Meta Platforms, Microsoft y el Departamento de Justicia de los Estados Unidos (DoJ) han revelado medidas independientes destinadas a combatir el ciberdelito y desarticular servicios que facilitan estafas, fraudes y ataques de phishing.

Como parte de estas acciones, la Unidad de Crímenes Digitales (DCU) de Microsoft informó la desactivación de 240 sitios web fraudulentos vinculados a un facilitador de ciberdelitos en Egipto, identificado como Abanoub Nady (alias MRxC0DER y mrxc0derii). Este individuo ofrecía a la venta un kit de phishing conocido como ONNX, y sus actividades delictivas se remontan al año 2017.

> *«Muchos actores de amenazas y ciberdelincuentes adquirieron estos kits y los utilizaron para llevar a cabo extensas campañas de phishing, evadiendo medidas de seguridad y accediendo ilegalmente a cuentas de usuarios de Microsoft. Si bien todos los sectores son vulnerables, la industria financiera ha sido un objetivo importante debido a la naturaleza sensible de los datos y transacciones que manejan. Un ataque exitoso de este tipo puede tener consecuencias devastadoras para las víctimas»,* explicó Steven Masada, representante de la DCU de Microsoft.

El kit de phishing ONNX, ofrecido como un servicio bajo el modelo *Phishing-as-a-Service* (PhaaS), tenía precios que oscilaban entre $150 mensuales y $550 por un paquete de seis meses. Según EclecticIQ, que documentó este kit en junio, una de sus características destacadas era su capacidad para incluir códigos QR en archivos PDF que redirigían a las víctimas a páginas falsas de inicio de sesión de Microsoft 365.

En ese mismo período, la identidad de Nady fue expuesta por DarkAtlas, lo que lo llevó a detener sus actividades abruptamente. Microsoft rastreó a Nady bajo el nombre Storm-0867 y advirtió que ONNX también fue señalado por la Autoridad Reguladora de la Industria Financiera de EE. UU. (FINRA), que alertó sobre su capacidad para eludir sistemas de autenticación de dos factores (2FA) interceptando solicitudes de verificación.

Además, Microsoft señaló que la plataforma PhaaS operaba con otros nombres, como

Caffeine y FUHRER, permitiendo campañas masivas de phishing. Los kits, distribuidos y configurados principalmente a través de Telegram, incluían plantillas de phishing y la infraestructura técnica necesaria para los ataques.

La compañía obtuvo una orden judicial del Distrito Este de Virginia para desactivar esta infraestructura maliciosa, bloqueando el acceso de los ciberdelincuentes y previniendo el uso futuro de estos dominios para ataques de phishing. Como co-demandante, participó LF Projects, LLC, propietario de la marca registrada ONNX, un estándar abierto para representar modelos de aprendizaje automático.

Por otro lado, el Departamento de Justicia anunció el cierre de PopeyeTools, un mercado en línea especializado en la venta de tarjetas de crédito robadas y herramientas para cometer fraudes financieros. Tres administradores del sitio, Abdul Ghaffar (25 años), Abdul Sami (35 años) y Javed Mirza (37 años), fueron acusados de conspiración para cometer fraude con dispositivos de acceso y tráfico de estos dispositivos. De ser condenados, podrían enfrentar hasta 10 años de prisión por cada delito.

Desde su creación en 2016, PopeyeTools había atraído a miles de usuarios en todo el mundo, generando ingresos estimados de $1.7 millones. La plataforma ofrecía datos financieros robados, listas de correos electrónicos para spam, plantillas de estafas y tutoriales, con la promesa de reembolsar o reemplazar tarjetas de crédito no válidas al momento de la compra. Además, el DoJ informó la confiscación de $283,000 en criptomonedas relacionadas con estas actividades.

En paralelo, Meta informó que eliminó más de dos millones de cuentas vinculadas a redes de estafa operadas desde Camboya, Myanmar, Laos, Emiratos Árabes Unidos y Filipinas. Estas operaciones, gestionadas por sindicatos delictivos organizados, se centraban en manipular a las víctimas mediante relaciones personales o románticas falsas, persuadiéndolas para que invirtieran en esquemas fraudulentos.

Meta explicó que estas redes atraen a personas con falsas ofertas de trabajo y las obligan a actuar como estafadores bajo amenazas de abuso físico. En mayo, Meta se unió a Coinbase,

Ripple y Match Group para crear una coalición llamada *Tech Against Scams*, con el objetivo de abordar esta amenaza y otras formas de fraude en línea. Por su parte, Google colabora con la Global Anti-Scam Alliance (GASA) y la DNS Research Federation (DNS RF) en esfuerzos similares.