La solución ampliamente utilizada para la gestión de contraseñas, 1Password, informó que identificó actividad potencialmente peligrosa en su instancia de Okta el 29 de septiembre, tras la violación de su sistema de soporte, aunque reiteró que no se accedió a la información de los usuarios.

> Pedro Canahuati, Director de Tecnología de 1Password, señaló en un aviso emitido el lunes que *«inmediatamente terminamos la actividad, realizamos una investigación y no encontramos indicios de compromiso de datos de usuarios o sistemas críticos, ya sea aquellos que utilizan los empleados o los usuarios finales».*

Se cree que la brecha ocurrió mediante el uso de una cookie de sesión, después de que un miembro del equipo de tecnología compartiera un archivo HAR con el soporte de Okta. El atacante llevó a cabo las siguientes acciones:

- Intento de acceder al panel de control del usuario del miembro del equipo de tecnología, aunque Okta lo bloqueó.
- Actualización de un proveedor de identidad federada (IDP) existente asociado a nuestro entorno de Google en producción.
- Activación del IDP.
- Solicitud de un informe sobre los usuarios con privilegios administrativos.

La compañía informó que se percató de la actividad maliciosa después de que el miembro del equipo de tecnología recibiera un correo electrónico con respecto al informe de usuarios administrativos *«solicitado».*

1Password también comunicó que ha tomado varias medidas para fortalecer la seguridad, incluyendo la restricción de accesos desde IDPs no relacionados con Okta, la reducción de la duración de las sesiones de usuarios administrativos, la implementación de reglas más rigurosas para la autenticación de múltiples factores (MFA) para los administradores y la disminución de la cantidad de superadministradores.

> La empresa afirmó: *«En colaboración con el soporte de Okta, se determinó que este incidente comparte similitudes con una campaña conocida en la que los actores de amenazas comprometen cuentas de superadministradores y posteriormente intentan manipular los flujos de autenticación y establecer un proveedor de identidad secundario para suplantar a los usuarios dentro de la organización afectada».*

Vale la pena destacar que el proveedor de servicios de identidad ya había advertido sobre ataques de ingeniería social organizados por actores de amenazas con el fin de obtener permisos de administrador elevados.

Hasta el momento de esta redacción, no está claro si estos ataques guardan alguna relación con Scattered Spider (también conocido como 0ktapus, Scatter Swine o UNC3944), que ha sido conocido por enfocarse en Okta mediante ataques de ingeniería social con el propósito de obtener privilegios elevados.

Este desarrollo surge pocos días después de que Okta revelara que actores de amenazas no identificados utilizaron credenciales robadas para ingresar a su sistema de gestión de casos de soporte y sustraer archivos HAR sensibles que podrían emplearse para infiltrarse en las redes de sus clientes.

La empresa informó que el evento afectó aproximadamente al 1 por ciento de su base de clientes. Entre los otros clientes afectados por este incidente se incluyen BeyondTrust y Cloudflare.

> *«La actividad que observamos sugiere que llevaron a cabo una exploración inicial con la intención de permanecer sin ser detectados con el propósito de recopilar información para un ataque más sofisticado»,* indicó 1Password.