

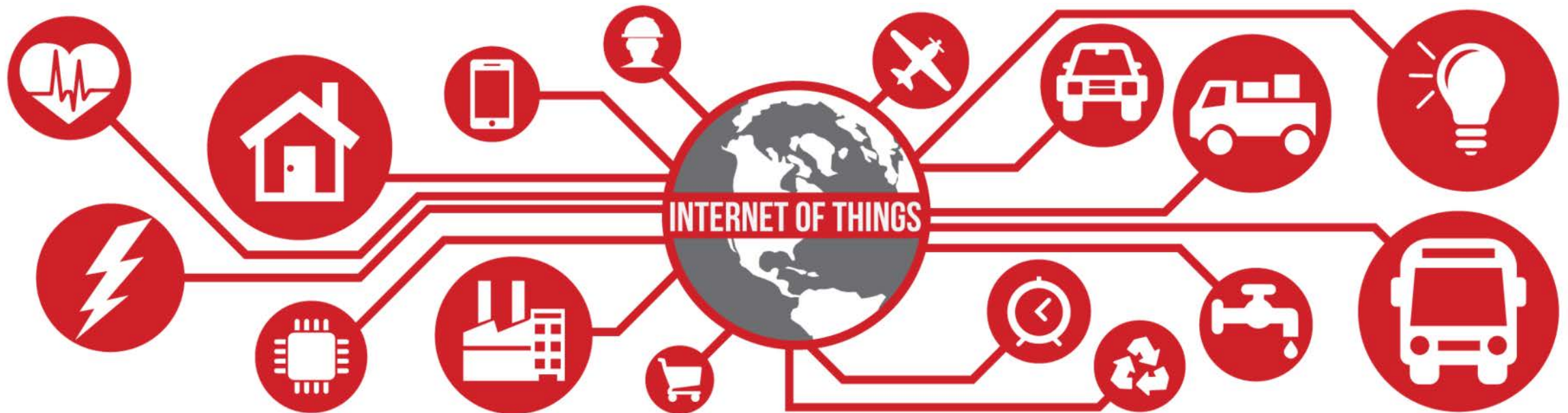
**Павел Новиков,**

Руководитель группы исследований безопасности телекоммуникационных систем  
Positive Technologies

# Победы и поражения крупных компаний в попытке обуздать легион уязвимых вещей

**POSITIVE TECHNOLOGIES**

[ptsecurity.ru](https://ptsecurity.ru)



- Я сделал новую СУБД для IoT
- Я сделал новый суперкомпьютер для IoT
- Я сделал датчик для IoT
- Я сделал GSM для IoT
- А мы 5G уже сразу для IoT делаем!



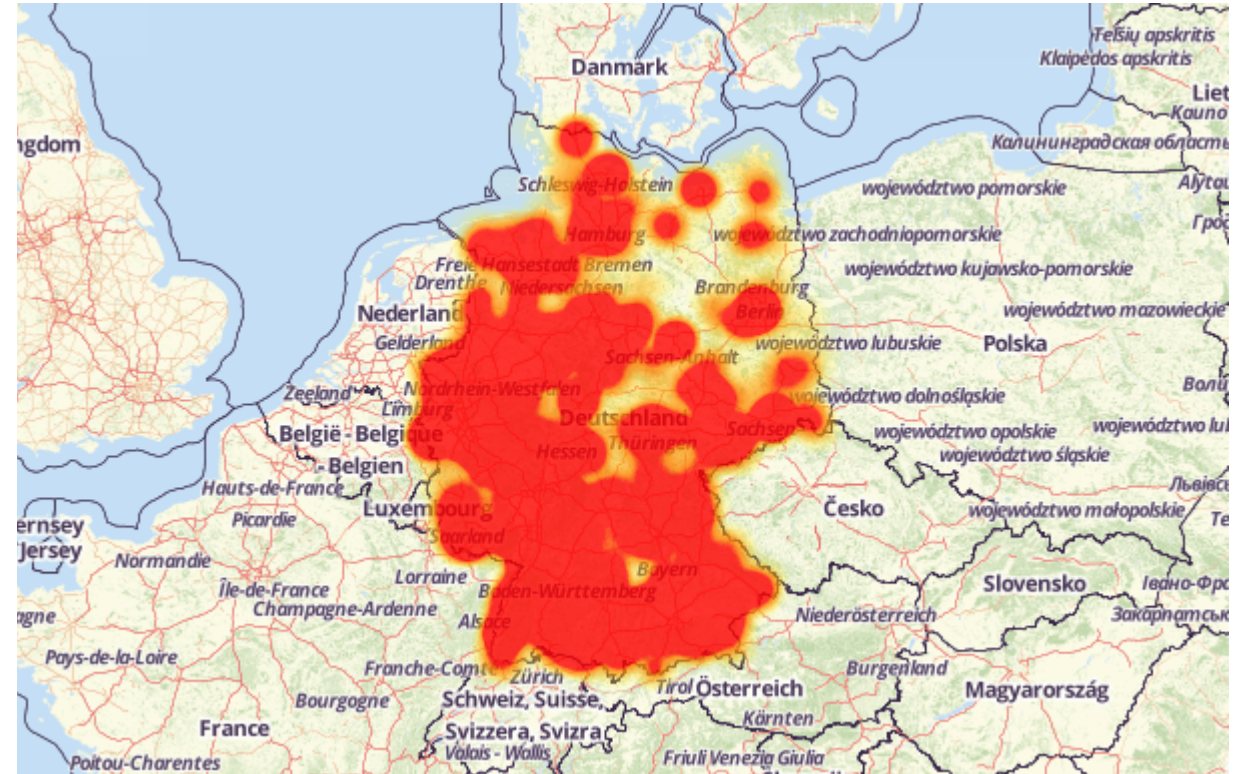
- Словарные учетные данные, более 60 комбинаций
- Telnet доступный из сети интернет
- Владельцы устройств не знают о проблеме
- Хакеры перехватывают друг у друга
- TR-069



