



Ciberseguridad en dispositivos IoT

Amenazas y soluciones

**Cátedra Economía
de la Ciberseguridad**
USC-INCIBE



Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA



incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Cátedra Economía de la Ciberseguridad

USC-INCIBE

CECOCIB



Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA



SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGÉNCIA ARTIFICIAL



Plan de
Recuperación,
Transformación
y Resiliencia



cecocib.gal

Antonio Vázquez Blanco

Email: antonio.vazquez@tarlogic.com

Mastodon: [@antoniovazquezblanco@mastodon.social](https://mastodon.social/@antoniovazquezblanco)

Twitter: [@antonvblanco](https://twitter.com/antonvblanco)



Índice

- 01 – Introducción**
- 02 – Concienciación y conocimiento**
- 03 – Adecuación**
- 04 – Configuración**
- 05 – Ciberseguridad**
- 06 – Conclusiones**

01

Introducción



¿Qué es IoT?

Cualquier dispositivo “conectado”
capaz de medir y transmitir datos



¿Con cuántos dispositivos IoT interactuamos cada uno de nosotros?

2 dispositivos IoT por persona de media en el mundo

5 dispositivos IoT por persona de media en Europa



Existen 5 dispositivos por
cada persona de media,
capturando y transmitiendo
datos constantemente...

