Stratégiai Védelmi Kutatóintézet
ELEMZÉSEK 2019/14.

2019. július 02.

Felméry Zoltán:[1] A szervezett bűnözés általi internetes fenyegetettség értékeléséről szóló Europol jelentés ismertetése

Az elemzés az Europol által 2018. szeptemberében publikált, „*A szervezett bűnözés internetes fenyegetését vizsgáló jelentés*” (Internet Organised Crime Threat Assessment) legfontosabb eredményeit kívánja bemutatni a magyar olvasóközönség számára. Az Europol a jelentés ötödik éve történő közreadásával a kiberbűnözés rendészeti és bűnüldözési fókuszú értékelését kívánja megvalósítani. Közreadásának elsődleges célja, hogy átfogó képet adjon a jelenlegi és a jövőben várható, online elkövetett biztonsági fenyegetésekről és bűncselekményekről.

Mint az már korábban is jeleztük, terveink szerint, a Nemzeti Közszolgálati Egyetem Eötvös József Kutatóközpontjának Stratégiai Védelmi Kutatóintézete a belbiztonság stratégiai területeinek alakulását értékelő önálló elemző munkája mellett, a jövőben nagyobb hangsúlyt kíván fektetni a területet érintő és figyelmet érdemlő nemzetközi dokumentumok ismertetésére is. Elemzésünk e folyamatba illeszkedik.

Vezetői összefoglaló

- A 2018. évi IOCTA jelentés elsődlegesen három területre koncentrál, és kiemelten a számítógépes bűnözésnek, a gyermekek online szexuális kizsákmányolásának, valamint a pénzforgalmi csalásoknak a jellemzőit mutatja be.
- A rosszindulatú szoftveres támadások között továbbra is a különböző zsarolóprogramok az uralkodók. A zsarolóprogramok okozta veszteségek 2016 és 2017 között tizenötszörösükre növekedtek, a tendencia pedig minden bizonnyal a jövőben is folytatódni fog.
- Az adatok illetéktelen eltulajdonítása egyaránt kiemelt fenyegetés. A 2017-ben elkövetett legnagyobb adatsértés során több mint 100 millió személy volt érintett.
- Mivel a túlterheléses támadásoknál a lebukás kockázata és a támadás költsége is alacsony, ez az egyik legközkedveltebb támadástípus. A 2017. évet érintően az EU bűnüldöző hatóságainak 65 százaléka számolt be ilyen esetről.
- A gyermekek szexuális kizsákmányolását ábrázoló tartalmak előállítása napjainkban is folytatódik, az előállított tartalom mennyisége pedig növekszik.

Egy korábbi elemzésünkben az Europol elemzési tevékenységének rövid jellemzésével, valamint a 2017. évben megjelent SOCTA (*Serious and Organised Crime Threat Assessment*) jelentés bemutatásával foglalkoztunk.[2] Elemzésünkben megemlítettük, hogy az Europol a SOCTA mellett rendszeresen közread további dokumentumokat is. A legfontosabb ilyen dokumentum egyrészt a terrorizmus helyzetéről és tendenciáiról szóló jelentést (*EU Terrorism Situation and Trend Report*; TE-SAT), ami a vizsgált időszakban sikertelenül végrehajtott, megakadályozott, illetve sikeresen végrehajtott terrorcselekményeket mutatja be és értékeli. Másrészt, a szervezett bűnözés internetes fenyegetettségét vizsgáló jelentés (*Internet Organised Crime Threat Assessment*; IOCTA), ami azokra a kiberbűnözés eredményezte jelenségekre hívja fel a figyelmet, amelyek beavatkozást igényelnek. Mivel azt az ígéretet tettük, hogy a belbiztonság stratégiai területeinek alakulását értékelő önálló elemző munkánk mellett, a jövőben nagyobb hangsúlyt kívánunk fektetni a területet érintő és figyelmet érdemlő nemzetközi dokumentumok ismertetésére is, elemzésünkben a 2018. évi IOCTA jelentés legfontosabb megállapításait igyekszünk bemutatni. Írásunk egy összefoglaló, kizárólag a legfontosabb jelenségekre és jellemzőkre kon-

[1] Felméry Zoltán: a Nemzeti Közszolgálati Egyetem Stratégiai Védelmi Kutatóközpontjának tudományos munkatársa, valamint a Budapesti Corvinus Egyetem Vállalkozásfejlesztési Intézetének tudományos segédmunkatársa. E-mail: felmery.zoltan@uni-nke.hu

[2] FELMÉRY Zoltán: A súlyos és szervezett bűnözés általi fenyegetettség értékeléséről szóló Europol jelentés ismertetése, [online], forrás: svkk.uni-nke.hu, [2019.06.17.]

centrál. A részletekért érdeklődő olvasóknak célszerű kézbe venniük az eredeti jelentést. Elöljáróban érdemes megállapítanunk azt is, hogy a jelentés bemutatását nem informatikusok végzik, és vélhetőleg olvasóközönségünk sem informatikusokból áll. Ezért az alábbiakban arra törekszünk, hogy az átlagemberek számára is közérthető megállapításokat közöljünk a jelentésből, melynek következtében a különböző technológiai megoldások ismertetésétől eltekintünk.

