جهات مرتبطة بشبكة Com تستخدم الاتصالات الصوتية الاحتيالية للاستيلاء على حسابات سحابية وسرقة البيانات والابتزاز



أفادت Unit 42 برصد موجات متكررة من الاتصالات الاحتيالية منذ أغسطس 2026 نفذتها جهات مرتبطة بشبكة Com، وأدت إلى سرقة بيانات ومحاولات ابتزاز، مستهدفة قطاعات مالية وصحية وقانونية.

- تذكر Unit 42 التابعة لشركة Palo Alto Networks أنها تتابع وتستجيب لموجات عديدة من هجمات الاتصال الصوتي الاحتيالي منذ أغسطس 2026.
- تُنسب الحملات إلى جهات تهديد مرتبطة بشبكة Com.
- النتائج المذكورة هي سرقة بيانات ومحاولات ابتزاز مع الاستيلاء على حسابات سحابية.
- القطاعات المستهدفة المذكورة: الخدمات المالية والرعاية الصحية والخدمات القانونية في الولايات المتحدة وبريطانيا وأستراليا، إضافة إلى قطاعات أخرى مثل الإنشاءات.

أعلنت وحدة Unit 42 التابعة لشركة Palo Alto Networks أنها ترصد وتستجيب لموجات عديدة من هجمات التصيد الصوتي (vishing) تنفذها جهات تهديد مرتبطة بشبكة Com منذ أغسطس 2026. وقد أفضت هذه الحملات إلى سرقة بيانات ومحاولات ابتزاز، ويشير عنوان الخبر إلى الاستيلاء على حسابات سحابية.

الجهات المستهدفة

وفق التقرير، تقع الضحايا في قطاعات الخدمات المالية والرعاية الصحية والخدمات القانونية في الولايات المتحدة وبريطانيا وأستراليا، ومن الأهداف الأخرى قطاع الإنشاءات وغيره. ولا يذكر المقتطف المتاح أسماء ضحايا محددة ولا أهدافاً في المملكة.

الأهمية للمؤسسات في المملكة

يعتمد التصيد الصوتي على إقناع شخص عبر الهاتف لا على استغلال ثغرة برمجية، لذلك لا تكفي التحديثات التقنية وحدها لسد هذه الفجوة. وتتعامل المؤسسات المالية والصحية والقانونية في المملكة مع بيانات حساسة مماثلة وتستخدم خدمات سحابية مشابهة، ما يجعل النمط ذا صلة رغم عدم الإبلاغ عن نشاط إقليمي. ولا يوضح المقتطف نصوص المكالمات أو الخطوات التقنية بدقة، فينبغي عدم افتراض تفاصيل تتجاوز ما نشرته Unit 42.

الخطوة العملية التالية

يُنصح باعتبار هذا الخبر دافعاً لمراجعة آلية تحقق مكتب المساعدة والموظفين من هوية المتصلين، وكيفية اعتماد استعادة الحسابات السحابية وتغييرات الصلاحيات. ويُستحسن الاطلاع على منشور Unit 42 الكامل للحصول على المؤشرات والإرشادات التفصيلية.

ما يجب فعله الآن

1. اشتراط التحقق عبر معاودة الاتصال برقم معروف قبل أن يعيد مكتب المساعدة ضبط بيانات الدخول أو المصادقة متعددة العوامل لأي حساب سحابي.
2. توعية الموظفين، وخاصة مكتب المساعدة والفرق المالية والقانونية، بالتصيد الصوتي وبالإبلاغ الفوري عن المكالمات المشبوهة.
3. مراجعة خطوات اعتماد استعادة الحسابات السحابية وتغييرات الصلاحيات المرتفعة، مع إضافة معتمد ثانٍ للطلبات عالية المخاطر.
4. فحص سجلات التدقيق السحابية بحثاً عن عمليات دخول غير معتادة أو تسجيل جديد للمصادقة متعددة العوامل أو تنزيل بيانات بكميات كبيرة.
5. الاطلاع على تقرير Unit 42 الكامل وإضافة مؤشراته إلى المراقبة عند الاقتضاء.