02

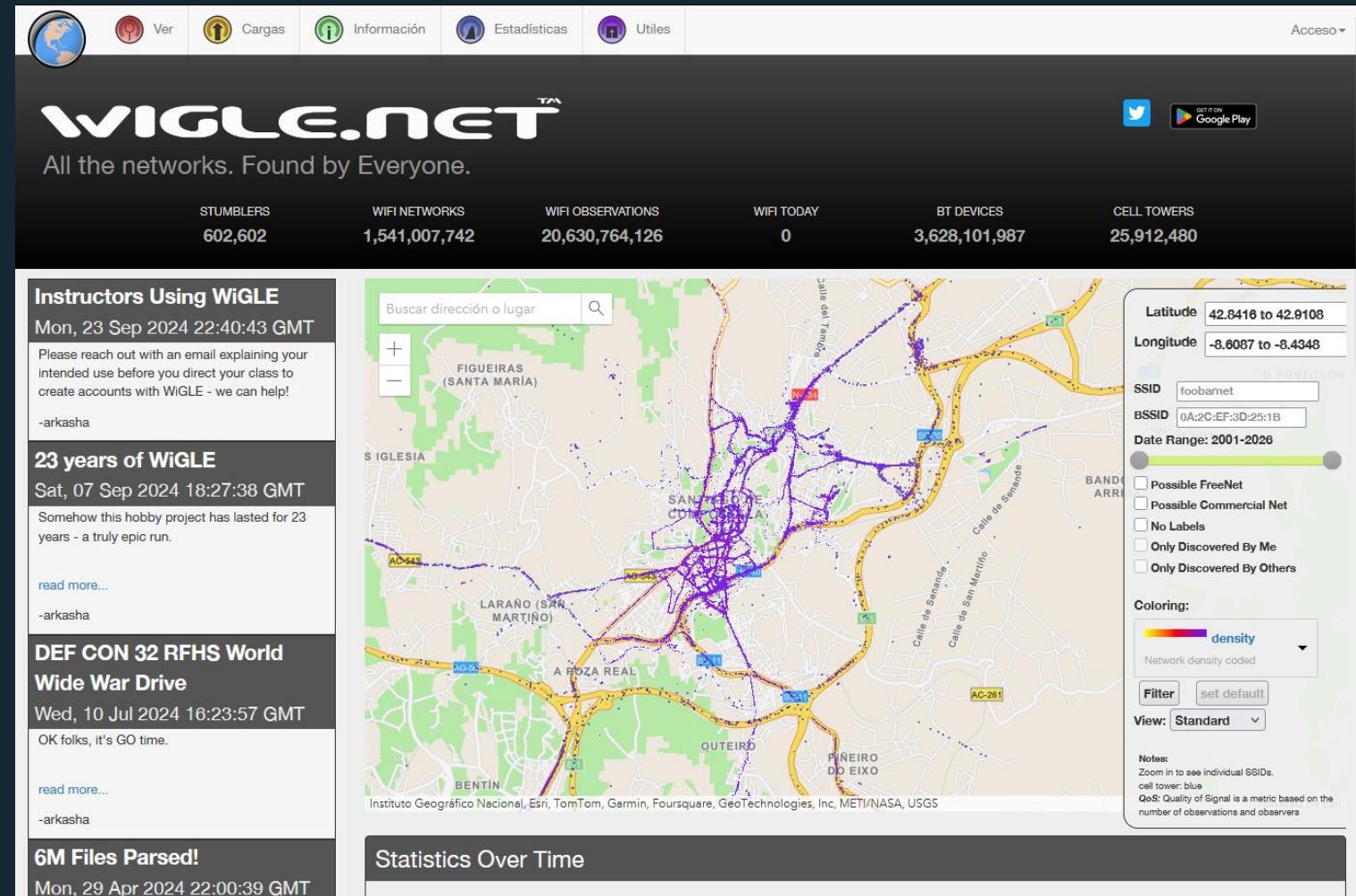
Concienciación y conocimiento



¿Qué datos estamos compartiendo ahora mismo en esta sala?

- Todos llevamos un teléfono encima
- Muchos tendremos el WiFi encendido...

Existen servicios y proyectos como WiGLE que construyen mapas a nivel mundial de ubicaciones de redes Wi-Fi...



Durante el
funcionamiento habitual,
nuestros dispositivos
envían “Probe Requests”
Wi-Fi para consultar si
alguna red conocida está
cerca de nosotros...

CH 1][Elapsed: 6 s][2022-08-15 20:22									
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
D2:69:10:37:F5:94	-28	4	0	0	4	54	WEP	WEP	Home_Network
BSSID STATION PWR Rate Lost Frames Notes Probes									
(not associated)	02:00:00:00:06:00	-49	0 - 1	102	8	StarLucks_Coffee_Free_WiFi			
(not associated)	02:00:00:00:05:00	-49	0 - 1	102	8	HomeAlone			

<https://tbhaxor.com/wifi-traffic-recon-using-aircrack/>



Sin quererlo, estamos
compartiendo los lugares donde
hemos estado o incluso donde
vivimos...



La tecnología IoT ha sido diseñada para ser “sencilla” de usar y adoptar para el usuario...

El IoT está pensado para que nos rodee en todo momento...

En ocasiones, ya no contamos con la opción de usar o no algunos servicios IoT...

Es muy difícil conocer las implicaciones del uso de esta tecnología sin un conocimiento técnico...



Concienciación y conocimiento:

Es difícil conocer las implicaciones del uso de la tecnología IoT sin un conocimiento técnico...

La accesibilidad de la información no es especialmente buena.

