هجوم على GlobeTopper: سرقة بيانات اعتماد API واسترداد بطاقات هدايا بقيمة 70 ألف دولار



تسبب هجوم سيبراني على GlobeTopper، موزّع بطاقات الهدايا الرقمية، بخسائر إيرادات تقدَّر بـ2.5 مليون دولار، وحصل المهاجم على بيانات اعتماد API واستردّ بطاقات بقيمة 70 ألف دولار.

- أفادت الشركة الأم iQSTEL برصد الاختراق في 22 أكتوبر، وإيقاف المنصة عن العمل فجر 23 أكتوبر.
- حصل المهاجم على بيانات اعتماد API ومفاتيح التكامل لبعض العملاء من الشركات، وجرى إلغاؤها واستبدالها.
- استُردّت بطاقات هدايا رقمية بقيمة 70 ألف دولار ولا يمكن حظرها أو استعادتها، وستتحمل الشركة الخسارة.
- أُطلقت منصة أعيد بناؤها على AWS في 31 أكتوبر، واستُعيدت العمليات التجارية على مراحل بدءًا من 1 نوفمبر.

- لا يزال التحقيق جاريًا لمعرفة ما إذا جرى الوصول إلى بيانات أخرى للعملاء أو بيانات شخصية أو مدفوعات أو مزوّدين.

تعرّضت GlobeTopper، وهي موزّع لبطاقات الهدايا الرقمية لقطاع الأعمال، لهجوم سيبراني عطّل عملياتها. وتقدّر شركتها الأم iQSTEL خسائر الإيرادات بنحو 2.5 مليون دولار، وتفيد بأن المهاجم استردّ بطاقات هدايا رقمية بقيمة 70 ألف دولار.

ما حدث

وفق إفصاح iQSTEL المقدَّم إلى هيئة الأوراق المالية والبورصات الأمريكية، رُصد الاختراق في 22 أكتوبر، ثم لوحظ نشاط غير مصرّح به إضافي في اليوم التالي، فأوقفت الشركة المنصة وجميع الخوادم المتأثرة فجر 23 أكتوبر. ونُشرت منصة أعيد بناؤها بالكامل على AWS في 31 أكتوبر، وعادت العمليات التجارية تدريجيًا بدءًا من 1 نوفمبر.

حصل المهاجم على بيانات اعتماد API ومفاتيح التكامل الخاصة ببعض عملاء الشركة من الأعمال. وقد أُلغيت هذه البيانات واستُبدلت، وزُوّد العملاء المتأثرون ببيانات جديدة مع قيود وصول إضافية. ولم ترصد الشركة حتى الآن أي استخدام غير مصرّح به لها.

ما لم يتضح بعد

ما زال التحقيق جاريًا لتحديد ما إذا جرى الوصول إلى بيانات أخرى للعملاء أو بيانات شخصية أو بيانات مدفوعات أو مزوّدين. وتقول الشركة إنها لا تستطيع حظر البطاقات المستردّة أو استعادتها. ولم تعدّ الحادثة جوهرية حتى الآن. ورفضت iQSTEL الإجابة عن أسئلة إضافية، ولم تُدرج أي مجموعة فدية الشركة ضمن ضحاياها.

أهمية الخبر

تستخدم متاجر التجزئة وتطبيقات التقنية المالية ومنصات المكافآت منصة GlobeTopper عبر واجهة API. وتبيّن الحادثة للجهات المرتبطة بمزوّدين مماثلين أن تسرّب بيانات التكامل قد يتحول إلى خسارة مالية مباشرة، وأن توقف المزوّد قد يعطّل الخدمات.

ما يجب فعله الآن

1. حصر بيانات اعتماد API ومفاتيح التكامل المستخدمة مع المزوّدين الخارجيين، والتأكد من وجود مالك لكل منها وجدول انتهاء صلاحية أو تدوير.
2. تقييد المفاتيح بنطاقات عناوين IP والصلاحيات وحدود المعاملات، ومراقبة أي أحجام غير معتادة في الإصدار أو الاسترداد.
3. التأكد من أن عقود المزوّدين تُلزمهم بالإبلاغ الفوري عن الحوادث وإلغاء بيانات الاعتماد، بما يتوافق مع متطلبات الأطراف الخارجية في ضوابط الأمن السيبراني الأساسية (NCA ECC) وإطار الأمن السيبراني للقطاع المالي (SAMA CSF) حيثما ينطبق.
4. اختبار القدرة على تدوير المفاتيح المخترقة بسرعة وعلى تشغيل الخدمات عند توقف أحد المزوّدين.
5. على المؤسسات التي تستخدم GlobeTopper تدوير بيانات الاعتماد ومراجعة النشاط منذ أواخر أكتوبر.