El equipo de investigación de Microsoft Defender ATP ha compartido sus hallazgos sobre una nueva variante de malware que roba criptomonedas y que ya ha infectado alrededor de 80,000 computadoras.

Este 26 de noviembre, los analistas de seguridad de Microsoft, revelaron que el malware, denominado como Dexphot, ya había infectado cerca de 80 mil dispositivos desde octubre de 2018, llegando a su punto máximo en el mes de junio de este año.

Según los informes, el código malicioso secuestra los procesos legítimos del sistema para disfrazar su actividad nefasta, con el objetivo final de ejecutar un minero de criptomonedas en el dispositivo infectado.

Cuando los usuarios infectados intentan eliminar el malware, los servicios de monitoreo y las tareas programadas desencadenarán la reinfección.

> *«Dexphot no es el tipo de ataque que genera la atención de los medios convencionales; es una de las innumerables campañas de malware que están activas en un momento dado. Su objetivo es muy común en los círculos cibercriminales: instalar un minero de monedas que silenciosamente roba recursos informáticos y genera ingresos para los atacantes»,* dice el informe.

El malware Dexphot es similar en muchos aspectos al código malicioso recientemente descubierto en los archivos de audio WAV. Este tipo de campaña de malware permite a los piratas informáticos desplegar mineros de CPU en el dispositivo de la víctima, robando recursos de procesamiento y generando miles de dólares al mes a partir de la criptomoneda minera.

Este tipo de cargas de malware son cada vez más populares entre los hackers, ya que proporcionan un beneficio financiero mientras operan en segundo plano sin el conocimiento del usuario. A este ataque se le conoce como cryptojacking.