Los actores de amenazas están focalizando sus ataques en servidores mal configurados y vulnerables que ejecutan Apache Hadoop YARN, Docker, Atlassian Confluence y servicios Redis, como parte de una nueva campaña de malware diseñada para distribuir un minero de criptomonedas y establecer un shell inverso para acceso remoto persistente.

Según el informe compartido por el investigador de seguridad de Cado, Matt Muir, los atacantes utilizan estas herramientas para desplegar código de explotación, aprovechando configuraciones erróneas comunes y explotando vulnerabilidades de día cero para llevar a cabo ataques de Ejecución de Código Remoto (RCE) e infectar nuevos hosts.

La compañía de seguridad en la nube ha denominado a esta actividad como *«Spinning YARN»*, con similitudes con los ataques en la nube atribuidos a TeamTNT, WatchDog y un grupo denominado Kiss-a-dog.

La secuencia comienza con la implementación de cuatro nuevas cargas útiles Golang, capaces de identificar y explotar automáticamente hosts susceptibles de Confluence, Docker, Hadoop YARN y Redis. Las utilidades propagadoras utilizan masscan o pnscan para buscar estos servicios.

Muir explicó que, para comprometer Docker, los atacantes generan un contenedor y escapan de él hacia el host subyacente.

El acceso inicial allana el camino para desplegar herramientas adicionales que instalan rootkits como libprocesshider y diamorphine para ocultar procesos maliciosos. Además, se introduce la utilidad de shell inverso de código abierto Platypus y, finalmente, se ejecuta el minero XMRig.

> *«Es evidente que los atacantes están invirtiendo un tiempo considerable para comprender los tipos de servicios expuestos a la web en entornos en la nube, manteniéndose actualizados sobre las vulnerabilidades informadas y utilizando este conocimiento para infiltrarse en los entornos objetivo»,* señaló la empresa.

Este desarrollo coincide con la revelación de Uptycs sobre la explotación de fallos de seguridad conocidos en Apache Log4j (CVE-2021-44228) y Atlassian Confluence Server y Data Center (CVE-2022-26134) por parte de la banda 8220 Gang. Esto forma parte de una ola de ataques dirigidos a la infraestructura en la nube desde mayo de 2023 hasta febrero de 2024.

Los investigadores de seguridad Tejaswini Sandapolla y Shilpesh Trivedi afirmaron que el grupo identifica posibles puntos de entrada en sistemas en la nube aprovechando escaneos de internet en busca de aplicaciones vulnerables. Luego, explotan vulnerabilidades no parcheadas para obtener acceso no autorizado.

Una vez dentro, despliegan técnicas avanzadas de evasión, demostrando un profundo conocimiento sobre cómo navegar y manipular entornos en la nube. Esto incluye desactivar la aplicación de medidas de seguridad, modificar reglas de firewall y eliminar servicios de seguridad en la nube para garantizar que sus actividades maliciosas permanezcan indetectadas.

Estos ataques, dirigidos tanto a hosts Windows como Linux, buscan implementar un minero de criptomonedas, pero no antes de seguir una serie de pasos que priorizan el sigilo y la evasión.

Este escenario también sigue a la utilización abusiva de servicios en la nube destinados principalmente a soluciones de inteligencia artificial (IA) para distribuir mineros de criptomonedas y alojar malware.

> *«Con la necesidad de acceso a grandes cantidades de potencia de procesamiento de GPU tanto para la minería como para la IA, existe cierta transferibilidad a sus entornos de hardware base»,* señaló HiddenLayer el año pasado.

Cado, en su Informe de Hallazgos de Amenazas en la Nube de H2 2023, destacó que los actores de amenazas están enfocando cada vez más sus ataques en servicios en la nube que

requieren conocimientos técnicos especializados para ser explotados, y que el cripto-minado ya no es el único motivo.

> *«Con el descubrimiento de nuevas variantes de ransomware para Linux, como Abyss Locker, observamos una tendencia preocupante de ransomware en sistemas Linux y ESXi. La infraestructura en la nube y Linux ahora está sujeta a una variedad más amplia de ataques»,* advirtió.