

# Informe de Análisis de Seguridad con Shodan

**Asunto:** Exploración y Análisis de Cámaras de Seguridad Expuestas en Internet

**Fecha:** 3 de Agosto de 2025

**Analista:** Giampiero Castillo

---

## Índice

- 1. Introducción y Preparación del Ejercicio**
  - 1.1. Objetivo del Análisis
  - 1.2. Dispositivo Seleccionado
- 2. Fase de Recopilación de Datos (Paso a Paso)**
  - 2.1. Búsqueda Inicial del Producto
  - 2.2. Filtrado Geográfico y por Red
  - 2.3. Identificación de Puertos y Servicios
  - 2.4. Análisis Detallado de un Host Específico
- 3. Análisis de Vulnerabilidades Identificadas**
- 4. Evaluación de Riesgos Asociados**
- 5. Recomendaciones de Seguridad**
- 6. Conclusión**

---

## 1. Introducción y Preparación del Ejercicio

### 1.1. Objetivo del Análisis

El presente informe tiene como objetivo demostrar el uso de la herramienta de inteligencia de fuentes abiertas Shodan para identificar, analizar y evaluar los riesgos de seguridad asociados a dispositivos de Internet de las Cosas (IoT) expuestos públicamente. El análisis se centra en descubrir configuraciones inseguras y proponer medidas correctivas para mitigar las amenazas.

### 1.2. Dispositivo Seleccionado

Para este ejercicio, se ha seleccionado un tipo de dispositivo conocido por su frecuente exposición y vulnerabilidades: las cámaras de seguridad que utilizan el software de servidor "webcamXP". Este software es comúnmente utilizado para la transmisión de video en vivo y a menudo se encuentra mal configurado, sin la autenticación adecuada.

## 2. Fase de Recopilación de Datos (Paso a Paso)

A continuación, se detalla el proceso metodológico seguido en Shodan.io para la recopilación de información.

### 2.1. Búsqueda Inicial del Producto

El primer paso consistió en realizar una búsqueda general para identificar todos los dispositivos que exponen el software "webcamXP". Para ello, se utilizó el filtro <product:>.

## Imagen 1

The screenshot shows the Shodan search interface with the query "product:webcamXP" entered in the search bar. The results page displays a total of 108 findings. Navigation links include "View Report", "Browse Images", "View on Map", and "Advanced Search".

Esta consulta devolvió 108 resultados a nivel global, confirmando que es un producto bastante expuesto. El panel izquierdo de Shodan permitió observar un resumen de los países con más dispositivos, los puertos más comunes (como 8080, 8090 y 80) y las organizaciones (proveedores de internet) que los alojan, como Charter Communications en Estados Unidos o Telefónica en España, lo que da una idea de la distribución de estos dispositivos por proveedor de servicios (Imágenes 1, 2, 3.)

## Imagen 2

The screenshot shows the Shodan search interface with the query "product:webcamXP" entered in the search bar. The results page displays a total of 108 findings. It includes sections for "TOP COUNTRIES" (United States, Germany, Spain, Russian Federation, Hungary) and "TOP PORTS" (8080, 80, 8090, 7777, 8888). A "Product Spotlight" box highlights the "webcamXP 5" device, showing its IP address (69.146.36.55), organization (Charter Communications LLC), location (United States, Butte), and a sample of its HTTP response headers.

TOP COUNTRIES	COUNT
United States	25
Germany	16
Spain	8
Russian Federation	8
Hungary	5
<a href="#">More...</a>	

TOP PORTS	COUNT
8080	31
80	13
8090	10
7777	6
8888	5
<a href="#">More...</a>	

**Product Spotlight: Free, Fast IP Lookups for Open Ports and**

**webcamXP 5**

69.146.36.55  
syn-069-146-036-055.res.spectrum.com  
Charter Communications LLC  
United States, Butte  
iot

HTTP/1.1 200 OK  
Connection: close  
Content-type: text/html; charset=utf-8  
Content-Length: 8104  
Cache-control: no-cache, must-revalidate  
Date: Wed, 30 Jul 2025 14:55:45 GMT  
Expires: Wed, 30 Jul 2025 14:55:45 GMT  
Pragma: no-cache  
Server: webcamXP 5