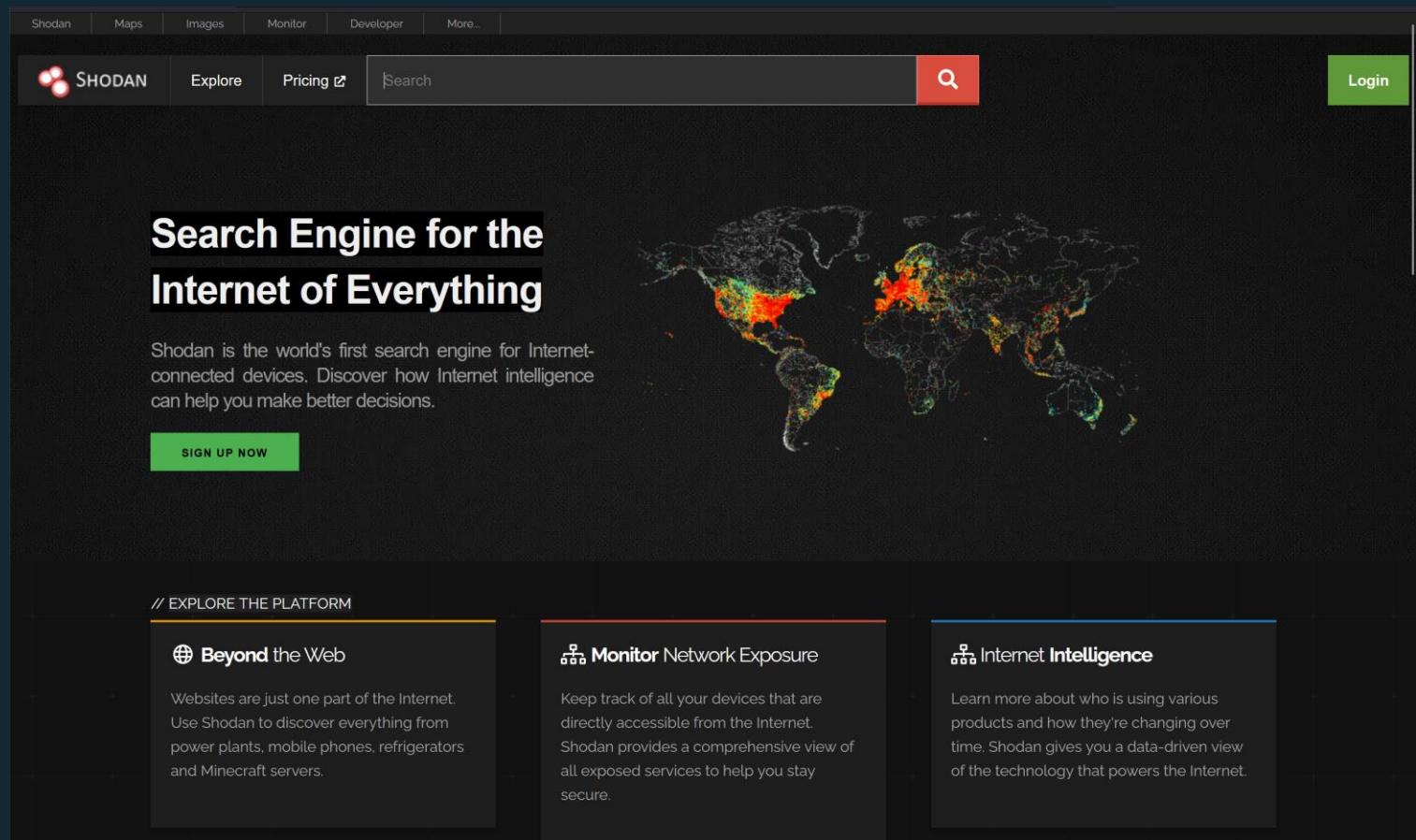
Es muy complicado concienciarnos de los problemas de privacidad hasta que ya han ocurrido.

03

Adecuación

¿Quién conoce el servicio Shodan?

¿En qué se diferencia de otros motores de búsqueda?



The screenshot shows the Shodan homepage with a dark background. At the top, there is a navigation bar with links for Shodan, Maps, Images, Monitor, Developer, and More. Below the navigation bar is a header with the Shodan logo, a search bar containing the placeholder "Search", a red search button with a magnifying glass icon, and a green "Login" button. The main headline reads "Search Engine for the Internet of Everything". Below the headline, a subtext states: "Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions." A green "SIGN UP NOW" button is located below this text. To the right of the headline is a world map where highly connected or exposed devices are represented by colored dots (red, orange, yellow, green), primarily concentrated in North America, Europe, and Asia. Below the main headline, there are three sections under the heading "// EXPLORE THE PLATFORM": "Beyond the Web" (describing Shodan as a search engine for the Internet of Things), "Monitor Network Exposure" (describing the service for tracking device accessibility), and "Internet Intelligence" (describing the platform for analyzing network data).

