Impacto de las vulnerabilidades en cámaras IP

Isabel Garcia Padilla, Javier Taberner Nicolas, Roxana Madalina Gogonea

Introducción

La pregunta que ha dado origen a este estudio es saber cuántas cámaras IP (como categoría de cámara digital) están abiertas y pueden ser hackeadas, es decir vulnerables, en todo el mundo. En un principio la idea original era averiguar el número de cámaras que podrían ser objeto de vulnerabilidades, pero restringiéndonos a España. La búsqueda no fue muy productiva ya que no encontramos la cantidad suficiente para que el estudio fuera representativo.

¿Por qué cámaras IP?

Una cámara IP es una cámara que emite las imágenes directamente a internet sin necesidad de un ordenador. Una cámara de red incorpora su propio miniordenador, lo que le permite emitir vídeo por sí misma. Además de comprimir el vídeo y enviarlo, puede tener una gran variedad de funciones:

- Envío de correos electrónicos con imágenes.
- Activación mediante movimiento de la imagen.
- Activación mediante movimiento de sólo una parte de la imagen.
- Activación a través de otros sensores.
- Control remoto para mover la cámara y apuntar a una zona.
- Programación de una secuencia de movimientos en la propia cámara.
- Posibilidad de guardar y emitir los momentos anteriores a un evento.

Las cámaras IP permiten ver en tiempo real qué está pasando en un lugar, aunque esté a miles de kilómetros de distancia. Son cámaras de vídeo de gran calidad que tienen incluido un ordenador a través del que se conectan directamente a Internet.

Características de un cámara IP

1. Grabador de datos
   Hoy en día muchos de los sistemas de videovigilancia o cámaras de seguridad también llevan sistemas de grabación de imágenes automáticos. Se puede acceder desde cualquier dispositivo conectado a Internet.
2. Visión en vivo
   Con las cámaras IP se puede ver qué está pasando en este preciso momento. El usuario se conecta a través de Internet a una dirección IP que tienen sus cámaras, algunos modelos permiten interacción con la ayuda de audio incorporado y las funciones de tomar fotografías y grabar en video lo que está pasando.
3. Microordenador Una cámara IP tiene incorporado un ordenador, pequeño y especializado en ejecutar aplicaciones de red.

Problemas cámaras IP vulnerables

Además de problemas relacionados con la privacidad de los ususarios, las vulnerabilidades en cámaras IP también pueden ser utilizadas para llevar a cabo otro tipo de ataques a partir de botnets creadas con estos dispositivos.

Las cámaras IP son altamente vulnerables ya que gran parte de sus usuarios no dan la importancia que deberían a las configuraciones de seguridad, dejando en muchas ocasiones contraseñas por defecto o directamente sin ningún tipo de protección.

Internet nos ofrece varias maneras de buscar las cámaras que se encuentran accesibles desde cualquier parte del mundo, siendo la más conocida y utilizada Shodan. Este buscador nos permite buscar todo tipo de dispositivos conectado a Internet. Para ofrecer este servicio, Shodan recorre toda la red mandando peticiones a puertos y esperando su respuesta, toda esta información la va almacenando en una base de datos que cualquier usuario puede consultar.

Pero también hay páginas como Insecam que se encargan de hacer las búsquedas por nosotros y nos ofrecen un listado con todas las cámaras accesibles. Visitado esta web, se puede ver que estas cámaras graban todo tipo de lugares: negocios, garajes, carreteras, hoteles e incluso hogares.

Lo más grave de estas webs es que no sólo nos proporcionan la imagen que emiten las cámaras, sino también su ubicación y aquí es donde nuestra seguridad física y no solo intromisión privada que unas imágenes que se emiten al mundo, ya que dicta físicamente donde nos situamos. Este hecho ha generado nuevos problemas, uno de ello siendo el aumento en robos en hogares.

Por otro lado, hay que destacar que año tras año el número de cámaras de videovigilancia se ha visto aumentado no sólo a nivel mundial sino también a nivel estatal. Este hecho multiplica los problemas de privacidad con los que tienen que lidiar instituciones como la AEPD.

Idea inicial

La pregunta inicial constaba en determinar qué cámaras de las que hay abiertas públicamente, no cumplían con la ley de protección de datos. Para ello, la idea era utilizar la información devuelta por la API de Shodan. Esta devuelve un listado en formato JSON de la información que recoge de cada cámara encontrada. De esta manera, la idea consistía en intentar determinar en cada una de los objetos devueltos, ciertas palabras clave que nos permitiesen determinar si se trataba de una cámara que pudiera mostrar contenido que infringiese la ley de protección de datos.

A lo largo de esta fase se encontraron varios problemas que supusieron un cambio en la pregunta inicial. En primer lugar, al disponer de una cuenta gratuita de Shodan, la utilización de su API para este tipo de usuarios es limitada, permitiendo sólo obtener las 100 primeras búsquedas y no dejando utilizar filtros que permiten afinar más las búsquedas. Por otro lado, en los resultados de las búsquedas, no se nos devolvía información sobre qué podrían estar enfocando las cámaras por lo tanto, la idea inicial de utilizar palabras clave para poder clasificarlas no se podría aplicar. Por otro lado, en un primer instante se pensó acotar el estudio a España pero dado que la información encontrada no representaba un gran volumen de datos, se decidió hacer un estudio a nivel mundial.

Llegados a este punto, decidimos cambiar la pregunta y determinar **qué fabricantes de cámaras son más vulnerables**. Para ello se han tenido que utilizar dos fuentes de datos diferentes:

1. En primer lugar un dataset con la información de los CVEs. Este fichero ya viene preparado para su utilización en R por lo tanto sólo se ha necesitado parsear los datos para que estuviesen en el formato necesario para el estudio.

2. Como en los casos anteriores, la API de Shodan para recoger la información sobre las cámaras IP. Para facilitar su uso, se ha utilizado una librería para R que nos ha permitido obtener directamente un dataset con los resultados de las búsquedas.

Cómo se verá a continuación, a pesar de la gran variedad de fabricantes de cámaras IP, la información obtenida no ha sido la esperada inicialmente.

El primer problema con el que nos encontramos a la hora de recoger los datos necesarios, fue determinar la lista de cámaras de las que haríamos el estudio.