<https://www.bleepstatic.com/content/hl-images/2016/12/12/Mirai.jpg>



- Deutsche Telekom
- Более 900 000 устройств
- Speedport Arcadyan



Подозреваемый задержан в аэропорту  
<https://habrahabr.ru/company/pt/blog/322712/>

- 800 000 аккаунтов пользователей скомпрометировано
- Более 2М аудиозаписей в сети
- MongoDB со всеми данными пользователей доступна в сети Интернет без пароля



20 января 2016 в 17:16

## Хакеры взламывают видеоняни, терроризируют детей и выкладывают в сеть их фотографии новость

Умный дом, Поток видео, Информационная безопасность, Гаджеты, Видеотехника

Если ваш маленький ребёнок говорит, что слышит монстров в своей комнате, и при этом в детской стоит радио/видеоняня – лучше послушайте его. В сентябре 2015 исследователи проверили множество устройств для того, чтобы следить за детьми, и пришли к выводу: почти все они имеют уязвимости.



Пара из Сан-Франциско не могла понять, почему их трёхлетний сын не может уснуть. Он рассказывал, что «телефон» с ним разговаривает. Понимание пришло только тогда, когда его мама поздно вечером услышала из комнаты, как радионяня говорила «Проснись, маленький мальчик, папочка ищет тебя». Когда мама вошла в комнату, камера повернулась в ее сторону и голос добавил «Смотрите, кто-то зашёл». Другая семья из Миннесоты обнаружила фотографии своего ребёнка в сети. Эти фото сделаны с помощью детского монитора.

<https://geektimes.ru/post/269474/>

25 января 2016 в 16:23

## Что не так с безопасностью в Интернете Вещей: Как Shodan стал «поисковиком спящих детей»

Информационная безопасность\*, Блог компании Positive Technologies



Знаменитый поисковый сервис Shodan не так давно запустил раздел, позволяющий пользователям просматривать изображения с уязвимых подключенных к интернету веб-камер. За короткое время работы в кадр уже попали плантации конопли, задние дворы банков, детские спальни, кухни, гостиные, бассейны, школы и колледжи, лаборатории, магазины.

<https://habrahabr.ru/company/pt/blog/275853/>



18 декабря 2015 в 12:03

## Дети и родители в Сети: история взлома сервисов VTech

Информационная безопасность\*, Блог компании ua-hosting.company



Утечка данных пользователей различных сервисов из-за взлома последних — далеко не редкость, к сожалению. Стоит только вспомнить нашумевший взлом сервиса измен Ashley Madison, когда в Сеть утекли данные миллионов пользователей. Огромное количество пользователей оказались просто ботами, но это ничего не меняет — каждый из нас уязвим.

