DE IBK

Támadás alatt a mobilfizetési rendszerek

A pénzügyi csalások evolúciója napjainkra új szintre lépett. A kiberbűnözők egyre kifinomultabb módszerekkel használják ki az olyan **mobilfizetési rendszereket**, mint például az Apple Pay és a Google Wallet. A korábban **mágnescsíkos kártyák** másolására épülő csalások mára kezdik **elveszíteni jelentőségüket**, helyüket pedig azok az eljárások veszik át, amelyek a **kontakt nélküli fizetés, a digitális tárcák és az emberi figyelmetlenség** kombinációját használják ki.

A támadók a klasszikus adathalász stratégiákat egy új szintre emelték. Hamis weboldalak és digitális platformok sorát hozzák létre, amelyek megszólalásig hasonlítanak hivatalos szolgáltatásokra, legyen szó csomagküldő cégekről, webshopokról vagy állami portálokról. A csalás kulcsmomentuma ott következik be, amikor **a megszerzett kártyaadatok** átkerülnek a támadók kezébe, akik ezeket **digitális tárcákhoz kapcsolják**. Speciális szoftverek segítenek a kártyaadatok formátumának pontos replikálásában, így a tárcák gond nélkül elfogadják azokat. Ezután a bűnözők okostelefonjaikkal **kontakt nélküli fizetéseket hajtanak végre boltokban**, vagy **ATM-ekből pénzt vesznek fel**. A rendszeres működéshez a bűnszervezetek ipari méretben szerzik be az okostelefonokat, előre telepített fizetési alkalmazásokkal. Automatizált eszközökkel gyorsítják fel a kártya linkelési folyamatot, így egyetlen áldozattól akár több, részben kitöltött űrlapon keresztül is képesek újabb és újabb kártyaadatokat megszerezni.

Egyes esetekben a megszerzett digitális tárcákat a **dark weben értékesítik**, alternatív módot kínálva az adatok hasznosítására. Ily módon a bűnözők minimalizálják a lebukás kockázatát, és gyakran hónapokkal később monetizálják a megszerzett adatokat.

Egy másik fejlett technika az úgynevezett „Ghost Tap”, amely az NFC-alapú relay támadások egyik változata. Ebben a módszerben **két eszköz között, valós időben** továbbítják a fizetési információkat. Egy legitim NFC alkalmazás segítségével az egyik eszköz olvasóként működik, míg a másik, általában egy bűntárs végrehajtja a tranzakciót.

Egy másik változatban a támadók nem közvetlenül a kártyaadatok megszerzésére fókuszálnak, hanem **social engineering-gel** próbálják rávenni az áldozatokat arra, hogy **rosszindulatú alkalmazásokat telepítsenek**. Ezek gyakran hivatalos szolgáltatások (pl. kormányzati vagy banki applikációk) álcáját veszik fel, és **ellenőrzésre hivatkozva** arra kérik a felhasználót, hogy **helyezze NFC-képes bankkártyáját a telefonhoz**. A szoftver ekkor **leolvassa és továbbítja az adatokat** a támadóknak.

A digitális pénzügyi megoldások kétségtelenül kényelmesek, azonban az ezekhez kapcsolódó biztonsági kockázatok folyamatos növekedése világossá teszi, hogy a technológiai fejlődés mellett elengedhetetlen a megfelelő **védelem és az éberség** is.

Felhasználók számára javasolt biztonsági intézkedések:

- Az egyszeri használatra létrehozott vagy korlátozott érvényességű **virtuális bankkártyák** csökkentik a visszaélések kockázatát.
- A digitális tárcák helyett alkalmazott **hagyományos kártyás tranzakciók** kisebb támadási felületet jelentenek a jelenlegi csalási módszerekkel szemben.
- Csak **megbízható forrásból** (pl. hivatalos alkalmazásboltból) **származó szoftverek** használata, különösen, ha azok banki, állami vagy fizetési szolgáltatást ígérnek.
- Antivírus és **mobilbiztonsági alkalmazások** képesek jelezni az adathalász próbálkozásokat és a gyanús viselkedést.
- A **valós idejű értesítések** lehetővé teszik, hogy a felhasználó azonnal észlelje a gyanús tranzakciókat, és gyorsan intézkedjen.
- Az **ujjlenyomat vagy arcfelismerés alapú azonosítás** megbízható védelmet nyújt a jogosulatlan hozzáférés ellen.
- Rendszeres **figyelemfelhívó kampányok és biztonsági tanácsok** segítik a felhasználókat a fenyegetések felismerésében.