Imagen 3

TOP ORGANIZATIONS	
<b>Charter Communications Inc</b>	8
<b>Telefonica de Espana SAU</b>	8
<b>EWE-TEL</b>	6
<b>Comcast Cable Communications, Inc.</b>	5
<b>Deutsche Telekom AG</b>	3
<b>More...</b>	
TOP OPERATING SYSTEMS	
<b>Windows</b>	8
<b>Ubuntu</b>	1

## 2.2. Filtrado Geográfico y por Red

Para acotar la búsqueda y analizar un entorno específico, se aplicaron filtros geográficos. Por ejemplo, para encontrar dispositivos en Estados Unidos, se utilizó el filtro <country:>.

Imagen 4

The screenshot shows the Shodan search interface. At the top, there's a search bar with the query "product:webcamXP" and "country:US". Below the search bar, it says "TOTAL RESULTS 30". There are three buttons: "View Report", "Browse Images", and "View on Map". A banner at the bottom reads "Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Ch".

Esta búsqueda redujo significativamente los resultados, permitiendo un análisis más enfocado. De manera similar, se podría usar el filtro <net:> para buscar dentro de un rango de red específico (por ejemplo, <net:"80.58.0.0/16"> si se investiga un ISP concreto: Imagen 5) o el filtro <geo:> con coordenadas para buscar en una ciudad (<geo:"40.41,-3.70"> para Madrid: Imagen 6).

Imagen 5

The screenshot shows the Shodan search interface with the query "net:80.58.0.0/16". The results page displays 7,265 total results. A prominent result is highlighted for the IP address 80.58.163.141, which is identified as a staticip.rima-lde.net device running RTSP/1.0. The result includes a timestamp of 2025-07-31T16:59:15.902426, a CSeq value of 1, and a WWW-Authenticate header. There are also links for "View Report", "Browse Images", and "View on Map".

Imagen 6

The screenshot shows the Shodan search interface with the query "geo:40.41,-3.70". The results page displays 2,650,015 total results. A prominent result is highlighted for the IP address 81.46.223.78, which is identified as a mail.grouperfaier.com device running VCloud4. The result includes a timestamp of 2025-07-31T17:09:01.9893, an SSL certificate section, and a detailed log entry for a failed request to 79.116.76.53.

### 2.3. Identificación de Puertos y Servicios

Se observó que la mayoría de estos dispositivos operan en el puerto 8080. Se puede refinar la búsqueda para encontrar solo aquellos que operan en dicho puerto y que, además, no implementan un servidor web seguro (HTTP en lugar de HTTPS). A continuación algunos ejemplos:

(Imágenes 7, 8,9)

