Han surgido más detalles sobre un bot malicioso en Telegram conocido como Telekopye, utilizado por actores de amenazas para llevar a cabo estafas de phishing a gran escala.

> *«Telekopye tiene la capacidad de generar sitios de phishing, correos electrónicos, mensajes de texto y otras tácticas»,* señaló Radek Jizba, investigador de seguridad de ESET, en un nuevo análisis.

Los responsables de esta operación, apodados Neanderthals, gestionan la empresa criminal como si fuera una entidad legítima, estableciendo una estructura jerárquica que involucra a distintos miembros desempeñando diversos roles.

Una vez que nuevos aspirantes, conocidos como Neanderthals, son reclutados a través de anuncios en foros clandestinos, se les invita a unirse a canales específicos en Telegram destinados a la comunicación entre ellos y para llevar un registro de las transacciones.

El objetivo principal de esta operación es llevar a cabo uno de los tres tipos de estafas: vendedor, comprador o reembolso.

En el primer escenario, los Neanderthals se presentan como vendedores y buscan atraer a incautos Mamuts para que compren un artículo inexistente. En las estafas de compradores, los Neanderthals se disfrazan como compradores para engañar a los Mamuts (comerciantes) y obtener sus detalles financieros para apropiarse de sus fondos.

Otras situaciones caen en la categoría de estafas de reembolso, en las que los Neanderthals engañan nuevamente a los Mamuts bajo el pretexto de ofrecer un reembolso, solo para deducir la misma cantidad de dinero nuevamente.

La firma de ciberseguridad con sede en Singapur, Group-IB, previamente informó que la actividad rastreada como Telekopye es la misma que Classiscam, un programa de estafa como servicio que ha generado a los actores criminales $64.5 millones en ganancias ilícitas desde su aparición en 2019.

> *«En el escenario de estafa del vendedor, se aconseja a los Neanderthals que preparen fotos adicionales del artículo por si los Mamuts solicitan más detalles. Si los Neanderthals están utilizando imágenes descargadas en línea, se espera que las modifiquen para dificultar la búsqueda de imágenes»*, señaló Jizba.

La selección de un Mamut para una estafa de comprador es un proceso cuidadoso que tiene en cuenta el género de la víctima, su edad, experiencia en los mercados en línea, calificación, reseñas, número de transacciones completadas y el tipo de artículos que están vendiendo, lo que indica una etapa preparatoria que implica una investigación de mercado exhaustiva.

Además, los Neanderthals utilizan rastreadores web para examinar listados en mercados en línea y seleccionar a un Mamut ideal que probablemente caiga en el esquema fraudulento.

En el caso de que un Mamut prefiera el pago y la entrega en persona de los bienes vendidos, los Neanderthals afirman *«que están demasiado lejos o que se van de la ciudad por un viaje de negocios durante unos días»*, al tiempo que demuestran un interés elevado en el artículo para aumentar la probabilidad de éxito de la estafa.

También se ha observado que los Neanderthals utilizan redes privadas virtuales (VPN), proxies y la red Tor para mantener su anonimato, al mismo tiempo que exploran estafas inmobiliarias creando sitios web falsos con listados de apartamentos para atraer a los Mamuts a pagar una tarifa de reserva haciendo clic en un enlace que dirige a un sitio de phishing.

> *«Los Neanderthals se comunican con el legítimo propietario de un departamento, simulan interés y solicitan diversos detalles, como fotos adicionales y la calidad de los vecinos del departamento»,* mencionó Jizba.

> *«Posteriormente, los Neanderthals utilizan toda esta información para crear su propio anuncio en otro sitio web, ofreciendo el departamento en alquiler. Reducen el precio esperado del mercado en aproximadamente un 20%. El resto de la situación es prácticamente idéntico al escenario de estafa del vendedor».*

Esta revelación surge mientras Check Point describe una estafa tipo «rug pull» que logró sustraer casi $1 millón al atraer a víctimas desprevenidas para que invirtieran en tokens falsos y realizaran operaciones simuladas para simular legitimidad.

> *«Una vez que el token había atraído a suficientes inversores, el estafador ejecutó el último movimiento: retirar la liquidez del grupo de tokens, dejando a los compradores con las manos vacías y sin fondos»,* explicó la empresa.