<https://habrahabr.ru/company/ua-hosting/blog/273423/>

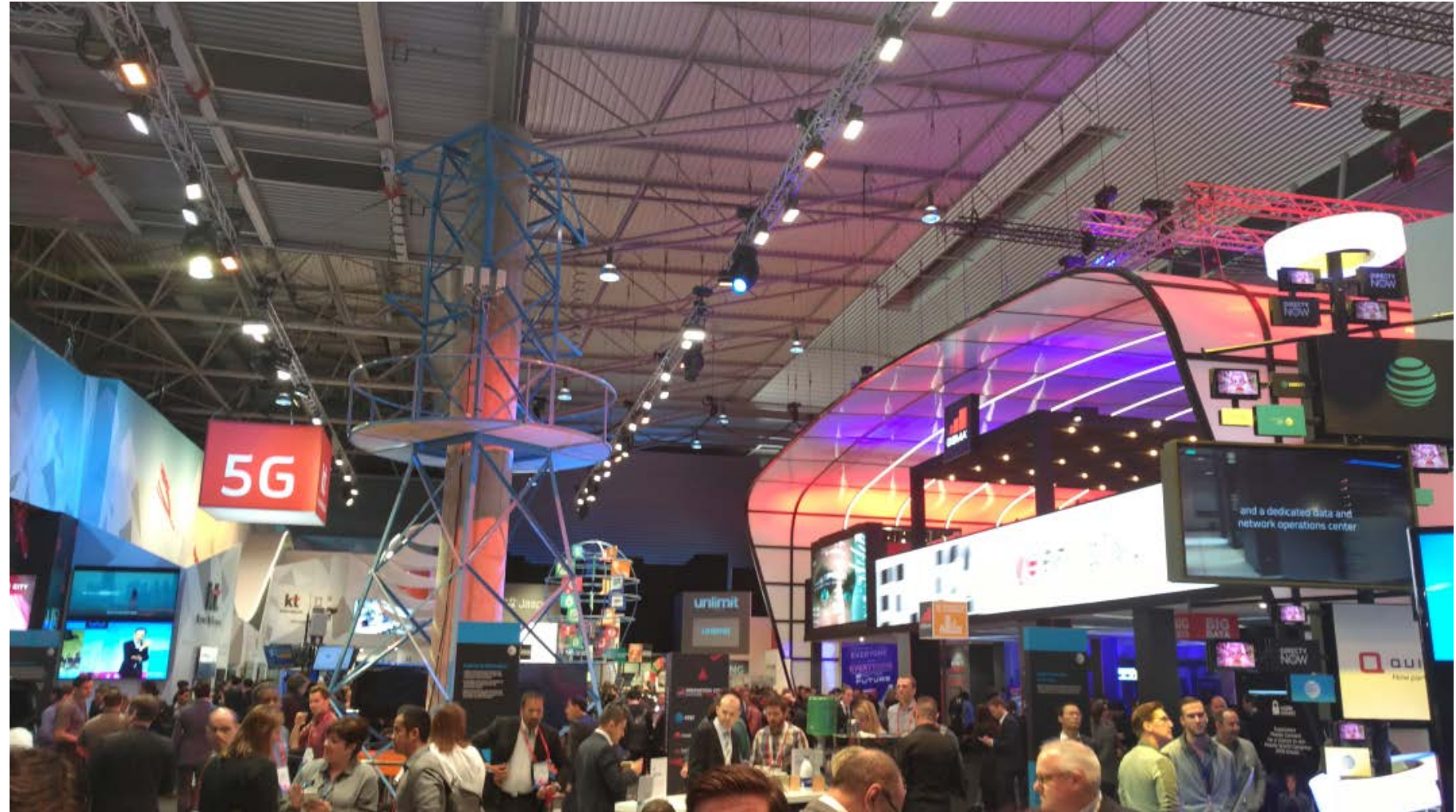








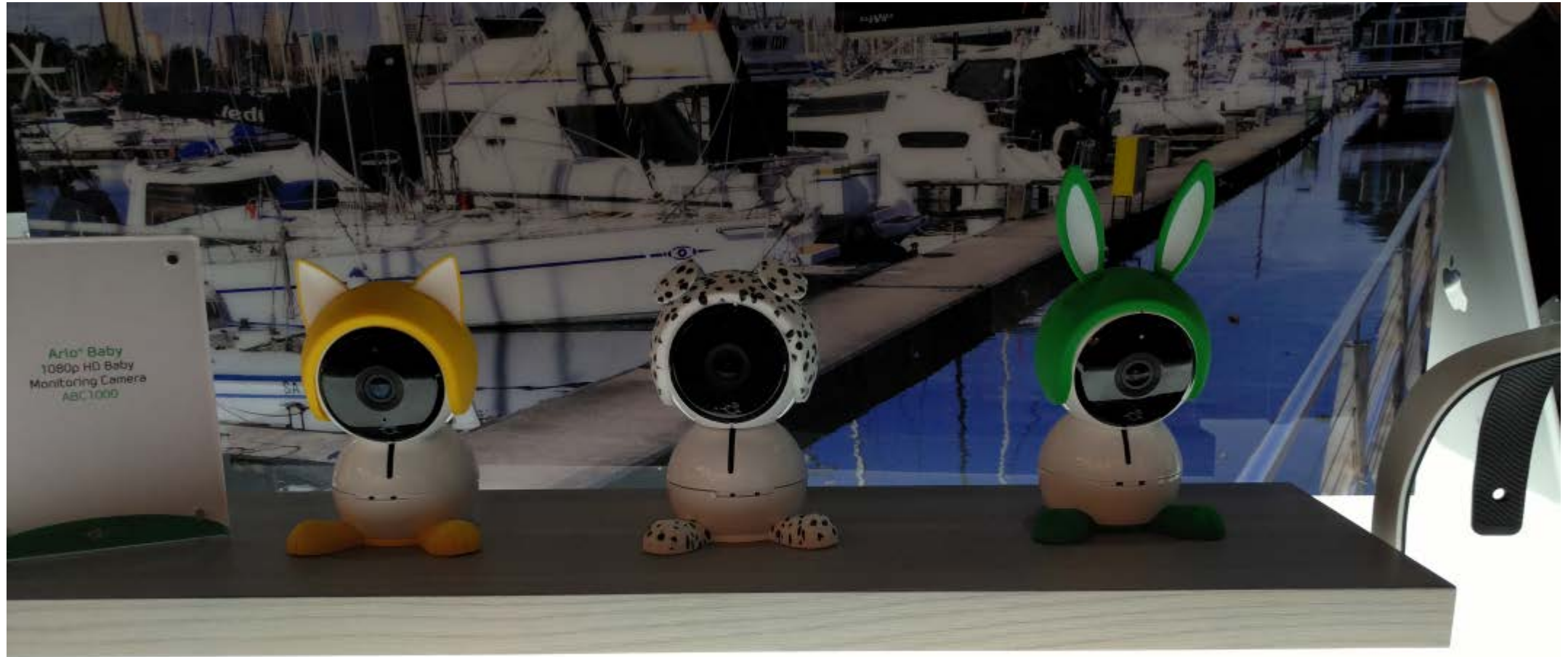








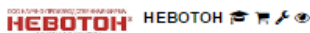






# Вернемся к делу: «умный» дом

POSITIVE TECHNOLOGIES



**NEVOTON**  
г. Санкт-Петербург  
ул. Грибакиных д.25, корп.3  
(показать на карте)  
+7 (812) 327-49-56  
<http://domoton.ru>  
[domoton@nevoton.ru](mailto:domoton@nevoton.ru)



