La popular plataforma de intercambio de noticias sociales Reddit, reveló que fue víctima de un incidente de seguridad que permitió a hackers no identificados obtener acceso no autorizado a documentos internos, código y algunos sistemas comerciales no especificados.

La compañía lo atribuyó a un *«ataque de phishing sofisticado y altamente dirigido»* que tuvo lugar el 5 de febrero de 2023, dirigido a sus empleados.

El ataque implicó el envío de *«indicaciones que suenan plausibles»* que redirigen a un sitio web que se hace pasar por el portal de intranet de Reddit en un intento de robar credenciales y tokens de autenticación de dos factores (2FA).

Se cree que las credenciales de un solo empleado fueron suplantadas de esta forma, lo que permitió al atacante acceder a los sistemas internos de Reddit. El empleado afectado autoinformó el hackeo.

Sin embargo, la compañía enfatizó que no existe evidencia que sugiera que sus sistemas de producción fueron violados o que los datos no públicos de los usuarios se vieron comprometidos. No hay indicios de que la información a la que se accedió haya sido publicada o distribuida en línea.

> *«La exposición incluyó información de contacto limitada para (actualmente cientos de) contactos y empleados de la compañía (actuales y anteriores), así como información limitada de anunciantes»*, dijo Reddit.

Además, dijo que *«recientemente se han informado ataques de phishing similares»* sin tomar nombres específicos. No reveló a qué código fuente se accedió después de un lapso de seguridad.

El desarrollo es otra indicación de cómo los hackers están encontrando cada vez más formas de burlar el 2FA configurando páginas similares que son capaces de realizar ataques de adversario en el medio (AitM).