En un primer instante se pensó en extraer toda la información relacionada con cámaras de los CPEs, posteriormente filtrar los CVEs que estuviesen relacionados con vulnerabilidades de cámaras encontradas en los CPEs y por último, con la ayuda de Shodan hacer las búsquedas que nos permitiesen determinar cuántas cámaras se veían afectadas por estos fallos de seguridad. Pero el problema que tuvimos es que, buscando vulnerabilidades, observamos que había información sobre cámaras que no estaban presentes en el fichero de los CPEs, por lo tanto descartamos hacer la búsqueda a partir de los CPEs.

En la siguiente prueba, nos centramos en extraer los CVEs que definiesen una vulnerabilidad relacionada con cámaras IP y una vez obtenida dicha información, buscar cuántas cámaras, junto a sus modelos y versiones, se veían afectadas a nivel mundial por estas vulnerabilidades. Pero a causa de hacer búsquedas muy acotadas, los resultados obtenidos no fueron suficientes para poder sacar ningún tipo de conclusiones. Además al buscar sólo modelos vulnerables, no podíamos determinar que cámaras no eran vulnerables.

En la tercera y última prueba, intentamos hacer búsquedas más genéricas, por fabricantes de cámaras IP y posteriormente extraer información extra de modelos y versiones, a partir de los resultados devueltos por Shodan. De esta manera, analizando los resultados que Shodan devuelve al hacer búsquedas por diferentes modelos de cámaras, se escogieron los siguientes fabricantes: **AXIS, D-Link, TP-Link, Canon, Vivotek y Sony**. El criterio de selección de cámaras se basó en analizar qué resultados de Shodan nos devolvían información extra sobre modelo y versión de cámaras. Esto último fue un problema ya que cada fabricante muestra los datos de sus cámaras de una manera distinta y no todos hacen pública esta información por lo tanto Shodan no la puede indexar.

Esta última prueba se realizó con la idea de poder obtener otras posibles cámaras vulnerables que no se habían encontrado con la prueba anterior, además de incluir modelos que no son vulberables. Para poder obtener dicha información, se tuvieron que seguir los siguientes pasos:

1. Hacer las búsquedas de cada uno de los fabricantes escogidos.

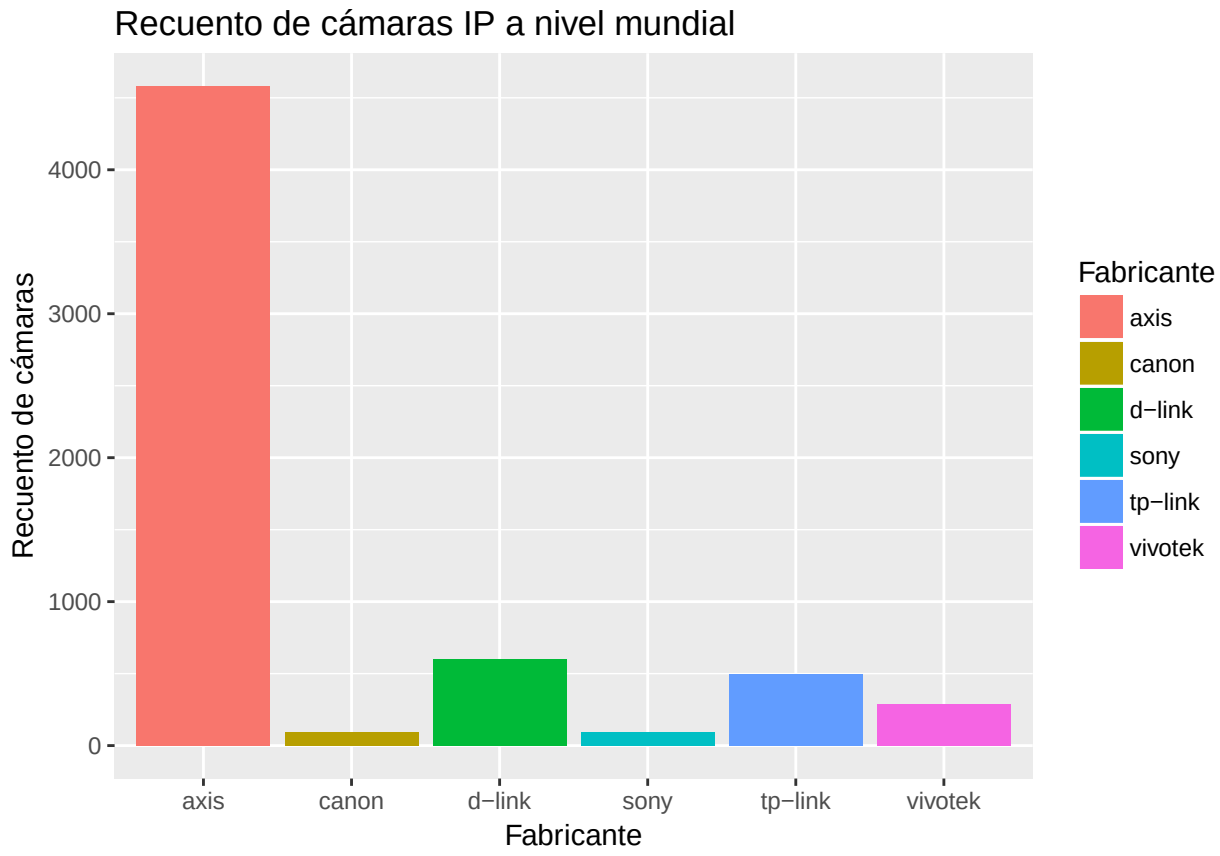
2. Extraer información relevante a partir de los resultados obtenidos, en concreto nos centramos en obtener el modelo y la versión de cada cámara. Como ya se ha mencionado, cada fabricante muestra lo datos de sus cámaras de una manera distinta, por lo tanto este paso resultó más complejo ya que se tuvo que implementar una función de extracción de información diferente para cada fabricante. Por otro lado, tres de los fabricantes buscados no incluyen información del modelo ni versión, acotando aún más el estudio.