**Фибилоджик**  
Московская обл.  
г. Лобня, ул. Фестивальная, 8, корп.2  
(показать на карте)  
+7 (499) 508-0924  
<http://www.phoebe-logic.ru>  
[mail@phoebe-logic.ru](mailto:mail@phoebe-logic.ru)



**5smart**  
г. Москва  
Спартановская площадь, д.14, стр.3  
(показать на карте)  
8 (800) 333-78-79  
<http://www.5smart.ru>  
[hello@5smart.ru](mailto:hello@5smart.ru)



**ZW-Store**  
Москва  
1 Иргышский проезд д.8 стр1  
(показать на карте)  
+7 (495) 227-19-88  
<http://zw-store.ru/>  
[info@zw-store.ru](mailto:info@zw-store.ru)



**ZWHouse**  
Москва  
Орджоникидзе, 12  
(показать на карте)  
+7 (495) 641 01 42  
<http://zwhouse.ru>  
[info@zwhouse.ru](mailto:info@zwhouse.ru)



**Битеч**  
Севастополь  
проспект Октябрьской Революции, 20  
офис Г.К. «Рублевка»  
(показать на карте)  
+7 (978) 704-47-31  
<http://www.bitech.spb>  
[info@bitechinfo.ru](mailto:info@bitechinfo.ru)



**Мой Дом**  
Ростов-на-Дону  
ул. 1-ой Конной армии 37В  
(показать на карте)  
+7 (8632) 56-52-51  
<http://www.homemakerstore.com>  
[hnmstore@bk.ru](mailto:hnmstore@bk.ru)



**APV Technologies**  
г. Санкт-Петербург  
Савушкина 83, Бизнес-центр "Антарес"  
(показать на карте)  
+7 (921) 927-55-87  
<http://www.apvcom.ru>  
[info@apvcom.ru](mailto:info@apvcom.ru)



**Z-LIFE**  
Москва  
Нахимовский проспект, 24  
(показать на карте)  
+7 (499) 550-80-99  
<http://www.z-life.ru>  
[super@z-life.ru](mailto:super@z-life.ru)



**ИТ-Решения**  
Иркутск  
п.Новая Разводная, ул.Морокая, д.18  
(показать на карте)  
+7 (3952) 950-831  
<http://www.ИТ-дом.орг>  
[brv@it-sol38.ru](mailto:brv@it-sol38.ru)



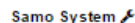
**Плеиз-Инжиниринг**  
г. Казань  
ул. Богатырева д.7  
(показать на карте)  
+7 (843) 239-23-27  
<http://www.ipsumgroup.ru>  
[info@ipsumgroup.ru](mailto:info@ipsumgroup.ru)



**HomeIQ**  
г. Москва  
ул. Челябинская, 19  
(показать на карте)  
+7 (495) 765-5895  
<http://homeiq.ru>  
[info@homeiq.ru](mailto:info@homeiq.ru)



**Плеер.ру**  
г. Москва  
ул. Мастерская 4 (вход со стороны 3-го  
Автозаводского проезда)  
(показать на карте)  
+7 (495) 775-04-75  
<http://www.pleer.ru>



**Samo System**  
Московская обл.  
Одинцовский р-н, пос. Горки-10, д.23  
(показать на карте)  
+7 (495) 565-37-34  
<http://www.samosystem.ru>  
[info@samosystem.ru](mailto:info@samosystem.ru)



**boxsmart.ru**  
Москва  
ул. Серебрянская набережная, 29  
Бизнес-центр Silver City  
(показать на карте)  
+7 495 133 90 54  
<http://www.boxsmart.ru>



**Бюро интеллектуальных систем**  
Нижний Новгород  
ул. Белинского, д.15  
(показать на карте)  
+7 (831) 423-43-77  
<http://www.nnbis.ru>  
[contact@nnbis.ru](mailto:contact@nnbis.ru)



**Доминко**  
г. Уфа  
Республика Башкортостан  
ул. Достоевского д.133, оф.217  
(показать на карте)  
+7 (347) 262-91-24  
<http://www.dominko.ru>  
[info@dominko.ru](mailto:info@dominko.ru)



**Метаматика**  
Уфа  
ул. Комсомольская д. 1/1  
(показать на карте)  
+7 (989) 95-95-891  
<http://metamatica.ru>  
[info@metamatica.ru](mailto:info@metamatica.ru)



**НАНО-ОРГ**  
Москва  
ул. Серебрянская набережная, 29  
Бизнес-центр Silver City  
(показать на карте)  
+7 (499) 705-73-92, +7 (925) 853 08 50  
<http://www.nano-dom.com>  
[info@nano-dom.com](mailto:info@nano-dom.com)



