Dr. Packosz Nikiforosz vezető főtanácsos

Sándor-palota

nikiforosz.packosz@sandorpalota.hu

ÖSSZEFÜGGÉSTELEN ÖSSZEFÜGGÉSEK – AVAGY EGY BŰNESET (KIBER)TÉRBELI VÁZLATA

Absztrakt

A bűnözésföldrajz alapvetően a fizikai térhez kötődő bűncselekmények térbeli jellemzőit vizsgálja. Napjainkban azonban egyre kevesebb ilyen típusú bűncselekményt követnek el, a kiber térben viszont egyre több jogsértő cselekmény történik. Kutatásomban azt bizonyítom, hogy egyes online bűnelkövetők esetében van létjogosultsága a térbeli aspektusú vizsgálatoknak.

Az esettanulmányban az elektronikus fizetési rendszerek elleni visszaélések leggyakoribb megjelenési formáit, illetve azok gyakorlati kihívásait kívánom bemutatni, kiemelten a bűnüldözői kapacitások és a nyomozó hatóság privát szektorral történő együttműködésének perspektívájában. Röviden érintem továbbá az elkövető motivációját és a viselkedésének szociológiáját.

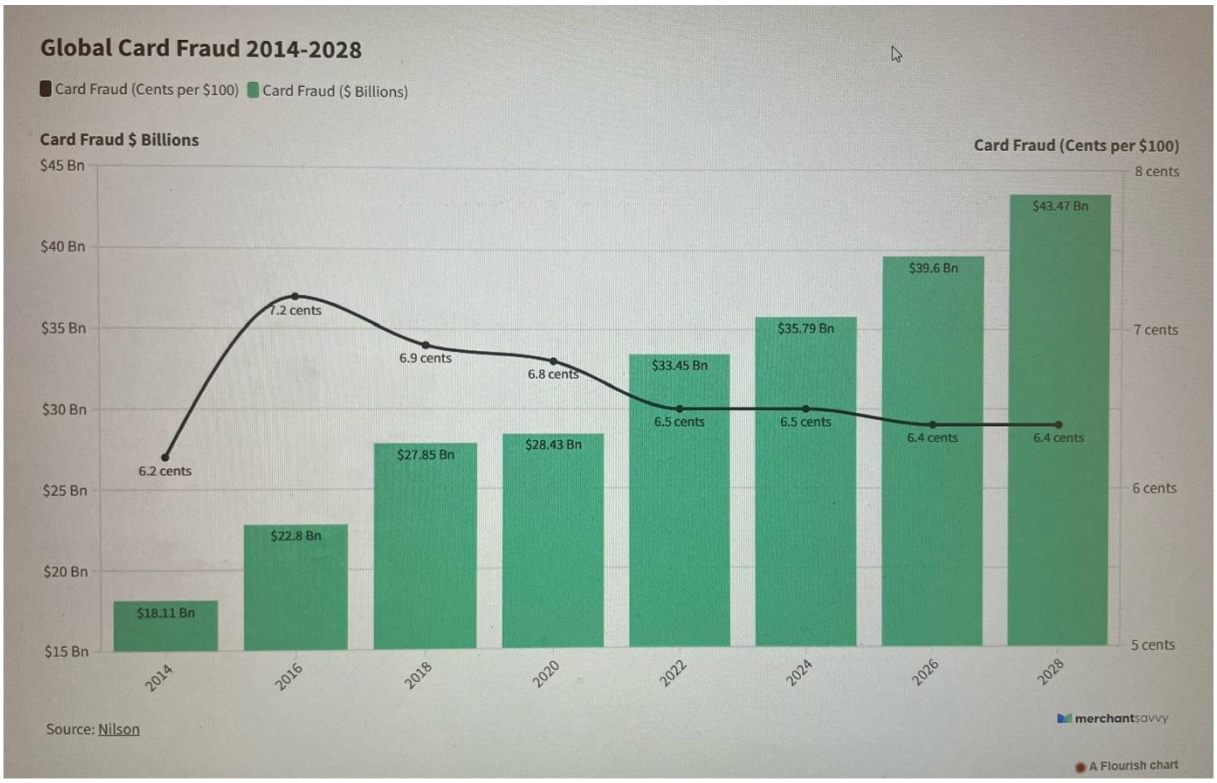
Kulcsszavak: elektronikus fizetési visszaélések, TOR böngésző, online inkognitó, félprofi elkövető(k)

