Las redes de comunicaciones, los medios audiovisuales, los distribuidores de servicios de Internet (ISP), los proveedores de soluciones tecnológicas (TI), y los portales kurdos en Holanda han sido objeto de una reciente operación de ciberespionaje orquestada por un grupo de amenaza vinculado a Turquía conocido como Sea Turtle.

> *«Las plataformas digitales de los objetivos mostraban vulnerabilidades ante ataques que se aprovechan de las cadenas de suministro y técnicas de intrusión, las cuales el grupo de atacantes utilizó para recoger información con motivaciones políticas, incluyendo datos personales de comunidades minoritarias y posibles opositores políticos»*, expresó la empresa de seguridad neerlandesa Hunt & Hackett en su análisis del viernes.
>
> *«La información sustraída probablemente será utilizada con fines de vigilancia o recolección de datos sobre grupos específicos o individuos.»*

Sea Turtle, también identificado como Cosmic Wolf, Marbled Dust (antes conocido como Silicon), Teal Kurma y UNC1326, fue identificado inicialmente por el equipo de Cisco Talos en abril de 2019, describiendo operaciones patrocinadas por un estado que tenían como objetivo a organizaciones públicas y privadas en el Medio Oriente y norte de África.

Se cree que las acciones vinculadas al grupo se han desarrollado desde enero de 2017, usando principalmente tácticas de secuestro de DNS para dirigir a objetivos potenciales que intentaban acceder a un dominio específico hacia un servidor controlado por el grupo, donde se recopilaban sus credenciales.

> *«Es muy probable que la campaña de Sea Turtle represente una amenaza más significativa que DNSpionage, dado el enfoque del grupo en apuntar a distintos registros y entidades DNS»,* afirmó Talos en aquel momento.

Hacia finales de 2021, Microsoft destacó que el grupo lleva a cabo actividades de recolección de inteligencia para proteger intereses estratégicos turcos en regiones como Armenia, Chipre, Grecia, Irak y Siria, atacando a empresas de telecomunicaciones y TI con el objetivo de *«establecer una posición inicial antes de alcanzar su objetivo principal»,* aprovechando vulnerabilidades conocidas.

Recientemente, se reveló que el grupo ha empleado una herramienta sencilla denominada SnappyTCP, un shell TCP inverso para sistemas Linux (y Unix), en ataques realizados entre 2021 y 2023, según el equipo de Inteligencia de Amenazas de PricewaterhouseCoopers (PwC).

> *«Este shell web proporciona capacidades básicas de [comando y control], y posiblemente se use para asegurar una presencia constante. Existen al menos dos versiones principales; una que utiliza OpenSSL para establecer conexiones cifradas y otra que no incluye esta función y envía información sin cifrar»,* indicó la empresa.

Los recientes descubrimientos de Hunt & Hackett indican que Sea Turtle sigue operando de manera sigilosa, empleando técnicas avanzadas para eludir la detección y acceder a archivos de correo electrónico.

En un incidente de 2023, se detectó que se utilizó una cuenta de cPanel legítima pero comprometida para instalar SnappyTCP en el sistema. Aún no está claro cómo los atacantes lograron obtener estas credenciales.

> *«Mediante SnappyTCP, los atacantes enviaron instrucciones para duplicar un archivo de correo electrónico usando la herramienta tar, ubicándolo en el directorio público del sitio web accesible desde la web»,* destacó la firma.
>
> *«Es probable que hayan extraído dicho archivo directamente desde esa ubicación.»*

Para enfrentar este tipo de amenazas, es esencial que las organizaciones implementen medidas de seguridad robustas, como políticas de contraseñas estrictas, autenticación de dos factores (2FA), restricciones en los intentos de inicio de sesión, monitoreo del tráfico SSH y mantenimiento actualizado de todos los sistemas y aplicaciones.