Una vez obtenida la lista de cámaras junto a su información técnica, se cruzó con los datos obtenidos de los CVEs. De esta manera se encontraron un total de 183 cámaras vulnerables que como en los casos anteriores, no son suficientes para poder hacer un estudio real de la situación mundial de vulnerabilidades en este tipo de dispositivos. Además como en los casos anteriores, el único fabricante del que se han podido encontrar cámaras vulnerables es AXIS. Esto no quiere decir que los demás fabricantes no lo sean sino que a causa de no disponer de suficientes datos, no se han podido encontrar vulnerabilidades.

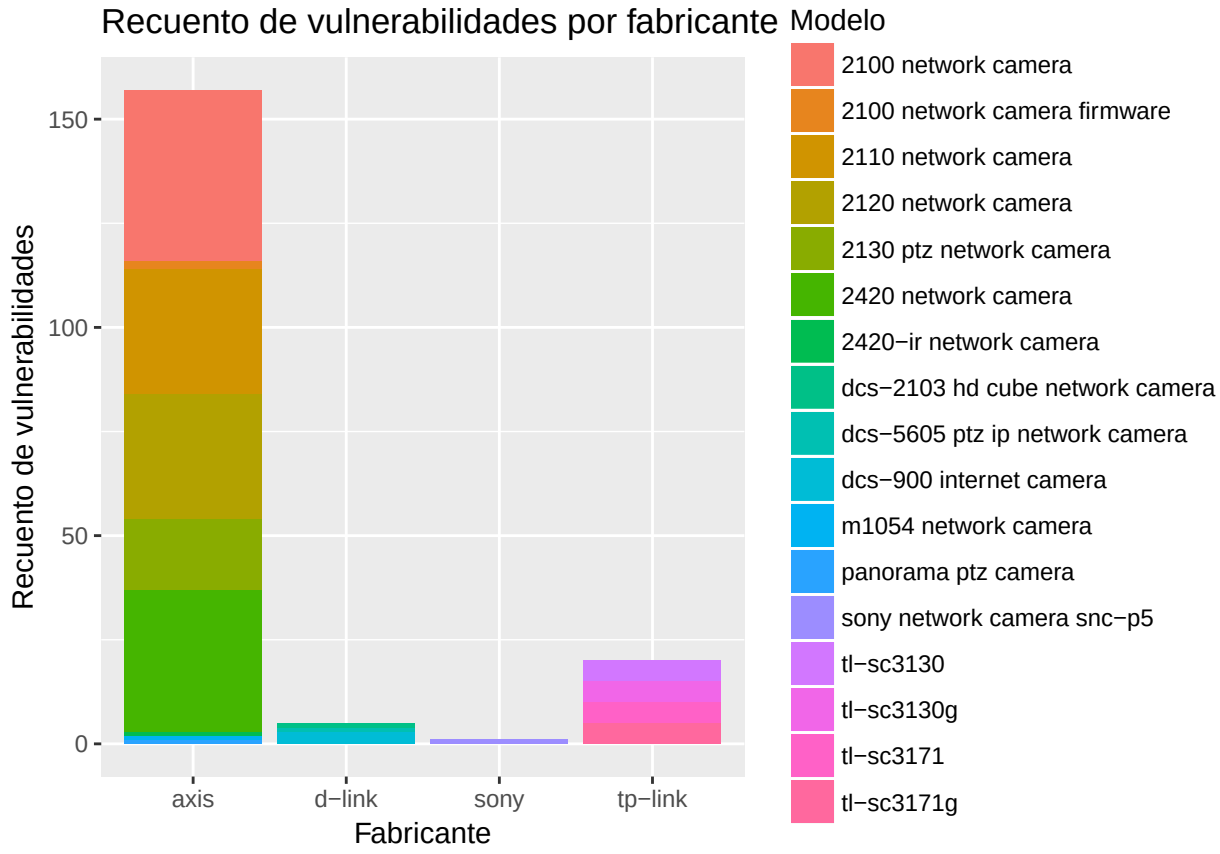
Análisis de resultados

Como se ha adelantado, la información obtenida no es suficiente como para poder realizar un estudio concluyente del estado de las vulnerabilidades presentes en las cámaras IP encontradas a nivel mundial.

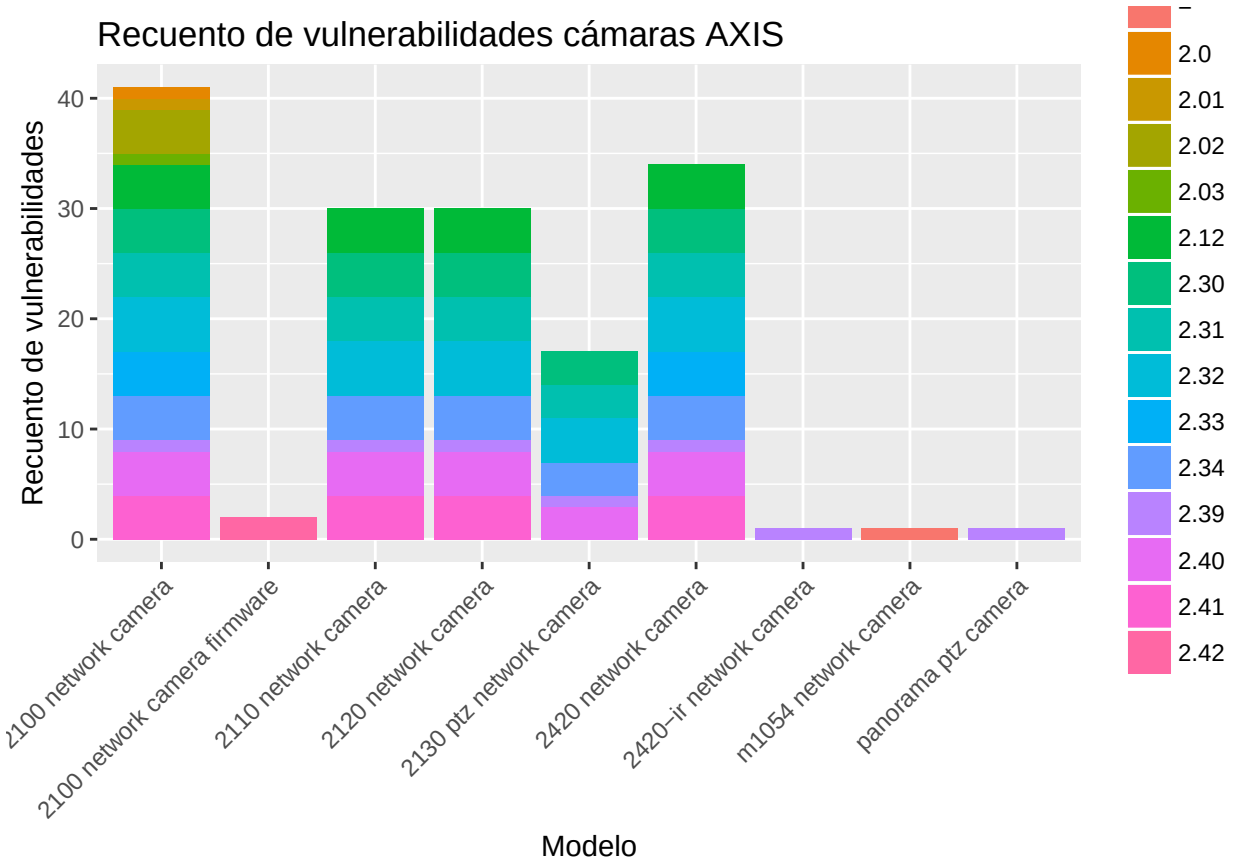
Como podemos observar en la siguiente gráfica, el mayor productor, vendedor de cámaras IP, según la información que hemos podido obtener es AXIS (fabricante sueco de cámaras de red para las industrias de seguridad física y videovigilancia). Su gran expansión se debe ya sea a su precio o a su expansión al mercado del mundo de las cámaras IP de videovigilancia. Esta marca es seguida por D-Link y TP-Link, proveedores no sólo de cámaras IP si no también de otros tipos de equipos de red.



