Click Studios, la compañía de software australiana detrás de la aplicación de administración de contraseñas Passwordstate, notificó a sus clientes que deben restablecer sus contraseñas después de un ataque a la cadena de suministro de software.

La compañía con sede en Adelaide, dijo que un mal actor utilizó técnicas sofisticadas para comprometer el mecanismo de actualización del software y lo utilizó para lanzar malware en las computadoras de los usuarios.

Al parecer, la violación ocurrió entre el 20 de abril a las 8:33 PM UTC y el 22 de abril a las 0:30 AM UTC, por un período total de aproximadamente 28 horas.

> *«Sólo los clientes que realizan mejoras In-Place entre las horas indicadas anteriormente, se cree que son afectados. Las actualizaciones manuales de Passwordstate no se ven comprometidas. Es posible que se haya recopilado los registros de contraseñas de los clientes afectados»,* dijo la compañía.

El desarrollo se informó por primera vez por el sitio de noticias de tecnología polaca Niebezpiecznik. No está claro quiénes son los atacantes o cómo comprometieron la función de actualización del administrador de contraseñas. Click Studios dijo que se está llevando a cabo una investigación sobre el incidente, pero dijo que *«el número de clientes afectados parece ser muy bajo».*

Passwordstate es una solución local basada en web utilizada para la gestión de contraseñas empresariales, que permite a las compañías almacenar contraseñas de forma segura, integrar la solución en sus aplicaciones y restablecer contraseñas en una variedad de sistemas, entre otros.

El software es utilizado por 29,000 clientes y 370,000 profesionales de seguridad y TI en todo el mundo, contando varias compañías Fortune 500 que abarcan verticales como banca, seguros, defensa, gobierno, educación y manufactura.

Según un análisis inicial compartido por la compañía de seguridad CSIS Group con sede en Dinamarca, la actualización con malware llegó en forma de archivo ZIP, «*passwordstate_upgrade.zip*», que contenía una versión modificada de una biblioteca llamada «*moserware.secretsplitter.dll*».

El archivo, a su vez, estableció contacto con un servidor remoto para obtener una carga útil de segunda etapa «*upgrade_service_upgrade.zip*», que extrajo los datos de Passwordstate y exportó la información a la red CDN del adversario. Click Studios dijo que el servidor fue retirado el 22 de abril a las 7:00 am UTC.

La lista completa de información comprometida incluye el nombre de la computadora, el nombre de usuario, nombre de dominio, nombre del proceso actual, ID del proceso actual, los ID de todos los procesos en ejecución, los nombres de todos los servicios en ejecución, el nombre para mostrar y estado, la dirección del servidor proxy de la instancia de Passwordstate, nombres de usuario y contraseñas.

Clic Studios lanzó un paquete de revisiones que ayudaría a los clientes a eliminar la DLL manipulada del atacante y sobrescribirla con una variante legítima. También se recomienda que las empresas restablezcan todas las credenciales asociadas con los sistemas externos (firewalls, VPN, etc.), así como la infraestructura interna, como los sistemas de almacenamiento, sistemas locales, entre otros, además de cualquier otra contraseña almacenada en Passwordstate.