspeed**
- Full security report
- Our presentation at Pass The Salt 2020



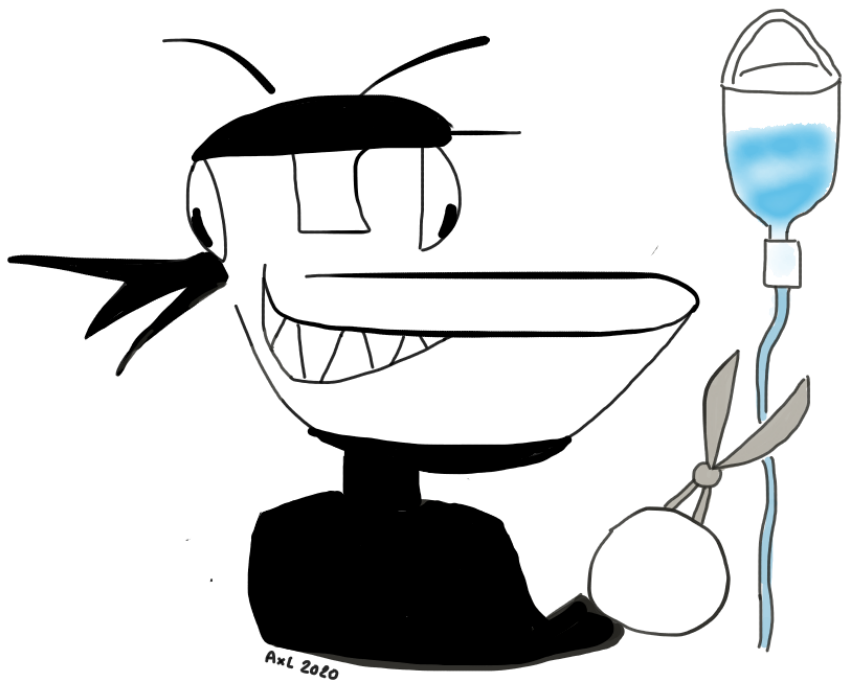
PCB of the glucose sensor

Often, they are basic vulnerabilities!

"telnet service on port 1023 with hard-coded credentials"
"does not implement authentication or authorization"
"storage of passwords in a recoverable format"

Are cybercriminals attacking the health sector?

How much?



A list of recent attacks

June 2019	Hospital	Cabestany, France	Médipôle Saint Roch
June 14, 2019	Healthcare	Florida, US	NCH Healthcare System faces email phishing attack on payroll system. 73 employees fell victim to the phishing attack. ref
July 2019	Hospital	Michigan, US	5,500 patient's health info exposed after phishing attack at Michigan Medicine ref
August 14, 2019	Health group	France	Attack on medical establishments of Ramsay-Générale de Santé. Ransomware. ref
August 22, 2019	Healthcare	Alberta, Canada	Physician's gmail account hacked and may have leaked 7,000 patients data. Alberta Health Services. ref
August 26, 2019	Dental	US	Attack on backup of Digital Dental Record software of DDS safe ASIP . REvil ransomware.
Jan 22, 2020	Hospital	France	Centre Hospitalier de La Bassee, Nord. Emotet. Ransom asked of 8000 euros per desktop. Got in by infected email from another healthcare institute which had been hacked
February	Health sector	US	NRC Health breach. They administers patient survey tools to hospitals. Patient data was accessed.

Are cybercriminals attacking connected medical devices?

Are cybercriminals attacking connected medical devices?

Only few known cases

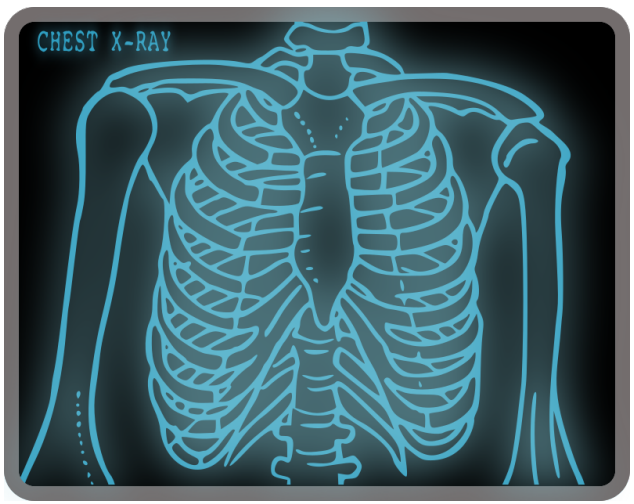
MEDJACK 2015-2017

- Compromised: Respiratory gate PC, fluoroscopy workstation, X-Ray, MRI
- Dropped malware on the network, such as Conficker, Kido...
- TrapX MEDJACK report

Orangeworm 2018

- Found on machines controlling X-Rays and MRI
- Kwampirs trojan
- Threat intelligence report