1. Bevezetés – beszédes számok

A bűnözés térbeliségének vizsgálta több mint két évszázadra vezet vissza. Olyan bűncselekményeket vizsgáltak a kutatók, amelyek jól köthetők a földrajzi térhez. Ezek többségében vagyon és személy elleni deliktumok voltak. Az elmúlt közel egy évtized hazai és nemzetközi trendjét figyelve azt láthatjuk, hogy csökken a hagyományos, a földrajzi térhez konkrétan köthető bűncselekmények száma (pl. lopás, emberölés, betörés, gépjárműlopás) (Mátyás 2022). A csökkenéssel párhuzamosan viszont megjelentek a kibertében elkövetett bűncselekmények, melyek évről évre egyre nagyobb részesedést érnek el a hazai és a külföldi bűncselekményi statisztikában. A szakemberek egyöntetű véleménye szerint ezen bűncselekmények részarányának jelentős mértékű növekedése várható már a közeljövőben is.

A kibertében elkövetett bűncselekmények nyomozása sok esetben speciális ismereteket igényel, a nyomozás során pedig szükséges speciális protokollok, nyomozási módszerek kidolgozása. Ebben a kérdésben rendkívül fontos, hogy már a felderítési szakban segítse és támogassa a rendőrség munkáját az ügyészség (Vári 2017). Úgy gondolom, hogy bizonyos típusú kiberbűncselekmények esetében a földrajzi szemlélet is segíthet a felderítésben. Az alábbiakban bemutatott esettanulmány azt mutatja be, hogy az elkövető beazonosításában a földrajzi tényezők is segítettek.

A Merchant Savvy, független fizetésfeldolgozásra szakosodott elemző csoport 2024-es fizetési visszaélésekkel összefüggésben kiadott statisztikája és prognózisa szerint, a bankkártyás csalásokból eredő kár 2024-ben globálisan elérheti a közel 36 milliárd dollárt, ami a 10 évvel korábbi adatokkal összevetve kétszeres növekedést jelent (1. ábra). Árnyalja a képet, hogy a kártyánként 100 dollár költésre levetítve okozott kár gyakorlatilag stagnál, tehát a bankkártya kibocsátások (és felhasználások) mértékének növekedése okozza a károsszeg duplázását.



1. ábra: A bankkárytás visszaélésekkel globálisan okozott kár és becsült kár 2014-2028 között (forrás: https://www.merchantsavvy.co.uk/payment-fraud-statistics/)

Ugyanezen statisztikák szerint az online fizetési rendszerek elleni visszaélések leggyakoribb (dobogós) elkövetési formái az adathalászat, a saját ügyfelek által elkövetett csalárd műveletek, és az ún. „card testing”, azaz a bankkártya adatok jogosulatlan felhasználási módozatai (például ide soroljuk az alacsony értékű vásárlásokat a bankkártya adatok tesztelésére, melyeket jellemzően maga az adatszerző elkövető hajt végre, ezzel növelve az eladásra kínált adatok értékét; az online piactereken végrehajtott termék vagy szolgáltatás vásárlásokat; a bankkártya adat csalárd visszatérítéshez történő felhasználását) (2. ábra).

2. ábra: A leggyakrabban előforduló fizetési csalások rangsora 2021 és 2023. évben (forrás: https://www.merchantsavvy.co.uk/payment-fraud-statistics/)

Van tehát egy kövér (több milliárd dolláros) számadatunk és mögötte a favorit és a jól ismert, mégis hatékony elkövetői módszerek (Chen, Christopher 2022).

