EVERYTHING IS A TARGET - YOUR HEALTH DATA IS NEXT

THE AV-TEST INSTITUTE

- MORE THAN 30 IT-SPECIALISTS
- MORE THAN 15 YEARS EXPERIENCE IN ANTI-MALWARE-RESEARCH

- **ONE OF THE LARGEST MALWARE REPOSITORIES WORLDWIDE**
- **STATIC AND DYNAMIC MALWARE ANALYSIS WITH IN-HOUSE TOOLS**
- **400 CLIENT- AND SERVERSYSTEMS**
- **1.000 TERABYTE TESTDATA**
- **MORE THAN 5.000 INIDIVIDUAL AND COMPARATIVE TESTS PER YEAR**

- ANALYSIS, TESTING, DEVELOPMENT, CONSULTING & SERVICES FOR VENDORS, MAGAZINES, GOVERNMENT AGENCIES & COMPANIES

EVERYTHING IS A TARGET.
YOUR HEALTH DATA IS NEXT

THE AV-TEST INSTITUTE

- **MORE THAN 30 IT-SPECIALISTS**
- **MORE THAN 15 YEARS EXPERIENCE IN ANTI-MALWARE-RESEARCH**

- **ONE OF THE LARGEST MALWARE REPOSITORIES WORLDWIDE**
- **STATIC AND DYNAMIC MALWARE ANALYSIS WITH IN-HOUSE TOOLS**
- **400 CLIENT- AND SERVERSYSTEMS**
- **1.000 TERABYTE TESTDATA**
- **MORE THAN 5.000 INIDIVIDUAL AND COMPARATIVE TESTS PER YEAR**

- **ANALYSIS, TESTING, DEVELOPMENT, CONSULTING & SERVICES FOR VENDORS, MAGAZINES, GOVERNMENT AGENCIES & COMPANIES**

EVERYTHING IS A TARGET.
YOUR HEALTH DATA IS NEXT

AGENDA

Who

… wants access to the data?

Why

… would they want access to the data?
… should you care?

How

… can they get access to the data?

EVERYTHING IS A TARGET.
YOUR HEALTH DATA IS NEXT

(Cyber) Criminals

EVERYTHING IS A TARGET.
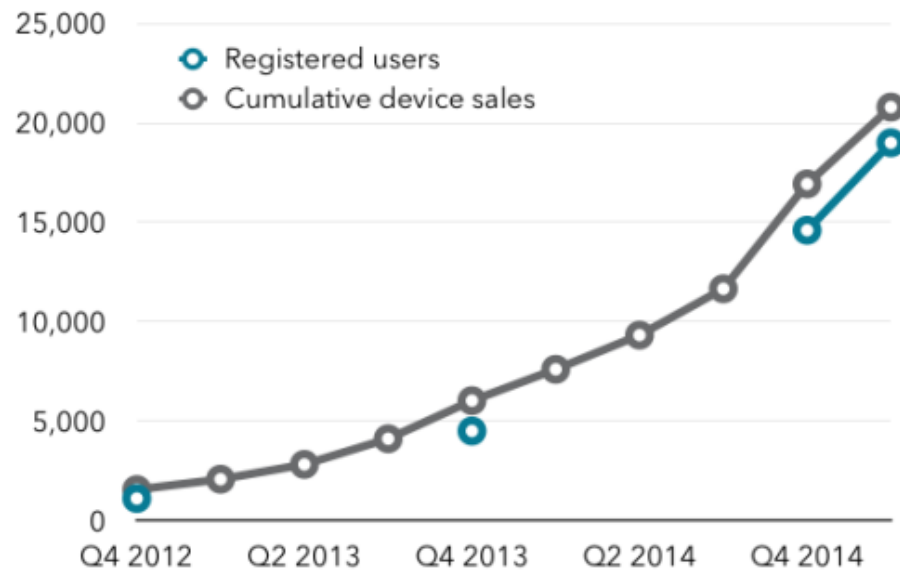YOUR HEALTH DATA IS NEXT