Az Europol az IOCTA ötödik éve történő közreadásával a kiberbűnözés rendészeti és bűnüldözési fókuszú értékelését kívánja megvalósítani. A jelentés közreadásának elsődleges célja, hogy átfogó képet adjon a jelenlegi és a jövőben várható, online elkövetett biztonsági fenyegetésekről és bűncselekményekről. Egyrészt bemutatja az ilyen típusú bűncselekmények közelmúltbéli alakulását, másrészt képet ad számunkra a bűnüldöző szervek által végzett folyamatos tevékenységről. A 2018. évi jelentés elsődlegesen három területre koncentrál, és kiemelten a számítógépes bűnözésnek, a gyermekek online szexuális kizsákmányolásának, valamint a pénzforgalmi csalásoknak a jellemzőit mutatja be.

Számítógépes bűnözés

A számítógépes bűnözés – vagy gyakori szóhasználattal, kiberbűnözés – egy olyan bűnözési forma, amit számítógépek, számítógép-hálózatok és egyéb információtechnológiai eszközök használatával követnek el. Elsődlegesen a rosszindulatú szoftveres támadásokat[3], a személyes és ipari adatok illetéktelen eltulajdonítását, valamint a különböző szolgáltatásmegtagadással járó támadásokat[4] foglalja magában. E bűncselekmények célja az anyagi és/vagy reputációs károkozás. A leggyakoribb célpontok a kulcsfontosságú iparágak és a társadalom számára kritikus infrastruktúra (egészségügyi, telekommunikációs, pénzügyi, közlekedési iparág és ezek hálózatai).

A rosszindulatú szoftveres támadások között továbbra is a különböző zsarolóprogramok az uralkodók. Térnyerésük ugyan folyamatosan lassul, azonban az anyagi indíttatásból elkövetett támadások esetén, a rendvédelmi szervek és a vállalatok szerint is megelőzik a trójai programokat.[5] A zsarolóprogramok okozta veszteségek 2016 és 2017 között tizenötszörösükre növekedtek[6], a tendencia pedig minden bizonnyal a jövőben is folytatódni fog. Ezen támadásokkal kapcsolatban két jelenség mindenképpen figyelemre méltó. Egyrészt, ugyan a mobileszközök ellen intézett támadások még gyerekcipőben járnak és egyelőre általában csak különböző földrajzi területekre koncentráltan jelennek meg (Afrika, Ázsia, Észak-Amerika), az online bankolásról mobil bankolásra történő áttéréssel egyidejűleg, a mobilokra specializálódott rosszindulatú szoftverek elterjedése sem várat sokat magára. Másrészt, a nyilvános jelentések szerint, az anyagi motivációjú globális kibertámadásokat egyre nagyobb mértékben nemzetállamok szervezik.

Az adatok illetéktelen eltulajdonítása egyaránt kiemelt fenyegetés. Köszönhetően annak, hogy az egyszer illegálisan eltulajdonított adatok további bűncselekmények elkövetésére használhatóak fel. A 2017-ben elkövetett legnagyobb adatsértés során több, mint 100 millió személy volt érintett. A globálissá váló és korábban sosem látott mértékű olyan támadásokban, mint a „Wannacry” és a „Notpetya” botrányok, 150 ország 300 ezer felhasználója volt érintett, és kizárólag az előbbi 4 milliárd dolláros veszteséget okozott.[7] A hálózatokba történő illetéktelen behatolás mögött általában mindig valamilyen tiltott adatszerzés igénye húzódik meg.

