Docker ha ganado popularidad como servicio para empaquetar e implementar aplicaciones de software, pero los hackers también han estado aprovechando esto para buscar formas de apuntar a puntos finales de API expuestos creando imágenes con malware para facilitar ataques distribuidos de denegación de servicio (DDoS) y minar criptomonedas.

Según un informe publicado por el equipo de inteligencia de amenazas de Unit 42, de Palo Alto Networks, el propósito de estas imágenes de Docker es generar fondos mediante la implementación de un minero de criptomonedas utilizando contenedores Docker y aprovechando el repositorio Docker Hub para distribuir dichas imágenes.

> *«Los contenedores Docker proporcionan una forma conveniente de empaquetar software, lo cual es evidente por su creciente tasa de adopción. Esto, combinado con la extracción de monedas, facilita que un actor malintencionado distribuya sus imágenes a cualquier máquina que admita Docker e instantáneamente comienza a usar sus recursos informáticos para el criptojacking»*, dijeron los investigadores.

Docker es una conocida solución de plataforma como servicio (Paas) para Linux y Windows, que permite a los desarrolladores implementar, probar y empaquetar sus aplicaciones en un entorno virtual contenido, de una forma que aísla el servicio del sistema host.

La cuenta, ahora eliminada de Docker Hub, llamada *«azurenql»*, consistía en ocho repositorios que albergaban seis imágenes maliciosas capaces de extraer Monero, una criptomoneda centrada en la privacidad.

El autor del malware detrás de las imágenes utilizó un script de Python para activar la operación de criptojacking y aprovechó las herramientas de anonimato de la red como ProxyChains y Tor para evadir la detección de la red.

El código de extracción de monedas dentro de la imagen luego explotó el poder de procesamiento de los sistemas infectados para extraer los bloques.

Las imágenes alojadas en esta cuenta se extrajeron colectivamente más de 2 millones de veces desde el inicio de la campaña en octubre de 2019, con una de las ID de billetera utilizadas para generar más de 525.38 XMR, equivalentes a unos 36 mil dólares.

Servidores Dockers expuestos con malware DDoS

Además, en una nueva operación de escaneo masivo detectada por investigadores de Trend Micro, los servidores Docker desprotegidos están siendo atacados con al menos dos tipos diferentes de malware, XOR DDoS y Kaiji, para recopilar información del sistema y llevar a cabo ataques DDoS.

> *«Los atacantes generalmente usaban botnets para realizar ataques de fuerza bruta después de buscar puertos abiertos de Secure Shell (SSH) y Telnet. Ahora, también están buscando servidores Docker con puertos expuestos (2375)»,* dijeron los investigadores.

Cabe mencionar que tanto XOR DDoS como Kaiji son troyanos de Linux conocidos por su capacidad para realizar ataques DDoS, además de estar escritos completamente desde cero con el lenguaje de programación Go para apuntar a dispositivos IoT a través de SSH.

La variedad de malware XOR DDoS funciona mediante la búsqueda de hosts con puertos API Docker expuestos, seguido del envío de un comando para enumerar todos los contenedores alojados en el servidor de destino, y posteriormente comprometerlos con el malware XOR DDoS.

Del mismo modo, el malware Kaiji escanea Internet en busca de hosts con el puerto expuesto 2375 para implementar un contenedor ARM falso (linux_arm) que ejecuta el binario Kaiji.

> *«Mientras que el ataque XOR DDoS se infiltró en el servidor Docker para infectar todos los contenedores alojados en él, el ataque Kaiji despliega su propio contenedor que albergará su malware DDoS»,* dijeron los investigadores.

Además, las dos piezas de malware recopilan detalles como nombres de dominio, velocidades de red, identificadores de procesos en ejecución e información de CPU y red que se requieren para montar un ataque DDoS.

> *«Los actores de amenazas detrás de las variantes de malware actualizan de forma constante sus creaciones con nuevas capacidades para que puedan desplegar sus ataques contra otros puntos de entrada»,* agregaron los investigadores.
>
> *«Como son relativamente convenientes para implementar en la nube, los servidores Docker se están convirtiendo en una opción cada vez más popular para las empresas. Sin embargo, estos también los convierten en un objetivo atractivo para los ciberdelincuentes que buscan constantemente sistemas que puedan explotar».*

Es recomendable que los usuarios y organizaciones que ejecutan instancias Docker comprueben lo antes posible si exponen los puntos finales API en Internet, cierren los puertos y se apeguen a las mejores prácticas recomendadas.