# Puede un hacker robar información de su Smart Tv? La vulnerabilidad de los televisores modernos peligro al acecho

Medina Díaz Granados Luis Daniel
luismedinadiazg@hotmail.com
Universidad Piloto de Colombia

*Resumen*—Este documento aborda los componentes específicos de VULNERABILIDAD de datos encontrados en un dispositivo como también de amenazas puntuales que se encuentran integrados al TELEVISOR con Sistema SMART TV y que sugiere una estrategia para hacer frente a estas áreas desprovistas de seguridad y de algunas recomendaciones específicas adecuadas para distintos usuarios sobre estas vulnerabilidades. La seguridad en estos sistemas, no es algo de interés para muchos usuarios que compran estos aparatos sin embargo, si corresponde a aquellas personas que tengan que ver con seguridad informática en cualquiera de sus ramas.

*Índice de Términos*—Black Hat, DNS poisoning, drive-by download, ISEC Partners, SmartHub, Webkit, y Reset.

*Abstract*—This paper addresses the specific components of VULNERABILITY data found on a device as well as specific threats that are integrated with the SMART TELEVISIONS TV System and suggests a strategy to address these areas that lack adequate security and some specific recommendations for different users on these vulnerabilities. Security in these systems is not something of interest to many users who buy these devices however, if it corresponds to those who have to do with computer security in all its branches.

## I. INTRODUCCIÓN

Los TELEVISORES convencionales que conocíamos en su gran mayoría solo eran aparatos electrónicos destinados a la recepción y reproducción de señales de televisión con una pantalla y mandos o controles en un cascaron robusto con tubo de imagen. Hoy en día sea a convertido en todo un equipo multimedia parecido a un ordenador de mesa o laptop prestando diversas funcionalidades las cuales día a día el auge de usuarios por optar a un equipo de estos, se hace más popular pero al mismo tiempo crece un problema que viene en acecho si no se logra fortalecer la seguridad en los futuros equipos, brindando de forma controlada y precisa las vulnerabilidades que se están presentando con el pasar de los meses.

En estos momentos los TELEVISORES con sistema SMART TV, se compone de numerosas funciones de las cuales las más básicas y utilizables son *Conectividad Wi-Fi, Twitter, Facebook, Skype o conexiones de dispositivos USB y de Ordenadores en sus puertos incorporados HDMI*, brindando al hacker un sin números de fallas de seguridad, como es la de dejar a merced la información alojada en los dispositivos conectados al aparato, como también poder ser espiado mediante la activación de la cámara integrada enfocando todo lo que tiene al frente y la del micrófono de alta calidad oyendo las conversaciones. Todo esto se logra sin que el *usuario* en ese momento se percate que está siendo observado y escuchado por un hacker.

## II. PIONEROS E INVESTIGADORES DE FUTUROS ATAQUES

Es importante mencionar a dos personajes en estos temas como lo son *Aaron Grattafiori y Josh Yavor*, ingenieros de seguridad en *ISEC Partners*.

En su presentación Black Hat ambos investigadores describieron en un SMART TV SAMSUNG, un dispositivo Linux configurado

con un navegador Webkit para abrir páginas web y ejecutar aplicaciones. Por lo tanto, es un sistema que soporta las mismas vulnerabilidades que han sufrido navegadores basados en ese motor y que han sido documentadas y parcheadas con el paso del tiempo.

En la presentación mostraron dos vulnerabilidades en SmartHub, la aplicación encargada de muchas de las funcionalidades interactivas del TELEVISOR y que podrían ser explotadas por un usuario local o remoto, por ejemplo, activar la webcam del SMART TV y espiar a una supuesta víctima tanto con la imagen como con sonido y de *Ataques de tipo DNS poisoning y drive-by download*, estos muestran cómo las vulnerabilidades pueden ser combinadas para *conseguir credenciales de usuario local, el historial de búsqueda, caché, cookies y la contraseña inalámbrica*.

