DOI: 10.38146/BSZ.2022.3.9

ÉRDEKES BŰNCSELEKMÉNYEK, TANULSÁGOS NYOMOZÁSOK

Egy dark weben elkövetett bűncselekmény felderítésének tanulságai, a nemzetközi összefogás jelentősége

Valóban nincs reális esély a dark neten elkövetett bűncselekmények elkövetőinek felderítésére?

Lessons learned from the detection of a crime committed on the dark web, the importance of international cooperation

Is there really no realistic chance of detecting the perpetrators of crimes committed on the darknet?

Hertelendi Lajos
Dr. kooperatív szerkesztő, rendőr alezredes
Belügyminisztérium,
Belügyi Szemle Szerkesztősége
hertelendi.lajos@bmkszf.hu

Absztrakt

Cél: Már korábban is számos, büntetőjogi és kriminalisztikai tanulságokkal bíró cikk jelent meg a Belügyi Szemlében. A régi-új rovatként újraindított „*Érdekes bűncselekmények, tanulságos nyomozások*" rovat több szempontból is különös és jövőbe látó gondolatként született meg a Szerkesztőség égisze alatt. Munkásságuk során maguk a szerkesztők is sok olyan jellegű eseménnyel találkoztak, amelyet később szakavatott bűnügyes kollégák vetettek papírra, és ezen esetek többségükben jó alapot szolgáltattak egy-egy leíró vagy empirikus tanulmány elkészítéséhez, amelyek hozzájárultak a leendő nyomozó kollégák felkészítéséhez, vagy éppen az adott ügy jogi szempontból történő feldolgozásához. További célként került megfogalmazásra, – hasonlóan a Belügyi Szemle korábbi lapszámai azonos című rovatában megjelent esetleírásokhoz – hogy az új rovat keretein belül megjelenő tanulmányok hasznosíthatók legyenek a büntetőjogi

és kriminalisztikai szemináriumokon. Az újrainduló rovattal tehát egyfajta hiánypótló szerepet is betölteni kíván a szerző, ezzel is hozzájárulva a rendvédelmi- és a joghallgatók praxisorientáltabb felkészítéséhez.
Módszertan: A tanulmány egy elemző és leíró jellegű elméleti kutatás, amely a vizsgált esetleírás dimenzióit mutatja be.
Megállapítások: A szerző a tanulmány közzétételével egy olyan érdekes bűnügyet és annak felderítését ismerteti, amely a szélesebb közvélemény körében is érdeklődésre tarthat számot, de az olvasók, a kutatók, és a hallgatók is profitálhatnak az eset feldolgozásából, elemzéséből. Az új cselekmények azonosítására a társadalom, a rendőrség, a politika új szavakat, kifejezéseket alkotott: hackelés, gyermekpornográfia, phishing, dark web, adathalászás, rosszindulatú programok.
Érték: Az esetleírás konkrét bűncselekményt dolgoz fel, az elkövetett cselekmények jogi megítélése és nyomozása, sikeres felderítés, valamint a levonható tanulságok figyelembevételével. Jelen tanulmányban olyan, a Büntető Törvénykönyvben nevesített magatartásokat mutat be a szerző, amelyek esetében nem feltétlenül szükséges a kibertér felhasználása, azonban a már elkövetett cselekményekből további, büntetendő magatartási formák bontakozhatnak ki.

Kulcsszavak: dark web, bűncselekmény, felderítés, nemzetközi összefogás

Abstract
Aim: A number of articles with criminal and forensic lessons have already been published in Belügyi Szemle. The *"Interesting Crimes, Instructive Investigations"* section, which was relaunched as an old-new column, was born under the auspices of the Editorship in several respects as a special and forward-looking idea. In the course of their work, the editors themselves encountered many events that were later put on paper by professional criminal colleagues, and most of these cases provided a good basis for a descriptive or empirical study that contributed to prepare the prospective investigators or to process the case from a legal point of view. An additional goal has been formulated - similarly to the case descriptions published in the previous column of Belügyi Szemle - to ensure that the studies published within the framework of the new section can be utilized in criminal law and forensic seminars. The author intends to play a kind of gap-filling role with the restart of the column, thus to contribute to a more practice-oriented preparation of law enforcement and law students.
Methodology: The study is an analytical and descriptive theoretical research that presents the dimensions of the examined case study.

