La utilización de Cloudflare R2 por parte de agentes de amenazas para albergar páginas de phishing ha experimentado un incremento de 61 veces durante los últimos seis meses.

> *«La mayoría de las campañas de phishing se centran en obtener credenciales de inicio de sesión de Microsoft, aunque también se han encontrado algunas páginas dirigidas a Adobe, Dropbox y otras aplicaciones en la nube»,* comentó Jan Michael, investigador de seguridad de Netskope.

Cloudflare R2, similar a servicios como Amazon Web Service S3, Google Cloud Storage y Azure Blob Storage, es un servicio de almacenamiento de datos diseñado para la nube.

Esta tendencia surge a medida que el número total de aplicaciones en la nube desde las cuales se originan descargas de malware ha aumentado a 167, destacando Microsoft OneDrive, Squarespace, GitHub, SharePoint y Weebly como las cinco principales fuentes.

Las campañas de phishing identificadas por Netskope no solo utilizan Cloudflare R2 para distribuir páginas estáticas de phishing, sino que también aprovechan la oferta Turnstile de la empresa, un reemplazo de CAPTCHA, para ocultar estas páginas detrás de barreras anti-bot y así evadir la detección.

Este enfoque impide que escáneres en línea, como urlscan.io, puedan acceder al sitio de phishing real, ya que la prueba CAPTCHA resulta en un fallo.

Además, como estrategia adicional para evadir la detección, los sitios maliciosos están diseñados para cargar el contenido únicamente cuando se cumplen ciertas condiciones.

> *«El sitio web malicioso requiere que un sitio de referencia incluya una marca de tiempo después de un símbolo de almohadilla en la URL para mostrar la página de phishing real. Por otro lado, el sitio de referencia necesita recibir un sitio de phishing como parámetro»,* explicó Michael.

En caso de que no se proporcione un parámetro de URL al sitio de referencia, los visitantes son redirigidos a www.google[.]com.

Esta tendencia surge un mes después de que la compañía de ciberseguridad revelara detalles sobre una campaña de phishing que alojaba sus páginas de inicio de sesión falsas en AWS Amplify, con el propósito de robar credenciales bancarias y de Microsoft 365 de los usuarios, junto con detalles de pago con tarjeta a través de la API de Bot de Telegram.