**СЛ ХОУМ**  
г. Санкт-Петербург  
ул. Фарфоровская д.6, оф.108  
(показать на карте)  
+7 (812) 244-03-46  
<http://www.slhome.ru/>  
[info@slhome.ru](mailto:info@slhome.ru)



**Скат**  
г. Москва  
Нахимовский пр-т д.24, ТК Стройсити,  
салони: А-1, Б-4, офис №2  
(показать на карте)  
+7 (495) 644-28-18  
<http://lokat.pro>  
[sale@skat.pro](mailto:sale@skat.pro)



**Смарт-Оптим**  
г. Нижний Новгород  
ул. Бекетова д.13П, оф.204  
(показать на карте)  
+7 (8312) 81-84-94  
<http://smartoptima.ru>  
[info@smartoptima.ru](mailto:info@smartoptima.ru)



**СминХаус**  
г. Сочи  
Краснодарский край  
ул. Горького д.60/4, оф.40  
(показать на карте)  
8 (800) 200-58-85/+7 (961) 582-02-02  
<http://www.sminhouse.ru>  
[shadow@sochi.ru](mailto:shadow@sochi.ru)



**Умная Электроника**  
г. Москва  
ул. Осуевский вал д.5, стр.20, оф.Т1  
(показать на карте)  
+7 (495) 565-33-78, 8 800 3335378  
<http://www.smarttron.ru>  
[info@smarttron.ru](mailto:info@smarttron.ru)



**KZK ASTANA ENGINEERING**  
Казахстан  
Астана, ул. Жигенкуловой 6  
(показать на карте)  
+7 (7172) 34 59 78, +7 708 088 00 87, +7  
702 882 62 09  
[591d5a@gmail.com](mailto:591d5a@gmail.com)



**Дисиб**  
г. Барнаул  
Алтайский край  
ул. Энтузиастов д.54 оф. 5  
(показать на карте)  
+7 (3852) 577-752  
<http://ldi-sib.ru>  
[di22r@mail.ru](mailto:di22r@mail.ru)



**Рободом**  
Геленджик  
ул. Луначарского, 6  
(показать на карте)  
+7 (918) 467-45-31  
<http://www.robodom.pro>  
[dom@robodom.pro](mailto:dom@robodom.pro)



**Умный дом для всех**  
г. Санкт-Петербург  
ул. Литовская 10 оф.2312  
(показать на карте)  
+7 (812) 428-13-17  
<http://smarthome2you.ru>  
[info@smarthome2you.ru](mailto:info@smarthome2you.ru)



BroadLink SC1 Kit Home Alarm Set Door Window PIR Sensor Smart Remote Control App

**\$58.50**

Buy It Now

Free international shipping

Only 1 left!  
6 watching

From China

Top-rated seller



Kit Smart Socket KERUI G19 GSM Home Alarm System,WiFi IP Camera,Pet Friendly

**\$169.99**

Buy It Now

Free international shipping

55 watching  
See more like this

From China

Top-rated seller



Original Xiaomi Smart Home Security Kit Wireless Sensor Control Smart Device Set

**\$48.39**

Buy It Now

20 watching

From China

Top-rated seller



DCH-100KT mydlink Home SMART & Home HD Starter Kit by D-Link

**\$148.89**

Buy It Now

25 watching

From Bulgaria



Xiao mi Mi Smart Home Kit (Updated Version) Gate way

**5 009,07 py6.** / lot

6 pieces / lot

Free Shipping

★★★★★ (25) | Orders (36)



Broadlink S1C SmartOne Wireless Alarm&Security Kit Detector

**2 408,27 py6.** / Set

Free Shipping

★★★★★ (139) | Orders (180)



2017 New Arrival Broadlink S1/S1C SmartOne Alarm &

**2 408,27 py6.** / piece

Free Shipping

★★★★★ (67) | Orders (103)



2017 New Version Original Xiaomi Smart Home Kit Gateway

**3 439,78 py6.** / piece

Free Shipping

★★★★★ (87) | Orders (114)



2016 Xiaomi mijia Gate-way+Door /Window,Temperature

**584,27 - 1 791,42 py6.** / piece

Free Shipping

★★★★★ (16) | Orders (55)



Free Shipping RU Broadlink Smart Home Kit With S1C Kit,

**9 036,13 py6.** / piece

Free Shipping

Orders (0)



Broadlink S1C Smart Home Kit 433MHZ S1 Smartone Door

**2 573,05 py6.** / piece

Free Shipping

★★★★★ (12) | Orders (11)



DIY Home alarm kit ZigBee smart home kit of ZigBee hub+Smoke

**13 761,51 py6.** / Set

Shipping: 589,09 py6. / lot via Russia Express-SPSR

Order (1)



К нам на тестирование попало несколько комплектов «умных» домов крупных телекомов

- Хаб
- Набор беспроводных датчиков, использующих популярную технологию
- Камера

Что забыл разработчик?

```
# iptables -L
```

```
reject    tcp  --  anywhere
```

```
anywhere
```

```
tcp dpt:ssh /* Close-SSH */
```

