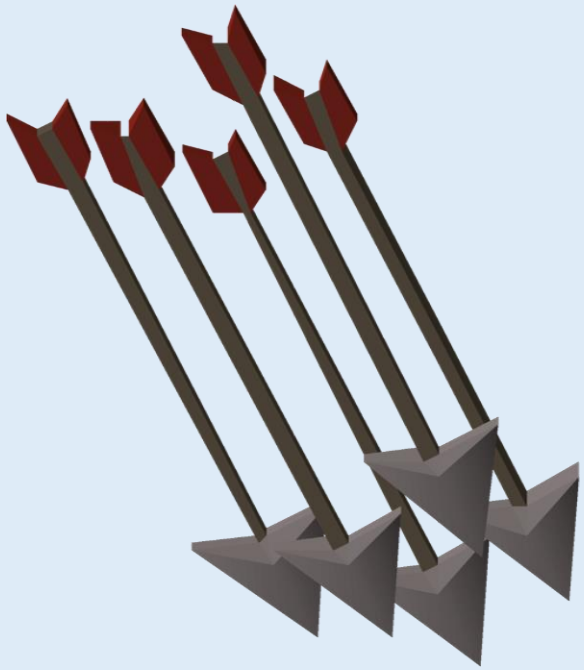
Hírlevél

A Veszprémi Rendőrkapitányság Bűnmegelőzési Melléklete – 2023 3. szám

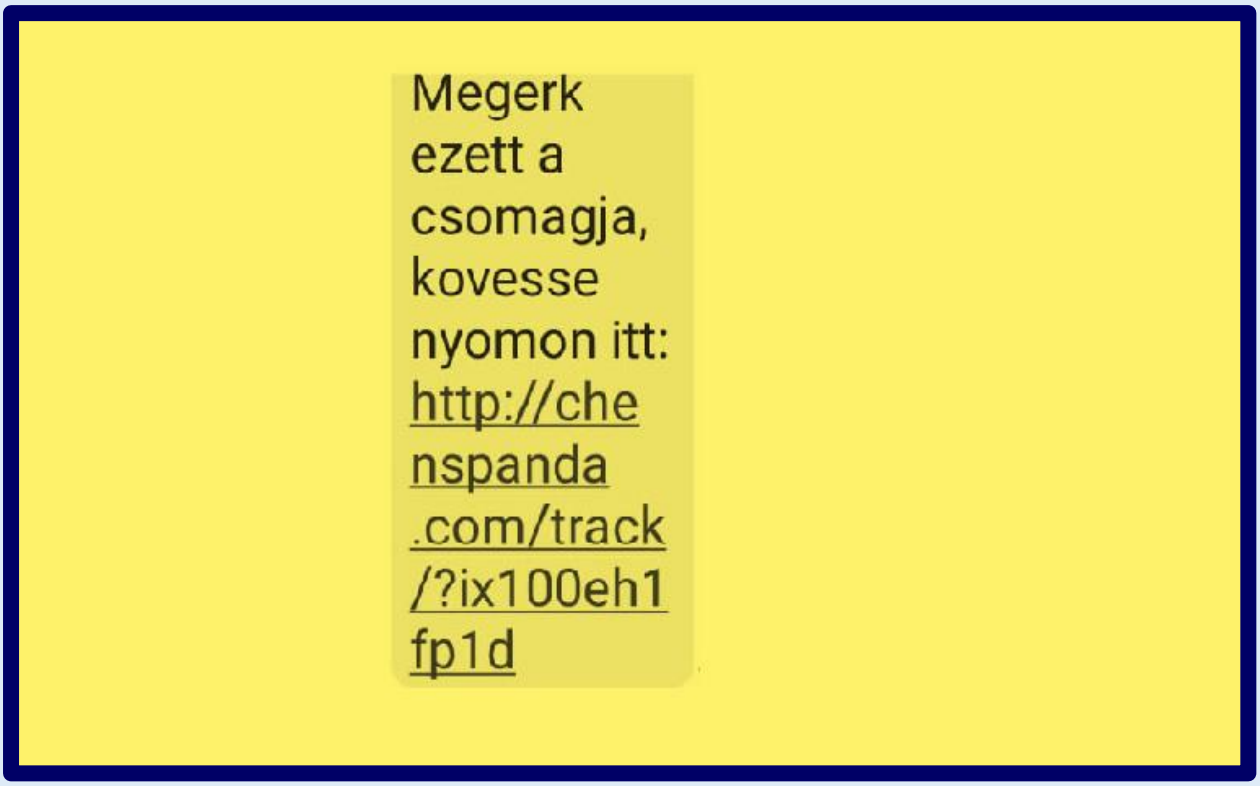
TARTALOM

Folytatjuk az online csalások különféle módszereinek és módszercsoportjainak a bemutatását. Előző számunk témáihoz hasonlóan maradunk továbbra is a tömegesen alkalmazott primitívebb módszereknél, azonban ezúttal azokra térünk rá, amelyek elkövetése során a csalók már nem csapdát állítanak, hanem potenciális áldozatok után kutatva tömegesen küldenek ki e-maileket, esetleg SMS-eket, jellemzően számukra ismeretlen személyeknek. A módszer alapja számos aktív postafiók címének begyűjtése és azok felhasználása. A számítógépről egyetlen gombnyomással, mint a nyílzápor zúdul a címzettekre a csalók üzenete. Hogy mi lehet ezek tartalma, azt a továbbiakban részletezzük.



Postafiókok csellel történő támadása

A potenciális áldozat e-mail címére leggyakrabban hivatalosnak látszó leveleket küldenek a csalók, de az információs csatorna lehet SMS is, ez esetben egy rövid üzenet formájában indul a támadás. Az állítólagos küldő leggyakrabban közüzemi szolgáltató, piacvezető bank, csomagküldő szolgálat vagy streaming szolgáltató. A levél úgy készül, hogy a Google képkeresőjéből megszerzik az adott cég logóját és abból megalkotják a levél fejlécét. A levél tartalma sok esetben fizetési felszólítás, a szolgáltatás felfüggesztésének kilátásba helyezése. Ilyenkor általában egy olyan hátralékra hivatkoznak, ami elég jelentéktelen ahhoz, hogy a címzett késztetést érezzen annak azonnali rendezésére. Ha nagyobb összeget adnának meg, akkor az érintett valószínűleg utánanézne annak, hogy hogyan állhatott elő ez a tartozás és komolyabban belemerülne a témába, ezzel pedig a megtévesztés