La popular compañía de software empresarial Citrix, que brinda servicios a la milicia de Estados Unidos, al FBI y muchas otras corporaciones, reveló el pasado fin de semana una violación masiva de datos de su red interna por parte de *«delincuentes cibernéticos internacionales».*

Citrix informó que el FBI advirtió el miércoles que piratas informáticos extranjeros comprometían sus sistemas de TI y robaron *«documentos comerciales»*, agregando que la compañía no sabe exactamente qué documentos obtuvieron los piratas informáticos ni cómo ingresaron.

Sin embargo, el FBI cree que los malhechores probablemente utilizaron un ataque de *«rociado de contraseñas»* donde los atacantes adivinaron contraseñas débiles para obtener una posición temprana en la red de la compañía para lanzar ataques más extensos.

> *«Aunque no está confirmado, el FBI informó que los piratas informáticos probablemente usaron una táctica conocida como la explotación de contraseñas, mediante uso masivo de contraseñas débiles. Una vez que lograron un punto de apoyo con acceso limitado, trabajaron para eludir capas adicionales de seguridad»,* dijo Citrix.

Aunque Citrix no reveló muchos detalles sobre la violación de seguridad, los investigadores de la firma de información de seguridad Resecurity, detallaron más sobre el asunto, diciendo que se alertó previamente a los Feds y Citrix sobre el *«ataque dirigido y la violación de datos».*

Resecurity afirmó que el grupo de hacers IRIDIUM respaldado por Irán, golpeó a Citrix en diciembre del año pasado y nuevamente el lunes 4 de marzo, robando al menos 6 TB de archivos internos confidenciales, incluidos correos electrónicos, planos y otros documentos.

IRIDIUM es un grupo de piratería vinculado a Irán que también estuvo detrás de los recientes ataques cibernéticos contra más de 200 agencias gubernamentales de todo el mundo,

compañías de petróleo y gas, compañías tecnológicas, entre otras.

Las técnicas de IRIDIUM incluyen eludir las autenticaciones de múltiples factores para aplicaciones y servicios críticos para un acceso no autorizado adicional a canales VPN y SSO.

La violación masiva de datos en Citrix fue identificada como parte de *«una sofisticada campaña de espionaje cibernético respaldada por un estado-nación debido a la fuerte focalización en el gobierno, el complejo militar-industrial, las compañías de energía, las instituciones financieras y las grandes empresas involucradas en áreas críticas de la economía»,* dijo Resecurity.

> *«Basados en nuestro análisis reciente, los actores de amenazas aprovecharon una combinación de herramientas, técnicas y procedimientos (TTP) que les permiten llevar a cabo intrusiones en la red para acceder al menos a 6 terabytes de datos confidenciales almacenados en la red empresaria del Citrix, incluida la correspondencia por correo electrónico, archivos en recursos compartidos en red y otros servicios utilizados para la gestión de proyectos y adquisiciones»,* agrego.

Charles Yoo, presidente de Resecurity, dijo a NBC que IRIDIUM se abrió camino en la red interna de Citrix hace unos diez años, y que ha estado acechando al sistema de la compañía desde entonces.

La compañía con sede en Florida destacó que no había indicios de que los hackers comprometieran ningún producto o servicios de Citrix, y que lanzara una *«investigación forense»*, además de contratar a una de las principales compañías de seguridad cibernética y realizara *«acciones»* para asegurar su red interna.

Al igual que la violación de la OPM, las consecuencias del incidente de seguridad de Citrix podrían afectar a una gama más amplia de objetivos, ya que la compañía posee datos confidenciales de otras compañías, incluida la infraestructura crítica, el gobierno y las empresas.