TLP: WHITE
Szabadon terjeszthető!

Tájékoztatás
a Semmelweis Egyetem nevével és arculati elemeivel visszaélő, káros csatolmányt tartalmazó levelekkel kapcsolatban

(2022. szeptember 21.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatást ad ki a Semmelweis Egyetem nevével és arculati elemeivel visszaélő, káros csatolmányt tartalmazó **csaló levelekkel** kapcsolatban.

Az Intézetünknél tett eddigi bejelentések alapján a kampányban küldött hamis levelek

- látszólag **Dr. Arató Andrástól** érkeznek,
- megfogalmazásuk magyartalan és több nyelvtani hibát is tartalmaz,
- a levél csatolmányában egy pdf fájl (**Ajánlatkérés szám222109_10397.pdf**) található, amelyen keresztül egy trójai típusú káros kód (AveMaria) töltődhet le az áldozat eszközére.

Feladó: arato.andras©med.semmelweis-univ.hu <copy@ivet.bg>
Elküldve: 2022. szeptember 21. 4:21
Tárgy: Ajánlatkérés, szám: 222109-10397

kedves, Üdvözlet a Semmelweis Egyetemről,

Semmelweis Egyetem vagyunk. Van egy költségvetésünk, amelyet magyar kormányunk Belügyminisztériuma társfinanszíroz. Ehhez a költségvetéshez árajánlatra van szükségünk. Kérjük, 2022. szeptember 27-ig nyújtsa be ajánlatát. Keresse meg a mellékletet, és tudassa velünk, ha további információra van szüksége.

Köszönöm és minden jót.

DR. ARATÓ ANDRÁS
EGYETEMI TANÁR, IGAZGATÓHELYETTES

SEMMELWEIS EGYETEM
I. SZ. GYERMEKKLINIKA
1083. Budapest, Bókay János utca 53.
+36 20 913 2817
arato.andras@med.semmelweis-univ.hu

1. ábra: példa a Semmelweis Egyetemet megszemélyesítő csaló levélre

A káros csatolmányú levelek kiszűrése érdekében a Nemzeti Kibervédelmi Intézet az alább indikátorok tiltását / szűrését javasolja:

Ip: 172[.]245[.]120[.]8

Url: hXXp[:]//172.245.120.8/Aj%C3%A1nlatk%C3%A9r%C3%A9s%20sz

Csatolt PDF állomány:

Ajánlatkérés szám222109_10397.pdf

sha256: 5b43708f821bee8a5341bbabef6e1a6c44f6e165c2c4bf64b3a810e92ac8e9dc

További állományok:

Ajánlatkérés szám222109·10397·pdf.zip

sha256: 1dfcccdd32ed323bbe2749f317ce31dc0b9ae06c8972558d76b46df0b437d30e

Ajanlatkeres szam221909·10397·pdf.exe

sha256: aeb049faf805c590ca7125f2eae56483200815aa964b7cb9677d4a5d63b1bcd1

A fenti indikátorok szűrésén túl javasolt a fogadó oldalon az SPF rekordok ellenőrzésének kikényszerítése. Az SPF beállítások megfelelő alkalmazásával biztosítható, hogy ha olyan szervezet nevében érkezik levél, akinek van beállított SPF rekordja, akkor a fogadó oldali levelezőrendszer azt visszaellenőrizve meg tudja állapítani a feladó valódiságát. Az SPF rekorddal kapcsolatos bővebb információ az NBSZ NKI weboldalán[1] érhetőek el, ahol az elektronikus levelezés biztonsági beállításaival kapcsolatban további javaslatokat talál a Közigazgatási Kibervédelmi Eszköztárban[2].

További hivatkozások:

- [1] https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/spf/
- [2] https://nki.gov.hu/wp-content/uploads/2019/03/NKI_White_Paper.pdf

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu