UAT-11985 تستخدم دعوات فعاليات مزيفة في تصيّد وسيط ضد حسابات Google لمنتسبي مؤسسات بحثية في تايوان



كشف باحثون عن حملة تصيّد موجّه تنفذها جهة تهديد متقدمة ضد منتسبي مؤسسات بحثية في تايوان، توجّه الضحايا إلى إطار وسيط يسرق بيانات حسابات Google ورموز المصادقة متعددة العوامل.

- الحملة تصيّد موجّه تنفذه جهة تهديد متقدمة مستمرة تُتتبَّع باسم UAT-11985.
- المستهدفون أفراد مرتبطون بمؤسسات بحثية في تايوان.
- وفق عنوان الخبر، يعتمد الطُّعم على دعوات فعاليات مزيفة.
- يُحوَّل الضحايا إلى إطار تصيّد من نوع الوسيط (AitM).
- صُمم الإطار لالتقاط بيانات دخول حسابات Google ورموز المصادقة متعددة العوامل.

ما الذي ورد في التقرير

نشر باحثون تفاصيل حملة تصيّد موجّه تُنسب إلى جهة تهديد متقدمة مستمرة تُتتبَّع باسم UAT-11985، وتستهدف أفرادًا مرتبطين بمؤسسات بحثية في تايوان. ووفق عنوان التقرير، يقوم الطُّعم على دعوة فعالية مزيفة.

يُحوَّل من يفتح الرابط إلى إطار تصيّد من نوع الوسيط (AitM) صُمم لسرقة بيانات دخول حسابات Google مع رموز المصادقة متعددة العوامل (MFA).

لماذا يهمّ ذلك

تقع أطر AitM بين المستخدم وخدمة تسجيل الدخول الحقيقية، فيمكنها التقاط الرمز المؤقت الذي يدخله الضحية إضافة إلى كلمة المرور. وهذا يعني أن المصادقة متعددة العوامل القائمة على الرموز وحدها لا تحمي الحساب بالكامل من هذا الأسلوب. ولا يتضمن المقتطف المتاح تفاصيل تقنية إضافية أو أعداد الضحايا أو الإسناد الكامل، ولن نتجاوز ما ورد فيه.

ورغم أن الحملة موثقة ضد جهات في تايوان، فالأسلوب غير مرتبط بمنطقة بعينها. فالباحثون والأكاديميون وكل من يتلقى دعوات فعاليات ومؤتمرات، ومنهم العاملون في مؤسسات سعودية تتعاون مع شركاء بحثيين، قد يتعرضون لطُّعم مشابه.

الموقف العملي

يُنصح بالتعامل بحذر مع دعوات الفعاليات غير المتوقعة التي تطلب تسجيل الدخول بحساب Google، ومراجعة مدى قدرة ضوابط الهوية لديكم على مقاومة تمرير بيانات الاعتماد لحظيًا. وفيما يلي خطوات متناسبة للجهات المنظمة.

ما يجب فعله الآن

1. تنبيه الموظفين، ولا سيما العاملين في البحث والأوساط الأكاديمية والتواصل مع الشركاء، من دعوات الفعاليات المزيفة التي تقود إلى صفحات تسجيل دخول Google.
2. نقل المستخدمين ذوي الصلاحيات العالية والمخاطر الأعلى، متى أمكن، إلى مصادقة مقاومة للتصيّد مثل مفاتيح FIDO2 أو مفاتيح المرور بدل المصادقة القائمة على الرموز.
3. مراجعة قواعد تصفية البريد وفحص الروابط للرسائل ذات طابع الدعوات الواردة من مرسلين مجهولين.
4. مراقبة سجلات تسجيل الدخول في Google Workspace بحثًا عن مواقع غير معتادة أو أجهزة جديدة أو جلسات تلي نقرة تصيّد مشتبه بها.
5. تجهيز مسار واضح للموظفين للإبلاغ عن التصيّد المشتبه به وإعادة تعيين بيانات الدخول وإلغاء الجلسات بسرعة.