Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

Adathalászat

Áttekintés

Az email napjaink egyik legfontosabb kommunikációs módszere. Nem csak a mindennapi munkánkban használjuk, hanem segítségével tartunk kapcsolatot a családtagokkal és barátokkal is, de az online üzletek ezek segítségével tudnak visszaigazolást küldeni a megrendelt termékekről, vagy a bankok tájékoztatnak bennünket a folyószámlánk állapotáról. Amióta világszerte rengeteg ember napi munkája függ az email-ektől, azóta a kiberbűnözők is elsődleges támadási felületként tekintenek rá. Az OUCH! e havi számában az email-es támadások leggyakoribb fajtáját, az adathalász támadásokat vizsgáljuk meg, illetve kitérünk arra is, hogy milyen lépéseket tehetünk a saját biztonságunk érdekében.

A szerzőről

Dr. Lance Hayden a Berkeley Research Group vezérigazgatója. A biztonsággal kapcsolatos kultúra és viselkedésmód szakértője, a People-Centric Security: Transforming Your Enterprise Security Culture című könyv szerzője. További információkat a **www.linkedin.com/in/drhayden** linken találhatunk a tevékenységéről.

Adathalászat

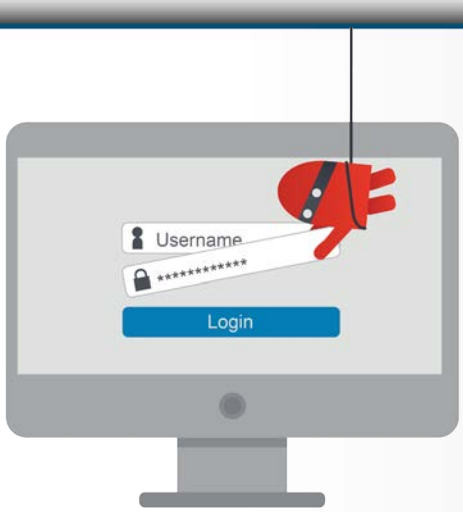
Az adathalász támadás során a támadó megpróbál rávenni bennünket, hogy email-ben vagy egy közösségi oldalon keresztül érkezett üzenetben lévő hivatkozásra kattintva megnyissunk egy weboldalt vagy egy csatolt dokumentumot. Amennyiben áldozatául esünk egy ilyen támadásnak, akkor azt kockázatjuk, hogy a személyes, bizalmas adataink bűnözők kezébe kerülnek, vagy kártékony kóddal fertőződik meg a számítógépünk. A kiberbűnözők keményen dolgoznak azért, hogy az általuk küldött levelek minél meggyőzőbbek legyenek. Például olyan levelet küldenek, amely úgy néz ki, mintha baráttól vagy olyan megbízható cégtől jött volna, amellyel amúgy is kapcsolatban állunk. Az ilyen levelek esetében email címet hamisítanak, vagy olyan logót tesznek a levélbe, amit a bankunk is használ, majd az ilyen hamis leveleket több millió embernek küldik el. Azt nem tudhatják, hogy ki sétál be a csapdába, de azt igen, hogy minél több potenciális áldozatot vesznek célba, annál nagyobb az esélye annak, hogy sikert érnek el. Az adathalász támadás a hálóval való halászatra hasonlít. Nem tudhatjuk, hogy milyen halat fogunk ki, de minél nagyobb hálóval próbálkozunk, annál több halat foghatunk ki. A támadóknak számos módjuk van arra, hogy elérjék, amit akarnak:

- **Információk begyűjtése**: a támadók célja, hogy megszerezzék a személyes adatainkat (jelszavak, hitelkártya számok, banki adatok, stb.). Ennek érdekében egy olyan weboldalra mutató hivatkozást küldenek nekünk, ami megtévesztésig hasonlít egy általunk ismert weboldalhoz, ami azt kéri tőlünk, hogy adjuk meg a személyes adatainkat. Mivel azonban ez egy hamis weboldal, az összes beírt információnk közvetlenül a támadókhoz kerül.