Findings: By publishing this study, the author describes an interesting crime and its detection that may be of interest to the public, but that readers, researchers, and students may also benefit from processing and analysing the case. To identify the new acts, the society, the police, politics have created new words and phrases: hacking, child pornography, phishing, dark web, malware.
Value: The case report deals with a specific crime, taking into account the legal assessment and investigation of the acts committed, the successful detection, and the lessons to be learned. In the present study, the author presents behaviours named in the Penal Code for which the use of cyberspace is not necessary, but additional forms of behaviour that can be punished may emerge from the acts already committed.

Keywords: dark web, crime, intelligence, international cooperation

Bevezetés

Az internet a modernkori kommunikáció legmeghatározóbb eszköze, amely szinte bármilyen emberi tevékenység kiszolgálására alkalmas. A földrajzi határok átívelhetőségével, kultúrák találkozásával megannyi lehetőség vált elérhetővé számunkra. Felhasználásával kutatómunkát végezhetünk, barátokat találhatunk, üzleti konferenciákat bonyolíthatunk le utazás nélkül, de a kikapcsolódásunk színteréül is szolgálhat.

A kibertér hirtelen tört be a hétköznapi ember életébe, ezzel nem hagyva időt annak felhasználó szintű elsajátítására, amely leginkább a társadalom biztonságtudatosságának hiányosságaiban mutatkozik meg.

Az új környezetben az emberi kreativitás határok nélkül bontakozhat ki, ezzel számtalan előnye mellett jelentős mennyiségű új bűncselekményformát, vagy régi magatartások átalakulását eredményezve. Ebből pedig egyenes út vezetett ezen bűncselekmények kapcsán a meglévő jogszabályi környezet módosításához is.

A kiberbűnözés meghatározásához először az internetet kell vizsgálni mint elengedhetetlen eszközt, ami nélkül gyakorlatilag nem lehetne ilyen módon bűncselekményt elkövetni. Nem lehet egy egyszerű technológiának tekinteni, ami önmagában eredményezheti ezeket a destruktív cselekményeket, inkább egy üres lapként kell elképzelni, amit a társadalom tagjai egyénenként töltenek meg tartalommal.

Jelen tanulmányban olyan, a Büntető Törvénykönyvben (2012. évi C. törvény a Büntető Törvénykönyvről, a továbbiakban: Btk.) nevesített magatartások kerülnek bemutatásra, amely alapcselekményhez nem feltétlenül szükséges a kibertér

felhasználása, azonban a már elkövetett cselekményekből további, büntetendő magatartások bontakozhatnak ki. A számítógépes bűnözői magatartások csoportosításából jelen tanulmányban kétféle magatartástípus kerül kiemelésre, amely magatartások felderítése új gyakorlatokat és másfajta gondolkodásmódot, szervezettséget és együttműködést igényel a bűnüldöző szervek részéről.

Az első ilyen magatartáscsoport a kiskorúak sérelmére elkövethető nemi élet szabadsága és nemi erkölcs elleni bűncselekményekhez köthető. Ezek, a gyermek sérelmére elkövetett olyan értelmi, érzelmi és erkölcsi fejlődését veszélyeztető magatartások, amelyek a sértettnek még a teljesen ki nem fejlődött tudatát, személyiségét jelentősen károsítják, ezzel befolyásolva későbbi élete alakulását is.

A Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály Nyomozó Osztálya eljárást folytatott a Btk. 197. § (2) bekezdésébe ütköző és a (4) bekezdés a) pont ab) alpontja szerint minősülő, az elkövető nevelése, felügyelete alatt álló, tizenkettedik életévét be nem töltött sértett sérelmére elkövetett szexuális erőszak bűntett és más bűncselekmények elkövetésének megalapozott gyanúja miatt T. János budapesti lakos ellen.

A nyomozás elrendelésére az Eltűnt és Kizsákmányolt Gyermekek Nemzeti Központja (National Center for Missing and Exploited Children – (NCMEC) bűnügyi jelzése alapján került sor.

