Nový malvér zneužije vašu platobnú kartu v reálnom čase. Stačí jeden telefonát

14.8.2026 - Filip Spevár | Zajtra studio spol

Za novou vlnou podvodov s bezkontaktnými kartami stojí kombinácia troch vecí, ktoré samy o sebe nové nie sú: telefonátu tváriaceho sa ako banka a dvoch aplikácií v telefóne obete. Podľa portálu Malwarebytes Labs opísali analytici spoločnosti Group-IB novú rodinu NFC relay malvéru WindRelay, ktorá údaje z karty preposiela útočníkovi v reálnom čase.

Útok sa začína hovorom. V opísanom prípade sa volajúci vydával za pracovníka banky a rozhovor trval trinásť minút. Za ten čas presvedčil obeť, aby si nainštalovala aplikáciu označenú menom jej vlastnej banky. V skutočnosti išlo o **trójskeho koňa SpyNote**, ktorý útočníkovi odovzdal telefón a potichu doinštaloval druhú aplikáciu, o ktorej už obeť nevedela.

Prečo musí podvod bežať v reálnom čase

Bezkontaktná platba nie je statický kód, ktorý sa dá skopírovať a použiť o týždeň. Karta pri každom priložení vygeneruje **jednorazový kryptogram** platný len pre danú transakciu, takže druhý raz sa použiť nedá. Práve preto musí celý podvod bežať naživo: údaje putujú k útočníkovi v tom istom momente, ako obeť drží kartu pri svojom telefóne.

Vyzeralo to nasledovne. Útočníci na diaľku otvorili skutočnú bankovú aplikáciu obete a dojednali **pôžičku v jej mene**. Počas hovoru ju zároveň požiadali, aby fyzickú kartu priložila k telefónu a zadala k nej PIN. Druhá aplikácia v tej chvíli preposlala údaje na zariadenie, ktoré útočník držal pri platobnom termináli alebo pri bankomate s bezkontaktným výberom hotovosti.

Telefonát tak nie je len návnadou, ale aj riadiacim kanálom celého útoku. Útočník ním prekonáva váhanie obete, reaguje na jej zmätok a načasuje presné momenty inštalácie, priloženia karty aj zadania PIN. Bez človeka na druhej strane linky by celá technická časť nefungovala, pretože každý krok musí prísť v správnom poradí a v správnej chvíli.

Rodina, ktorú na Slovensku poznáme

Ide o rozrastajúcu sa kategóriu podvodov, ktorej sa hovorí **ghost tapping**. Patria do nej aj skôr opísané rodiny NGate a SuperCard X a práve pod menom NGate deteguje obe nové aplikácie aj Malwarebytes. Rovnaký typ útoku pritom Slovensku cudzí nie je, o vlne NFC podvodov sme písali na jar. Novinkou nie je samotné preposielanie údajov, ale jeho spojenie s malvérom, ktorý útočníkovi otvorí telefón dokorán.

Pôvodná analýza Group-IB je v tomto konkrétna. Tím pre ochranu pred podvodmi prepojil nájdené aplikácie s kampaňami, ktoré cielili na obete **v Česku, na Slovensku a v Slovinsku**. Na VirusTotal našiel 23 vzoriek nahratých od novembra 2025 do júla 2026 a tie napodobňujú inštitúcie z cielených krajín, vrátane textu v jazyku danej krajiny. Niektoré majú dokonca prispôsobené prvky rozhrania.

Nie je to pritom prvý raz. Už vlani ESET odhalil aplikácie, ktoré sa vydávali priamo za **Národnú banku Slovenska** alebo za Českú národnú banku, a fungovali na tom istom princípe: telefonát, priloženie karty k mobilu, zadanie PIN. Podľa Lukáša Štefanka, výskumníka ESET, ktorý ich odhalil, je žiadosť o inštaláciu aplikácie alebo o PIN počas hovoru vždy varovný signál. Slovenská firma vtedy

zaznamenala viac než tridsaťpäťnásobný nárast podvodov s NFC, hoci absolútne počty zostávali nízke.

Nemali by ste prehliadnuť:

- **Nové triky podvodníkov: Zneužívajú NFC čipy, deepfake videá aj umelú inteligenciu**
- **Kybernetickí útočníci zneužívajú meno ZSE. Falošné faktúry skrývajú malvér kradnúci údaje**
- **Smartfónový podvod storočia? Ako prezident Trump svoje ovečky zrejme pripravil o 60 miliónov**

Obrana je jednoduchá a je celá v rukách používateľa, pretože aplikáciu si obeť inštaluje sama. **Banka o inštaláciu aplikácie z odkazu nežiada**, a to ani cez správu, ani cez prehliadač, ani počas hovoru. Ak niekto volá a tvrdí, že je z banky, najistejšie je zložiť a zavolať späť na oficiálne číslo. Aplikácie sťahujte len cez Obchod Play a neočakávanú žiadosť o povolenie na ovládanie zariadenia berte ako varovanie.

Koľko ľudí už o peniaze prišlo, analýza neuvádza, takže toto číslo sa oplatí sledovať. Isté je, že chyba nie je v bezkontaktných platbách, tie fungujú tak, ako majú. Zlyháva človek, ktorého niekto trinásť minút presviedčal, a to je zároveň jediné miesto, kde sa dá útok zastaviť. Rovnaký princíp mimochodom využíva aj sofistikovaný phishing mierený na Slovákov.

Nielen táto značka má čo ukázať

Mimo bezpečnosti sa v posledných dňoch riešilo najmä to, čo príde na jeseň. Informácie z beta verzie systému potvrdili zostavu novej série iPhonov vrátane otázky, či medzi nimi bude aj skladací model. Meta po vlne kritiky sprísnila pravidlá pre svoje inteligentné okuliare, ktoré bez viditeľnej diódy už nenahrajú. A Netflix pustil vyššiu kvalitu aj do Chromu, takže na počítači už netreba samostatnú aplikáciu.

https://www.mojandroid.sk/novy-malver-zneuzije-vasu-platobnu-kartu-v-realnom-case-staci-jeden-telefonat