Imagen 7

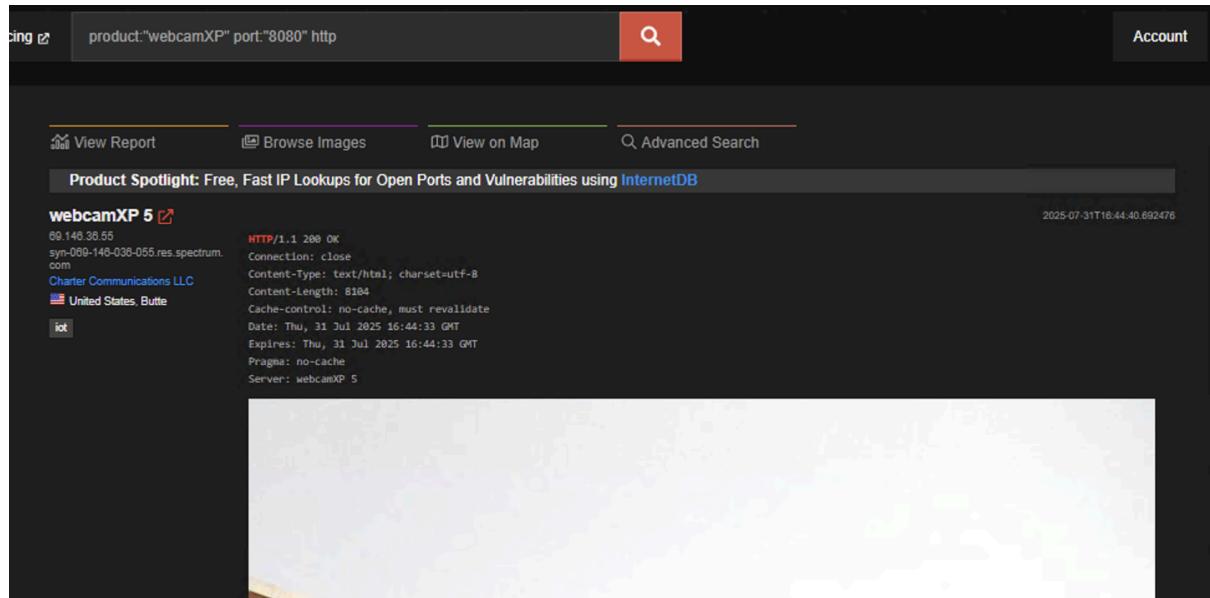


Imagen 8

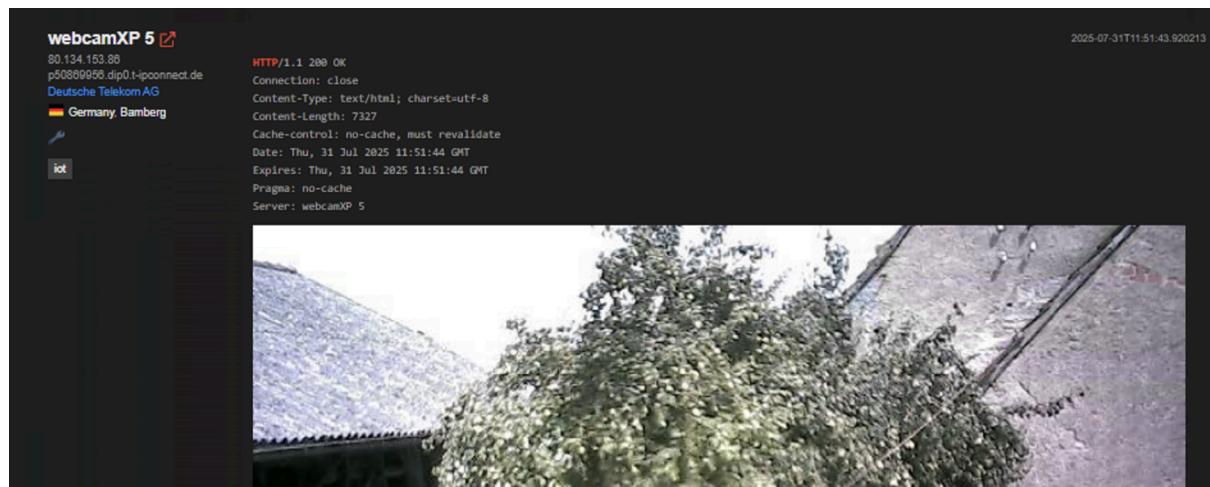
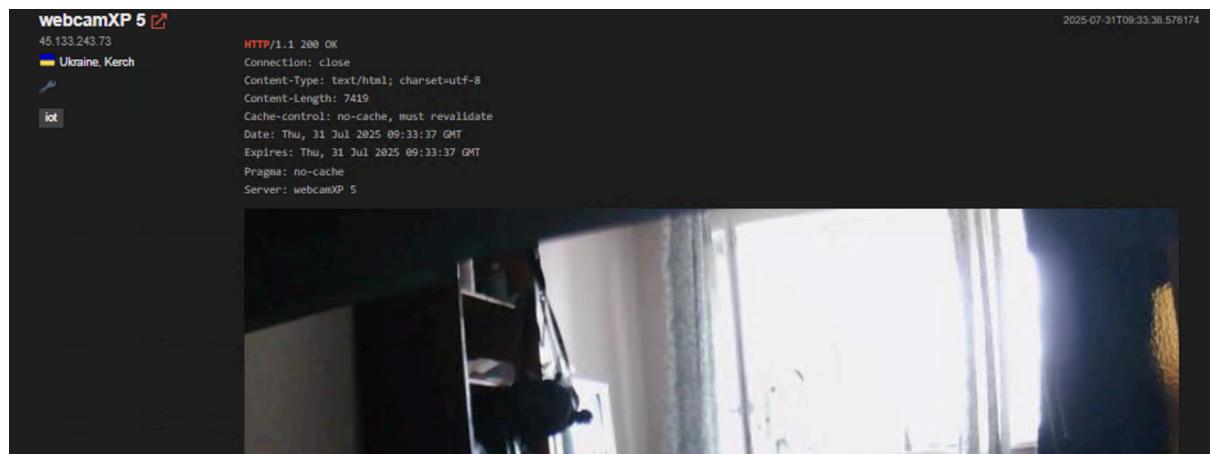


