OUCH!

SANS SECURITY AWARENESS

Havi biztonság tudatossági hírlevél mindenkinek

Vezérigazgatói csalás / BEC

Mi az a vezérigazgatói csalás / BEC?

A kibertámadók tovább fejlesztik azt az email alapú támadást, amit vezérigazgatói csalásnak (CEO Fraud) vagy Üzleti E-mail Kompromittációnak (Business Email Compromise – BEC) neveznek. Ez egy célzott e-mail alapú támadás, ami arra veszi rá az áldozatot, hogy olyan tevékenységeket végezzen, melyet nem lenne szabad. A legtöbb esetben a rossz fiúk célja a pénzszerzés. Ami igazán veszélyessé teszi ezt a támadástípust az az, hogy a támadók információkat gyűjtenek az áldozatról a támadás indítása előtt. A biztonsági megoldások számára azért nehéz a támadás megállítása, mert maga a támadás nem tartalmaz fertőzött levélcsatolmányt, vagy rosszindulatú hivatkozást, amiket fel lehet ismerni. Hogyan is működik a támadás?

A támadó az Internet segítségével kutatást végez a leendő áldozatáról és a vele kapcsolatban álló személyekről. Például, ha mi vagyunk a célpontjuk, akkor felkutatják, hogy ki a főnökünk a munkahelyen, vagy talán az ingatlanügynököt, akivel otthonról együtt dolgozunk. A támadó ekkor előkészít egy e-mailt, amiben azt színleli, hogy egyike ezeknek az embereknek, és elküldi nekünk ezt a levelet. A levél sürgős, és arra kér minket, hogy tegyünk meg valamit most azonnal, mint például egy számla kiegyenlítése, utalás címzettjének módosítása, vagy meggyőz minket arról, hogy válaszként küldjünk el egy bizalmas dokumentumot. A levél azért lehet hatékony, mert nyomást gyakorol ránk, hogy azt tegyük, amit a támadó szeretne. Alább található két példa, hogyan is működhet egy ilyen típusú támadás.

Pénzátutalás: A kiberbűnözők pénzt akarnak. Alapos kutatást végeznek a céggel kapcsolatban, ahol dolgozunk, például azonosítják azt a személyt, aki a kifizetésekért, vagy az átutalásokért felelős. Ezt követően a támadók levelet küldenek ezeknek a személyeknek, azt színlelve, hogy az Ő főnökük vagy magas rangú vezetőjük. Az e-mail tartalma szerint vészhelyzet van, és azonnal pénzt kell utalni egy új számlára. Az e-mail nyomást gyakorol az áldozatra, hogy hibázzon és a valóságban a pénz a kiberbűnözőnek kerül átutalásra.

Adócsalás: A kiberbűnözők az emberek személyes információi után kutatnak, hogy azokat felhasználva csaljanak az adóval. A leggyorsabb módja ennek az az, ha egy cég összes dolgozójának ellopják az adatait. A kiberbűnözők kikutatják, ki dolgozik a személyzeti osztályon, ezt követően egy hamis levelet küldenek ennek a személynek, azt tettetve, hogy felső vezető, vagy a jogi osztály munkatársa küldte. A levél tartalma egy olyan történet, mely szerint az összes dolgozó adóval kapcsolatos információját sürgősen el kell küldeni. A személyzeti részlegen dolgozó azt hiszi, hogy a bizalmas információt egy felső vezetőnek küldi, miközben valójában azokat a kiberbűnöző kapja meg.

Önvédelem

Mit tehetünk saját védelmünk érdekében? A józan ész használata a legjobb védekezés. Az alábbiakban találhatóak a leggyakoribb jellemzők, amikre gyanakodhatunk:

- A levél nagyon rövid (gyakran csak pár mondat), a sürgősség látszatát kelti, és az aláírás szerint a levelet mobil eszközről küldték.
- Erős sürgetést tartalmaz, és arra biztat, hogy sértsük meg a munkáltatónk eljárásrendjét. Mindig kövessük a munkahelyi eljárásrendeket és szabályokat, még akkor is, ha úgy tűnik, hogy a levelet a főnökünk, vagy a vezérigazgató küldte.
- A levél munkával kapcsolatos, de személyes email címről küldték, mint pl.: @gmail.com vagy @hotmail.com.
- Úgy tűnik, hogy a levelet egy felső vezető, munkatárs, vagy partner küldte, akit ismerünk, vagy akivel együtt dolgozunk, de a levél hangvétele különbözik a megszokottól.
- A levélben fizetési információkat is megadott a feladó, de ezek eltérnek a korábban kapott feladatoktól, mint például azonnali fizetés kérése egy másik bank számlájára.

Ha azt gyanítjuk, hogy a munkahelyünkön célkeresztbe kerültünk, szakítsunk meg minden interakciót a támadóval és jelentsük a vezetőnknek. Ha otthon váltunk célponttá, vagy áldozattá, és már végrehajtottuk az utalást, azonnal jelentsük az esetet a bankunknak, majd a bűnüldöző szerveknek.

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

Don Cavender *egy visszavonult FBI különleges ügynök, több, mint 22 év tapasztalattal a digitális nyomrögzítés és a kiberbűnözés terén. Mostanában a kiberbűnöző csoportokra koncentrál Washington DC-ben, mint BEC koordinátor. Képzéseket szervez és kutatásokat folytat a digitális nyomrögzítés és a kibernyomozás területén.* @don_cavender https://www.linkedin.com/in/donald-cavender

Hivatkozások

Pszichológiai manipuláció:	https://www.sans.org/u/HE3
Állítsuk meg az adathalászatot:	https://www.sans.org/u/HE8
Állítsuk meg a malwereket:	https://www.sans.org/u/HEd
Biztonságos bejelentkezés:	https://www.sans.org/u/HEi

Az OUCH! a Sans Security Awareness részleg által közzétett és a Creative Commons BY-NC-ND 4.0 licensz alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra. A Fordításért vagy további információért lépjen kapcsolatba velünk a www.sans.org/security-awareness/ouch-newsletter címen. Szerkesztette: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Fordította: Tikos Anita

SANS SECURITY AWARENESS
© SANS Institute 2018
NEMZETI KIBERVÉDELMI INTÉZET