YOU ARE THE TARGET IN THE IOT
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 INDIVIDUAL AND COMPARATIVE TESTS PER YEAR
- ANALYSIS, TESTING, DEVELOPMENT, CONSULTING & SERVICES FOR VENDORS, MAGAZINES, GOVERNMENT AGENCIES & COMPANIES

04.12.2015
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 individual and comparative tests per year
- Analysis, testing, development, consulting & services for vendors, magazines, government agencies & companies

04.12.2015

YOU ARE THE TARGET IN THE IOT
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?
WHO WANTS ACCESS?

(Cyber) Criminals
WHO WANTS ACCESS?

Users
WHO WANTS ACCESS?

Multi Billion Dollar Companies
By 2016 Gartner predicts **6.4 billion** devices will be connected to the internet -- and **5.5 million new 'things'** will join them **each day**.

### Table 1: Internet of Things Units Installed Base by Category (Millions of Units)

<table>
<thead>
<tr>
<th>Category</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer</td>
<td>2,277</td>
<td>3,023</td>
<td>4,024</td>
<td>13,509</td>
</tr>
<tr>
<td>Business: Cross-Industry</td>
<td>632</td>
<td>815</td>
<td>1,092</td>
<td>4,408</td>
</tr>
<tr>
<td>Business: Vertical-Specific</td>
<td>898</td>
<td>1,065</td>
<td>1,276</td>
<td>2,880</td>
</tr>
<tr>
<td>Grand Total</td>
<td>3,807</td>
<td>4,902</td>
<td>6,392</td>
<td>20,797</td>
</tr>
</tbody>
</table>

### Table 2: Internet of Things Endpoint Spending by Category (Billions of Dollars)

<table>
<thead>
<tr>
<th>Category</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer</td>
<td>257</td>
<td>416</td>
<td>546</td>
<td>1,534</td>
</tr>
<tr>
<td>Business: Cross-Industry</td>
<td>115</td>
<td>155</td>
<td>201</td>
<td>566</td>
</tr>
<tr>
<td>Business: Vertical-Specific</td>
<td>567</td>
<td>612</td>
<td>667</td>
<td>911</td>
</tr>
<tr>
<td>Grand Total</td>
<td>939</td>
<td>1,183</td>
<td>1,414</td>
<td>3,010</td>
</tr>
</tbody>
</table>

Source: Gartner (November 2015)
WHY WOULD THEY WANT ACCESS?

- Smart Home is already a big market with lots of big brand names
  - nest
  - HomeKit
  - Samsung SmartThings

- Most people use smart home for security

Figure 3: Security is the top benefit for half of Americans

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home would be more secure</td>
<td>50%</td>
</tr>
<tr>
<td>Monitor activity at home while away</td>
<td>46%</td>
</tr>
<tr>
<td>Cut costs and lower energy bills</td>
<td>40%</td>
</tr>
<tr>
<td>Home would be more convenient</td>
<td>35%</td>
</tr>
<tr>
<td>Better protection from fire, floods, etc</td>
<td>29%</td>
</tr>
<tr>
<td>Feel more tech savvy</td>
<td>19%</td>
</tr>
</tbody>
</table>

Source: Lowe’s via Greentechmedia
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
WHY WOULD THEY WANT ACCESS?

- What kind of data is there anyway?

<table>
<thead>
<tr>
<th>Fitness Tracker</th>
<th>Smart Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-axis accelerometer</td>
<td>Room Temperature</td>
</tr>
<tr>
<td>Pedometer</td>
<td>House/Apartment Layout</td>
</tr>
<tr>
<td>Activity Tracker (Walking, Running, Biking)</td>
<td>Air Quality/CO2 Level</td>
</tr>
<tr>
<td>Sleep Tracker</td>
<td>Noise Level</td>
</tr>
<tr>
<td>Heart Rate/Pulse</td>
<td>Power Consumption</td>
</tr>
<tr>
<td>Oxygen</td>
<td>TV Usage</td>
</tr>
<tr>
<td>GPS</td>
<td>At home/not at home</td>
</tr>
<tr>
<td>Skin Temperature</td>
<td>Who is at home</td>
</tr>
<tr>
<td>Galvanic Skin Response</td>
<td>How many people are at home</td>
</tr>
<tr>
<td>Stress Level</td>
<td>Usage of devices</td>
</tr>
<tr>
<td>Notifications from the Smartphone</td>
<td></td>
</tr>
</tbody>
</table>
WHY WOULD THEY WANT ACCESS?

