Los investigadores de seguridad informática han descubierto una infraestructura de ataque que se está utilizando como parte de una *«campaña potencialmente masiva»* contra entornos nativos de la nube.

> *«Esta infraestructura se encuentra en las primeras etapas de pruebas y despliegue, y consiste principalmente en un gusano en la nube agresivo diseñado para aprovechar las APIs expuestas de JupyterLab y Docker con el fin de desplegar el malware Tsunami, robar credenciales en la nube, secuestrar recursos e infectar aún más mediante el gusano»,* declaró Aqua, una empresa especializada en seguridad en la nube.

La actividad, denominada Silentbob en referencia a un dominio AnonDNS creado por el atacante, se cree que está vinculada al infame grupo de criptominería conocido como TeamTNT, debido a similitudes en tácticas, técnicas y procedimientos (TTPs). Sin embargo, no se descarta la posibilidad de la participación de un *«imitador avanzado».*

La investigación de Aqua fue impulsada por un ataque dirigido a su sistema señuelo a principios de junio de 2023, lo que llevó al descubrimiento de cuatro imágenes de contenedores maliciosos diseñadas para detectar instancias expuestas de Docker y Jupyter Lab, y desplegar un minero de criptomonedas junto con una puerta trasera llamada Tsunami.

Esto se logra mediante un script de shell programado para ejecutarse al iniciar el contenedor, el cual utiliza el escáner ZGrab basado en Go para localizar servidores mal configurados. Docker ha eliminado las imágenes del registro público. A continuación, se presenta la lista de imágenes:

- shanidmk/jltest2 (44 descargas)
- shanidmk/jltest (8 descargas)
- shanidmk/sysapp (11 descargas)
- shanidmk/blob (29 descargas)

Además de ejecutar un minero de criptomonedas en el equipo infectado, la imagen shanidmk/sysapp está configurada para descargar y ejecutar otros binarios adicionales, los cuales Aqua ha identificado como posibles respaldos de criptomineros o el malware Tsunami.

También se descarga por el contenedor un archivo llamado *«aws.sh.txt»*, un script que probablemente está diseñado para realizar un escaneo sistemático del entorno en busca de claves de AWS para su posterior extracción.

Según Aqua, se encontraron 51 servidores con instancias expuestas de JupyterLab en el mundo real, todos los cuales han sido objeto de explotación activa o muestran indicios de haber sido explotados por actores de amenazas. Esto incluye un *«ataque manual en vivo a uno de los servidores que utilizó masscan para escanear APIs de Docker expuestas».*

> *«En un principio, el atacante identifica un servidor mal configurado (ya sea una API de Docker o JupyterLab) y despliega un contenedor o utiliza la Interfaz de Línea de Comandos (CLI) para escanear e identificar posibles víctimas adicionales»,* indicaron los investigadores de seguridad Ofek Itach y Assaf Morag.

> *«Este proceso está diseñado para propagar el malware a un número cada vez mayor de servidores. La carga secundaria de este ataque incluye un minero de criptomonedas y una puerta trasera, siendo esta última la que utiliza el malware Tsunami como su herramienta preferida».*