Los ciberdelincuentes se están haciendo pasar por plataformas criptográficas populares como Binance, Celo y Trust Wallet, con correos electrónicos falsificados y páginas de inicio de sesión falsas en un intento de robar los datos de inicio de sesión y transferir fondos virtuales de forma engañosa.

> *«A medida que las criptomonedas y los tokens no fungibles (NFT) se vuelven más comunes y capturan los titulares por su volatilidad, existe una mayor probabilidad de que más personas sean víctimas de fraude al intentar explotar a las personas por monedas digitales»,* dijo Proofpoint.

> *«El auge y la proliferación de las criptomonedas también ha proporcionado a los atacantes un nuevo método de extracción financiera».*

El equipo de investigación de Microsoft 365 Defender se hizo eco recientemente de la selección de datos confidenciales de criptomonedas por parte de los actores de amenazas, que advirtió sobre la amenaza emergente de cryware en el que se saquean claves privadas, frases iniciales y direcciones de billetera con el objetivo de desviar monedas virtuales por medio de transferencias fraudulentas.

La rápida popularidad de Web3 en los últimos años ha provocado un cambio en el panorama del phishing, allanando el camino para una variedad de mecanismos de explotación e ingeniería social que tienen como objetivo robar criptomonedas de distintas formas, desde la recolección de credenciales hasta el uso de malware de ladrón de productos básicos.

Esto incluye correos electrónicos no deseados que contienen enlaces a URL no autorizadas que descargan malware y redirigen a los usuarios a una página de inicio de recolección de credenciales o incluso a versiones falsas de plataformas comerciales de NFT como OpenSea. Otras campañas incitan a las víctimas potenciales a ingresar sus frases iniciales.

En un ataque de phishing detectado por la empresa de seguridad empresarial en febrero de 2022, se observó un señuelo con el tema de Trust Wallet que animaba a los destinatarios de correo electrónico, específicamente estudiantes universitarios, a verificar sus billeteras ingresando las frases de recuperación.

Un habilitador crucial de estas campañas personalizadas es la relativa facilidad con la que se pueden crear sitios web de destino falsificados utilizando kits de phishing, lo que permite que los actores de amenazas menos capacitados distribuyan y administren a gran escala.

Los operadores de phishing como servicio (PHaaS) como BulletProofLink, que ofrecen plantillas de phishing, servicios de spam, servicios de alojamiento a prueba de balas y servicios de recolección de credenciales, entre otros, incentivan aún más el esquema de ciberdelincuente.

Los kits, que se actualizan y amplían continuamente, están diseñados para imitar diferentes marcas, como blockchain[.]com, así como otros NFT y otros proveedores de servicios de monederos de criptomonedas.

También son destacados los intentos de compromiso de correo electrónico comercial (BEC) para facilitar la transferencia fraudulenta de monedas digitales a través de mensajes que solicitan criptomonedas bajo la apariencia de pagos de proveedores y solicitudes de donación para apoyar el esfuerzo de la guerra de Ucrania.

Estos hallazgos se producen cuando las pérdidas por delitos relacionados con las criptomonedas aumentaron un 79% año tras año en 2021, y la Comisión Federal de Comercio (FTC) de Estados Unidos dijo que más de 46,000 personas informaron haber perdido más de mil millones de dólares en monedas digitales debido a estafas.

Además, la empresa de análisis Blockchain Chainalysis, descubrió que el crimen basado en

criptomonedas alcanzó un nuevo máximo histórico en 2021, incluso cuando las direcciones ilícitas recibieron 14 mil millones de dólares en el transcurso del año, frente a 7.8 mil millones de dólares en 2020.

> *«Las amenazas cibernéticas a las criptomonedas no son nuevas, sin embargo, a medida que el público en general experimenta una creciente adopción de las criptomonedas, es más probable que las personas se involucren con señuelos de ingeniería social utilizando dichos temas»,* dijo Sherrod DeGrippo, vicepresidente de investigación y detección de amenazas en Proofpoint.

> *«Las criptomonedas se generalizaron con los anuncios de Superbowl este año y los actores de amenazas tomaron nota de la oportunidad de un día de pago rápido. No existe un método más fácil de extracción financiera que la transferencia ilícita de criptomonedas».*