Users

Multi Billion Dollar Companies
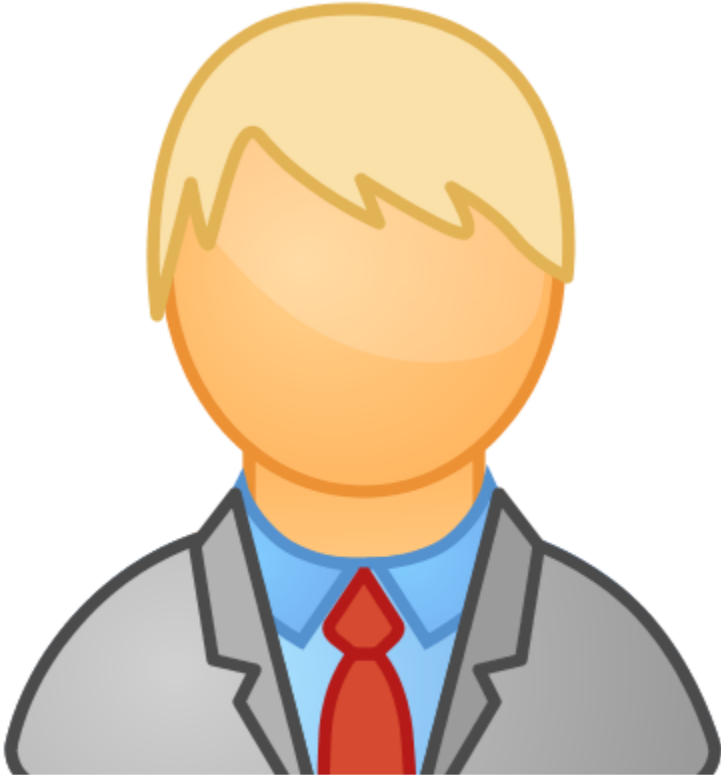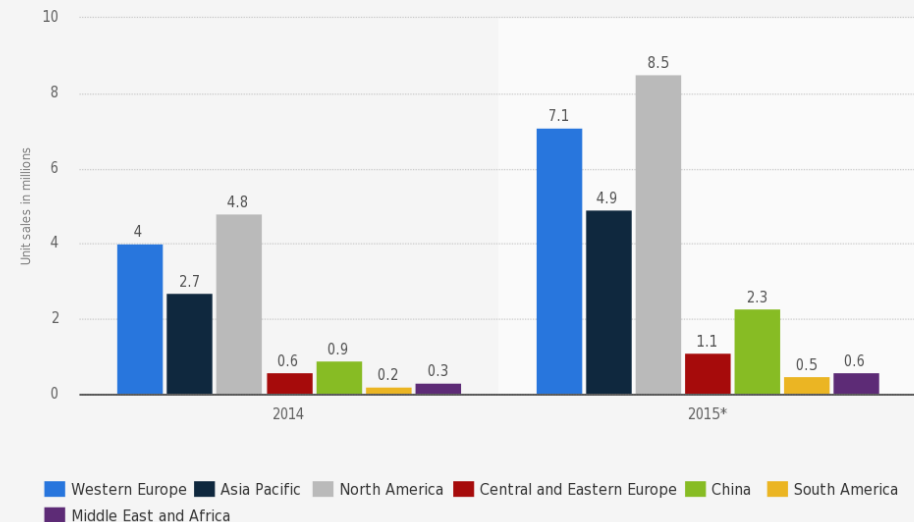
WHY WOULD THEY WANT ACCESS?

- Fitness Trackers may be the next big thing with millions of users
- None or weak security concepts
- Lots of interesting and sensitive data

Measures of base size, 000s

- ○ Registered users
- ○ Cumulative device sales

Source: Fitbit filings, Jackdaw Research

Forecast unit sales of health and fitness trackers worldwide from 2014 to 2015 (in millions), by region

Source::
GfK
© Statista 2015

Additional Information:
Worldwide; 2014 to 2015

EVERYTHING IS A TARGET.
YOUR HEALTH DATA IS NEXT

WHY WOULD THEY WANT ACCESS?

- What kind of data is there anyway?
    - X-axis accelerometer
    - Pedometer
    - Activity Tracker (Walking, Running, Biking, Driving)
    - Sleep Tracker
    - Heart Rate/Pulse
    - Oxygen
    - GPS
    - Skin Temperature
    - Galvanic Skin Response
    - Stress Level
    - Notifications from the Smartphone

- Merkel mahnt, es mit dem **Datenschutz nicht zu übertreiben** (Don't overdo data privacy) http://heise.de/-2812931

- **German Chancellor Angela Merkel: „Daten sind der Rohstoff der Zukunft" (Data: The Resource of the Future)**