Medical devices as entry points



Old OS, no update, vulnerabilities, outside security perimeter etc

Attackers move laterally on the network

Search for monetizable info

Finance department

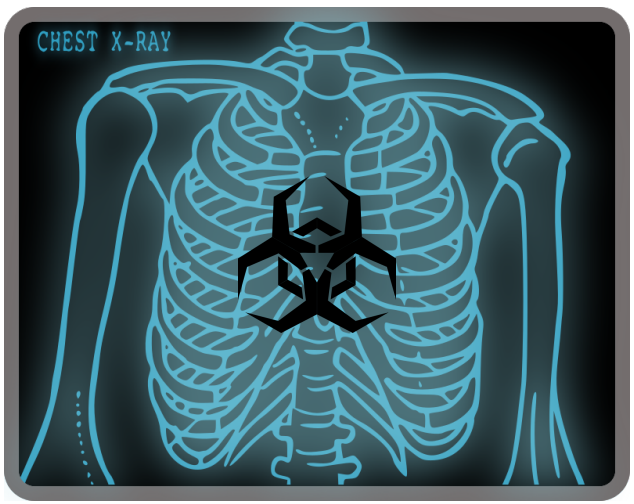
EHR

Staff database

Medical devices as entry points

Finance department

Attack entry point



Old OS, no update, vulnerabilities, outside security perimeter etc

Attackers move laterally on the network

Search for monetizable info

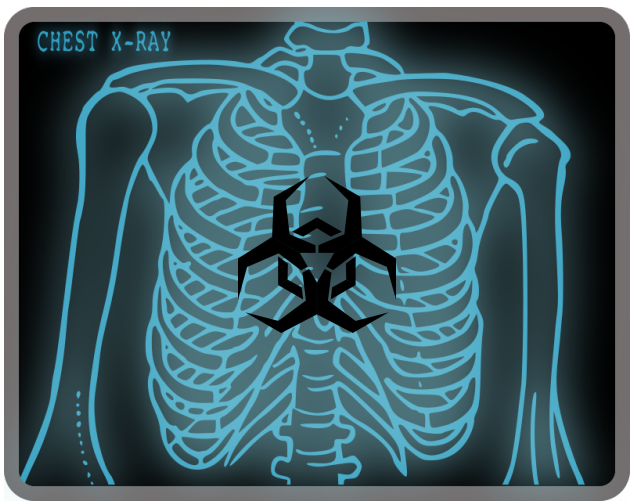
EHR

Staff database

Medical devices as entry points

Finance department

Attack entry point



Old OS, no update, vulnerabilities, outside security perimeter etc

Attackers move laterally on the network

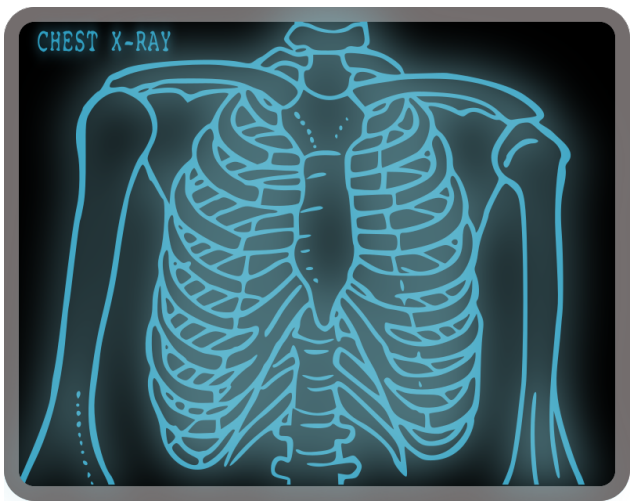
Search for monetizable info

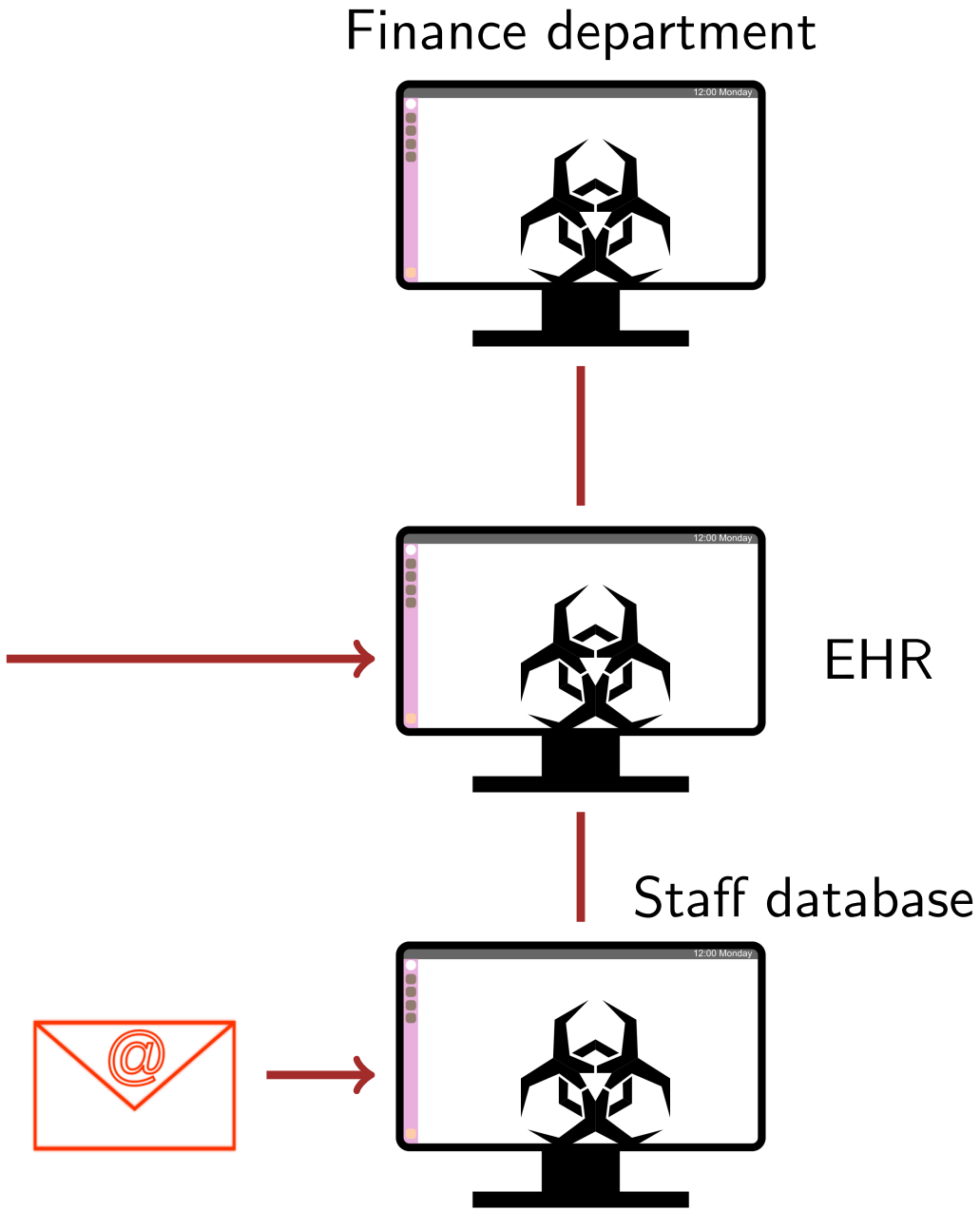
EHR

