SMART TV: ¿UNA PUERTA TRASERA EN NUESTRO HOGAR?

Autora:
Denise Giusto Bilic
Security Researcher

ESET ENJOY SAFER TECHNOLOGY™

CONTENTIDO

INTRODUCCIÓN

Los televisores inteligentes son parte de la vida cotidiana de millones de usuarios alrededor del mundo. A medida que adquieren mayores funcionalidades, la cantidad y la sensibilidad de los datos que manejan es cada vez más relevante para el mundo del cibercrimen. Cuanto más usuarios adquieren esta tecnología, mayor es el incentivo que encuentran los cibercriminales para diseñar nuevas formas de aventajar la diversidad que el ecosistema de Internet de las Cosas propone en la actualidad.

El hecho de que la mayoría de los televisores inteligentes corran hoy alguna distribución basada en Android implica la conformación de un ambiente donde es más sencillo para los atacantes generar códigos maliciosos capaces de afectar equipos de un diverso abanico de fabricantes, facilitando la transición del malware que actualmente existe para plataformas móviles a sistemas operativos para televisores.

El objetivo de este artículo es resaltar cuáles son las motivaciones de los cibercriminales para comprometer Smart TV, revisar el estado del mercado, destacar los diferentes factores que representan un riesgo para la información de los usuarios que utilicen estos dispositivos y, finalmente, repasar algunos consejos de seguridad para reforzar el sistema operativo y las aplicaciones destinadas a estas plataformas.

EL PANORAMA ACTUAL DE LOS TELEVISORES INTELIGENTES

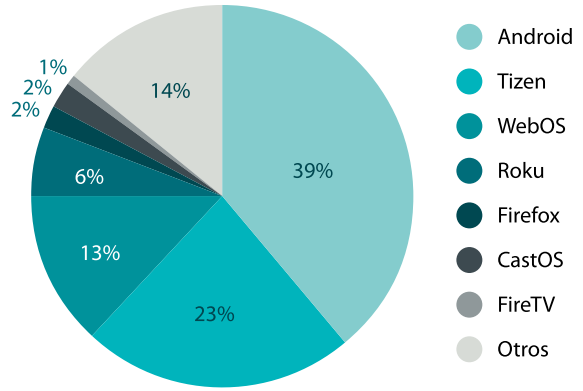
Cada vez son más los dispositivos conectados a Internet. No solo vemos un incremento en las conexiones en automóviles o heladeras, sino también en pequeños dispositivos como sensores de humedad, luces y hasta juguetes. Al igual que sucede con toda tecnología emergente que posea una cantidad cada vez mayor de usuarios, la seguridad es un elemento clave en estos dispositivos, ya que se vuelven un nuevo blanco para los atacantes.

Entre los equipos que han adquirido nuevas funcionalidades en los últimos años, destacan los televisores, que han cambiado su esencia hasta volverse "inteligentes", evolucionado hasta incorporar capacidades similares a los celulares actuales.

Con sus pantallas de alta resolución, cámaras, micrófonos y novedosas interfaces orientadas a la experiencia de usuario, estos televisores ya forman parte de un gran porcentaje de hogares. Tanto así que, según *Statista*, en 2018 *se vendieron más de 114 millones de televisores inteligentes* alrededor del mundo. De acuerdo a una publicación de *IHS Markit*, este volumen *representaría el 70% de todos los televisores vendidos* durante ese año.

Ese mercado se ha convertido un diverso ecosistema de fabricantes de hardware y proveedores de sistemas operativos y aplicativos. Cuando vemos el reporte de *market share* conducido por *IHS Markit*, no debería sorprendernos que Android TV sea actualmente el sistema operativo para televisores inteligentes más popular, incluyendo las implementaciones puras de Android TV y aquellas modificadas por muchos fabricantes chinos. Por su parte, Tizen de Samsung y WebOS de LG ocuparon el segundo y tercer puesto en la lista de sistemas operativos con mayor segmento de mercado.

Gráfico 1 Market Share para televisores inteligentes en 2018



Fuente: *IHS Markit TV Sets Intelligence Service Premium. Disponible en: https://www.broadbandtvnews.com/2018/07/17/smart-tv-share-jumps-to-70-of-tv-shipments*

Ahora bien, aunque el precio de estos equipos se ha vuelto paulatinamente más accesible, algunos recurren a otras tecnologías para acceder a las funcionalidades inteligentes. Así, en la práctica los consumidores pueden optar por dos enfoques suplementarios a la hora de adquirir televisores: ya sea un equipo que venga de fábrica con el sistema operativo inteligente, o bien, un televisor con conectores HDMI, y convertirlo en inteligente conectándolo a un dispositivo externo de streaming. Esta segunda opción, usualmente más económica, provocó la rápida masificación y diversificación de productos de transmisión de video.

Mientras nos adentramos en el 2019, quizás tres de los dispositivos de streaming más conocidos sean Apple TV, Chromecast de Google y Fire TV de Amazon. Sin embargo, más allá de los productos fabricados por compañías confiables y con importante trayectoria, existen otras decenas de modelos que ofrecen funcionalidad similar, conocidos como

"TV boxes" o "streaming boxes". Usualmente, se trata de equipos que corren modificaciones de Android o Android TV y pertenecen a un variado universo de fabricantes, muchos de los que se desconoce el enfoque de gestión de seguridad que manejan o el nivel de seguridad que ofrecen a sus usuarios en cuanto a, entre otras cosas, detección y mitigación de vulnerabilidades.

Imagen 1 Dispositivos de streaming para televisores

Recientemente, se ha sumado un nuevo jugador al mercado de las Android TV boxes: la NVIDIA Shield, que rápidamente se convirtió en el equipo de streaming favorito entre la comunidad de usuarios gracias al respaldo de una marca importante (NVIDIA, compañía reconocida por sus GPU y circuitos integrados) y a las capacidades de sus componentes electrónicos. Compatible con SmartThings, streaming por HDMI y dos puertos USB, la NVIDIA Shield es un Android TV box con características específicamente dirigidas a gamers.

Imagen 2 NVIDIA Shield

Otro actor que gana fuerza dentro de los dispositivos de streaming, y que *ha acrecentado su participación en mercado occidental*, es Roku, que en algunos lugares llega a competir directamente con Chromecast . Esta plataforma construida específicamente para televisores ha acaparado el 20% de los Smart TV en el mercado estadounidense, y no da señales de echarse atrás.

MOTIVACIONES PARA EL ATAQUE A TELEVISORES INTELIGENTES

Los cibercriminales persiguen un claro objetivo con sus campañas maliciosas: la generación de dinero. Es decir, requieren de información capaz de ser vendida, de datos para extorsionar, de equipos para secuestrar o de capacidad de procesamiento para utilizar. Los televisores inteligentes cuentan con todas las características mencionadas anteriormente, lo que los vuelve un blanco atractivo para comprometer. A continuación, se mencionan algunos de los factores que ponen a la nueva generación de televisores en el radar de los atacantes.

Credenciales de acceso

Debido a que los sistemas operativos para televisores inteligentes funcionan con base en sistemas móviles, muchas de las aplicaciones actualmente disponibles para teléfonos pueden también ser accedidas a través de estos dispositivos. Ya sea que se las instale mediante tiendas oficiales o a través de repositorios externos, los juegos, redes sociales, gestores de correo y apps de streaming de programas de televisión son algunas de las opciones que tiene el usuario al momento de configurar su Smart TV.

