Teslacrypt, El Ransomware Que Se Dirige A Los Gamers

El Ransomware es una de las últimas tácticas utilizadas por los ciberdelincuentes para obtener dinero de los usuarios. **CryptoLocker** llegó a los titulares el año pasado, la encriptación de los archivos en las máquinas infectadas hasta que se paga un rescate. Ahora, la misma idea se ha extendido al mundo de los juegos gracias a **Teslacrypt**.

Teslacrypt funciona de la misma manera que CryptoLocker, pero su razón de ser es buscar los juegos y descargar el contenido para las docenas de títulos populares y exigir el rescate por estos. Hasta que las víctimas pagan hasta $500 USD en Bitcoins, o hacer un pago $1,000 USD por PayPal, de lo contrario no habrá manera de acceder a los juegos.

A pesar de las similitudes con CryptoLocker, analistas de seguridad en Bromium dicen que el malware proviene de un grupo diferente de los cibercriminales y no comparte ningún código que los relacionen. Las infecciones vienen a través de un sitio de entretenimiento comprometido que utiliza una vulnerabilidad de Flash para redirigir los visitantes. **El sitio está basado en WordPress**, Bromium dice que podría haber sido comprometida utilizando cualquiera de una serie de exploits.

Una vez que el ordenador ha sido infectado, el malware comienza una búsqueda de 185 tipos de diferentes archivos, más de la mitad de los cuales están asociados con los juegos. En la lista de títulos específicos se encuentran Call of Duty, Half-Life 2 y Fallout 3, así como juegos en línea como World of Warcraft y títulos de Steam.

Vadim Kotov, de Bromium Labs dijo:

> *La extensión de los archivos son el blanco. Concretamente se trata de los datos de usuario de perfil, partidas guardadas, mapas, mods etc. A menudo no es posible restaurar este tipo de datos incluso después de volver a instalar un juego a través de Steam.*

Mientras **CryptoLocker fue crackeado** para que las víctimas pudieran descifrar sus archivos sin tener que pagar un rescate, esto todavía tiene que esperar para que sea posible con **Telsacrypt**.