Staff database

There are many other entry points for malware

The most common entry point are not through medical devices, but **phishing, emails**





We haven't ever seen any direct and intentional health impact

but there has been indirect or unintentional impact e.g patients re-routed to another hospital

- Maze authors say they won't attack healthcare during COVID-19
- DoppelPaymer offer their decryptor for free

Oh, so cybercriminals have morals???

Morals?

Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack

The Maze ransomware group has published personal and medical details of thousands of former patients of a London-based medical research company after a failed attempt to disable the firm's computer systems

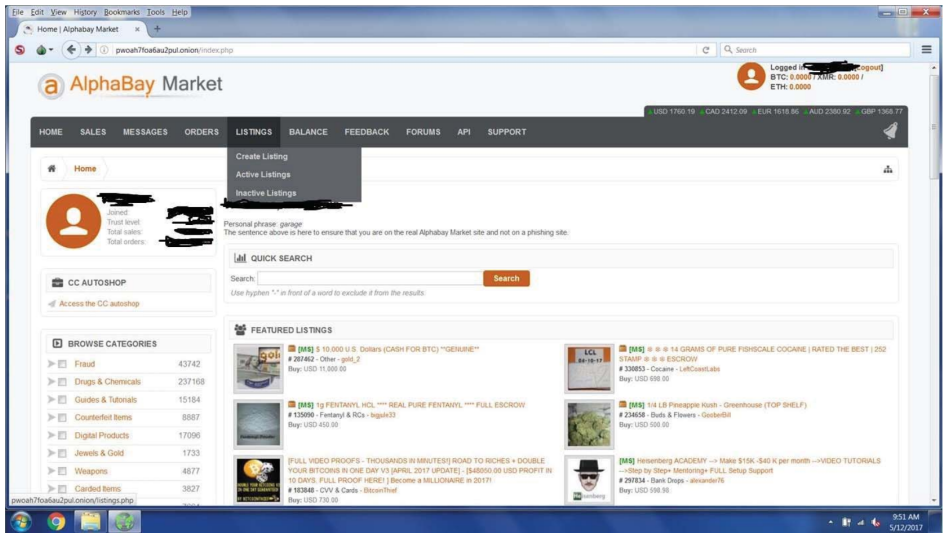
Hammersmith Medicines Research hit by Maze in March 2020

