Havi biztonságtudatossági hírlevél számítógép-felhasználók számára

OUCH!

Ebben a kiadványban...

- **Áttekintés**
- **Adathalász támadások**
- **Védd magad!**

Adathalász email támadások

VENDÉG SZERKESZTŐ

Mostani kiadásunk vendég szerkesztője Pieter Danhieux, aki az ausztráliai BAE Systems Detica-nál dolgozik (www.baesystemsdetica.com.au), illetve a SANS Intézet behatolás tesztelés kurzusának oktatója.

ÁTTEKINTÉS

Az email-t tekinthetjük az egyik legfontosabb kommunikációs módszernek. Nemcsak a munkahelyünkön használjuk, hanem a családunkkal és barátainkkal való kapcsolattartásra. Ezenkívül a cégek email-ek segítségével biztosítanak számunkra számos terméket és szolgáltatást, mint például egy online vásárlás visszaigazolását vagy az online banki számlakivonatokat. Mivel nagyon sok ember email levelezésre van utalva, nem meglepő, hogy a kiberbűnözők is az egyik kiemelt támadási felületnek tekintik. Hírlevelünkben bemutatjuk a legáltalánosabb email-es támadásokat, és az ezek elleni védelmi lehetőségeket.

ADATHALÁSZ TÁMADÁSOK

Az adathalászatként eredetileg azokat az email támadásokat jellemezték, ahol az online banki felhasználóneveket és jelszavakat próbálták meg ellopni. A szóhasználat mára megváltozott, és gyakorlatilag minden email alapú támadásra használják. Az adathalászat a social engineering technikát használja, amikor a kiberbűnözők megpróbálnak becsapni, hogy elvégezz valamilyen műveletet. Az ilyen támadások gyakran indulnak azzal, hogy a kiberbűnözők egy olyan email-t küldenek, amelyben egy megbízható barátot, bankot vagy a kedvenc online áruházat imitálnak. Ezek az email-ek megpróbálnak rávenni arra, hogy például kattints egy az üzenetben lévő hivatkozásra, nyiss meg egy csatolt állományt vagy válaszolj egy üzenetre. A kiberbűnözők úgy készítik elő az ilyen email-eket, hogy az meggyőzően nézzen ki, majd elküldik ezeket több millió ember számára. Az ilyen esetekben nincs konkrét célpontja a támadásnak, és azt sem tudják, ki fog besétálni a csapdájukba. Egyszerűen arról van szó, hogy minél több embernek küldik el a leveleket, annál több embert csaphatnak be. Az adathalász támadások az alábbi négy módszert követhetik:

- **Információszerzés:** A kiberbűnözők célja, hogy rákattints egy hivatkozásra, amely egy olyan weboldalra visz, amely felhasználónevet és jelszót, esetleg hitelkártya vagy PIN kódot kér. A weboldal úgy néz ki mintha valódi lenne, hasonlít az online banki vagy bolti oldalakra, ennek ellenére ezek az oldalak a támadó által készített hamisítványok, amelyek segítségével megpróbálja ellopni a bizalmas pénzügyi adatokat.

Adathalász email támadások

- **A számítógép megfertőzése káros hivatkozással:** Ebben az esetben a kiberbűnöző célja ismét az, hogy rákattints az email-ben érkezett hivatkozásra. Azonban az adatlopás helyett az a cél, hogy megfertőzze a számítógéped. Amennyiben megnyitod a hivatkozást egy olyan weboldalra jutsz, amely titokban megtámadja a számítógéped, és ha sikerrel jár megfertőzi azt.
- **A számítógép megfertőzése káros csatolmánnyal:** Ezek olyan adathalász email-ek, amelyek káros csatolmányokat tartalmaznak, mint például fertőzött PDF vagy Microsoft Office dokumentumok. Ha megnyitod ezeket a dokumentumokat, megtámadják a számítógéped, és siker esetén teljes hozzáférést adnak a támadónak.
- **Átverések:** Ezek olyan kísérletek, amikor a bűnözők megpróbálnak becsapni. Klasszikus példák ezekre olyan értesítések, amelyek például lottónyereményről, természeti katasztrófák utáni jótékonysági adománygyűjtésről vagy olyan magas rangú hivatalnokokról szólnak, akiknek több millió dollárt szeretnének a segítségeddel átutalni, és ehhez a segítséged kérik. Nem szabad bedőlni az ilyen csalásoknak, mivel ezek mögött is bűnözők állnak, akik a pénzed akarják megszerezni.

