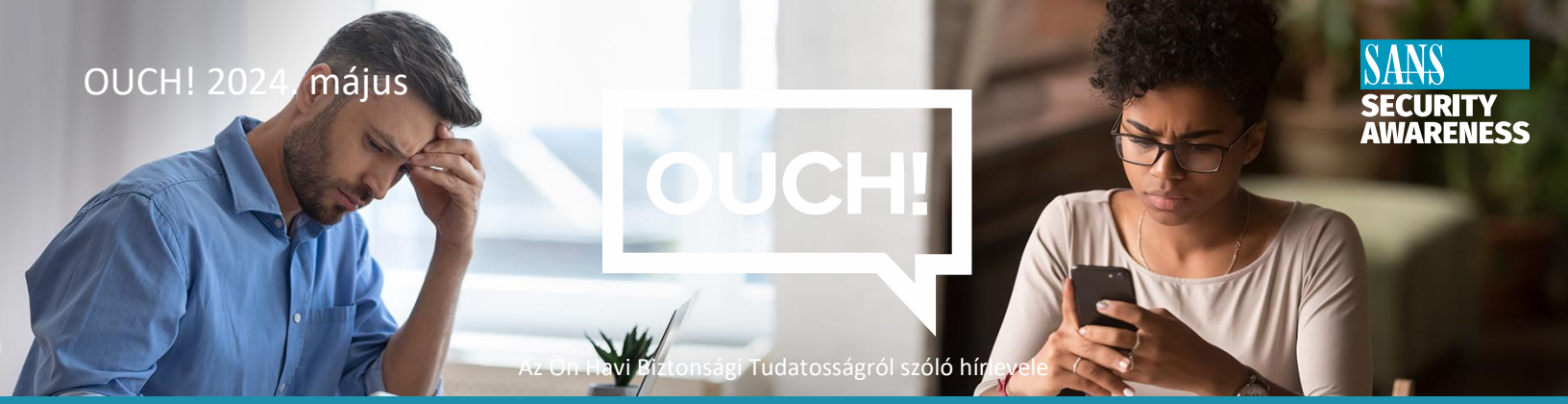

Top Három Módszer, Ahogy A (Kiber)támadók Célpontjává Válunk

Áttekintés

A pszichológiai manipulációs (social engineering) támadások, melyek során a támadók olyasmire vesznek rá minket, amit nem kéne megtennünk, napjaink leggyakoribb kibertámadási módszerei. Az ilyen támadások mögötti elgondolás nem új találmány, évezredek óta alkalmazzák szélhámosok és csalók. Ami valóban újdonság, hogy manapság az internet lényegesen megkönnyíti a kiberbűnözők számára, hogy bárhol, bárkinek kiadhassák magukat, és bárkit célba vehessenek. Az alábbiakban bemutatjuk azt a három leggyakoribb social engineering módszert, amelyekkel a támadók megpróbálhatnak minket megtéveszteni.

Adathalászat

Az adathalászat egy hagyományos pszichológiai manipulációs módszer, amely során a támadók e-mailt küldenek nekünk, hogy rávegyenek valamire, amit nagyon nem kéne megtennünk. Azért is nevezik a módszert adathalászatnak, mert olyan, mint mikor horgászunk egy tónál: Kidobjuk a csalit, de nem tudhatjuk, mi fog a horogra akadni. A módszer mögötti stratégia az, hogy a kibertámadók megpróbálnak minél több megtévesztő adathalász e-mailt küldeni, hogy a lehető legtöbben essenek áldozatul. Napjainkra az adathalász támadások egyre kifinomultabbá és célzottabbá váltak, a támadók gyakran kifejezetten személyre szabják az e-maileket (ezt hívjuk spear phishingnek, azaz célzott adathalász támadásnak is).

Smishing

A smishing lényegében SMS-alapú adathalászatot jelent, mely során e-mail helyett telefonra küldenek szöveges üzenetet a támadók. A szöveges üzenet érkezhet iMessage, Google Message formájában, vagy akár a Whatsappon keresztül is. A smishing egyre nagyobb népszerűsége mögött több magyarázat is áll: Az első, hogy ezeket a szöveges üzenet alapú támadásokat jóval nehezebb kiszűrni, mint az email alapúakat. Másodszor, mivel a támadók által küldött üzenet általában elég rövid, kevés a szövegkörnyezet, emiatt nehezebben tudjuk megállapítani, hogy valós-e az értesítés. A harmadik az SMS-ekhez társított emberi reakció: hozzászoktunk ahhoz, hogy az üzenetekre gyorsan reagáljunk. Mindezeken felül pedig a kibertámadók is igyekeznek adaptálódni a változásokhoz, ha mi egyre ügyesebben szúrjuk ki az adathalász e-maileket, akkor nekik is ideje egy új módszerhez folyamodni, az üzenetküldéshez.