Что забыл разработчик?

```
# iptables -L
```

```
reject tcp -- anywhere
```

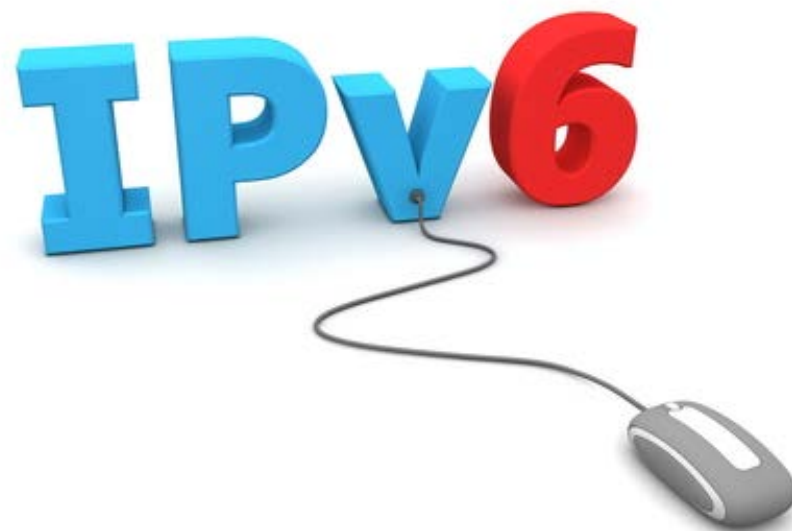
```
anywhere
```

```
tcp dpt:ssh /* Close-SSH */
```

```
ifconfig
```

```
fe80::295:69ff:feaa:e4f6/64 Scope:Link
```

IP6TABLES



Что забыл разработчик?

```
/system/bin/iptables -A INPUT -i eth0 -p tcp --destination-port 80 -j DROP
```

```
/system/bin/iptables -A INPUT -i eth0 -p tcp --destination-port 8080 -j DROP
```



## Что забыл разработчик?

```
/system/bin/iptables -A INPUT -i eth0 -p tcp --destination-port 80 -j DROP
```

```
/system/bin/iptables -A INPUT -i eth0 -p tcp --destination-port 8080 -j DROP
```

```
netcfg
ccmni2    DOWN          0.0.0.0/0
ccmni1    DOWN          0.0.0.0/0
ccmni0    UP            10.210.252.225/8
sit0      DOWN          0.0.0.0/0
ifb1      DOWN          0.0.0.0/0
ifb0      DOWN          0.0.0.0/0
eth0      UP            192.168.100.141/24
ap0       UP            192.168.43.1/24
lo        UP            127.0.0.1/8
wlan0     DOWN          0.0.0.0/0
tunl0     DOWN          0.0.0.0/0
ip6tnl0   DOWN          0.0.0.0/0
```



Что забыл разработчик?

```
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack ttl 64
7080/tcp  open  empowerid    syn-ack ttl 64
8080/tcp  open  http-proxy   syn-ack ttl 64
```

ДОСТУП К ИНТЕРФЕЙСУ УПРАВЛЕНИЯ РОУТЕРОМ.

Введите "Имя пользователя" и "Пароль". Настройки по-умолчанию: admin/admin.

Ночной кошмар настоящего  
параноика:  
«умные» камеры



<http://gooosha.ru/wp-content/uploads/2013/02/webcam-choice-2.jpg>

- Злоумышленник может получить доступ к видео- и аудиопотоку камеры
- В некоторых случаях злоумышленник может заставить камеру говорить что угодно
- Китайские производители не стесняются оставлять бэкдоры в камере
- Если не знать от чего именно эта прошивка, может сложиться впечатление, что она от самоходной лазерной турели с автоматическим наведением (количество излишнего функционала зашкаливает)
- Из-за огромного количества некачественного кода в камерах обнаружено множество уязвимостей нулевого дня



<https://www.kb.cert.org/vuls/id/547255>

Vulnerability Note VU#547255

Dahua IP cameras Sonia web interface is vulnerable to stack buffer overflow

Original Release date: 18 Jul 2017 | Last revised: 26 Jul 2017

 Print

 Tweet

 Send

 Share

Overview

Dahua IP camera products using firmware versions prior to V2.400.0000.14.R.20170713 include a version of the Sonia web interface that may be vulnerable to a stack buffer overflow.

Description

CWE-121: Stack-based Buffer Overflow - CVE-2017-3223

Dahua IP camera products include an application known as Sonia (/usr/bin/sonia) that provides the web interface and other services for controlling the IP camera remotely.

Versions of Sonia included in firmware versions prior to DH\_IPC-Consumer-Zi-Themis\_Eng\_P\_V2.408.0000.11.R.20170621 do not validate input data length for the 'password' field of the web interface. A remote, unauthenticated attacker may submit a crafted POST request to the IP camera's Sonia web interface that may lead to out-of-bounds memory operations and loss of availability or remote code execution.

The issue was originally identified by the researcher in firmware version DH\_IPC-HX1X2X-Themis\_EngSpnFrn\_N\_V2.400.0000.30.R.20160803.

Impact

A remote, unauthenticated attacker may submit a crafted POST request to the IP camera's Sonia web interface that may lead to out-of-bounds memory operations and loss of availability or remote code execution.

