Bazuka: إطار جديد لبرمجيات أندرويد الخبيثة يستخدم شاشات مزيفة لإخفاء سرقة بيانات الدخول



كشفت ThreatFabric عن Bazuka، إطار جديد لبرمجيات أندرويد الخبيثة يدمج نماذج لغوية كبيرة لإدارة الضحايا على نطاق واسع، واكتُشف أواخر أكتوبر 2026 أثناء تحقيق في تروجان مصرفي يعتمد تمرير NFC.

- Bazuka إطار جديد غير معروف سابقاً لبرمجيات أندرويد الخبيثة، وليس تروجان بغرض واحد.
- يوفّر دمج نماذج لغوية كبيرة (LLM) لإدارة الضحايا والتحكم بهم على نطاق واسع.
- يشير العنوان إلى استخدام شاشات مزيفة لإخفاء سرقة بيانات الدخول والتحكم بالجهاز.
- اكتشفته شركة ThreatFabric الهولندية لأمن الجوال في أواخر أكتوبر 2026.
- جاء الاكتشاف أثناء التحقيق في تروجان مصرفي يعتمد تمرير NFC.

وصف باحثو ThreatFabric، وهي شركة هولندية متخصصة في أمن الجوال، إطاراً جديداً غير معروف سابقاً لبرمجيات أندرويد الخبيثة باسم Bazuka. وتفيد الشركة بأنها رصدته في أواخر أكتوبر 2026 أثناء تحقيقها في تروجان مصرفي يعتمد تمرير NFC.

ما الذي نُشر

يوصف Bazuka بأنه إطار برمجي خبيث متكامل وليس أداة واحدة. وأبرز ما يميّزه دمج النماذج اللغوية الكبيرة (LLM)، بما يساعد المشغّلين على إدارة الضحايا والتحكم بهم على نطاق واسع. ووفق العنوان، يعتمد على شاشات مزيفة تُعرض فوق التطبيقات لإخفاء سرقة بيانات الدخول والتحكم بالجهاز.

المقتطف المتاح من المصدر موجز، لذلك لا تتوفر هنا تفاصيل عن طريقة الانتشار أو الجهات والمناطق المستهدفة أو مؤشرات الاختراق التقنية.

لماذا يهم ذلك

تعتمد المؤسسات المالية وعملاؤها بدرجة كبيرة على القنوات الجوالة. وإطار يخفي نشاطه خلف شاشات مزيفة قد يصعّب على المستخدم ملاحظة سرقة بيانات الدخول، كما أن ارتباطه بتحقيق في تروجان مصرفي يشير إلى السياق المصرفي.

المطلوب مراجعة هادئة لا قلق مبالغاً فيه. ينبغي للفرق الاطلاع على تقرير ThreatFabric الكامل عند توفره، والتحقق من أن ضوابط مكافحة الاحتيال عبر الجوال وحماية الأجهزة تغطي إساءة الاستخدام القائمة على الشاشات المزيفة.

ما يجب فعله الآن

1. الحصول على تقرير ThreatFabric الكامل واستخراج مؤشرات الاختراق لإدخالها في أدوات رصد التهديدات.
2. مراجعة قدرة تطبيق الجوال المصرفي وأنظمة مكافحة الاحتيال على كشف هجمات الشاشات المزيفة وسلوك التحكم غير الطبيعي بالجهاز.
3. تذكير العملاء والموظفين بالتثبيت من المتاجر الرسمية فقط والحذر من طلبات الأذونات غير المتوقعة، خاصة إذن إمكانية الوصول.
4. التأكد من تسجيل أجهزة أندرويد المؤسسية في نظام إدارة الأجهزة المحمولة مع قيود على تثبيت التطبيقات.
5. التأكد من أن إجراءات الاستجابة للحوادث ومكافحة الاحتيال تغطي سيناريوهات البرمجيات الخبيثة على الجوال وسرقة بيانات الدخول.