Microsoft advierte sobre una nueva variante de la botnet srv que explota múltiples vulnerabilidades de seguridad en aplicaciones web y bases de datos para instalar mineros de criptomonedas en sistemas Windows y Linux.

La compañía tecnológica nombró a la nueva versión como Sysrv-K, que arma una serie de exploits para obtener el control de los servidores web. La botnet de cryptojacking surgió por primera vez en diciembre de 2020.

> *«Sysrv-K escanea Internet para encontrar servidores web con varias vulnerabilidades para instalarse. Las vulnerabilidades van desde el cruce de rutas y la divulgación remota de archivos hasta la descarga arbitraria de archivos y las vulnerabilidades de ejecución remota de código»,* dijo Microsoft.

Esto incluye también CVE-2022-22947, con puntuación CVSS de 10.0, una vulnerabilidad de inyección de código en Spring Cloud Gateway, que podría explotarse para permitir la ejecución remota arbitraria en un host remoto a través de una solicitud creada con fines malintencionados.

Cabe mencionar que el abuso de CVE-2022-22947 llevó a la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) a agregar la falla a su Catálogo de Vulnerabilidades Explotadas Conocidas.

Un diferenciador clave es que Sysrv-K busca archivos de configuración de WordPress y sus copias de seguridad para obtener las credenciales de la base de datos, que luego se utilizan para secuestrar servidores web. También se dice que actualizó sus funciones de comunicación de comando y control para hacer uso de un Bot de Telegram.

Una vez infectado, el movimiento lateral se facilita por medio de claves SSH disponibles en la máquina de la víctima, para implementar copias del malware en otros sistemas y hacer crecer el tamaño de la red de bots, poniendo efectivamente en riesgo a toda la red.

> *«El malware Sysrv aprovecha las vulnerabilidades conocidas para propagar su malware Cryptojacking. Garantizar que las aplicaciones de cara al público se mantengan actualizadas con los últimos parches de seguridad es fundamental para evitar que los atacantes oportunistas comprometan los sistemas»*, dijeron los investigadores de Lacework Labs el año pasado.

Además de proteger los servidores expuestos a Internet, Microsoft también aconseja a las organizaciones que apliquen actualizaciones de seguridad de forma oportuna y construyan una higiene de credenciales para reducir el riesgo.