## III. SEGURIDAD

Es de trascendental importancia la implementación cómo en los ordenadores de mesa y en laptops con entradas de puerto de red o conectividad WiFI la *seguridad de Firewalls* con *requisitos de autenticación* para cuando el usuario encienda su TELEVISOR, ingrese al sistema y por medio de una interfaz amigable digite el nombre y contraseña para acceder a su perfil logrando utilizar las distintas funciones de forma segura.

Sabemos que un hacker, puede definir varios propósitos, como la de robar datos de los dispositivos conectados al SMART TV, utilizar los distintos componentes entre esos la de la *activación del micrófono incorporado, la manipulación completa de cambiar los canales, el volumen* y de las cuales ya se han venido detectando desde hace un par de años con las referencias antiguas de estos dispositivos y que ahora con las últimas series vemos que han mejorado algunas de las vulnerabilidades encontradas y señaladas anteriormente.

En un futuro se obtendrá en cada uno de estos sistemas, una seguridad fiable y estandarizada que mantendrá la información protegida ante un ataque hacker, complicando los procedimientos que utilizan para realizar estos tipos de penetraciones sin quitarle rendimiento al equipo por lo robusto del desarrollo que se necesite en estos nuevos dispositivos.

## IV. QUE TIPOS DE HACK SE HAN DADO EN LOS TELEVISORES SMART TV

Los ataques disponibles para este sistema no son sencillos, ya que la documentación y el software disponible para dicho procedimiento, aún en esta época es insuficiente y no se encuentra mucha información disponible en la web para lograr realizar un estudio preciso de las distintas referencias encontradas en el mercado para cometer un tipo de ataque de forma controlada y sencilla. Un software solido capaz de penetrar estos TELEVISORES con diversos sistemas operativos no está aún disponible de forma completa. En el mercado se encuentra cantidades de marcas de SMART TV de las cuales los más nombrados son LG *y* SAMSUNG cabeza en ventas a nivel mundial.

Si una persona con ciertas habilidades y conocimientos en hacking desea lograr una penetración en alguno de estas marcas con este sistemas, puede lograr estropear el aparato en la investigación que realice, perdiendo un valor considerable en dinero si de prácticas necesitamos hacer para lograr ejecutar un plan de ataque pero con el problema que si se llega a descomponer este dispositivo, no se logrará incluso ni recuperar con el botón *Reset*. Con esta opción que viene de fábrica, puede restaurar el sistemas al momento de un falló general del aparato, y si al final no se logra reparar con esta acción, el dispositivo quedaría inservible para poder volverlo a utilizarlo en la investigación.

Esto es un punto a favor para los usuarios ya que los hackers actualmente tienen que trabajar

lentamente por carecer de información a estos tipos de prácticas de penetración y actualmente están a ciegas.

Pero una de las ventajas que si tiene estos hackers, es que estos sistemas son muy similares a los *Smarphones*. Los SMART TV cuentan con una plataforma capaz de realizar descargas de aplicaciones e instalarlas en el para actualizar el *Fremware* que trae de fábrica a una versión mejorada realizando ajustes en sus funciones.

También los TELEVISORES vienen con aplicaciones desarrolladas en *HTML, Java o Flash* en la cual se deben actualizar con parches de seguridad para no ser atacado por las vulnerabilidades que día a día se van filtrando por medio de estos programas al sistema. Instalar un software malicioso, se puede ejecutar por varias maneras por medio de un *rootkit* o ingresar por medio de alguna VULNERABILIDAD de algún software instalado en el dispositivo o por el *SDK* del SMART TV.


Figura 1: Samsung Smart Tv Apps Developer SDK 5.0

Con un *Rootkit*, puede activar la cámara o el audífono percibiendo todo lo que se puede ver y escuchar en el dispositivo, registrando en tiempo real audio y video instalado en una vivienda hogareña o en un sitio comercial donde se distribuya estos sistemas o aún más importante, en algún lugar dentro de una organización donde se puede grabar conversaciones importantes de una sala de juntas tomando fotografías de las personas que se encuentra en ese recinto y como sabemos el TELEVISOR está conectado las 24 horas del día durante todo los meses del año.

