El proveedor de servicios de identidad Okta emitió una advertencia el viernes sobre ataques de ingeniería social organizados por actores de amenazas con el objetivo de obtener permisos de administrador de alto nivel.

> *«En las últimas semanas, varios clientes de Okta con sede en los Estados Unidos han informado de un patrón constante de ataques de ingeniería social contra el personal del servicio de asistencia de TI. En estos ataques, los perpetradores han intentado convencer al personal del servicio de asistencia de TI para que restablezca todos los factores de autenticación multifactor (MFA) inscritos por usuarios altamente privilegiados»,* declaró la empresa.

Los atacantes luego procedieron a abusar de las cuentas de Okta Super Administrador altamente privilegiadas para suplantar a usuarios dentro de la organización comprometida. Según la compañía, esta campaña se llevó a cabo entre el 29 de julio y el 19 de agosto de 2023.

Aunque Okta no reveló la identidad de los actores de amenazas, las tácticas empleadas muestran todas las características distintivas de un grupo de actividad conocido como Muddled Libra. Se ha sugerido que este grupo tiene cierta similitud con Scattered Spider y Scatter Swine.

En el núcleo de estos ataques se encuentra una herramienta de phishing comercial llamada 0ktapus, que proporciona plantillas predefinidas para crear portales de autenticación falsos de aspecto realista y, en última instancia, para recopilar credenciales y códigos de autenticación multifactor (MFA) falsos. Además, esta herramienta incluye un canal de control y comando (C2) incorporado a través de Telegram.

Palo Alto Networks Unit 42 informó anteriormente en junio de 2023 a The Hacker News que varios actores de amenazas están *«incorporándola a su conjunto de herramientas».* Además, señaló que *«el simple uso del kit de phishing 0ktapus no necesariamente califica a un actor de amenazas como parte de Muddled Libra».*

También se indicó que no se encontró suficiente información sobre los objetivos, la persistencia o los objetivos para confirmar una relación entre el actor y un grupo no categorizado rastreado por Mandiant, propiedad de Google, bajo el nombre de UNC3944, que también se sabe que emplea técnicas similares.

Phelix Oluoch, investigador de Trellix, señaló en un análisis publicado el mes pasado que *«Scattered Spider ha sido observado principalmente atacando a empresas de telecomunicaciones y organizaciones de externalización de procesos comerciales (BPO)».* Sin embargo, actividades recientes indican que este grupo ha ampliado sus objetivos a otros sectores, incluyendo organizaciones de infraestructura crítica.

En los ataques más recientes, se afirma que los actores de amenazas ya poseen contraseñas de cuentas de usuario privilegiadas o *«tienen la capacidad de manipular el flujo de autenticación delegada a través de Active Directory (AD)»* antes de contactar al servicio de asistencia de TI de la empresa objetivo para solicitar el restablecimiento de todos los factores de MFA asociados con la cuenta.

Luego, se utiliza el acceso a las cuentas de Super Administrador para otorgar privilegios más altos a otras cuentas, restablecer autenticadores inscritos en cuentas de administradores existentes e incluso eliminar los requisitos de segundo factor en las políticas de autenticación en algunos casos.

> Okta señaló: *«El actor de amenazas fue observado configurando un segundo proveedor de identidad para actuar como una 'aplicación de suplantación' y acceder a aplicaciones dentro de la organización comprometida en nombre de otros usuarios. Este segundo proveedor de identidad, también controlado por el atacante, funcionaría como un proveedor de identidad 'fuente' en una relación de federación entrante (a veces llamada 'Org2Org') con el objetivo».*

> *«A través de este proveedor de identidad 'fuente', el actor de amenazas manipuló*

> *el parámetro de nombre de usuario de los usuarios objetivo en el segundo proveedor de identidad 'fuente' para que coincidiera con un usuario real en el proveedor de identidad 'objetivo' comprometido. Esto proporcionó la capacidad de iniciar sesión de forma única (SSO) en aplicaciones en el proveedor de identidad 'objetivo' como el usuario objetivo».*

Como medidas de mitigación, la empresa recomienda que los clientes refuercen la autenticación resistente al phishing, fortalezcan los procesos de verificación de identidad del servicio de asistencia, habiliten notificaciones para los usuarios finales sobre dispositivos nuevos y actividades sospechosas, y revisen y restrinjan el uso de roles de Super Administrador.