Los expertos en ciberseguridad han detectado un nuevo ataque que aprovecha configuraciones erróneas en Apache Hadoop y Flink para desplegar mineros de criptomonedas en entornos específicos.

> *«Este ataque resulta especialmente intrigante debido al uso de empaquetadores y rootkits por parte del atacante para ocultar el malware. El malware borra el contenido de directorios específicos y modifica configuraciones del sistema para evitar su detección»,* indicaron los investigadores de seguridad de Aqua, Nitzan Yaakov y Assaf Morag, en un análisis publicado a principios de esta semana.

La cadena de infección dirigida a Hadoop explota una configuración incorrecta en el ResourceManager de YARN (Yet Another Resource Negotiator), encargado de rastrear recursos en un clúster y programar aplicaciones.

En concreto, la configuración errónea puede ser aprovechada por un actor de amenazas remoto y no autenticado para ejecutar código arbitrario mediante una solicitud HTTP manipulada, sujeta a los privilegios del usuario en el nodo donde se ejecuta el código.

Los ataques dirigidos a Apache Flink, de manera similar, se centran en una configuración incorrecta que permite a un atacante remoto lograr la ejecución de código sin autenticación.

Estas configuraciones incorrectas no son novedosas y han sido explotadas en el pasado por grupos con motivaciones financieras, como TeamTNT, conocido por dirigirse a entornos de Docker y Kubernetes con el objetivo de llevar a cabo cripto-minería y otras actividades maliciosas.

No obstante, lo que destaca en este último conjunto de ataques es el uso de rootkits para ocultar los procesos de cripto-minería después de obtener un punto de apoyo inicial en las aplicaciones de Hadoop y Flink.

> *«El atacante envía una solicitud no autenticada para implementar una nueva aplicación. El atacante puede ejecutar un código remoto enviando una solicitud POST a YARN, solicitando lanzar la nueva aplicación con el comando del atacante»,* explicaron los investigadores.

El comando está diseñado para limpiar el directorio /tmp de todo el contenido existente, recuperar un archivo llamado «dca» desde un servidor remoto y ejecutarlo, seguido de la eliminación de todos los archivos en el directorio /tmp una vez más.

La carga útil ejecutada es un binario ELF empaquetado que actúa como un descargador para recuperar dos rootkits y un binario de minero de criptomonedas Monero. Es relevante destacar que varios adversarios, incluido Kinsing, han optado por utilizar rootkits para ocultar la presencia del proceso de minería.

Para garantizar la persistencia, se crea una tarea cron para descargar y ejecutar un script de shell que implementa el binario 'dca'. Un análisis adicional de la infraestructura del actor de amenazas revela que el servidor de preparación utilizado para recuperar el descargador se registró el 31 de octubre de 2023.

Como medidas de mitigación, se recomienda que las organizaciones implementen soluciones de seguridad basadas en agentes para detectar cripto-mineros, rootkits, binarios obfuscados o empaquetados, así como otros comportamientos sospechosos en tiempo de ejecución.