Una búsqueda rápida da 3.6M de cámaras conectadas a internet...

Shodan | Maps | Images | Monitor | Developer | More... |

SHODAN | Explore | Downloads | Pricing | camera | 🔍

TOTAL RESULTS
3,655,986

TOP COUNTRIES

COUNTRY	RESULTS
United States	513,493
Viet Nam	479,783
Germany	204,884
China	143,230
United Kingdom	140,726
More...	

TOP PORTS

PORT	RESULTS
80	1,111,613
443	503,400
81	296,337
8080	130,533
82	103,636
More...	

TOP ORGANIZATIONS

ORGANIZATION	RESULTS
Viettel Group	249,931
Vietnam Posts and Telecommunications Group	146,592
Deutsche Telekom AG	102,530

View Report | Browse Images | View on Map | Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

301 Moved Permanently 🔗

185.11.152.8
progetti.unicatt.it
centrodibioetica.unicatt.it
tasse.unicatt.it
mariannum.unicatt.it
graduateprograms.unicatt.it
Università Cattolica del Sacro Cuore
Italy, Milan

SSL Certificate

HTTP/1.1 301 Moved Permanently
Date: Tue, 11 Mar 2025 16:34:35 GMT
Server: Apache
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: POST, GET
Vary: Origin
Location: <https://www.un...>

130.164.189.41 🔗

Saudi Telecom Company JSC
Saudi Arabia, Dammam

HTTP/1.1 200 OK
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Content-Type: text/html
X-Content-Type-Options: nosniff
Date: Tue, 11 Mar 2025 19:38:55 GMT
ETag: 1741281656
Content-Length: 481
X-XSS-Protection: 1; mode=block
Last-Modified: Mon, 27 Feb 2023 11:28:22 GMT
Connection: Kee...

50.215.76.110 🔗

Comcast Cable Communications, LLC
United States, Houston

HTTP/1.1 200 OK
Date: Tue, 11 Mar 2025 10:40:16 GMT
Server: Webs
X-Frame-Options: SAMEORIGIN



Muchas son
públicas y se
utilizan para
distintos servicios
públicos...



Otras son públicas y
probablemente no
deberían serlo...



Otras son públicas y
probablemente no
deberían serlo...









Cuando compramos o consumimos tecnología IoT, debemos hacer el ejercicio de si el uso que le damos es adecuado o no...

03

Configuración



¿Quién conoce Strava?

El mapa se trata de Strava Heatmaps, una agregación de todas las actividades deportivas que se suben a la web procedentes de muchos dispositivos IoT como relojes, pulseras, zapatillas, medidores de pulso...



Por defecto Strava opta por subir toda la actividad del usuario a la web sin confirmación...



