Hackers conocidos como Kinsing se están aprovechando de vulnerabilidades de seguridad antiguas y recientemente reveladas en Oracle WebLogic Server para entregar malware de minería de criptomonedas.

La compañía de seguridad cibernética Trend Micro dijo que encontró que el grupo con motivación financiera aprovechaba la vulnerabilidad para eliminar scripts de Python con capacidades para deshabilitar funciones de seguridad del sistema operativo (SO) como Linux con seguridad mejorada (SELinux) y otros.

Los operadores detrás del malware Kinsing tienen un historial de búsqueda de servidores vulnerables para cooptarlos en una botnet, incluyendo Redis, SaltStack, Log4Shell, Spring4Shell y la vulnerabilidad de Atlassian Confluence (CVE-2022-26134).

Los atacantes de Kinsing también estuvieron involucrados en campañas contra entornos de contenedores por medio de puertos API abiertos de Docker Daemon mal configurados para lanzar un criptominero, y posteriormente, propagar el malware a otros contenedores y hosts.

La última ola de ataques implica que el actor arma CVE-2020-14882 (puntaje CVSS: 9.8), un error de ejecución remota de código (RCE) de dos años, contra servidores sin parches para tomar el control del servidor y soltar cargas maliciosas.

Cabe mencionar que la vulnerabilidad ha sido explotada en el pasado por múltiples botnets para distribuir mineros de Monero y la backdoor Tsunami en sistemas Linux infectados.

La explotación exitosa de la vulnerabilidad se logró mediante la implementación de un script de shell que es responsable de una serie de acciones: eliminar el registro del sistema /var/log/syslog, desactivar las funciones de seguridad y los agentes de servicio en la nube de Alibaba y Tencent, y matar los procesos del minero de la competencia.

Luego, el script de shell procede a descargar el malware Kinsing desde un servidor remoto, al mismo tiempo que toma medidas para garantizar la persistencia por medio del trabajo cron.

> *«La explotación exitosa de esta vulnerabilidad puede conducir a RCE, que puede permitir a los atacantes realizar una gran cantidad de actividades maliciosas en los sistemas afectados. Esto puede variar desde la ejecución de malware hasta el robo de datos críticos e incluso el control total de una máquina comprometida»,* dijo Trend Micro.

Los atacantes de TeamTNT regresan con nuevos ataques

El desarrollo se produce cuando los investigadores de Aqua Security identificaron tres nuevos ataques vinculados a otro grupo de cryptojacking *«vibrante»* llamado TeamTNT, que cerró voluntariamente en noviembre de 2021.

> *«TeamTNT ha estado buscando un Docker Daemon mal configurado e implementando alpine, una imagen de contenedor vanilla, con una línea de comando para descargar un script de shell (k.sh) a un servidor C2»,* dijo Assaf Morag, investigador de Aqua Security.

La notable cadena de ataque es que parece estar diseñada para romper el cifrado SECP256K1, que de tener éxito, podría darle al actor la capacidad de calcular las claves de cualquier billetera de criptomonedas. Dicho de otra forma, la idea es aprovechar el alto pero ilegal poder computacional de sus objetivos para ejecutar el solucionador ECDLP y obtener la clave.

Otros dos ataques montados por el grupo implican la explotación de servidores Redis expuestos y API de Docker mal configuradas para implementar mineros de monedas y binarios de Tsunami.

El objetivo de TeamTNT de las API REST de Docker ha sido bien documentado durante el año

pasado. Pero en un error de seguridad operacional detectado por Trend Micro, se descubrieron las credenciales asociadas con dos de las cuentas de Docker Hub controladas por el atacante.

Se dice que las cuentas, alpineos y dandeep078, se usaron para distribuir una variedad de cargas maliciosas como rootkits, kits de explotación de Kubernetes, ladrones de credenciales, mineros XMRig Monero e incluso el malware Kinsing.

> *«La cuenta alpineos se usó en intentos de explotación en nuestros honeypots tres veces, desde mediados de septiembre hasta principios de octubre de 2021, y rastreamos las direcciones IP de las implementaciones hasta su ubicación en Alemania»*, dijo Nitesh Surana, de Trend Micro.

> *«Los actores de amenazas iniciaron sesión en sus cuentas con el registro de DockerHub y probablemente olvidaron cerrar sesión».*

Trend Micro dijo que la imagen maliciosa de alpineos se había descargado más de 150,000 veces y agregó que notificó a Docker sobre estas cuentas.

También recomienda a las organizaciones configurar la API REST expuesta con TLS para mitigar los ataques de adversario en el medio (AiTM), así como usar almacenes de credenciales y ayudantes para alojar las credenciales de los usuarios.