Por otro lado, AXIS, como fabricante más utilizado por los usuarios y siempre con los datos que disponemos, es casualmente la marca con la que más vulnerabilidades presentan sus productos, concretamente 157.



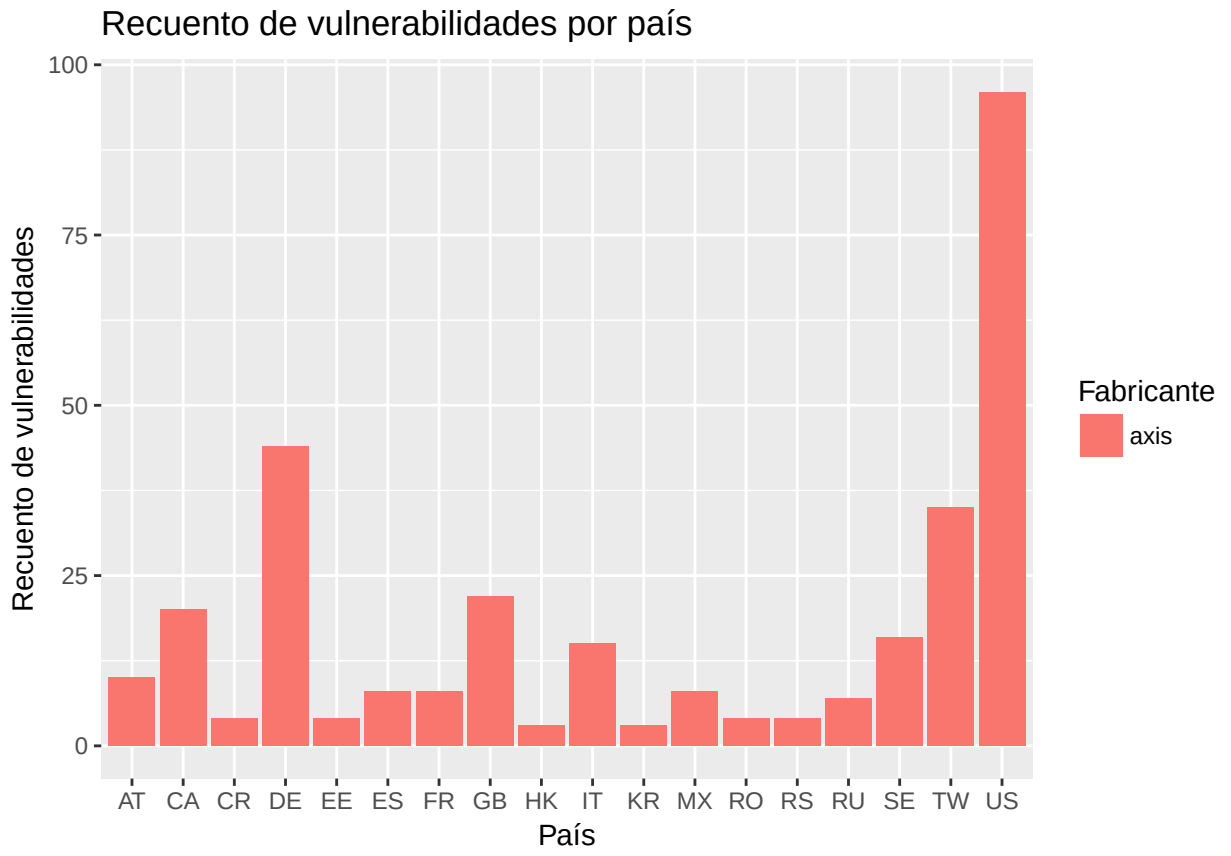
A partir de los datos encontrados, se puede observar que es especialmente vulnerable el modelo AXIS 2100 Network Camera.



