Investigadores en ciberseguridad han advertido sobre un nuevo tipo de fraude de inversión que combina publicidad engañosa en redes sociales, publicaciones que imitan marcas conocidas y testimonios en video generados con inteligencia artificial (IA) protagonizados por figuras famosas, lo que lleva a las víctimas a pérdidas financieras y de información personal.

> *«El objetivo principal de los estafadores es dirigir a las víctimas a sitios de phishing y formularios diseñados para recolectar su información personal»*, explicó ESET en su Informe de Amenazas del segundo semestre de 2024.

La empresa de ciberseguridad eslovaca ha denominado esta amenaza «Nomani», un juego de palabras que significa «sin dinero». Según ESET, este fraude creció más del 335 % entre la primera y la segunda mitad de 2024, con un promedio de más de 100 nuevas URL detectadas diariamente entre mayo y noviembre de ese año.

El esquema opera mediante anuncios falsos en plataformas de redes sociales, algunos de los cuales están dirigidos a personas que ya han sido víctimas de fraudes. Los estafadores utilizan tácticas que incluyen referencias a Europol e INTERPOL, prometiendo ayudar a las víctimas a recuperar su dinero robado mediante un enlace.

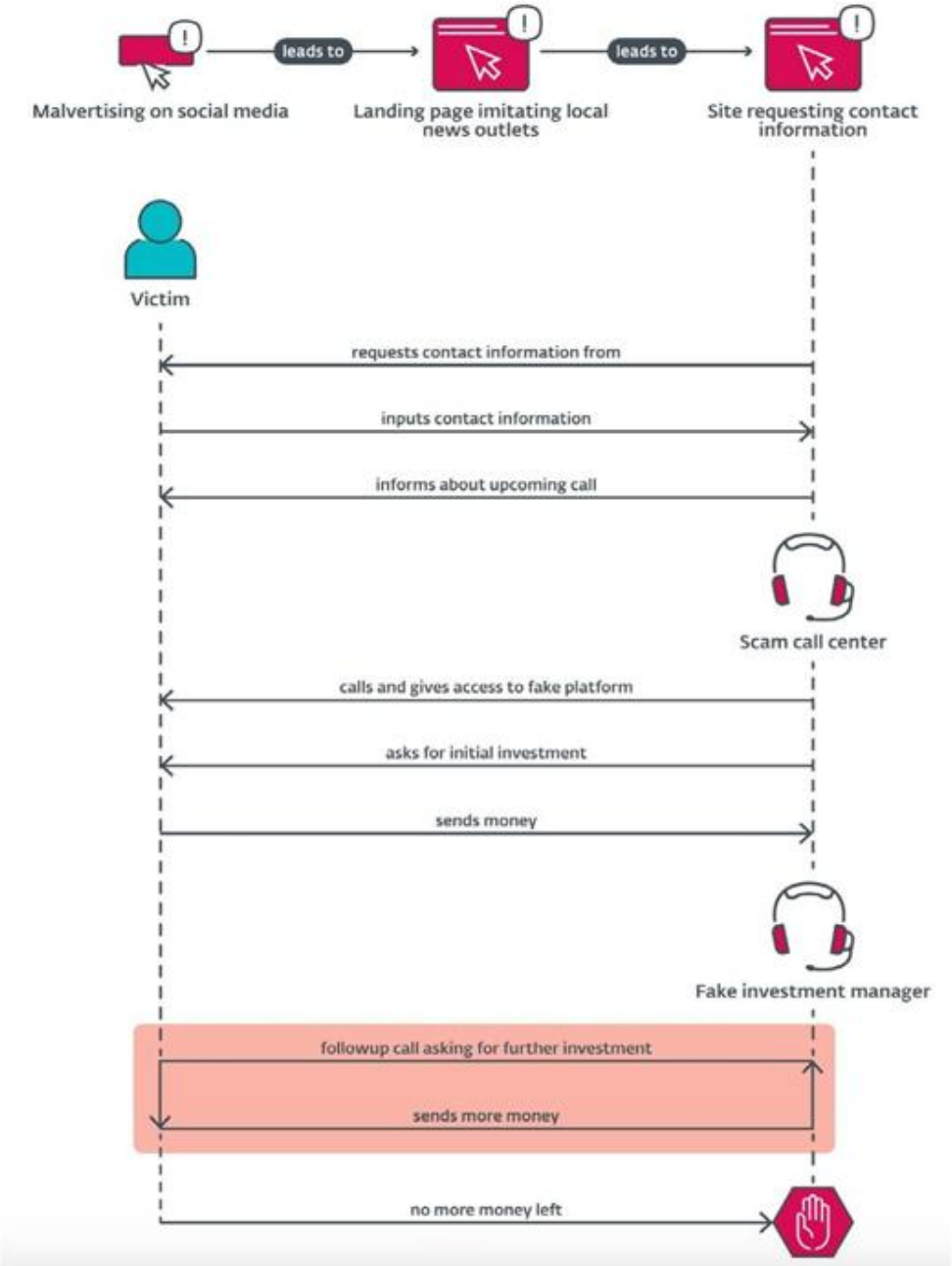
Estos anuncios son publicados desde una mezcla de perfiles falsos y cuentas legítimas robadas, vinculadas a pequeñas empresas, agencias gubernamentales y microinfluencers con miles de seguidores. También se distribuyen a través de publicaciones en Messenger y Threads, así como reseñas falsas y favorables en Google.

