

استغلال أدوات اختبار الاختراق المعتمدة على الذكاء الاصطناعي في هجمات على بنوك كورية جنوبية



استخدم جهة تهديد أدوات ARTEX AI وعملاء Claude لاختراق عدة بنوك كورية جنوبية وكشف بيانات العملاء وتعطيل الأنظمة، مما دفع المطور لإغلاق المصدر.

- مهاجم ناطق بالصينية استهدف بنك Shinhan وبنك KB Kookmin وبنك Hana باستخدام مجموعة اختبار الاختراق ARTEX AI وعملاء Claude
- الاختراقات كشفت بيانات العملاء الشخصية ومعلومات البطاقات الائتمانية وتسببت في تعطيل الأنظمة في بعض المؤسسات
- تتبع CrowStrike الهجوم عبر دلائل مفتوحة تحتوي على سجلات جلسات Claude وملفات تكوين ARTEX
- مطور ARTEX أغلق مصدر المشروع بعد تأكيد استخدامه في هجمات حقيقية رغم بقاء نسخ مشتقة متاحة

- المهاجم لم يكن لديه خطة لتحقيق الربح واستخدم أدوات الذكاء الاصطناعي لتحديد قنوات بيع البيانات على تيليجرام

ملف الهجوم والأثر

أطلقت جهة تهديد هجمات منسقة ضد عدة مؤسسات مالية كورية جنوبية في وقت سابق من هذا الشهر، مستغلة أدوات اختبار الاختراق المدعومة بالذكاء الاصطناعي لاختراق الدفاعات. استهدفت الحملة بنك Shinhan وبنك KB Kookmin وبنك Hana، مما أدى إلى كشف البيانات الشخصية للعملاء ومعلومات البطاقات الائتمانية. عانت بعض المؤسسات من انقطاعات في الأنظمة خلال الحادثة. عقدت الحكومة الكورية الجنوبية اجتماعاً طارئاً وأصدرت دعوات لاتخاذ تدابير أمنية فورية عبر البنية التحتية الحيوية لتقنية المعلومات.

الإسناد الفني والأدوات المستخدمة

أكدت CrowdStrike أن المهاجم استخدم ARTEX AI، وهي مجموعة اختبار اختراق ذاتية التشغيل كانت مفتوحة المصدر وظهرت في الصين، إلى جانب عملاء Claude. اكتشف الباحثون دلائل مفتوحة تحتوي على سجلات جلسات Claude Code وملفات تكوين ARTEX وملفات ذاكرة Claude التي كشفت عن البنية التحتية للهجوم. اعتمدت نسخة ARTEX على DeepSeek v4.1-flash كنموذج لغوي كبير أساسي، مدعوماً بـ GLM-5.3 و Grok 4.6 لجلسات Claude Code إضافية. تشير الأدلة إلى أن المهاجم وصل إلى DeepSeek عبر وكيل أو موزع لواجهة برمجة تطبيقات النماذج اللغوية الكبيرة.

كشف التحقيق أن المهاجم استخدم نفس أدوات الذكاء الاصطناعي لإنشاء سيرة ذاتية، مما كشف عن غير قصد تفاصيل الهوية ومعلومات الاتصال وحساب تيليجرام. قيّمت CrowdStrike أن جهة التهديد قد تكون مواطناً صينياً يبلغ من العمر 26 عاماً درس في جامعة جنوب الصين للتكنولوجيا ويقيم في ماومينغ بمقاطعة قوانغدونغ. لكن التناقضات في التفاصيل الشخصية—بما في ذلك تاريخ ميلاد أولي مدرج في 2007—تعني أن الهوية لا يمكن تأكيدها بشكل موثوق.

توفر الأداة ونية تحقيق الربح

تشير السجلات إلى أن المهاجم لم يكن لديه خطة محددة مسبقاً لتحقيق الربح من بيانات البنوك المسروقة واستشار Claude لتحديد مجموعات بيع البيانات على تيليجرام المركزة على كوريا. بعد تأكيد استخدام ARTEX كسلاح في هجمات حقيقية، أوقف المطور التحديثات العامة وجعل المشروع مغلق المصدر. ومع ذلك، تظل النسخ المشتقة باللغتين الإنجليزية والكورية من قاعدة الشفرة الحالية متاحة، مما يحافظ على إمكانية وصول جهات التهديد الأخرى إلى الأداة.

ما يجب فعله الآن

1. مراجعة وتعزيز سياسات إدارة بيانات الاعتماد لمنع الوصول غير المصرح به باستخدام بيانات اعتماد صالحة، والتي تظل ناقل هجوم رئيسي
2. تقييم التعرض لأدوات اختبار الاختراق المدعومة بالذكاء الاصطناعي من خلال مراقبة نشاط المسح أو التعداد الآلي غير المعتاد عبر الأنظمة الحيوية
3. تنفيذ مراقبة معززة لأنماط الوصول إلى واجهات برمجة التطبيقات، خاصة الاتصالات بوكلاء أو موزعي

النماذج اللغوية الكبيرة التي قد تشير إلى استطلاع بمساعدة الذكاء الاصطناعي

4. التحقق من بقاء الضوابط الأمنية فعالة بعد الوصول الأولي، حيث تنخفض معدلات المنع بشكل كبير بمجرد حصول المهاجمين على بيانات اعتماد صالحة

5. التنسيق مع مزودي معلومات التهديدات لتحديد مؤشرات الاختراق المرتبطة بمشتقات ARTEX وأطر الهجوم المماثلة بمساعدة الذكاء الاصطناعي

6. إجراء تمارين محاكاة لهجمات معززة بالذكاء الاصطناعي ضد البنية التحتية المصرفية لاختبار قدرات الكشف والاستجابة