Post-COVID19 attacks on health sector

March 2020	Laboratory	UK	Hammersmith Medicines Research hit by rMaze ansomware. This medical facility was meant to test coronavirus vaccines
March 2020	Hospital	Czech Republic	Brno University Hospital was hit by ransomware
March 2020	Hospital	US	Seattle Children's Hospital faces more and more phishing attacks, targeting their accounts payable department
March 22, 2020	Medical network	France	AP-HP, a medical network, in Paris was targeted b a DoS. AP-HP Paris handles 39 health facilities. The attack did not cause any damage.
April 2020	Foundations	USA	WHO, NIH, CDC, Bill and Melinda Gates Foundation. The breach leaked 25,000 emails and passwords.
April 2020	Healthcare	Arizona, USA	Magellan Health hit by ransomware. First, they exfiltrated data: 365000 patient accounts. Phishing email impersonating client. They stole login credential of employees, personal info, employee id snumber, sensitive patient details (ssn, taxpayer)

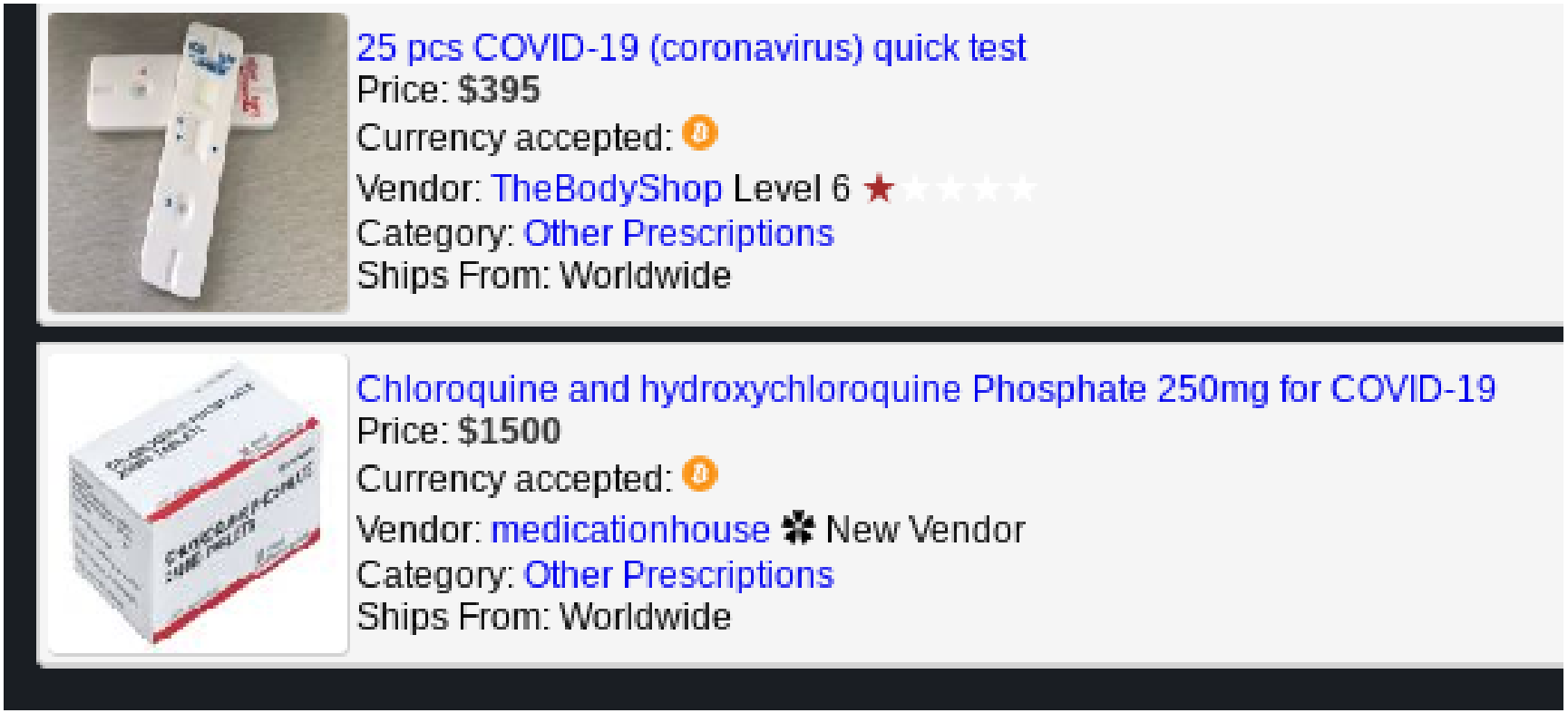
Why are cybercriminals attacking hospitals? Example