Az eset és jogi megítélése, nyomozása

Az első elemzett magatartás egy olyan cselekménysorozatot mutat be, amelynek elkövetését a gyermekkel fizikai érintkezésben hajtották végre, azonban annak következményeként készült elektronikai anyagok kibertérbe való kikerülése adott lehetőséget a nemzetközi gyermekvédő szervezeteknek arra, hogy a nyomozó hatósággal közösen a bűncselekményt teljeskörűen felderítsék, az elkövetőt pedig büntetőeljárás alá vonják.

Az NCMEC, az Amerikai Egyesült Államokban üzemelő nonprofit szervezet, amelynek küldetése segítséget nyújtani az eltűnt gyermekek megtalálásában, valamint csökkenteni a gyermekek szexuális kizsákmányolását és megelőzni a gyermekek áldozattá válását. A szervezet a munkavégzése során együttműködik a rendvédelmi szervekkel, cégekkel, családokkal és áldozatokkal.

A szervezet által megküldött jelzésben 269 darab gyermekpornográf felvétel szerepelt. A felvételeken látható kiskorú személyek a nemiséget súlyosan szeméremsértő nyíltsággal, célzatosan, a nemi vágy felkeltésére irányuló módon kerültek ábrázolásra, és azok közül 46 darab egyértelműen egy adott áldozatról, egy 9–11 év körüli lánygyermekről készült. Az említett

gyermekpornográf tartalmakat a Google rendszerébe egy T. J. nevű felhasználó töltötte fel 2018 februárja decembere között. A feltöltésekkor használt bejelentkezési IP címek is ismertek voltak, akárcsak a Google-fiók regisztrációja során megadott telefonszám és e-mail címek is. Az azonos áldozatot ábrázoló fájlok – az elnevezésük alapján – feltehetően 2017. december 26. és 2018. október 24. között készültek.

Ezen felvételek ellenőrzésére az International Child Sexual Exploitation Database (ICSE) adatbázisban került sor, amelyből az a következtetés volt levonható, hogy más személy részére nem kerültek átadásra, illetve nem lettek hozzáférhetővé téve a felvételek. Az ICSE adatbázis egy, az Interpol által létrehozott, a tagállamok által közvetlenül hozzáférhető, gyermekek szexuális kizsákmányolásával összefüggő nemzetközi kép-, illetve videófelvételeket tartalmazó adatbázis, mely tartalmazza a tagállamok hatóságai által nyomozásaik során megtalált és az adatbázisba feltöltött gyermekpornográf tartalmú fájlokat.

Az említett kiskorú személy arcképe – különös tekintettel a külső jegyei (hajszín, orrszélesség, ajkak, szemöldök íve) – és életkora alapján sikerült egyértelműen beazonosítani a személyazonosságát, és így megállapítást nyert, hogy azonos a kiskorú Cs. Gy. budapesti lakossal. A rendelkezésre álló további adatok alapján végrehajtott adatkérések és elemzések eredményeként megállapításra került, hogy a jelzésben szereplő felvételeket T. J. budapesti lakos tölthette fel a saját Google-fiókjába, és a felvételek nagy valószínűséggel a kiskorú és családja tartózkodási helyén készülhettek. A beazonosított és rendelkezésre álló háttérinformációk okán, valamint a sértett személyiségének megóvása és lelki-testi sérülésének elkerülése érdekében a bűncselekmény(ek) további elkövetése, megszakítása volt az elsődleges cél, amely halasztást nem tűrő intézkedéseket követelt meg a nyomozóktól.

A bűncselekmény realizálási szakaszában sor került T. J. elfogására, a lakó- és tartózkodási helyén kutatás és lefoglalás foganatosítására, amelynek keretében lefoglalásra kerültek a tulajdonában/használatában lévő számítástechnikai és informatikai eszközök, adathordozók, mobiltelefonok. A lefoglalt eszközök adatmentését követően megtörtént az adattartalmak, különös tekintettel az azokon lévő fénykép- és videófelvételek elemzése.

Az összes felvétel áttekintése után megállapítást nyert, hogy T. J. számos alkalommal követett el szexuális jellegű bűncselekményt az élettársa gyermeke, kiskorú Cs. Gy. sérelmére, és ezeket rendszeresen dokumentálta is az aktuálisan használt mobiltelefonjával. A felvételek metaadatait a készítő nem változtatta meg, azok csupán a többszöri átmásolás eredményeként módosultak. A kiskorút ábrázoló felvételek jelentős része azonos hosszúsági és szélességi koordinátát tartalmazott, melyek az ő és családja tartózkodási helyére mutattak, amit

a képeken látható háttér, használati tárgyak és bútorzat is megerősített. A gyermekpornográf felvételek mindegyike megtalálható volt a T. J. elfogásakor a tőle lefoglalt mobiltelefon memóriakártyáján, illetve a szintén nála lévő adathordozón, azaz nevezett ezeket magánál tartotta.

