LemonDuck, una botnet de minería de criptomonedas multiplataforma, apunta a Docker para extraer criptomonedas en sistemas Linux como parte de una campaña activa de malware.

> *«Ejecuta una operación de minería anónima mediante el uso de grupos de servidores proxy, que ocultan las direcciones de las billeteras. Evade la detección al apuntar al servicio de monitoreo de Alibaba Cloud y deshabilitarlo»,* dijo CrowdStrike.

Conocido por atacar entornos Windows y Linux, LemonDuck está diseñado principalmente para abusar de los recursos del sistema para minar Monero. Pero también es capaz de robar credenciales, movimiento lateral y facilitar el despliegue de cargas útiles adicionales para actividades de seguimiento.

> *«Utiliza una amplia gama de mecanismos de difusión (correos electrónicos de phishing, exploits, dispositivos USB, fuerza bruta, entre otros) y ha demostrado que puede aprovechar rápidamente noticias, eventos o el lanzamiento de nuevos exploits para ejecutar campañas efectivas»,* detalló Microsoft en julio pasado.

A inicios de 2021, las cadenas de ataque que involucran a LemonDuck aprovecharon las vulnerabilidades de Exchange Server recién parcheadas para obtener acceso a máquinas Windows obsoletas, antes de descargar puertas traseras y ladrones de información, incluyendo Ramnit.

La última campaña detectada por CrowdStrike aprovecha las API de Docker expuestas como un vector de acceso inicial, utilizándolas para ejecutar un contenedor falso para recuperar un archivo de script de shell Bash que está disfrazado como un archivo de imagen PNG inofensivo desde un servidor remoto.

Un análisis de datos históricos muestra que el actor de amenazas ha utilizado droppers de

archivos de imágenes similares alojados en dominios asociados con LemonDuck desde al menos enero de 2021, dijo la compañía de seguridad cibernética.

Los archivos del dropper son clave para lanzar el ataque, con el script de shell descargando la carga útil real que luego elimina los procesos de la competencia, desactiva los servicios de monitoreo de Alibaba Cloud y finalmente descarga y ejecuta el minero de monedas XMRig.

Debido a que las instancias en la nube comprometidas se convierten en un semillero de actividades ilícitas de minería de criptomonedas, los hallazgos subrayan la necesidad de proteger los contenedores de posibles riesgos a lo largo de la cadena de suministro de software.

TeamTNT apunt a AWS, Alibaba Cloud

La divulgación de produce cuando Cisco Talos expuso el conjunto de herramientas de un grupo de delitos cibernéticos llamado TeamTNT, que tiene un historial apuntando a la infraestructura de la nube para el criptojacking y la colocación de backdoors.

Las cargas útiles de malware, que se dice que se modificaron en respuesta a divulgaciones públicas anteriores, están diseñadas principalmente para apuntar a Amazon Web Services (AWS) y, al mismo tiempo, se enfocan en la minería de criptomonedas, la persistencia, el movimiento lateral y la desactivación de soluciones de seguridad en la nube.

> *«Los ciberdelincuentes que son descubiertos por los investigadores de seguridad deben actualizar sus herramientas para seguir operando con éxito»,* dijo el investigador de Talos, Darin Smith.

> *«Las herramientas utilizadas por TeamTNT demuestran que los ciberdelincuentes se sienten cada vez más cómodos al atacar entornos modernos como Docker, Kubernetes y proveedores de nube pública, que tradicionalmente han sido evitados*

> *por otros ciberdelincuentes que se han centrado en entornos locales o móviles».*

Spring4Shell explotado para minería de criptomonedas

Además, en otro ejemplo de cómo los actores de amenazas cooptan rápidamente fallas recientemente reveladas en sus ataques, el error crítico de ejecución remota de código en Spring Framework (CVE-2022-22965) se ha convertido en un arma para implementar mineros de criptomonedas.

Los intentos de explotación hacen uso de un shell web personalizado para implementar los mineros de criptomonedas, pero no antes de apagar el firewall y finalizar otros procesos de minería de moneda virtual.

> *«Estos mineros de criptomonedas tienen el potencial de afectar a una gran cantidad de usuarios, especialmente porque Spring es el marco más utilizado para desarrollar aplicaciones de nivel empresarial en Java»,* dijeron los investigadores de Trend Micro, Nitesh Surana y Ashish Verma.