A nemzetközileg egységes (jog)szabályok szerint az érintett pénzintézetnek meg kell térítenie az ügyfelek bűncselekményből eredő kárát, kivéve, ha az ügyfél súlyosan gondatlan, vagy szándékos károkozó magatartást tanúsít(ott). A bizonyítási teher ugyan a pénzintézetet terheli

(Belovics et al. 2023), de a rendelkezésre álló infrastruktúra/technológia adta szolgáltatói „fölény” tükrében mindez korántsem olyan nehézkes és bonyolult, mint korábban.

Nézzük, miként illeszkedik ebbe az önkényesen kiválasztott információkkal lefestett kusza képbe (és mennyire aktuális) a Nemzeti Nyomozó Iroda több mint 10 évvel ezelőtti, a Btk. 375.§ (1) bekezdésébe ütköző információs rendszer felhasználásával elkövetett csalás bűntett megalapozott gyanúja miatt S. Balázs ellen lefolytatott nyomozása.

2. A nyomozás első fázisa – avagy meddig lehet a mocsárban dagonyázni?

Az egyik legnagyobb hazai pénzintézet rendszerében nagy mennyiségű csalárd online tranzakciót (áru és szolgáltatás vásárlásokat) észleltek, melyeket jogosulatlanul megszerzett bankkártya adatokkal hajtottak végre. Az érintett bankkártya adatok különböző (magánszemély és céges) ügyfelekhez voltak köthetőek, azonban a bankkártyák felhasználási történetének lekérdezése, majd elemzése során a pénzintézet compliance szakemberei egyértelműen megállapították az adatok ún. közös illegális megszerzési pontját (Dal Pozzolo et al. 2017, Nicolini – Leonelli 2021), ami első körben egyazon elkövetőre, vagy elkövetői körre utal(hatot)t. Adódott azonban a kérdés, hogy maga az „adatszerző elkövető” használta-e fel a megszerzett bankkártya adatokat online vásárlásokhoz, vagy a csalárd tranzakciókat már egy másik elkövető hajtotta végre, aki a bankkártya adatokhoz másod/sokadik kézből jutott hozzá (pl.: megvásárolta). A kérdéstől függetlenül választ kaptunk az ügy aktualitására, vagyis az absztraktban említett dobogós módszerek közül kettő (az adathalászat és a card testing) is megmutatkozik történetünkben.

A jogosulatlan tranzakciók napi szinten folyamatosak voltak (áru és szolgáltatás megrendelések), de a banki feldolgozás (észlelés) – és ennek következtében a nyomozás – lépéshátrányba került. A károsszeg egyre nőtt, s vele párhuzamosan a türelmetlenség (minden irányból) fokozódott.

A pénzintézet oldaláról 0-24 órás „figyelőztetést” rendeltek el a már felhasznált, illetve a vélelmezetten azonos időben/helyen kompromittált kártya adatok vonatkozásában, melynek eredményéről haladéktalanul (rövid úton távbeszélőn és elektronikus levélben) tájékoztatták a nyomozás vezetőjét.

Bűnüldözői oldalról a kötelező protokollok kötötték le a kapacitás nagy részét, melybe bele tartozott a jogosulatlan online tranzakciókhoz köthető IP címek (egyedi hálózati azonosítók) megállapítása, földrajzi helyhez kapcsolása és a kapott adatok(címek) elemzése, értékelése. E tekintetben már az első körös adatokból látszott, hogy az elkövető feltehetően a valós IP cím

