Bitdefender

Hogyan lehet kiszúrni a telefonos adathalászatot?

A Bitdefender segítségével mutatjuk!

A mobilos adathalászat egyre népszerűbb a kiberbűnözők körében, mivel az emberek egy részét viszonylag könnyű megtéveszteni, és nem mindenki hajlandó biztonsági megoldást telepíteni a telefonjára.

A Bitdefender 2021-es online viselkedésről szóló jelentése szerint a rendszeresen internetezők:

- 2/3-ada akár 3 eszközt is használ erre a célra;
- a felhasználók fele a mobiltelefonján internetezik;
- online bejelentkezési adataikat egyharmaduk automatikusan megjegyezteti a platformmal, egynegyedük pedig le is írja valahova az adatokat;
- 61%-ka tapasztalt legalább egy kiberfenyegetést az év során;
- a telefonos átverések és adathalászat az összes fenyegetés 59%-át tették ki;
- a felhasználók 15%-ka semmilyen biztonsági megoldást sem használ;
- a vírusírtót, végpontvédelmi rendszert használók 30%-ka semmilyen védelmi szoftvert nem használ a mobiltelefonján.

Akik elutasították a védelmi rendszer használatát, leggyakrabban az alábbiakra hivatkoznak:

- „az okostelefonomba beépített online biztonsági rendszer van” (16%);
- „online szokásaim nem igényelnek mobilbiztonsági megoldást” (14%);
- „a biztonsági termékeket nehéz telepíteni” (9%);
- „túl sok a téves figyelmeztetés” (9%);
- „összeférhetetlenség az eszközön lévő más alkalmazásokkal” (8%);
- „az okostelefonok nincsenek kitéve káros kódoknak” (7%);
- „lelassul tőle a mobiltelefon” (6%)

... és a lista folytatódik. Sőt, a válaszadók 13%-ka egyenesen így fogalmazott: „Nem bízom a vírusirtókban és azok gyártóiban”.

Ezek a tévhitek azonban arra ösztönzik a kiberbűnözőket, hogy folyamatosan fejlesszék módszereiket, hiszen egyre nagyobb bevétellel kecsegtethetnek a támadások. És ugye tudjuk jól: minden szituhoz kiválóan alkalmazkodnak.

Ijesztegetés vagy csali?

Az SMS adathalászat (röviden Smishing) néven is ismert mobil adathalász technikák az SMS-t használják fel. A támadók egy olyan üzenetet jelenítenek meg a készüléken, amely valamilyen cselekvésre akarja rávenni a leendő áldozatot. Ilyen esetekben is a megszemélyesítést használják módszerként, tehát valamilyen ismert szolgáltató, szervezet nevében küldik az üzenetet. Csakúgy, mint a hagyományos adathalászat során, a támadók gyakran az érzelmekre is próbálnak hatni, és sürgető hangnemet használnak

Az SMS szövege lehet például a következő:

„Új hangüzenetet kapott a [telefonszám] címről. Hallgassa meg itt [URL]”

„Ön nyert egy iPhone 13-at! Kövesse ezt a linket [URL], hogy átvehesse a nyereményét”.

„Megérkezett a csomagja, kövesse nyomon itt [URL]”

„Önt részmunkaidős / teljes foglalkoztatásra választották ki. WhatsApp alkalmazáshoz adja hozzá a [telefonszám] számot.”

„A bankjánál meg kell változtatni bejelentkezési adatait, amelyet itt [URL] megtehet.”

"Jelentkezzen be, hogy megerősítse személyazonosságát. [URL]”

"Az Ön számlája veszélybe került. Hívja az alábbi [telefonszám] számot a részletekért.”

„Ezt figyeld. Ezt nem fogod elhinni [URL]”

... és így tovább.

