Miért esünk könnyen áldozatul az SMS csalásoknak?

Az ESET szakemberei bemutatják az új SMS csalást és a szükséges teendőket, ha letöltöttük az adatlopó alkalmazást

Sajtóközlemény – 2021.03.26./PResston PR

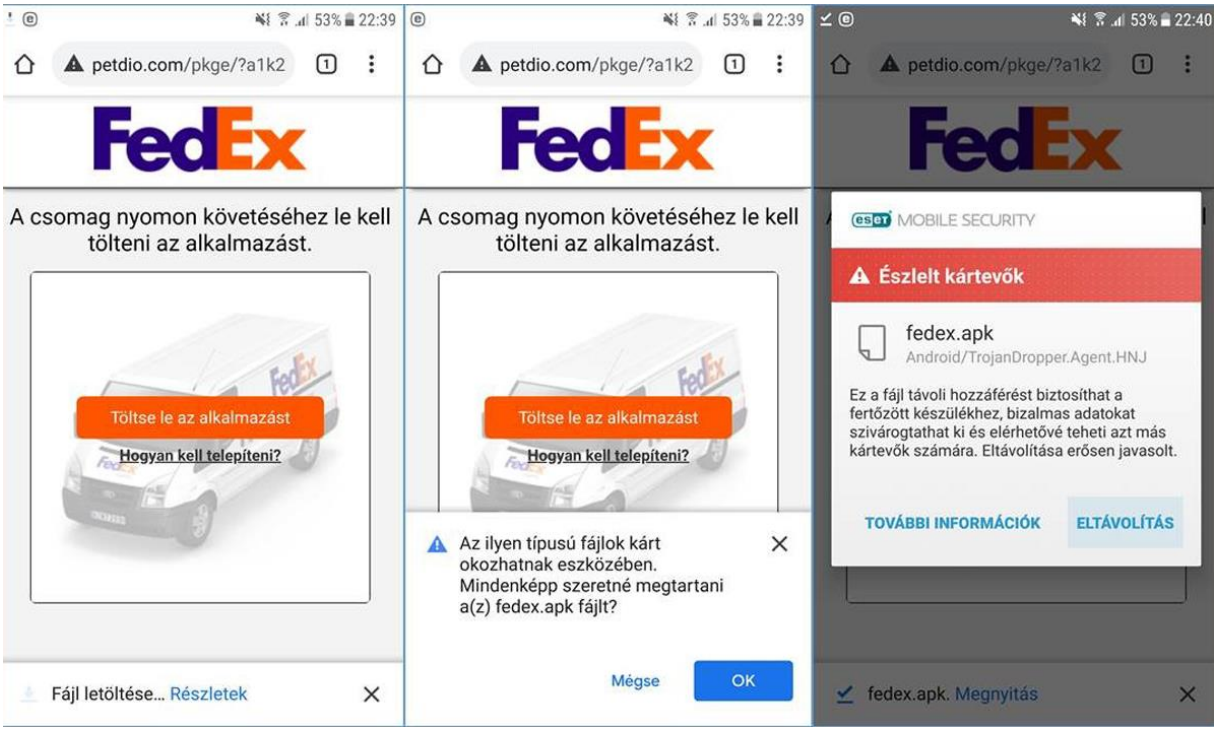
Egy új csalássorozat terjed hazánkban, amely a járvány és a korlátozó intézkedések hatására egyre népszerűbb házhozszállítást igyekszik kihasználni. A koronavírus járvánnyal kapcsolatban a biztonsági szakemberek már többször említették, hogy a kiberbűnözők nagyon kreatív módon igyekeznek kihasználni az aktuális híreket, körülményeket. Nincs ez másképp most sem: az elmúlt napokban a webshopos vásárlások számának növekedéséhez igazodva futárszolgálatok nevében küldenek üzeneteket a csalók.

„Több olyan megkereséssel fordultak hozzánk az elmúlt napokban, miszerint tömegesen érkeznek magyar nyelvű, de ékezeteket nélkülöző SMS-ek, amely „Megerkezett a csomagja, kovesse nyomon itt: http://...” üzenetet tartalmaznak. A jelenségre a rendőrség is figyelmeztet. A beszámolók alapján több különféle számról is kaphatunk ilyen SMS-t, a csalók valószínűleg egy egész SIM kártya arzenált vetnek be annak érdekében, hogy elkerüljék, hogy a szolgáltató, észlelve a tömeges kiküldéseket, letiltsa valamelyik telefonszámot. A tapasztalatok alapján 20-as és 30-as hazai számokról érkeznek az üzenetek, de nem kizárt, hogy 70-es telefonszámról is érkezik ilyen üzenet.” – számol be az új csalássorozatról **Csizmazia-Darab István, a Sicontact Kft. IT biztonsági szakértője**.

