Detectan ataques continuos de malware de criptominería automática mediante tácticas de evasión mejoradas

Autor: I. Stepanenko

Fecha: Monday 24th of January 2022 10:16:46 AM

Una campaña de minería de criptomonedas en curso ha mejorado su arsenal al mismo tiempo que agrega nuevas tácticas de evasión de defensa que permiten a los actores de amenazas ocultar las intrusiones y actuar bajo el radar, según una investigación publicada este miércoles.

Desde que se detectó por primera vez en 2019, hasta ahora se han registrado un total de 84 ataques contra sus servidores honeypot, cuatro de las cuales ocurrieron en 2021, según investigadores de DevSecOps y la compañía de seguridad en la nube Aqua Security, que han estado rastreando la operación del malware en los pasados tres años. Se han detectado 125 ataques en estado salvaje solo en el tercer trimestre de 2021, lo que indica que los ataques no se ralentizaron.

Los ataques iniciales involucraron la ejecución de un comando malicioso al ejecutar una

imagen básica llamada *«alpine:latest»*, que resultó en la descarga de un script de shell llamado *«autom.sh».*

> «Los adversarios comúnmente usan imágenes vanilla junto con comandos maliciosos para realizar sus ataques, porque la mayoría de las organizaciones confían en las imágenes oficiales y permiten su uso. A lo largo de los años, el comando malicioso que se agregó a la imagen oficial para llevar a cabo el ataque apenas ha cambiado. La principal diferencia es el servidor desde el que se descargó el script de shell autom.sh», dijeron los investigadores.

El script de shell inicia la secuencia de ataque, lo que permite al adversario crear una nueva cuenta de usuario con el nombre *«akay»* y actualizar sus privilegios a un usuario root, utilizando los comandos arbitrarios que se ejecutan en la máquina comprometida con el objetivo de extraer criptomonedas.

Aunque las primeras etapas de la campaña en 2019 no incluyeron técnicas especiales para ocultar la actividad minera, las versiones posteriores muestran las medidas extremas que sus desarrolladores han tomado para mantenerla invisible a la detección e inspección, la principal de ellas es la capacidad de deshabilitar los mecanismos de seguridad y recuperar un script de shell de minería ofuscado que se codificó en Base64 cinco veces para sortear las herramientas de seguridad.

Las campañas de malware llevadas a cabo para secuestrar computadoras para extraer criptomonedas han estado dominadas por múltiples actores de amenazas como Kinsing, que se ha encontrado escaneando Internet en busca de servidores Docker mal configurados para ingresar a los hosts desprotegidos e instalar una cepa de minero de criptomonedas previamente indocumentada.

Además de eso, se ha observado que un grupo de hacking llamado TeamTNT golpea servidores de base de datos Redis no seguros, instancias de Alibaba Elastic Computing

Service (ECS), API de Docker expuestas y clústeres de Kubernets vulnerables para ejecutar código malicioso con privilegios de root en los hosts de destino, además de implementar cargas útiles de minería de criptomonedas y ladrones de credenciales.

Además, las cuentas de Docker Hub comprometidas también se han empleado para alojar imágenes maliciosas que luego se utilizaron para distribuir mineros de criptomonedas.

En las últimas semanas, se ha abusado de las fallas de seguridad en la biblioteca de registro Log4j, así como las vulnerabilidades descubiertas recientemente en Atlassian Confluence, F5 BIG-IP, VMware vCenter y Oracle WebLogic Servers para apoderarse de las máquinas para extraer criptomonedas, un esquema conocido como cryptojacking.

A inicios del mes, el fabricante de dispositivos de almacenamiento conectado a la red (NAS) QNAP advirtió sobre el malware de minería de criptomonedas dirigido a sus dispositivos que podría ocupar alrededor del 50% del uso total de la CPU.

«Los mineros son una forma de bajo riesgo para que los ciberdelincuentes conviertan una vulnerabilidad en efectivo digital, y el mayor riesgo para su flujo de efectivo es que los mineros de la competencia descubran los mismos servidores vulnerables», dijo el investigador senior de amenazas de Sophos, Sean Gallagher, en un análisis de minería de Tor2Mine, que implica el uso de un script de PowerShell para deshabilitar la protección contra malware, ejecutar una carga útil de minero y recolectar las credenciales de Windows.

> «La campaña Autom ilustra que los atacantes se están volviendo más sofisticados, mejorando continuamente sus técnicas y su capacidad para evitar ser detectados por las soluciones de seguridad», dijeron los investigadores.

Para protegerse contra estas amenazas, se recomienda monitorear la actividad sospechosa del contenedor, realizar análisis dinámicos de imágenes y escanear de forma rutinaria los entornos en busca de problemas de configuración incorrecta.