Un grupo de hackers motivado financieramente está rastreando activamente Internet en busca de instancias de Apache NiFi desprotegidas, con el fin de instalar de forma encubierta un minero de criptomonedas y facilitar el movimiento lateral.

Los hallazgos provienen del SANS Internet Storm Center (ISC), que detectó un aumentoen las solicitudes HTTP de «/nifi» el 19 de mayo de 2023.

> *«La persistencia se logra por medio de procesadores temporizados o entradas a cron. El script de ataque no se guarda en el sistema. Los scripts de ataque solo se guardan en la memoria»,* dijo el Dr. Johannes Ullrich, decano de investigación del SANS Technology Institute.

Una configuración de honeypot permitió al ISC determinar que el punto de apoyo inicial está armado para lanzar un script de shell que elimina el archivo *«/var/log/syslog»,* desactiva el firewall y finaliza las herramientas de criptominería de la competencia, antes de descargar y ejecutar el malware Kinsing desde un servidor remoto.

Cabe mencionar que Kinsing tiene un historial de aprovechamiento de vulnerabilidades divulgadas públicamente en aplicaciones web de acceso público para llevar a cabo sus ataques.

En septiembre de 2022, Trend Micro detalló una cadena de ataque idéntica que usó vulnerabilidades antiguas de Oracle WebLogic Server (CVE-2020-14882 y CVE-2020-14883) para entregar el malware de minería de criptomonedas.

Los ataques seleccionados montados por el mismo actor de amenazas contra servidores NiFi expuestos también implican la ejecución de un segundo script de shell que está diseñado para recopilar claves SSH del host infectado para conectarse a otros sistemas dentro de la organización de la víctima.

Un indicador notable de la campaña en curso es que las actividades reales de ataque y

escaneo se llevan a cabo por medio de la dirección IP 109.207.200[.]43 contra el puerto 8080 y el puerto 8443/TCP.

> *«Debido a su uso como plataforma de procesamiento de datos, los servidores NiFi por lo general tienen acceso a datos críticos para el negocio. Los servidores NiFi son probablemente objetivos atractivos, ya que están configurados con CPU más grandes para admitir tareas de transformación de datos. El ataque es trivial si el servidor NiFi no está protegido*«, dijo SAN ISC.