Las credenciales de acceso a estas cuentas, además de otras como la de Google o iTunes, pueden igualmente ser capturadas por códigos maliciosos o vulnerabilidades que afecten al sistema operativo o las aplicaciones. En la mayor parte de los casos, las credenciales robadas se venden en los mercados negros; otras veces, se utilizan para suplantar la identidad del usuario en otras campañas maliciosas, por ejemplo, para enviar correos adjuntos maliciosos.

Acceso a la cámara y micrófono

La mayor parte de los televisores inteligentes posee micrófonos que les permiten funcionar, entre otras cosas, como asistentes de voz. Además, muchos incluyen cámaras para utilizar aplicaciones de conferencias y juegos. Sin embargo, estos sensores pueden del mismo modo servir a los atacantes, permitiéndoles acceder no solo al sistema de archivos, sino también al entorno físico que rodea al usuario, observando el movimiento en el hogar o grabando conversaciones.

Las vulnerabilidades que permiten a un atacante acceder a la cámara no son una novedad. Allá por 2013, *un fallo en televisores Samsung permitía a los atacantes activar la transferencia de video y sonido*, y registrar todo lo que ocurría en el hogar de sus usuarios. Además de convertir al televisor en un equipo que todo lo ve y todo lo oye, la vulnerabilidad permitía controlar las aplicaciones de redes sociales, publicar información en nombre de los usuarios y acceder a los archivos de sus víctimas.

En 2017, un investigador de seguridad demostró una técnica para *desplegar una señal de radio no autorizada para comprometer a los televisores* conectados a Internet. Una vez comprometido por el atacante, el televisor podía usarse para llevar adelante una lista aparentemente interminable de acciones maliciosas, incluso para espiar al usuario a través del micrófono y la cámara, y para espiar el tráfico de la red.

Además de vulnerabilidades como estas, no debemos dejar de considerar el malware que, a través de exploits o ingeniería social, puede obtener los permisos necesarios para activar estas funcionalidades una vez que se ha instalado en el equipo. Al ganar el control de estos sensores, un atacante puede utilizar la información recolectada para extorsionar a sus víctimas.

Fotos, videos y archivos personales

De igual manera que los teléfonos, los televisores poseen la capacidad de almacenar archivos que pueden ser de valor para el usuario. Fotos, videos, documentos personales y datos de aplicaciones pueden quedar guardados en el sistema de archivos. Estos datos sirven a los cibercriminales para vender la información, cifrarla y pedir un rescate (ransomware) o extorsionar a sus víctimas amenazándolas con su publicación.

Capacidad de procesamiento

La utilización de los procesadores de los dispositivos informáticos es otro factor que resulta atractivo para los cibercriminales. Una tendencia que crece en este sentido es la minería de criptomonedas, que puede lograrse mediante la instalación de malware en el equipo, o a través de scripts que se ejecutan mientras el usuario navega páginas web.

Además de la minería, los atacantes pueden utilizar la capacidad de procesamiento de un equipo para orquestar otros ataques. En 2018, se descubrieron *variantes de la botnet Mirai capaces de comprometer a televisores inteligentes*. Estas variantes peticionaban a los servidores maliciosos un listado de IP, potencialmente para la realización de ataques distribuidos de denegación de servicio (DDoS).

Conexión a otros equipos hogareños

Los televisores vulnerables o comprometidos pueden convertirse en un punto de entrada desde el cual controlar otros dispositivos dentro la misma red. Teléfonos, sensores IoT, asistentes de hogar, computadores y routers suelen estar conectados a los Smart TV mediante una única red Wi-Fi, Bluetooth o ad hoc. Esto posibilita la aparición de escenarios donde un atacante puede espiar el tráfico entre dispositivos, manipular interfaces de control para cambiar configuraciones o robar información, redirigir conexiones a sitios maliciosos o lograr la explotación de vulnerabilidades y la ejecución de código malicioso en otros equipos de la red.

¿CÓMO PUEDE COMPROMETERSE UN SMART TV?

Al momento de comprometer sistemas, los cibercriminales poseen un arsenal de herramientas que pueden utilizar de forma combinada para ejecutar código malicioso en el entorno de la víctima. Acceder a una simple página web, instalar un ejecutable desde repositorios no confiables o simplemente no corroborar la configuración por defecto del equipo son acciones que podrían hacer peligrar la integridad del sistema. A continuación, se explican algunos de los vectores de ataque que utilizan los atacantes para lograr ejecutar su código malicioso en los dispositivos de los usuarios.

Ejecución de códigos maliciosos

La instalación de malware en el televisor suele ser el objetivo de muchas campañas maliciosas, como medio para ganar control del equipo. Sin embargo, para entender la incidencia de los códigos maliciosos en los televisores debemos primero repasar algunas cuestiones de mercado. Después de todo, es *vox populi* que el cibercrimen y las finanzas mantienen un *affaire* desde hace décadas.

Como establecimos anteriormente, Android es el sistema operativo más utilizado por televisores inteligentes. Además, concentra el 88%[1] del mercado de celulares, lo que la convierte en la plataforma móvil más utilizada. Aunque fue originalmente diseñada para teléfonos inteligentes, su dominio hoy se extiende a tabletas televisores, wearables e, incluso, autos.

Android ha experimentado grandes mejoras desde aquellos primeros años en el mercado. Con el pasar del tiempo, ha incorporado más resiliencia hacia exploits, mayor aislamiento entre las aplicaciones instaladas (propiedad denominada *sandboxing*) y reducción de la superficie de ataque al limitar la cantidad de procesos corriendo con permisos de root, y aún más los permisos del usuario. Estas mejoras –y muchas otras que les siguieron–, inicialmente pensadas para teléfonos inteligentes, impactaron positivamente cuando la plataforma comenzó a expandirse a otros dispositivos IoT.

Sin embargo, la principal motivación de los cibercriminales para desarrollar códigos maliciosos es la obtención de rédito económico a través del robo de información sensible, del secuestro de los datos o del dispositivo mediante ransomware, o del minado de criptomonedas. En el mundo del cibercrimen, una mayor cantidad de usuarios significa un número mayor de potenciales víctimas, lo que se traduce en un alto porcentaje de éxito para los ciberdelincuentes, que continúan encontrando formas de comprometer estos equipos.

En este contexto, el malware para equipos con Android continúa complejizándose y diversificándose. Dado que Android y Android TV comparten la misma arquitectura base, exceptuando algunas restricciones mayormente asociadas a la utilización de la interfaz de usuario, gran parte de los códigos maliciosos pensados para celulares son igualmente capaces de funcionar en televisores inteligentes.

En lo que a Android respecta, la tasa de detección de nuevos tipos de códigos maliciosos promedia las 300 nuevas variantes mensuales. Esta tendencia es preocupante, puesto que usualmente se trata de códigos que tienen consecuencias sumamente perjudiciales para los dueños de los terminales: pérdida de información sensible, inutilización de los dispositivos y verdaderos gastos económicos.

[1] Dato correspondiente al segundo trimestre de 2018. Fuente: Ventas de smartphones a usuarios finales por sistemas operativos, Statista. Disponible en *https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems.*

Dependiendo del mecanismo que utilice el malware para infectar al equipo, se lo suele clasificar en virus, gusano o troyano. Los virus son el tipo más antiguo de infección, hoy prácticamente inexistente. Se trata de archivos de usuario que han sido modificados para agregarles algún comportamiento malicioso. El proceso de desinfección consiste en remover la sección maliciosa para obtener el archivo original.