Imagen 9



Esta consulta es útil para identificar sistemas que transmiten datos, incluyendo potenciales credenciales de inicio de sesión, sin cifrado (HTTP y no HTTPS.) El banner de servicio en los resultados de Shodan confirma la versión del software y el servidor (webcamXP 5.) Por ejemplo, el banner de la *Imagen 7*, muestra la siguiente información:

Proveedor de línea (ISP) y *hostname*, en este caso se trata de *Charter Communications LLC* y *syn-069-146-036-055.res.spectrum.com* respectivamente. A su vez, la parte .res indica que el dispositivo se encuentra en una casa (res = residential.)

Por otro lado, se muestra la ubicación del dispositivo. Shodan proporciona la IP exacta (69.146.36.55), de manera que al buscarla en [whatismyipaddress.com](http://whatismyipaddress.com) arroja que se encuentra en una ciudad del estado de Montana llamada *Butte* (*Imagen 10*)

Imagen 10

The screenshot shows the homepage of WhatIsMyIPAddress.com. At the top, there is a search bar with the placeholder "Enter Keywords or IP Address..." and a "Search" button. Below the search bar are navigation links: "MY IP", "IP LOOKUP", "HIDE MY IP", "VPNS ▾", and "TOOLS ▾". The main content area has a dark blue header with the text "IP Details For: 69.146.36.55". To the left of the map, a list of IP details is provided:

Decimal:	1167205431
Hostname:	syn-069-146-036-055.res.spectrum.com
ASN:	33588
ISP:	Charter Communications LLC
Services:	None detected
Country:	United States
State/Region:	Montana
City:	Butte
Latitude:	46.0038 (46° 0' 13.75" N)
Longitude:	-112.5347 (112° 32' 5.05" W)

To the right of the details is a map of Montana with a red marker indicating the location of Butte. Below the map is a red button labeled "CLICK TO CHECK BLACKLIST STATUS". At the bottom of the main content area, a note states: "Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from IP2Location."

## 2.4. Análisis Detallado de un Host Específico

Buscando la dirección IP anterior, se puede realizar un análisis profundo. Al hacer clic en dicha IP, Shodan muestra toda la información que ha recopilado sobre el host. En esta captura (Imagen 11), se pueden identificar:

Imagen 11

The screenshot shows the Shodan search interface for the IP address 69.146.36.55. On the left, under 'General Information', details are provided for the host: Hostnames (syn-069-146-036-055.res.spectrum.com), Domains (spectrum.com), Country (United States), City (Butte), Organization (Charter Communications LLC), ISP (Charter Communications LLC), and ASN (AS33588). On the right, under 'Open Ports', port 8080/TCP is listed, running the service 'webcamXP 5'. The service banner indicates it's version 5, running on HTTP/1.1 200 OK, and includes standard headers like Content-Type, Content-Length, Cache-Control, Date, Expires, Pragma, and Server.

- **Dirección IP:** ip:"69.146.36.55"
- **Sistema Operativo:** Seguramente alguna versión de Windows ya que WebcamXP 5 es una aplicación desarrollada exclusivamente para dicho OS. Esto se puede ver en la Imagen 3 “Top Operating Systems: Windows 8 Ubuntu 1”
- **Hostname:** [syn-069-146-036-055.res.spectrum.com](#) (analizado anteriormente)
- **Puertos Abiertos:** 8080 está expuesto públicamente y entrega una interfaz de administración o video en vivo. Esto podría permitir ver cámaras sin autenticación. Acceder a configuraciones sensibles. Intentos de fuerza bruta contra la interfaz.
- **Servidor:** WebcamXP 5

Esta información detallada es crucial para la posterior evaluación de riesgos.

