Az Ön havi biztonságtudatossági hírlevele

Személyre szabott csalások

Áttekintés

A kiberbűnözők mindig újabb és kreatívabb megoldásokkal állnak elő, hogy átverjék az embereket. Egy új, egyre népszerűbb csalástípus a személyre szabott csalás. A kiberbűnözők megkeresik, vagy megvásárolják több millió ember adatait, és a megszerzett adatokat használják arra, hogy személyre szabják támadásukat. Az alábbiakban bemutatjuk, hogy miként működnek ezek a csalások, és végigveszünk pár gyakori példát is. Minél többet tudunk az ilyen jellegű csalásokról, annál könnyebben fel tudjuk ismerni és el tudjuk kerülni azokat.

Hogyan működik?

Az email vagy telefon alapú csalások nem jelentenek újdonságot, a kiberbűnözők már évek óta próbálják átverni az embereket ezekkel az eszközökkel. Egyik a sok példa közül: “Ön nyert a lottón”, vagy a híres “nigériai herceg” átverés. Azonban, ezen hagyományos csalások során a kiberbűnözők nem tudják, kit céloztak meg. Egyszerűen csak elkészítenek egy általános üzenetet, amit emberek millióinak küldenek el. Mivel ezek a csalások ennyire általánosak, könnyen fel tudjuk őket ismerni. A személyre szabott csalás más, mivel a kiberbűnözők először kutatást végeznek, és egy testre szabott üzenetet küldenek minden egyes várható áldozatnak. Ezt úgy hajtják végre, hogy találnak, vagy vásárolnak egy nagy adatbázist emberek neveivel, jelszavaival, telefonszámaival, vagy más adatokkal. Az ilyen információk viszonylag könnyen elérhetőek a sok feltört weboldalnak köszönhetően. Ilyen információk szinte mindenki által hozzáférhetőek a közösségi média felületeken, illetve a bárki számára hozzáférhető kormányzati adatbázisokban is. A bűnözők aztán mindenkit célba vesznek, akiről információval rendelkeznek.

Az általánosan elterjedt módszerek, amit a bűnözők használnak a félelemre és a zsarolásra alapulnak, amivel arra kényszeríthetnek minket, hogy fizessünk nekik. A támadás a következőképpen néz ki: az emberekről információkat - ideértve a jelszavakat és bejelentkezési neveket - keresnek vagy vásárolnak feltört weboldalakról. Megkeresik a hozzánk tartozó fiókazonosítókat ezekben az adatbázisokban és küldenek nekünk (illetve mindenki másnak, aki az adatbázisban szerepel) egy levelet, mely tartalmaz pár személyes adatot is, ideértve azt a jelszót is, amit a feltört oldalon használtunk. A támadó a jelszavunkra mintegy bizonyítékként hivatkozik, amivel azt tanúsítja, hogy feltörte a számítógépünket vagy egyéb eszközünket, de ez természetesen nem igaz. A bűnöző ezt követően azt állítja, hogy miután betört a számítógépünkre, azon kapott minket, hogy online pornót néztünk. A levélben megfenyeget minket, hogy ha nem fizetjük ki a kért összeget, akkor a kínos online tevékenységünkkel kapcsolatos bizonyítékait megosztja a barátainkkal és családunkkal.

A trükk, ami majdnem minden esetben érvényes, hogy a bűnöző sohasem törte fel a rendszerünket. Azt sem tudják, hogy mi kicsodák vagyunk vagy, hogy mely weboldalakat látogattuk meg. A hacker egyszerűen csak megpróbálja kihasználni a

rendelkezésére álló kevés személyes adatot, hogy azok segítségével elhitesse velünk, hogy feltörte a gépünket vagy eszközünket, és arra próbál rávenni minket, hogy fizessünk neki. Emlékezzünk arra, hogy a rossz fiúk hasonló technikákat használhatnak a telefon alapú csalások esetében is.

Mit tegyünk?

Ismerjük fel, hogy az ilyen emailek vagy telefonhívások csalások. Teljesen természetes érzés a rémültség, amikor felismerjük, hogy valaki személyes információkkal rendelkezik rólunk. Mindazonáltal emlékezzünk arra, hogy a feladó hazudik. A támadás egy automatizált tömegkampány része, nem egy ellenünk szóló célzott támadás. A kiberbűnözők napjainkban egyre könnyebben férnek hozzá személyes adatokhoz, tehát a jelenleginél több személyre szabott csalásra számíthatunk a jövőben. Néhány apró nyom ami, segíthet nekünk a felismerésükben:

- **Bármikor sürgős levelet, hívást vagy üzenetet kapunk, kezdjünk el gyanakodni. Ha valaki megpróbál olyan érzelmeinkre hatni, mint a félelem vagy a sürgősség, akkor csak azt szeretné elérni, hogy hiba elkövetésébe hajszoljon minket.**
- **Ha valaki a fizetséget BitCoinban, ajándékutalványban, vagy más, nem követhető módon kéri**
- **Amikor gyanús üzenetet kapunk, keressünk rá a Google segítségével, hogy mások is jelentettek-e hasonló támadást**

Végezetül, a józan ész használata a legjobb védekezés. Továbbá javasolt egyedi, erős jelszó használata minden online fiókunk esetében. Nem emlékszünk minden jelszavunkra? Használjunk jelszó manager alkalmazást. Mindezeken túl, engedélyezzük a kétfaktoros azonosítást, ahol csak lehetőség van rá.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

A szerzőről

Lenny Zeltser *egy kiberbiztonsági veterán. Anti-malware megoldásokat fejleszt a Minerva Labs-nál és biztonsági képzéseket tart a SANS intézetnél. Tapasztalatokkal rendelkezik továbbá a biztonsági szolgáltatások és a konzultáció területén is. Kövesse őt a* zeltser.com/blog *oldalon és a* @lennyzeltser.

Hivatkozások

A pszichológiai manipuláció:	https://www.sans.org/u/MUU
Állítsuk meg az adathalászatot:	https://www.sans.org/u/MUZ
Keressünk rá Magunkra:	https://www.sans.org/u/MV4
Jelszókezelő programok:	https://www.sans.org/u/MV9