- Dec 2013 - Feb 2014: *TDS* (aka DS) hacks into **University of Pittsburgh Medical Center** (UPMC). He steals PII of 65K employee hospitals
- Sells the data on *Alphabay* and *Evolution*
- Other criminals buy the info, use it for income tax return fraud
- Money converted in **Amazon gift cards**
- Merchandise shipped to Venezuela
- June 2020, Hacker arrested



Alphabay darknet marketplace shutdown in 2017

Health: where do cybercriminals make money? Trends



Yellowbrick darknet marketplace - August 2020

Empire Market - Darknet - August 2020

Medicine for chronic disease

Omnia Labs, Rapid Acting Insulin Pen, 300iu

Omnia Labs, Rapid Acting Insulin Pen, 300iu

Sold by **omnialabsaus** - 1 sold since April 25, 2019 Vendor Level 6 Trust level 6

	Features		Features
Product Class	Physical Package	**Origin Country**	Australia(c)
Quantity Left	**Unlimited**	**Ships to**	Australia(c)
Ends In	Never	**Payment**	Escrow

	Bulk Discounts	Price	
Bulk Discount	From qty 5 to 9	USD 54.20	0.00442488 BTC
Bulk Discount	From qty 10 to 20	USD 50.59	0.00412989 BTC

Combined Shipping Free if purchased on another item - 4 days - USD + 0.00 / order

Purchase price: **USD 57.81**

Qty: 1 Buy Now Queue

Empire Market - Darknet - August 2020

Medicine for chronic disease

Escrow **Insulin NovoRapid Flexpen 3 ml.**
$12 / 0.000978 BTC
Vendor: **[View Listings] 6pack** **+20, -0, 100%**
Category: **Others**
Ships From: **Sweden**

Escrow **10X 1cc U-100 Insulin Syringe 28G (0.36mm X 13mm) combo package**
$10 / 0.000815 BTC
Vendor: **[View Listings] canadianconnection** **+0, -0, ?%**
Category: **Others**
Ships From: **Canada**

Silk Road - Darknet - August 2020

Particularly useful for people with poor health insurance coverage

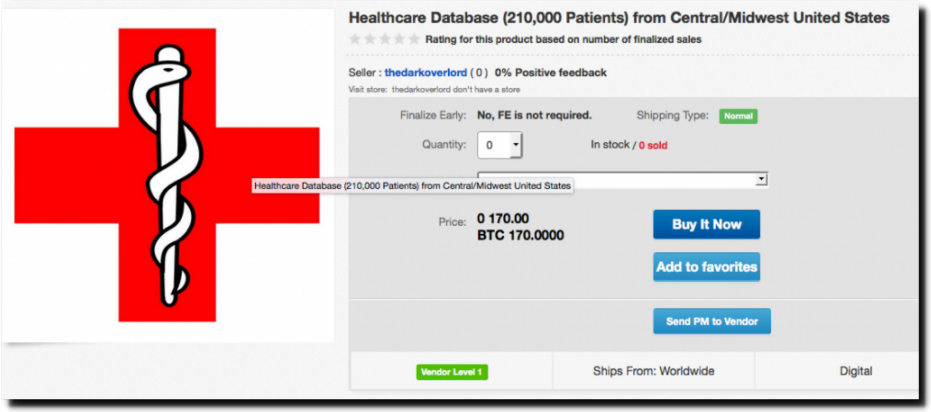
Making money out of despair: scams, traffic...

Escrow B17 Injection (CURE FOR CANCER)
$899 / 0.073274 BTC
Vendor: **[View Listings] nocopsformiles6** **+0, -0, ?%**
Category: **Others**
Ships From: **United Kingdom**

Escrow Anti Cancer Drugs
$80 / 0.006520 BTC
Vendor: **[View Listings] maryjohanna** **+5, -0, 100%**
Category: **Others**
Ships From: **me**

Escrow Kidney Organ Trafficking
$2000 / 0.163012 BTC
Vendor: **[View Listings] bodypartsguy** **+0, -0, ?%**
Category: **Others**
Ships From: **No Ships From Specified**

Selling information to other criminals



Wall Street market place - 2018

Fresh 100k Medicare data with DOB Medicare

Category: Online Business -> SSN / DOB / Other PII

Price (Fiat): EUR 99 ($117.85 £89.46 AUD163.27 CAD156.51)