## 3. Análisis de Vulnerabilidades Identificadas

El análisis de los datos recopilados a través de las consultas anteriores reveló un patrón de vulnerabilidades comunes:

1. **Acceso sin Autenticación:** Un número de cámaras permitían el acceso directo a la transmisión de video sin solicitar usuario ni contraseña. Shodan muestra en la cabecera HTTP respuestas HTTP/1.1 200 OK sin redirección a una página de login.
2. **Software Desactualizado:** Los banners revelaron versiones antiguas de "webcamXP", las cuales son conocidas por tener vulnerabilidades de seguridad que podrían permitir la ejecución remota de código o la toma de control del dispositivo.
3. **Exposición de Información Sensible:** Tomando la dirección IP y buscándola en buscadores como <http://whatismyipaddress.com> (analizado anteriormente) y yendo más allá (usando [maps.google.com](https://maps.google.com)) se puede incluso saber qué tipo de edificio es y dónde se encuentra exactamente.)

4. **Uso de Protocolos Inseguros:** La comunicación a través de HTTP (puertos 80, 8080) en lugar de HTTPS expone cualquier dato de inicio de sesión a ataques de tipo Man-in-the-Middle.

#### 4. Evaluación de Riesgos Asociados

La exposición de estas cámaras con las vulnerabilidades identificadas conlleva riesgos significativos:

- **Intrusión y Espionaje (Riesgo Alto):** El riesgo más evidente es la violación de la privacidad. Actores maliciosos pueden acceder a las transmisiones en vivo para espiar a individuos en sus hogares, empleados en oficinas o para planificar robos físicos al monitorear rutinas.
- **Uso como Punto de Pivot (Riesgo Alto):** Un atacante que toma control de una cámara puede usarla como punto de entrada a la red interna de la organización o del hogar, escalando el ataque para acceder a ordenadores, servidores de archivos u otros dispositivos críticos.
- **Inclusión en Botnets (Riesgo Medio):** Los dispositivos IoT comprometidos son frecuentemente utilizados para formar botnets que luego se emplean para lanzar ataques DDoS a gran escala.
- **Daño Reputacional (Riesgo Medio):** En el caso de una empresa, la noticia de que sus cámaras de seguridad son accesibles públicamente puede causar un grave daño a su reputación y a la confianza de sus clientes.

#### 5. Recomendaciones de Seguridad

Para mitigar los riesgos identificados, se proponen las siguientes recomendaciones de seguridad para los propietarios de estos dispositivos:

1. **Cambiar Credenciales por Defecto:** La primera y más importante medida es cambiar el nombre de usuario y la contraseña que vienen de fábrica por credenciales fuertes y únicas.
2. **Habilitar la autenticación:** Asegurarse de que el acceso a la interfaz web y a la transmisión de video esté siempre protegido por contraseña.
3. **Actualizar el Firmware y Software:** Mantener el software (en este caso "webcamXP") y el firmware de la cámara siempre en su última versión para corregir vulnerabilidades conocidas.
4. **Segmentación de la Red:** Colocar las cámaras y otros dispositivos IoT en una red separada (VLAN) de la red corporativa o doméstica principal. Esto limita la capacidad de un atacante para moverse lateralmente en caso de que un dispositivo sea comprometido.
5. **Configurar un Firewall:** Utilizar un firewall para restringir el acceso a los puertos de la cámara únicamente desde direcciones IP autorizadas. Si no se necesita acceso remoto, bloquear todo el tráfico entrante desde Internet.
6. **Deshabilitar Servicios Innecesarios:** Si la cámara ofrece servicios adicionales como FTP, Telnet o UPnP y no se utilizan, deben ser deshabilitados para reducir la superficie de ataque.

## **6. Conclusión**

El ejercicio demuestra que Shodan es una herramienta extremadamente eficaz para auditar la exposición de dispositivos en Internet. El caso de las cámaras con "webcamXP" ilustra un problema generalizado en el mundo del IoT: la prevalencia de configuraciones por defecto inseguras y la falta de mantenimiento. La seguridad no es un estado, sino un proceso continuo que requiere vigilancia y la aplicación proactiva de buenas prácticas, tanto por parte de los fabricantes como de los usuarios finales.