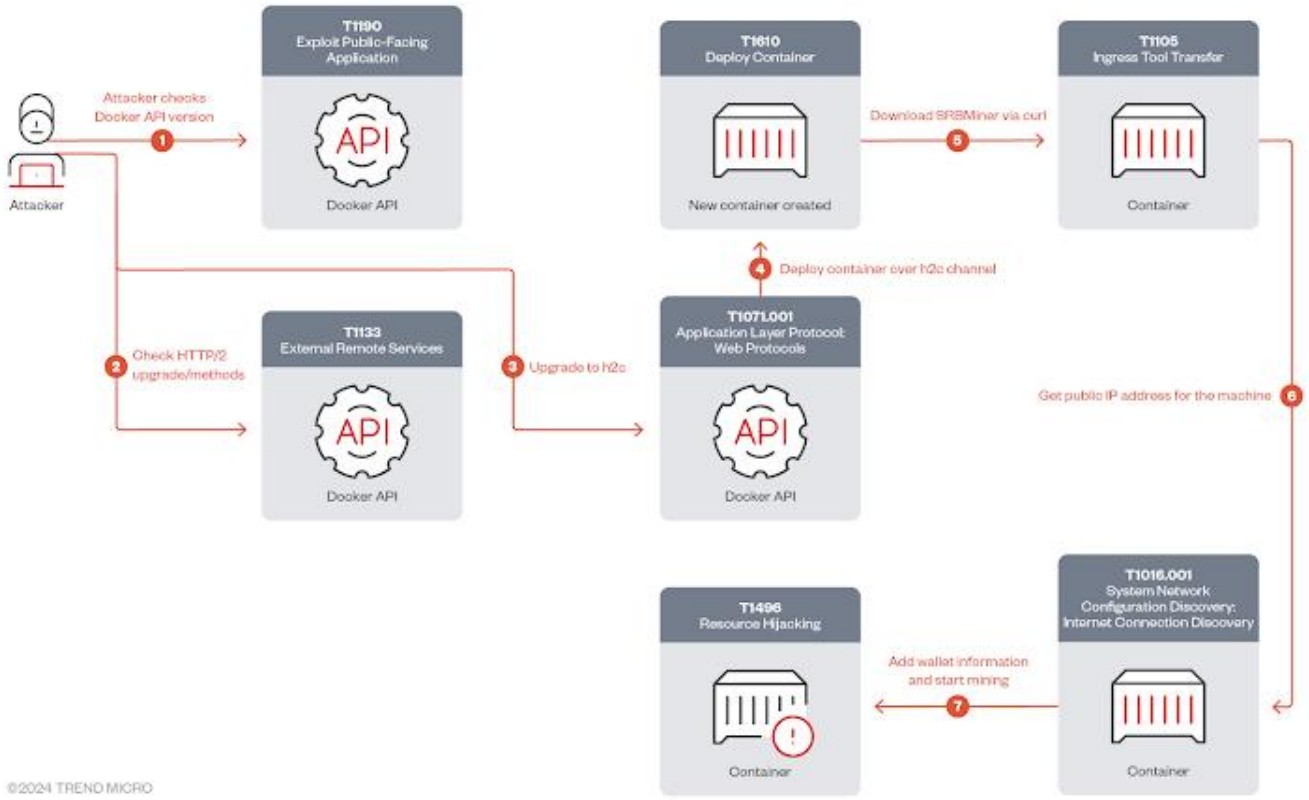
Actores maliciosos han sido detectados atacando servidores de la API remota de Docker para implementar el minero de criptomonedas SRBMiner en instancias comprometidas, según un nuevo informe de Trend Micro.

> *«En este ataque, el atacante utilizó el protocolo gRPC sobre h2c para evadir las soluciones de seguridad y llevar a cabo sus operaciones de minería de criptomonedas en el host de Docker»*, señalaron los investigadores Abdelrahman Esmail y Sunil Bharti en un informe técnico publicado hoy.
>
> *«El atacante primero comprobó la disponibilidad y versión de la API de Docker, luego realizó solicitudes de actualización para gRPC/h2c y usó métodos gRPC para manipular las funciones de Docker».*

El ataque comienza con un proceso de reconocimiento en el que el atacante busca hosts de la API de Docker expuestos públicamente y comprueba la posibilidad de actualizar el protocolo HTTP/2, con el objetivo de realizar una solicitud de conexión al protocolo h2c (HTTP/2 sin cifrado TLS).

Posteriormente, el atacante verifica los métodos gRPC que permiten realizar varias tareas relacionadas con la administración de entornos Docker, como verificaciones de estado, sincronización de archivos, autenticación, gestión de secretos y reenvío de SSH.

Una vez que el servidor procesa la solicitud de actualización de conexión, se envía una petición gRPC *«/moby.buildkit.v1.Control/Solve»* para crear un contenedor y utilizarlo para minar la criptomoneda XRP usando la carga maliciosa de SRBMiner, alojada en GitHub.



> *«En este caso, el atacante aprovechó el protocolo gRPC sobre h2c, logrando eludir varias capas de seguridad para desplegar el minero de criptomonedas SRBMiner en el host de Docker y realizar minería de XRP de forma ilícita»*, explicaron los investigadores.

Este informe se publica mientras la compañía de ciberseguridad también ha observado que atacantes están explotando servidores expuestos de la API remota de Docker para distribuir el malware perfctl. La campaña consiste en buscar dichos servidores, crear un contenedor Docker con la imagen «ubuntu:mantic-20240405» y ejecutar una carga útil codificada en Base64.

El script shell, además de verificar y eliminar instancias duplicadas de sí mismo, genera un

script bash que incluye otra carga útil codificada en Base64. Esta última descarga un archivo binario malicioso disfrazado como un archivo PHP («avatar.php») y entrega una carga maliciosa llamada httpd, en línea con un informe reciente de Aqua.

Se recomienda a los usuarios proteger los servidores de API remota de Docker implementando controles de acceso sólidos y mecanismos de autenticación para evitar accesos no autorizados, monitoreando cualquier actividad sospechosa e implementando las mejores prácticas de seguridad para contenedores.