Price (XMR): 1.241068070703

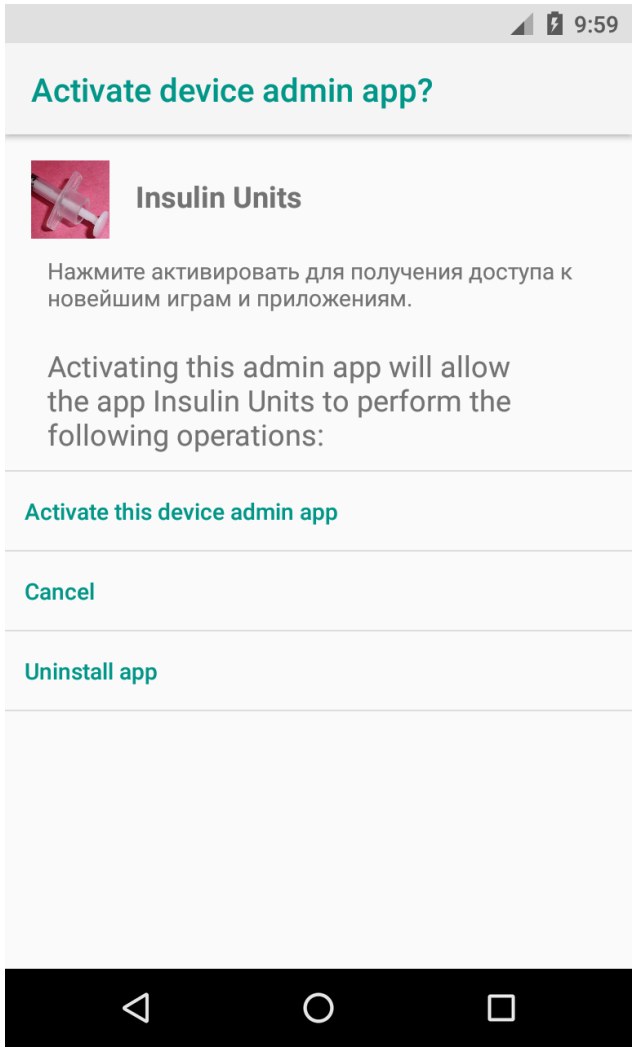
Measurement unit: Piece

Shipping: from: Digital / Service to: Digital / Service

Views: 134

White House Market - Darknet - August 2020

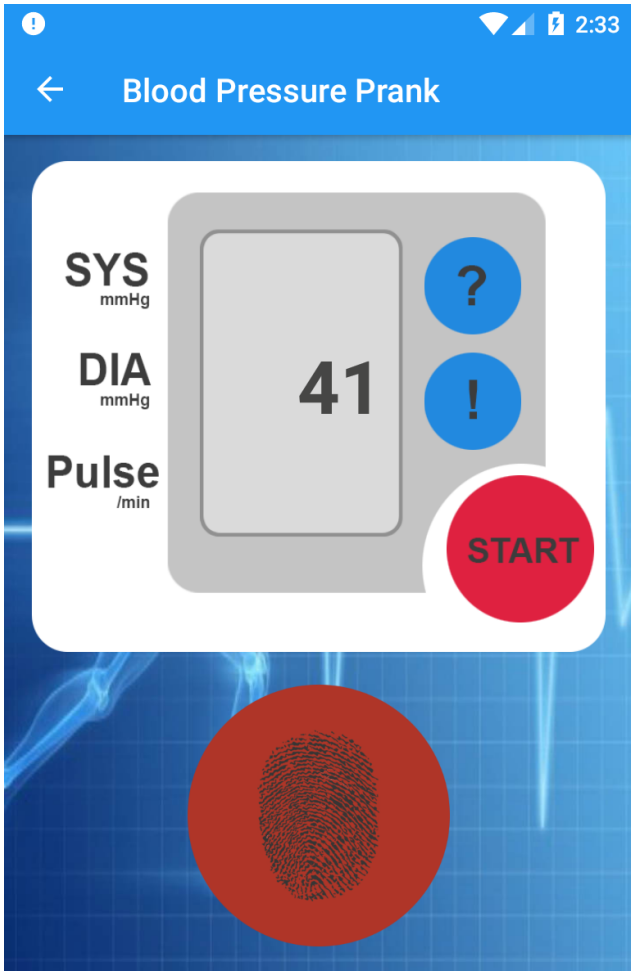
Medical malware on smartphones



Fake app - Adware - 2016

- We used to have *low level adware/ pranks/ scam*
- Tech report: Android malware abusing medical apps for diabetes