meghiúsulhatna. A feltüntetett csekély összeg megfizetésére a levélbe beépített linken keresztül van lehetőség. Ez azonban egy csaló honlapra vezet át, ami jól utánozza a hivatkozott cégét, esetleg a sértett bankjának honlapját. A lényeg bakkártya vagy netbanki belépési adatok megszerzése, valós fizetési folyamatként álcázva azt.



A csalók egyszerűbb módon is megszerezhetik az érintett adatait, amennyiben az adott szolgáltató nevében adategyeztetésre hívják fel. Ez az adatok egy bizonyos körében akár indokolható is lehet, mert az ügyfél címe, telefonszáma és e-mail címe nem életre szóló, így azok változását nyilván célszerű a cégnek nyomon követnie. Egyéb adatok megadása viszont már veszélyes lehet.

A banki adatok közül egyedül a bankszámlaszám az, amelynek nyilvánossá válása nem hordoz önmagában kockázatot. Minden más banki adat azonban igen. Nem is életszerű az, hogy az ügyfél számlavezető bankja a bankkártya száma után érdeklődjön, amikor ő maga bocsátotta korábban azt az ügyfél rendelkezésére. Ezek az adathalász kísérletek azonban sokszor azért lehetnek sikeresek, mert a sértettek sietnek, és nem gondolják végig, nem értékelik azt a szituációt amibe kerültek, hanem mindezt mellőzve azonnal és automatikusan cselekednek. A megtévesztés pedig gyakran azért is lehet sikeres, mert az adathalászatot általában valami másnak (pl. bankkártyás fizetési folyamatnak) álcázzák a csalók. Ez esetben a sértett a kellő körültekintést azért mulasztja el, mert teljes tévedésben van azzal kapcsolatban, amit éppen végeztetnek vele. E bűncselekmények megelőzését leginkább az szolgálja, ha a potenciális áldozatok általában is tájékozottak, figyelemmel kísérik az online csalásokkal kapcsolatos híradásokat, ismerik a leggyakrabban alkalmazott módszereket.