r/GarminWatches



Search in r/GarminWatches



r/GarminWatches

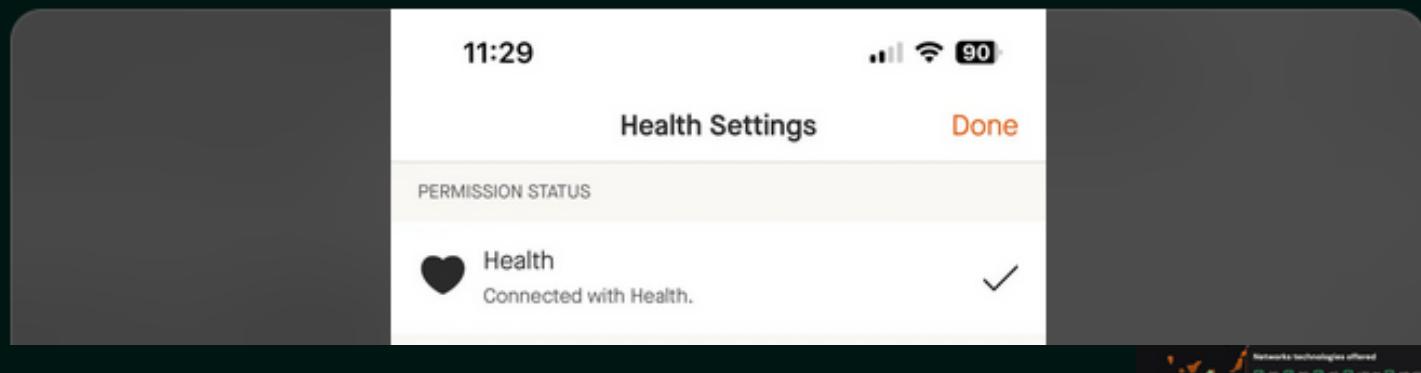
sjfu10

How do I stop automatic uploads to Strava?

Forerunner

I've just switched to a FR965 from an Apple Watch and one thing that's confusing me is how to stop every activity uploading to Strava.

On Apple watch there was a section to view imports and I could select which activities I'd like to upload to Strava (image attached) - is this possible with Garmin?