Medical malware on smartphones



Blood pressure prank - 2017

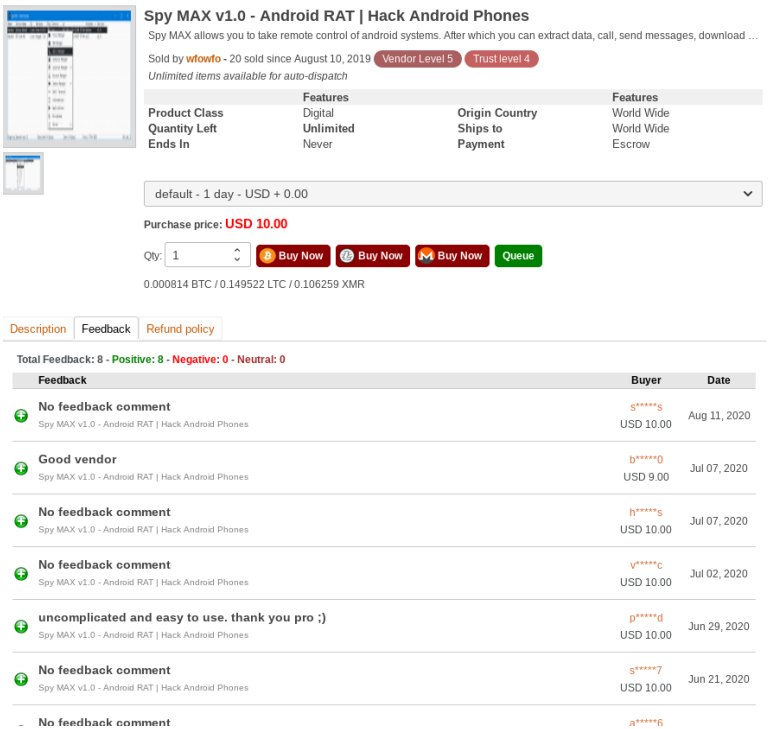
- We used to have *low level adware/ pranks/ scam*
- Tech report: Android malware abusing medical apps for diabetes

Medical malware on smartphones

SMS Trojan Dialer - 2019

- We used to have *low level adware/ pranks/ scam*
- Tech report: Android malware abusing medical apps for diabetes

Medical malware on smartphones



SpyMax sold on Empire Market - Darknet - August 2020

- We used to have *low level adware/ pranks/ scam*
- Tech report: Android malware abusing medical apps for diabetes
- Now, **more sophisticated malware**: obfuscated malware, RAT
- Reversing of BankBot spyware in COVID-19 alert app, Reversing of spyware in app faking Aarogya Setu - Summer 2020.

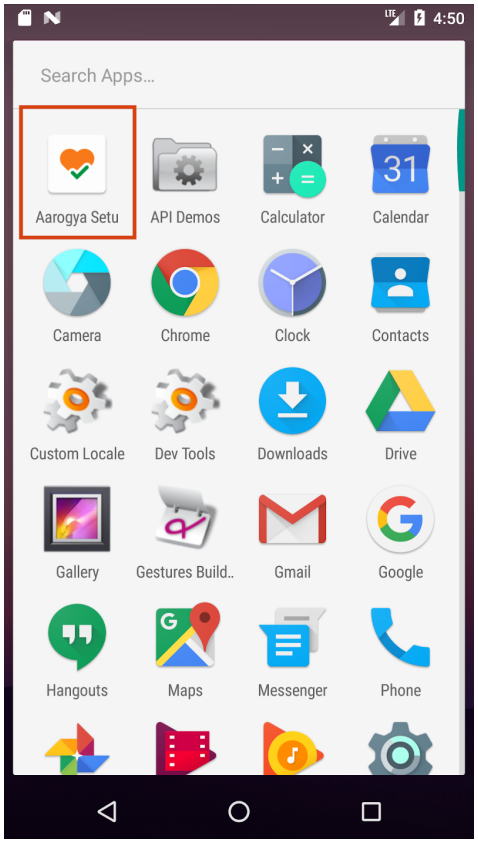
Medical malware on smartphones

```
this.writePref(ctx, "VNC_Start_NEW", "https://old.mandamientos.ga");
this.writePref(ctx, "Starter", "https://old.mandamientos.ga");
this.writePref(ctx, "time_work", "0");
this.writePref(ctx, "time_start_permission", "0");
this.a.getClass();
this.writePref(ctx, "urls", "" + "http://old.mandamientos.ga".replace(" ", ""));
this.a.getClass();
this.writePref(ctx, "urlInj", "" + "".replace(" ", ""));
this.a.getClass();
this.writePref(ctx, "interval", "" + 10000);
this.writePref(ctx, "name", "false");
this.writePref(ctx, "perehvat_sws", "false");
this.writePref(ctx, "del_sws", "false");
this.writePref(ctx, "network", "false");
this.writePref(ctx, "gps", "false");
this.writePref(ctx, "madeSettings", "1 2 3 4 5 6 7 8 9 10 11 12 13 ");
```

Default configuration of Android/Bankbot posing as COVID-19 app

- We used to have *low level adware/ pranks/ scam*
- Tech report: Android malware abusing medical apps for diabetes
- Now, **more sophisticated malware**: obfuscated malware, RAT
- Reversing of BankBot spyware in COVID-19 alert app, Reversing of spyware in app faking Aarogya Setu - Summer 2020.

