OUCH! 2022. január

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Így ismerjük fel és kezeljük az üzenetküldéses támadásokat!

Mik azok az üzenetküldéses támadások?

A smishing (az SMS és az adathalászat szavak egyesítéséből képzett kifejezés) olyan támadásokat jelent, amelyek akkor fordulnak elő, amikor a számítógépes támadók SMS-t vagy hasonló üzenetküldési technológiákat használnak arra, hogy rávegyenek bennünket valamilyen olyan tevékenységre, amelyet nem szabadna megtennünk. Például megtévesztenek bennünket, hogy elküldjük vagy telefonbeszélgetés során megadjuk bankkártya adatainkat, vagy rávesznek, hogy töltsünk ki egy online kérdőívet, amelyben személyes adatokat kérnek tőlünk. Csakúgy, mint az e-mailes adathalász támadások esetében, a kiberbűnözők gyakran az érzelmeket használják ki, hogy cselekvésre ösztönözzenek bennünket, például sürgetéssel vagy a kíváncsiság felkeltésével. Az üzenetküldéses támadásokat az teszi annyira veszélyessé, hogy a szövegben sokkal kevesebb információ és nyom található, mint az e-mailekben, így azt is sokkal nehezebb észlelni, hogy valami nincs rendben.

Gyakori átverési mód például az olyan üzenetek, amelyek arról szólnak, hogy nyertünk egy iPhone-t, és ahhoz, hogy megkapjuk az ajándékot, csupán egy linkre kell kattintanunk, hogy kitöltsünk egy kérdőívet. A valóságban nem létezik ilyen nyereménytelefon, a felmérés csupán átverés, amelynek célja, hogy a kiberbűnözők összegyűjtsék személyes adatainkat. Egy másik példa lehet egy olyan üzenet, amely szerint egy csomagunk nem kézbesíthető, és ebben egy olyan webhelyre mutató hivatkozás szerepel, ahol a kézbesítés befejezéséhez szükséges információkat kellene megadnunk a „szolgáltatási díjak” fedezésére, beleértve a hitelkártya adatainkat. Egyes esetekben ezek a webhelyek akár egy jogosulatlan mobilalkalmazás telepítését is kérhetik, amely megfertőzi, majd átveszi az irányítást eszközünk felett.

A kiberbűnözők néha kombinálják a telefonos és üzenetküldéses támadásokat. Például először egy szöveges üzenetet küldenek – mintha az a bankunktól érkezne – amelyben egy sürgős kifizetés engedélyezésére kérik. Az üzenetben azt kérik, hogy válaszoljunk IGEN-nel vagy NEM-mel a fizetés megerősítéséhez. Ha válaszolunk, a kiberbűnözők tudni fogják, hogy „horogra akadtunk”, és fel fognak hívni, mintha bankunk csalási osztályáról telefonálnának. Ezután megpróbálnak rávenni bennünket arra, hogy eláruljuk pénzügyi és hitelkártya adatainkat, vagy megadjuk netbankos fiókunk bejelentkezési nevét és jelszavát.

Az üzenetküldéses támadások felismerése és megállítása

Íme néhány kérdés, amelyeket fel kell tenniünk magunknak, hogy felismerjük az üzenetküldéses támadások leggyakoribb jeleit:

- Az üzenet rendkívüli sürgősség érzését kelti, és megpróbál siettetni vagy cselekvésre kényszeríteni?
- Az üzenet olyan webhelyre visz, amely személyes – például hitelkártya – adatokat, jelszavakat vagy egyéb bizalmas információkat kér, amelyekhez másoknak nem szabadna hozzáférnie?
- Túl jól hangzik az üzenet ahhoz, hogy igaz legyen? (Nem, sajnos nem nyertünk új iPhone-t.)
- A hivatkozott webhely vagy szolgáltatás arra kényszerít, hogy nem szabványos fizetési módokkal, például Bitcoinnal, ajándékkártyákkal vagy Western Union-átutalással fizessek?
- Az üzenet elkéri a többtényezős hitelesítési kódot, amely a telefonra érkezett, vagy amelyet a banki alkalmazás generált?
- Az üzenet úgy néz ki, mint egy „téves szám?" Ha ezen kérdések valamelyikére a válasz igen, ne válaszoljunk rá, ne próbáljuk meg felvenni a kapcsolatot a feladóval; hanem egyszerűen töröljük az üzenetet!

Ha látszólag egy hivatalos szervezettől kaptunk üzenetet, amelyben figyelmeztetnek bennünket, akkor közvetlenül a szervezettel vegyük fel velük a kapcsolatot! Ne használjuk az üzenetben szereplő telefonszámot, inkább egy megbízható számot hívjunk! Például, ha szöveges üzenetet kapunk a bankunktól, amelyben jelzik, hogy probléma van a bankszámlánkkal vagy a hitelkártyánkkal, vegyük fel a kapcsolatot közvetlenül a bankkal vagy a hitelkártya-társasággal, felkeresve az adott pénzintézet hivatalos weboldalát, vagy közvetlenül tárcsázva őket a bankkártya vagy hitelkártya hátulján lévő telefonszám használatával! Ne feledjük továbbá, hogy a legtöbb kormányzati szerv, például az adó- vagy bűnüldöző szervek soha nem szöveges üzenetben, hanem inkább levélben keresnek meg minket.

Az üzenetküldéses támadások ellen mi magunk vagyunk a legjobb védelem.

A szerzőről

Jeff Lomas a Las Vegas-i rendőrség kibernyomozója, emellett a SANS SEC487 nyílt forrású hírszerzési (OSINT) tanfolyam oktatója. Jeff csúcstechnológiás pénzügyi bűncselekmények ügyében nyomoz, beleértve az üzleti e-mailekkel kapcsolatos kompromittációkat, az üzenetküldéses adathalászatot, a zsarolóprogramokat, valamint az összetett kriptovaluta lopási és pénzmosási ügyeket.

Források

Állítsuk meg az adathalászatot: https://www.sans.org/newsletters/ouch/stop-that-phish/
Pszichológiai manipulációs támadások: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Vishing - Telefonos csaló hívások: https://www.sans.org/newsletters/ouch/vishing/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)