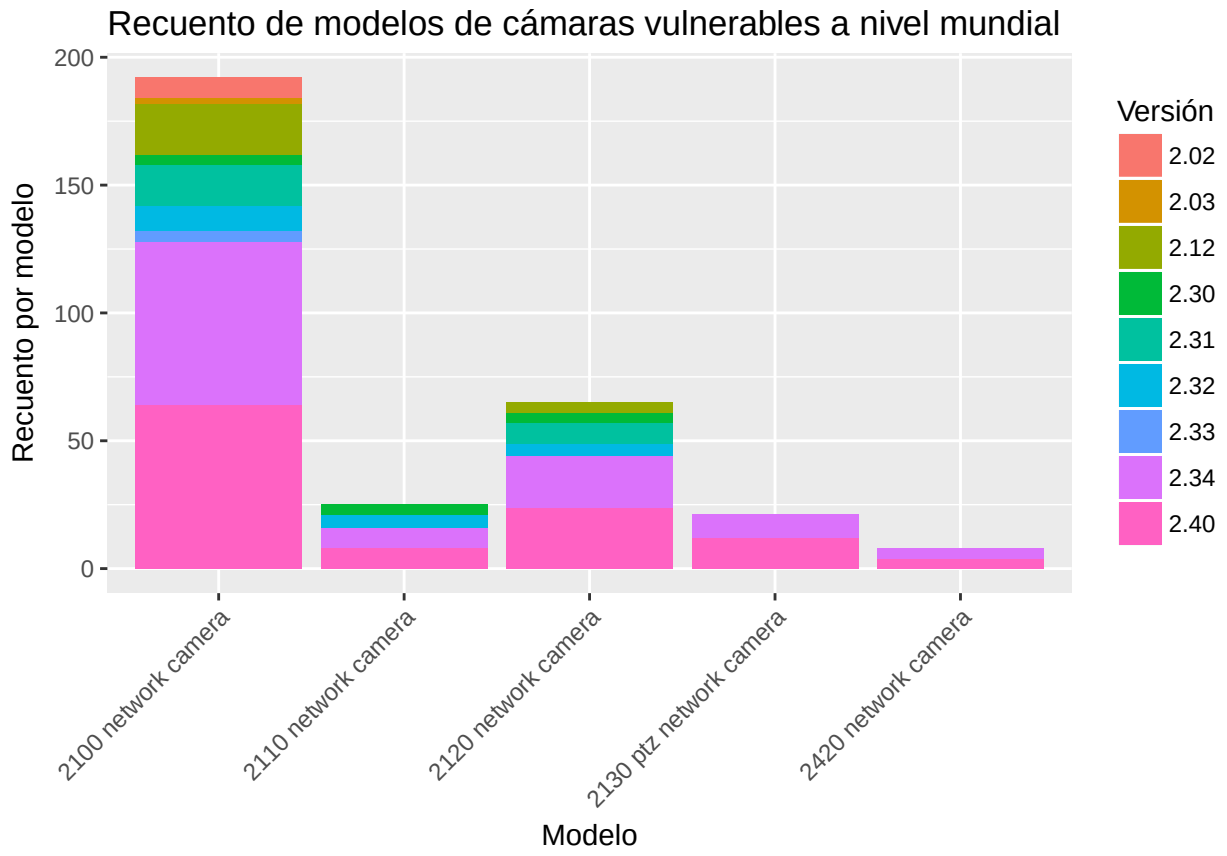
Por otro lado, analizando sus versiones, no se puede determinar ningún patrón relacionado con este dato ya que como se puede observar en la gráfica anterior, las vulnerabilidades están repartidas entre todas las versiones, por lo tanto no se podría decir que una modelo en concreto es más seguro que otro.

Cruzando la información obtenida de los CVEs y con Shodan, tenemos como resultado las vulnerabilidades presentes entre las cámaras encontradas a nivel mundial. A pesar de lo esperado inicialmente y como ya se ha adelantado en el apartado anterior, sólo se han conseguido encontrar cámaras vulnerables AXIS. Esto se debe principalmente a que la información encontrada con Shodan no ha sido lo suficientemente detallada como para poder extraer todos los datos necesarios para realizar el estudio.

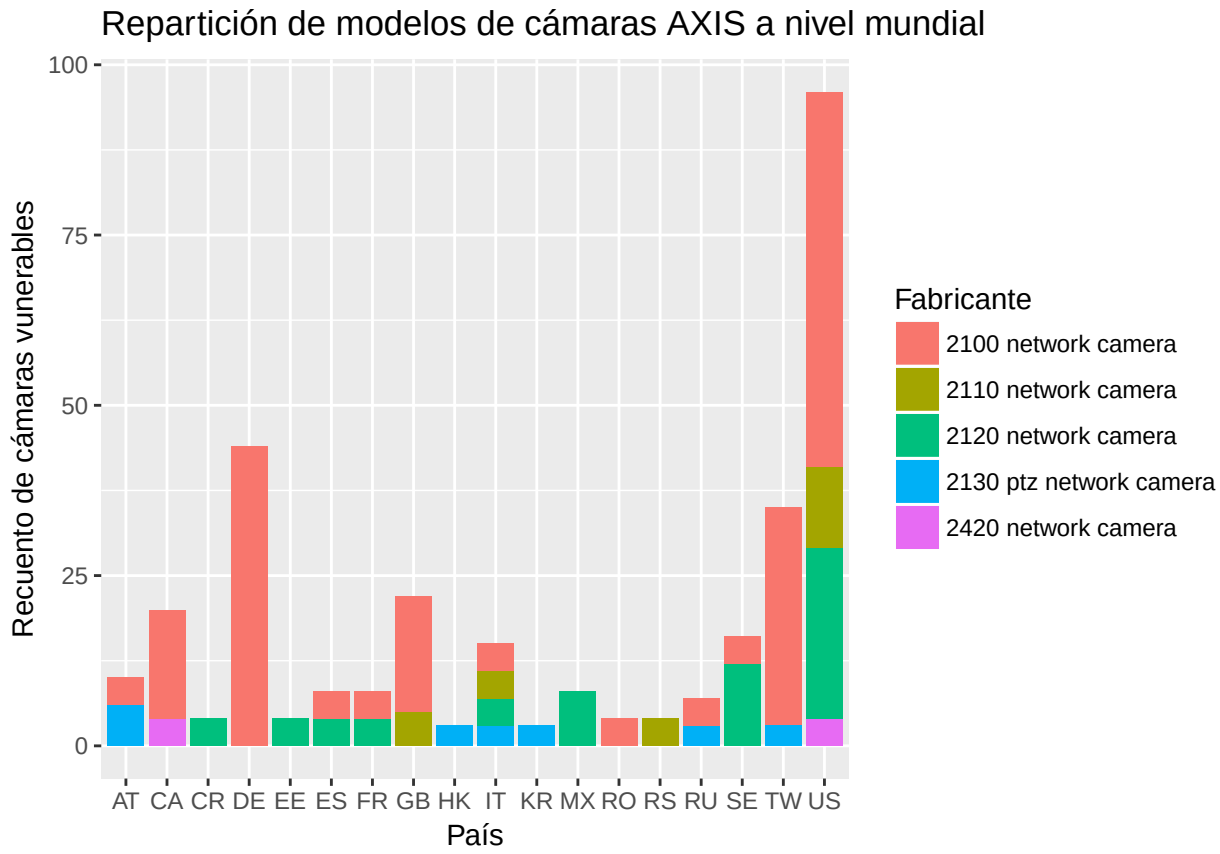
De esta manera, a nivel mundial, se han encontrado un total de 311 cámaras vulnerables, repartidas de la siguiente manera:



