Investigadores de ciberseguridad han expuesto a dos actores maliciosos que llevan a cabo estafas de inversión mediante falsos respaldos de celebridades y ocultan su actividad usando sistemas de distribución de tráfico (TDS).

Las agrupaciones de actividad han sido denominadas *Reckless Rabbit* (Conejo Imprudente) y *Ruthless Rabbit* (Conejo Despiadado) por la firma de inteligencia de amenazas DNS Infoblox.

Se ha observado que estas campañas atraen a víctimas a través de plataformas falsas, como intercambios de criptomonedas, promocionadas en redes sociales. Un componente clave es el uso de formularios web para recolectar datos personales.

> *«Reckless Rabbit crea anuncios en Facebook que conducen a artículos falsos con supuestos respaldos de celebridades sobre plataformas de inversión. El artículo incluye un enlace al sitio fraudulento, que contiene un formulario web diseñado para que el usuario ingrese su información personal y 'se registre' en la inversión»,* explicaron los investigadores Darby Wise, Piotr Glaska y Laura da Rocha.

Algunos formularios incluso ofrecen la opción de generar automáticamente una contraseña, lo cual se usa para avanzar a la siguiente fase del ataque: las validaciones.

Los actores maliciosos hacen solicitudes HTTP GET a servicios legítimos de validación de IP como ipinfo[.]io o ipapi[.]co para filtrar tráfico de países que no son de su interés. También verifican que los correos y teléfonos ingresados sean reales.

Si el usuario pasa estos filtros, es redirigido a través de un TDS a la plataforma de estafa donde se le persuade para invertir su dinero, o a una página que le indica esperar una llamada.

> *«Algunas campañas incluso usan centros de llamadas para guiar al usuario en la creación de una cuenta y la transferencia de fondos. Si el usuario no pasa la*

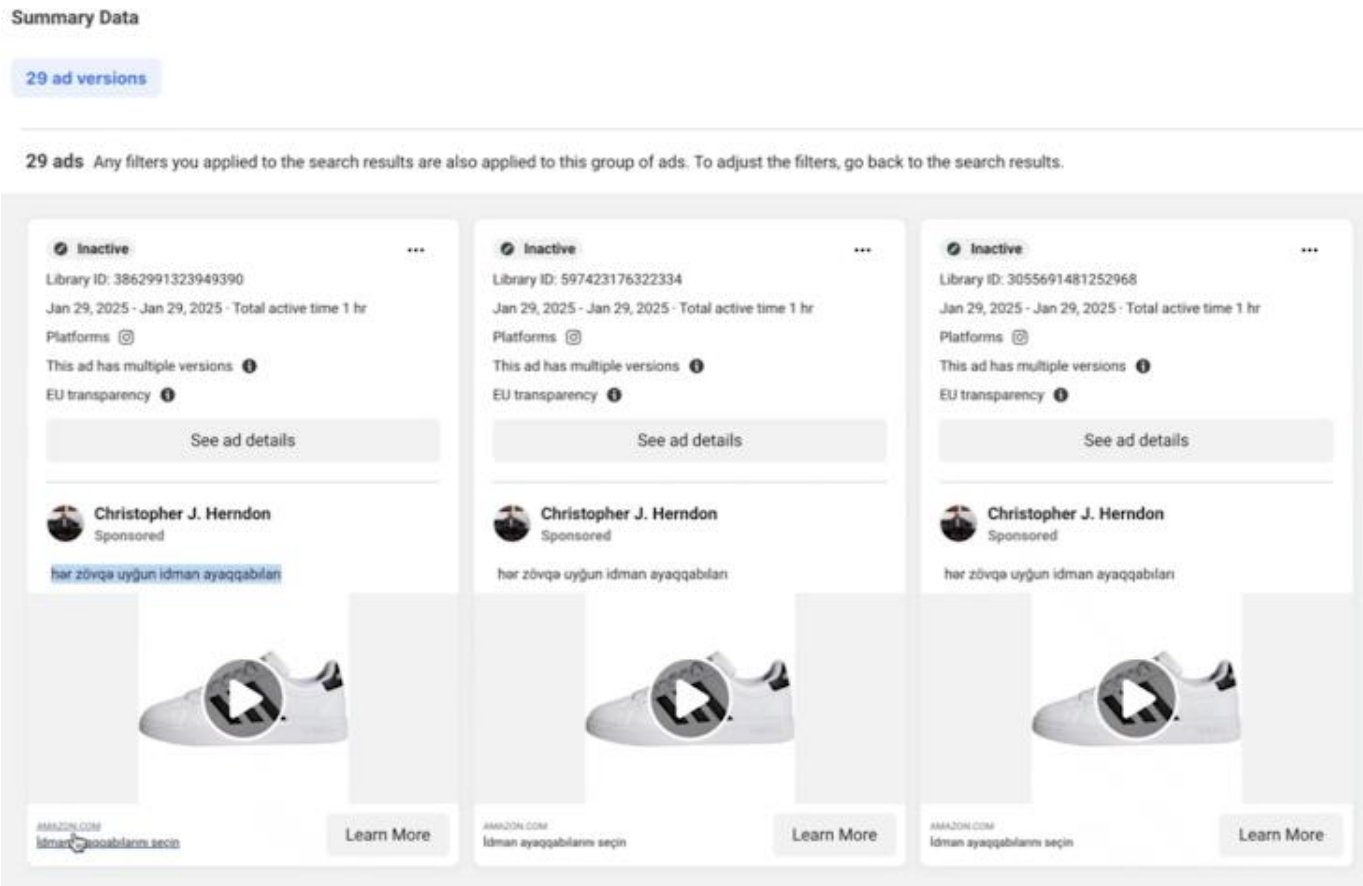
> *validación, simplemente ve una página de agradecimiento»*, detallaron los expertos.

