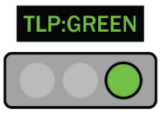
Malware Analyzer Sandbox

GYORSHAJTÁSI BÍRSÁG CSALÓ SMS

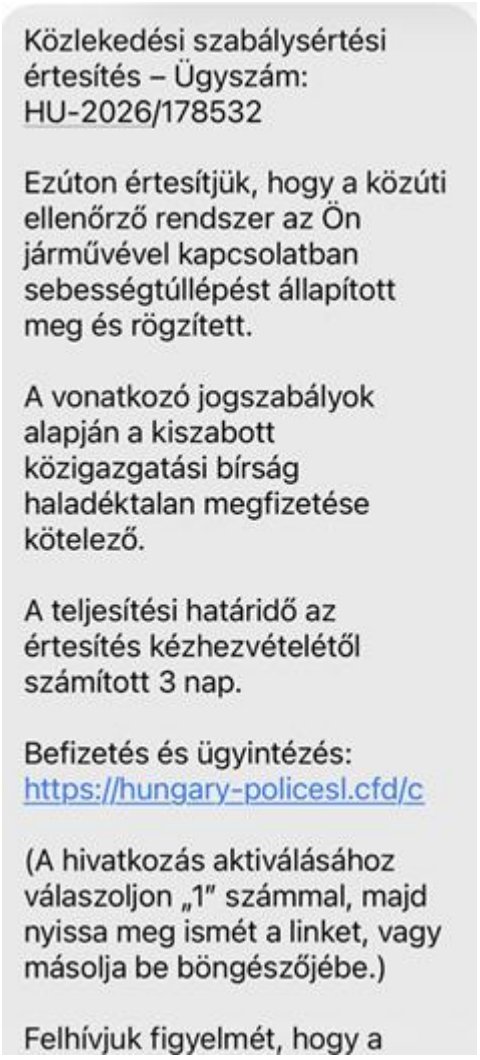
TÁJÉKOZTATÓ



NEMZETI
KIBERBIZTONSÁGI
INTÉZET

Gyorshajtási bírság adathalász üzenet

Több személy jelezte részünkre, hogy az elmúlt időszakban üzenetküldő alkalmazásba érkezett részére gyorshajtási bírságot színlelő (Gépkocsival nem rendelkező személyek is!), adathalász linket tartalmazó SMS. Az üzenetben a hxxps[://]hungary-policesl[.]cfd/c adathalász hivatkozást (és különböző végződésű variánsait) helyezték el, valamint SMS-ben történő válaszüzenetet vártak.