- Personal Data is worth a lot of money

Company name	Facebook	LinkedIn	Yahoo	Google
Market cap (in billions)	$100.56	$31.31	$27.67	$282.20
Number of users (in millions)	1,110	225	627	1,300
Revenue (in billions)	$1.813	$0.366	$1.135	$13.110
Per user valuation	$90.59	$131.55	$44.13	$217.08
Average Revenue per User (ARPU)	$1.63	$1.53	$1.81	$10.09

EVERYTHING IS A TARGET.
YOUR HEALTH DATA IS NEXT
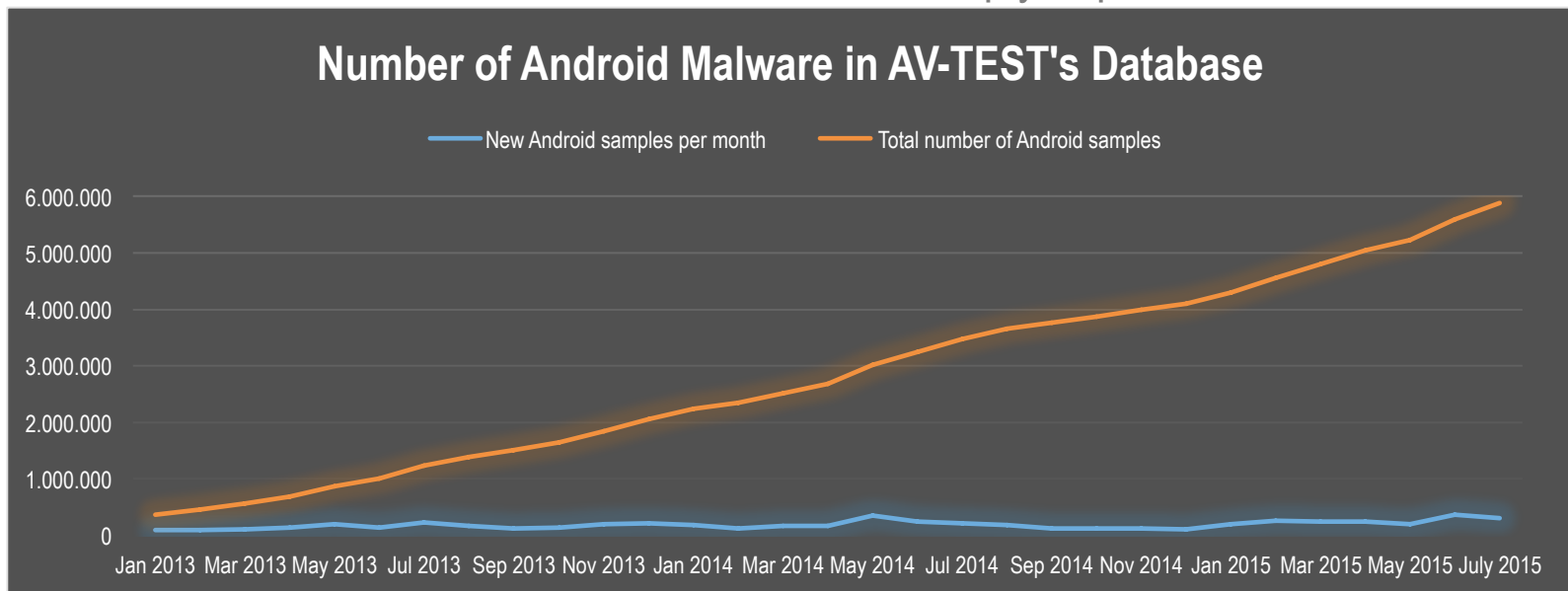
WHY WOULD THEY WANT ACCESS?

- **Insurance** Companies provide **Discounts**
  - Vitality (Insurance Company, UK): „The healthier you get, the more we're able to offer you. It's a virtuous circle that's good for you, good for us, and good for society."

- **German Insurance Companies** will pay subsidies:
  - „Nach der AOK Nordost hat inzwischen auch die Techniker Krankenkasse Wearables und Fitnesstracker offiziell in ihr Bonusprogramm aufgenommen – darunter auch die Apple Watch." http://heise.de/-2817046
  - They claim they are not interested in the data (yet)

- **Users** may want to **manipulate** the data for better discounts

- **Attackers** may **hold the data to ransom** and threaten the user with loss of their discounted rates

- **Tracking of users** becomes even easier
  - "Security Expert Warns of Criminals Using Facebook to Plan Home Burglaries"
  - You don't even need to actively post, attackers will read the GPS of your fitness tracker
  - „Health-Schufa" (consumer reporting agency) may prevent you from getting the job, the bank loan or the wife you wanted

- "**Wearable tech** will transform sport – but will it also **ruin athletes' personal lives**?"
  - "Wearable technologies and big-data analytics are enabling coaches, trainers and general managers to analyze previously unquantifiable aspects of athletic performance in fine detail. But as more technology gets strapped on to professional athletes, some are beginning to express concern over how such devices could be used to track their diet, sleep patterns and life off the field."
  - By faking data you could manipulate careers or even destroy them

WHY WOULD THEY WANT ACCESS?

