

TLP: WHITE
Szabadon terjeszthető!

Tájékoztatás

az Országos Rendőr-főkapitányság nevével visszaélő, káros csatolmányt tartalmazó levéllel kapcsolatban
(2020. március 30.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatót ad ki az **Országos Rendőr-főkapitányság nevével visszaélő, káros csatolmányt tartalmazó levéllel kapcsolatban.**

Feladó: Rendőrség <meghivas@police.hu>
Dátum: 2020. március 30., hétfő 10:08
Címzett: [REDACTED]
Tárgy: Rendőrségi meghívó értesítés



Üdvözlét,
Reméljük, hogy jóhiszeműen elfogadja ezt a levelet.

Meghívjuk Önt a rendőrség központjába folyamatos nyomozás céljából.

Kérjük, olvassa el a mellékelt dokumentumokat, és ha szükséges, vegye fel a kapcsolatot ügyvédjével.

Dátum: 2020. április 1
Idő: 11:00

Üdvözlettel,
Dr. Balogh János


ORSZÁGOS RENDŐR-FŐKAPITÁNYSÁG

Cím: 1199 Budapest, Tere utca 4-6.

Posta cím: 1803 Budapest, Pf. 314.

Telefon: 1/442-8800

Fax: 1/443-5733

BM telefon: 33-104, 33-140

BM fax: 33-133

Intézetünk számos bejelentést kapott az Országos Rendőr-főkapitányság nevében kiküldött, káros csatolmányt tartalmazó levéllel kapcsolatban. A levél egy **pdf.iso** megnevezésű csatolmányt tartalmaz, ami valójában egy tömörített, futtatható (exe) fájl. A csatolmány megnyitásával egy Trójai program (Trojan:Win32/Wacatac.C!ml) települ fel a felhasználó számítógépére.

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



E-mail feladójának IP címe / domain:

95.110.200[.]162 / alicomitalia[.]it

Káros csatolmánnyal kapcsolatos indikátorok:

MD5: eaf9064591fbc41ea4f761c0fb0bd5c1

SHA256: 5a36ac00bd4da98cda282ce51a3ecc070a5e37c03154f415016b64735be11a8b

Command-and-control szerver IP: 172.111.188[.]199

A fenti indikátorok szűrésén túl javasolt továbbá 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. SPF rekorddal kapcsolatos információ a <https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/spf/> oldalon található. Az elektronikus levelezés biztonsági beállításaiával kapcsolatban további javaslatok a [Közigazgatási Kibervédelmi Eszköztárban](#) találhatóak.

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