Medical malware on smartphones



Spyware posing as India' Aarogya Setu COVID-19 tracing app

- We used to have *low level adware/ pranks/ scam*
- Tech report: Android malware abusing medical apps for diabetes
- Now, **more sophisticated malware**: obfuscated malware, RAT
- Reversing of BankBot spyware in COVID-19 alert app, Reversing of spyware in app faking Aarogya Setu - Summer 2020.

Upcoming trends

- **Drug** sale still occurs a lot on the darknet. **We've witnessed it.**
- The rest (malware coordination, development, specific requests...) is moving to IM
- Upcoming issue: more and more **complex medical malware on smartphones**, and more and more people using them for **healthcare**!

Take away

- **Medical IoT are not gadgets**. Stop saying we can do without them! Engage in protecting them.
- Understand cybercriminals **don't care if you have the flu** or COVID-19, but they **use unsecure hosts** for criminal activities and **make money** out of information they steal. Medical info is particularly valuable.
- Nearly all **medical devices have vulnerabilities**. We should at least commit to **fixing the very stupid ones**!
- The **Darknet is not dead**. Lots of drugs are still sold on it today.

Contact: aapvrille@fortinet.com
Twitter: @cryptax

Many thanks to

- **Aamir Lakhani** for many discussions & research, specially on Darknet
- **Copenhagen CyberCrime Conference** for inviting me!

https://www.fortinet.com - https://fortiguard.com

Missing medicine / demand spike

Normal Escrow

Diazepam 20 x 10mg Kern Pharma - 2 FREE XANAX (Clone)

$18.27 BTC

all: *Afghanistan*

PillsInc

5.00

Buy now

Anxiety disorders, sedative. Helps manage COVID-19. Demand spike during COVID-19.
Dark Market - August 2020

COVID-19 TEST | Corona test | 2019-nCOV/COVID-19 IgG/IgM Rapid Test Device

IMPORTANT NOTICE Fully CE and FDA approved and certified Tested and in use in German and France hospitals There is…

Sold by **NMBRS** - 0 sold since May 08, 2020 Vendor Level 5 Trust level 4

	Features		Features
Product Class	Physical Package	**Origin Country**	Europe
Quantity Left	**Unlimited**	**Ships to**	World Wide
Ends In	Never	**Payment**	Escrow

	Bulk Discounts	Price	
Bulk Discount	From qty 25 to 50	USD 23.68	0.00193155 BTC

Shipping EU with Track and Trace - 7 days - USD + 11.87 / order

Purchase price: **USD 29.61**

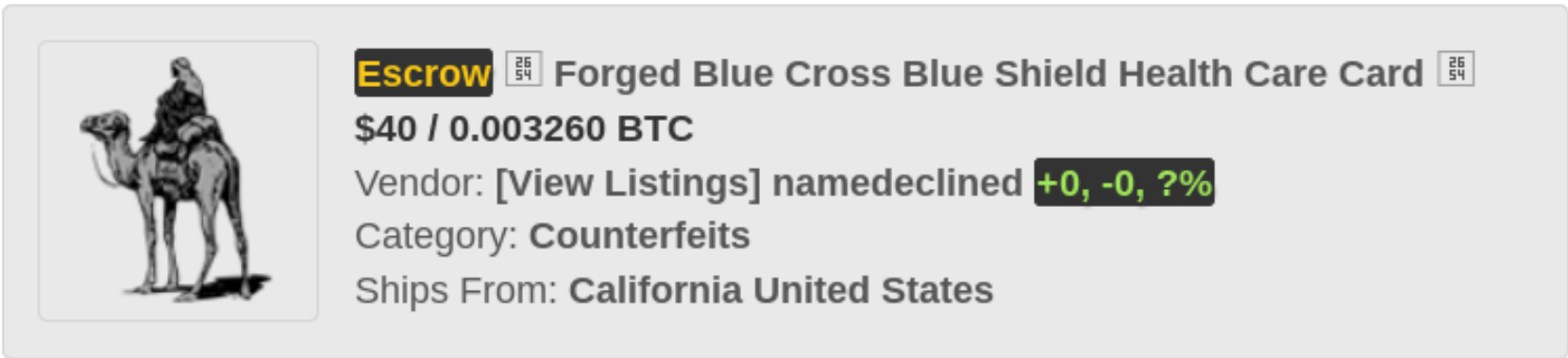
Test approved for use in French and German hospitals, Empire Market, August 2020

COVID-19 test strips diagnostic kit for Self-test CORONAVIRUS

Price: 108.11 EUR

Currencies accepted: BTC
Vendor: MrLegalize (100.0%, 0 sales)
Ships from: Switzerland
Ships to: Worldwide
Marketplace: Dark Market
Key words: *test diagnostic covid test coronavirus covid infected minutes aid*
Match score: 81.803
Info loaded in 4.41s

Kilos - Darknet search engine - August 2020



Forged Blue Cross Blue Shied insurance card.
Silk Road - August 2020