Una técnica importante es el uso de un algoritmo de generación de dominios registrados (RDGA), también usado por grupos como Prolific Puma y Revolver Rabbit, para crear los dominios de los sitios fraudulentos.

A diferencia de los algoritmos tradicionales (DGA), los RDGA usan un algoritmo secreto para registrar dominios. Reckless Rabbit lleva generando estos dominios desde abril de 2024, enfocados en Rusia, Rumania y Polonia, y excluyendo países como Afganistán y Somalia.

Los anuncios en Facebook incluyen contenido disfrazado como productos de Amazon para evadir controles, mostrando un dominio señuelo como «amazon[.]pl», pero redirigiendo a sitios como «tyxarai[.]org».

Por su parte, *Ruthless Rabbit* opera desde al menos noviembre de 2022, también apuntando a Europa del Este, y destaca por usar su propio sistema de validación («mcraftdb[.]tech»).



Quienes superan la validación son llevados a una plataforma falsa donde deben ingresar datos financieros.

> *«Un TDS permite fortalecer la infraestructura de los atacantes, ocultando contenido malicioso de investigadores y bots»,* dijo Infoblox.

No es la primera vez que se detectan estas estafas. En diciembre de 2024, ESET reveló un esquema similar, llamado *Nomani*, que usaba videos con IA y figuras públicas para engañar.

En abril, autoridades españolas arrestaron a seis personas por una gran estafa de criptomonedas con anuncios falsos generados por IA.

Renee Burton, vicepresidenta de inteligencia en Infoblox, indicó que aún se investiga si hay conexión entre esos casos y los de los conejos maliciosos.

> *«Actores como Reckless y Ruthless Rabbit seguirán tratando de engañar a más usuarios. Estas estafas han resultado tan rentables que seguirán creciendo en cantidad y sofisticación»,* advirtieron los investigadores.

