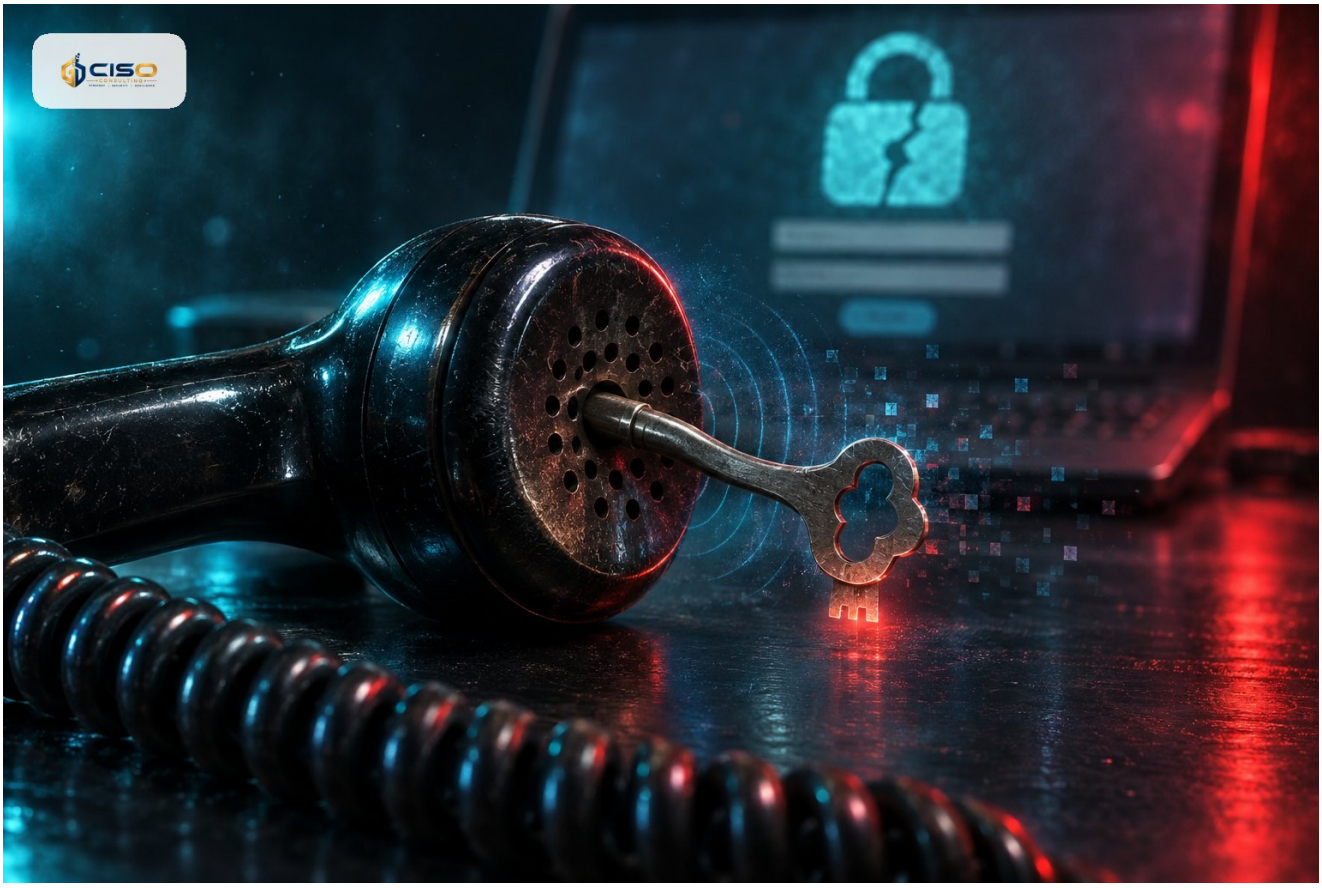
مجموعة الابتزاز «Inception» تشنّ حملة تصيّد صوتي تستهدف بيانات الدخول الموحّد



مجموعة ابتزاز جديدة تُدعى Inception تستخدم الاتصالات الهاتفية ومواقع دخول مزيفة تحاكي Okta لسرقة بيانات الدخول الموحّد. وتربطها Okta بمجموعة مرتبطة بـShinyHunters بينما تنفي المجموعة ذلك.