A csomagunk nyomkövetésére felszólító SMS minden esetben tartalmaz egy linket, amelyet megnyitva látszólag egy ismert futárszolgálat oldalára kerülünk. Itt arra kérnek minket, hogy a csomagunk nyomon követeséhez töltsünk le és telepítsünk egy alkalmazást. Ha így teszünk, egy „.apk” kiterjesztésű fájl töltődik le a telefonunkra, amely kártevőt tartalmaz. Fontos megjegyezni, hogy ez a vírus csak akkor jelent veszélyt, ha a telefonunkon ki van kapcsolva az ismeretlen forrásokból történő telepítés tiltása. Ha ez be van kapcsolva, akkor jelezni fog, hogy nem megbízható a telepítő, és külön engedélyt kell adnunk ahhoz, hogy települhessen a készülékre – természetesen ezt ne adjuk meg neki.

Jelenlegi információnk alapján a telepítés után az adatlopó program egy távoli szerverre továbbítja a készüléken található, a kártékony kód által összegyűjtött személyes adatokat. A megszerzett adatok között akár jelszavak, címjegyzékek, banki azonosító adatok is lehetnek.

Az első gyanús jel, hogy a linkek domain nevei nem hasonlítanak egyik létező csomagküldő szolgálat webcíméhez sem, bár van, amelyikben szerepel a „track”, azaz nyomkövetés szó. Látszólag ahány SMS, annyiféle weboldalra mutatnak a linkek.
További, adathalász próbálkozásokra jellemző intő jeleket is felismerhetünk, mint például a gyenge helyesírás, a hiányzó ékezetek, az idegen domain név és a kattintható link küldése, melyek mind ott szerepelnek a bűnözők eszköztárában.



Mit tegyünk, ha ilyen SMS-t kapunk?
A tapasztalatok eddig azt mutatják, hogy az SMS megnyitása önmagában nem veszélyes. Több esetben a link megnyitásakor maga a Chrome böngésző figyelmeztet, hogy az adott weboldalt már többen is gyanúsnak jelentették. Emellett a legbiztosabban a naprakész vírusvédelmi programok fogják meg ezeket a próbálkozásokat.
Az ESET Mobile Security program például "Android/TrojanDropper.Agent.HNJ" néven azonosított és blokkolt egy olyan fedex.apk nevű alkalmazást, amelyet egy ilyen gyanús linkről letöltöttek.

Ha már letöltöttük és telepítettük a kártékony alkalmazást, akkor a gyári állapotra való visszaállítás jelenthet biztos megoldást.

Ezt azonban csak végszükség esetén érdemes alkalmazni, ugyanis ezzel a módszerrel minden adatunk és fájlunk törlődik a telefonról. Érdemes első lépésben letöltenünk egy ismert, megbízható vírusvédelmi programot, és egy teljes ellenőrzést futtatnunk az eszközön.

Fontos megjegyezni, hogy egyik módszer sem képes arra, hogy a már ellopott, illetéktelen kezekbe került adatainkat visszahozza, így érdemes lehet a bankunkat is értesíteni a történtekről.

Miért esünk könnyen áldozatul az SMS csalásoknak?

Van valami, amiben a csalók nagyon ügyesek – mégpedig a manipulációban. Emellett folyamatosan fejlesztik a trükkjeiket, és új módszereket próbálnak ki annak érdekében, hogy rávegyék az embereket arra, hogy megtegyenek valamit, amit lehet, hogy amúgy kétszer meggondolnának. Az e-mailben történő adathalászatról szerencsére egyre több szó esik, így ezeket a próbálkozásokat már egyre nagyobb eséllyel szűrik ki sikeresen a felhasználók, az SMS adathalászatról („smishing") azonban viszonylag keveset hallhattunk mostanáig.

Az e-mailekkel ellentétben az SMS esetében csak egy telefonszámot látunk, nincs feladó cím, amit ellenőrizhetnénk. Ráadásul némelyikük képes észrevétlenül beilleszteni magát egy korábbi, valódi csevegés-folyamba. Ahogy egyre gyakrabban élünk az online rendelés és házhozszállítás lehetőségével, a különböző értesítések gyakran egy végtelen értesítésfolyammá olvadhatnak össze, amit gyanútlanul átfutunk. Ha több csomagot is várunk, akkor még kisebb az esélye, hogy feltűnik, ha hamis értesítést kapunk. Sőt, még ha nem is várunk éppen semmilyen küldeményt, akkor is felülkerekedhet rajtuk a kíváncsiság, és úgy érezzük, rá kell kattintanunk a linkre, hogy kiderítsük, milyen csomagról van szó.

Mire figyeljünk a telefonunk biztonsága érdekében?

A mai okostelefonok tulajdonképpen apró számítógépek, tele személyes adatokkal, fontos fájlokkal – gondoljuk csak az e-mail fiókunkra vagy a netbank alkalmazásokra.