Por su parte, los gusanos son códigos maliciosos que tienen capacidades de propagación autónoma: no necesitan del usuario para replicarse en otros sistemas, sino que usualmente sacan provecho de unidades extraíbles infectadas o explotación de vulnerabilidades en otros equipos conectados a la misma red.

Finalmente, encontramos a los troyanos, el tipo de malware más frecuente en la actualidad. Los troyanos son aplicaciones que ocultan su objetivo principal y que, por lo general, se camuflan como juegos, programas para acceder a servicios bancarios, y otro tipo de software.

A su vez, los virus, gusanos y troyanos pueden clasificarse según el tipo de acción maliciosa que realicen sobre el equipo que han afectado. Por ejemplo, en el mundo digital podemos encontrar troyanos tipo bot que responden a comandos remotos, o troyanos que roban información (spyware) o que la secuestran (ransomware).

El *auge del ransomware* ha ciertamente marcado un antes y un después en la historia del malware, determinando un nuevo rumbo en el modelo económico del cibercrimen. Los televisores inteligentes no son inmunes a este tipo de infecciones. Muchos usuarios han descargado en las redes la frustración de ver sus televisores secuestrados por variantes similares a *Simplocker* o al *Virus de la Policía*.

Imagen 3 Smart TV comprometido con una variante del Virus de la Policía.

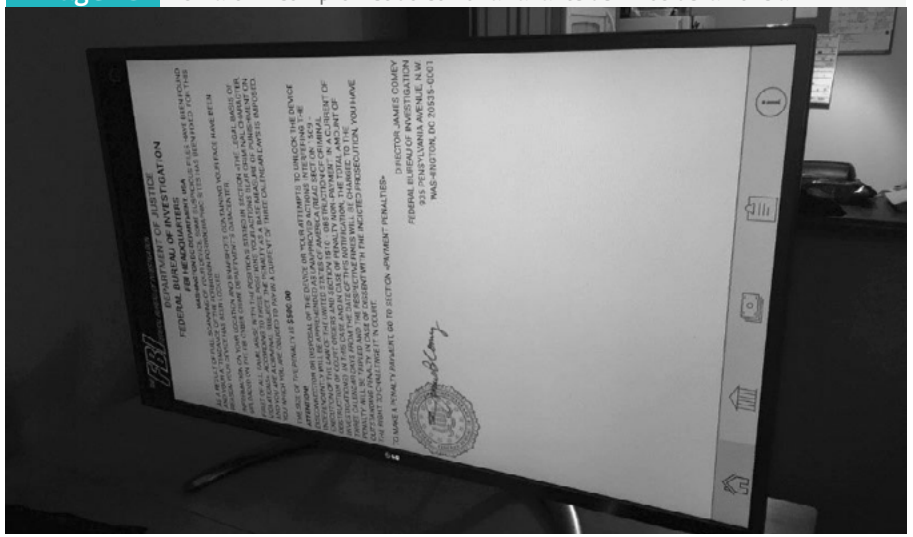


Imagen por Darren Cauthon, disponible en https://twitter.com/darrencauthon/status/813096722989809665.

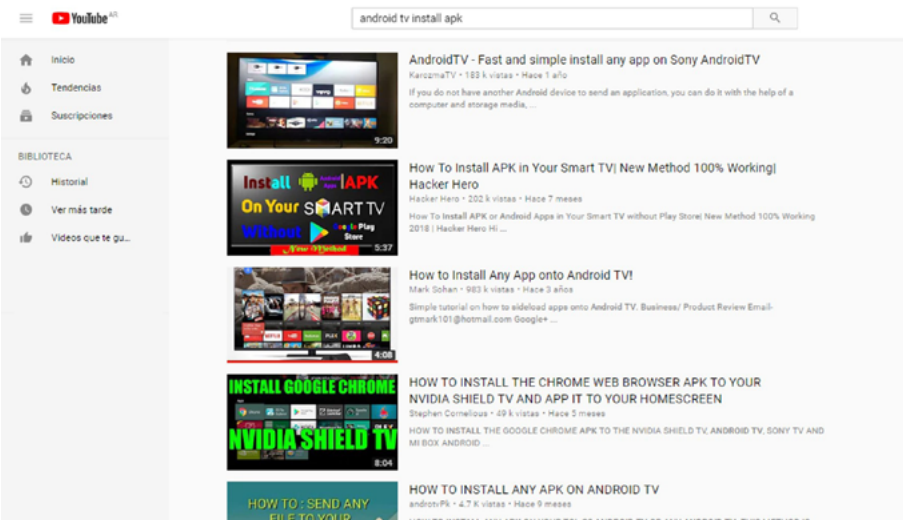
Otra de las tendencias en los últimos años ha sido el *cryptojacking* (es decir, el secuestro de la capacidad de procesamiento de un equipo ajeno para ganar dinero mediante la minería de monedas) y, como era de esperarse, los atacantes encontraron rápidamente la manera de sacar provecho de la cantidad de horas que pasas viendo tu serie favorita en tu Smart TV.

ADB.Miner es la evidencia de cómo el malware orientado a la minería de criptomonedas se ha complejizado adquiriendo capacidades de autopropagación, siendo capaz de instalarse en televisores inteligentes mediante la explotación de puertos de depuración abiertos debido a configuraciones inseguras. *Otras amenazas* similares surgirían con el paso del tiempo.

Factores que facilitan la distribución del malware para Android TV

Para complicar el panorama, debido a que muchas aplicaciones no están disponibles en la tienda Google Play Store de Android TV, los usuarios buscan instalarlas por otros medios. Con solo unos pocos clics pueden encontrarse decenas de tutoriales en línea indicando a los usuarios cómo instalar aplicaciones por fuera de la tienda oficial.

Imagen 4 Tutoriales para la instalación de apps en Android TV por fuera de la tienda oficiales en YouTube.



Muchos de estos tutoriales incluyen una guía sobre cómo *rootear* el equipo. El *rooteo* o *rooting* es un proceso que permite obtener permisos de administrador sobre el dispositivo para realizar modificaciones al sistema operativo, sus aplicaciones y sus configuraciones, mejorar el rendimiento o liberarse de algunas prestaciones o restricciones añadidas por los fabricantes de los dispositivos.

Cuando una aplicación se ejecuta con permisos root, deja de correr en un entorno limitado y gana acceso a todo el sistema de archivos. Si esta aplicación resulta ser maliciosa, el daño que puede provocar al usuario es mucho mayor: robar información de las cuentas de otras aplicaciones, ejecutar un *keylogger* o inhabilitar componentes de seguridad del sistema son algunas de las acciones que estaría habilitada a realizar.

Este procedimiento podría facilitar la instalación de aplicaciones maliciosas en el equipo: no solo existe el riesgo de instalar falsas apps de rooteo que embeban código malicioso, sino que además se simplifica la tarea de otros programas maliciosos que posteriormente intenten comprometer al terminal. De hecho, el malware para Android más agresivo intenta ejecutar exploits para saltar las protecciones de superusuario antes de realizar la acción maliciosa para la que fue pensado.

Al mismo tiempo que aconsejan *rootear* el sistema, los tutoriales en línea suelen indicar los pasos a seguir para la instalación de tiendas no oficiales en el equipo. Estas tiendas presentan un riesgo a los usuarios, no solo porque pueden ser troyanos, además pueden distribuir aplicaciones potencialmente peligrosas o malware.

