

برمجية هيرودو الخبيثة تستبدل تطبيقات البنوك لتجاوز الضوابط الأمنية



برمجية خبيثة جديدة على أندرويد تستبدل تطبيقات البنوك الأصلية بنسخ معدلة تعطل فحوصات التوقيع والوصول وتحقق السلامة لسرقة بيانات الاعتماد والتحكم عن بُعد.

- برمجية هيرودو تلغي تثبيت تطبيقات البنوك الأصلية وتستبدلها بنسخ معدلة تعطل الفحوصات الأمنية باستخدام أطر اعتراض
- تُوزع البرمجية عبر تطبيقات تبدو مشروعة للتسوق أو المحتوى الإيجابي أو الدراما القصيرة تعمل كمحطات
- التطبيقات المعدلة تتجاوز التحقق من التوقيع وتخفي خدمات الوصول وتزيل حماية لقطة الشاشة وتتلاعب بفحوصات Play Integrity
- البرمجية تسرق كلمات مرور البنوك ورموز الدفع ورسائل SMS وتوفر بث الشاشة والوصول للكاميرا للمشغلين

- تستهدف تطبيقات بنوك في إندونيسيا والصين والهند والمكسيك والمغرب وتايلاند مع آلاف بيانات الاعتماد في خادم خلفي غير محمي

نظرة عامة على التهديد

حدد باحثو أمن الأجهزة المحمولة سلالة برمجيات خبيثة متطورة على أندرويد تُدعى **هيرودو** تستخدم أسلوباً غير معتاد للتهرب من ضوابط أمن تطبيقات البنوك. بدلاً من محاولة التراكب أو اعتراض التطبيقات المصرفية المشروعة، تستبدل البرمجية الخبيثة التطبيقات بالكامل بنسخ معدلة تعطل الآليات الأمنية المدمجة.

تُوزع البرمجية عبر تطبيقات تبدو مشروعة للتسويق أو المحتوى الإباحي أو الدراما القصيرة تعمل كما هو معلن لكنها تعمل كمحفلات. بمجرد التثبيت، تعرض هذه التطبيقات إشعارات تحديث مزيفة تطالب المستخدمين بمنح أذونات الوصول. ثم تلغي هيرودو تثبيت التطبيق المصرفي الأصلي، وتنزل نسخة معدلة، وتستخدم امتيازات الوصول لتثبيت البديل دون وعي المستخدم.

أساليب التهرب التقنية

تحتفظ التطبيقات المصرفية المعدلة بكل الكود الأصلي تقريباً لكنها تدمج محرك اعتراض مبني على أطر مفتوحة المصدر. عند التشغيل، يستبدل التطبيق المعدل شهادة التوقيع الأصلية عند الاستعلام، ويخفي خدمات الوصول الممكنة من الكشف، ويزيل حماية لقطة الشاشة لتمكين المشاهدة عن بُعد، ويتلاعب بشهادات تصديق المفاتيح بينما يُرسل طلبات Play Integrity عبر بنية تحتية يسيطر عليها المشغلون.

يشير الباحثون إلى أن محرك الاعتراض يعمل داخل عملية التطبيق المصرفي نفسه، مما يحوّل دفاعات التطبيق ضد ذاته فعلياً. لكن توجد قيود معينة: تم تسريب صندوق مفاتيح التصديق المرفق علناً وأدرجت جوجل اثنتين من شهاداته كمخرقة، مما يجعل فحوصات الإبطال من جانب الخادم قادرة على كشف هذه التزويرات.

القدرات التشغيلية والاستهداف

بمجرد التفعيل، يمكن لهيرودو سرقة كلمات مرور البنوك ورموز الدفع وبيانات اعتماد فتح الجهاز ورسائل SMS. توفر البرمجية للمشغلين قدرات بث الشاشة والوصول لكاميرات الجهاز. تجمع صفحات الدفع المزيفة رموز الدفع وتعرض رسائل نجاح ملفقة لخداع الضحايا أثناء سرقة البيانات.

لاحظ الباحثون استهداف البرمجية لتطبيقات مصرفية في إندونيسيا والصين والهند والمكسيك والمغرب وتايلاند. كشفت لوحة خلفية غير محمية عن آلاف إداخلات بيانات اعتماد التطبيقات مع بيانات الجهاز وشاشة القفل والملف المالي، رغم أن إجمالي عدد الضحايا لا يزال مجهولاً. يصف باحثو الأمن هذا بأنه تصعيد متعمد في برمجيات أندرويد المصرفية الخبيثة، ينقل التركيز من فحوصات سلامة الجهاز إلى الآليات الأمنية المضمنة في التطبيقات المصرفية نفسها.

ما يجب فعله الآن

1. تطبيق التحقق من سلامة التطبيق وفحوصات التصديق من جانب الخادم لجميع معاملات الخدمات المصرفية عبر الهاتف المحمول
2. ربط التحقق من السلامة بجلسات المستخدم والإجراءات المحمية بدلاً من الاعتماد فقط على فحوصات

جانب العميل

3. نشر تحليلات سلوكية وضوابط مخاطر المعاملات تعمل بشكل مستقل عن أمن التطبيق من جانب العميل
4. مراجعة وتعزيز سياسات أمن تطبيقات الهاتف المحمول لكشف وحظر تثبيت التطبيقات من مصادر غير رسمية
5. توعية العملاء بمخاطر تحميل ملفات APK الجانبي ومنح أذونات الوصول لتطبيقات غير نظامية
6. مراقبة الأنماط الشاذة مثل أحداث إعادة تثبيت التطبيق متبوعة بنشاط معاملات غير عادي