- University of Illinois: Using a **homegrown app** on a Samsung Gear Live smartwatch, the researchers were able to **guess what a user was typing** through data "leaks" produced by the watches' motion sensors. https://www.ece.illinois.edu/newsroom/article/11762
  - Researchers were essentially able to **guess passwords**
  - **Android malware** is on the rise. It could simply implement this as well

Number of Android Malware in AV-TEST's Database

— New Android samples per month   — Total number of Android samples

HOW CAN THEY GET ACCESS?

- **AV-TEST evaluated** the security of **9 popular fitness trackers**, results are available at
    - https://www.av-test.org/en/news/news-single-view/test-fitness-wristbands-reveal-data/
    - https://www.av-test.org/fileadmin/pdf/avtest_2015-06_fitness_tracker_english.pdf

- **Majority of devices had security issues** that allowed unauthorized local or remote acces to the data or even the manipulation of data

- Security issues were reported to several vendors
    - Fitbit is going to release a firmware update fixing two critical security issues after working on this with us for the last few weeks
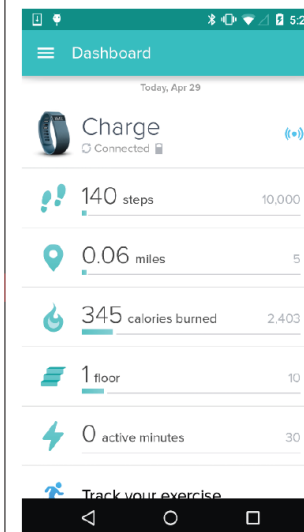   - Others didn't reply at all and devices are still vulnerable

Live-Data, provides Fitness Data without authentication

Notifications can be enabled to share the data in (near) real time

In the upcoming fix the data will be encrypted

```
1   // ... Initialize Bluetooth LE scanning via standard Bluetooth LE protocol
2   // ... Establish connection to "Charge" via standard Bluetooth LE protocol
3   // ... Discover services running on tracker via standard Bluetooth LE protocol
4
5   public void onServicesDiscovered(BluetoothGatt gatt, int status) {
6       //Fitness data service; UUID from service discovery
7       BluetoothGattService service = gatt.getService(UUID.fromString("558dfa00-4fa8-4105-9f02-4eaa93e62980"));
8
9       //Enable notifications to retrieve fitness data whenever it has changed;
10      BluetoothGattCharacteristic serviceCharacteristic = service.getCharacteristic(UUID.fromString("558dfa01-4fa8↵
        -4105-9f02-4eaa93e62980"));
11
12      setCharacteristicNotification(gatt, serviceCharacteristic, true);
13      // ... Be notified whenever updated fitness data is available
14  }
15
16  public void onCharacteristicChanged(BluetoothGatt gatt, BluetoothGattCharacteristic characteristic) {
17      //Fetch the data
18      byte[] data = characteristic.getValue();
19  }
```

