Kiberbűnözés és támadási módszereik

A kiberbűnözők (internetes csalók) különböző módszerekkel próbálják a személyes adatokat, pénzügyi és banki információkat megszerezni vagy vírussal megfertőzni az informatikai eszközöket.

Adathalász regisztrációs, felszólító és promóciós levelek

Számos új adathalász tevékenység jelent meg az elmúlt években, legjellemzőbbek ugyanakkor továbbra is az egyszerű adathalász e-mailek, amelyek gyakran regisztráció megerősítésének, fizetési felszólításnak vagy hivatalos levélnek álcázzák magukat.

Az adathalász e-mailek leggyakrabban ismert szolgáltatók vagy hivatalos közigazgatási oldalak arculatát másolják le és általában tartalmaznak egy hivatkozást, aminek a ráklikkelésére szólítják fel a felhasználót. Gyakran sürgetik is a címzettet, hogy ne legyen ideje, hanem ijedtében hozza meg a gyors döntést. (pl. utolsó figyelmeztetés, késedelmi kamat, hihetetlen kedvezmények, stb.). A hivatkozásra klikkelve a csalók által üzemeltetett ugyancsak ellopott arculati elemekkel ellátott oldal nyílik meg, ahol ténylegesen bekérik a fenti személyes, kicsalni kívánt információkat vagy már a kártékony kód le is fut a felhasználó számítógépén. A leggyakrabban bekért információ az e-mail cím, felhasználó név és a jelszó, hiszen a felhasználók többsége sajnos ugyanazt a jelszót adja meg bármilyen regisztrációs felületen, ami az e-mail címének a jelszava.

A kiberbűnözők mindent megtesznek annak érdekében, hogy ezek az áloldalak, illetve az adathalász e-mailek hasonlítsanak a felhasználók által jól ismert felületekre, levelekre. Vannak azonban árulkodó jelek, amelyek segítenek a csalás kiszűrésében.

- Mindig ellenőrizzük le, hogy ki a tényleges feladója a levélnek!
- Figyeljünk a nyelvezetre, hivatalos levélben nem a „Szia” a megszólítás, ritkán tegeződünk.
- Figyeljük az anomáliákat, sokszor a levél tárgya eltér a levél tartalmától. (pl: A tárgyban „Fizetési felszólítás az elmaradt áramszámla ügyében” szerepel, a szöveg törzsében pedig már elmaradt „gázdíjról” tájékoztatnak.
- Ha nem rendeltünk semmit, nem várunk és nem is küldtünk csomagot, akkor a futárcégek sem küldenek csomagkövetési tájékoztatást.

Itt jegyezném meg, hogy egyre gyakoribbak az SMS formájában érkező postai csomagátvétellel, hamis nyereményjátékokkal küldött linkek, amelyek ugyancsak álweboldalakra irányítanak, és személyes adatok megadására kérnek egy csomag átvétele érdekében.

Telefonos „Call center” csalások

Egyre elterjedtebb csalási forma akár önállóan, akár egy másik csalás sikerességét alátámasztva, megerősítéseként. A csaló telefonon általában egy pénzintézet alkalmazottjaként mutatkozik be és a személyes adatok bekérése után ugyancsak „sokkolja” az áldozatot különböző mondatokkal.

- A rendszer gyanús tevékenységet észlelt.
- Pénzt próbáltak utalni egy külföldi számlára.
- Valaki többször próbált sikertelenül bejelentkezni a netbank felületre.

Az ezekhez hasonló mondatok és a higgadt, nyugodt „segítőkész" hangvételű telefonbeszélgetések célja, hogy az áldozat együttműködő legyen a cél ugyancsak a bankkártya adatok, a jelszavak megszerzése, de egyre gyakoribb a távvezérlő szoftverek telepíttetése is, ahol a csaló hozzáférhet a gyanútlan felhasználó számítógépéhez korlátlanul.

Mobil applikációk

Az okos mobileszközök egyre nagyobb száma miatt meg kell említeni ezeket a készülékeket is, hiszen a körültekintés nélküli telepített applikációk is nagyban veszélyeztetik ezen eszközök biztonságát. Az áruházból letöltött alkalmazások engedélyeit mindig át kell nézni, sajnos a gyakorlat az „Elfogadom az összes engedélykérést" a legjellemzőbb. A csalók ebben az esetben vélt vagy valós hasznos funkcióval ruházzák fel a telefont, ami működése közben a megadott engedélyeknek megfelelően adatot képes továbbítani harmadik fél felé, általában a felhasználó tudta nélkül. A legjellemzőbben játék vagy más szórakoztató szoftvernek álcázott applikáció engedélyt kap alapértelmezetten a tárhelyhez, a kamerához, a mikrofonhoz, a névjegyzékhez, az üzenetekhez és a hálózati erőforrásokhoz egyaránt.

Zsaroló vírusok

A támadás célja a direkt pénzszerzés, általában valamilyen kriptovalutában. A kártékony kód egy hamis weboldalról vagy adathalász email hivatkozásban található linkre kattintva kerül a felhasználó számítógépére. A vírus is egy szoftver, de ebben az esetben a célja nem a hatékony munkavégzés támogatása, hanem a csalás eszköze. A nevéből adódóan nem az azonnali rendszerbénítás a célja, hiszen akkor nem tudna információkat kijuttatni az áldozat számítógépéről, hanem a „megfigyelés" és a legmegfelelőbb időbeni aktivizálódás, vagyis a vírus feltehetőleg már hetekkel a tünetek megjelenése előtt már a számítógépen futott. A legmegfelelőbb idő pedig az, amikor elég adatot gyűjtött a számítógépről és az összes csatlakoztatott háttértároló -és adathordozó eszközön lévő adatot titkosítja és zárolja a számítógépet. A képernyőn kizárólag a „helyreállításhoz" szükséges információk látszódnak, vagyis hová kell utalni a kriptovalutát. Amennyiben nincsen naprakész biztonsági mentés a fájlokról, elég nagy károkat tud okozni az efféle támadás, hiszen csak abban az esetben állíthatók vissza a fájlok, ha fizetünk a zsarolónak. A félreértés elkerülése végett jelzem, hogy a rendszeres biztonsági mentést preferálom, az utóbbit sajnos tényként kellett közölnöm.

A fentiekből kiderül, hogy az internet és a telekommunikációs eszközök használata rengeteg potenciális veszélyforrást rejt, viszont megfelelő vírusvédelemmel, odafigyeléssel, tájékozottsággal és rendszeres szakszerű adatmentéssel lényegesen csökkenthető a kitettség és az okozott kár mértéke.

Hajdara Gábor