Un APK (del inglés, *Android Aplication Package*) es un archivo ejecutable de aplicaciones para Android, similar a un *ZIP con algunas modificaciones*. Existen *diferentes maneras* en las que un atacante podría fácilmente hacerse del APK de una aplicación legítima para inyectarle código malicioso y distribuirlo a través de mercados fraudulentos.

Conjuntamente, los ciberdelincuentes apuestan a la Ingeniería Social, esperando atentamente el lanzamiento oficial de apps populares para distribuir versiones falsas de estas, como ocurrió con *Pokémon GO*, *Prisma* o

Dubsmash. La inmediatez con que estas aplicaciones maliciosas consiguen cientos y hasta miles de descargas es un motivo de preocupación, especialmente cuando se ejecutan en un entorno inseguro repleto de datos sensibles.

Vulnerabilidades

Una vulnerabilidad es un agujero de seguridad que permite a un atacantecomprometer un sistema a través de la explotación de dicha debilidad. Dependiendo de la gravedad de una vulnerabilidad determinada, un ciberdelincuente puede ejecutar código de forma arbitraria, obtener más privilegios que los de un usuario estándar, provocar denegaciones de servicio, entre otras potenciales acciones maliciosas.

Los fallos en la programación de sistemas operativos para televisores inteligentes no existen solo en la ficción. Hacia fines de 2018, expertos descubrieron fallos de seguridad en equipos con Roku que permitían *controlar el dispositivo de forma remota* mediante API públicas. Poco antes, investigadores descubrieron vulnerabilidades que permitían *obtener una línea de comandos* de forma ilegítima en algunos modelos de Smart TV. Otros ataques más complejos involucraban la *utilización de comandos HbbTV* (*Hybrid Broadcast Broadband TV*) para ganar permisos de administrador y ejecutar acciones maliciosas. No se requiere mucho esfuerzo para encontrar decenas de ejemplos similares.

El hecho de que estos televisores incluyan funcionalidades de asistentes de voz y se vinculen a una gran variedad de sensores IoT abre otro potencial vector de ataque. Los asistentes de hogar se han diversificado ofreciendo variados precios y servicios a un amplio público con diferentes necesidades, lo que está causando un *rápido crecimiento en sus ventas*. La cantidad de información que estos manejan y el hecho de que poco a poco se conviertan en el punto central para el comando y control de un sinfín de sensores los vuelve un blanco atractivo para el cibercrimen.

Mientras los televisores inteligentes replican la funcionalidad de estos asistentes, los posibles caminos de acceso se multiplican para los atacantes. Tomemos por ejemplo el caso de Chromecast. Este servicio mantiene un puerto abierto para soportar una API a la que cualquier otro equipo en la red puede conectarse para peticionar información o realizar modificaciones en la configuración, levantando preocupaciones en torno a las *consecuencias que esto tiene para la privacidad* de los usuarios. En la siguiente imagen podemos ver el puerto abierto por Chromecast en una NVIDIA Shield.

Imagen 5 Servicio de Chromecast en NVIDIA Shield

```
root@Atacante:~# nmap -sV -T4 -F 192.168.1.102

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-22 22:09 -03
Nmap scan report for 192.168.1.102
Host is up (0.11s latency).
Not shown: 98 closed ports
PORT     STATE SERVICE    VERSION
8008/tcp open  http?
8009/tcp open  ssl/ajp13?
MAC Address: 00:04:4B:AB:2C:1A (Nvidia)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.44 seconds
```

Las vulnerabilidades no solo pueden presentarse en el firmware, el sistema operativo o las aplicaciones que corren en un televisor inteligente, sino también en otros dispositivos conectados, como ocurrió a principios de 2019 con el *ataque masivo a miles de dispositivos Chromecast, Smart TV y asistentes de voz Google Home*, debido a routers mal configurados.

Malas configuraciones

Además del riesgo de que el usuario instale malware o de que existan vulnerabilidades en el sistema operativo o firmware, los Smart TV pueden presentar malas configuraciones por defecto, introducidas por los vendors al momento de modificar el sistema operativo de base para incluir nuevas funcionalidades, o bien, por el usuario.

La existencia de puertos abiertos o de mecanismos de depuración habilitados, el uso de usuarios y contraseñas por defecto o con bajo nivel de seguridad, el mantener habilitados servicios que no se utilizan y el uso de protocolos inseguros son algunas de las configuraciones que podrían causar una brecha de seguridad en el equipo.

Un claro ejemplo de esto son las *masivas infecciones* que a principios de 2018 *afectaron a miles de televisores inteligentes* corriendo versiones de Android TV – y, consecuentemente, otras distribuciones para televisores basadas en Android, como Fire TV – debido a un error en la configuración por defecto de fabricantes asiáticos que liberaron equipos con configuraciones inseguras, exponiendo a sus usuarios. Tras infectar el equipo, estos códigos eran capaces de minar criptomonedas (Monero) mientras el equipo se encontraba encendido.

Bluetooth

Así como como ocurre con los teléfonos inteligentes y las computadoras, los televisores incorporan la capacidad de conectarse mediante redes PAN (Personal Area Network), siendo Bluetooth el protocolo más utilizado en esta categoría. Sin embargo, el uso de Bluetooth no queda absorto de pecados.

En 2017, una vulnerabilidad nombrada *BlueBorne* dejó a más de *5.000 millones* de dispositivos vulnerables, incluyendo diferentes modelos de televisores. Tan solo un año después, una *nueva vulnerabilidad* volvió a poner en jaque la confidencialidad de los datos transmitidos mediante un fallo criptográfico que permitía a un atacante acceder a la información intercambiada entre dos equipos vulnerables.

Ataque físico

Además de los ataques a la infraestructura de red que pueden realizarse si los dispositivos de red no se encuentran correctamente configurados, los televisores inteligentes y TV boxes poseen conectores que podrían ser vulnerados para ejecutar comandos. Sus puertos USB pueden ser utilizados para la ejecución de scripts maliciosos o la explotación de vulnerabilidades.

Por ejemplo, un atacante podría generar un script que simule la presencia de un usuario en un Android TV. Algunos gadgets permiten realizar esta tarea de forma rápida y sencilla, como el famoso –o infame– *Bash Bunny* de Hak5. De esta forma, el atacante puede automatizar un variado popurrí de acciones maliciosas basadas en la interacción con la interfaz de usuario y ejecutar el ataque en pocos segundos, simplemente conectando un dispositivo similar en apariencia a una memoria USB.

La Ingeniería Social al servicio del malware moderno

En toda campaña maliciosa, un componente esencial en la propagación de amenazas y explotación de vulnerabilidades es la *Ingeniería Social*. La diversidad que presentan los usuarios de televisores inteligentes en cuanto a conocimientos de los peligros informáticos es tan grande, que resulta muy sencillo para los ciberdelincuentes encontrar una brecha de seguridad en los hábitos de utilización de los dispositivos por parte de los usuarios.

Si se considera que prácticamente todos los televisores inteligentes cuentan con un cliente para acceder a cuentas de correo electrónico,

y que también incluyen navegadores capaces de visualizar sitios web, entendemos que muchos riesgos multiplataforma se extienden al uso de Smart TV.

El *phishing* es una amenaza informática a través de la cual los cibercriminales suplantan a una entidad de confianza como un banco u otra empresa para robar información de la víctima. Por lo general, el phishing suele provenir de un correo electrónico en el que se le indica al destinatario que deberá entregar determinados datos, de lo contrario, se lo amedrenta indicándole que su cuenta o servicio podría presentar problemas.

