RIASZTÁS Magyarország Ügyészségének nevével visszaélő ransomware támadásokkal kapcsolatban

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) riasztást ad ki Magyarország Ügyészségének nevével és arculati elemeivel visszaélő, zsarolóvírus fertőzéshez vezető adathalász üzenetekről.

A bejelentések alapján a támadók hamis, hivatalos megkeresés látszatát keltő leveleket küldenek, amelyekben ügyészségi alkalmazottak nevével élnek vissza. A kampány célja az, hogy a felhasználó a levélben szereplő hivatkozásra kattintson, majd a megtévesztő oldalon keresztül rosszindulatú fájlt töltsön le. A fertőzés végső célja a végponton található dokumentumok, képek, archívumok és más állományok titkosítása, majd váltságdíj követelése.

A támadás több lépcsőben zajlik. A címzett egy olyan e-mailt kap, amely hivatalos eljárás megindítására hivatkozik. A feladó minden esetben hamis, valójában egy @outlook.hu címről érkezik. Az Ügyészség a kapcsolattartáshoz @mku.hu címet használ. A levelek tárgya a beérkezett mintákban változatosak, Tájékoztatás a [Cég neve] ügyében rendelkezésre álló büntetőeljárási iratokról vagy hasonló szövegezéssel érkeznek.

Tartalma az alábbi:

Tisztelt [Címzett]!
*Ezúton értesítjük, hogy a [Cégnév] Kft. (adószám: ***, székhely: ***) tekintetében a hatályos magyar jogszabályok alapján büntetőeljárás van folyamatban.*
Az ügyhöz kapcsolódó iratok elektronikus formában az alábbi linken érhetők el:

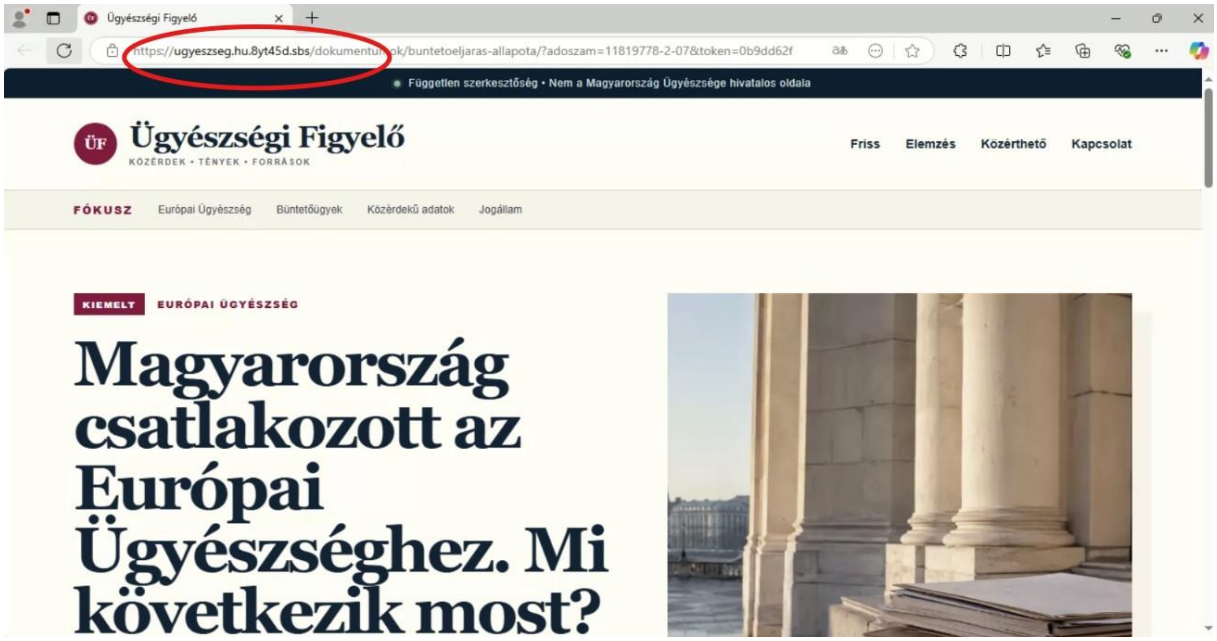
[Az Ügyészség nevével és arculati elemeivel visszaélő google share link]

Kérjük, hogy a fenti hivatkozáson elérhető dokumentumokat megismerni szíveskedjen.
Szükség esetén nyilatkozatát vagy észrevételeit a vonatkozó jogszabályi rendelkezéseknek megfelelően, az előírt határidőn belül nyújthatja be.
Jelen értesítés kizárólag tájékoztatásul szolgál.

