



Masterhacks - La firma de seguridad Check Point Software Technologies, informó que los subtítulos de películas que se ven por medio de Popcorn Time y servicios similares, pueden infectar de virus al ordenador.

Se identificó una vulnerabilidad que podría permitir a los hackers tomar el control del dispositivo por medio de un código dañino que se inserta en los archivos de subtítulos. La vulnerabilidad se identificó en varias plataformas de streaming, lo que pone en peligro a más de 200 millones de usuarios.

La amenaza se encuentra en los sitios web que los usuarios utilizan para descargar los subtítulos en varios idiomas.

«A diferencia de otros esquemas tradicionales de los ciberataques, los cuales tanto las firmas de seguridad como los usuarios conocen, los subtítulos de películas se perciben como archivos de texto benignos», explicó Check Point en su blog.

«Esto significa que los usuarios, los antivirus y otras soluciones de seguridad aprueban los archivos sin siquiera intentar evaluar su naturaleza real, dejando así a millones de usuarios expuestos a este riesgo», agregó.

La empresa identificó a Popcorn Time, VLC, Kodi y Stremio como algunos de los servicios afectados por la vulnerabilidad, pero cree que problemas parecidos pueden presentarse en otros software.

VLC, Kodi y Stremio afirman ya haber arreglado el problema, por lo que lanzaron versiones actualizadas disponibles para su descarga. Por otro lado, Popcorn ya solucionó el problema, pero aún no ha lanzado la descarga en el sitio oficial.

«Check Point ha exagerado esto de manera significativa», dijo Keith Herrington, representante de XMBC, a CNET. «Es muy raro que descargues un subtítulo en un archivo zip, y cualquier sitio de subtítulos decente deberían evaluarlos por cosas raras como éstas. Y aun cuando tengas acceso al sistema de archivos, no puedes ejecutar el código, que es lo que



necesita el malware», agregó Keith, creador de Kodi.

«Sin la capacidad de ejecutar el código, es muy pero muy difícil para cualquiera perpetrar algún daño», puntualizó.