Por otro lado, los *fraudes electrónicos o scams* también son amenazas que suelen llegar a través de correo electrónico o redes sociales. A diferencia del phishing, los scams utilizan premios falsos para seducir a la potencial víctima. En el texto es común observar que los atacantes solicitan datos personales del usuario y una suma de dinero que debe depositarse antes de poder cobrar el premio (dicha suma suele ser considerablemente más alta que el monto solicitado a pagar). Al tratarse de amenazas que hacen uso del correo electrónico y de sitios web para operar, ambos ataques pueden afectar a usuarios de televisores inteligentes de igual modo que a una persona que utiliza una laptop o teléfono.

Las ciberestafas tienen la característica de mutar con asombrosa velocidad, pudiendo aparecer, comprometer a miles de usuarios y desaparecer en cortos períodos de tiempo. Quizás una de las campañas fraudulentas de mayor dimensión que hemos atestiguado recientemente fue aquella que simulaba cupones de descuentos en nombre de múltiples empresas de renombre, extendiéndose a través de múltiples países, llegando a reunir más de 22 millones de víctimas alrededor del mundo. Investigadores del laboratorio de ESET Latinoamérica desarrollaron un *reporte* donde el lector podrá encontrar más información al respecto.

MEDIDAS DE PROTECCIÓN

Para proteger nuestros equipos de todos estos riesgos de seguridad podemos tomar acciones preventivas que nos aseguren la mitigación de ataques en nuestros televisores inteligentes. A continuación, examinaremos algunas de las buenas prácticas a seguir.

Soluciones de seguridad

Existen diversas *soluciones de seguridad* que ofrecen protección contra amenazas para Smart TV, en particular, para aquellas distribuciones basadas en Android. Estas soluciones cuentan con módulos capaces de prevenir infecciones por malware y de detectar páginas fraudulentas para bloquear el acceso a ellas (funcionalidad denominada *antiphishing*). Otra capa de protección que deben incluir estas soluciones es la de protección de los puertos USB, para evitar que los códigos maliciosos puedan colarse mediante estos conectores.

Dado que los televisores no se encuentran exentos de ser robados, muchas de estas soluciones permiten incluso gestionar el equipo de manera remota en caso de robo o extravío, ya sea para bloquearlo, borrar sus datos, capturar imágenes desde la cámara o bien obtener la posición actual del dispositivo.

Configuraciones seguras

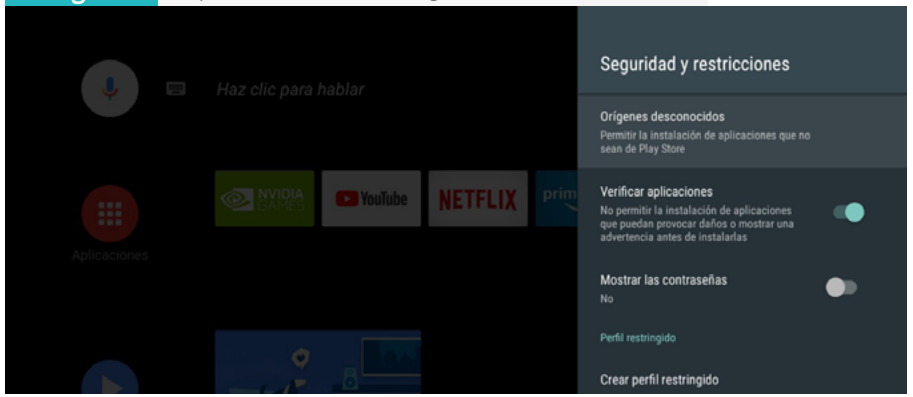
Reforzar los ajustes del dispositivo para asegurarnos de no dejar huecos de seguridad debiese ser una de las primeras precauciones a tomar luego de adquirir un nuevo televisor inteligente o aparato de streaming.

Dado que, como vimos al comienzo del artículo, la mayoría de los usuarios posee equipos basados en Android, utilizaremos una NVIDIA Shield con Android 8 Oreo para ejemplificar algunas configuraciones de seguridad importantes. Puede que el procedimiento sea algo diferente para otros fabricantes, pero usualmente podrá encontrarse una opción análoga para cada uno de los siguientes puntos.

Menú de seguridad

El menú de seguridad suele ser el sitio más sencillo donde comenzar el chequeo de las configuraciones del equipo. En la próxima ilustración pueden verse las opciones de seguridad que encontramos en la NVIDIA Shield, que pueden accederse desde “Ajustes”.

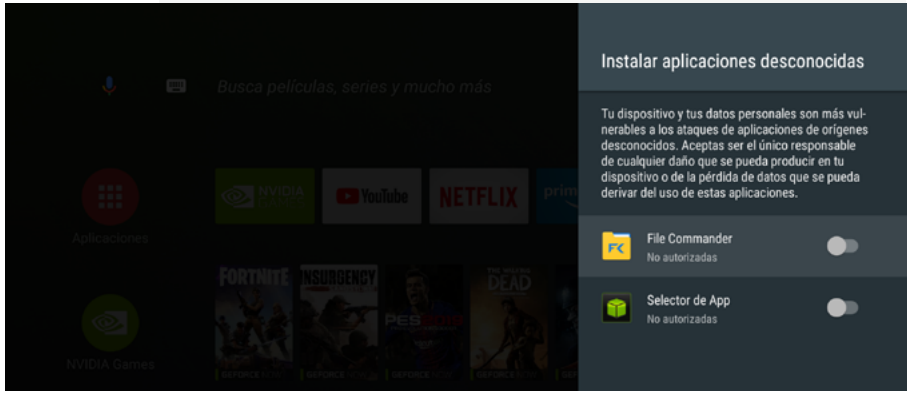
Imagen 6 Opciones del menú de seguridad en NVIDIA Shield.



En orden descendente encontramos:

- **Orígenes desconocidos**. A diferencia de las viejas versiones de Android, donde la habilitación de orígenes desconocidos se aplicaba de manera global y uniforme a todas las aplicaciones instaladas, en las nuevas versiones es posible restringir el permiso de forma particular para cada aplicación. A menos que se tenga mucha confianza en el aplicativo y su desarrollador, se recomienda mantener deshabilitada la instalación desde fuentes desconocidas para todas las apps

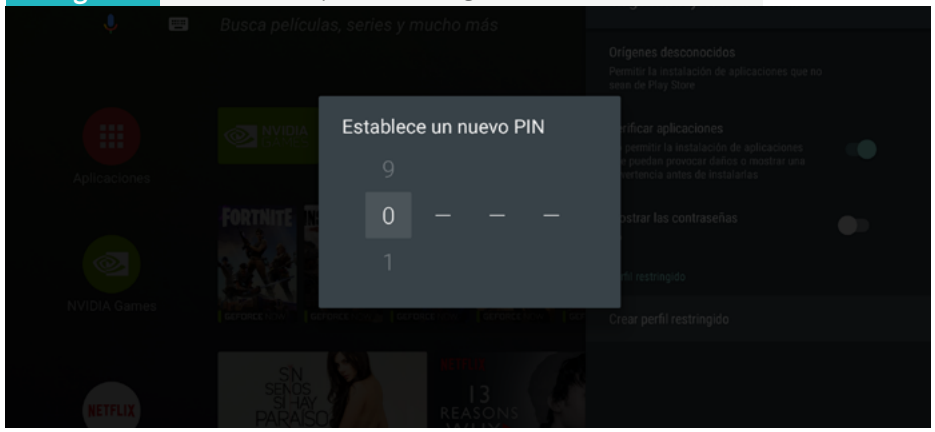
Imagen 7 Aplicaciones con permisos para instalar aplicaciones desconocidas en Android TV.



