El gobierno de Estados Unidos ha impuesto hoy sanciones a una compañía fachada que ocultó una operación de piratería masiva perpetrada por el gobierno iraní contra sus propios ciudadanos, empresas extranjeras y gobiernos en el extranjero.

Se impusieron sanciones a la *«Rana Intelligence Computing Company»*, también conocida como Rana Institute o Rana, así como a 45 empleados actuales y anteriores, como gerentes, programadores o expertos en piratería.

Funcionarios estadounidenses dijeron que Rana operaba como fachada del Ministerio de Inteligencia y Seguridad de Irán (MOIS). Los principales deberes de Rana eran montar campañas de piratería nacionales e internacionales.

A través de sus operaciones locales, Rana ayudó a monitorear a ciudadanos iraníes, disidentes, periodistas, ex empleados del gobierno, ambientalistas, refugiados, estudiantes, profesores y cualquier persona considerada una amenaza para el régimen local.

Externamente, Rana también pirateó las redes gubernamentales de países vecinos, pero también empresas extranjeras en los sectores de viajes, académico y telecomunicaciones. Los funcionarios dijeron que Rana usó el acceso a las empresas extranjeras pirateadas para rastrear a las personas que el MOIS consideraba una amenaza.

A lo largo de los años, las operaciones de piratería de Rana dejaron un largo rastro de pistas que las empresas de seguridad cibernética rastrearon hasta Irán.

Las investigaciones sobre estas operaciones pasadas vinculadas a Rana se pueden encontrar en informes de seguridad cibernética sobre las actividades de un grupo de piratería conocido como APT39, Chafer, Cadelspy, Remexi o ITG07, todos los nombres diferentes fueron dados por distintas firmas de seguridad, pero se refieren al mismo actor de amenazas, Rana.

Sin embargo, durante mucho tiempo, nadie supo siquiera que Rana existía, y mucho menos que era una empresa fachada para APT39 y el régimen iraní.

ZDNet publicó un artículo en mayo de 2019 sobre Rana, en el que documentó la filtración de información confidencial relacionada con grupos de piratería iraníes.

En ese momento, entidades filtraron el código fuente del malware APT34, datos sobre los servidores backends de MuddyWater y fragmentos de documentos internos de Rana etiquetados como «*secretos*».

> *«Estos documentos contienen listas de víctimas, estrategias de ciberataques, supuestas áreas de acceso, una lista de empleados y capturas de pantalla de sitios web internos relevantes para los sistemas de espionaje»*, dijo la compañía israelí ClearSky en mayo de 2019.

En ese momento, la filtración de Rana se consideró extraña porque no encajaba con las otras dos. Las primeras dos filtraciones fueron realizadas por APT34 y MuddyWater, fueron dos grupos de piratas iranías muy conocidos.

Por otro lado, se describió a Rana como un contratista del gobierno.

En ese entonces, las empresas de seguridad sospechaban que Rana también era una APT (Amenaza Persistente Avanzada) iraní, pero nadie podía vincular a Rana con ningún grupo conocido.

El misterio se resolvió hoy. En comunicados de prensa del Departamento del Tesoro de Estados Unidos y la Oficina Federal de Investigaciones, el gobierno de Estados Unidos vinculó formalmente a Rana con APT39 y el MOIS por primera vez.

Según los comunicados, algunas de estas operaciones podrían haber cruzado la línea de la recopilación de inteligencia a los abusos contra los derechos humanos, como arrestos injustificados, seguidos de intimidación física y psicológica por parte de agentes del MOIS.

Las sanciones de hoy prohíben a las empresas estadounidenses hacer negocios con Rana y

sus 45 empleados actuales o anteriores.

Al mismo tiempo que las sanciones de hoy, el FBI también emitió una notificación de la industria privada (PIN) con ocho conjuntos separados y distintos de malware utilizados por Rana (MOIS) para realizar sus actividades de intrusión en computadoras.