A felvételek elemzését követően megállapítást nyert az is, hogy T. J. összesen 1297 db gyermekpornográf felvételt tartott, melyből 279 db az említett kiskorút ábrázolta, és azok saját készítésűek voltak.

Az összes elemzés befejezését követően T. J. a következő elkövetett magatartások alapján volt megalapozottan gyanúsítható. A bűncselekmény elkövetésével megalapozottan gyanúsítható személy budapesti tartózkodási helyén az akkor még 12. életévét be nem töltött, a nevelése és felügyelete alatt álló kiskorú Cs. Gy-vel szexuális cselekményt végeztetett oly módon, hogy a kiskorút arra kérte, hogy a testét, nemi szervét érintse meg. Később, több másik esetben, a fentiekben írtakon túlmenően, már T. J. érintette meg a kiskorú nemi szervét, orális módon szexuális cselekményt végeztetett, majd anális közösülést imitált, és a nemi szervét a kiskorú gyermek nemi szervéhez nyomva végzett szexuális cselekményt.

Jól látható az események elemzéséből, hogy fokozatosan, egyre komolyabb, nagyobb lelki és testi sérülést okozó cselekményeket követett el az elkövető. A „család" említett tartózkodási helyén végzett szexuális cselekményekről a saját használatú mobiltelefonjával fénykép- és videófelvételeket készített, amelyeket a nemiséget súlyosan szeméremsértő nyíltsággal, célzatosan, a nemi vágy felkeltésére irányuló módon ábrázolt. Ezen kívül a nevelése és felügyelete alatt álló kiskorú Cs. Gy-ről legalább 12 alkalommal készített gyermekpornográfnak minősülő felvételeket.

A lefoglalt és elemzett bizonyítékok alátámasztották, hogy T. J. 1297 darab gyermekpornográfnak minősülő felvételt tárolt több adathordozón, melyből 279 darab a kiskorú Cs. Gy-t ábrázolta. T. J. a gyanúsítotti kihallgatásain azt nyilatkozta, hogy a felvételek többségének készítésére nem emlékszik, valamint a szexuális jellegű cselekményekkel azt volt a célja, hogy a kiskorút felvilágosítsa a nemi életről, és arról, hogy már kellő fejlettséggel rendelkezik.

Az elkövetőről igazságügyi elmeorvos- és pszichológus szakértői vélemény is készült, amely megállapította, hogy a beszámítási és cselekvési képessége teljes, nem korlátozott, és a cselekmények elkövetésének idején sem volt az. Az ügy sajátossága volt, hogy T. J. által elkövetett súlyos lelki és testi sérelmet okozó cselekmény ellenére a kiskorú sértett édesanyja folyamatosan érdeklődött az elkövetővel kapcsolatban, és a bizonyított cselekmények ellenére továbbra is erős érzelmi vonzódása van T. J. iránt, és bízik annak mielőbbi szabadlábra kerülésében.

Az igazságszolgáltatási gépezet azonban jól működött, T. J-t a Fővárosi Törvényszék folytatólagosan elkövetett szexuális erőszak bűntett, folytatólagosan elkövetett szexuális visszaélés bűntett, és gyermekpornográfia bűntett elkövetése miatt 9 év 3 hónap fegyházban végrehajtandó szabadságvesztésre, és 10 év közügyektől eltiltásra ítélte, melyet a Fővárosi Ítélőtábla helybenhagyott.