Add a comment

Sort by: Best

Search Comments

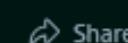
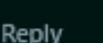


Jekyllhyde • 1y ago

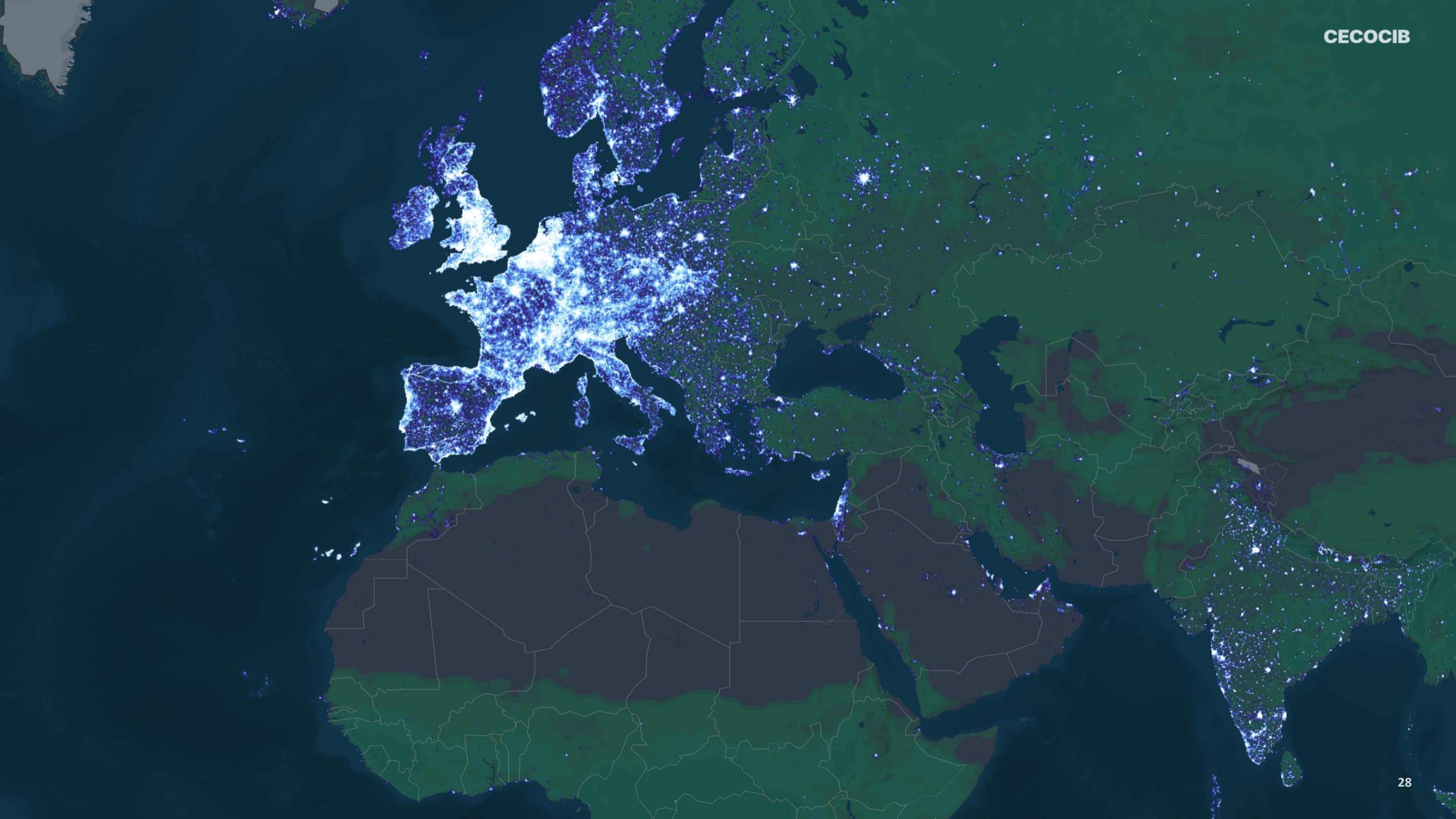
Unfortunately it is all or nothing, however, in Strava, you can set your default activity status to Only You. then no one will see an activity unless you edit it and make it public.