- 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)
WHY WOULD THEY WANT ACCESS?

- Personal Data is worth a lot of money

<table>
<thead>
<tr>
<th>Company name</th>
<th>Facebook (in billions)</th>
<th>LinkedIn (in millions)</th>
<th>Yahoo (in millions)</th>
<th>Google (in billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market cap</td>
<td>$100.56</td>
<td>$31.31</td>
<td>$27.67</td>
<td>$282.20</td>
</tr>
<tr>
<td>Number of users</td>
<td>1,110</td>
<td>225</td>
<td>627</td>
<td>1,300</td>
</tr>
<tr>
<td>Revenue</td>
<td>$1.813</td>
<td>$0.366</td>
<td>$1.135</td>
<td>$13.110</td>
</tr>
<tr>
<td>Per user valuation</td>
<td>$90.59</td>
<td>$131.55</td>
<td>$44.13</td>
<td>$217.08</td>
</tr>
<tr>
<td>Average Revenue per User (ARPU)</td>
<td>$1.63</td>
<td>$1.53</td>
<td>$1.81</td>
<td>$10.09</td>
</tr>
</tbody>
</table>
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](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
WHY WOULD THEY WANT ACCESS?

- **Tracking of users** becomes even easier
  - „Health-Schufa“ (consumer reporting agency) may prevent you from getting the job, the bank loan or the wife you wanted because of your health data
  - **Individulal pricing/Price discrimination** already done today (Gas/Petrol costs more on public holidays) and can be more used in future when shops know who you are, how much money you have, what you like etc.

- **“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
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](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
WHY WOULD THEY WANT ACCESS?

- Following our Research of **Fitness Trackers** we got inquiries of different **public authorities**
  - **Pathologist** that was working on a case of a dead person wearing a fitness tracker. Would it be possible to determine the **time of death** by the tracker data? Would it be possible to **forge this data**?
  - **Police Authorities** that are interested to know whether this data can **prove or disprove alibis**. What did a person possibly do during a certain time? Did the heart beat rate go up or was it steady? Is there GPS information? Was there a sync to the cloud, meaning there was internet connectivity?
University of Applied Sciences Münster, Germany: Multimedia Content Identification Through Smart Meter Power Usage Profiles
https://epic.org/privacy/smartgrid/smart_meter.pdf

Smart Meters can become surveillance devices and “allow intrusive identification and monitoring of equipment within consumers’ homes (e.g., TV set, refrigerator, toaster, and oven). Our research shows that the analysis of the household’s electricity usage profile at a 0.5s−1 sample rate does reveal what channel the TV set in the household was displaying. It is also possible to identify (copyrightprotected) audiovisual content in the power profile that is displayed on a CRT1, a Plasma display TV or a LCD2 television set with dynamic Backlighting”
WHY WOULD THEY WANT ACCESS?

- There has been something in the media ...
  - **Burglars** used to check Facebook, Google+ or Twitter if persons are going on vacation and if the house is free to break in. Now they could just access **thousands of insecure Smart Home** systems to know exactly when **somebody is home or not**.
AV-TEST examined the security of over 30 IoT devices during the last two years.

18 Smart Home Devices

14 Fitness Trackers

We are testing more devices every week and new publications are planned already.

Credit for the research has to go to my team: AV-TEST Threat Research lead by Ulf Lösche and the two researchers Eric Clausing and Michael Schiefer.
HOW CAN THEY GET ACCESS?

- **Majority of devices had security issues** that allowed unauthorized local or remote access to the data or even the manipulation of data.
- We are seeing **similar problems** in **different product categories**.
- **All components** of the products are **prone to security issues**
  - The device itself (firmware)
  - The apps to control/configure the device
  - The web/cloud services
- **Security issues were reported to several vendors**
  - Only a few actually responded and out of those only some acknowledged the security issues and fixed them.
  - Others didn‘t reply at all and devices are still vulnerable.
**HOW CAN THEY GET ACCESS? (Example 1)**

