# Odinštalujete ho, no vráti sa späť. Nový Android malvér kradne PIN , heslá aj bankové údaje

**18.9.2026 - Lenka Ivančíková | Zajtra studio spol.**

**Bezpečnostná firma Zimperium odhalila nový Android malvér RatHat, za ktorým má podľa všetkého stáť skupina pôsobiaca z Číny. Kradne bankové heslá, jednorazové kódy aj PIN a na rozdiel od bežných škodlivých aplikácií sa po odinštalovaní dokáže sám vrátiť.**

Výskumný tím zLabs správu zverejnil 16. septembra. RatHat sa šíri hlavne cez cielené podvodné SMS, cez reklamy vedúce na falošné stránky na sťahovanie a cez diskusné fóra. Obeť si do telefónu sama stiahne **inštalačný súbor APK**, ktorý vyzerá ako legitímna aplikácia. V jednej verzii sa vydával za známu streamovaciu službu a útočník mu neskôr môže zmeniť ikonu, napríklad na Chrome.

Malvér v mobile | Zdroj: ChatGPT

## Sám si zapne ladenie a získa prístup k systému

Kľúčom je povolenie pre **službu dostupnosti**. Keď ho malvér dostane, sám sedemkrát ťukne na číslo zostavy, odomkne možnosti pre vývojárov, zapne **bezdrôtové ladenie** a z obrazovky si prečíta šesťmiestny párovací kód. Spáruje sa potom s ladiacim rozhraním ADB v tom istom telefóne a bez akéhokoľvek počítača získa **oprávnenia na úrovni shellu**. S nimi spustí dve skryté služby, ktoré bežia mimo samotnej aplikácie.

Práve to robí odstránenie také ťažké. Pri pokuse o odinštalovanie RatHat zobrazí **falošné chybové hlásenie** v štýle Google Play. A keď sa aplikáciu predsa podarí zmazať, skrytá služba beží ďalej, malvér nainštaluje znova a vráti mu všetky povolenia bez toho, aby sa používateľa na čokoľvek pýtal. Aplikácia si navyše môže vypýtať práva správcu zariadenia, s ktorými vie pri pokuse o odstránenie **telefón vymazať**.

**Nemali by ste prehliadnuť:**

- **Nový malvér zneužije vašu platobnú kartu v reálnom čase. Stačí jeden telefonát**
- **Kybernetickí útočníci zneužívajú meno ZSE. Falošné faktúry skrývajú malvér kradnúci údaje**
- **Google rozširuje Scam Detection aj na Xiaomi. Upozorní na podvody**

## PIN prezradí aj dotyk prsta

Nad bankovými a kryptomenovými aplikáciami RatHat zobrazuje **falošné prihlasovacie obrazovky**, zachytáva SMS aj notifikácie s jednorazovými kódmi a nahráva obrazovku. Najzákernejšie je čítanie surových dotykov na displeji. Z polohy prsta a z rozloženia klávesníc hlavných výrobcov malvér poskladá PIN, heslo aj gesto na odomknutie, takže neuspejú ani vlastné klávesnice bankových aplikácií. Podobne ako malvér s umelou inteligenciou, ktorý pred časom opísal ESET, aj RatHat si pomáha **generatívnou AI**. Tá mu podľa štruktúry obrazovky radí, kam ťuknúť.

Zimperium hovorí o globálnom zameraní na finančné aplikácie, menovite však uvádza len čínske platobné služby **WeChat a Alipay**. Slovenské banky ani Slovensko medzi cieľmi nespomína.

Najlepšou obranou tak zostáva opatrnosť pri odkazoch v SMS a vyhýbanie sa inštalácii aplikácií z neznámych stránok, ktorú Google navyše sťažuje. Inštalácia mimo Obchodu Play po novom trvá dlhšie. Kto nepozná aplikáciu, ktorá žiada o službu dostupnosti, nemal by jej ju povoliť.

## Čo nové u ostatných výrobcov

Meta zablokovala trik s okuliarmi, ktorý umožňoval nahrávať ľudí bez rozsvietenej kontrolky, čo je dobrá správa pre súkromie okolia. Sony rozširuje ponuku slúchadiel o lacnejšiu verziu obľúbeného modelu. A Lenovo predstavilo dva tablety Yoga, ktoré mieria na multimédiá aj prácu na cestách.

https://www.mojandroid.sk/novy-android-malver-rathat-kradne-pin-aj-bankove-hesla-po-odinstalovani-sa-sam-v