Google dijo el miércoles que obtuvo una orden judicial temporal en Estados Unidos para interrumpir la distribución de un malware de robo de información basado en Windows llamado CryptBot y así *«desacelerar»* su crecimiento.

Mike Trinh y Pierre-Marc Bureau, de Google, dijeron que los esfuerzos son parte de los pasos que toma la compañía para *«no solo responsabilizar a los operadores criminales de malware, sin también a aquellos que se benefician de su distribución».*

Se estima que CryptBot infectó más de 670,000 computadoras en 2022 con el objetivo de robar datos confidenciales, como credenciales de autenticación, inicios de sesión en cuentas de redes sociales y billeteras de criptomonedas de los usuarios de Google Chrome.

Los datos recolectados después se exfiltran a los hackers, quieren venden los datos a otros atacantes para usarlos en campañas de violación de datos. CryptBot se descubrió por primera vez en la naturaleza en diciembre de 2019.

El malware se entrega de forma tradicional a través de versiones modificadas maliciosamente de paquetes de software legítimos y populares, como Google Earth Pro y Google Chrome, que se alojan en sitios web falsos.

Además, una campaña de CryptBot descubierta por Red Canary en diciembre de 2021, implicaba el uso de KMSPico como vector de entrega, una herramienta no oficial que se utiliza para activar ilegalmente Microsoft Office y Windows sin una clave de licencia.

Después, en marzo de 2022, BlackBerry reveló detalles de una versión nueva y mejorada del ladrón de información malicioso que se distribuyó a través de sitios piradas comprometidos que pretenden ofrecer versiones *«crackeadas»* de varios software y videojuegos.

Se cree que los principales distribuidores de CryptBot, según Google, están operando una *«empresa criminal mundial»* con sede en Pakistán.

Google dijo que tiene la intención de usar la orden judicial, otorgada por un juez federal en el

Distrito Sur de Nueva York, para *«eliminar los dominios actuales y futuros que están vinculados a la distribución de CryptBot»*, lo que detiene la propagación de nuevas infecciones.

Para mitigar los riesgos que plantean dichas amenazas, se recomienda descargar software solo de fuentes conocidas y confiables, analizar las reseñas de que el sistema operativo y el software del dispositivo se mantengan actualizados.

La divulgación se produce semanas después de que Microsoft, Fortra y el Centro de Análisis e Intercambio de Información de Salud (Health-ISAC) se unieran legalmente para desmantelar los servidores que alojaban copias heredadas e ilegales de Cobalt Strike para evitar el abuso de la herramienta por parte de los hackers.