Solution

Apply update

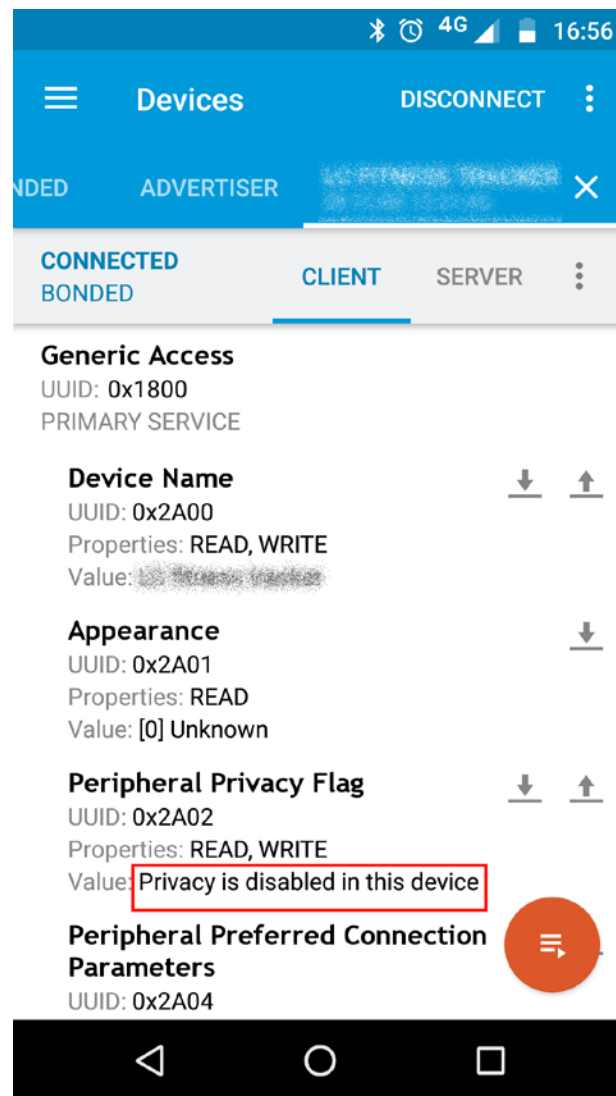
Dahua has released firmware version DH\_IPC-ACK-Themis\_Eng\_P\_V2.400.0000.14.R.20170713.bin to address this issue. All affected users should update their firmware as soon as possible. If you have any questions, you may contact [cybersecurity@dahuatech.com](mailto:cybersecurity@dahuatech.com).

Vendor Information (Learn More)

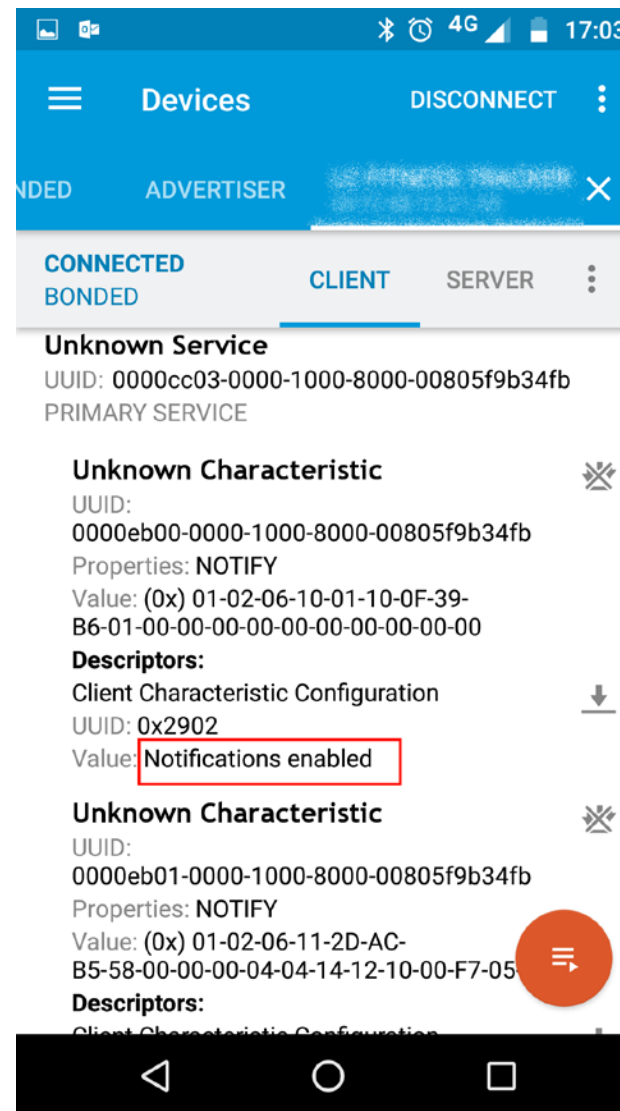
Vendor	Status	Date Notified	Date Updated
Dahua Security	Affected	31 May 2017	17 Jul 2017

