Se descubrió una *«funcionalidad peligrosa»* en la suite de Microsoft 365, que podría ser potencialmente abusada por un actor malicioso para rescatar archivos almacenados en SharePoint y OneDrive para lanzar ataques a la infraestructura de la nube.

El ataque de ransomware en la nube permite lanzar malware de cifrado de archivos para *«cifrar archivos almacenados en SharePoint y OneDrive de una forma que los haga irrecuperables sin copias de seguridad dedicadas o una clave de descifrado del atacante»,* dijo ProofPoint en un informe.

La secuencia de infección se puede realizar utilizando una combinación de API de Microsoft, scripts de interfaz de línea de comandos (CLI) y scripts de PowerShell, agregó la compañía.

El ataque, en esencia, depende de una función de Microsoft 365 llamada AutoSave, que crea copias de versiones de archivos anteriores cuando los usuarios realizan ediciones en un archivo almacenado en OneDrive o SharePoint Online.

Comienza con la obtención de acceso no autorizado a la cuenta de SharePoint u OneDrive de un usuario objetivo, seguido por el abuso del acceso para exfiltrar y cifrar archivos. Las tres vías más comunes para obtener el punto de apoyo inicial implican la violación directa de la cuenta por medio de ataques de phishing o fuerza bruta, engañar a un usuario para que autorice una aplicación OAuth de terceros no autorizada o tomar el control de la sesión web de un usuario que ha iniciado sesión.

Pero una diferencia en la actividad tradicional de ransomware de punto final en este ataque es que la fase de cifrado requiere bloquear cada archivo en SharePoint Online o OneDrive más que el límite de versión permitido.

Microsoft elaboró el comportamiento de control de versiones en su documentación de la siguiente forma:

> *«Algunas organizaciones permiten versiones ilimitadas de archivos y otras aplican*

> *limitaciones. Es posible que descubra, después de registrar la última versión de un archivo, que falta una versión anterior. Si su versión más reciente es la 101.0 y nota que ya no hay una versión 1.0, significa que el administrador configuró la biblioteca para permitir solo 100 versiones principales de un archivo. La adición de la versión 101 hace que se elimine la primera versión. Solo quedan las versiones 2.0 a 101.0. De manera similar, si se agrega una versión 102, solo quedan las versiones 3.0 a 102.0».*

Al aprovechar el acceso a la cuenta, un atacante puede crear demasiadas versiones de un archivo o, de forma alternativa, reducir el límite de versiones de una biblioteca de documentos a un número bajo como «1» y luego cifrar cada archivo dos veces.

> *«Ahora todas las versiones originales (antes del atacante) de los archivos se pierden, dejando solo las versiones cifradas de cada archivo en la cuenta de la nube. En este punto, el atacante puede pedir un rescate a la organización»,* explicaron los investigadores.

Microsoft, en respuesta a los hallazgos, dijo que las versiones anteriores de los archivos pueden recuperarse y restaurarse potencialmente durante 14 días adicionales con la ayuda del Soporte de Microsoft, un proceso que Proofpoint descubrió que no tuvo éxito.

> *«Esta técnica requiere que un usuario ya haya sido completamente comprometido por un atacante. Alentamos a nuestros clientes a practicar hábitos informáticos seguros, lo que incluye tener precaución al hacer clic en enlaces a páginas web, abrir archivos adjuntos desconocidos o aceptar transferencias de archivos»*, dijo un portavoz de Microsoft.

Para mitigar los ataques, se recomienda aplicar una política de contraseña segura, exigir la

autenticación multifactor (MFA), evitar descargas de datos a gran escala en dispositivos no administrados y mantener copias de seguridad externas periódicas de archivos en la nube con datos confidenciales.

Microsoft por su parte, llamó aún más la atención sobre una función de detección de ransomware de OneDrive que notifica a los usuarios de Microsoft 365 sobre un posible ataque y permite a las víctimas restaurar sus archivos.

Microsoft también alienta a los usuarios comerciales a utilizar el acceso condicional para bloquear o limitar el acceso al contenido de SharePoint y OneDrive desde dispositivos no administrados.

> *«Los archivos almacenados en un estado híbrido tanto en el punto final como en la nube, como a través de carpetas de sincronización en la nube, reducirán el impacto de este nuevo riesgo, ya que el atacante no tendrá acceso a los archivos locales del punto final. Para realizar un flujo de rescate completo, el atacante tendrá que comprometer el punto final y la cuenta de la nube para acceder al punto final y a los archivos almacenados en la nube»,* dijeron los investigadores.