Postafiókok támadása zsarolással

Az interneten szörfözve megszoktuk már, hogy gyakran korábbi böngészéseink tárgyaival, érdeklődési körünkkel összhangban álló hirdetésekkel bombáznak minket. Úgy tűnik nem csak a legális kereskedelem, hanem egyre inkább a bűnözés is célirányossá válik és módszereit az egymástól jól elkülöníthető potenciális áldozati csoportok sajátosságainak megfelelően dolgozza ki. Ezek jó része a közösségi oldalakon keresztül vagy e-mailban is „becserkészhető”.

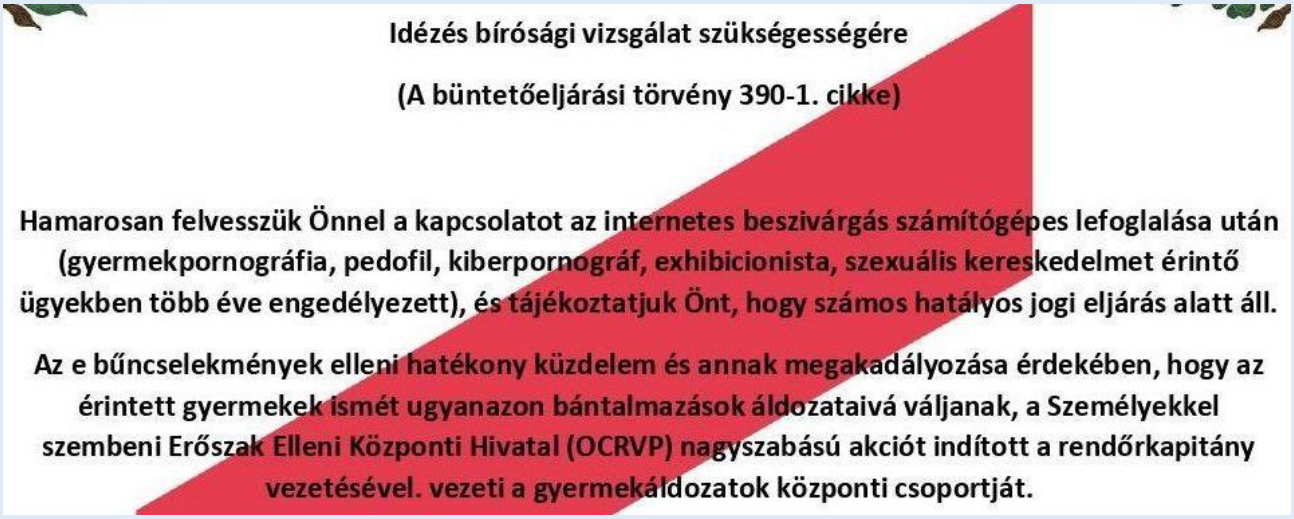
Csalók postafiók tulajdonosok tömegeinek küldenek zsaroló e-maileket, melyek küldője magát profi programozóként bemutatva azt állítja, hogy egy felnőtt tartalmakra épülő honlapon keresztül vírussal fertőzte meg a számítógépét. Az ismeretlen azt is állítja, hogy ennek eredményeként átvette az ellenőrzést a gép felett, mindent lát, ami megjelenik a képernyőn és a kamerát, valamint a mikrofont tetszése szerint tudja ki-be kapcsolni, továbbá hozzáfér az érintett által használt közösségi oldalak névjegyzékéhez is. A zsaroló kilátásba helyezi, hogy áldozata valamennyi ismerősének elküldi azt az általa összevágott videót, mely párhuzamosan mutatja a nézett filmet és az érintett filmnézés közbeni magatartását, reakcióját.

Az internethasználók közül sokan néznek pornót, akik egy része ezt titokban teszi, vagy legalábbis nem vállalja ezt fel a környezete előtt. Ha a zsaroló e-mail címzettje ebbe a kategóriába tartozik, akkor nagy valószínűséggel pánikba esik és engedelmeskedni fog a bűnözőnek, aki felajánlja, hogy egy bizonyos pénzösszegért cserébe eltekint a kilátásba helyezett „akciójától". Az anonimitás érdekében a zsaroló a fizetés teljesítését nagy valószínűséggel kriptovalutában (pl. Bitcoin) kéri és az alábbi mondatokkal zárhatja üzenetét:

„50 órája van (2 nap +) a fizetés megszervezésére. A levél elolvasásáról automatikusan értesítést kapok, ezért az időzítő attól a pillanattól indul, amikor elolvasta ezt a levelet.
Ha megtudom, hogy megpróbálta megosztani ezt az e-mailt bárki mással, akkor privát videója azonnal mindenki számára elérhető lesz!"

