دعوات مزيفة لفعاليات OpenAI وSpaceX وAnthropic لسرقة بيانات دخول حسابات Microsoft وGoogle



يرسل مهاجمون دعوات مزيفة لفعاليات تستغل أسماء OpenAI وSpaceX وAnthropic لاستدراج الموظفين، عبر منصتين للتصيد كخدمة تسرق بيانات دخول Microsoft وGoogle وجلسات المصادقة.

- دعوات مزيفة لفعاليات تحمل أسماء OpenAI وSpaceX وAnthropic تستهدف الموظفين.
- تقف وراء الحملات منصتان مختلفتان للتصيد كخدمة.
- الهدف سرقة بيانات دخول حسابات Microsoft وGoogle.
- تستهدف الهجمات جلسات المصادقة أيضاً وليس كلمات المرور فقط.
- يجري استغلال علامات تقنية معروفة كطُعم.

ما الذي ورد في التقرير

وفق ما نشره موقع BleepingComputer، يرسل مهاجمون دعوات إلى فعاليات مزعومة مرتبطة بـ OpenAI وSpaceX وAnthropic بهدف استدراج الموظفين إلى هجمات تصيّد. وتعتمد الحملات على منصتين مختلفتين للتصيد كخدمة، توفران للمهاجمين بنية جاهزة لهذا النوع من الاحتيال.

يتمثل الهدف في سرقة بيانات دخول حسابات Microsoft وGoogle إضافة إلى جلسات المصادقة. وتكمن أهمية استهداف الجلسات في أن الجلسة المسروقة قد تتيح الوصول إلى الحساب حتى لو لم تكفِ كلمة المرور وحدها.

أهمية الخبر

يأتي الطُعم على شكل دعوة من علامة تقنية بارزة، وهي رسالة قد تثير فضول الموظفين فيفتحونها خلال العمل. وتمنح حسابات Microsoft وGoogle المؤسسية عادةً وصولًا إلى البريد والمستندات وخدمات الأعمال، لذا قد يترتب على اختراق حساب واحد أثر واسع في جهة خاضعة للتنظيم.

ولا يقدّم المقتطف المتاح من المصدر تفاصيل إضافية عن حجم الحملات أو الضحايا أو المنصتين بعينهما، ولذلك ينبغي التعامل مع الخبر بوصفه مؤشراً على أسلوب مهاجمين قائم حالياً، لا تهديداً مؤكداً لقطاع بعينه.

الخطوات المقترحة

تجمع الاستجابة العملية بين توعية المستخدمين وتقوية ضوابط تسجيل الدخول والجاهزية للتصرف سريعاً عند الاشتباه في تعرض حساب. وتمثل الإجراءات أدناه نقطة انطلاق مناسبة.

ما يجب فعله الآن

1. تنبيه الموظفين إلى أن الدعوات غير المطلوبة لفعاليات من شركات تقنية معروفة قد تكون تصيداً، وحثهم على الإبلاغ بدلًا من النقر.
2. مراجعة ضوابط تسجيل الدخول في Microsoft وGoogle، مع تفضيل المصادقة متعددة العوامل المقاومة للتصيد حيثما توفرت.
3. التأكد من القدرة على إلغاء الجلسات النشطة وإعادة تعيين بيانات الدخول بسرعة عند الاشتباه باختراق حساب.
4. رصد أنشطة تسجيل الدخول غير المعتادة واستخدام جلسات أو رموز جديدة في حسابات Microsoft وGoogle.
5. إدراج طُعم دعوات الفعاليات في أقرب تمرين للتوعية بالتصيد.