© SANS Institute 2015

Adathalászat

- **Káros tartalomra mutató hivatkozás**: a támadó célja, hogy átvegye az irányítást az áldozat rendszere felett. Ennek érdekében káros tartalomra mutató hivatkozást küld, ami az áldozatot egy olyan weboldalra viszi, amely – sikeres támadás esetén – az eszközön keresztül megfertőzheti a rendszerét.
- **Káros tartalmú csatolmány**: a támadó célja – hasonlóan az előzőhöz – megfertőzni az áldozat eszközét, és átvenni felette az irányítást. A különbség az, hogy ebben az esetben a levélhez csatolt melléklet (pl. egy Word dokumentum) megnyitásakor hajtódik végre a támadás, aminek következtében megfertőződhet a számítógépünk.
- **Csaló email-ek**: vannak olyan adathalász email-ek is, amelyeket csalók küldenek a potenciális áldozatoknak. Ezek a levelek azzal próbálnak átverni bennünket, hogy azt állítják, megnyertük a lottót, jótékonysági szervezetnek mutatják be magukat, és támogatást gyűjtenek, vagy éppen abban kérnek segítséget, hogy több millió dollárt kellene eljuttatni egyik helyről a másikra. A levelekre adott válasszal a csalók vagy előleget kérnének, vagy hozzáférést a bankszámlánkhoz, hogy így fosszanak ki bennünket.



A legjobb védekezés a józan ész használata. Ha egy email vagy üzenet gyanús vagy túl szép, hogy igaz legyen, akkor lehet, hogy adathalász támadás.

Így védekezzünk!

Az email-ek és üzenetek megnyitása és elolvasása az esetek túlnyomó többségében rendben van. Ahhoz, hogy az adathalász támadások működjenek, a bűnözőknek trükköket kell bevetniük, de ezeknek mindig van valami nyoma, így könnyen lelepleződhetnek:

- az üzenet olyan dolgot sugall, hogy azonnal cselekedni kell, mielőtt „valami rossz dolog” történik (pl. felfüggesztik a felhasználói fiókunkat). A támadó célja, hogy a siettetéssel hibát kövessünk el;
- ha kapunk egy email-t olyan csatolmánnyal, amire nem számítottunk, vagy a levél arra akar rávenni bennünket, hogy nyissuk meg a csatolmányt (pl. azzal, hogy még be nem jelentett elbocsátásokról van benne szó, munkatársak fizetési adatait tartalmazza, vagy hogy az adóhivatal vizsgálatot indított ellenünk);
- a nevünk helyett egy általános megszólítást tartalmaz („Kedves Ügyfelünk!”). A barátok és jellemzően a ügyfelek is a nevünkön szólítanak meg bennünket;
- az email bizalmas információt kér (pl. banki adatok, jelszavak);
- az üzenet azt állítja, hogy hivatalos szervezettől érkezett, de ennek ellenére feltűnően hibás nyelvtannal íródott, vagy pedig privát email címeket tartalmaz (@gmail.com, @freemail.hu);

© SANS Institute 2015

Adathalászat

- az üzenet furcsa vagy nem hivatalosnak látszó hivatkozást tartalmaz. Ilyen esetben vigyük az egérmutatót a hivatkozás fölé, és egy felugró kis ablakban látni fogjuk, hogy az kattintásra hová is vinne bennünket. Ha a levélben lévő hivatkozás és a felugró ablak URL címe nem ugyanaz, akkor ne kattintsunk rá! Mobil eszköz esetén, ha az ujjunkkal lenyomva tartjuk a hivatkozást, ugyanezt érhetjük el. Egy biztonságosabb megoldás, ha kimásoljuk vagy beírjuk a helyes hivatkozást a böngészőbe, és úgy nyitjuk meg;
- az üzenetet olyan embertől kaptuk, akit ugyan ismerünk, de a levél hangvétele és szóhasználata mégsem olyan, mintha az a személy lenne a valódi küldő. Ha gyanakszunk, akkor inkább hívjuk fel az illetőt, és kérdezzük meg, hogy valóban ő küldte-e a levelet! A kiberbűnözők könnyen tudnak olyan email-t készíteni, ami látszólag egy baráttól vagy munkatárstól érkezett.

Ha egy email vagy üzenet adathalász támadásnak tűnik, akkor egyszerűen töröljük! A legjobb védekezés a józan ész használata.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

A pszichológiai manipuláció (social engineering): https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_hu.pdf

A biztonság megőrzése öt lépésben: https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201410_hu.pdf

Feltörtek, mit tegyek?: https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-2014-05_hu.pdf

SANS napi biztonsági tipp (angolul): https://www.sans.org/tip_of_the_day.php

OUCH! a SANS Securing The Human program által közzétett hírlevél, amelyre Creative Commons BY-NC-ND 4.0 licensz feltételei vonatkoznak. A hírlevél szabadon terjeszthető vagy felhasználható tudatosító programban, addig amíg az nem kerül módosításra. A fordításért vagy további információért kérjük írjon az ouch@securingthehuman.org címre.

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó