مجموعة تهديد متقدم تستخدم دعوات فعاليات مزيفة لسرقة بيانات حسابات Google ورموز المصادقة متعددة العوامل



كشف باحثون عن حملة تصيّد موجّه تنفذها مجموعة تهديد متقدم ضد أفراد مرتبطين بمؤسسات بحثية في تايوان، تحوّل الضحايا إلى إطار وسيط يسرق بيانات Google ورموز المصادقة متعددة العوامل.

- الحملة تصيّد موجّه تنفّذه جهة تهديد متقدم مستمر.
- المستهدفون أفراد مرتبطون بمؤسسات بحثية في تايوان.
- يُحوَّل الضحايا إلى إطار تصيّد من نوع الوسيط (AitM).
- صُمم الإطار لسرقة بيانات حسابات Google ورموز المصادقة متعددة العوامل.
- يشير العنوان إلى استخدام دعوات فعاليات مزيفة كطُعم.

ما الذي تم الإبلاغ عنه

كشف باحثون عن حملة تصيّد موجّه تنفذها مجموعة تهديد متقدم ضد أفراد مرتبطين بمؤسسات بحثية في تايوان. يجري تتبع النشاط تحت اسم UAT-11985، ويتمثل الطُعم المذكور في دعوة فعالية مزيفة.

يُحوَّل من ينقر على الطُعم إلى إطار تصيّد من نوع الوسيط (AitM)، صُمم لالتقاط بيانات حسابات Google ورموز المصادقة متعددة العوامل معًا.

أهمية الأمر للجهات في المملكة

الأهداف المذكورة في تايوان، ولا يشير المصدر إلى نشاط داخل المملكة. ومع ذلك تبقى التقنية ذات صلة، فصفحة AitM تتوسط المستخدم وخدمة الدخول الحقيقية، فيمكنها التقاط كلمة المرور والرمز الصحيح لحظيًا. وتوفر الرموز المرسلة برسائل SMS أو المولّدة في تطبيق حماية محدودة ضد هذا الأسلوب.

يُعد الباحثون والأكاديميون وموظفو الدراسات والتنفيذيون الذين تصلهم دعوات مؤتمرات وفعاليات بانتظام أهدافًا طبيعية لهذا النوع من الطُعوم، ويكون الأصل المعرّض هو حسابات البريد والتعاون السحابية التي تعتمد تسجيل الدخول عبر Google.

التوجه المقترح

يُنصح بالتعامل بحذر مع دعوات الفعاليات غير المتوقعة التي تطلب تسجيل الدخول، ومراجعة مدى مقاومة طرق المصادقة المعتمدة لهجمات الترحيل. لا يورد المصدر مؤشرات اختراق، لذا يُعتمد على مراقبة أنشطة تسجيل الدخول لديكم.

ما يجب فعله الآن

1. تذكير الموظفين، خاصة في المكاتب البحثية والتنفيذية، بالتحقق من دعوات الفعاليات عبر قناة مستقلة قبل تسجيل الدخول.
2. دراسة نقل المستخدمين الأعلى خطورة إلى مصادقة مقاومة للتصيّد مثل مفاتيح FIDO2 أو مفاتيح المرور.
3. مراقبة تسجيلات الدخول إلى حسابات Google بحثًا عن مواقع وأجهزة وجلسات غير معتادة ومعالجة التنبيهات سريعًا.
4. إدراج تصيّد AitM في برامج التوعية والمحاكاة مع توضيح أن طلب رمز المصادقة لا يثبت سلامة الموقع.
5. التأكد من وجود إجراء للاستجابة لسرقة بيانات الدخول المشتبه بها يشمل إنهاء الجلسات وإعادة تعيين كلمات المرور.