NEMZETI KIBERBIZTONSÁGI INTÉZET
+36-1-336-4833 csirt@nki.gov.hu

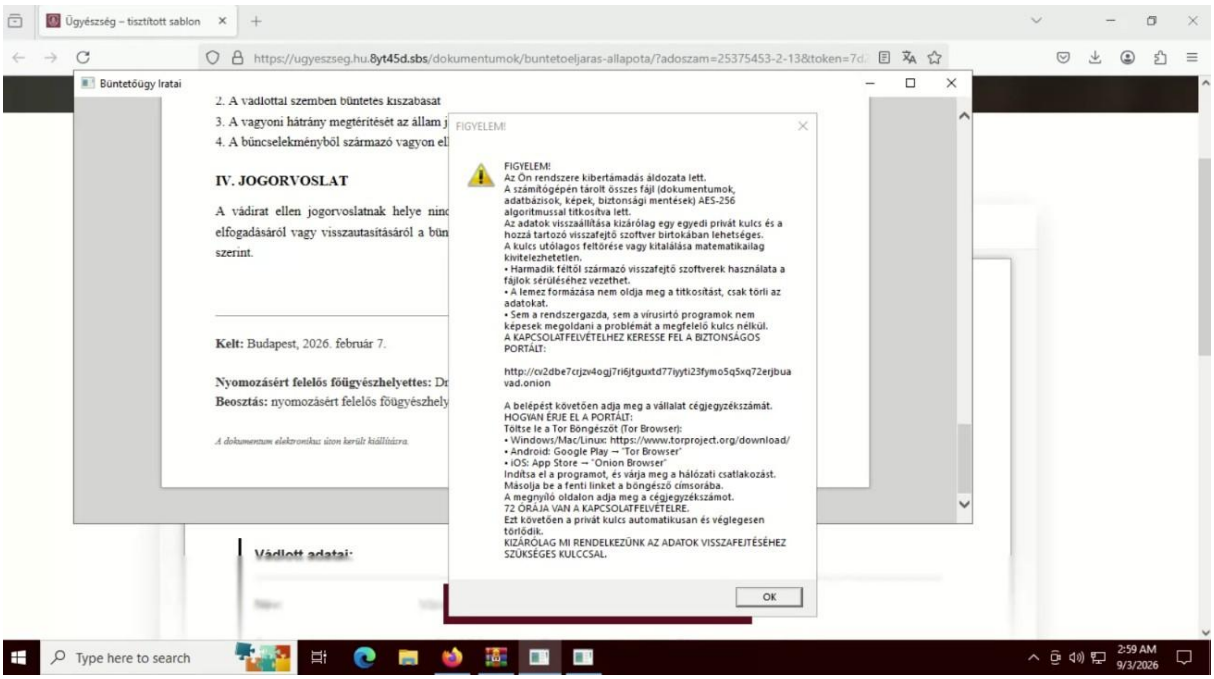
Tisztelettel:
xy
Magyar Ügyészség

A levél egy olyan google share linket tartalmaz, amely átirányít egy első ránézésre hivatalos oldalra hasonló, valójában azonban megtévesztő domainre. A böngésző címsorában egy ugyeszseg.hu kezdetű, azonban hamisított link látszik.



1. ábra A hamis oldal és a megtévesztő domain

Ezen az oldalon a címzettet további kattintásra ösztönzik, amelynek eredményeként elindul a zárolás. A zsarolóprogram a titkosítás megkezdése után a fájlnevek elé „ZÁROLT_” előtagot helyez, miközben a fájl kiterjesztése változatlan maradhat. A megjelenített üzenet szerint a támadók .onion oldalt adnak meg a kapcsolatfelvételhez, és azt állítják, hogy kizárólag ők képesek a fájlok visszaállítására.



2. ábra A zsaroló levél

Felismerési pontok:

- Az ügyészség hivatalos e-mail címeinek végződése: @mku.hu. @outlook.hu-s vagy más e-mail címről nem érkezhet az Ügyészségtől levél.
- Az üzenetben szereplő link látszólag hasonlíthat egy hivatalos oldalra, ténylegesen azonban megtévesztő domainre mutat.
- A hivatkozás megnyitása után további kattintásra, dokumentum megtekintésére vagy letöltésre próbálják rávenni a felhasználót.

Javasolt intézkedések:

- Ne kattintsunk az ilyen levelekben szereplő hivatkozásokra!
- Mindig ellenőrizzük a weboldal címét a böngésző címsorában!
- Ne töltsünk le és ne futtassunk a levélből, illetve az abban szereplő oldalról elérhető fájlt.

- Mindig ellenőrizzük a feladó valódi elnevezését, vezetőjének nevét, e-mail címét.
- Az ügyészség honlapján ezek az adatok naprakészen megtalálhatók: www.ugyeszseg.hu/elerhetosegek/ugyeszsegek
- Ha az ellenőrzés sem ad egyértelmű választ, akkor érdemes az ügyészség tényleges elérhetőségein rákérdezni arra, hogy tőlük érkezett-e az e-mail.
- Amennyiben a felhasználó a linkre kattintott vagy futtatható állományt indított el, az érintett eszközt haladéktalanul le kell választani a hálózatról.
- Javasolt a kapcsolódó levelezési naplók, proxy-naplók, végponti események és letöltési előzmények azonnali vizsgálata.
- A fertőzött vagy gyanús rendszer újraindítása, illetve további használata előtt javasolt az incidenskezelési eljárás megindítása és a bizonyítékok megőrzése.

Eddig ismert, tiltandó indikátorok:

Domain:

7ny4t[.]com
ugyeszseg[.]hu[.]8yt45d[.]sbs

IP:

195[.]242[.]118[.]139
195[.]242[.]118[.]142

e-mail:

dr[.]brigitta[.]rigo@outlook[.]hu
dr[.]barbara[.]kormos@outlook[.]hu
dr[.]aniko[.]lendvai@outlook[.]hu
dr[.]adrienn[.]csizmadia@outlook[.]hu
dr[.]almos[.]hegyi@outlook[.]hu
dr[.]tamara[.]vakulya@outlook[.]hu

Ransomware:

8165fc45.enc
MD5 09F51C860B370FC6D6BA35D1A4CF5C74
SHA1 6B6F138DA1907A65854650E7EC5DFB038565B26F
SHA256
7563E58E395E367083D52E8B406CD68BE69C0A3A217CA760E91F7345D27A4AF4

A legfrissebb információkért kérjük ügyfeleinket, hogy folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.

+36-1-336-4833 csirt@nki.gov.hu