Adathalászat és a social engineering

Néha az adathalászok social engineering trükkjeit arra is használják, hogy rosszindulatú szoftvereket juttassanak el a gyanútlan áldozatokhoz. A **FluBot** például egy különösen veszélyes kártevő, amely mobileszközökön található banki adatokra vadászik, és a smishing-támadásokkal megegyező módon kerül az áldozatok telefonjára. A FluBotról korábban már mi is írtunk, **itt el is olvashatod.**

A kiberbűnözők néha az e-mailes adathalászatot a telefonos adathalászattal együtt, ezen módszereket kombinálva használják. Például az ajándékkártya-csalások hasonló analógia mentén is működhetnek. A csalók egy sürgető hangnemű e-mailt küldenek a potenciális áldozatnak, de teszik mindezt egy munkatárs vagy ismerős nevében (az e-mail cím hasonlítani fog a megszemélyesített fél nevére), és elkérik a felhasználó mobiltelefonszámát. Ezután teljesen simán tudnak SMS-t

küldeni az áldozatnak, és nyomást is tudnak rá gyakorolni, hogy vásárolja meg az ajándékkártyát. Miután az illető megvásárolta a kártyát, a támadók lekapartatják annak hátoldalán található kódot, majd fényképet kérnek róla.

Hogyan védekezhetünk?

Most, hogy tudjuk, mire kell figyelni, sokkal könnyebb lesz kiszúrni a csalást. Legalábbis reméljük. Ha mégis kétségek merülnek fel, akkor mindig javasolt kapcsolatba lépni egy másik csatornán azzal, akinek a nevében akarják elkövetni a csalást. Legyen szó barátról, munkatársról, vagy éppen az egyik szolgáltatónkról.

- Fontos, hogy ne higgyük el, hogy prémium kategóriás készüléket nyertünk, vagy minket sorsoltak ki a főnyereményre. Ami túl szép ahhoz, hogy igaz legyen, az általában nem az.
- Az SMS-ben érkezett linkekre semmiképp sem javasolt a kattintás, és a megadott telefonszámokat sem érdemes felvenni egyetlen csevegő alkalmazásba se.
- A kapkodás sosem jó. Szánjunk időt arra, hogy átgondoljuk az üzenet tartalmát, és adott esetben nézzünk utána a feladónak, vagy a megszemélyesített szervezetnek más fórumokon. Például az adott cég hivatalos elérhetőségein.
- Soha ne válaszoljunk olyan szöveges üzenetekre, amiben PIN kódot, online banki jelszót vagy más bizalmas adatot kérnek! Ha ez mégis megtörtént, akkor azonnal értesítsük a releváns pénzintézetet!

- Fontos megjegyezni, hogy egyetlen szolgáltató sem kér SMS-ben jelszavakat vagy PIN-kódokat, sem más bizalmas adatokat!

Bár az éberség gyakorlása és a kellő elővigyázatosság nagyszerű módja az adathalászat elleni küzdelemnek, egyes kampányok már elég kifinomultak ahhoz, hogy még a gyakorlottabbakat is becsaphassák. Ezért egyre fontosabb, hogy biztonságunkat és magánéletünket erre a célra kifejlesztett eszközökkel és szakértelemmel védjük.

A Bitdefender Mobile Security for iOS és Android megszűri a bejövő adatokat, és blokkol mindent, ami fenyegetésnek tűnik. Köszönhetően a több millió beérkező és megvizsgált mintának, a Bitdefender első kézből származó és friss információkkal rendelkezik a legújabb csalásokról is. Emellett egy titkosítási réteget is hozzáad a védelmi rendszerhez, hogy megakadályozza az adatok helytelen kezelését. Az új **Scam Alert funkció** extra lépéseket tesz, és még azelőtt csapást mér a csalókra, hogy az áldozatnak esélye lenne kapcsolatba lépni a rosszindulatú tartalommal.

Bár az éberség mindenképpen segít, egy dedikált biztonsági megoldás valószínűleg a legegyszerűbb módja annak, hogy meghiúsítsa a telefonos adathalászatot. Ez azt jelenti, hogy még kiberbiztonsági szakértőnek sem kell lenni ahhoz, hogy megvédjük magunkat és eszközünket a támadási kísérletekkel szemben.