



Malware Shlayer afecta a uno de cada 10 usuarios de MacOS

Una campaña de troyanos que intenta engañar a los usuarios de MacOS para hacer que descarguen software malicioso, sigue siendo el malware más común que se encuentran los usuarios de Mac.

El malware Shlayer apareció por primera vez a inicios de 2018, y se utiliza principalmente para instalar adware malicioso en los sistemas de los usuarios, con la intención de generar ingresos a partir de anuncios emergentes y enlaces que aparecen implacablemente en el navegador de la víctima.

A dos años de eso, las cifras de [Kaspersky Lab](#) revelan que el malware se ha dirigido a más de uno de cada diez usuarios de MacOS, por lo que es la amenaza de malware para MacOS más extendida.

El método clave de distribución de Shlayer se da por medio de falsas actualizaciones de Flash que se han infiltrado en miles de sitios web.

Se encuentra por lo general en sitios web que permiten a los usuarios transmitir ilegalmente programas de televisión y eventos deportivos, y a menudo dicen al usuario que deben descargar una actualización Flash falsa para ver su contenido elegido. Instalar esto es lo que permite que Shlayer llegue al sistema.

El malware también se ha distribuido por medio de sitios web legítimos, con enlaces a sitios web que descargan el malware en los sistemas de los usuarios de Apple que se encuentran ocultos en las notas al pie de los artículos de Wikipedia y descripciones de videos de YouTube. Los investigadores han descubierto alrededor de 700 dominios diferentes que se vinculan a una variedad de sitios web legítimos.

Los usuarios de todo el mundo han sido víctimas de los ataques de Shlayer, con el mayor número de víctimas en Estados Unidos, Alemania, Francia, Reino Unido, y demuestra que los usuarios de MacOS no son invulnerables al malware, como a veces se afirma. Mientras tanto, la campaña no muestra signos de desaceleración mientras genera ingresos para sus operadores.



«La plataforma MacOS es una buena fuente de ingresos para los ciberdelincuentes, que buscan constantemente nuevas formas de engañar a los usuarios y utilizan activamente técnicas de ingeniería social para difundir su malware. Este caso demuestra que tales amenazas pueden encontrarse incluso en sitios legítimos», dijo Anton Ivanov, analista de seguridad de Kaspersky Lab.

Para evitar ser víctimas de Shlayer y otros programas maliciosos, los investigadores recomiendan que los usuarios tengan cuidado y solo instalen software y actualizaciones de fuentes confiables.

«Afortunadamente para los usuarios de MacOS, las amenazas más extendidas que se dirigen a MacOS actualmente giran en torno a alimentar publicidad ilícita en lugar de algo más peligroso, como robar datos financieros», dijo Ivanov.