



SLOVÁCI SA VO VEĽKOM VRHLI NA KRYPTOMENY A PODVODNÍCI SA Z TOHO SNAŽIA ŤAŽIŤ

Zvyšujúca sa hodnota kryptomien neušla pozornosti mnohých Slovákov. Vidina rýchleho zhodnotenia peňazí je dôvodom, prečo v týchto dňoch stále viac a viac ľudí ochotne investuje do bitcoinu, etherea a ostatných kryptomien. Na investovaní do kryptomien nie je nič zlé. Odporúčame však starostlivo vybrať spoločnosti, cez ktoré chcete investovať. Aj váš počítač môže byť zneužitý na diaľku! Ťaženie virtuálnych kryptomien je pre mnohých z vás neznámym pojmom, s ktorým sa nestretávate. Napriek tomu môžete byť na túto činnosť využívaný. Zjednodušene - hekeri do Vášho počítača dostanú softvér, prostredníctvom ktorého ho budú využívať na ťaženie kryptomeny a s tým spojený zisk do svojej peňaženky. Ako môžete CRYPTOJACKING rozpoznať? Počítač sa začne prehrievať, výkonnosť baterky sa značne zníži, systém bude pomalý. V takom prípade použite antivírusový program s cieľom vyhľadania malvéru, ktorý za toto všetko môže.

NFC tunneling

Ďalší typ podvodu, ktorý v bankovom sektore registrujeme od začiatku augusta je NFC tunneling, ktorých výskyt sme doteraz registrovali viac v okolitých krajinách ako na Slovensku. Uvádzame vám päť bodov NFC tunneling:

1. Telefonát s "ponukou výnosu z investícií", kedy sa podvodník predstaví ako pracovník finančnej spoločnosti alebo investičného portálu a tvrdí, že chce obeť vyplatiť zisk z investície
2. Inštrukcia na inštaláciu aplikácie HopToDesk, prípadne na inštaláciu podvodnej aplikácie podobnej aplikácii banky. Tu pod zámienkou technickej pomoci ide na obeť požiadavka, aby si do mobilu nainštalovala aplikáciu na vzdialený prístup, zatiaľ najčastejšie HopToDesk.

3. Získanie úplnej kontroly nad mobilom obeť, teda po udelení oprávnení má podvodník prístup k zariadeniu. Môže inštalovať ďalšie aplikácie (napr. HandyPay), čítať správy, spúšťať bankové aplikácie či manipulovať s dátami obeť.
4. Zneužitie NFC technológie, spôsobom že podvodník vyzve obeť, aby k mobilu priložila svoju platobnú kartu (obrazovkou dole, aby obeť nič nevidela). Pomocou NFC tunnelingu prevezme podvodník údaje z platobnej karty a preniesie ich do svojho zariadenia.
5. Následne výber z bankomatu podporujúceho NFC výbery.

Polícia odporúča ako sa chrániť:

- Nikdy si neinštalovať aplikácie na pokyn cudzej osoby, ani v prípade, že sľubuje finančný zisk.
- Neposkytnúť nikomu vzdialený prístup k svojmu zariadeniu.
- Nenechať sa presvedčiť, aby sa prikladala kartu k mobilu.
- PIN kód ku karte, heslá či prístupy do internet bankingu nezdierať s nikým ani s „pracovníkmi banky“.
- Ak sú čo i len malé pochybnosti, ihneď kontaktovať svoju banku.
- V prípade, že bola aplikácia obeťou už nainštalovaná alebo bol poskytnutý prístup, okamžite kontaktovať banku a políciu.

Polícia upozorňuje, aby ste zvážili komu zveríte svoje peniaze na investovanie. Ak nerozumiете investovaniu a kryptomenám v žiadnom prípade neposielať peniaze cudzím osobám!