

استخدام بيانات اعتماد ConnectWise المخترقة للوصول إلى 173 مستأجر Microsoft 365



استغل مهاجمون بيانات اعتماد Microsoft 365 مخترقة تعود لخدمة ConnectWise Cloud Backup للوصول غير المصرح به إلى 173 بيئة M365 تابعة للعملاء في حملة نشطة.

- اخترق مهاجمون مجهولون بيانات اعتماد Microsoft 365 تابعة لخدمة ConnectWise Cloud Backup
- استُخدمت بيانات الاعتماد المخترقة للوصول إلى 173 مستأجر Microsoft 365 تابع للعملاء دون تصريح
- ConnectWise Cloud Backup هي خدمة نسخ احتياطي واستعادة سحابية يستخدمها مزودو الخدمات المُدارة
- الحملة نشطة حالياً و قيد التحقيق من قبل باحثي الأمن السيبراني

نظرة عامة على الحادث

حدد باحثو الأمن السيبراني حملة نشطة استغل فيها مهاجمون بيانات اعتماد **Microsoft 365** مخترقة تعود لخدمة **ConnectWise Cloud Backup** للحصول على وصول غير مصرح به إلى بيانات العملاء. الخدمة، المعروفة سابقاً باسم SkyKick، هي منصة نسخ احتياطي واستعادة سحابية مصممة لمزودي الخدمات المُدارة. مكّنت بيانات الاعتماد المخترقة المهاجمين من تسجيل الدخول إلى 173 مستأجر Microsoft 365 منفصل يعود لعملاء ConnectWise.

مخاطر وصول الأطراف الثالثة

يسلط الحادث الضوء على المخاطر المرتبطة بوصول مزودي الخدمات الخارجيين إلى البيانات السحابية. تتطلب خدمة ConnectWise Cloud Backup وصولاً ذا صلاحيات مرتفعة إلى مستأجري Microsoft 365 للعملاء لتنفيذ عمليات النسخ الاحتياطي والاستعادة. عندما تُخترق بيانات اعتماد واحدة ذات وصول واسع، يمكن للمهاجمين استغلال علاقة الثقة هذه للتغلّب الجانبي عبر بيانات عملاء متعددة. يوضح نطاق الاختراق - 173 مستأجراً متأثراً - كيف يمكن لنقطة اختراق واحدة في البنية التحتية لمزود الخدمة أن تتسلسل عبر قاعدة عملائه بالكامل.

الوضع الحالي

تظل الحملة نشطة بينما يواصل الباحثون التحقيق في النطاق والأثر. يجب على المؤسسات التي تستخدم ConnectWise Cloud Backup أو خدمات مماثلة من أطراف ثالثة لها وصول مفوض إلى بيانات Microsoft 365 الخاصة بها مراجعة سجلات الوصول وأحداث المصادقة بحثاً عن نشاط مشبوه. لم يتم الكشف عن هوية المهاجمين أو أهدافهم النهائية.

ما يجب فعله الآن

1. مراجعة جميع صلاحيات وصول مزودي الخدمات الخارجيين إلى Microsoft 365 والمنصات السحابية الأخرى، مع توثيق الأذونات المفوضة والحسابات ذات الصلاحيات المرتفعة
2. تدقيق سجلات المصادقة لمستأجري Microsoft 365 لتحديد أي نشاط تسجيل دخول مشبوه من بيانات اعتماد ConnectWise Cloud Backup أو خدمات النسخ الاحتياطي الأخرى
3. تطبيق سياسات الوصول المشروط التي تتطلب مصادقة متعددة العوامل لجميع حسابات الخدمة ذات الوصول المفوض إلى البيانات السحابية
4. إنشاء مراقبة مستمرة لوصول الأطراف الثالثة ذي الصلاحيات المرتفعة، مع تنبيهات لأنماط المصادقة غير المعتادة أو الوصول من مواقع غير متوقعة
5. مراجعة وتحديث إجراءات إدارة مخاطر الموردين لتشمل مراجعات وصول منتظمة ومتطلبات تدوير بيانات الاعتماد لمزودي الخدمات المُدارة
6. التحقق من أن مزودي خدمات النسخ الاحتياطي والاستعادة يحتفظون ببيانات اعتماد منفصلة لكل عميل بدلاً من بيانات اعتماد مشتركة ذات وصول واسع