SANS SECURITY AWARENESS

Szöveges adathalászat / „Smishing” támadás

Áttekintés

A leggyakoribb módszerek, amelyekkel a számítógépes támadók megkísérlik becsapni vagy átverni az embereket, azok az e-mailek (ezt gyakran adathalászatnak nevezik) vagy telefonhívások útján elkövetett csalások. Mivel a technológia folyamatosan fejlődik, a bűnözők mindig új módszereket próbálnak ki, beleértve az olyan üzenetküldési technológiák felhasználásával történő csalásokat, mint például a szöveges üzenetküldés, az iMessage/Facetime, a WhatsApp, a Slack vagy a Skype. Itt találhat néhány egyszerű lépést, amelyekkel megvédheti magát és képes lehet észlelni / megállítani ezeket a gyakori támadásokat.

Mik azok az üzenetküldéses támadások?

Az üzenetküldéses támadások (amelyeket néha az angol „adathalászat - phishing” szóra utalva Smishingnek hívnak) során a számítógépes támadók SMS-t, vagy üzenetküldési technológiákat használnak annak érdekében, hogy kapcsolatba lépjenek Önnel, és megpróbálják rávenni olyan tevékenységre, amelyet nem lenne szabad megtennie. Előfordulhat, hogy rá akarják venni egy rosszindulatú linkre való kattintásra, vagy egy telefonhívásra, amelynek során megszerezhetik banki adatait. Csakúgy, mint a hagyományos adathalász e-mail támadások esetén, a bűnözők gyakran az érzelmeire próbálnak hatni. Az üzenetküldéses támadásokat azonban az teszi annyira veszélyessé, hogy sokkal informálisabbak és személyesebbek, mint az e-mailek, így valószínűbb, hogy azok áldozatává válik. Ráadásul az üzenetküldéses támadásoknál kevesebb információ és jel áll rendelkezésre, ami alapján felismerheti, hogy valami nincs rendben vagy gyanús. Amikor furcsa vagy gyanús üzenete érkezik, kezdje azzal, hogy felteszi magának a kérdést, van-e értelme ennek az üzenetnek, vajon miért kaptam meg? A támadások leggyakoribb jelei az alábbiak.

- Sürgetés érzete, amikor valaki megpróbálja rávenni Önt valamely cselekvés elvégzésére.
- Kér az üzenet személyes információkat, jelszavakat vagy más érzékeny adatokat, amelyekhez másnak nem szabadna hozzáférnie?
- Túl jól hangzik az üzenet ahhoz, hogy igaz legyen? Nem, nem nyert a lottón, főleg azon, amelyen sosem vett részt.
- Egy üzenet, amely úgy tűnik, hogy az egyik munkatársától vagy barátjától érkezett, de a fogalmazás módja nem ismerős. Lehet, hogy a felhasználói fiókja kompromittálódott és azt egy támadó vette át, illetve a támadó másnak adja ki magát, ezzel Önt becsapva egy cselekvés végrehajtására veszi rá.

Ha olyan üzenetet kap, amely erőteljes reakciót vált ki Önből, várjon egy pillanatot, és adjon egy esélyt arra, hogy megnyugtassa magát és gondolja át, mielőtt válaszolna.

Néha a bűnözők az e-mailes és üzenetküldéses támadásokat még kombinálják is. Például az ajándékkártya-csalások is működhetnek így. A számítógépes támadók sürgős e-mailt küldenek Önnek, a barátja vagy munkatársa nevében, majd elkérik az Ön mobiltelefonszámát. Ezután ismételt szöveges üzeneteket küldhetnek, és nyomást gyakorolhatnak az ajándékkártyák megvásárlására. Miután megvásárolta azt, a támadók lekapartatják a kártya hátoldalán található kódot, majd fényképet kérnek arról. Egy másik gyakori támadás egy videó vagy kép formájában arra szólít fel, hogy „ezt figyeld" („ezt nem fogod elhinni!"). Ezzel használják ki a kíváncsiságát. Ha az üzenet úgy néz ki, mintha valamelyik ismerősétől származna, mielőtt cselekedne hívja fel az érintettet, hogy ellenőrizze az üzenet hitelességét.

Ha egy hivatalos szervezettől kapott üzenetet, amely figyelmezteti Önt, akkor közvetlenül vegye fel velük a kapcsolatot. Például, ha szöveges üzenetet kap a bankjától, amelyben jelzik, hogy probléma van a bankszámlájával vagy a hitelkártyájával, vegye fel a kapcsolatot közvetlenül a bankkal vagy a hitelkártya-társasággal, felkeresve a bank webhelyét, vagy közvetlenül tárcsázva őket a bankkártya vagy hitelkártya hátulján lévő telefonszám használatával. Ne feledje, hogy a legtöbb kormányzati ügynökség, mint például az adó- vagy bűnüldöző szervek, szöveges üzenettel nem lépnek Önnel kapcsolatba.

Az üzenetküldéses támadások ellen Ön a legjobb védelem.

Magyar Kiadás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. Az NKI 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 https://nki.gov.hu oldalon olvasható.

A szerzőről

Jen Fox *a „DEF CON 23" rendezvényen, a pszichológiai manipuláció területén kiosztott „black badge – fekete kitűző" díj tulajdonosa, aki biztonsági tudatossági oktatással foglalkozik a Domino biztonsági program szakértőjeként. Kövesd a Twitteren:* @j_fox.

Források

Pszichológiai befolyásolás:	http://www.sans.org/u/XAQ
Adathalászat megállítása:	http://www.sans.org/u/XAV
Telefonos átverés:	http://www.sans.org/u/XB0
Csaló szöveges üzenetek jelentése:	https://www.consumer.ftc.gov/articles/0350-text-message-spam