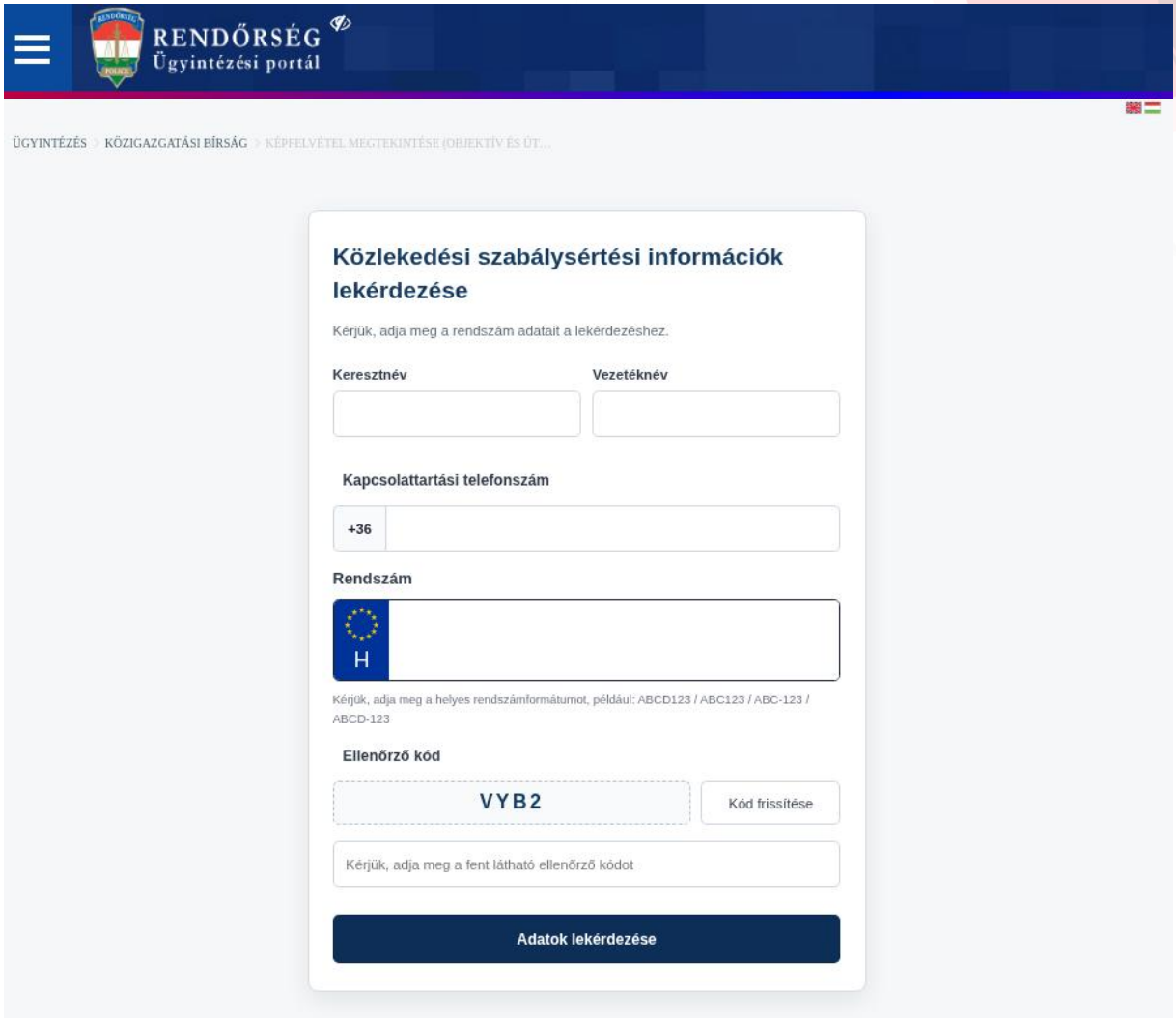


1. ábra Csaló SMS

Az adathalász hivatkozás működése

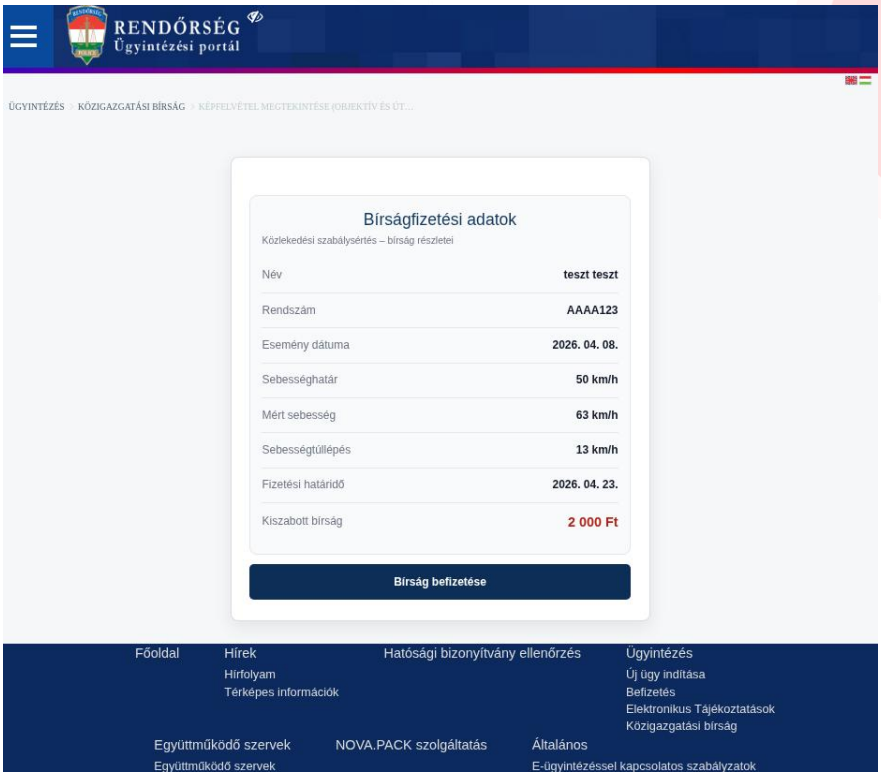
Jellemzően Iphone-t használó személyek kapták meg az üzenetet, és mivel ezeknél a készülékeknél az ismeretlen küldőtől származó hivatkozások alapértelmezetten le vannak tiltva, ezért kérik a „hivatkozás aktiválásához" a válaszüzenetet a csalók. Válaszüzenet küldésekor megbízhatónak tekinti a készülék a feladót, így elérhetővé válik a link megnyitása. Az adathalász link megnyitásakor a felhasználó egy, a **rendőrségi Ügykezelési portál által használt arculati elemeket alkalmazó adatbekérő oldalt** lát, amelyen meg kell adnia a **nevét, a telefonszámát és a gépjármű rendszámát**. Az oldal alján egy ellenőrző mező is helyet

kapott annak érdekében, hogy az oldal leellenőrizze, hogy valós felhasználó próbálja meg kitölteni az adatokat.