- **Verificar aplicaciones**. Esta opción permite activar el escaneo de apps maliciosas de Google. Esto habilita a Google a proteger el equipo de cualquier malware conocido o aplicación potencialmente peligrosa.
- **Mostrar las contraseñas**. De encontrarse activado, el usuario podrá ver los caracteres que ingresa al completar campos de credenciales en un formulario. De no ser necesario, se recomienda mantener desactivado para dificultar el robo de datos.

- Crear perfil restringido. Esta opción funciona como un control parental, permitiendo crear un perfil de usuario para el que solo algunas aplicaciones estarán disponibles. Cada vez que se active o desactive este nuevo perfil, se solicitará al usuario que ingrese un PIN de cuatro dígitos. Dado que los *perfiles restringidos* tienen acceso limitado a la administración del equipo, pueden utilizarse para restringir el acceso que se tiene en el equipo cuando no se lo está usando, ya que Android TV no brinda opciones de bloqueo de dispositivo.

Imagen 8 Activación de perfiles restringidos en Android TV.

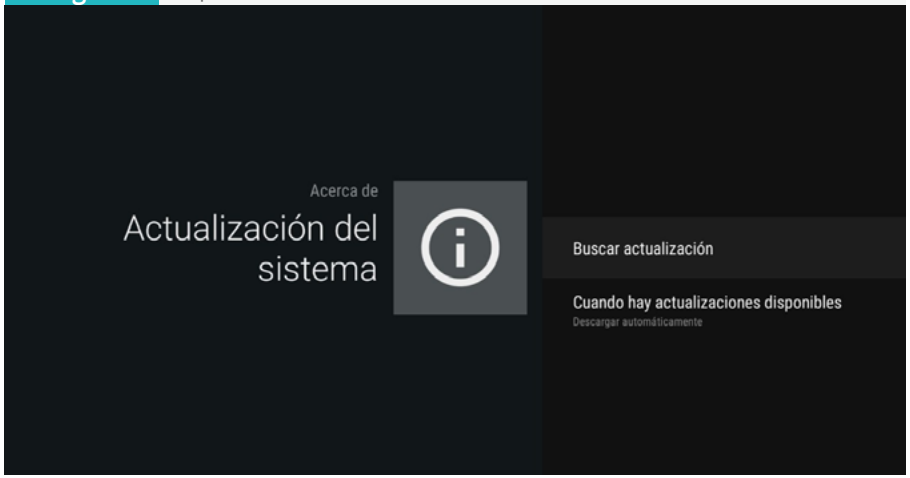


Actualizaciones

La actualización del sistema operativo de las aplicaciones que corren en el equipo es sumamente importante. La mejor opción resulta siempre automatizar la búsqueda e instalación de nuevas versiones y parches de seguridad, para así no depender del usuario. Usualmente, los procesos de actualización pueden configurarse desde el menú de ajustes del equipo.

Si navegamos desde **Ajustes → Información → Actualización del sistema** nos encontraremos con el menú que se observa en la siguiente captura de pantalla. En él podremos seleccionar la opción de "**Buscar actualización**", que nos permitirá corroborar en el momento si existe alguna versión o parche de seguridad aún no instalado, y la opción "**Cuando hay actualizaciones disponibles**" donde el usuario deberá activar la descarga automática de actualizaciones.

Imagen 9 Opciones de actualización del sistema en Android TV en NVIDIA Shield.



No debemos olvidarnos de configurar la actualización automática de las apps instaladas en el dispositivo. Esto puede hacerse desde los ajustes de Google Play Store.

Imagen 10 Activación de actualización automática de apps en Google Play Store.

Configuración de Google Play Store

En la imagen anterior podemos observar otras dos configuraciones que hacen a la seguridad integral del equipo. Por un lado, encontramos la opción de activar el *Control parental*: ejercer el control sobre el contenido que acceden los más chicos es sumamente aconsejable, ya que ayuda a limitar el uso de aplicaciones potencialmente peligrosas para su privacidad.

Por otro lado, tenemos la opción de Autorización de compra, que solicitará ingresar la contraseña de la cuenta antes de confirmar cualquier compra en la tienda.

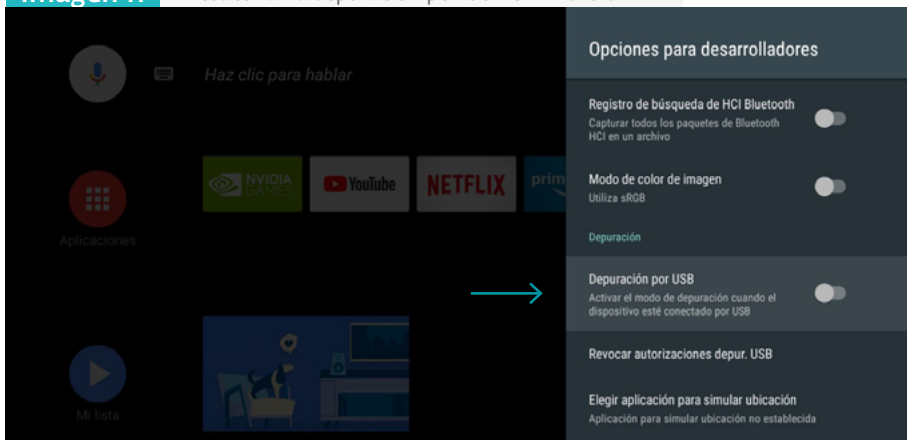
Deshabilitar la depuración por defecto

Anteriormente mencionamos el caso de ADB.Miner, detectado por los productos de ESET como variantes de *Android/Coinminer.X:* un criptominero capaz de propagarse de un equipo a otro sacando provecho de puertos de depuración habilitados.

La depuración puede activarse desde las opciones de desarrollador de Android, que debiesen estar ocultas en equipos de fábrica y pueden habilitarse desde el menú de información sobre el equipo. Un televisor puede depurarse a través del puerto USB o utilizando TCP-IP. En ambos casos, el sistema requerirá que se autorice la conexión antes de permitir acceso al equipo remoto.

Si el Smart TV no se utilizará como dispositivo de prueba de aplicaciones en un entorno de desarrollo, entonces lo mejor es mantener los puertos de depuración desactivados (en Android, la herramienta adb –*Android Debug Bridge*– se ejecuta por defecto en el puerto 5555). De lo contrario, si se es desarrollador y se necesita depurar algún aplicativo, quizás sea buena práctica revocar periódicamente las autorizaciones de depuración existentes y chequear si tenemos conexiones establecidas en el puerto 5555.