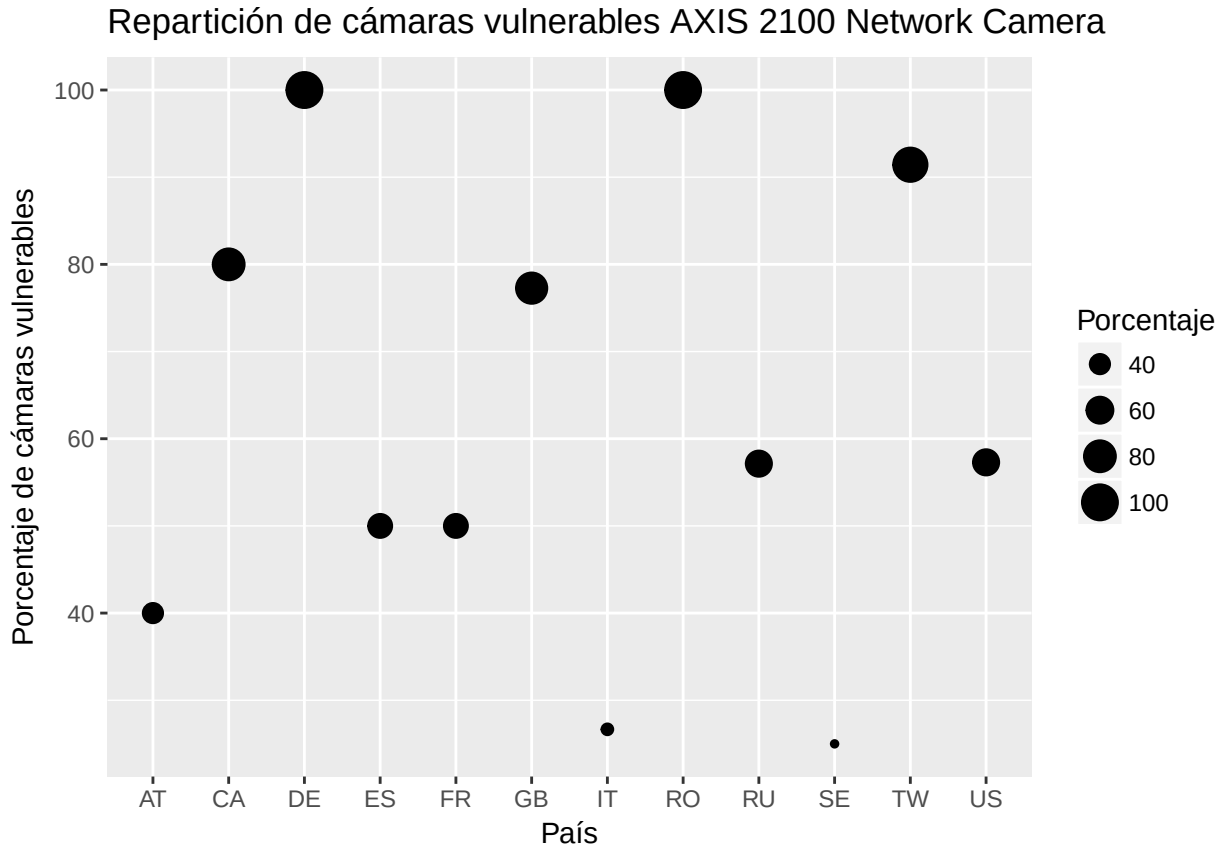
Hay que destacar que, a nivel mundial, no se han encontrado cámaras vulnerables AXIS de todo los modelos si no que, en concreto, sólo 5 presentan problemas de seguridad.