elfedésére, azaz az online anonimitás megőrzésére kifejlesztett TOR böngészőn keresztül hajtja végre az illegális műveleteket. Erre lehetett következtetni abból, hogy ahány tranzakció, annyiféle (különböző) IP cím került regisztrálásra a szolgáltatók rendszerében. A TOR böngészőnek alapvető funkciója, hogy a szolgáltatók semmilyen vonatkozásban sem tudják követni a felhasználói aktivitást (letöltések, oldal látogatások) és a lehetséges beazonosítási adatokat (valós IP címek). Az inkognitó fenntartásának lényegi módszere, hogy a TOR böngésző az azt – világszerte aktuálisan az internethez rajta keresztül csatlakozó – felhasználó más személyek (eszközeinek) IP címét osztja ki (méghozzá rövid időközönként váltakozva és randomizált módon) az elsődleges felhasználónak, tehát az elsődleges felhasználó szolgáltatói szemszögből látszólag mindig más és más IP címmel jelentkezik fel az internetre, ráadásul ez a fellépő IP cím is folyamatosan változik.

Az online piactereken megrendelt áruk mögött – a már említett megtévesztő IP címek mellett – hamis okmányokkal regisztrált felhasználói profilok, „dobós" rövid ideig használt telefonszámok, és ad-hoc jelleggel (a futárnak telefonos helyszíni pontosítással) megadott budapesti kiszállítási címek voltak (Nagy 2023).

Az elkövető kalandvágyát, valamint biztonságérzetét mutatta a szintén hamis okmányokkal megnyitott online szerencsejáték egyenleg folyamatos, de közvetett módon – mobiltelefon egyenlegről – történő feltöltése. Bár ez azzal az apró kötelezettséggel járt, hogy a nyeremény „felvételére" – a pénzmosás elleni szabályokra tekintettel – kizárólag a befizetett összeg minimum egy alkalommal történő megjátszása esetén volt lehetőség. Aki jártas az online szerencsejáték világában, az tudja, hogy ez a követelmény csekély haszonnal, azonban (főleg más pénzén) kockázatmentesen teljesíthető (pl. Rafael Nadal első körös Roland Garros meccsének megjátszásával).

Eredményre vezető lehetőséggel kecsegtetett továbbá az elkövető által a MÁV online felületén megvásárolt vonatjegyek „nyomába" eredni, azonban a vásárlások rendszerint az indulás előtt kevesebb, mint 1 órával történtek, illetve a jegyek másodosztályra, tehát nem fix helyre szóltak.

3. Nyomós érdekek és összefüggések

Az ügyre fordított erőforrásokat tovább növelve, az alábbi időbeli és térbeli csomópontok körvonalazódtak, melyekre támaszkodva úgy tűnt, legalább „lőtávon belülre" került az igazságszolgáltatás és a pénzügyi szektor közös érdekeinek érvényesítése.

Egyrészt megállapítható volt az elkövető preferált vasúti útvonala (3. ábra), Szolnok – Budapest – Szolnok és az utazások jellemző időpontja (14-16 óra közötti idő). Másrészt az online

piactereken történt vásárlások kiszállítási helyszínei egyre inkább Budapest VI. kerületére koncentrálódtak. Harmadrészt összegyűlt egy olyan magyar IP címek alapján összeállított személyi adatbázis, amely (a TOR böngészőről ismertetettek alapján) legalább 99,9%-a, de nagy eséllyel 100%-a nem függ(het) össze az elkövetéssel, mégis feltűntek benne szolnoki címekhez köthető személyek és ezt a szolnoki vonalat erősítették a „dobós”, ideig-óráig használt SIM kártyák feljelentkező bázisállomásainak földrajzi pozíciói is.

3. ábra Magyarország vasúti térképe, pirossal jelölve a Budapest-Szolnok útvonal

4. A csillagok állása – avagy a befektetett munka megtérül!?

A nyomozás három hónapja tartott, és természetesen egy péntek délután érkezett a jelzés a bankbiztonság részéről, hogy a feltételezett elkövető másfél órán belüli indulással újabb Szolnok-Budapest vonatjegyet vásárolt, ráadásul két darabot és első osztályra (fix helyre). Talán vissza nem térő alkalom (elkövetői hiba/elbizakodottság), ami az ügyben beosztott készenléti rendszernek köszönhetően gyorsan megszervezhető akcióra adott lehetőséget, no meg arra, hogy bebizonyosodjon, 1 órán belül teljesíthető autóval a Budapest – Szolnok útvonal.