- **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

---

```java
// ... Initialize Bluetooth LE scanning via standard Bluetooth LE protocol
// ... Establish connection to "Charge" via standard Bluetooth LE protocol
// ... Discover services running on tracker via standard Bluetooth LE protocol

public void onServicesDiscovered(BluetoothGatt gatt, int status) {
    //Fitness data service: UUID from service discovery
    BluetoothGattService service = gatt.getService(UUID.fromString("558dfa00-4fa8-4105-9f02-4eaa93e62980"));

    //Enable notifications to retrieve fitness data whenever it has changed;
    BluetoothGattCharacteristic serviceCharacteristic = service.getCharacteristic(UUID.fromString("558dfa01-4fa8-4105-9f02-4eaa93e62980"));

    serviceCharacteristic.setNotification(gatt, serviceCharacteristic, true);
    // ... Be notified whenever updated fitness data is available
}

public void onCharacteristicChanged(BluetoothGatt gatt, BluetoothGattCharacteristic characteristic) {
    //Fetch the data
    byte[] data = characteristic.getValue();
}
```
HOW CAN THEY GET ACCESS? (Example 1)

- **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

![Image with hexadecimal data]

Welcome Text "STEPGEEK HI THERE HOWDY"

UNIX Epoch → Tracker Systemtime

UNIX Epoch → Alarm Clock time

<table>
<thead>
<tr>
<th>2D020000</th>
<th>00000100</th>
<th>0002D02</th>
<th>00000000</th>
<th>51100000</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>00099A8</td>
<td>02702852</td>
<td>09002911</td>
<td>00D402A6</td>
</tr>
<tr>
<td>03000000</td>
<td>00000000</td>
<td>20011000</td>
<td>00000020</td>
<td>20202020</td>
</tr>
<tr>
<td>20202020</td>
<td>20535445</td>
<td>50475454</td>
<td>4B202048</td>
<td>49205448</td>
</tr>
<tr>
<td>45524520</td>
<td>20484F57</td>
<td>44592020</td>
<td>20202000</td>
<td>00000000</td>
</tr>
<tr>
<td>00000000</td>
<td>00000000</td>
<td>00000000</td>
<td>00000000</td>
<td>01102700</td>
</tr>
<tr>
<td>06200000</td>
<td>00000000</td>
<td>00000000</td>
<td>00000000</td>
<td>000AFFF0</td>
</tr>
<tr>
<td>3F03F03F</td>
<td>03F0381C</td>
<td>00000000</td>
<td>02000000</td>
<td>00E71400</td>
</tr>
<tr>
<td>000AFFF0</td>
<td>3F03F03F</td>
<td>03F0381C</td>
<td>00000000</td>
<td>03000000</td>
</tr>
<tr>
<td>00000000</td>
<td>000AFFF0</td>
<td>3F03F03F</td>
<td>03F0381C</td>
<td>00000000</td>
</tr>
<tr>
<td>04000000</td>
<td>00000000</td>
<td>000AFFF0</td>
<td>3F03F03F</td>
<td>03F0381C</td>
</tr>
<tr>
<td>00000000</td>
<td>02007924</td>
<td>A8060000</td>
<td>00009000</td>
<td>01234798</td>
</tr>
<tr>
<td>06000000</td>
<td>0009006D</td>
<td>37000000</td>
<td>00000000</td>
<td>0000087</td>
</tr>
<tr>
<td>E4000000</td>
<td>00000000</td>
<td>0000002A</td>
<td>20000000</td>
<td>0000091</td>
</tr>
<tr>
<td>0100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C002</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
HOW CAN THEY GET ACCESS? (Example 3)

- Bluetooth Connectivity
  - **Pairing 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 successful connection (and without authentication) **data could be manipulated**
Smart Home Device that does **everything unencrypted**

- Login to webportal, sending **username and password in cleartext**

```plaintext
POST /login HTTP/1.1
Host: max.eq-3.de
Connection: keep-alive
Referer: http://max.eq-3.de/login.jsp
Content-Length: 64
Cache-Control: max-age=0
Origin: http://max.eq-3.de
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Linux; U; Android 4.0.4; de-de; SonyEricsson[...] Build/4.1.B--
.0.131) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
Accept-Encoding: gzip, deflate
Accept-Language: de-DE, en-US
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
x-wap-profile: http://wap.sonyericsson.com/UAProtocol/ [...].xml
Cookie: JSESSIONID=[...]

user=[...]&pwd=[...]&submit=submit&mobile=false&productKey=
```

- Same for actual usage of the device, anyone in the network can **take control with simple HTTP requests**
Smart Home Device that offers **backup of the configuration in the cloud**