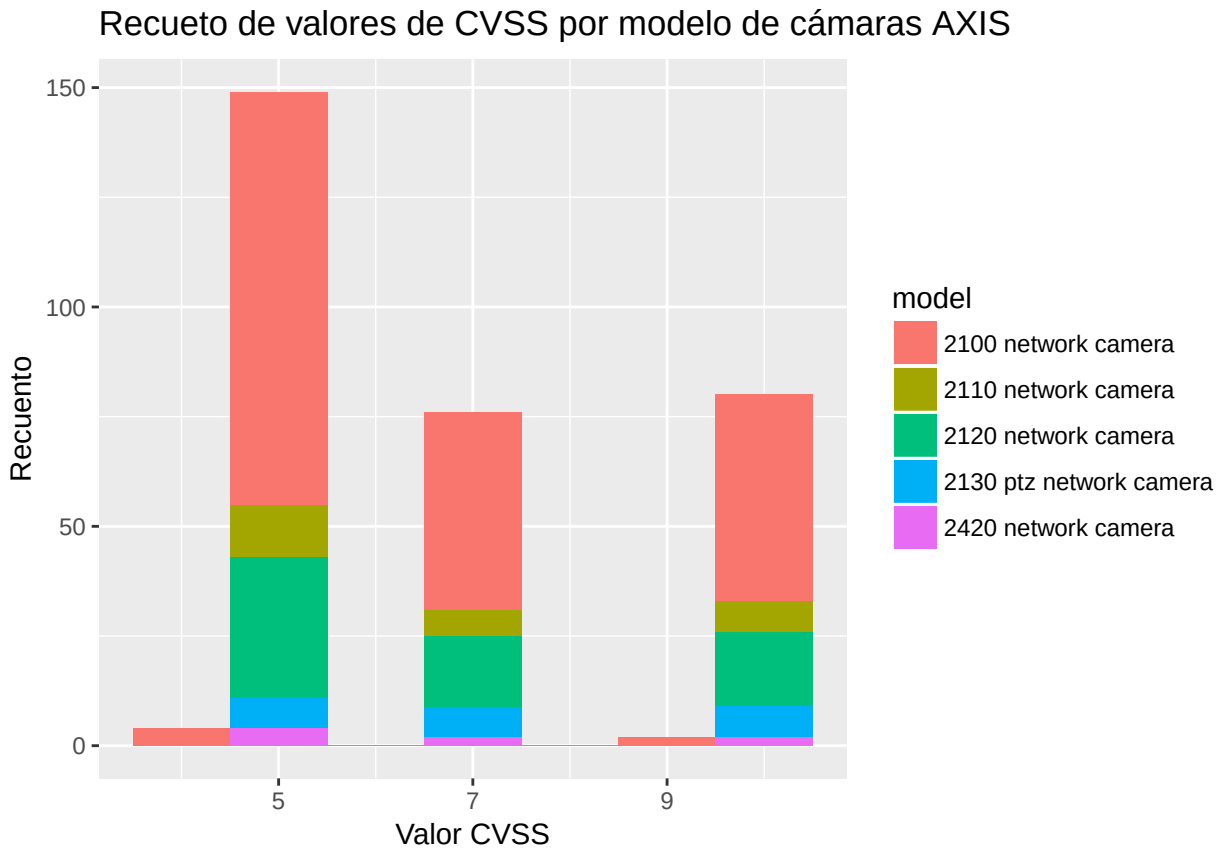
De esta manera, los diferentes modelos vulnerables se reparten de la siguiente forma:



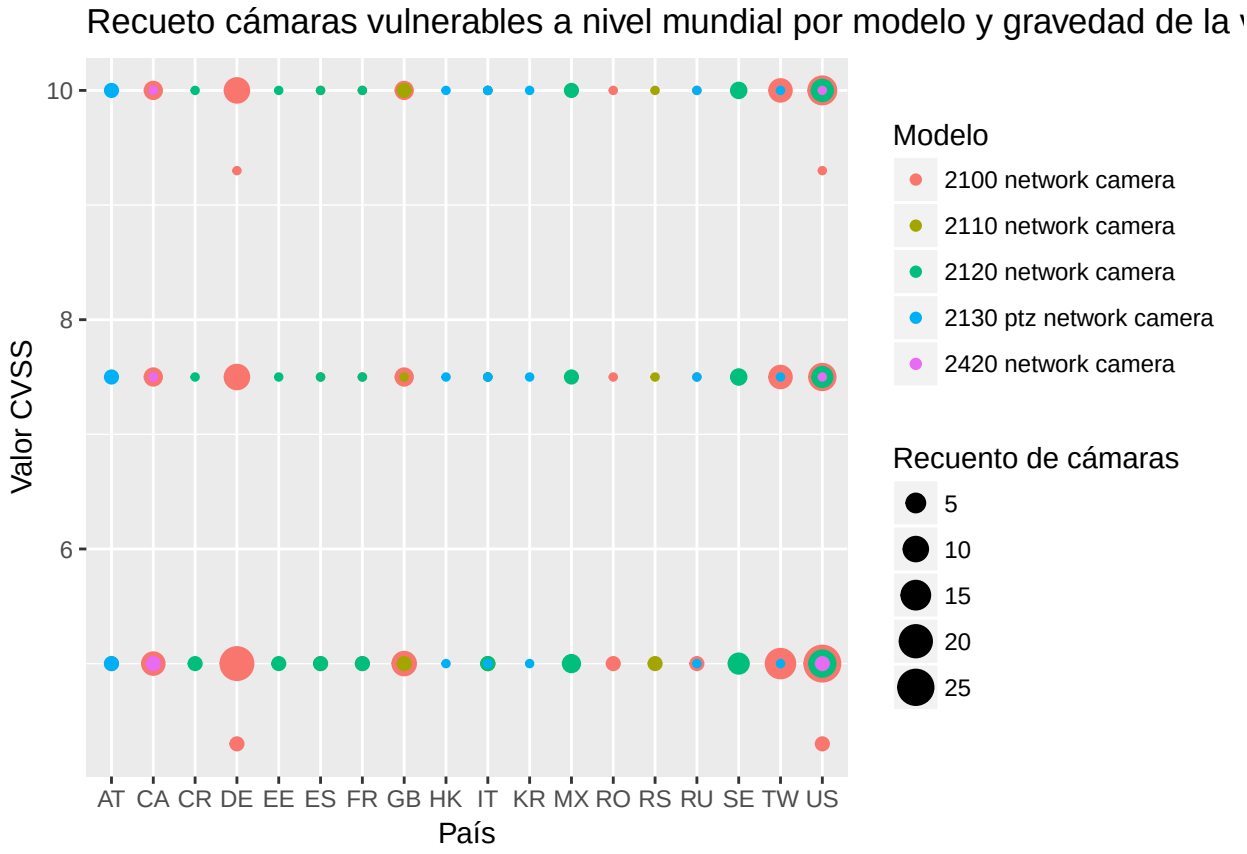
Dada la lista de países que cuentan con cámaras vulnerables AXIS y sabiendo que el modelo 2100 Network Camera es el más vulnerable, podríamos determinar en qué medida los países que cuentan con cámaras AXIS se ven afectados por este modelo.



Pero el número de cámaras vulnerables no es el único dato importante a la hora de analizar cómo de inseguro es un dispositivo si no que hay otro dato, llamado CVSS (Common Vulnerability Scoring System) que nos permite determinar la gravedad de una vulnerabilidad. De esta manera, volviendo a la lista de cámaras vulnerables encontradas a nivel mundial, podemos determinar cómo de grave puede llegar a ser el impacto de éstas.