- ظهرت Inception في 17 نوفمبر وأعلنت سبعة ضحايا مزعومين، ولم تؤكد أي جهة منها حدوث اختراق علنًا.
- تقول ReversingLabs إن النشاط بدأ أواخر أكتوبر، ورصدت 21 نطاقًا لتصيّد الدخول الموحّد و41 نطاقًا يُعتقد أنها بنية الحملة و4 نطاقات مشتبهًا بها.
- تعتمد الحملة على الهندسة الاجتماعية الهاتفية ومواقع بطابع قانوني تحاكي Okta وNetIQ/OpenText Access Manager.
- تقدّر Okta أن المجموعة O-UNC-053 المرتبطة سابقًا بـShinyHunters غيّرت علامتها على

الأرجح، وتنفي Inception أي ارتباط.

- التوصيات: مصادقة مقاومة للتصيّد، وتعزيز التحقق من الهوية في مكتب المساندة، ومراجعة السجلات منذ 21 أكتوبر 2026.

ارتبط اسم مجموعة ابتزاز جديدة تُدعى Inception بحملة واسعة تستهدف بيانات الدخول الموحّد (SSO) لشركات حول العالم. ظهرت المجموعة في 17 نوفمبر وذكرت على موقع الابتزاز الخاص بها سبعة ضحايا مزعومين، ولم تؤكد أي جهة منهم علنًا تعرضها لاختراق.

ما هو معروف

تتابع ReversingLabs نشاط المجموعة وتقول إنه بدأ أواخر أكتوبر. وقد أكدت وجود 21 نطاقًا يُستخدم في تصيّد الدخول الموحّد، و41 نطاقًا يُعتقد أنها تدعم بنية الحملة، و4 نطاقات أخرى مشتبه بها. وتنتحل هذه البنية صفة عشرات العلامات المعروفة، لكن وجود النطاقات لا يثبت أن تلك الشركات استُهدفت أو اختُرقت.

يبدو أن الحملة تعتمد على الهندسة الاجتماعية عبر الهاتف لا على رسائل البريد، وهو أسلوب يشبه ما ارتبط بمجموعة ShinyHunters. وتستخدم Inception مواقع بطابع قانوني تحاكي خدمات المصادقة المؤسسية، وأبرزها Okta إضافة إلى NetIQ/OpenText Access Manager.

الإسناد محل خلاف

ربطت Okta المجموعة بالعنقود O-UNC-053 الذي نسبته سابقًا إلى ShinyHunters. وتقول إنه واصل تسجيل نطاقات تصيّد بعد تعطيل الجهات الأمنية لنشاط ShinyHunters، وأطلق الحملة ذات الطابع القانوني أواخر أكتوبر، ثم بدأ موقع التسريب الخاص بـInception منتصف نوفمبر. ولأن البنية والأساليب بقيت ثابتة، ترجّح Okta أنه غيّر علامته.

ترفض Inception ذلك، وتقول إنها تعمل باستقلال، وإن تشابه الأهداف واستخدام خدمات تسجيل نطاقات وشبكات CDN مشتركة لا يثبت ارتباطًا، وإن أدوات خاصة متداولة بين جهات مستقلة.

لماذا يهم ذلك

تتيح بيانات الدخول الموحّد الوصول إلى أنظمة متعددة دفعة واحدة، والاتصال الهاتفي يستهدف الموظفين ومكاتب المساندة لا مرشحات البريد. وعلى الجهات التي تستخدم Okta أو مزوّد هوية مماثلاً أن تعدّ ذلك دافعًا لمراجعة ضوابط الهوية أيًا كانت نتيجة الإسناد.

ما يجب فعله الآن

1. فرض مصادقة مقاومة للتصيّد مثل مفاتيح FIDO2 أو passkeys للدخول الموحّد، بدءًا بالحسابات ذات الصلاحيات العالية وحسابات مكتب المساندة.
2. تشديد التحقق من الهوية في مكتب المساندة عند إعادة تعيين كلمات المرور وعوامل MFA، مع اشتراط معاودة الاتصال أو تأكيد مستقل.
3. مراجعة سجلات DNS والوكيل ومزوّد الهوية منذ 21 أكتوبر 2026 بحثًا عن نشاط مشبوه ونطاقات دخول

مشابهة.

4. توعية الموظفين وفرق الدعم بمحاولات الانتحال الهاتفي التي تشير إلى تسجيل الدخول أو إشعارات قانونية.
5. تجهيز مسار استجابة لحوادث اختراق الدخول الموحّد المشتبه بها، يشمل إلغاء الجلسات والتحقق من متطلبات الإبلاغ للجهات التنظيمية.