VÉDD MAGAD!

A legtöbb esetben egy egyszerű email megnyitása biztonságos. A legtöbb támadás úgy működik, hogy valamit tenned kell az email elolvasása után (például megnyitni egy csatolmányt vagy egy hivatkozást, esetleg válaszolni). Íme néhány jel, amelyből tudni lehet, hogy az email egy támadás része.

- Legyél gyanakvó, ha egy email „azonnali cselekvést” igényel vagy a sürgősség érzetét kelti. Ez a bűnözők által használt általános technika, mivel az emberek könnyebben hibáznak ha sietnek.

A józan ész elvén, amennyiben egy email szokatlannak vagy túl szépnek tűnik, ahhoz hogy igaz legyen, az valószínűleg egy támadás.

- Legyél gyanakvó, amennyiben az email "Kedves Ügyfél" vagy más egyéb általános megszólítást használ. Amennyiben a banktól érkezett volna, ők tudnák a neved.
- Legyél gyanakvó nyelvtani vagy helyesírási hibák esetén, mivel a cégek többsége gondosan ellenőrzi az üzeneteket elküldés előtt.
- Ne kattints a hivatkozásokra! Inkább másold ki az URL-t és illeszd be a böngészőbe! Még ennél is jobb, ha te magad gépeled be a teljes címet.
- Vidd az egeret a hivatkozás fölé! Ezzel ellenőrizheted az igazi címet, ahova a kattintás után fogsz jutni. Amennyiben a valódi cél más, mint ami az email-ben látszik, az csalás jele lehet.

Adathalász email támadások

- Legyél gyanakvó a csatolmányokkal kapcsolatban, és csak olyat nyiss meg, amit vártál!
- Attól, hogy egy barátodtól érkezett leveled nem jelenti azt, hogy ő küldte. Előfordulhat, hogy a barátod számítógépe fertőzött, vagy valaki feltörte és a kártékony szoftver a névjegyzékben szereplő összes személynek email-t küld. Amennyiben egy gyanús email-t kapsz egy megbízható barátodtól vagy kollégádtól, hívd fel és kérdezd meg, valóban ő küldte-e! Mindig az általad ismert telefonszámot használd, vagy amit önállóan ellenőrizni tudsz, sose azt, ami az üzenetben van!

Amennyiben a levél elolvasása után úgy gondolod, hogy az egy adathalász vagy csaló levél, egyszerűen töröld ki. Végső soron az email biztonságos használata csak a józan eszünkön múlik. Amennyiben valami gyanúsnak látszik, vagy túl jónak ahhoz, hogy igaz legyen, az valószínűleg egy támadás. Ilyenkor egyszerűen töröld a levelet.

HIVATKOZÁSOK

Az alábbi hivatkozások közül néhány a TinyURL szolgáltatással került rövidítésre, hogy könnyebben olvasható legyen. Az esetleges biztonsági problémák miatt az OUCH! mindig a TinyURL előnézeti funkcióját használja, amely megmutatja a hivatkozás valódi célját, valamint engedélyt kér mielőtt továbblép a weboldalra.

OnGuard Online –
http://www.onguardonline.gov/phishing

Adathalász támadások felismerése:
http://preview.tinyurl.com/3c2axs8

OpenDNS Adathalász Védelem:
http://www.opendns.com/phishing-protection

Általános Biztonsági Feltételek:
http://preview.tinyurl.com/6wkpae5

SANS Napi Biztonsági Javaslata:
http://preview.tinyurl.com/6s2wrkp

Biztonságos Internet:
http://preview.tinyurl.com/arhv37c

TUDJON MEG TÖBBET

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

A nemzeti/kormányzati CERT szerepet Magyarországon 2005 óta a Puskás Tivadar Közalapítványon belül működő CERT-Hungary Központ látja el. A PTA CERT-Hungary Központ közhasznú feladatként támogatja a magyar társadalom felkészülését az internet minél tudatosabb és biztonságosabb használatára. További információ a http://www.cert-hungary.hu oldalon olvasható.

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy

Fordította: Birkás Bence, Benyó Pál