

La criptominería se posiciona como una amenaza de seguridad importante

Check Point ha vuelto a actualizar su Índice de Impacto Global de Amenazas, esta vez con los datos de octubre.

Según su clasificación, **la principal amenaza sigue siendo el *malvertising* RoughTed, a quien sigue el *ransomware* Locky.**

El top 3 cuenta con una novedad, que es la entrada como tercer amenaza más frecuente de **Seamless traffic redirector**. Como su propio nombre indica, su objetivo es redireccionar a sus víctimas a una web maliciosa de forma silenciosa e infectarlas por *exploit kit* para descargar *malware* en los equipos.

Otra novedad tiene que ver con el incremento del *malware* de minería de criptomonedas. De hecho, a lo largo de octubre han sido muchas las empresas que han sufrido la acción de **CoinHive**. Este criptomintero que busca minar la divisa Monero sin pedir permiso al usuario se sitúa como la **sexta amenaza más importante** del mes. Desde Check Point destacan que CoinHive usa una gran cantidad de recursos del equipo afectado.

“La aparición de Seamless y CoinHive pone de manifiesto una vez más la necesidad de tecnologías avanzadas de prevención de amenazas para proteger las redes contra los ciberdelincuentes”, indica Maya Horowitz, directora del grupo de Inteligencia de Amenazas de Check Point.

“La criptominería es un nuevo actor silencioso pero muy importante en el panorama del *malware*”, añade Horowitz. Es una amenaza “que permite a los ciberdelincuentes obtener grandes ingresos mientras que los *endpoints* y las redes de las víctimas sufren una disminución de su rendimiento”.