A szolnoki vasútállomáson az indulásra készülő szerelvényben a „keresett székben” nem kis meglepetésre, az IP címek alapján összeállított adatbázisban (szolnoki lakcímmel rendelkező) szereplő személy, volt megtalálható/elfogható (ennek banális okára később visszatérünk).

S. Balázs birtokában volt egy hátizsák, tele SIM kártyákkal, inaktív mobiltelefon készülékekkel és egy laptoppal, no meg néhány korábban (fel)használt, gyűrött vonatjeggyel. Társaságában barátja, Z. Sándor ült, akiről kiderült, hogy Budapesten a VI. kerületben található a tartózkodási helye, ahol a megtartott házkutatáson szinte hiánytalanul előkerültek a lopott kártyaadatokkal megrendelt elektronikai cikkek is.

Elfogását követően – tapasztalva a tudatos rendőri intézkedést, valamint látva a házkutatás során célzottan keresett és megtalált eszközöket – az elkövető részletes, feltáró jellegű beismerő vallomást tett. Olyan módon adta elő a bűncselekmény elkövetésének mozzanatait, amit csak és kizárólag a tényleges elkövető tudhatott (tettes tudomás).

A gyanúsított teljes mértékű együttműködésének (és kármegtérítési szándékának) köszönhetően a nyomozás gyors lezárására és sallangmentes vádemelésre kerülhetett sor. Mindeközben, tehát még a bűntetőeljárás hatálya alatt S. Balázs – a nyomozó hatóság és az ügyészség engedélyével – Németországba távozott, ahol egy logisztikai cégnél kezdett el dolgozni (itt fél év elteltével középvezetővé léptették elő), növelve ezzel a kármegtérítési képességét is.

5. Elkövetői profil és egy jelentéktelen hiba

S. Balázs 24 éves (volt), főállásban egy árufuvarozó cégnél dolgozott sofőrként. Szabadidejében autodidaktaként kezdte megismerni a Darknet különböző fórumain a lopott bankkártya adatok felhasználási lehetőségeit, s elhatározta, hogy bankkártya adatokat vásárol. Nyilvánvaló volt, hogy nem professzionális elkövető, és nem is törekszik jelentősebb mértékű anyagi haszonra.

Testnevelő tanár apja kiskorától egyedül nevelte, átlagon felüli szigorral. Az alapvetően helyes értékrenddel bíró fiatalember mégsem találta helyét a társadalomban, szociális értelemben marginális helyzetben érezte magát.

Összességében középszintű elkövetőnek minősíthetjük, képességei alul maradtak a számítástechnikában magasan kvalifikált hackerekénél, de egy átlagos bankkártya tolvajnál sokkal kifinomultabb és konspiratívabb magatartást tanúsított.

Végül térjünk vissza az IP címek alapján összeállított, 99,9-100%-ig haszontalannak tekintett adatbázisra, illetve arra, hogyan szerepel(hetet)t abban mégis S. Balázs. A válasz a TOR böngésző beállítási funkcióiban (a részletekben…) rejlett, ugyanis a már említett randomizálva megjelenített IP címek közös halmazába az alapbeállítás szerint bekeveredhet az elsődleges felhasználói IP cím is. Amennyiben a saját IP cím eshetőleges megjelenítését a felhasználó

mindenképpen ki akarja zárni, a beállítások menü pontban egy „pipával” teheti meg. S. Balázs ezt elmulasztotta, így véletlenszerűen, de a temérdek tranzakció közé bekerült saját, valós IP címe. Az ügy minden bizonnyal ezen elkövetői malőr nélkül is egyező eredménnyel zárult volna, így mindezt csupán érdekes adalékként szolgál az ügy megismeréséhez.

