Un grupo de hackers lanzó una nueva campaña de cryptojacking el 24 de noviembre, escaneando hasta 59 mil redes IP para encontrar plataformas Docker que tienen puntos finales API expuestos en línea, según informó ZDNet.

La campaña está dirigida a instancias vulnerables de Docker para implementar malware criptográfico para generar fondos para el grupo de piratería mediante la minería de Monero.

Este problema de escaneo masivo fue descubierto por primera vez por la compañía estadounidense de seguridad Bad Packets LLC, el pasado 25 de noviembre.

Troy Mursch, director de investigación y cofundador de Bad Packets LLC, dijo que la actividad de explotación dirigida a las instancias expuestas de Docker no es nueva y ocurre muy frecuentemente.

En marzo de 2018, la empresa de ciberseguridad Imperva informó que 400 servidores Docker, a los que se podía acceder remotamente por medio de una debilidad API, contenían programas de minería Monero.

Musrch, quien supuestamente descubrió la campaña, informó a ZDNet que una vez que el grupo de hackers identifica un host expuesto, los atacantes implementan el punto final API para iniciar un contenedor Alpine Linux OS para ejecutar un comando que descarga y ejecuta un script Bash desde el servidor de los atacantes. Luego, el script instala un *«minero de criptomonedas XMRRig clásico».*

Según las declaraciones, los piratas informáticos extrajeron 14.82 XMR en los dos días que la campaña de orientación de Docker ha estado activa, lo que equivale a 835 dólares.

Docker es una herramienta para desarrolladores diseñada para simplificar los procesos de creación, implementación y ejecución de software mediante el uso de contenedores. Los contenedores permiten a los desarrolladores empaquetar una aplicación con todas las partes requeridas, como bibliotecas y otras dependencias.

Para evitar la vulnerabilidad detectada, Mursch recomienda que los usuarios que ejecutan instancias de Docker comprueben inmediatamente si están exponiendo sus puntos finales API en Internet, que cierren los puertos y finalicen los contenedores en ejecución no reconocidos.

Por otro lado, el pasado 25 de noviembre, la plataforma de intercambio BitBay, anunció que la plataforma eliminará Monero debido a preocupaciones de lavado de dinero. BitBay sigue otros intercambios como OKEx, que han eliminado la criptomoneda para cumplir con las pautas establecidas por el Grupo de Acción Financiera.