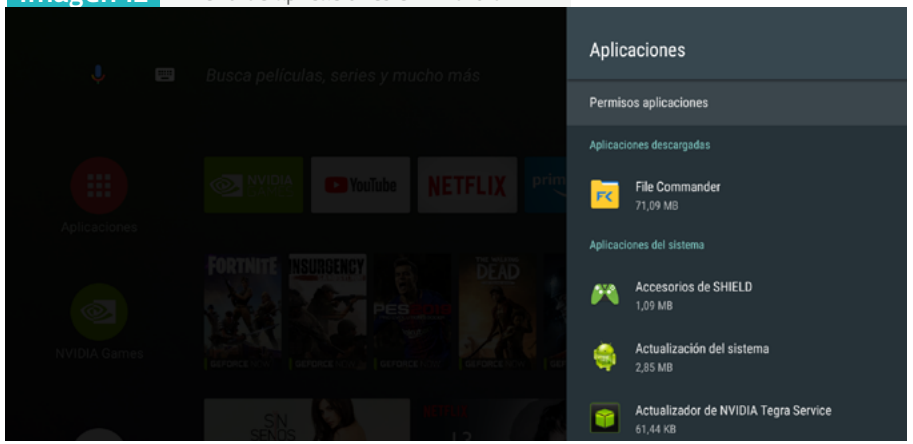
Imagen 11 Desactivar la depuración por USB en Android TV.



Restricción de permisos para aplicaciones

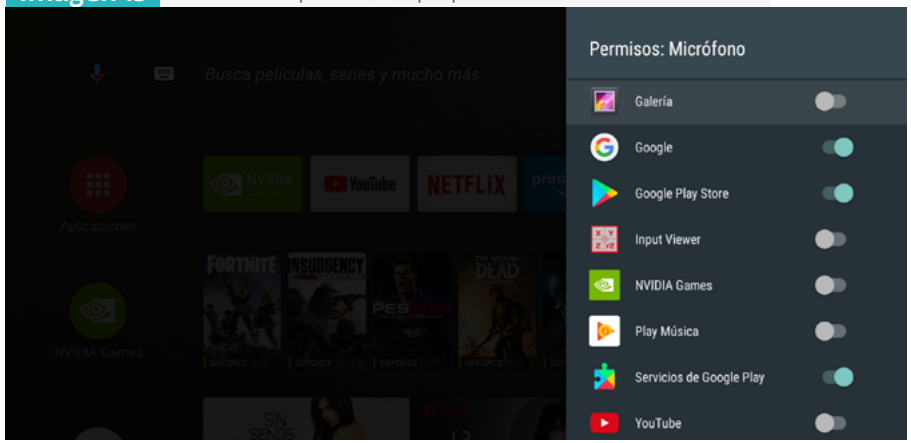
Las apps peticionan múltiples permisos para acceder a una gran variedad de funcionalidades. Estos permisos se peticionan al ejecutar el aplicativo, en el momento en que se necesita hacer uso de la funcionalidad. En esta instancia, el usuario puede otorgar el permiso, denegarlo por única vez o denegarlo de forma permanente. Sin importar la opción que elija, los permisos de cada app pueden restringirse de forma individual desde el menú de aplicaciones. Para hacerlo se debe acceder a Ajustes → Aplicaciones.

Imagen 12 Menú de aplicaciones en Android TV.



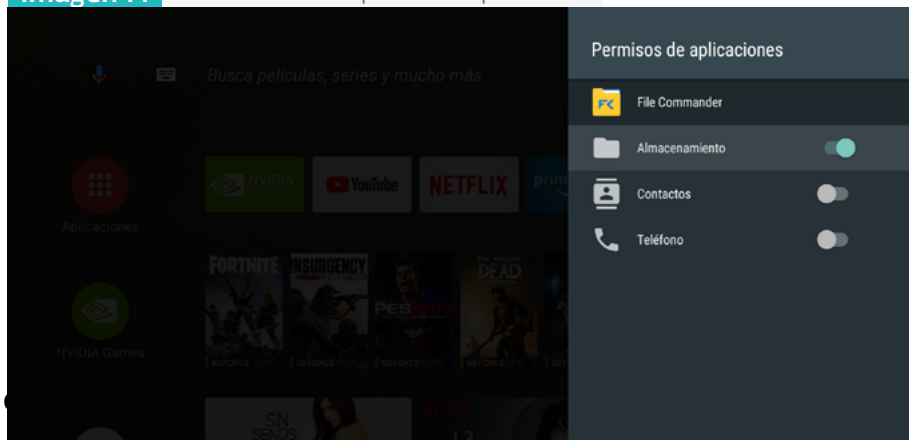
Si nos interesa ver qué aplicaciones pueden acceder a un determinado permiso, podemos ingresar a la opción **“Permisos aplicaciones”**, seleccionar el permiso en cuestión y activar o desactivar ese permiso para cada app que lo requiere.

Imagen 13 Listado de aplicaciones que pueden acceder al micrófono.



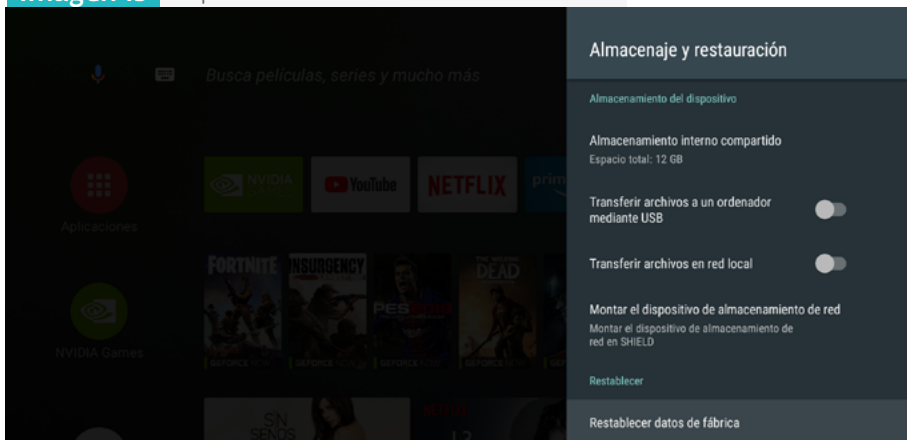
Por el contrario, si nos interesa administrar los permisos de una aplicación específica, podemos elegir la app en cuestión, seleccionar la opción "Permisos" y activar o desactivar cada permiso para esa app en concreto.

Imagen 14 Permisos de una aplicación en particular.



Otra de las opciones de seguridad que podemos encontrar en la sección Ajustes es el restablecimiento de fábrica, que nos permite borrar todos los datos almacenados en el equipo. Esta funcionalidad es muy útil cuando se piensa desechar o vender el equipo, o ante infecciones por algún malware muy persistente que pueda resultar difícil de remover de otro modo.

Imagen 15 Opciones de restablecimiento del sistema.



Deshabilitar la recolección de datos

Uno de los debates que se ha despertado en torno al uso de televisores inteligentes y el cuidado de la privacidad de los usuarios abarca la *recolección excesiva de datos* que puedan realizar los fabricantes y las aplicaciones sobre el equipo para capturar los hábitos de actividad y consumo del usuario.

En algunos casos, es posible deshabilitar las opciones de recolección desde el menú de configuraciones (es importante evaluar esto antes de adquirir un equipo y se recomienda recurrir siempre a marcas confiables). También es muy importante leer las políticas de privacidad que puedan asociarse al

sistema operativo o los aplicativos instalados por defecto, y cualquier otro software de manera general.

Reforzar la seguridad de la red

Aunque ciertamente ayuda, de poco sirve configurar correctamente el dispositivo sin construir un entorno de red seguro. Para proteger nuestros televisores, es igualmente importante asegurarse de que el router utilice protocolos seguros y credenciales fuertes, y que su firmware no posee vulnerabilidades como las que en el pasado habilitaron miles de infecciones por Mirai.

