Microsoft ha ampliado las funcionalidades de registro gratuito para todas las agencias federales de los Estados Unidos que utilizan Microsoft Purview Audit, sin importar el nivel de licencia, más de seis meses después de que se diera a conocer una campaña de ciberespionaje vinculada a China dirigida a dos docenas de organizaciones.

> La Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) informó que *«Microsoft activará automáticamente los registros en las cuentas de los clientes y extenderá el período de retención predeterminado de los registros de 90 días a 180 días».*

Asimismo, se indicó que estos datos proporcionarán nuevas telemetrías para ayudar a más agencias federales a cumplir con los requisitos de registro establecidos por el Memorándum M-21-31 de la Oficina de Administración y Presupuesto (OMB).

En julio de 2023, Microsoft reveló que un grupo de actividad estatal con sede en China, identificado como Storm-0558, obtuvo acceso no autorizado a aproximadamente 25 entidades en los Estados Unidos y Europa, así como a un pequeño número de cuentas individuales de consumidores relacionadas.

La compañía señaló que *«Storm-0558 opera con un alto nivel de destreza técnica y seguridad operativa».* Además, indicó que los actores están plenamente conscientes del entorno del objetivo, las políticas de registro, los requisitos de autenticación, así como las políticas y procedimientos.

Aunque se cree que la campaña comenzó en mayo de 2023, fue detectada un mes después de que una agencia federal de los Estados Unidos, posteriormente identificada como el Departamento de Estado, descubriera actividad sospechosa en los registros de auditoría no clasificados de Microsoft 365 y lo reportara a Microsoft.

La violación fue identificada mediante el aprovechamiento de un registro mejorado en Microsoft Purview Audit, específicamente utilizando la acción de auditoría del buzón

MailItemsAccessed que generalmente está disponible para los suscriptores Premium.

Microsoft posteriormente reconoció que un error de validación en su código fuente permitió que Storm-0558 falsificara tokens de Azure Active Directory (Azure AD) utilizando una clave de firma de consumidor de cuenta Microsoft (MSA) y luego los utilizará para penetrar en los buzones.

Se estima que los atacantes robaron al menos 60,000 correos electrónicos no clasificados de cuentas de Outlook pertenecientes a funcionarios del Departamento de Estado destinados en Asia Oriental, el Pacífico y Europa, según informó Reuters en septiembre de 2023. Beijing ha negado las acusaciones.

La empresa también enfrentó una intensa atención por no proporcionar capacidades de registro básicas pero cruciales a entidades que utilizan los planes más caros E5 o G5, lo que llevó a la compañía a realizar ajustes.

> *«Cumplimos plenamente con la vital importancia que desempeña el registro avanzado para permitir que las agencias federales detecten, respondan y prevengan incluso los ciberataques más sofisticados perpetrados por actores respaldados por estados con recursos significativos. Por esta razón, hemos estado colaborando en todo el gobierno federal para brindar acceso a registros avanzados de auditoría»,* afirmó Candice Ling de Microsoft.