El viernes, el Departamento de Justicia de los Estados Unidos (DoJ) reveló una acusación contra un individuo de nacionalidad iraní, señalándolo por su presunta participación en una campaña cibernética de varios años diseñada para comprometer entidades gubernamentales y privadas de los Estados Unidos.

Se informa que más de una docena de entidades fueron objeto de ataques, entre ellas, los Departamentos del Tesoro y de Estado de EE. UU., contratistas de defensa que respaldan programas del Departamento de Defensa de EE. UU., así como una firma contable y una empresa de hospitalidad, ambas con sede en Nueva York.

Alireza Shafie Nasab, de 39 años, afirmó ser especialista en ciberseguridad para una empresa llamada Mahak Rayan Afraz mientras participaba en una persistente campaña dirigida a los EE. UU., que se extendió al menos desde 2016 hasta aproximadamente abril de 2021.

> *«Según la acusación, Alireza Shafie Nasab participó en una campaña cibernética utilizando técnicas de spear-phishing y otras estrategias de hackeo para infectar más de 200,000 dispositivos víctima, muchos de los cuales contenían información de defensa sensible o clasificada»,* señaló Damian Williams, Fiscal de EE. UU. para el Distrito Sur de Nueva York.

Las campañas de spear-phishing eran coordinadas mediante una aplicación personalizada que permitía a Nasab y sus cómplices organizar y ejecutar sus ataques.

En un caso, los actores de amenazas comprometieron una cuenta de correo electrónico de un administrador perteneciente a un contratista de defensa no revelado, utilizando posteriormente el acceso para crear cuentas falsas y enviar correos electrónicos de spear-phishing a empleados de otro contratista de defensa y una firma consultora.

Además de los ataques de spear-phishing, los conspiradores se hicieron pasar por otras personas, en su mayoría mujeres, para ganarse la confianza de las víctimas y distribuir

malware en las computadoras de estas.

Se cree que Nasab, mientras trabajaba para la empresa de fachada, fue responsable de adquirir la infraestructura utilizada en la campaña, utilizando la identidad robada de una persona real para registrar un servidor y cuentas de correo electrónico.

Se le imputan cargos de conspiración para cometer fraude informático, conspiración para cometer fraude postal, fraude postal y robo de identidad agravado. En caso de ser declarado culpable de todos los cargos, Nasab podría enfrentar hasta 47 años de prisión.

A pesar de estar prófugo, el Departamento de Estado de EE. UU. ha ofrecido recompensas monetarias de hasta $10 millones por información que lleve a la identificación o localización de Nasab.

Mahak Rayan Afraz (MRA) fue identificada por primera vez por Meta en julio de 2021 como una empresa con sede en Teherán con vínculos con el Cuerpo de la Guardia Revolucionaria Islámica (IRGC), la fuerza armada de Irán encargada de defender el régimen revolucionario del país.

Este grupo de actividades, que también se superpone con Tortoiseshell, ha sido previamente vinculado a elaboradas campañas de ingeniería social, como hacerse pasar por un instructor de aeróbicos en Facebook en un intento de infectar la máquina de un empleado de un contratista de defensa aeroespacial con malware.

Estos acontecimientos coinciden con el anuncio de las fuerzas del orden alemanas sobre la desarticulación de Crimemarket, una plataforma de comercio ilícito de habla alemana con más de 180,000 usuarios, especializada en la venta de narcóticos, armas, lavado de dinero y otros servicios criminales.

Se han arrestado a seis personas en relación con la operación, incluido un sospechoso principal de 23 años, y las autoridades también incautaron teléfonos móviles, equipos informáticos, un kilogramo de marihuana, tabletas de éxtasis y 600,000 euros en efectivo.