2. ábra Adatbekérő felület

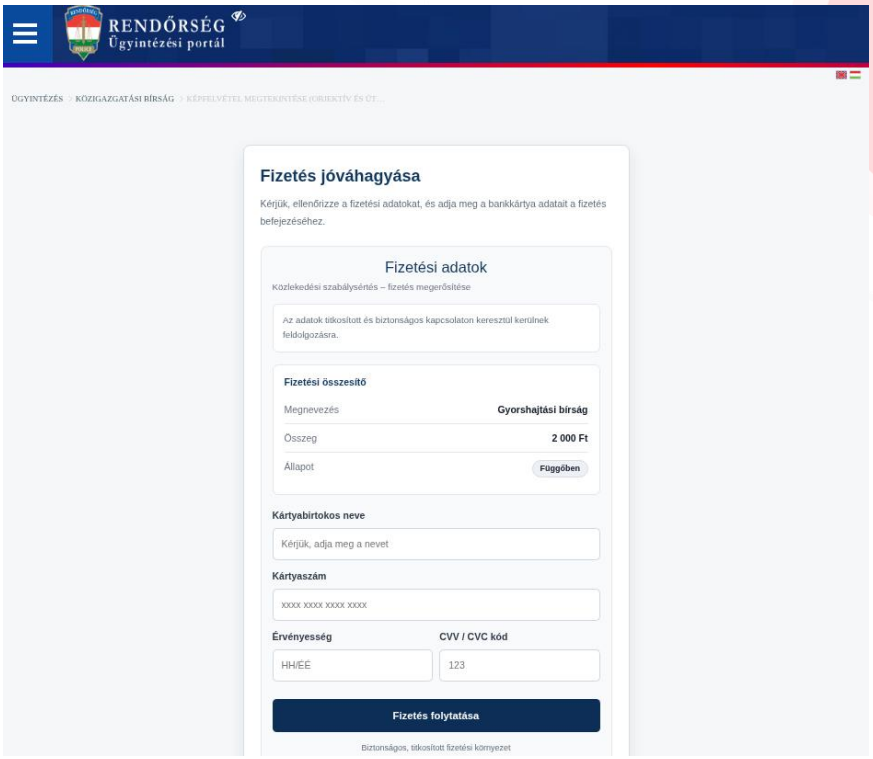
Az ellenőrző kód megadását követően egy ellenőrző felületre továbbít az oldal, ahol a korábban megadott adatokat ellenőrizteti vissza a felhasználóval, illetve tájékoztatja a hamisan generált gyorshajtási információkkal**.**



3. ábra Ellenőrzési felület

Az adathalász weboldal több személyes adat – név, telefonszám – megadását kéri a felhasználóktól. A megadott adatok a háttérben **a csalók által üzemeltetett szerverre kerülnek továbbításra**.

A következő lépésben az oldal **bankkártyaadatok megadását kéri** a felhasználótól, többek között a bankkártyaszám, a lejárati idő, valamint a CVC-kód megadását, a gyorshajtábírságának a megfizetésére hivatkozva.



4. ábra Fizetési oldal

Összefoglaló

Az SMS-ben terjesztett hivatkozás egy, **a Rendőrség nevével visszaélő adathalász weboldalra** irányítja a felhasználókat. Az oldal több lépésben próbál adatokat megszerezni: a felhasználót először egy ellenőrző felületen vezeti át, majd egy, a Rendőrségi Ügykezelési portál által használt arculati elemeket utánzó oldalon **személyes adatok (név, telefonszám)** megadását kéri. A folyamat végén **bankkártyaadatok megadására is felszólít**, egy állítólagos bírság kifizetésére hivatkozva.

Kockázatok

A megadott adatok a támadókhoz kerülhetnek, akik azokat **pénzügyi visszaélésekre, illetve további adathalász vagy csalási kísérletekhez** használhatják fel. Ezért kiemelten fontos, hogy a felhasználók **ne kattintson rá az ilyen SMS-ben található hivatkozásokra, és ne adják meg személyes vagy bankkártyaadataikat ismeretlen weboldalakon**.

Biztonsági javaslatok

- Kerülje az **SMS-ben vagy egyéb üzenetküldő alkalmazásokban** kapott hivatkozások megnyitását.
- **Tiltsa le a feladót**, vagy blokkolja a gyanús fiókot az adott üzenetküldő alkalmazásban.
- Használja a **spamként / kéretlen üzenetként történő jelentés** funkciót, ha az alkalmazás lehetőséget biztosít rá.
- **Ne válaszoljon** az ilyen jellegű üzenetekre!
- Kapcsolja be az **ismeretlen feladók szűrését**, ha az alkalmazás ezt lehetővé teszi.

- Kapcsolja ki az **olvasási visszaigazolások küldését**, ha erre lehetőség van (így a támadó kevesebb visszajelzést kap).
- Amennyiben elérhető, kapcsolja ki a **linkelőnézet automatikus megjelenítését**.
- Ellenőrizze, hogy az Ön által használt fiókoknál (pl. Apple ID, Google-fiók vagy más szolgáltatói fiók) **be van-e kapcsolva a kétfaktoros hitelesítés**.
- Használjon **erős és egyedi jelszavakat** az online fiókokhoz.
- Tartsa **naprakészen a készülék operációs rendszerét és az alkalmazásokat**.
- Amennyiben lehetséges, tiltsa le az **emelt díjas SMS- és mobil tartalomszolgáltatásokat** a mobilszolgáltatónál.
- **Rendszeresen ellenőrizze telefonszámláját** ismeretlen vagy gyanús díjak miatt.