Демо

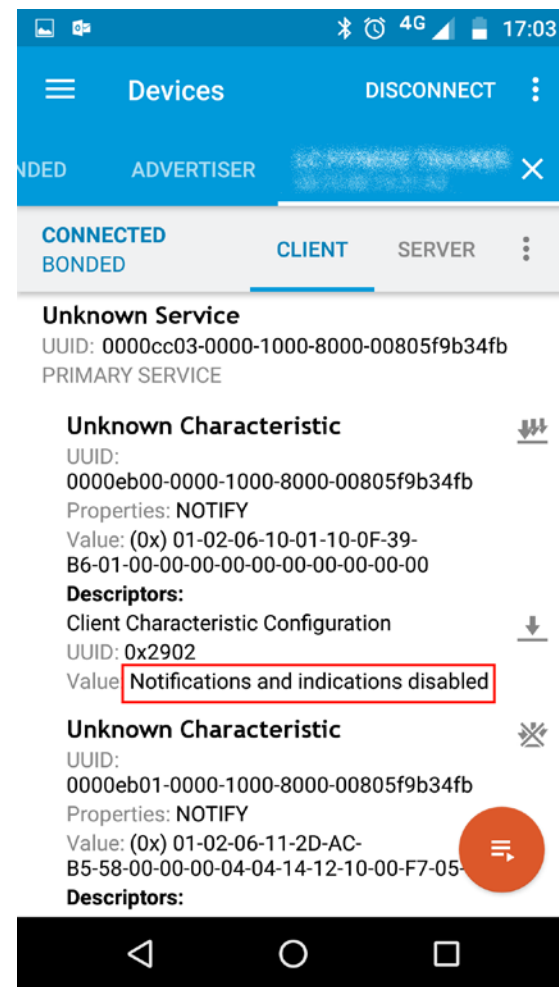
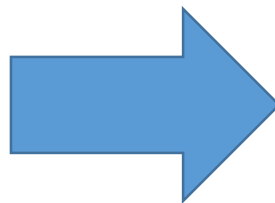
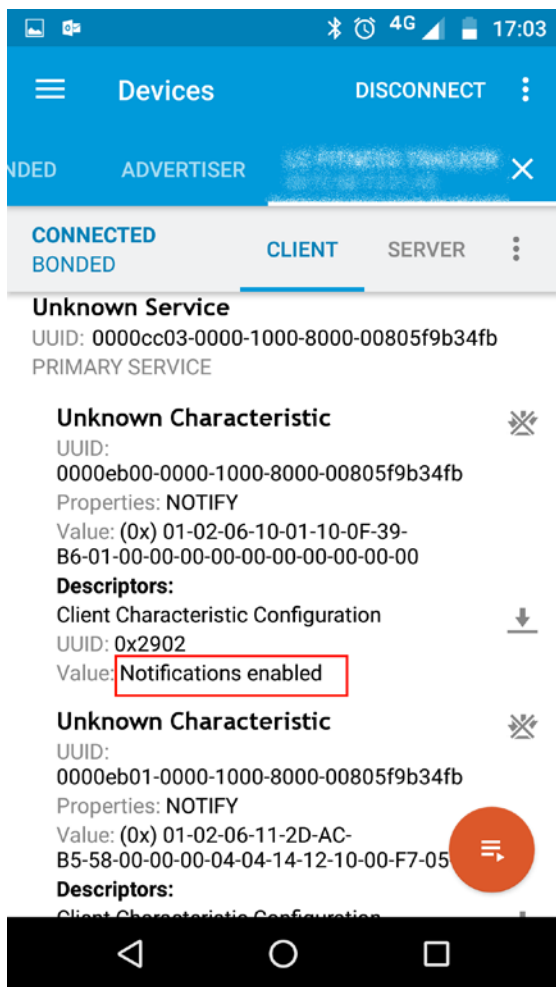
BTLE: авторизация? Не знаю.



BLTE: любой может подключиться  
и украсть ваши данные



## BLTE: любой может подключиться и украсть ваши данные





## Беспроводные датчики? Все не так плохо, но тоже есть проблемы

```
▼ Z-Wave Frame HeaderSinglecast(7) [0xffe20811 1->8]
  Home Id: 0xffe20811
  Source Node Id: 0x01
  0... .... = Routed: False
  .1... .... = ACK Req: True
  ..0. .... = Low Power: False
  ...0 .... = Speed Modified: False
  .... 0001 = Frame Type: Singlecast (1)
  .00. .... = Beam Control: 0
  .... 0111 = Sequence Number: 7
  MPDU Length in Bytes: 20
  Destination Node Id: 0x08
  Checksum: 0x1458
▼ Data (9 bytes)
  Data: 3305030200032d04ff
  [Length: 9]
```

```
33 - Command Class = COMMAND_CLASS_SWITCH_COLOR
05 - Command = SWITCH_COLOR_SET
03 - Color Component Count = 3
02 - Component ID = RED
00 - Red Value = 0
03 - Component ID = GREEN
2d - Green Value = 45
04 - Component ID = BLUE
FF - Blue Value = 255
```

В отличие от мелких неизвестных фирм, а также AliExpress и eBay, телекомы подходят к проблеме серьезно и системно. Все найденные ошибки и уязвимости переданы производителям, часть уже исправлены, и остальные, надеемся, будут исправлены.

У крупных телеком-компаний, долгое время занимающихся различными IT-технологиями, есть значительно больше понимания в области информационной безопасности, чем у компаний, ранее производивших выключатели.

Они на правильном пути, но IoT действительно бросает им вызов и заставляет наступать на старые грабли.





Спасибо за внимание!

POSITIVE TECHNOLOGIES

[ptsecurity.ru](http://ptsecurity.ru)