- It is possible to **crawl the cloud for ALL backups** of all users by just providing the serial number of the device which is easy to manipulate:

  ```
  ```

- If there is a backup for this serial number you will receive details for this backup:

  ```json
  [{"id":"16625","timestamp":"1438147643","devices":"0","rooms":"0","scenes":"0","description":"please do not delete","softVersion":"4.041","version":"4.041","compatible":true},
  {"id":"16582","timestamp":"1438094009","devices":"0","rooms":"0","scenes":"0","description":"some Test","softVersion":"4.041","version":"4.041","compatible":true}]
  ```

- Once you have the ID you can **download the given backup** by supplying the required information to:

  ```
  POST /getBackup.php HTTP/1.1
  ```
HOW CAN THEY GET ACCESS? (Example 5)

- It is possible to **delete the backup**
  
  POST /deleteBackup.php HTTP/1.0

- It is possible to **replace the backup** and this is where it gets interesting.

- The backup is just a **plain LiteSQL Database** and stores **username, password (hashed) and user privileges**

- You can **add new users** and/or **change privileges to superuser** and **upload the configuration for other devices**. If they use the backup they will use the forged information.

```
401 25 SendNotifications false
402 25 TrackUser 0
403 25 UserType "SuperUser"
404 25 deviceIcon "she"
405 25 host "06bbd7e9e38c3592b34015b5a01d0f"
406 25 initialWizard true
407 25 pin "123456"
408 25 sipDisplayName "Horn"
409 25 sipUserID "1234567890"
410 25 sipUserPassword "SP@123"
411 25 useOptionalAvpPin false
412 25 usePin false
413 20 Email "nie@example.de"
414 20 HotelModeRoom 0
415 20 Latitude 0.0000000000000000
416 20 Location "00"
```
HOW CAN THEY GET ACCESS? (Example 6)

- A **smart home product** that has a **backdoor** in the device
- The device phones home every few minutes

```bash
#!/bin/sh -x
SERIAL=`fw_printenv serial | cut -d'-' -f 2`
cd /tmp
rm -f /tmp/$SERIAL
wget http://update.xxxxx.com/philia/phone_home/$SERIAL
if [-z /tmp/$SERIAL ]; then #file not empty
    if [-x /usr/sbin/update.philia.com/output.tmp/$SERIAL ]
        /usr/bin/nosh
        /usr/bin/socat
            TCP4:udp:192.168.1.123:12345
            /tmp/$SERIAL
    else
        # file not running
    fi
else
    # file not empty
fi
```

- If successful the local box will open a **SSH connection to the remote server** which has then **full control over the local box**
- This connection can be manipulated and control over the SSH connection can be taken, resulting in full control over the local box
HOW CAN THEY GET ACCESS? (Example 7)

- A **smart home product** that uses **SSL for the remote connection** but doesn’t verify the connection, so man-in-the-middle attacks are possible.
- Once this succeeds it is possible to **read the encrypted network traffic** including an access token that can be used to take over the connection.
- No further logins are necessary once you got the access token.
- The **access token remains valid** even after the user logs out of the active session:
  - It is possible to retrieve **user information** including the **PIN for local access** to the device, resulting in **full control over the box**.
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
WHAT SHOULD BE DONE?

- Actually two perspectives are important …
WHAT SHOULD BE DONE?

- Actually two perspectives are important …
WHAT SHOULD BE DONE?

- **Technology Improvements**
  - **Threat Modeling**, yes even if you are building a *smart fridge* …
  - Security-by-Design
  - Robust implementation: Secure libraries? Secure OS?
  - External penetration/security testing to improve internal processes
  - External verification/certification to introduce and enforce security standards
  - External security measures: security appliance in the network, security software on the client devices (Smartphone, Tablet, PC)
WHAT SHOULD BE DONE?

- Users have no chance to know whether an App or device is secure → Technology improvements
- Users often don’t know what data is being collected and processed
- Non-Technical Improvements
  - Privacy Laws:
    - What data is allowed to be collected?
    - … to be transmitted?
    - … to be processed?
    - Who is allowed to do this?
    - Is this opt-in, opt-out or even mandatory?
  - Education of users
    - Tell them about possible security issues
    - Give guidelines on how to secure their systems and devices

04.12.2015
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 not many real-world attacks. The possibility is there, but attacks will only be carried out on a larger scale when someone gains benefit from this.

- 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!