Ha csak a címzettek néhány százalékára sikerül a bűnözőnek ráijeszteni, akkor is jelentős bevételekre számíthat, ezért ne lepődjön meg senki, ha ilyen vagy ehhez hasonló tartalmú levelet kap! Ezek általában csak blöffre épülnek, de akad esetenként példa arra is, hogy csellel, fortéllyal ráveszik a kiszemelt áldozatot arra, hogy róla kompromittáló videót készíthessenek a webkameráján keresztül. Ez esetben viszont már valós zsarolási potenciál lesz az elkövetők birtokában.

Egyre gyakoribb, hogy büntetőeljárásban kiállított idézéssel próbálnak ráijeszteni az e-mail címzettjére külföldi csalók. Ez esetben messzebbre mennek és gyermekpornográfiával gyanúsítják meg, ami már büntetőjogi kategória. Ezek a „hivatalos iratok" egyelőre még alkalmatlannak tűnnek a megtévesztésre, mert olyan sok bennük a tetten érhető hiba, azonban minőségük hónapról hónapra javul. Újabban már volt, vagy jelenleg is hivatalban lévő magyar rendőri vezetők neveit szerepeltetik azokon aláíróként.



Idézés bírósági vizsgálat szükségességére

(A büntetőeljárási törvény 390-1. cikke)

Hamarosan felvesszük Önnel a kapcsolatot az internetes beszivárgás számítógépes lefoglalása után (gyermekpornográfia, pedofil, kiberpornográf, exhibicionista, szexuális kereskedelmet érintő ügyekben több éve engedélyezett), és tájékoztatjuk Önt, hogy számos hatályos jogi eljárás alatt áll.

Az e bűncselekmények elleni hatékony küzdelem és annak megakadályozása érdekében, hogy az érintett gyermekek ismét ugyanazon bántalmazások áldozataivá váljanak, a Személyekkel szembeni Erőszak Elleni Központi Hivatal (OCRVP) nagyszabású akciót indított a rendőrkapitány vezetésével. vezeti a gyermekáldozatok központi csoportját.

Kiberpajzs

KiberPajzs néven közös oktatási és kommunikációs együttműködésről döntött a **Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság, az Nemzetbiztonsági Szakszolgálat-Nemzeti Kibervédelmi Intézet, illetve az ORFK**. A digitális pénzügyi bűnözők ma elsősorban a fogyasztók érzelmi manipulálásával, illetve megtévesztésével támadnak. Így a KiberPajzs szervezői a lakossági ügyfelek pénzügyi tudatosságának erősítése, a kiberkockázatok minél hatékonyabb kezelése érdekében fognak össze.

Az együttműködés honlapja a **kiberpajzs.hu**, melyen már jelenleg is számos csalás módszerének leírása megtalálható, melyek segítik a weblap látogatóját abban, hogy idejekorán felismerje, ha sérelmére bűncselekményt kísérelnek meg elkövetni. Ezen bűncselekmények felderítése, sértettjeik kártalanítása még bizonytalan, az egyedül hatékony megoldásnak a megelőzés tűnik. A támadások elhárítására pedig csak azok képesek, akik kellőképpen felkészültek a témában.

A Veszprém vármegyei rendőrség elnevezésű Facebook oldalon a Veszprém Vármegyei Rendőrfőkapitányság sajtószolgálata rendszeresen megosztja az aktuális híreket, közleményeket. Ezek között az online csalások is szerepelnek, továbbá az azok megelőzését segítő információk.

Információkéréssel forduljon hozzánk bizalommal!
Veszprémi Rendőrkapitányság
8200 Veszprém, Bajcsy-Zsilinszky utca 2.
Tel: 06-88/428-022
E-mail: **rauszi@veszprem.police.hu**

A kiadásért felel: Rausz István r. ezredes rendőrkapitány