[3] A rosszindulatú szoftveres támadásokhoz lásd: Malware. In: Paul J. SPRINGER: Encyclopedia of Cyber Warfare. ABC-CLIO. Santa Barbara, California. 2017. 173. o.
[4] A szolgáltatásmegtagadással járó támadásokhoz lásd: Distributed Denial-Of-Service Attack. In: Paul J. SPRINGER: Encyclopedia of Cyber Warfare. ABC-CLIO. Santa Barbara, California. 2017. 91. o.
[5] A trójai programokhoz lásd Trojan Horse. In: Paul J. SPRINGER: Encyclopedia of Cyber Warfare. ABC-CLIO. Santa Barbara, California. 2017. 295. o.
[6] Steve MORGAN: Global ransomware damage costs predicted to exceed $5 billion in 2017, In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.17.]
[7] Jonathan BEER: “WannaCry” ransomware attack losses could reach $4 billion In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.17.]

Legnagyobb mértékben pedig személyes, pénzügyi és orvosi adataink kerülnek veszélybe. Az illetéktelen adatszerzés 73 százalékban külső személyek részéről történik, némileg meglepő módon azonban 27 százalékban szervezeten belüli szereplők az elkövetők. A törvénytelen behatolás 50 százalékban szervezett bűnözői csoportokhoz köthető, míg a behatolás motivációja 76 százalékban az anyagi haszonszerzés.[8] Az adathalászat továbbra is növekvő tendenciát mutat, a 2018. évben az Unió tagországainak 75 százalékában volt folyamatban lévő eljárás valamilyen tiltott adatszerzés ügyében. Igaz ugyan, hogy kizárólag az elkövetők által megcélzott felhasználók alacsony hányada „kapja be a csalit" (ez az arány körülbelül 4 százalék[9]), de egyetlen felhasználó manipulálása is elég lehet teljes szervezetek kompromittálásához. Mondanunk sem kell, hogy a manipulációs kísérletek különösen gyakoriak a pénzügyi iparágban, ahol nem csak a szektor vállalatainak alkalmazottai, hanem az ügyfélkör is gyakorta támadás alatt áll.

Az anyagi, ideológiai, politikai és egyéb rosszindulatú szándékok motiválta szolgáltatásmegtagadással járó-, vagy más néven túlterheléses támadások, magántulajdonú és közszektorbeli szervezetek ellen egyaránt irányulnak. Mivel ez esetben a lebukás kockázata és a támadás költsége is alacsony, ez az egyik legközkedveltebb támadástípus. A fentiek miatt ez a támadástípus egyre gyakoribba válik. A 2017. évet érintően az EU bűnüldöző hatóságainak 65 százaléka számolt be ilyen esetről, míg harmaduk szerint a jövőben is nőni fog az ilyen típusú támadások száma.

Az Európai Unió egyes országai abban a tekintetben is heterogének, hogy esetükben mennyiben célzott támadásokról, illetve véletlenszerűen kiválasztott áldozatokról van szó. Az általunk bemutatott jelentés szerint általánosságban az azonban elmondható, hogy a bűnözők szakértővé válásával és a szofisztikáltabb technológiai eszközök hozzáférhetővé válásával, egyre nő a célzottan kiválasztott áldozatok aránya. Egyúttal egyre kevesebb támadást követnek el magánszemélyek ellen, míg ezzel párhuzamosan egyre nő a kisvállalkozások, vagy akár a még nagyobb célpontok elleni támadások aránya. A tendencia mögött a nagyobb profitszerzés igénye és lehetősége húzódik meg. Érdekes – látszólagos – ellentmondás, hogy bár a kibertér növekvő használata által egyre nő a pszichológiai manipuláció lehetősége, a spamekkel, egyéb manipulációs technikákkal és a hozzáférhető új megoldásokkal (például a távoli asztali szolgáltatásokkal) végrehajtott, a biztonsági rések kiaknázására irányuló akciók száma összességében csökkenést mutat. Ugyanakkor az áldozatok manipulálása révén megvalósított adathalászat, leggyakrabban továbbra is emailen keresztül történik. Az áldozatok megvezetésének sokféle célja van. Személyes adatok megszerzése, felhasználói fiókok feltörése, személyazonosságok eltulajdonítása, törvénytelen kifizetések indítása csak néhány ok a számtalan közül.

A rosszindulatú szoftverekkel végrehajtott támadások költségeit nehéz aggregáltan számszerűsíteni. Egyes becslések szerint azonban 2017-ben ez az összeg meghaladhatta az öt milliárd dollárt, mára pedig akár az évi 11,5 milliárd dollárt is elérheti.[10] Más források szerint a 2016. és 2017. évben végrehajtott 35 nagyobb méretű támadás akár 25 milliárd dollár hasznot is hajthatott az elkövetők számára.[11]