Vishing

A vishing, azaz a hangalapú adathalászat olyan módszer, mely során a támadó e-mail vagy szöveges üzenet helyett telefonhívással, esetleg hangüzenettel próbálja megtéveszteni a felhasználót. A hangalapú támadások bár jóval időigényesebbek, hiszen a támadó közvetlenül lép kapcsolatba és beszél az áldozattal, mégis jóval hatékonyabbak, ugyanis telefonon keresztül sokkal könnyebben lehet erős érzelmeket kelteni a felhasználóban, például sürgetni őt. Ha egyszer vonalba kerülünk egy ilyen támadóval, megfigyelhetjük, hogy nem fogja hagyni, hogy letegyük a telefont addig, amíg meg nem kapja, amit akar.

A Támadások Felismerése és Megállítása

Nem számít, hogy a kibertámadók a három módszer közül melyiket választják, szerencsére vannak a támadásoknak közös jellemvonásaik, amelyeket mi magunk is felismerhetünk:

- **Urgency**: Minden olyan üzenet, amely erőteljes sürgősségérzetet kelt bennünk, amiben a támadó nagyon gyors cselekvésre sarkall minket. Ilyen lehet például egy látszólag kormányzati szervezettől érkezett üzenet, amely azt állítja, hogy ha nem fizetjük be azonnal az adóhátralékunkat, akkor börtönbe kerülünk.

- **Nyomásgyakorlás**: Minden olyan üzenet, amely arra kényszeríti a munkavállalót, hogy hagyja figyelmen kívül vagy kerülje meg a vállalat biztonsági irányelveit.

- **Kíváncsiság**: Minden olyan üzenet, amely túlzottan kíváncsivá tesz, vagy túl jól hangzik ahhoz, hogy igaz legyen. Jó példa erre egy kézbesíthetetlen UPS csomag, vagy egy Amazon visszatérítésről kapott értesítés.

- **Hangnem**: Bármilyen üzenet, amely látszólag egy ismerősünktől, kollégánktól érkezett, de a hangnem, vagy a megfogalmazás stílusa nem rá vall, esetleg az aláírása nem stimmel.

- **Érzékeny információ**: Minden olyan üzenet, amelyben érzékeny adatokat kérnek tőlünk, például a jelszavunkat, vagy a bankkártyánk adatait.

- **Általános**: Látszólag megbízható szervezettől érkezett az üzenet, azonban túl általános megszólítást használ, például "Kedves Ügyfél!". Ha az Amazontól csomagunk érkezik, vagy esetleg a szolgáltatónak számlázási problémája van, akkor tudni fogják a nevünket.

- **Személyes email cím**: Minden olyan e-mail, amely látszólag valós szervezettől vagy kollégától származik, azonban személyes email címet használ, például @gmail.com vagy @hotmail.com**.**

Ha figyelünk ezekre a gyakori jelekre, akkor nagyban hozzájárulhatunk saját védelmünkhöz.

A szerzőről

Mary Jane Suarez Partain a Women in CyberSecurity (WiCyS) programigazgatója. Tevékenysége középpontjában az áll, hogy forrásokat és programokat biztosítson a nők számára a kiberbiztonság területén, ezáltal hozzájárulva a szakmába való toborzásukhoz, megtartásukhoz és fejlesztésükhöz. Szenvedélyesen törekszik egy olyan befogadó környezet megteremtésére, ahol mindenki úgy érezheti, hogy értékelik és szívesen fogadják.

Források

Állítsuk meg a telefonos csalóhívásokat: https://www.sans.org/newsletters/ouch/stop-phone-call-scams
Egyre trükkösebbek az adathalász támadások: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/
Érzelmi triggerek – Így csapnak be minket a kibertámadók: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Meghekkeltek, most mit csináljak: https://www.sans.org/newsletters/ouch/im-hacked-now-what/

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