Tanulság

Tekintettel arra, hogy az internet, illetőleg a dark web nagyban megkönnyíti a gyermekpornográf felvételek terjesztését és megszerzését, ezért a kibertér növekedésével a nyomozó hatóságoknak egyre nagyobb kihívást jelent az ilyen felvételek terjedésének visszaszorítása és az elkövetők felelősségre vonása. Bár a gyermekpornográfiával kapcsolatba hozható elkövetők nagyobb része „csupán" fogyasztó, és mások által készített tartalmakat szerez meg saját használatra, nyilvánvalóan vannak olyan elkövetők és elkövetői körök is, akik a tartalmak készítéséért felelősek. Amennyiben gyanú merül fel arra vonatkozóan, hogy magyarországi személy készít gyermekpornográf tartalmat, a rendőrség mindent megtesz annak érdekében, hogy a személyt azonosítsa, hiszen ezáltal nemcsak az ilyen tartalmak terjedésével veszi fel a harcot, hanem – ami még fontosabb – egy kiskorú sérelmére elkövetett, akár még folyamatban lévő szexuális bűncselekményt is megszakít, és megakadályozza a további abúzust.

Sikeres felderítés a dark weben

A második magatartáscsoport kibermegtévesztéssel és lopással azonosítható, ezek a tipikus adatszerző, phising (adathalász) tevékenységek, amelyek felhasználásával vagyon elleni bűncselekmények elkövetésére nyílik lehetőség, azonban az elkövetésének a befejezetté válása nem feltétlenül megy végbe azonnal, vagy magát az elkövetést, a megkárosítást a sértett hosszabb idő eltelte után fogja észlelni. A 21. században egyre nagyobb figyelmet kapnak a különböző készpénz-helyettesítő fizetési eszközök, ezzel háttérbe szorítva a készpénzhasználatot. Az idő előrehaladtával a készpénz alternatíváitól eddig mereven elzárkózó személyek is egyre nyitottabbá válnak a készpénz-helyettesítő fizetési eszközök használatára, melyet a 2020-as és 2021-es évet jelentősen meghatározó járványhelyzet is elősegített. A járványhelyzet által okozott visszaesés ellenére viszont Magyarországon továbbra is a készpénz a leggyakrabban és legnagyobb értékben igénybe vett fizetőeszköz (URL1).

A készpénz-helyettesítő fizetési eszközök egyes jogalkalmazási kérdései

Készpénz-helyettesítő fizetési eszköz a csekk, az elektronikus pénz, valamint a pénzforgalmi szolgáltató és az ügyfél közötti keretszerződésben meghatározott olyan személyre szabott dolog vagy eljárás, amely lehetővé teszi az ügyfél számára a fizetési megbízás megtételét.[1] Ezek mellett készpénz-helyettesítő fizetési eszköznek minősül a kincstári kártya és a személyi jövedelemadóról szóló törvény felhatalmazása alapján kiadott elektronikus utalvány is, feltéve, hogy ezek információs rendszer útján kerülnek felhasználásra.[2] A legismertebb és legelterjedtebb készpénz-helyettesítő fizetési eszköz Magyarországon a bankkártya.

A készpénz-helyettesítő fizetési eszközök vonatkozásában elkövetett bűncselekményeknek a jogalkotó az új Btk. elkészítése során kiemelt figyelmet szentelt.

A Btk. a Pénz- és bélyegforgalom biztonsága elleni bűncselekmények elnevezésű XXXVIII. fejezetében szabályozza a készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekményeket, azaz a készpénz-helyettesítő fizetési eszköz hamisítását, a készpénz-helyettesítő fizetési eszközzel való visszaélést, illetve a készpénz-helyettesítő fizetési eszköz hamisításának elősegítését.

Ezeket egészíti ki a vagyon elleni bűncselekmények között az információs rendszer felhasználásával elkövetett csalás elektronikus készpénz-helyettesítő fizetési eszközzel megvalósítható tényállása.

Az elmúlt években a készpénz-helyettesítő fizetési eszközök népszerűsödésével az ezekkel kapcsolatos, ezeket érintő bűncselekmények száma is ugrásszerűen növekedett, amit remekül reprezentál az alábbiakban ismertetett, a közelmúltban a dark neten felderített készpénz-helyettesítő fizetési eszközzel visszaélés.

A dark net, avagy dark web („a sötét web”)

A dark net, avagy dark web („a sötét web”) egy gyűjtőfogalom azon weboldalak számára, melyek titkosított hálózatokon találhatók, és rejtett IP címmel rendelkeznek (URL2).

Ez leegyszerűsítve azt jelenti, hogy a felhasználók teljes anonimitást élveznek, amikor ezen weboldalakat böngészik, hiszen a naplófájlokban nincs nyoma

1 A hitelintézetekről és pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 6. § (1) bekezdésének 55. pontja alapján.

