¿Puede el ransomware seguir accediendo a los datos almacenados en servicios en la nube como OneDrive o Google Drive?

Respuesta breve: Sí. Aunque el almacenamiento en la nube estuvo alguna vez fuera del alcance del ransomware, los atacantes han adaptado sus métodos y ahora pueden apuntar a los datos almacenados en la nube mediante técnicas como el mapeo de unidades y, más comúnmente hoy en día, el robo de claves de API y tokens de sesión.

Cómo ha cambiado el enfoque del ransomware hacia los datos en la nube

Cuando el trabajo remoto impulsó un rápido cambio hacia el almacenamiento en la nube, tanto las empresas como los ciberdelincuentes se estaban adaptando al nuevo entorno al mismo tiempo. En las primeras etapas de este cambio, el ransomware normalmente no podía tocar los archivos almacenados en plataformas en la nube: si los datos residían en la nube en lugar de en un servidor local, los atacantes generalmente los dejaban en paz porque carecían de una vía directa hacia ellos.

Eso cambió cuando los atacantes aprendieron a conectar manualmente el almacenamiento en la nube, como una cuenta de Amazon, OneDrive o Google Drive, a un sistema infectado. Lo hicieron montando el almacenamiento en la nube como una letra de unidad local, de forma similar a cómo un dispositivo USB aparece como su propia unidad en una computadora. Una vez montados de esta manera, los archivos basados en la nube quedaban tan expuestos al cifrado como los archivos de un disco duro local.

La mayor amenaza actual: claves y tokens robados

A medida que el uso de la nube maduró, las tácticas de los atacantes volvieron a cambiar. En lugar de montar unidades manualmente, muchos ahora van tras las claves de API y los tokens de sesión: credenciales que otorgan acceso directo, a nivel de programa, a las cuentas y datos en la nube. Obtener una de estas es comparable a robar una contraseña, salvo que a menudo proporciona un acceso más amplio y rápido a los recursos en la nube que una contraseña robada por sí sola.

Este cambio es importante porque la misma velocidad y escalabilidad que hacen valiosa la computación en la nube para los equipos de TI legítimos ahora también está disponible para los atacantes. Entre los clientes de Cyber Crucible el año pasado, más de la mitad experimentó un intento de robo de un token de sesión en la nube destinado a secuestrar la sesión activa de un usuario, mientras que menos del 9 % sufrió algún compromiso real de datos. Esto sugiere que los atacantes están priorizando el robo de credenciales y tokens como su principal punto de entrada, con el robo de datos como objetivo secundario.

¿Los datos en la nube están automáticamente seguros?

El almacenamiento en la nube no garantiza protección contra el ransomware ni el robo de datos. Simplemente cambia el método que los atacantes deben usar para acceder a esos datos, desplazando el riesgo principal hacia el compromiso de credenciales y tokens de sesión en lugar del cifrado directo de archivos.

https://player.vimeo.com/video/1047006345?texttrack=es

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

Revision #2
Created 2026-07-24 02:11:37 UTC by Dennis Underwood
Updated 2026-08-06 18:34:22 UTC by Dennis Underwood