Una operación policial internacional resultó en el desmantelamiento de WT1SHOP, un mercado criminal en línea que se especializó en la venta de credenciales de inicio de sesión robadas y otra información personal.

La incautación se llevó a cabo por las autoridades portuguesas, los funcionarios estadounidenses tomaron el control de cuatro dominios utilizados por el sitio web: *«wt1shop[.]net», «wt1store[.]cc», «wt1store[.]com» y «wt1store[.]red.».*

> *«El sitio web vendió más de 5.85 millones de registros de información de identificación personal (PII), incluidas aproximadamente 25,000 licencias de conducir/pasaportes escaneados, 1.7 millones de credenciales de inicio de sesión para varias tiendas en línea, 108,000 cuentas bancarias, 21,800 tarjetas de crédito»*, dijo el Departamento de Justicia de Estados Unidos (DoJ).

El Departamento de Justicia también presentó una denuncia penal contra Nicolai Colesnicov, acusando al sujeto de 36 años de la República de Moldavia de administrar el mercado. Colesnicov fue acusado de conspiración y tráfico de dispositivos de acceso no autorizado.

Según documentos judiciales no sellados, WT1SHOP ofreció un mecanismo de pago que facilitó el tráfico de PII robada utilizando Bitcoin. La tienda de cuentas tenía 106,273 usuarios registrados y 94 vendedores con un total de aproximadamente 5.85 millones de credenciales disponibles para la venta hasta diciembre de 2021.

Las credenciales de inicio de sesión incluían aquellas pertenecientes a minoristas e instituciones financieras, cuentas de correo electrónico, cuentas de PayPal y tarjetas de identificación, así como acceso y operación remota de computadoras, servidores y dispositivos de red sin autorización.

El Departamento de Justicia también dijo que la policía pudo rastrear las transacciones de Bitcoin realizadas en WT1SHOP, junto con las direcciones de correo electrónico y la información de inicio de sesión de las cuentas, hasta llegar a Colesnicov, lo que permitió a las

autoridades determinar su papel como administrador del mercado negro.

De ser declarado culpable, Colesnicov enfrenta una sentencia máxima de 10 años en una prisión federal.

El desarrollo se produce más de un año después de que las agencias de aplicación de la ley de Estados Unidos, Alemania, Países Bajos y Rumania interrumpieran y derribaran la infraestructura de un mercado clandestino conocido como Slilpp que se especializaba en el comercio de credenciales de inicio de sesión robadas.