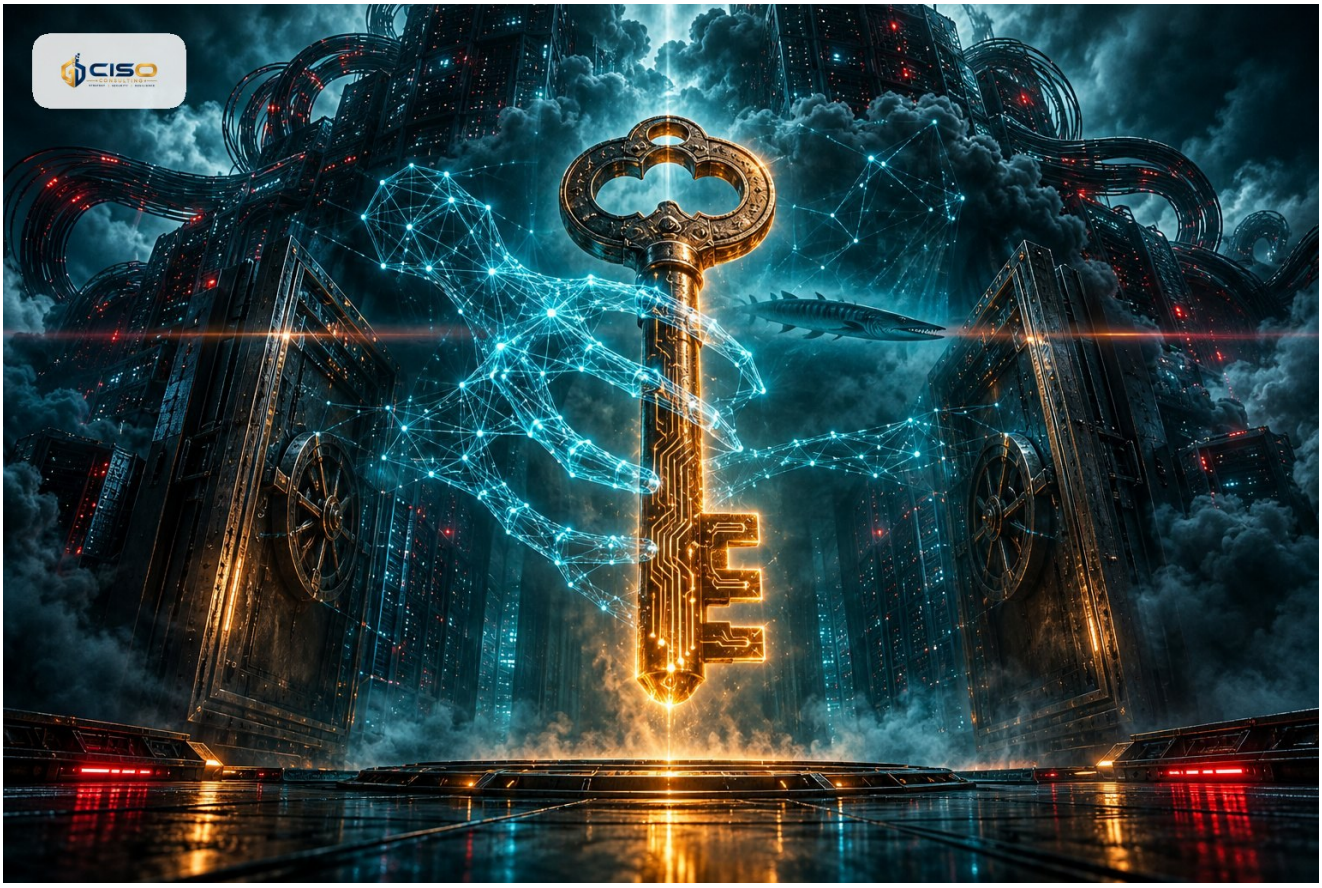
Barracuda تربط اختراق بيئتها السحابية بمفتاح وصول مسروق وإطار ARTEX للاختبار بالذكاء الاصطناعي



أفادت Barracuda بأن المهاجمين الذين اخترقوا بيئتها السحابية مطلع هذا الشهر استخدموا مفتاح وصول سحابي مسروقًا مع إطار ARTEX للاختبار بالذكاء الاصطناعي. ولا يتضمن المقتطف تفاصيل إضافية.

- تعرضت بيئة Barracuda السحابية، وهي شركة أمن شبكات وبريد إلكتروني، للاختراق مطلع هذا الشهر.
- استخدم المهاجمون مفتاح وصول سحابيًا مسروقًا.
- استعانوا كذلك بإطار ARTEX للاختبار الأمني المعتمد على الذكاء الاصطناعي.
- لا يوضح النص المتاح الأثر أو العملاء المتأثرين أو إجراءات المعالجة.

ما الذي أُعلن

ربطت Barracuda، المزوّدة لحلول أمن الشبكات والبريد الإلكتروني، اختراق بيئتها السحابية بهجوم جمع بين مفتاح وصول سحابي مسروق وإطار ARTEX للاختبار الأمني بالذكاء الاصطناعي. ووفق التقرير، وقع الاختراق مطلع هذا الشهر.

النص المتاح لنا مقتطف قصير فقط، ولا يوضح كيف جرى الحصول على المفتاح، ولا البيانات أو الأنظمة التي وصل إليها المهاجمون، ولا ما إذا تأثر عملاء، ولا ما اتخذته Barracuda من إجراءات. لذلك لم نذكر أيًّا من ذلك.

أهمية الخبر

يبرز الحادث أمرين: الأول أن بيانات اعتماد سحابية مكشوفة واحدة كانت كافية للدخول إلى بيئة مزوّد أمني. والثاني أن المهاجمين يستخدمون أدوات اختبار مدعومة بالذكاء الاصطناعي، وهو ما قد يسرّع استكشاف البيئة السحابية بعد الوصول إليها.

وبالنسبة للجهات التي تعتمد على Barracuda أو غيرها من مزوّدي الأمن، فالأجدى مراجعة تعرّضها هي بدل التكهن بتفاصيل هذه الحالة. ويُنصح بمتابعة بيانات Barracuda الرسمية وتحديث التقييم عند صدور تفاصيل إضافية.

المقاربة المقترحة

اعتبروا الخبر فرصة لمراجعة كيفية إصدار مفاتيح الوصول السحابية وتخزينها وتدويرها ومراقبتها في بيئتكم، ومدى سرعة علمكم بأي حادث لدى مزوّد يمسّكم.

ما يجب فعله الآن

1. حصر مفاتيح الوصول السحابية وبيانات اعتماد الخدمات، وإلغاء أو تدوير ما كان غير مستخدم أو واسع الصلاحيات أو طويل العمر.
2. تفعيل المراقبة والتنبيه لأي استخدام غير معتاد للمفاتيح السحابية، مثل مواقع جديدة أو نشاط API غير متوقع.
3. التحقق من استخدام منتجات Barracuda ومتابعة إشعاراتها الرسمية لأي توجيهات للعملاء.
4. مراجعة بنود الإبلاغ عن الحوادث في عقود مزوّدي الأمن والتأكد من تحديث جهات الاتصال.
5. إدراج سيناريوهات سرقة بيانات الاعتماد والهجمات المدعومة بالذكاء الاصطناعي في المراجعة السحابية القادمة أو تمرين المحاكاة.