Como se puede observar, muchas de las cámaras encontradas a nivel mundial, cuentan con problemas de seguridad cuyo impacto puede no llegar a ser representativo mientras que un total de 80 cámaras cuentan con vulnerabilidades cuyo valor de CVSS es máximo. De esta manera, si analizamos cómo se reparten los diferentes modelos de cámaras AXIS vulnerables junto a la gravedad de estas vulnerabilidades obtenemos los siguientes datos:



Conclusiones

En primer lugar, como se ha comentado a lo largo del informe, los datos que se han obtenido no han sido suficientes para realizar un estudio detallado y por lo tanto, no nos han permitido contestar a la pregunta hecha inicialmente. Aún así, cabe destacar el gran problema que está suponiendo la falta de aplicación de medidas de seguridad en este tipo de dispositivos. Éstos van desde la creación de botnets hasta problemas de privacidad que irán siendo cada vez más críticos a causa de un aumento masivo en el número de instalaciones de cámaras IP.

Por lo tanto, los usuarios tienen que estar concienciados de los problemas que este tipo de dispositivos pueden generar y de la importancia de la seguridad para poder evitar ataques informáticos o filtraciones de información no deseada.

Posibles soluciones a las vulnerabilidades de las cámaras IP

La seguridad de los dispositivos IoT no es la mejor. Muchos fabricantes no se toman la seguridad de sus equipos ni la de los usuarios en serio. Por ejemplo, expertos en seguridad han detectado que las cámaras IP presentan una grave vulnerabilidad, permite anular completamente la seguridad SSL que está presente en estos dispositivos, repercutiendo notablemente en la seguridad de la cámara IP y la información ofrecida.

Los fallos de seguridad asociados a dispositivos IoT son muy variados. El mayormente detectado compromete seriamente las comunicaciones del dispositivo. En la actualidad, todos los fabricantes basan las soluciones en dispositivos IoT en sistemas cloud. Es decir, para que el usuario pueda acceder y controlar en este caso la cámara IP, se crean servicios en una nube propia del fabricante, facilitando el acceso de los usuarios a sus dispositivos.

El problema es que para ello es necesario utilizar Internet. Parece bastante fácil obtener información de

comunicaciones que no se envían cifradas. Sin ir más lejos, solo sería necesario un programa como Wireshark y estar conectado si es posible a la misma red que el dispositivo.

Partiendo de que la seguridad de los puntos de acceso Wi-Fi no es a mejor en la mayoría de las situaciones, este segundo punto tampoco sería un problema.

Pero, ¿y si el dispositivo tampoco ofrece garantías en lo que se refiere a seguridad? Como hemos descubierto en los modelos de diferentes cámaras de Axis. Tenemos todos los ingredientes para que se produzca el robo de información.

Expertos en seguridad han detectado que los dispositivos de este fabricante, poseen la clave SSL almacenada en el firmware. Es decir, con un programa similar a Binwalk podríamos obtener este dato. Pero el problema es aún mucho más importante. Tras analizar varios modelos, se ha comprobado que la clave es compartida por todos los modelos de cámaras IP. La obtención de esta información permitiría la realización de ataques MitM y el robo de información aunque esta viaje cifrada, ya que se dispone de la clave de acceso. Es decir, la contraseña SSL contenida en el firmware.

Por qué hay tantas cámaras que disponen de sus propios motores de búsqueda? El problema, en resumen, es que normalmente tanto el usuario como los fabricantes de cámaras priorizan la facilidad de uso por encima de la seguridad del dispositivo. Por eso, las cámaras de vigilancia pueden hackearse fácilmente mediante fuerza bruta.

Sin embargo, hay métodos para minimizar el riesgo:

1. El primero es actualizar de forma regular el firmware y usar contraseñas seguras (además de cambiarlas a menudo). Las instrucciones para llevar a cabo estos pasos suelen estar en la guía de usuario o la página web de soporte del producto.
2. En segundo lugar, se deberían desactivar las características que no se vayan a usar. Esto se aplica en particular a los diferentes servicios de la nube con los que muchas cámaras web están equipadas por defecto.
3. Habilitar el acceso HTTPS a la cámara, pero en ese caso seguramente se ha de utilizar un certificado autoemitido que haría aparecer varias alertas en el navegador.
4. Modificar el router doméstico para aislar la red interna del exterior, permitiendo así un acceso exclusivo a solo algunas funciones seleccionadas del dispositivo.
5. Un dispositivo intermedio de almacenamiento conectado en red. Hasta las cámaras básicas IP cuentan con un software de videovigilancia.

Aspectos a mejorar y trabajos futuros

A lo largo de la realización de este trabajo han surgido varios problemas e ideas que se podrían tener en cuenta para una futura mejora y ampliación del proyecto:

1. El aspecto principal a mejorar es el proceso de obtención de los datos ya que éste ha sido la causa principal de que el resultado obtenido no fuese el esperado. Como se ha comentado, el principal inconveniente ha sido el no disponer de información completa de modelo y versión de los diferentes fabricantes de cámaras IP, impidiendo poder determinar las vulnerabilidades de ciertos fabricantes de cámaras. Por lo tanto, si se encontrase una manera alternativa de obtener la información necesaria, se dispondría de datos suficientes para realizar un estudio detallado de las cámaras más vulnerables a nivel mundial.
2. Para la realización de este proyecto se han escogido un total de 6 modelos de cámaras, pero para que el estudio sea real, se tendría que hacer un análisis de todos los modelos presentes en el mercado o al menos incluyendo todos los fabricantes más populares. Esto se podría llevar a cabo disponiendo de un dataset de CPEs completo ya que como se ha detallado en los apartados anteriores, el que se ha utilizado para este trabajo no estaba completo.

3. Por otro lado, una parte muy interesante a continuar con el estudio sería no sólo ver cuántas vulnerabilidades tienen determinadas marcas sino de qué tipo, pero esta pregunta nos queda limitada a la dificultad que hemos tenido por los medios técnicos utilizados en la búsqueda de datos para el estudio.
4. Como se había pensado inicialmente, otro estudio podría centrarse en determinar qué cámaras infringen la ley de protección de datos, pero para ello se tendría que buscar una manera de analizar qué tipo de información están captando las diferentes cámaras de videovigilancia presentes en la red.