Un nuevo actor de amenazas DNS llamado Savvy Seahorse está empleando técnicas avanzadas para atraer a sus objetivos hacia plataformas de inversión falsas y así apoderarse de fondos.

> *«Savvy Seahorse es un actor de amenazas DNS que persuade a las víctimas para que creen cuentas en plataformas de inversión falsas, realicen depósitos en una cuenta personal y luego transfieran esos depósitos a un banco en Rusia»,* según un informe publicado la semana pasada por Infoblox.

Los objetivos de estas campañas incluyen hablantes de ruso, polaco, italiano, alemán, checo, turco, francés, español e inglés, evidenciando que los actores de amenazas están ampliando sus ataques de manera extensa.

Los usuarios son atraídos a través de anuncios en plataformas de redes sociales como Facebook, al mismo tiempo que son engañados para proporcionar su información personal a cambio de presuntas oportunidades de inversión con rendimientos elevados, utilizando bots falsos de ChatGPT y WhatsApp.

Lo destacado de estas estafas financieras radica en el uso de registros de nombre canónico DNS (CNAME) para crear un sistema de distribución de tráfico (TDS), permitiendo a los actores de amenazas eludir la detección desde al menos agosto de 2021.

Un registro CNAME se utiliza para mapear un dominio o subdominio a otro dominio (es decir, un alias) en lugar de señalar a una dirección IP. Una ventaja de esta estrategia es que, al cambiar la dirección IP del host, solo se requiere actualizar el registro A DNS del dominio raíz.

Savvy Seahorse aprovecha esta técnica registrando varios subdominios de corta duración que comparten un registro CNAME (y, por ende, una dirección IP). Estos subdominios específicos se crean mediante un algoritmo de generación de dominios (DGA) y están vinculados al dominio principal de la campaña.

La naturaleza siempre cambiante de los dominios y las direcciones IP también otorga resistencia a los esfuerzos para desactivar la infraestructura, permitiendo a los actores de amenazas crear de forma continua nuevos dominios o modificar sus registros CNAME hacia una dirección IP diferente cuando sus sitios de phishing se ven afectados.

Aunque actores de amenazas como VexTrio han utilizado DNS como TDS, este descubrimiento marca la primera vez que se emplean registros CNAME con este propósito.

Las víctimas que hacen clic en los enlaces incrustados en los anuncios de Facebook son instadas a proporcionar sus nombres, direcciones de correo electrónico y números de teléfono, siendo luego redirigidas a la falsa plataforma de comercio para agregar fondos a sus cuentas.

> *«Un detalle relevante es que el actor valida la información del usuario para excluir el tráfico de una lista predefinida de países, incluyendo Ucrania, India, Fiyi, Tonga, Zambia, Afganistán y Moldavia, aunque no está claro por qué se eligieron estos países en particular»,* destacó Infoblox.

Este hallazgo coincide con la revelación de Guardio Labs sobre el secuestro de miles de dominios pertenecientes a marcas e instituciones legítimas utilizando una técnica llamada «*CNAME takeover*» para difundir campañas de correo no deseado.