Okta, una empresa especializada en la gestión de identidades y el control de acceso, ha emitido una alerta acerca de una reciente oleada de ataques de ingeniería social dirigidos a los agentes de servicio de atención técnica de clientes en Estados Unidos.

Los atacantes buscan engañar a los agentes para que restablezcan la autenticación de múltiples factores (MFA) para usuarios con altos niveles de privilegios, lo que les permitiría obtener acceso administrativo total a la cuenta de Okta del individuo afectado.

Metodología de los ataques

Estos ataques por lo general comienzan con un correo electrónico proveniente de una cuenta comprometida, como la de un ejecutivo u otro individuo de alto perfil, solicitando al agente de servicio de atención técnica restablecer la MFA con fines de seguridad o para resolver problemas.

Si el agente cae en la artimaña, será redirigido a un sitio web falso de Okta que aparenta ser auténtico, y luego se le instará a ingresar sus credenciales.

Una vez que los atacantes obtienen las credenciales del agente, pueden iniciar sesión en la cuenta de Okta de la víctima, deshabilitar la MFA y obtener acceso administrativo completo.

¿Cómo protegerse?

Para resguardarse de estos ataques, es fundamental mantenerse alerta y mostrar escepticismo frente a solicitudes no solicitadas. Nunca ingrese sus credenciales en un sitio web en el que no confíe y siempre verifique que la URL coincida con el sitio web genuino de Okta.

Asegúrese de mantener actualizado su software de MFA y capacite a los agentes de servicio de atención técnica para detectar y reportar ataques de phishing. Además, utilice contraseñas robustas, active la MFA en todas sus cuentas, mantenga actualizado su software y ejerza cautela al compartir información personal en línea.

Sea precavido ante correos electrónicos o llamadas no solicitadas y reporte de inmediato cualquier actividad sospechosa.

Siguiendo estos consejos, podrá ayudar a protegerse de los atacantes de Okta y otras amenazas cibernéticas.

Recuerde que, incluso los sistemas de administración de identidades y accesos más seguros, pueden ser vulnerables ante los ataques de ingeniería social. Manténgase informado y tome medidas proactivas para salvaguardar sus cuentas e información personal.