Ugyanúgy megfertőződhetnek vírusokkal és más kártevőkkel, mint a laptopjaink, asztali gépeink, ezért Android rendszereken elengedhetetlen tehát a naprakész vírusvédelem, illetve az alkalmazások és az operációs rendszer biztonsági frissítéseinek mihamarabbi telepítése. Emellett kulcsfontosságú kérdés, hogy honnan és milyen programokat telepítünk.

Normál helyzetben érdemes ragaszkodni a hivatalos Google Play áruházhoz, és blokkolni minden egyéb külső forrásból származó program telepítését (egyébként ez az alapértelmezett állapot, hacsak át nem állítjuk).

A szakemberek felhívják a figyelmet arra is, hogy biztonságtudatos, óvatos hozzáállással is sokat tehetünk az eszközeink és adataink védelméért. Mindig figyelmesen járjunk el az üzenetekkel, és azonnal gyanakodjunk, ha olyan forrásból kapunk értesítést, ahol nem vagyunk ügyfelek, vagy nem is várunk küldeményt.
Várhatóan a csalók továbbra is egyre gyakrabban és egyre kreatívabb módszerekkel fognak próbálkozni, ezért nagyon fontos, hogy tudatában legyünk a technikáiknak, és tudatosan védekezzünk ellenük.

A bűnözők célja, hogy rávegyenek minket a gyors, meggondolatlan cselekvésre, mielőtt még az agyunk lassabb, racionálisabb fele közbeléphetne - ne hagyjuk nekik!

A mostani, Android rendszerek elleni, banki adatok megszerzésére irányuló incidens ismételten ráirányítja a figyelmet, hogy ma már ezen a platformon is ugyanolyan nélkülözhetetlen biztonsági elem a vírusvédelmi alkalmazás, mint a Windows és a többi rendszereken – így sok kellemetlen meglepetéstől kímélhetjük meg magunkat.

A Sicontact Kft.-ről röviden:

A Sicontact Kft. hazánkban az egyik legjelentősebb **IT biztonsággal foglalkozó** cég, az ESET termékek kizárólagos magyarországi forgalmazója. Mottója és küldetése, ami köré termékportfolióját kialakította: „**biztonság a digitális világban**". A Sicontact Kft. Magyarországon az **ESET NOD32** technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő. A cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact Kft. több ízben elny erte a kitüntető **Business Superbrands** díjat. Az ESET Smart Security programcsomagot többször is **az év antivírus megoldásának** választották.

A független tesztelő szervezet több díjjal is elismerte az otthoni ESET termékeket a 2019-es eredményeket összefoglaló riportjában:

- Arany díjat nyert a fejlett, célzott és fájlnélküli kártevő támadások kivédésében, amely új kategóriaként jelent meg 2019-ben. Az ESET volt azon két gyártó egyike, akik mind a 15 célzott támadást sikeresen blokkolták a tesztelés során.

- 2018-ban ezüst, majd 2019-ben arany díjat szerzett a rendszer gyorsaságára és teljesítményére gyakorolt hatást vizsgáló kategóriában, az ESET szoftverek alacsony erőforrásigényének köszönhetően.

- Bronz díjat nyertek el a téves riasztások kategóriájában, amelyek ugyanúgy gondot okozhatnak, mint egy valós fertőzés, ezért az elkerülésük kulcsfontosságú a biztonsági szoftvereknél.

A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban, magyar nyelvű terméktámogatással kínálja. Az ESET már több mint 25 éve biztosít védelmet a digitális világ fenyegetéseivel szemben. Egy kicsi és dinamikus vállalatból mára egy több mint 100 millió felhasználót számláló és 202 országot és területet lefedő globális márkává nőtte ki magát.

Rengeteg minden változott, de az alapvető törekvéseik és a hozzáállásuk változatlan maradt, továbbra is céljuk egy biztonságosabb digitális világ felépítése, amelyben mindenki élvezheti a biztonságos technológia előnyeit.

További információ és interjúegyeztetés:

Terdik Adrienne | **Ügyvezető igazgató** | **PResston PR** | **Rózsadomb Center** | **1025 Budapest** | **Törökvész u. 87-91.** | **T + 36 1 325 94 88** | **F +36 1 325 94 89** | **M +36 30 257 60 08** | adrienne.terdik@presstonpr.hu | **www.presstonpr.hu**

Szekeres Nikoletta | **PR vezető** | **PResston PR** | **Rózsadomb Center** | **1025 Budapest** | **Törökvész u. 87-91.** | **T + 36 1 325 94 88** | **F +36 1 325 94 89** | **M +36 30 831 64 56** | nikoletta.szekeres@presstonpr.hu | www.presstonpr.hu