También es posible realizar un tipo de ataque mediante el navegador que viene incorporado, la cual por medio de estas aplicaciones cargadas, se puede introducir información al momento de ingresar en páginas como *Facebook, Hotmail u otras cuentas* importantes la cual el usuario necesite configurarlas para lograr acceder e interactuar con él.

Estos sistemas por lo general son utilizados y conectados normalmente a la red *WIFI o Red Lan* para proporcionarle internet y así lograr obtener toda la capacidad que puede dar estos SMART TV en la semana y con las opciones de lograr instalar programas diseñados para esta plataforma, pero lo que sí es un poco triste es que es muy difícil mantener las actualizaciones para los complementos como *Flash, Java* porque estos sistemas no tienen un menú de alertas de notificaciones potente para poder avisar al usuario de ciertas filtraciones que puede tener al no actualizar estas aplicaciones a tiempo.

## V. Escenarios de Ataques

A nivel mundial, no está restringido la venta de estos sistemas SMART TV por ser un equipo inofensivo aparentemente, es por eso que comprar se hace sencillo obteniendo la serie que desee dependiendo de la capacidad adquisitiva que tenga el usuario al momento de la compra. Existen dos tipos de usuarios que representan los escenarios que expondremos en este artículo.

Los usuarios hogareños, normalmente son todos los usuarios que viven en casa, provista de personas aledañas a un núcleo familiar y que contiene normalmente de sala, comedor o dormitorio donde la persona encienda el equipo para visualizar los programas favoritos o para entretenerse en la comodidad de su hogar y los usuarios que tienen este sistema a nivel empresarial, las cuales tienen este sistema para presentar de forma controlada lo que se quiere que

se visualice por medio de la imagen en pantalla informando los detalles del tiempo o de la información de la organización o incluso presentaciones importantes que solo le compete al personal de la empresa ya que las pantallas pueden llegar a ser más de 60 pulgadas optimizando con más nitidez el audio y video que los proyectores convencionales conocidos como Video Bind.

*A. Escenario de ataque #1*

El TELEVISOR SMART TV instalado en el hogar y conectado a una la red de *Internet Lan o WIFI* las 24 horas del día sin ninguna restricción, con una velocidad de transmisión de 4 KB la cual normalmente ya se encuentra en nuestro país los paquetes básicos con esta velocidad dando trasferencia de datos de información con velocidades altas.

El atacante puede lograr ingresar por este sistema y activar la cámara web integrada para poder visualizar lo que está enfrente. En la mayoría de las veces un TELEVISOR es colocado de manera fija en la pared o un mueble con panorama proyectada a la sala o al dormitorio del usuario permitiendo observar de manera completa toda la dimensión de donde se encuentre este sistema logrando el atacante grabar todos los movimientos del usuarios.

*B. Escenario de ataque #2*

Se describe el mismo escenario anterior pero con la particularidad de la activación del micrófono incorporado en el sistema SMART TV, este actúa acatando las órdenes funcionales por medio del reconocimiento de voz, con acciones de cambio de canales, aumento y disminución del volumen entre otras funciones. La configuración se ejecuta grabando y guardando las funcionales básicas utilizadas por un usuario con su voz. El hacker mediante este sistema, puede filtrarse por medio de la red y lograr activar de manera controlada este micrófono burlando la seguridad del sistema, así puede lograr escuchar todo lo que se esté hablando en la sala, la cocina o en el dormitorio donde se encuentre este sistema instalado.

*C. Escenario de ataque #3*

Si el hacker tiene un nivel bueno puede lograr vulnerar las dos opciones, activando audio y video. Se obtiene información más comprometedora parar lograr la modalidad de extorsión, grabando día y noche hasta alcanzar un material importante para lograr someter a la persona a sus pretensiones.

*D. Escenario de ataque #4*

Los sistemas SMART TV permiten navegar como si fuera un ordenador a páginas reconocidas como *Facebook, Hotmail, Twitter, plataformas bancarias.* El usuario ingresa la información solicitada por la plataforma para acceder a estas cuentas por medio de un menú que posibilita el ingreso de datos como el nombre de usuario, contraseña permitiendo guardar estos datos para futuros accesos.

