TLP: WHITE
Szabadon terjeszthető!

Rendkívüli tájékoztató
Káros csatolmányú e-mail üzenetekkel kapcsolatban

(2021. szeptember 06.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **rendkívüli tájékoztató**t ad ki digitális **COVID-igazolványra hivatkozó, káros csatolmányt tartalmazó,** kéretlen elektronikus **levelekkel kapcsolatban**.

Intézetünkhöz több bejelentés érkezett olyan **trójai vírust terjesztő e-mailek** vonatkozásában, amelyek az Európai Unió által kiadott digitális Covid-igazolványra hivatkozva kísérlik meg a felhasználók megtévesztését.

A megtévesztő levelek tartalma szerint a címzett részére COVID-19 elleni védőoltás felvétele miatt európai uniós „**digitális Covid bizonyítvány**” került kiállításra, ami a levél csatolmányában található. *(lásd: 1. ábra).*

Figyelem! A levél melléklete vírusos állományt tartalmaz, semmiképp se nyissa meg azt!


Tisztelt Hölgyem / Uram!

Gratulálunk! Nyilvántartásunk szerint Ön bevette a covid-19 elleni védőoltását, és csatoltuk az Európai Unió digitális Covid-bizonyítványát. A mellékelt bizonyítvány más néven oltási/immunity tanúsítvány.
Ez az oltás bizonyítéka, tartalmaz egy QR -kódot, amely a tulajdonos (Ön) oltással, PCR -tesztekkel és Covid -helyreállítással kapcsolatos információihoz kapcsolódik. A COVID-19 elleni védőoltást kapott magyar állampolgárok, akik rendelkeznek ezzel a tanúsítvánnyal, tesztelési és karanténkötelezettség nélkül utazhatnak az EU-országok között.

Gratulálunk!! A bizonyítványról itt olvashat bővebben

Ügyfélkapu

Üdvözlettel:
Dr. Janoczkó Márton
háziorvos

1. Ábra: Példa a káros hivatkozást tartalmazó levélre

Az eddigi esetek alapján a levelek **látszólag a covid.bizonyitvany@ugyfelkapu.gov.hu** e-mail címről érkeznek, a levél tárgya pedig a „**Covid vakcina digitális tanúsítvány**”.

A levélben szereplő tömörített fájlban a *Lokibot* nevű **trójai vírus** egyik variánsa található. Az ilyen típusú kártevők elsődlegesen **információgyűjtő kémprogramok**, amelyek ─ többek között ─ a billentyűleütések figyelésére is képesek, ezáltal érzékeny adatok (például jelszavak) megszerzésére is alkalmasak.

Az NBSZ NKI javaslatai az ilyen és ehhez hasonló káros csatolmányú e-mailek kezelésével kapcsolatban:

- Soha **ne kattintson** az olyan e-mailben vagy SMS üzenetben érkező **hivatkozásokra**, amelyek ismeretlen állományok letöltését vagy bejelentkezési, személyes, egyéb adatok megadását kérik!
- Minden esetben külön **keressen rá** az érintett cég, vagy szervezet **hivatalos weboldalára**, és ott bejelentkezve **ellenőrizze** a kapott üzenet valódiságát!
- Az **üzenet valóságtartalmáról** az érintett cég, vagy szervezet **hivatalos tájékoztató felületein** elérhető kapcsolati adatokon keresztül is meggyőződhet.
- Előfordulhat, hogy az adathalász üzenetek csatolmányt is tartalmaznak (pl. egy Microsoft **Word dokumentum**, egy **tömörített, .iso** vagy **.pdf** kiterjesztésű fájlt). Ezeket **ne nyissa meg**, és **ne töltse le**!
- Amennyiben **adathalászatra utaló esemény**t tapasztal vagy azzal összefüggésben csalás áldozatává vált, haladéktalanul **tegyen bejelentést** a **csirt@nki.gov.hu** e-mail címen, vagy az **nki.gov.hu** weboldalon keresztül.
- Tekintse meg az NBSZ NKI "**E-mailed jött? Gondolkodj, mielőtt kattintasz!**" című tudatosító infografikáját az adathalászat felismeréséről.

IoC:

- Covid oltási bizonyítvány·PDF.zip
  - md5: 1632e24ac480bcfc9a97425f7a34ed83
  - sha256: 547f10cb9baa18d68fdbc548c2ed137f5337cda481935853e90a2da750a67d86
- Covid oltasi bizonyitvany PDF.exe
  - sha256: 257513a74ef01224b6b44fd5ee3067d27c3177c8363f8b49f0e4353b12452ced
- C2 szerver
  - 185.227.139[.]5
- HTTP/HTTPS kérés
  - hxxp[://]185[.]227[.]139[.]5/sxisodifntose[.]php/S7zr5v1fXI3Rb

Hivatkozások:

- https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/adathalaszat-legjobb-vedekezes-a-megelozes/
- https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/e-mailed-jott-gondolkodj-mielott-kattintasz/

Nemzetbiztonsági Szakszolgálat

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