Un individuo de nacionalidad rusa ha sido declarado culpable por su participación en el desarrollo y despliegue de un malware denominado TrickBot, según anunció el Departamento de Justicia de los Estados Unidos (DoJ).

Vladimir Dunaev, de 40 años, fue detenido en Corea del Sur en septiembre de 2021 y extraditado a los Estados Unidos un mes después.

> *«Dunaev creó modificaciones para navegadores y herramientas maliciosas que facilitaron la obtención de credenciales y la extracción de datos de computadoras infectadas. Además, mejoró el acceso remoto utilizado por los actores de TrickBot y diseñó un código de programa para eludir la detección por parte de programas de seguridad legítimos«*, informó el DoJ.

> *«Durante la participación de Dunaev en el esquema, TrickBot defraudó a más de $3.4 millones a 10 víctimas en el Distrito Norte de Ohio, entre ellas, escuelas en Avon y una empresa inmobiliaria en North Canton, mediante el uso de ransomware«.*

Dunaev, quien se declaró culpable de cometer fraude informático y robo de identidad, así como conspiración para cometer fraude bancario y fraude electrónico, se enfrenta a una condena máxima de 35 años de prisión. Su sentencia está programada para el 20 de marzo de 2024.

Dunaev es también el segundo desarrollador de malware del grupo TrickBot en ser arrestado, después de Alla Witte, una ciudadana letona condenada a dos años y ocho meses de prisión en junio de 2023.

Este desarrollo tuvo lugar aproximadamente tres meses después de que los gobiernos del Reino Unido y Estados Unidos impusieran sanciones a 11 individuos sospechosos de

pertenecer al grupo delictivo cibernético TrickBot.

TrickBot, inicialmente concebido como un troyano bancario en 2016, evolucionó para convertirse en una herramienta versátil capaz de cargar elementos adicionales en sistemas infectados y actuar como facilitador de acceso inicial en ataques de ransomware.

A pesar de sobrevivir a los intentos de las fuerzas del orden de desmantelar la botnet, la temida banda de ransomware Conti finalmente tomó el control de la operación. No obstante, tanto Conti como TrickBot sufrieron un golpe considerable el año pasado después de la invasión de Rusia a Ucrania, cuando Conti juró lealtad a Rusia.

Este acontecimiento desencadenó una serie de filtraciones conocidas como ContiLeaks y TrickLeaks, que revelaron información valiosa sobre las conversaciones internas e infraestructura de ambos grupos, culminando en el cierre de Conti y su desintegración en diversos grupos más pequeños.