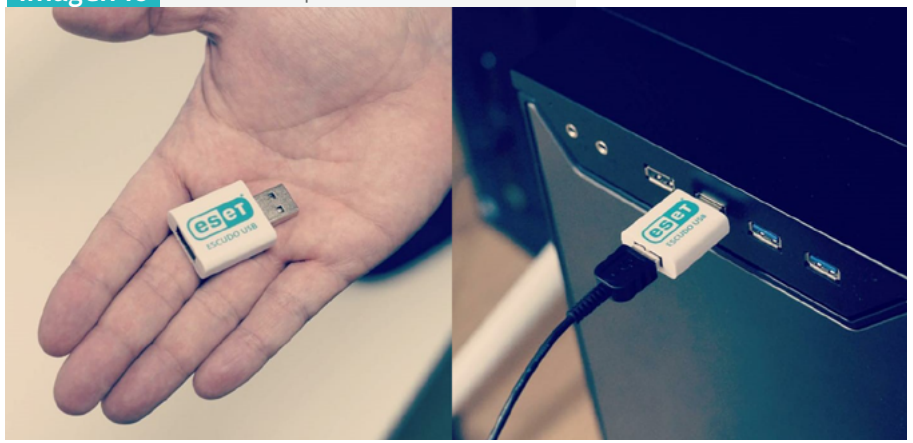
Para aprender más sobre cómo configurar la red de tu hogar de forma segura, te recomendamos acceder al curso de *seguridad en redes hogareñas* de ACADEMIA ESET.

Protección física

Para los equipos que se encuentren en espacios vulnerables –por ejemplo, en la sala de espera de una oficina o en una sala de estar donde se suelen realizar eventos con personas a quienes no conocemos muy bien–, se debe tener en cuenta la protección de las entradas físicas del dispositivo –del mismo modo que con cualquier otro dispositivo de red–, tanto de red como de USB. Para ello, podemos activar la protección lógica mediante soluciones de seguridad o, en el caso de las TV boxes, podemos utilizar cajas acrílicas con cerrojo, las mismas que se usan en otros sensores IoT.

Para proteger los puertos USB podemos también utilizar escudos USB: unos gadgets que se colocan entre el televisor y cualquier unidad externa que vaya a conectarse a él, e impiden cualquier ejecución indeseada de código.

Imagen 16 Escudo USB para unidades extraíbles.



Del mismo modo en que se utilizan bloqueadores de cámaras en laptops y equipos de escritorio, es recomendable tapar la cámara del televisor inteligente cuando no se la está utilizando. Aunque existen gadgets que cumplen esta función, una simple tira de cinta o nota adhesiva logrará el mismo cometido.

Buenas prácticas de seguridad

Finalmente, para reducir el riesgo de incidentes informáticos en televisores, es necesario educarse respecto a las mejores prácticas para el uso de dispositivos inteligentes, Internet, y tecnología en general. Para lograr esto, pueden seguirse algunos consejos como los detallados a continuación:

- Utiliza contraseñas seguras, procura no repetirlas entre diferentes plataformas y activa el *doble factor de autenticación* siempre que sea posible. Es importante utilizar los factores de doble autenticación que ofrecen muchos servicios en Internet.

- Procura utilizar solo tiendas oficiales para descargar aplicaciones, donde las probabilidades de infectarte con malware son más bajas –no nulas–. Asimismo, es fundamental leer el contrato de licencia que acompaña al software.

- Al instalar apps desde tiendas oficiales, revisa los comentarios, la valoración y los permisos que requieren antes de instalarlas. Pregúntate si los permisos que requiere son acordes a la funcionalidad del software y restringe cualquier permiso que no creas estrictamente necesario para que la aplicación pueda ejecutarse correctamente. Recuerda que algunos permisos representan riesgos de seguridad más elevados que otros, y podrían ser un *indicador de actividad maliciosa*.

- Para garantizar la disponibilidad de los archivos cuando son necesitados, es aconsejable que realices frecuentemente *copias de seguridad* de todos los datos en el equipo, o al menos de los más valiosos. La opción más sencilla de respaldo consiste en duplicar los archivos en la nube. De esta manera, aunque se pierda el equipo, la información podrá siempre ser accedida.

- Trata de evitar procesos de *rooting* o *jailbreaking*, ya que pueden interferir en los procesos de actualización del equipo y facilitar la instalación de malware.

- Desactiva el uso de conexiones inalámbricas Wi-Fi y Bluetooth cuando no se estén utilizando para prevenir amenazas que se propagan a través de dichos canales de comunicación.
- Utiliza redes conocidas y privadas, especialmente cuando manejes información sensible como datos crediticios o credenciales de inicio de sesión.

- Si no puedes conectarte mediante una red segura, procura utilizar una VPN para cifrar el contenido del tráfico.

- Ten cuidado con los mensajes que recibes mediante correo electrónico o redes sociales y que incluyan enlaces. Evalúa la seguridad del sitio al que ingresarás antes de hacer clic sobre él. Si recibes algún mensaje sobre promociones en línea, contacta a la entidad a la que corresponde la supuesta promoción para constatar si el mensaje es verídico.

- Asegúrate que el enlace que estés visitando pertenezca a la organización oficial. Si enviarás información confidencial, verifica si la conexión es cifrada mediante HTTPS –lo que puede usualmente observarse como un candado verde donde se encuentra la URL–, que el certificado sea firmado por una entidad confiable y que los detalles del dominio sean correctos, para evitar *ataques homográficos*.

- Intenta siempre ingresar al sitio de una organización escribiendo la URL en la barra de direcciones y no mediante los resultados de buscadores como Google, ya que los primeros resultados no siempre son los genuinos debido a una actividad conocida como black hat SEO.

- Cuando realices compras en línea procura utilizar tu tarjeta de crédito y no de débito, ya que es mucho más sencillo denunciar y revertir la situación en caso de que los datos sean robados.

- Ten en cuenta que tu información personal es muy valiosa para los cibercriminales. Piensa bien antes de compartirla en Internet. Cuantos menos datos personales subamos a las redes, menos expuesta va a estar nuestra información personal, sobre todo en el caso de fuentes poco confiables o poco conocidas.

- Si venderás tu televisor inteligente, asegúrate de borrar correctamente los datos del equipo para que tu información no pueda ser accedida por su nuevo dueño. En equipos con Android, el procedimiento no es muy diferente al *borrado en teléfonos móviles*.

CONCLUSIÓN

La protección de los activos de información puede entenderse como el diseño y puesta en marcha de un sistema de seguridad en capas, donde las barreras de protección se solapan unas sobre otras con el objetivo de dificultar la intrusión de un cibercriminal. En este contexto, la Internet de las Cosas demanda un cuidadoso análisis de los riesgos de seguridad presentes según la cantidad y diversidad de equipos que manejan datos sensibles, para poder así implementar un sistema de protección efectivo.

A medida que los televisores inteligentes ingresan cada vez más en nuestros hogares y oficinas, y mientras la información que les suministramos se vuelve incrementalmente más sensible, aumenta la probabilidad de un ataque, como así también la gravedad de sus consecuencias. Para prevenirlos, es importante que los usuarios entiendan el abanico de vectores de compromiso que puede poner en jaque la seguridad de su información y las tecnologías que pueden bloquearlos.

Sin embargo, cabe destacar que la protección no solo se logra a través de la instalación de una solución de seguridad, sino también mediante la concientización del usuario y la adopción de un comportamiento seguro con respecto a las amenazas informáticas.


ENJOY SAFER TECHNOLOGY™
www.eset.com/latam
esetla
@esetla
@esetla
ESET Latinoamérica