Három jótanács az adathalászat elleni védekezéshez

- Miben hasonlít a nagymamánk, az unokánk, a főnökünk, Elon Musk és a kedvenc bankunk?

- Abban, hogy mindegyikük nevében követnek el adathalász-jellegű kibertámadásokat. Így többmillió forintos csalások áldozataivá válhat családunk, munkáltatónk és saját cégünk is. Cikkünk négy pontban mutatja be az adathalász támadások típusait és az ellenük történő védekezés legegyszerűbb stratégiáit.

*

Egy új korba léptünk

A *Phishing*, vagy *adathalászat*, egy olyan módszer, amellyel a kiberbűnözők megtévesztő üzenetek küldésével bizalmas információkat lopnak el tőlünk, például:

- online banki bejelentkezési adatokat,
- bank - és hitelkártya adatokat,
- üzleti bejelentkezési adatokat, vagy jelszavakat.

Illetve a kiberbűnözők személyes adataink megszerzésével óriási adatbázisokat építenek ki, amelyeket aztán eladnak, vagy felhasználnak egy későbbi támadáshoz. Legszemélyesebb adatainkkal, például szexuális orientációnkkal, vallási és politikai nézeteink megszerzésével pedig még érzékenyebb csalikat készíthetnek nekünk a bűnözők.

Jó, ha tudjuk, hogy stanford-i és cambridge-i kutatók már 2011-ben kimutatták, hogy a social media platformokon mutatott aktivitásunk – posztjaink szóhasználata, like-jaink és emoji használatunk összeségével jól leírható pszichológiai alkatunk, amellyel előre jelezhető vásárlói preferenciánk és politika gondolkodásunk is. A Mesterséges Intelligencián (MI) alapuló adatelemzési technikákkal egy olyan korba léptünk, amikor a magánszféránk felszámolódik: minden általunk közzétett adat pontosabbá teszi a rólunk kialakított képet. Sőt, az ilyen elemzéseken alapuló kommunikációs stratégiák a személyiségünk fejlődését is képes befolyásolni, - erre figyelmeztet például Shoshana Zuboff, a Harvard Egyetem professzora is. Tehát, az MI-n alapuló adatelemző technikákkal nemcsak politikai gondolkodásunkat, vagy fogyasztói preferenciáinkat lehet elemezni, de sokkal könnyebb előállítani olyan üzeneteket, amelyekre nagyobb hajlandósággal rákattinthatunk.

Az adathalász tevékenységek típusai

A védekezés szempontjából a kiberbiztonsági szakértők az adathalász támadásokat a célpontjaik mérete és fókusza szerint három nagy csoportba osztják:

- A „szigonyozás” (Spearphishing) egy olyan jól irányzott, gyakran személyre szabott támadás, melynek fókuszpontjában kisebb csoportok, vállalatok, szervezetek állnak.
- „Eltereléses csalás” alkalmával (Business Email Compromise, BEC) üzleti emaileknek látszó fizetési felszólítások és beérkező ajánlatok a vállalatok felsővezetését, illetve a számlakiegyenlítésre jogosultakat célozza meg. Az eltereléses csalások veszélyeiről részletesebben itt írtunk.
- Ezeken kívül pedig, általános adathalászatnak, *Phishing*-nek nevezünk minden olyan adatbázisbővítő, nyomkövető üzenetet, amelynek célja, hogy minél több olvasóhoz eljusson.

A fókuszcsoportokon kívül a támadási stratégiákra is érdemes odafigyelnünk.

- A *klónozó adathalászat* taktikájával a támadó nem egy konkrét személyt vagy szervezetet, hanem egy csoportot vesz célba. A támadó egy hamis e-mailt hoz létre, amely legitim forrásból származónak tűnik, de az e-mailben található link egy olyan weboldalra vezet bennünket, ahol az áldozat személyes adatai kerülhetnek nyilvánosságra, vagy eszközére zsarolóvírus kerülhet.

- A *zsarolóvírusok*kal összekötött adathalászatkor egy rövid üzenetet kapunk, amelyben például egy csomagküldő, futárszolgálat kéri, hogy töltsük le az üzenetbe linkelt alkalmazást, hogy átvehessük egy korábban rendelt csomagunkat. Ezek a vírusok a teljes kontrollt is átvehetik a telefonunk felett, ellopva ezzel jelszavainkat, bankkártya-adatainkat is.