> *«Un grupo importante de cuentas que promueven los anuncios de Nomani incluye perfiles recién creados con nombres genéricos, pocos seguidores y casi ninguna publicación»,* indicó ESET.

Los sitios web asociados con estos enlaces solicitan datos de contacto y a menudo simulan

ser medios de comunicación locales; también emplean logotipos y marcas de organizaciones reales o promocionan servicios de gestión de criptomonedas bajo nombres cambiantes como Quantum Bumex, Immediate Mator o Bitcoin Trader.

Posteriormente, los ciberdelincuentes utilizan los datos recopilados para contactar directamente a las víctimas, persuadiéndolas de invertir en productos financieros falsos que aparentan generar ganancias extraordinarias. En algunos casos, las víctimas son convencidas de solicitar préstamos o instalar aplicaciones de acceso remoto en sus dispositivos.



> *«Cuando estas personas solicitan retirar las ganancias prometidas, los estafadores las obligan a pagar tarifas adicionales y proporcionar más información personal, como identificaciones o datos de tarjetas de crédito. Finalmente, los estafadores se*

> *apropian del dinero y de los datos personales y desaparecen, siguiendo el patrón típico de las estafas conocidas como 'pig butchering'»,* señaló ESET.

Se ha encontrado evidencia que sugiere que los responsables de Nomani son actores malintencionados de habla rusa, dada la presencia de comentarios en el código fuente escritos en cirílico y el uso de herramientas de Yandex para el seguimiento de visitantes.

Al igual que otras operaciones fraudulentas importantes, como Telekopye, se sospecha que este esquema involucra a diferentes grupos especializados en diversas etapas del ataque: el robo, la creación y el abuso de cuentas de Meta, la construcción de la infraestructura de phishing y la gestión de los centros de llamadas.

> *«Mediante el uso de técnicas de ingeniería social y la construcción de confianza con las víctimas, los estafadores suelen superar incluso las medidas de seguridad y las llamadas de verificación implementadas por los bancos para prevenir fraudes»,* explicó ESET.

Este caso coincide con el desmantelamiento de una red de fraude a gran escala en Corea del Sur que, según las autoridades, estafó cerca de $6.3 millones a sus víctimas mediante plataformas de comercio en línea falsas en una operación denominada MIDAS. Se han confiscado más de 20 servidores utilizados por la red y 32 personas involucradas han sido arrestadas.

Además de engañar a las víctimas mediante mensajes de texto y llamadas telefónicas, los responsables de los sistemas de comercio en casa (HTS) ilegales persuadieron a los usuarios para que invirtieran al ver videos en YouTube y unirse a chats en KakaoTalk.

> *«El programa interactúa con los servidores de corredores legítimos para obtener precios de acciones en tiempo real y utiliza bibliotecas de gráficos públicas para*

> *generar representaciones visuales»*, explicó el Instituto de Seguridad Financiera (K-FSI) en la conferencia Black Hat Europe.
>
> *«No obstante, no se realizan transacciones reales de acciones. La función principal del programa, una herramienta de captura de pantalla, se usa para espiar las pantallas de los usuarios, recopilar datos sin autorización y negar la devolución de los fondos.»*