El hacker puede introducirse y usurpar toda esta información para posterior uso delictivo logrando suplantar al usuario para efectuar compras electrónicas u otras transacciones. Estos tipos de ataques son conocidos como *DNS poisoning y drive by download*, las cuales demuestran cómo las vulnerabilidades pueden ser combinadas para *conseguir credenciales de usuario local, el historial de búsqueda, caché, cookies y la contraseña inalámbrica.*

*E. Escenario de ataque #5*

En general, los sistemas SMART TV son sistemas completos que contiene numerosas funciones aparte de la ya mencionadas pero también, cuenta con distintos puertos de entrada y salida como *HDMI y puertos USB 3.0,* en la cual se pueden conectar de manera sencilla los dispositivos de almacenamientos a través de estos puertos de entrada siendo reconocidos por el medio de manera rápida e instantánea sin ninguna restricción de seguridad.

Este sistema reconoce los diferentes formatos que pueden ser utilizados por el TELEVISOR la cual es una acción autónoma. Un hacker puede ingresar y visualizar los distintos archivos que contenga uno de estos medios de almacenamiento

conectados al sistema, sustraer la información importante o también contaminarlos por medio de un virus.

## VI. Conclusiones

No debemos ignorar que sin lugar a dudas veremos en los próximos años más de estas investigaciones y gradualmente nos encontraremos con ataques como *troyanos*, *spyware*, *adware*, entre otras amenazas a estas plataformas. Estos TELEVISORES con sistemas SMART TV tienen prácticamente los mismos vectores de ataques que los teléfonos inteligentes.

Si para el año 2013 se *detectaron 35.000 muestras maliciosas* y solo en el primer semestre del 2013 se registraron unas *47.000, 99% de ellas destinados al sistema operativo Android*, que podemos esperar para esta tecnología SMART TV la cual esta apenas empezando a crecer y se evidencia para el *año 2017 un estimado de ventas de unos 220 millones de Smart TV, cifra que sube desde los 54 millones que se prevé que serán vendidos este 2014*, según los últimos informes de Informa Telecoms & Media sobre televisiones inteligentes.

Así, el 31% de los hogares a nivel mundial tendrán al menos una televisión de este tipo en el plazo de 5 años, según informa, con una penetración que será mucho mayor en *América del Norte (63%) y Europa Occidental (64%).*

Ya sabemos que vendrán ataques en el futuro mediante este nuevo sistema ya que es muy atractivo para los hackers que los TELEVISORES tengan cámaras y micrófonos incorporados despertando el interés para los futuros hacker de este sistema.

Esperemos que estos sistemas con las nuevas series que vengan tengan, un nivel de seguridad óptima y fácil de usar para un usuario normal y que sea interactivo con un mecanismo informativo donde recalque la importancia de tener su *SMART TV seguro y libre de virus, gusanos y troyanos.*

## REFERENCIAS

[1] Eduard Kovacs. (2013, Agosto). Los expertos advierten que los Smart TVs de Samsung pueden ser secuestrados. [Online]. Disponible: http://news.softpedia.es/Los-expertos-advierten-que-los-Smart-TVs-de-Samsung-puedes-ser-secuestrados-373105.html

[2] (Marketing Directo). (2012, Noviembre). Las ventas de Smart TV superarán los 50 millones a nivel mundial pero la mayoría se quedarán sin conectar. [Online].Disponible: http://www.marketingdirecto.com/actualidad/medios/las-ventas-de-smart-tv-superaran-los-50-millones-a-nivel-mundial-pero-la-mayoria-se-quedaran-sin-conectar/

[3] Pamela Carrasco. (2013, Noviembre). Ataques a smartphones amenazan a usuarios latinoamericanos" Articulo. [Online].Disponible: http://infosurhoy.com/es/articles/saii/features/main/2013/11/15/feature-02?source=most_commented

[4] Development Guide Samsung. (2014, Enero). "Development Guidance for Multi-Application" Articulo. [Online].Disponible: http://www.samsungdforum.com/Guide/d33/index.html#about-document

**Autor**

Luis Daniel Medina Diaz Granados
Ingeniero de Sistemas
Lider QA Certificate International Software Testing
2014