TLP: WHITE
Szabadon terjeszthető!

Riasztás
Csomagküldő szolgáltatók nevével visszaélő, káros kód terjesztéssel összefüggő SMS üzenetekkel kapcsolatban

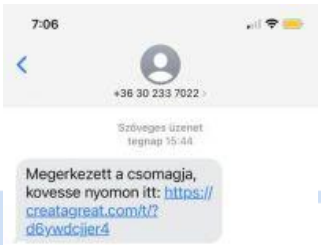
(2021. március 24.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztás**t ad ki a megnövekedett számú, **kéretlen szöveges üzenetek útján terjedő, látszólag csomagküldő szolgáltatóktól érkező, káros hivatkozást tartalmazó SMS üzenetekkel kapcsolatban**. A jelenleg rendelkezésre álló adatok alapján az SMS üzentekben, be nem fizetett szállítási díj vonatkozásában próbálnak meg pénzt, illetve adatokat megszerezni, valamint egyes esetekben Android operációs rendszerű eszközökre veszélyes **káros kód** letöltést végrehajtatni a felhasználóval.

Az SMS üzenetek főbb jellemzői

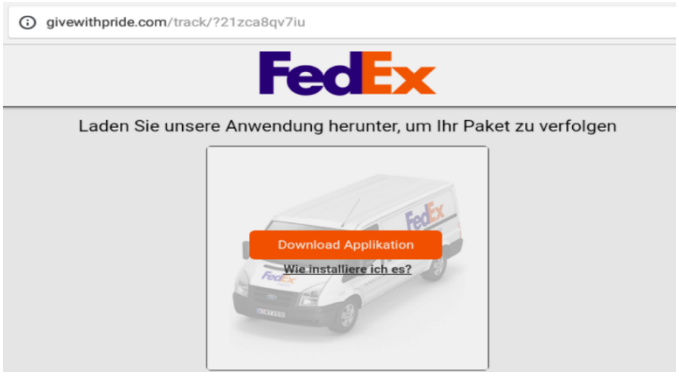
- A csaló üzenetet küldők a legtöbb esetben az SMS törzsében elhelyezett **hivatkozás megnyitására** igyekeznek rávenni a címzettet, például egy küldemény nyomon követésére **hivatkozva**.
- Egy ilyen üzenet tartalma: „**Megérkezett a csomagja, kovesse nyomon itt**: https://(valtozó hivatkozás)” (lásd: *1. ábra*)
- Az eddigi adatok alapján minden esetben magyar mobilszolgáltató hálózatából érkeztek az üzenetek. Fontos kiemelni, hogy az SMS-ekben szereplő URL-ek dinamikusan változnak.



A támadás menete

- Amennyiben az áldozat megnyitja az üzenetben kapott hivatkozást, egy csaló weboldal jelenik meg, amely sok esetben rendkívül jól **utánozza** a megszemélyesített cég valódi bejelentkezési felületét ─ például logók, színek, tipográfiai jellemzők ─ felhasználásával. A mostani esetek során legtöbbször a **FedEx** került megszemélyesítésre *(lásd: 2. ábra)*.

1. ábra: Példa káros hivatkozást tartalmazó üzenetre



2. ábra: A Fedex-et megszemélyesítő káros weboldal

- Ezek a káros oldalak egy **alkalmazás telepítésére** próbálják rávenni az áldozatot ─ a megtévesztés szerint a csomagküldemény nyomon követéséhez.
- Azonban ha a felhasználó letölti a feltételezett alkalmazást az eszközre, egy adatlopó képességekkel felruházott **Trójai vírus kerül telepítésre**. A vírus telepítése után majdnem minden szolgáltatáshoz hozzátudnak férni, mint például: SMS, MMS írás, küldés, Internet, Bluetooth, NFC, telefonkönyv stb..

Fertőzés esetén az NBSZ NKI javasolja, hogy az érintett eszközön haladéktalanul végezzenek el egy gyári visszaállítást.

Az NBSZ NKI javaslatai a káros tevékenységet végző SMS üzenetek kezelésével kapcsolatban:

- Soha **ne kattintson** az üzenetben levő applikáció letöltés **hivatkozásra**!
- Amennyiben az SMS üzenetben található **káros hivatkozás megnyitásra került**, haladéktalanul **értesítse az intézmény informatikai területét**!
- Minden esetben külön **keressen rá** az adott cég, vagy szervezet **hivatalos weboldalára**, és ott bejelentkezve **ellenőrizze** a kapott üzenet valóságtartalmát!
- **Incidens bejelentése az NBSZ NKI részére** a csirt@nki.gov.hu e-mail címen vagy az nki.gov.hu weboldalon keresztül, melyek során a feladó telefonszáma, valamint a szöveges üzenetben található hivatkozás is kerüljön rögzítésre.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu