Okta تربط مجموعة تصيّد صوتي مرتبطة بـ ShinyHunters بموقع تسريب جديد باسم INCEPTION



ترى Okta أن مجموعة تصيّد صوتي مرتبطة بـ ShinyHunters ربما أعادت تسمية نفسها إلى INCEPTION. وتخدع المجموعة ضحاياها لإدخال بيانات الدخول في صفحات تصيّد والموافقة على الوصول.

- تتتبع Okta Threat Intelligence المجموعة تحت الاسم O-UNC-053.
- سبق تقييم المجموعة على أنها مرتبطة بمجموعة الابتزاز ShinyHunters.
- قد تكون المجموعة أعادت تسمية نفسها واستمرت في عملياتها باسم INCEPTION.
- أسلوبها الرئيس هو التصيّد الصوتي الذي يدفع الضحايا إلى إدخال بيانات الدخول في صفحات تصيّد والموافقة على الوصول.
- يربط التقرير المجموعة بموقع جديد لتسريب البيانات.

أفادت فرقة Okta Threat Intelligence بأن مجموعة تهديد تتتبعها باسم O-UNC-053 ربما أعادت تسمية نفسها واستمرت في العمل باسم جديد هو INCEPTION. وكانت المجموعة قد قُيّمت سابقًا على أنها مرتبطة بمجموعة الابتزاز ShinyHunters، وتربطها Okta الآن بموقع جديد لتسريب البيانات.

ما هو معروف

تعتمد المجموعة على التصيّد الصوتي (vishing). يتصل المهاجمون بالأهداف هاتفيًا ويقنعونهم بإدخال بيانات الدخول في صفحات تصيّد وبالموافقة على طلبات الوصول. ولا يورد المقتطف المتاح تفاصيل إضافية عن الضحايا أو حجم النشاط أو البيانات المسرّبة، لذا لا ينبغي افتراضها.

أهمية الأمر للجهات المنظَّمة

يستهدف هذا النوع من الهجمات الأشخاص وإجراءات التحقق، لا ثغرات البرمجيات، ولذلك لا تعالجه التحديثات الأمنية وحدها. كما أن إعادة التسمية تعني أن المؤشرات وأسماء المجموعات قد تتغير بينما تبقى الأساليب كما هي، وقد تفوت الاستمرارية على الفرق التي تتابع التهديدات بالاسم فقط.

خطوات عملية

يُنصح بالتعامل مع الهندسة الاجتماعية عبر الهاتف بوصفها خطرًا دائمًا على الهوية، ومراجعة آلية تحقق الموظفين من المتصلين، وطريقة التعامل مع طلبات الموافقة على تسجيل الدخول، والتأكد من أن المستخدمين لا يوافقون على طلب لم يبدؤوه. ومن المفيد متابعة منشور Okta الأصلي للاطلاع على المؤشرات والتحديثات.

ما يجب فعله الآن

1. توعية الموظفين وفرق الدعم الفني بالتصيّد الصوتي، ولا سيما المتصلين الذين يدفعون المستخدم إلى إدخال بيانات الدخول عبر رابط أو الموافقة على طلب.
2. اشتراط التحقق بالاتصال العكسي على رقم معروف قبل أي إعادة تعيين لبيانات الدخول أو تغيير في الصلاحيات يُطلب هاتفيًا.
3. توجيه المستخدمين بعدم الموافقة على أي طلب مصادقة متعددة العوامل أو تسجيل دخول لم يبدؤوه، والإبلاغ عنه فورًا.
4. إضافة O-UNC-053 وINCEPTION إلى متابعة استخبارات التهديدات إلى جانب ShinyHunters، ومراقبة منشور Okta لمعرفة المؤشرات.
5. مراجعة سجلات الهوية والدخول الموحد بحثًا عن موافقات دخول غير معتادة أو تسجيل أجهزة جديدة.