Estafas de 'Cajas Misteriosas' se propagan por Facebook

Bitdefender advierte sobre un aumento en estafas de suscripción que usan más de 200 sitios web falsos para engañar a usuarios y obtener sus datos de tarjetas.

> *«Los criminales crean páginas de Facebook y publican anuncios para promover la clásica estafa de la 'caja misteriosa'. Ahora incluyen pagos recurrentes casi ocultos y enlaces a supuestas tiendas»,* dijo la empresa rumana.

Los anuncios promocionan ofertas de liquidación de marcas como Zara o prometen cajas con productos Apple por precios muy bajos (desde $2).

Los estafadores evitan la detección usando múltiples versiones del anuncio, siendo solo una la maliciosa, mientras las demás muestran imágenes inocentes.

Mientras *Reckless Rabbit* lleva operando desde abril de 2024 y se enfoca en Europa del Este, *Ruthless Rabbit* actúa desde 2022 con tácticas similares pero usando su propio sistema de validación.

Este tipo de fraude no es nuevo. Otras campañas han usado inteligencia artificial para crear videos falsos con figuras públicas, e incluso hay estafas relacionadas como las de «cajas misteriosas», que engañan a usuarios para que paguen suscripciones ocultas mediante

anuncios en Facebook.

Estas estafas, como las llevadas a cabo por *Reckless Rabbit* y *Ruthless Rabbit*, incluyen encuestas para verificar que las víctimas sean personas reales y no bots. Además, las páginas de pago engañan a los usuarios para que se suscriban a un servicio con cargos recurrentes, haciéndoles creer que obtendrán un descuento.

Los investigadores de Bitdefender, Răzvan Gosa y Silviu Stahie, explicaron que los delincuentes están invirtiendo dinero en anuncios que imitan a creadores de contenido conocidos, utilizando el mismo modelo de suscripción, que parece haberse convertido en la principal fuente de ingresos de estas estafas.

Los estafadores cambian frecuentemente las marcas que suplantan y han ampliado su enfoque más allá de las cajas misteriosas. Ahora también venden productos de baja calidad, artículos falsificados, inversiones fraudulentas, suplementos y otros productos engañosos.

Sanciones del Departamento del Tesoro de EE.UU. a milicia vinculada con la junta en Myanmar por centros de estafa:

Estas revelaciones se producen tras una serie de sanciones impuestas por el Departamento del Tesoro de los Estados Unidos contra el Ejército Nacional Karen (KNA), vinculado a Myanmar, por colaborar con redes criminales que manejan operaciones de estafa multimillonarias, además de facilitar la trata de personas y el contrabando transfronterizo.

Las sanciones también incluyen al líder del grupo, Saw Chit Thu, y a sus dos hijos, Saw Htoo Eh Moo y Saw Chit Chit. Saw Chit Thu ya había sido sancionado anteriormente por el Reino Unido en 2023 y por la Unión Europea en 2024 por su papel clave en el impulso de estas estafas en la región.

> *«Las estafas cibernéticas organizadas por el KNA generan miles de millones en ganancias para líderes criminales y sus cómplices, al mismo tiempo que arruinan*

> *financieramente a las víctimas y destruyen su confianza»,* declaró el subsecretario Michael Faulkender.

En este tipo de estafas conocidas como “romance baiting” o estafas románticas, los estafadores —quienes a menudo han sido víctimas de trata laboral con la promesa de empleos bien remunerados— son obligados a seducir a personas por internet para luego convencerlas de invertir en criptomonedas o plataformas de inversión falsas controladas por los criminales.

El Departamento del Tesoro explicó que el KNA obtiene enormes beneficios alquilando terrenos que controla a otras organizaciones delictivas, además de ofrecer apoyo logístico y energético a los centros de estafa y brindar seguridad en esos complejos ubicados en el estado de Karen.

Según la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), estos centros de fraude siguen en expansión a pesar de las medidas represivas recientes, generando beneficios anuales de aproximadamente 40 mil millones de dólares.