Habár a legtöbb adathalászat a mai napig email-ben történik, jó, ha tudjuk, hogy más csatornákon, illetve online platformokat is előszeretettel halásznak a kiberbűnözők:

- Social Media Phishing: vagyis a közösségi média platformok, mint például a Facebook, LinkedIn, Twitter, Instagram igazi vadászmező a kiberbűnözők számára. Ezeken a felületeken számos olyan információt osztunk meg, amelyet illetéktelenek hamar ellenünk fordíthatnak. Egyúttal ezek a platformok a legalkalmasabbak a gyors és nagy terjedelmű adatbázisok kiépítésére. 2021-ben több, mint 500 millió Facebook felhasználó telefonszáma került ki az internetre.
- Smishing: SMS általi adathalászat: Egy rövid üzenetben egy link segítségével egy applikáció letöltésére, vagy egy bizonyos honlap felkeresésére kérnek bennünket.
- Vishing: Telefonos adathalászatkor a támadó élőszóban vagy hangüzenetben, például a bankunk, vagy internetszolgáltatónk nevében csal ki tőlünk fontos információkat.

*

Pár gyakorlati példa a nagyvilágból:

Ahhoz, hogy a csalások közötti hasonlóságokat észre vehessük, érdemes pár megtörtént esetről szóló beszámolót is szemügyre vennünk:

- A BBC írta meg tavaly márciusban, hogy a bitcoin-láz egyik csúcsán, egy Elon Musk nevében írt Twitter-bejegyzésnek bedőlve több, mint 407.000 dollárt bukott egyetlen köln-i felhasználó.
- 2021 májusában a Colonial Pipeline-t - az Egyesült Államok egyik olajszállításért felelős cégének informatikai rendszerét egy zsarolóvírusos támadás érte. A bűnözők első lépésben 4.4 millió dollár váltságdíjat zsebeltek be. A hét folyamán azonban további kár érte a céget, mivel a lakosság pánikból elkezdte felvásárolni a még elérhető benzint. Így az eset további reputációs és bizalmi válsághoz vezetett az USA-ban. Az eset után az Amerikai Igazágügyi Minisztérium a zsarolóvírusos támadásokat terrorcselekményeknek minősítette. Az eset értő elemzését kollégánk tollából itt olvashatja.
- A Covid-19 világjárvány az online-rendeléseket is népszerűvé tette. Az előző karácsonyi szezon ideális körülményeket biztosított az adathalászoknak is. Az ünnepek előtt számos csomagküldő szolgálat nevében küldtek ki a hekkerek adathalász üzeneteket és zsarolóvírusokat. A támadók a Fedex, a DHL, az Amazon és a UPS nevében küldtek SMS-eket és e-maileket. Hasonló esetről például a német közszolgálati TV itt tudósított.

Három jótanács az adathalászat elleni védekezéshez:

1. **A kapkodás, a pánik és a mohóság a legrosszabb tanácsadók!**

Ne siessünk! Minden kattintást gondoljunk át kétszer. És tegyük fel a lehető legnaivabb kérdéseket magunknak.

2. **Ne lépjünk túl a gyanús jeleken!**

Nézzük meg figyelmesen, hogy: Melyik e-mail címről írt a feladó? Kaptunk-e erről a címről már korábban is e-mailt, SMS-t? Ha valóban a kollégám írt, miért nem szólt személyesen, vagy használt másik csatornát? Miért hív rejtett számról a bankom? Biztos, hogy hajnali kettőkör értesítenek bármiről is? Ha hivatalos ez az e-mail, miért nem szerepel rajta a megszokott digitális aláírás? Miért ajánl fel bárki is egy ennyire jó pénzügyi ajánlatot?

3. **Figyeljük meg saját érzelmeinket!**

A támadó üzenetek és hívások gyakran kényelmetlen szituációba hajszolnak bennünket. Az egyszerű felhasználó számára nehezen értelmezhető szaknyelv frusztráló lehet, akár szégyenérzetet is kelthet, így már fel sem merül bennünk, hogy miért kellene ilyen nagyon gyorsan cselekednünk. De biztos bennünk van a hiba?

A bizonytalanságot szülő helyzetekben jó kérdések lehetnek a következők: Biztos, hogy most azonnal le kell töltsem ezt az App-ot, - nem érne rá két óra múlva? Mit írnak erről a kedvezményről a bankom honlapján? Ez a telefonszám megegyezik a bankom honlapján lévővel? Nem volna jobb holnap, inkább személyesen rákérdezni? Valóban szükségszerű ez a frissítés, vagy inkább hívjam fel a rendszergazda csapatot telefonon? Ha valóban ilyen fontos ez a frissítés, miért nem szóltak róla hetekkel korábban?

Fontos, hogy a telefonos eseteknél se adjuk ki személyes adatainkat, időhúzásként például kérjünk másnapi visszahívást! Nincs az a késedelmi díj, ami a folyószámlánk feletti kontroll elvesztésénél fájóbb volna.

*

A legkisebb gyanú és bizonytalanság is szerencsésebb, mint egy támadás áldozatának lenni. Amennyiben úgy érzi, hogy cégének is szüksége lenne adatvédelmi és információbiztonsági képzésekre és technológiai megoldásokra, forduljon hozzánk bizalommal.