

TLP: CLEAR

Szabadon terjeszthető!

RIASZTÁS A MAGYAR ÜGYÉSZSÉG 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 elsődlegesen 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 levelek "Tájékoztatás a [Cég neve] Kft.-vel kapcsolatos eljárási dokumentumokról" tárgyban érkeznek, és az alábbi tartalommal:

Tisztelt [Címzett]!

Ezúton értesítjük, hogy a [Cégnév] Kft. (adószám: ***, székhely: ***) tekintetében a hatályos magyar jogszabályok alapján büntetőeljárás van folyamatban.

Az ügghöz kapcsolódó iratok elektronikus formában az alábbi linken érhetők el:

[Ransomware letöltési linkje]

Kérjük, hogy a fenti hivatkozáson elérhető dokumentumokat megismerni szíveskedjen.

Amennyiben az ügyben nyilatkozatot kíván tenni, illetve észrevételt kíván előterjeszteni, azt a vonatkozó jogszabályi rendelkezések szerint, a meghatározott határidőn belül teheti meg.

Jelen értesítés kizárólag tájékoztatásul szolgál.

Tisztelettel:

xy

Magyar Ügyészség

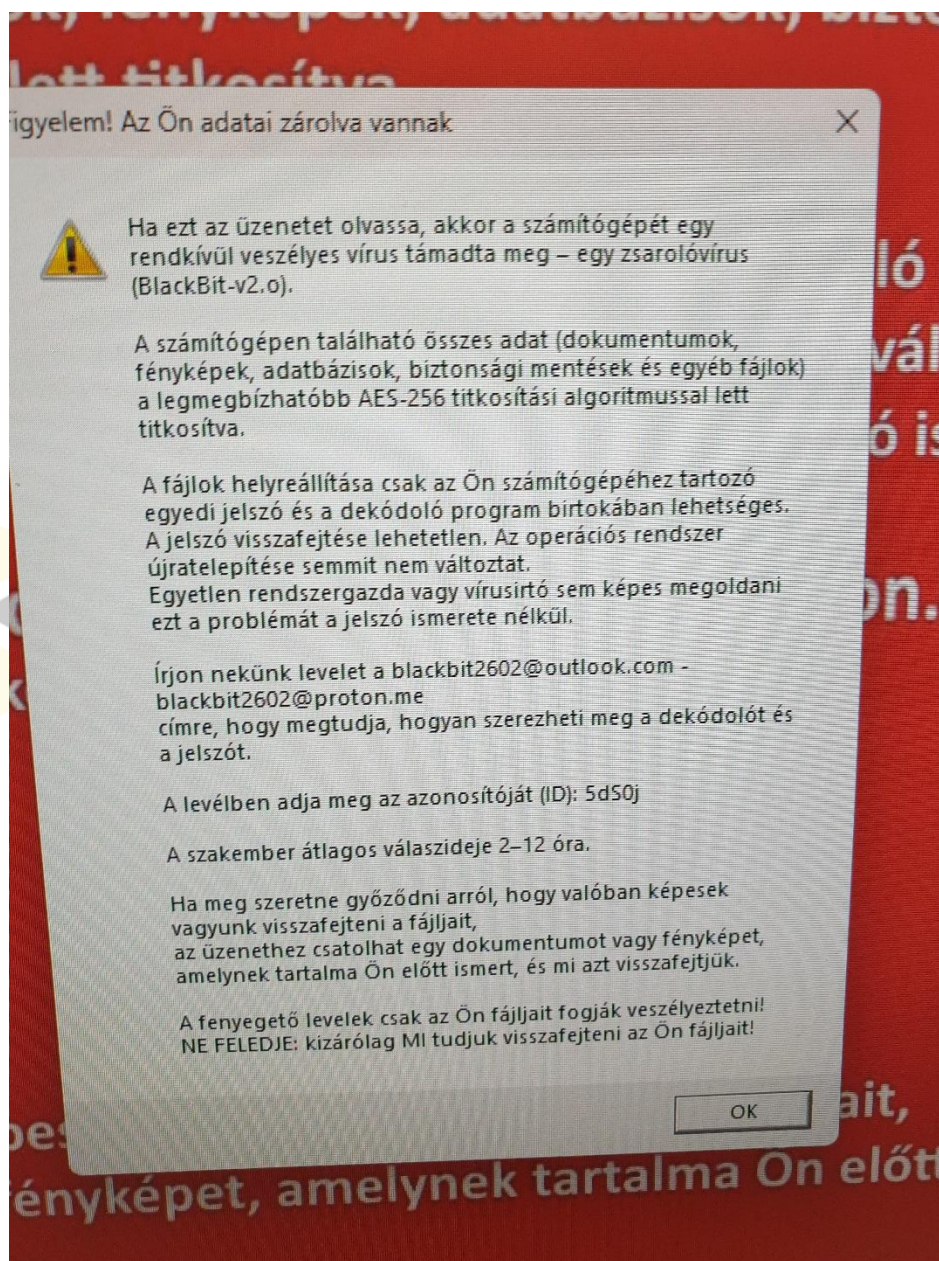
A levél egy olyan linket tartalmaz, amely első ránézésre hivatalos oldalra mutatónak tűnhet, valójában azonban megtévesztő domainre vezet. Ezen az oldalon a címzettet további kattintásra ösztönzik, amelynek eredményeként elindul a zárolás. A zsarolóprogram a titkosítás megkezdése után a fájlnevek elé „ZÁROLT_” előtagot helyez, miközben a fájl kiterjesztése változatlan maradhat. A fertőzéshez kapcsolódó váltságdíj üzenet magyar nyelven jelenik meg, és több esetben a „BlackBit-v2.0” megnevezés szerepel benne.

TLP: CLEAR

TLP: CLEAR

Szabadon terjeszhető!

A megjelenített üzenet szerint a **támadók e-mailes kapcsolatfelvételt kérnek**, és azt állítják, hogy kizárólag ők képesek a fájlok visszaállítására.



1. ábra A ransomnote szövegezése

Felismerési pontok

- Az ügyészség hivatalos e-mail címeinek végződése: **@mku.hu**. Gmail-es vagy más e-mail címről **nem** érkezik az **Ügyészségtől** levél.

TLP: CLEAR

TLP: CLEAR

Szabadon terjeszthető!

- Az üzenetben szereplő link látszólag hasonlíthat egy hivatalos oldalra, ténylegesen azonban **mejtévesztő 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.

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833

TLP: CLEAR