

حصان طروادة Hirudo لنظام أندرويد يستبدل تطبيقات البنوك بنسخ معدلة لتجاوز الحماية



حصان طروادة مصرفي جديد لنظام أندرويد يستبدل تطبيقات البنوك الشرعية بنسخ معدلة تتجاوز فحوصات الأمان المدمجة، ما يمثل تصعيداً في الاحتيال المالي عبر الأجهزة المحمولة يستهدف بنوكاً إندونيسية.

- حصان طروادة Hirudo يستبدل تطبيقات البنوك الشرعية بنسخ معدلة تتجاوز فحوصات الأمان الداخلية
- ثمانية تطبيقات مصرفية إندونيسية استُهدفت بنسخ بديلة
- التقنية تمثل تصعيداً جديداً في أساليب الاحتيال المالي عبر الأجهزة المحمولة
- شركة ThreatFabric الهولندية للأمن المحمول حددت التهديد
- الهجوم يعمل بالتحايل على ضوابط الأمان من داخل التطبيق نفسه

نظرة عامة على التهديد

حدد باحثون في الأمن السيبراني حضان طروادة مصرفي جديد لنظام أندرويد يُدعى **Hirudo** يستخدم تقنية متقدمة لاختراق أمن الخدمات المصرفية عبر الأجهزة المحمولة. على عكس البرمجيات الخبيثة المصرفية التقليدية التي تعرض شاشات تسجيل دخول مزيفة أو تعترض بيانات الاعتماد، يستبدل Hirudo تطبيقات البنوك الشرعية بنسخ معدلة مصممة خصيصاً لتجاوز فحوصات الأمان المدمجة في التطبيقات نفسها.

كشفت شركة ThreatFabric الهولندية للأمن المحمول عن التهديد بعد تحديد نسخ بديلة تستهدف ثمانية تطبيقات مصرفية إندونيسية. يمثل هذا النهج تصعيداً كبيراً في أساليب الاحتيال المالي عبر الأجهزة المحمولة، حيث تظهر التطبيقات الخبيثة وتعمل كبرمجيات مصرفية حقيقية بينما تقوض ضوابط الأمان من الداخل.

الآثار التقنية

تتحايل تقنية Hirudo على تدابير الأمن المحمول التقليدية بالعمل داخل ما يعتبره المستخدمون والعديد من أدوات الأمان تطبيق مصرفي شرعي. من خلال تعديل كود التطبيق الأصلي، يمكن للجهات المهددة تعطيل تثبيت الشهادات وفحوصات السلامة وآليات الحماية الأخرى التي تنفذها البنوك لتأمين قنواتها المحمولة. يتيح ذلك للمهاجمين اعتراض الاتصالات أو التلاعب بالمعاملات أو استخراج بيانات الاعتماد دون تفعيل تنبيهات الأمان التي تحمي العملاء عادةً.

اعتبارات إقليمية

بينما يركز الاستهداف الحالي على مؤسسات إندونيسية، فإن التقنية قابلة للنقل ويمكن تكييفها لتطبيقات مصرفية في أي سوق. ينبغي للمؤسسات المالية السعودية ملاحظة أن ناقل الهجوم هذا يتجاوز العديد من ضوابط الأمن المحمول التقليدية ويتطلب نهجاً شاملاً لأمن التطبيقات المحمولة وثقيف المستخدمين ورصد الاحتيال للكشف عن اختراقات مماثلة ومنعها.

ما يجب فعله الآن

1. مراجعة بنية أمن التطبيقات المحمولة للتأكد من تنفيذ فحوصات السلامة وتثبيت الشهادات وضوابط مكافحة التلاعب بشكل صحيح وعدم إمكانية تجاوزها بسهولة
2. تطبيق تقنيات الحماية الذاتية للتطبيقات في وقت التشغيل (RASP) أو تقنيات مماثلة تكتشف عندما تعمل التطبيقات المصرفية في بيئات معدلة أو مخترقة
3. تعزيز أنظمة رصد الاحتيال لاكتشاف أنماط المعاملات الشاذة التي قد تشير إلى استخدام تطبيقات محمولة مخترقة أو معدلة
4. تثقيف العملاء حول تنزيل التطبيقات المصرفية فقط من متاجر التطبيقات الرسمية والتحقق من صحة التطبيق قبل التثبيت
5. وضع إجراءات لرصد ظهور نسخ غير مصرح بها أو معدلة من تطبيقات المؤسسة المحمولة في متاجر التطبيقات أو المستودعات الخارجية
6. التنسيق مع موردي الأمن المحمول لضمان قدرة إمكانات الكشف في نقاط النهاية على تحديد النسخ المعدلة أو المعاد تغليفها من التطبيقات المصرفية الشرعية