خطوط الدفاع الرئيسية ضد احتيال الهوية الاصطناعية، وسرقة الهوية، والاستيلاء على الحسابات

مشهد التهديدات الآخذ في التطور

انضمام العملاء: سرقة الهوية واحتيال الهوية الاصطناعية

- تستغل عملية سرقة الهوية معلومات التعريف الشخصية (PII) الحقيقية المسروقة والمستندات لانتحال شخصية أفراد حقيقيين.
- تمزج عملية احتيال الهوية الاصطناعية عمدًا بين السمات الحقيقية والملفقة لإنشاء هويات وهمية قابلة للتطوير مع بيانات هوية معقولة ومتسقة.
- غالبًا ما تجتاز الهويات الاصطناعية إجراءات التحقق من الانضمام لأن المحتال يعمد إلى إنشاء الهوية والسجل والمستندات من البداية إلى النهاية.
- إن غياب ضحية واضحة في احتيال الهوية الاصطناعية يؤخر الإبلاغ ويسمح للمحتالين بترسيخ مصداقيتهم تدريجيًا.

مرحلة ما بعد فتح الحساب: الاستيلاء على الحسابات (ATO)

- يخترق المهاجمون بيانات الاعتماد عبر هجمات التصيد الاحتيالي وعمليات استبدال شرائح SIM وتقنيات الرجل في المنتصف.
- تصبح كلمات المرور ذات الاستخدام الواحد (OTP) وعوامل المصادقة الثابتة غير فعالة بشكل متزايد عند استخدامها بمفردها.
- يتيح الذكاء الاصطناعي (AI) التشغيل الآلي وتحقيق التوسع والاستمرارية عبر القنوات.

انتحال الشخصية باستخدام الذكاء الاصطناعي (عبر دورة الحياة المتقاطعة)

- يسمح التزييف العميق للمهاجمين بإنشاء هويات اصطناعية على نطاق واسع وتسليحها للاحتيال.
- يمكن لعمليات استبدال الوجوه وتقليد الأصوات وهجمات الحقن تجاوز فحوصات الحيوية غير الكافية وأنظمة التحقق من الهوية عبر الإنترنت.
- يعمل المهاجمون بشكل متزايد على دمج الوسائط المُنشأة بالذكاء الاصطناعي مع الأجهزة المخترقة ومحاكاة السلوك لتفادي الضوابط.

لماذا يبوء التحقق التقليدي بالفشل

- لم تعد المستندات ومعلومات التعريف الشخصية مرجعًا موثوقًا للحقيقة:
  - تكون الهويات المسروقة مدعومة بمستندات وبيانات شرعية
  - يمكن للمحتالين إنشاء مستندات مقنعة للغاية أو الحصول عليها لدعم الهويات الاصطناعية.
- لا يمكن لإجراءات التحقق في نقطة زمنية محددة اكتشاف الحالات الشاذة التي تحدث عبر الجلسات أو عبر القنوات.
- إن الضوابط المستندة إلى كلمات المرور ذات الاستخدام الواحد (OTP) هي عرضة لعمليات استبدال شرائح SIM والبرمجيات الخبيثة وهجمات الترحيل.
- لم يتم تصميم التحقق التقليدي لاكتشاف هجمات الحقن المدعومة بالذكاء الاصطناعي أو انتحال الهوية في الوقت الفعلي.

مصادقة الشخص باستمرار

- زيادة تكاليف المهاجمين من خلال فرض الاتساق الفوري بين الإشارات المتعددة.
- تقييم المخاطر والتمييز بين احتيال الهوية الاصطناعية، وسرقة الهوية، والاستيلاء على الحسابات باستخدام نماذج مخصصة.
- الانتقال من التحقق الثابت إلى المصادقة التكيفية المستندة إلى المخاطر عبر دورة حياة العميل.

مصفوفة التهديد: اكتشاف حالات احتيال الهوية الناشئة والحد منها

تهديد الاحتيال	الإشارات الرئيسية	كيفية اكتشافها	كيفية الحد منها
احتيال الهوية الاصطناعية	معلومات التعريف الشخصية المتسقة ولكن المصطنعة، والحد الأدنى من سجل الملفات، وأنماط إعادة استخدام الهوية	إجراءات التحقق من المستندات بالذكاء الاصطناعي، والرسم البياني للجهاز/الهوية، وإشارات الاتحاد	تحليل الشبكة، والربط بين المؤسسات، والانضمام على أساس المخاطر
سرقة الهوية	المستندات الشرعية التي تحتوي على تناقضات في السلوكية أو الجهاز	البيانات الحيوية وإجراءات التحقق من الحيوية، ومعلومات الجهاز، وعدم تطابق السلوك	المصادقة المعززة، وإعادة التحقق باستخدام البيانات الحيوية، والمراقبة المستمرة
الاستيلاء على الحسابات	تغيير السلوك، والجهاز/بروتوكول الإنترنت الجديد، والحالات الشاذة في الجلسة	البيانات الحيوية في السلوك، وتقييم مخاطر الجلسة	الضوابط التصعيدية التكيفية، والتدخل في الوقت الفعلي، والفحوصات على مستوى المعاملة

مبادئ التصميم وأفضل الممارسات

- **التحول المبكر نحو إدارة المخاطر:** اكتشف محاولات التزييف العميق والحقن أثناء الانضمام – وليس بعد تكبُّد الخسائر.
- **التكيّف افتراضيًا:** قم بتصعيد الضوابط ديناميكيًا استنادًا إلى السلوك والجهاز والسياق.
- **الضمان المستمر:** أعِد مصادقة المستخدمين باستمرار استنادًا إلى البيانات الحيوية السلوكية أثناء الأنشطة عالية المخاطر.
- **القرارات القابلة للتفسير:** ادعم التحقيقات وساعد في معالجة التدقيق التنظيمي.
- **المعلومات الاستخباراتية المتبادلة:** استخدم تغذيات الاتحاد ومعلومات التهديد الاستخباراتية لكشف أساليب الهجمات الناشئة وتقنياتها وإجراءاتها (TTP).
- **اختبار المرونة:** أجرِ بانتظام عمليات تحكم عبر الفريق الأحمر ضد الهجمات المدعومة بالذكاء الاصطناعي.

الدعوة إلى العمل

- افترض أنه يمكن تزوير الهوية بشكل مقنع، وضع ضوابط للحؤول دون حدوث ذلك.
- تجاوز الاعتماد على المستندات وكلمات المرور ذات الاستخدام الواحد كإشارات أساسية للثقة.
- اعتمد نهج اكتشاف متعدد الطبقات عبر الأدلة الرقمية والسلوك والجهاز وإشارات الشبكة
- اختبر الدفاعات باستمرار ضد أدوات التزييف العميق المتطورة.

مواد إضافية للقراءة

- **تنبيه عام صادر عن مركز شكاوى حرائم الإنترنت (IC3) التابع لمكتب التحقيقات الفيدرالي (FBI): احتيال الهوية الاصطناعية؛**
- **نشرة استخباراتية صادرة عن وزارة الأمن الداخلي (DHS) / تحقيقات الأمن الداخلي (HSI) حول شبكات الاحتيال؛**
- **الكشف عن الحرائم الإلكترونية: تعزيز التحقق من الهوية الرقمية ضد التزييف العميق**