El grupo de criptominería denominado 8220 se ha expandido en tamaño para abarcar hasta 30,000 hosts infectados, frente a los 2000 hosts en todo el mundo a mediados de 2021.

> *«8220 Gang es una de las muchas pandillas de crimeware poco calificadas que observamos continuamente que infectan hosts en la nube y operan una red de bots y mineros de criptomonedas por medio de vulnerabilidades conocidas y vectores de infección de fuerza bruta de acceso remoto»,* dijo Tom Hegel, de Sentinel One.

El crecimiento se ha visto impulsado por el uso de Linux y vulnerabilidades comunes de aplicaciones en la nube y configuraciones poco seguras para servicios como Docker, Apache WebLogic y Redis.

Activo desde inicios de 2017, el atacante de minería de Monero, de habla china, fue visto más recientemente apuntando a los sistemas Linux i686 y x86_64 mediante el armamento de una explotación de ejecución remota de código reciente para Atlassian Confluence Server (CVE-2022-26134) para eliminar la carga útil PwnRig del minero.

> *«Las víctimas no se identifican geográficamente, sino que simplemente se identifican por su acceso a Internet»,* dijo Hegel.

Además de ejecutar el minero de criptomonedas PwnRig, el script de infección también está diseñado para eliminar las herramientas de seguridad en la nube y llevar a cabo la fuerza bruta SSH por medio de una lista de 450 credenciales codificadas para propagarse lateralmente por medio de la red.

También se sabe que las versiones más nuevas del script emplean listas de bloqueo para

evitar comprometer hosts específicos, como servidores trampa que podrían señalar sus esfuerzos ilícitos.

El criptominero PwnRig, que se basa en el minero Monero de código abierto XMRig, también recibió actualizaciones propias, utilizando un subdominio falso del FBI con una dirección IP que apunta a un dominio legítimo del gobierno federal brasileño para crear una solicitud de grupo no autorizado y ocultar el destino real del dinero generado.

El aumento de las operaciones también se considera un intento de compensar la caída de los precios de las criptomonedas, sin mencionar que subraya una «batalla» intensificada para tomar el control de los sistemas de las víctimas de los grupos centrados en el criptojacking de la competencia.

> *«En los últimos años, 8220 Gang desarrolló lentamente sus scripts de infección de Linux simples pero efectivos para expandir una red de bots y un minero de criptomonedas ilícito. El grupo realizó cambios en las últimas semanas para expandir la botnet a casi 30,000 víctimas en todo el mundo»,* agregó Hegel.