Los hackers podrían aprovechar una vulnerabilidad sin parchear en Google Drive para distribuir archivos maliciosos disfrazados de documentos o imágenes legítimos, lo que permitiría a los atacantes realizar ataques de spear-phishing con una tasa de éxito bastante alta.

El problema de seguridad del que Google tiene conocimiento pero no ha corregido, reside en la funcionalidad «*administrar versiones*« que ofrece Google Drive, que permite a los usuarios cargar y administrar diferentes versiones de un archivo, así como en la forma en que su interfaz proporciona una nueva versión de los archivos a los usuarios.

La gestión de versiones debería permitir a los usuarios de Google Drive actualizar una versión anterior de un archivo con una nueva versión que tenga la misma extensión de archivo, pero no es así.

Según A. Nikoci, un administrador de sistemas profesional, que informó la falla a Google y luego la reveló públicamente, el usuarios afectado permite funcionalmente a los usuarios cargar una nueva versión con cualquier extensión de archivo para cualquier archivo existente en el almacenamiento en la nube, aún con un ejecutable malicioso.

Como se observa en los videos de Nikoci, al hacerlo, una versión legítima del archivo que ya se ha compartido entre un grupo de usuarios puede ser reemplazada por un archivo malicioso, que cuando se obtiene una vista previa en línea no indica los cambios realizados recientemente, pero cuando se descargan se pueden utilizar para infectar sistemas específicos.

> *«Google le permite cambiar la versión del archivo sin verificar si es del mismo tipo. Ni siguiera forzaron la misma extensión»,* dijo Nikoci.

No hace falta decir que el problema deja la puerta abierta para campañas de spear-phishing altamente efectivas que aprovechan la prevalencia generalizada de servicios en la nube como Google Drive para distribuir malware.

El desarrollo se produce cuando Google solucionó recientemente una falla de seguridad en Gmail que podría haber permitido a un atacante enviar correos electrónicos falsificados que imitan a cualquier cliente de Gmail o G Suite, incluso cuando las estrictas políticas de seguridad DMARC/SPF están habilitadas.

Las estafas de spear-phishing por lo general intentan engañar a los destinatarios para que abran archivos adjuntos maliciosos o hagan clic en enlaces que aparentan ser inofensivos, proporcionando de este modo información confidencial.

Este problema es parecido. La función de actualización de archivos de Google Drive está destinada a ser una forma sencilla de actualizar archivos compartidos, incluida la capacidad de reemplazar el documento con una versión completamente nueva del sistema. De esta forma, el archivo compartido se puede actualizar sin cambiar su enlace.

Sin embargo, sin ninguna validación para las extensiones de archivo, el fallo podría tener consecuencias potencialmente graves cuando los usuarios del archivo compartido, al recibir una notificación del cambio por correo electrónico, terminan descargando el documento e infectando de forma involuntaria sus sistemas con malware.

El escenario podría aprovecharse para montar ataques de caza de ballenas, una táctica de phishing que por lo general utilizan las bandas de criminales cibernéticos para hacerse pasar por personal de alta dirección en una organización y apuntar a individuos específicos, con la esperanza de robar información confidencial o obtener acceso a sus sistemas informáticos.

Lo que es peor, Google Chrome parece confiar implícitamente en los archivos descargados de Google Drive aún cuando son detectados por otro software antivirus como maliciosos.

Aunque no existe evidencia de que esta vulnerabilidad haya sido explotada en la naturaleza, no sería difícil para los atacantes reutilizarla para su beneficio debido a que los servicios en la nube han sido un vehículo para la entrega de malware en distintos ataques de spear-phishing en los últimos meses.

A inicios del año, Zscaler identificó una campaña de phishing que empleaba Google Drive para descargar un compromiso inicial de publicación de robo de contraseñas.

El mes pasado, Check Point Researh y Cofense destacaron una serie de nuevas campañas en las que se encontraron actores de amenazas no solo utilizando correos electrónicos no deseados para incrustar malware alojado en servicios como Dropbox y Google Drive, sino también explotando servicios de almacenamiento en la nube para alojar páginas de phishing.