5. Konklúzió

Az ilyen jellegű bűncselekmények esetén a tényleges elkövetői magatartás a kibertérben valósul meg, ugyanakkor az elkövetőnek „léteznie” kell valahol a fizikai valóságban is. Ez a kettő „pozíció” legalább közvetett módon utal egymásra, összefügg egymással, akármilyen kuszaságnak is tűnik a virtuális és a földrajzi lábnyomok visszafejtése.

S. Balázs ügyét a Nemzeti Nyomozó Iroda megoldotta. Teljes bizonyítottság, beismerő vallomás, kármegtérülés, gyors nyomozás befejezés, és egy „megtért” elkövető, aki szinte azonnal visszailleszkedett a társadalomba. Bár nem túl nagy, nem is túl bonyolult ügy, de kijelenthető, hogy kriminalisztikai és kriminológiai „happy end”-el zárult. Mégis az a véleményem, nem érte meg, pontosabban nem fogja megérni az ilyen és ehhez hasonló nyomozásokat lefolytatnia a magyar rendőri szerveknek. A mezzo szinten elhelyezkedő „S. Balázs féle” ügyek cseppek a tengerben, ár-érték arányban indokolatlanul sok kapacitást kötnek le, elvéve ezzel az erőforrást az egyre veszélyesebb, új típusú és új technológiákra is támaszkodó szervezett bűnözés elleni küzdelemtől.

Jelen publikáció egyik célja rávilágítani arra, hogy milyen motiváció és források állnak egyetlen semi-pro (félprofi), vagy ha tetszik másodállású bűnelkövető mögött. Egyben cél a gondolatébresztés is, hogyan lehet(ne) megelőzni és időben detektálni ezeket az „elcsábulásokat”, mert a legkevesebb kapacitást az a nyomozás köti le, amit le sem kell folytatni.

Vajon elegendő a specifikusan, szofisztikáltan betanított mesterséges intelligencia térnyerése, vagy emellett a bűnmegelőzés terén más, hagyományos (emberi) tényezők alkalmazása/figyelembevétele is szükséges?

A fentiek alapján úgy gondolom, hogy sikerült arra rávilágítanom, hogy a kiberbűncselekmények nyomozása során is van létjogosultsága a bűnözésföldrajznak. Természetesen nem azt kívántam bizonyítani, hogy a kriminálgeográfia a kulcs az online módon elkövetett deliktumok nyomozása során. Csupán azt szerettem volna hangsúlyozni, hogy a sikeres felderítésben szerepe lehet a bűnözési térképek készítésének, a térbeli adatgyűjtésnek és gondolkodásmódnak.

Felhasznált irodalom

Andrea Dal P. – Giacomo B. – Olivier C. – Cesare A. – Gianluca B. (2017): Credit Card Fraud Detection: a Realistic Modeling and a Novel Learning Strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8): 3784-3797
DOI: 10.1109/TNNLS.2017.2736643

Belovics E. – Molnár G. M. – Sinku P. (2023): Büntetőjog II. – Különös rész. ORAC Kiadó Kft., Budapest

Chen, C. (2022): The evolution of law against payment frauds, Routledge, London

Gianni N. – Lucia L. (2021): Financial Frauds on Payment Cards: The Role of Financial Literacy and Financial Education. The International Review of Financial Consumers, 6(1): 1-3.

Nagy Z. (2023): Az Interneten elkövethető tipikus bűncselekmények. In: Kovács Z. (szerk): A kibernyomozói munka bűntetőjogi sajátosságai. Nemzeti Közszolgálati Egyetem, Budapest, pp. 19-26.

Vári V. (2017): A nyomozás változó szerepe az új Be.-i törvényben In: Kiglics N. (szerk.): II. Turizmus és Biztonság Nemzetközi Tudományos Konferencia. Pannon Egyetem Nagykanizsai Campus, Nagykanizsa