Un grupo de piratas informáticos en la nube rastreado como 8220, actualizó su conjunto de herramientas de malware para comprometer los servidores Linux con el objetivo de instalar criptomineros como parte de una campaña de larga duración.

> *«Las actualizaciones incluyen el despliegue de nuevas versiones de un criptominero y un bot de IRC. El grupo ha actualizado activamente sus técnicas y cargas útiles durante el último año»,* dijo Microsoft Security Intelligence.

8220, activo desde principios de 2017, es un actor de amenazas de minería de Monero de habla china, llamado así por su preferencia para comunicarse con servidores de comando y control (C2) por medio del puerto 8220. También es el desarrollador de una herramienta llamada whatMiner, que ha sido cooptado por el grupo de hacking Rocke en sus ataques.

En julio de 2019, el equipo de seguridad en la nube de Alibaba descubrió un cambio adicional en las tácticas del adversario y señaló el uso de rootkits para ocultar el programa de minería. Dos años después, el grupo resurgió con variantes de la botnet IRC Tsunami y un minero personalizado *«PwnRig».*

Ahora, según Microsoft, se ha observado que la campaña más reciente que afecta a los sistema Linux i686 y x86_64 convierte en armas los exploits de ejecución remota de código para el Atlassian Confluence Server (CVE-2022-26134) y Oracle WebLogic (CVE-2019-2725) recientemente revelados para el acceso inicial.

Este paso es seguido por la recuperación de un cargador de malware desde un servidor remoto que está diseñado para eliminar el minero PwnRig y un bot de IRC, pero no antes de tomar medidas para evadir la detección borrando los archivos de registro y deshabilitando el software de seguridad y monitoreo en la nube.

Además de lograr la persistencia por medio de un trabajo cron, *«el cargador usa la herramienta de escaneo de puertos IP 'masscan' para encontrar otros servidores SSH en la red, y luego usa la herramienta de fuerza bruta SSH basada en GoLang 'spirit' para*

propagar», dijo Microsoft.

Los hallazgos se producen cuando Akamai reveló que la vulnerabilidad de Atlassian Confluence está siendo testigo de 20,000 intentos de explotación constantes por día que se lanzan desde aproximadamente 6000 IPs, frente a un pico de 100,000 inmediatamente después de la divulgación del error el 2 de junio de 2022. Se dice que el 67% de los ataques se originaron en Estados Unidos.

> *«A la cabeza, el comercio representa el 38% de la actividad de ataque, seguido por la alta tecnología y los servicios financieros, respectivamente. Estas tres verticales principales representan más del 75% de la actividad»*, dijo Chen Doysthman de Akamai.

Los ataques van desde sondeos de vulnerabilidad para determinar si el sistema de destino es susceptible a la inyección de malware, como web shells y criptomineros, dijo la compañía de seguridad en la nube.

> *«Lo que es particularmente preocupante es cuánto cambio hacia arriba ha obtenido este tipo de ataque en las últimas semanas. Como hemos visto con vulnerabilidades similares, es probable que este CVE-2022-26134 siga siendo explotado durante al menos los próximos dos años»,* agregó Doysthman.