EVERYTHING IS A TARGET.
YOUR HEALTH DATA IS NEXT

Replay Attack to manipulate data

- Device Time and Alarm clock can be changed
- Fitness Data can be erased

The upcoming fix will prevent this attack

```
2D020000  00000100  00002D02  00000000  51100000
00000000  000099A8  02702852  09002911  00D402A6
03000000  00000000  20011000  00000020  20202020
20202020  20535445  50474545  4B202048  49205448
45524520  20484F57  44592020  20202000  00000000
00000000  00000000  00000000  000045B2  4C550000
00000000  00000000  00000000  00000000  00000000
04000000  14820000  1C020110  0DFC0FC0  FC0FC0FF
FFC0FC0F  C0FC0000  BC7F0000  1C020110  0DFC0FC0
FC0FC0FF  FFC0FC0F  C0FC0001  907E0000  1C020110
0DFC0FC0  FC0FC0FF  FFC0FC0F  C0FC0002  E8800000
1C020110  0DFC0FC0  FC0FC0FF  FFC0FC0F  C0FC0003
04000000  0545B24C  550238B2  4C550124  B24C5504
38B24C55  04000000  01102700  80000000  000AFFF0
3F03F03F  03F0381C  00000000  02000000  00E71400
000AFFF0  3F03F03F  03F0381C  00000000  03000000
00000000  000AFFF0  3F03F03F  03F0381C  00000000
04000000  00000000  000AFFF0  3F03F03F  03F0381C
00000000  02007924  A8060000  00000900  01234798
06000000  0009006D  37000000  00000000  00000087
E4000000  00000000  0000002A  20000000  00000091
0100
C002
```
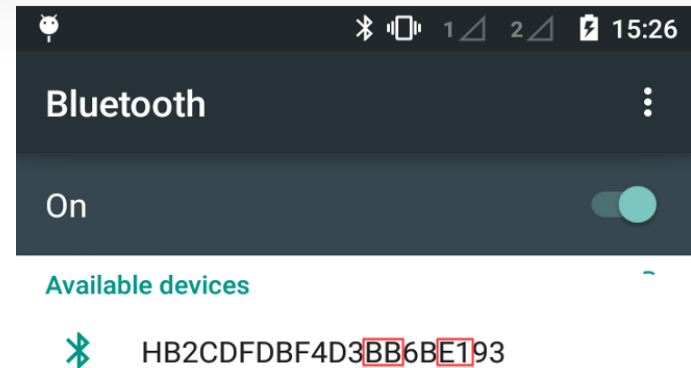
Welcome Text „STEPGEEK HI THERE HOWDY"

UNIX Epoch → Tracker Systemtime

UNIX Epoch → Alarm Clock time

EVERYTHING IS A TARGET.
YOUR HEALTH DATA IS NEXT

HOW CAN THEY GET ACCESS? (Example 2)

- Rebranded and distributed by several vendors (e.g. Acer)
- Pairing
  - **Requires a PIN**
  - 4-digit Hex-Code
  - Problem: **„Code"** can be extracted from the **device name**
- Manipulation
  - Original App uses a library to communicate with the tracker, this library can be (ab)used by anyone, no obfuscation, no other security measures
  - It was possible to write a fake App that has full access to the tracker and is able to manipulate the data

Bluetooth
On
Available devices
HB2CDFDBF4D3BB6BE193

- Bluetooth Connectivity
  - **Paring should (!) require hardware access** (by pressing a button on the tracker)
  - **Pairing and Connecting** was possible anyway (no matter if original or fake App, known or unknown Smartphone)

- Authentication
  - Original-App checks **Characteristics** to verify **authenticity of the device**
    - Serial-Number of `00002a25-0000-1000-8000-00805f9b34fb`
    - Software-Version of `00002a26-0000-1000-8000-00805f9b34fb`
    - Type-Description of `00002a27-0000-1000-8000-00805f9b34fb`
    - Hardware-Version of `00002a28-0000-1000-8000-00805f9b34fb`
    - Company Name of `00002a29-0000-1000-8000-00805f9b34fb`
  - Tracker doesn't perform any checks of **Smartphone** or **App** → **Anyone can connect**

- After succesful connection (and without authentication) **data could be manipulated**

HOW CAN THEY GET ACCESS?

- Why is that so?
  - **Vendors don't think about security** at all. One reply we got from a vendor: „Why would anyone hack a fitness tracker?"
  - Vendors have **no experience or knowledge** in the IT Security field
    - Even if they try to implement security, they fail
    - Old mistakes are repeated over and over again:
      - No authentication, broken authentication implementation
      - No encryption, bad encryption implementation
      - Mistakes we have seen 10 or 15 years ago in the traditional IT
  - **Tight deadlines**, market demands, **features** always come first
    - Fixing security after something happened is always more work and more expensive

Final Remarks

- Should **users** completely **abandon these devices**?
  - No, but they should be aware that a lot of devices will give away more information than they expect
  - There are a few devices that have a robust security implementation
  - Right now there are no known real-world attacks to fitness trackers. The possibility is there, but attacks will only be carried out on a larger scale when someone gains benefit from this.

- Should **insurance companies** really give **discounts based on fitness tracker** data?
  - Talk to us, we will tell you which device you can trust

- There is much more to come. Criminals (and companies) are way more creative and better in finding ways to monetarize this data

- Even legitimate ways to get (more or less) unauthorized access to your data are imaginable (**The resource of the future!**)

Thank you very much for your attention!