2 Btk. 459. § (1) bekezdés 19. pontja alapján.

annak, hogy mely weboldalakon járnak. A dark neten található weboldalak azonban a rejtett adatok miatt nem kerülnek a jól ismert keresőmotorok által indexelésre, így a Google-al például el sem érhetők. Erre speciális – az adott hálózatra jellemző – böngészők jöttek létre, mint például az I2P, a Freenet, és a jól ismert The Onion Router (TOR).

A sötét web által biztosított anonimitás sok lehetőséget kínál azon személyeknek, akik illegális tevékenységet kívánnak folytatni (jelen esetben lopott bankkártyaadatokkal kereskedni), erre tekintettel a bűnüldözés során elengedhetetlen ezen fórumok monitorozása.

Egy sikeres felderítés állomásai

A dark net hálózaton bankkártyaadatokkal és egyéb bankkártyás bűncselekmények kapcsán aktív kereskedők monitorozása során egy, a felhasználóneve alapján nagy valószínűséggel magyar állampolgárságú kereskedő került a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály nyomozóinak látóterébe.

Az FBI és különböző nemzeti hatóságok közös munkájának köszönhetően néhány éve az Alphabay és a Hansa Market nevű dark net piacokat bezárták, a domaineket lefoglalták. 2019. május elején pedig a Wall Street Market és a Valhalla nevű feketepiacok is bezárásra kerültek az FBI, a holland, a német és a finn hatóságok közös nyomozásának eredményeképpen (URL3).

Ez lehetőséget adott a nyomozó hatóság számára, hogy a beazonosított felhasználó vonatkozásában megkereséssel forduljanak az Europol Kiberbűnözés Elleni Központja (továbbiakban: Europol) felé a célból, hogy az Alphabay nevű feketepiac bezárásának eredményeképpen rendelkezésükre álló piaci adatbázisban ellenőrizzék a beazonosított felhasználónevű kereskedőt. Az Europol által megküldött adatokból kiderült, hogy a felhasználó az Alphabay nevű feketepiacon elsődlegesen mint vásárló volt jelen, számszerűsítve 390 db bankkártyaadatot szerzett meg jogosulatlanul.

A kereskedő kínálatában bank- és hitelkártyaadatok, PayPal belépési adatok, kábítószerek és vényköteles gyógyszerek is szerepeltek. A beszerzett adatok alapján a felhasználó a korábbi legnépszerűbb dark webes kereskedelmi felületeken – többek között az Alphabayen, illetve a Wall Street Marketen – egyaránt jelen volt.

A nyomozó hatóság, az Europollal történt további információcserének köszönhetően beazonosította a kereskedő vélt személyes adatait, a korábbi lakcímét, valamint az egyik e-mail címét is.

Az e-mail címet szolgáltató gazdálkodó adatkérésre közölte a hatósággal a regisztráló adatait, illetve a regisztráció során megadott másodlagos e-mail címét, mely másodlagos e-mail cím egy nyugat-magyarországi középiskolában került regisztrálásra. A középiskola szintén közölte a hatósággal a regisztrációs adatokat.

Ezen adatoknak hála sikeresen beazonosíthatóvá vált az e-mail fiókok regisztrálója, akinek a személyes adatai, illetve korábbi lakcíme megegyezett az Europol által korábban közöltekkel.

Ezt követően – kutatás keretein belül – a felhasználó bejelentett lakcímén több elektronikus készüléket (laptopok, winchesterek, mobiltelefon és microSD kártya) is lefoglaltak az eljáró nyomozók, melyek elemzése során további, összesen 7454 db, javarészt a VISA és a MasterCard nevű kártyatársaságokhoz tartozó külföldön kibocsátott, és más nevére szóló bankkártya adatait (kártyaszám, lejárati idő és háromjegyű kód) sikerült beazonosítani, melyek különböztek a hatóság által korábban beazonosított kártyaadatoktól.

Fentiek eredményeképpen a 33 éves gyanúsított megalapozottan gyanúsíthatóvá vált nem kevesebb, mint 7844 rendbeli elektronikus készpénz-helyettesítő fizetési eszközön tárolt adat jogosulatlan megszerzésével elkövetett készpénz-helyettesítő fizetési eszközzel visszaélés vétség elkövetésével.

