الكشف عن إطار البرمجيات الخبيثة Bazuka لأجهزة أندرويد: شاشات تراكب مزيفة وتكامل مع نماذج اللغة



كشفت ThreatFabric عن Bazuka، إطار برمجيات خبيثة جديد لأجهزة أندرويد يتكامل مع نماذج اللغة الكبيرة لإدارة الضحايا على نطاق واسع، واكتُشف أواخر أكتوبر 2026 أثناء تحقيق في حصان طروادة مصرفي.

- Bazuka إطار برمجيات خبيثة جديد لأجهزة أندرويد لم يكن معروفاً من قبل.
- يوفر تكاملًا مع نماذج اللغة الكبيرة (LLM) لإدارة الضحايا والتحكم بهم على نطاق واسع.
- اكتشفته شركة ThreatFabric الهولندية المتخصصة في أمن الهواتف في أواخر أكتوبر 2026.
- جاء الاكتشاف أثناء التحقيق في حصان طروادة مصرفي يعتمد على ترحيل NFC.
- يربط عنوان التقرير بينه وبين شاشات تراكب مزيفة تُخفي سرقة بيانات الدخول والتحكم بالجهاز.

وصف باحثو ThreatFabric، وهي شركة هولندية متخصصة في أمن الهواتف المحمولة، إطار برمجيات خبيثة جديداً لأجهزة أندرويد يحمل اسم **Bazuka**. ويفيد التقرير بأنه يتضمن تكاملًا مع نماذج اللغة الكبيرة (LLM) يساعد المشغّلين على إدارة الضحايا والتحكم بهم على نطاق واسع.

ما الذي ورد في التقرير

تقول ThreatFabric إنها اكتشفت التهديد في أواخر أكتوبر 2026 أثناء التحقيق في حصان طروادة مصرفي يعتمد على ترحيل NFC. وتصف الشركة Bazuka بأنه إطار متكامل للبرمجيات الخبيثة وليس أداة بغرض واحد. ويشير عنوان التقرير إلى استخدامه شاشات تراكب مزيفة لإخفاء سرقة بيانات الدخول والتحكم بالجهاز عن المستخدم.

لا يتضمن المقتطف المتاح لنا طرق الانتشار أو الدول والجهات المستهدفة أو مؤشرات الاختراق التقنية، ولذلك لا نفترض وجود أثر على المنظمات في المملكة.

أهمية الخبر

تزيد البرمجيات التي تجمع بين الخداع بالتراكب والإدارة المركزية لأعداد كبيرة من الأجهزة المصابة من المخاطر على تطبيقات الخدمات المصرفية عبر الجوال وتطبيقات العاملين. وعلى الجهات التي تخدم عملاءها عبر تطبيقات أندرويد، أو تتيح لموظفيها الوصول إلى الأنظمة عبر الأجهزة المحمولة، أن تعتبر ذلك فرصة لمراجعة دفاعاتها على الجوال.

الاستجابة العملية مراجعة هادئة لا ذعر: تحقق مما تستطيع ضوابط مكافحة الاحتيال وحماية الأجهزة لديك كشفه، وتأكد من قدرة فرقك على التصرف سريعاً عند نشر مؤشرات الاختراق، وذكّر العملاء والموظفين بعادات التثبيت الآمن.

ما يجب فعله الآن

1. راجع مصادر استخبارات التهديدات لديك بحثاً عن مؤشرات Bazuka التي تنشرها ThreatFabric، وأضفها إلى أدوات الكشف فور توفرها.
2. تحقق من قدرة تطبيقات الخدمات المصرفية عبر الجوال على كشف شاشات التراكب وسلوكيات الصلاحيات أو التحكم بالجهاز الخطرة.
3. تأكد من أن إدارة الأجهزة المحمولة تفرض تثبيت التطبيقات من المصادر المعتمدة فقط على أجهزة أندرويد المؤسسية.
4. اختبر قواعد مراقبة الاحتيال للجلسات المشبوهة التي تعقب إدخال بيانات الدخول من أجهزة قد تكون مخترقة.
5. أرسل إلى العملاء والموظفين تذكيراً موجزاً بعدم تثبيت التطبيقات من خارج المتاجر الرسمية ومنح صلاحيات غير متوقعة للجهاز.