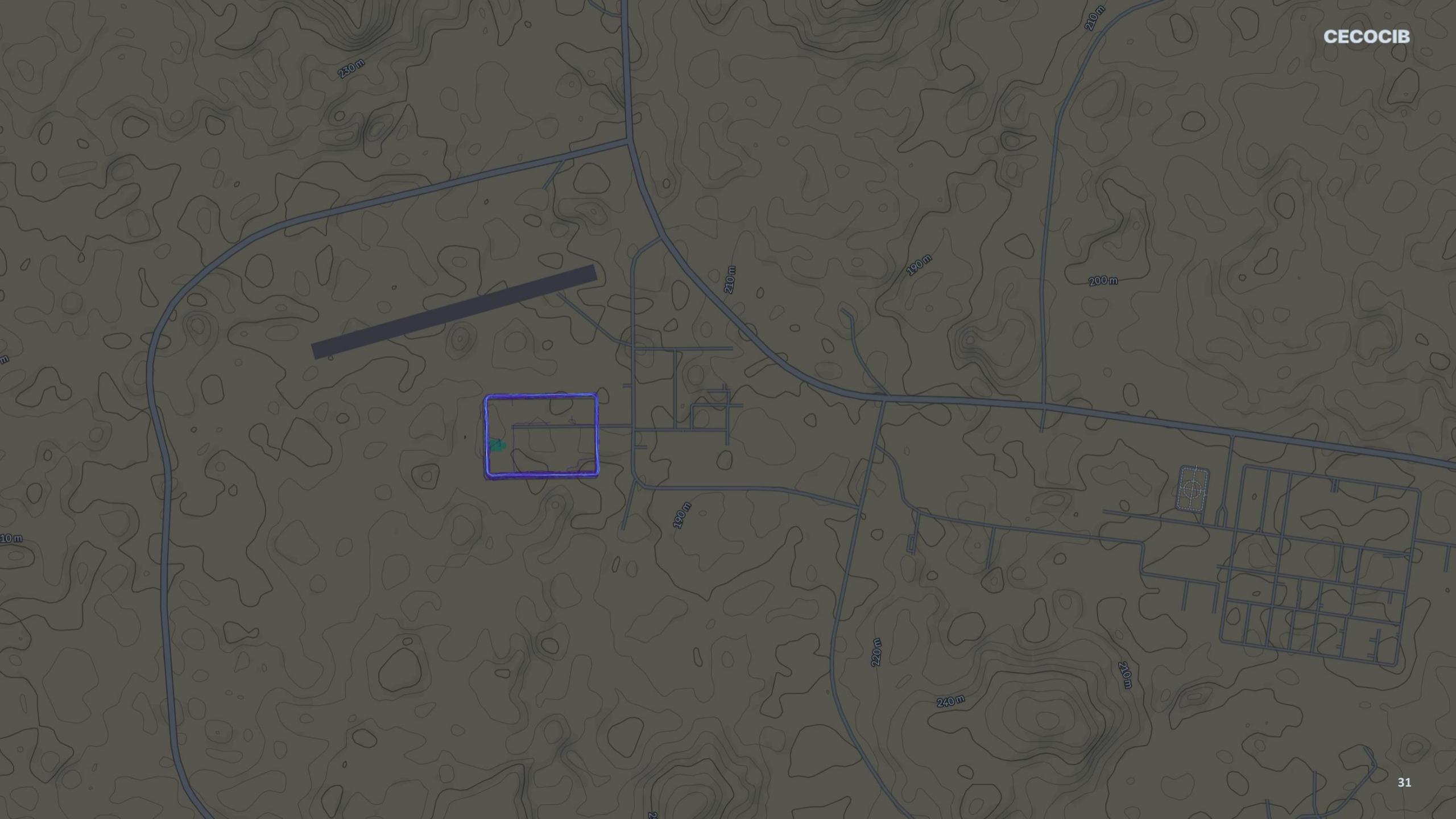


17



...

















El IoT está planteado para ser conectado y funcionar de manera sencilla y sin interacción del usuario...

En ocasiones, para lograr esto, se asumen configuraciones por defecto que no tienen porque adecuarse a las necesidades del usuario...



Cuando compramos o consumimos tecnología IoT, debemos, en la medida de lo posible, configurar adecuadamente los dispositivos para preservar nuestra privacidad...

05

Ciberseguridad



Hasta ahora hemos hablado de aspectos de seguridad que el usuario puede mejorar por si mismo. En la ciberseguridad es necesario que tanto el usuario como el fabricante participen...

Esta interacción, se da principalmente en dos momentos en la vida útil del dispositivo: Durante la compra del dispositivo y durante el ciclo de vida de este...

Durante la compra, debemos valorar factores más allá del precio, ya que, si buscamos productos muy baratos, serán baratos también en cuanto a seguridad...

Durante la vida del producto debemos hacer un esfuerzo por mantener el producto seguro: Actualizar el producto, cambiar contraseñas de manera periódica...





European Commission

Shaping Europe's digital future

Home Policies Activities News Library Funding Calendar Consultations AI Office

Home > Policies > Cybersecurity > Cybersecurity Policies > Cyber Resilience Act

Cyber Resilience Act

The Cyber Resilience Act enhances cybersecurity standards of products that contain a digital component, requiring manufacturers and retailers to ensure cybersecurity throughout the lifecycle of their products.

From baby-monitors to smart-watches, products and software that contain a digital component are omnipresent in our daily lives. Less apparent to many users is the security risk such products and software may present.

The [Cyber Resilience Act \(CRA\)](#) aims to safeguard consumers and businesses buying software or hardware products with a digital component. The Cyber Resilience Act addresses the inadequate level of cybersecurity in many products, and the lack of timely security updates for products and software. It also tackles the challenges consumers and businesses currently face when trying to determine which products are cybersecure and in setting them up securely. The new requirements will make it easier to take cybersecurity into account when selecting and using products that contain digital elements. It will be more straightforward to identify hardware and software products with the proper cybersecurity features.