A gyanúsított ellen folytatott nyomozást a rendőrség lezárta, a keletkezett iratokat vádemelési javaslattal küldte meg az ügyészség részére.

Összegzés

Valóban ilyen könnyűszerrel felderíthető egy dark weben elkövetett bűncselekmény, mint ahogy az a fentiekben leírtak alapján érezhető? A gyakorlat ennél árnyaltabb, azonban jelen eset több dolgot is jól szemléltet.

Elsősorban rámutat arra, hogy mekkora relevanciával bír az eredményes felderítés tekintetében az Europollal történő hatékony együttműködés. Kriminalisztikai aspektusból elengedhetetlen és indokolt az Europollal vagy az Europolon keresztül történő információcsere az olyan jellegű ügyekben, melyekben felmerül bármilyen nemzetközi jellegű elem. Kétségkívül az Europollal történt kooperáció híján ezen felderítés sem ilyen eredménnyel zárult volna.

Másodsorban megállapítható, hogy a dark neten elkövetett bűncselekmények esetében is van értelme a büntetőeljárás lefolytatásának. Sokakban kialakult az a tévképzet, hogy ezen bűncselekmények elkövetőinek azonosítására nincs reális esély. Tény, hogy a dark neten történő nyomozás némi szakértelmet igényel, viszont korántsem eredményezi az ott történő elkövetés miatt az ügy felderíthetetlenségét.

Végül, de nem utolsó sorban – visszakanyarodva az eredeti témához – megmutatja, hogy a készpénz-helyettesítő fizetési eszközökkel kapcsolatos, ezeket érintő bűncselekmények mennyisége állandóan növekszik. Az eredetileg a nyomozó hatóság látókörébe került 390 darab bankkártyaadat az elkövető lakcímén végrehajtott kutatás során további 7454 db bankkártyaadattal egészült ki, azaz megközelítőleg közel 8000 db bankkártyaadattal rendelkezett az elkövető oly módon, hogy a nyomozó hatósághoz ezek vonatkozásában feljelentés nem érkezett. Ebben természetesen közre játszik az a tényező is, hogy a bankkártyaadatok jelentős része külföldi tulajdonosokhoz volt köthető, viszont ily módon az is megállapítható, hogy az ilyen jellegű cselekményeknek jelentős része látens marad, és a sértettek döntő része nem is szerez tudomást arról, hogy érintett egy bűncselekmény elkövetésében.

Mit tehetünk mégis annak érdekében, hogy csökkentsük annak esélyét, hogy bankkártyaadatokkal visszaélés áldozataivá váljunk? A Magyar Nemzeti Bank és több pénzintézet is tájékoztatókat állított össze annak érdekében, hogy ügyfeleik esetében csökkentsék az ilyen jellegű bűncselekmény elkövetések számát (URL4). Az ezen tájékoztatókban foglaltak betartása minimalizálhatja áldozattá válásunk esélyét.

A cikkben található online hivatkozások

URL1: *A koronavírus-járvány hatása a készpénzállomány változására 2020. január-augusztus folyamán*. https://www.mnb.hu/letoltes/a-koronavirus-jarvany-hatasa-a-keszpenzallomany-valtozasara-2020-januar-augusztus-folyaman.pdf

URL2: *What is the dark web? The dark web defined and explained*. https://us.norton.com/internetsecurity-emerging-threats-what-is-the-deep-dark-web-30sectech.html

URL3: *Massive blow to criminal Dark Web activities after globally coordinated operation*. https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

URL4: *Bankkártyás csalások*. https://www.mnb.hu/fogyasztovedelem/bankkartyak/biztonsag/a-bankkartyas-csalasokrol

Alkalmazott jogszabályok

2013. évi CCXXXVII. törvény a hitelintézetekről és pénzügyi vállalkozásokról

2012. évi C. törvény a Büntető Törvénykönyvről

A cikk APA szabály szerinti hivatkozása

Hertelendi L. (2022). Egy dark weben elkövetett bűncselekmény felderítésének tanulságai, a nemzetközi összefogás jelentősége. *Belügyi Szemle*, *70*(3), 607–618. https://doi.org/10.38146/BSZ.2022.3.9