El popular servicio de marketing por correo electrónico y boletines Mailchimp, reveló otra brecha de seguridad que permitió a los hackers acceder a una herramienta interna de soporte y administración de cuentas para obtener información sobre 133 clientes.

> *«El actor no autorizado realizó un ataque de ingeniería social contra los empleados y contratistas de Mailchimp y obtuvo acceso a cuentas seleccionadas de Mailchimp usando las credenciales de los empleados comprometidas en ese ataque»,* dijo la empresa propiedad de Intuit.

Mailchimp dijo que identificó el problema el 11 de enero de 2023 y afirmó que no hay evidencia de que la parte no autorizada haya violado los sistemas Intuit u otra información del cliente más allá de las 133 cuentas.

También dijo que los contactos principales de todas las cuentas afectadas fueron notificadas dentro de las 24 horas, y desde entonces ha ayudado a los usuarios a recuperar el acceso a sus cuentas.

Sin embargo, la compañía con sede en Atlanta no reveló el tiempo que el intruso permaneció en sus sistemas ni los tipos exactos de información a los que accedió.

Pero WooCommerce, que es una de las cuentas afectadas, dijo que el incidente expuso los nombres de los usuarios, las URL de las tiendas, las direcciones de correo electrónico, pero no sus dats de pago, además de las contraseñas u otra información confidencial.

Solo en el último año, Mailchimp ha sido víctima de dos violaciones diferentes, la primera de las cuales involucró a un hacker que obtuvo acceso no autorizado a 319 cuentas de clientes en abril de 2022 con el objetivo de llevar a cabo estafas de phishing criptográfico.

Después, en agosto de 2022, la compañía cayó en otro ataque de ingeniería social organizado por un grupo llamado 0ktapus (también conocido como Scatter Swine), que resultó en el compromiso de 216 cuentas de clientes.