⊕ EN

 Search

 Share

Quick links

[Cyber Resilience Act](#)

[Questions and Answers - Cyber Resilience Act](#)

[Factsheet - Cyber Resilience Act](#)

[Impact Assessment - Cyber Resilience Act](#)



- Que los dispositivos no usen contraseñas por defecto
- Que haya un ciclo de mantenimiento mínimo
- Que existan medios de actualización que avisen al usuario
- Que exista un programa de respuesta a incidentes
- Que los dispositivos pasen al menos una auditoría de seguridad antes de salir a mercado



Cámaras AVTech y routers Huawei, efectados por la botnet Mirai

Por V. Garcia / 22 enero, 2025

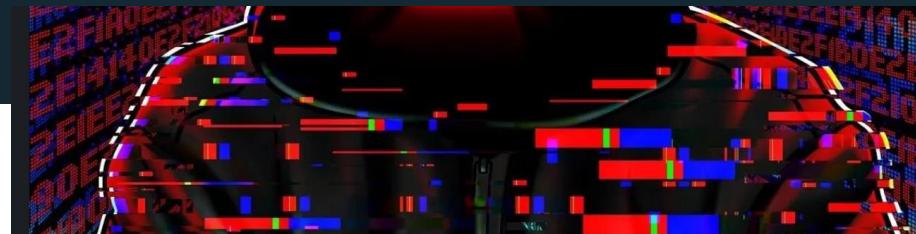
El malware Mirai, descubierto por primera vez en 2016, ha sido una amenaza persistente en el ámbito de la ciberseguridad. Es convirtiéndolos en bots controlados a denegación de servicio distribuido (DDoS).

Expertos en ciberseguridad nueva operación de ataque contra webcams y routers

CIBERSEGURIDAD MARIO BORDONABA | NOTICIA | 25.01.2025 - 07:40H



Esta botnet continua activa pese a los esfuerzos de las fuerzas de seguridad por desmantelarla, ya que está mostrando una gran resistencia.



La nueva botnet Gorilla lanza más de 300.000 ataques DDoS en 100 países.



Ethical Hacking Consultores
19,062 followers



October 7, 2024

Los investigadores de ciberseguridad han descubierto una nueva familia de malware de botnet llamada Gorilla (también conocido como GorillaBot) que es una variante del código fuente filtrado de la botnet Mirai.

La empresa de ciberseguridad NSFOCUS, que identificó la actividad el mes pasado, dijo que la botnet «emitió más de 300.000 comandos de ataque, con una densidad de ataque impactante» entre el 4 y el 27 de septiembre de 2024. No menos de 20.000 comandos diseñados para lanzar ataques distribuidos de denegación de servicio (DDoS) se han emitido desde la botnet todos los días en promedio.

Se dice que la botnet ha atacado a más de 100 países, universidades, sitios web gubernamentales, telecomunicaciones, bancos, juegos y apuestas. China, Estados Unidos, Canadá y Alemania han resultado ser los países más atacados.



Reciclar contraseñas o usar contraseñas por defecto, no actualizar los dispositivos, no protegerlos adecuadamente...

Todo ello puede hacer que se usen nuestros dispositivos IoT contra nosotros mismos...

06

Conclusiones



- Aunque las leyes mejoren progresivamente, como usuarios tenemos un deber muy importante
- Debemos concienciarnos de que el uso del IoT no es gratuito y conlleva una responsabilidad
- Aunque pensemos que no exponemos mucho sobre nosotros, existe mucha información online que puede ser agregada, por ello debemos ser precavidos
- Aun cuando no exponemos nuestra información, los dispositivos pueden usarse de manera maligna



Todos debemos involucrarnos e involucrar a aquellos que nos rodean, especialmente aquellos más vulnerables o que no tienen un acceso fácil a la información...



Cátedra Economía de la Ciberseguridad

USC-INCIBE

CECOCIB

Facultade de CC. Económicas e Empresariais
Universidade de Santiago de Compostela

Avda. de Castelao, s/n
15782 Santiago de Compostela

catedra.ciberseguridad@usc.es
+34 881811532



Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA



SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGÉNCIA ARTIFICIAL



Plan de
Recuperación,
Transformación
y Resiliencia



INSTITUTO NACIONAL DE CIBERSEGURIDAD

cecocib.gal