A jelentés szerint az európai általános adatvédelmi rendelet (The General Data Protection Regulation – GDPR) adatsértésekre vonatkozó új szabályozása minden bizonnyal növelni fogja az adatsértések rendészeti szervek részére történő bejelentési hajlandóságát. Annak köszönhetően, hogy a rendelet értelmében valamennyi adatsértés bejelentési kötelezettséggel jár 72 órán belül, a számítógépes bűnözés láthatósága javulhat. Annak visszaszorításához azonban további lépésekre van szükség. A jelentés szerint egyrészt olyan figyelemfelkeltő kampányok kellenek, amelyek tájékoztatnak a kiberbűnözés veszélyeiről. Másrészt, az érintettek nagyobb mértékű együttműködése is elkerülhetetlen. 2017-ben bekövetkezett néhány olyan támadás, amely

[8] Verizon: Ransomware, botnets, and other malware insights, 2018 Data Breach Investigations Report, In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.20.]
[9] Verizon: Ransomware, botnets, and other malware insights, 2018 Data Breach Investigations Report, In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.20.]
[10] Steve MORGAN: Global ransomware damage costs predicted to hit $11.5 billion by 2019, In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.20.]
[11] Tom SPRING: Google study quantifies ransomware profits, In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.20.]

megmutatta, hogy az egyes nemzetállami bűnüldöző hatóságok számára lehetetlen önállóan fellépni ezen új típusú fenyegetésekkel szemben. Ezen túl, az egyre kifinomultabbá váló bűnözői csoportok miatt, elengedhetetlen a bűnüldöző szervek képzése, valamint a nyomozati és igazságügyi tevékenységek további forrásokkal történő ellátása. Egyúttal szükséges az új technológiák (különösen a mesterséges intelligencia) bűnüldöző munkában történő felhasználása is.

Gyermekek online történő szexuális kizsákmányolása

A gyermekek szexuális kizsákmányolását ábrázoló tartalmak előállítása napjainkban is folytatódik, az előállított tartalom mennyisége pedig növekszik (pl.: az Európai Unió tagországainak 60 százaléka 2018-ban a tartalom mennyiségi növekedéséről számolt be). Az előállított tartalom növekedése részben új tartalmak megjelenését jelenti, részben a jobb felderítésnek köszönhető (azaz több esetre derül fény). Az új tartalmak növekedésének elsődleges indoka azonban továbbra is a felderítés és visszakövethetőség nehézsége és a lebukás alacsony kockázata. Az internethasználatot lehetővé tevő mobil eszközök elterjedése, az elektronikus platformok és szolgáltatások változatossága, az online anonimitás terjedése, a titkosítási megoldások széleskörű használata és a Darknet[12] használatának elterjedése alacsony kockázat mellett teszi lehetővé az érintettek számára ilyen tartalmú anyagok tárolását és egymás közt történő megosztását. A hagyományos kommunikációs eszközöket (email üzeneteket és közösségi média platformokat) az e tevékenységben érdekeltek változatlanul használják, a legtöbb tartalom azonban továbbra is közvetlenül a felhasználók között cserél gazdát. A különböző peer-to-peer megosztási elven működő platformok[13] a legfontosabb csatornák az ilyen jellegű tartalmak terjesztésekor. A világszerte terjedő internetkapcsolat következtében megjelent az élőben közvetített szexuális gyermekbántalmazás. Köszönhetően annak, hogy a beágyazott streaming lehetőségeket tartalmazó applikációk kedveltségének növekedése nagyban hozzájárult a saját előállítású, élőben közvetített tartalmak terjedéséhez. Az EU tagországainak fele arról számolt be, hogy növekvő mértékben találkoznak ezzel a tevékenységgel. A tevékenység különösen elterjedt az EU határain kívül, ahol a törvénykezés és a bűnüldözés kevésbé képes követni az e területet érintő gyors technológiai változásokat. A legnagyobb mértékben a Fülöp-szigetek érintett, de a világ más területei – például Kenya – is gyakori helyszínei a szexuális visszaéléseknek és azok interneten történő közvetítésének.[14]

A szexuális zaklatást a leggyakrabb esetben egy családtag vagy egy közeli ismerős követi el.[15] Az internethasználó korosztály esetén ugyanakkor egyre nagyobb mértékben fordul elő az a jelenség, hogy egy olyan elkövető bukkan fel szinte a semmiből, akivel azelőtt sohasem találkoztak az áldozatok. Mivel egyre több fiatalkorú fér hozzá az internethez és a közösségi média platformjaihoz, az online szexuális zaklatás is növekszik. A zaklatás ráadásul gyakran jár együtt kényszerítéssel és zsarolással is.[16] Az áldozatok az esetek többségében 8 és 14 év közötti fiatalok. A jelentésben megfogalmazott feltételezések szerint a jövőben egyre fiatalabb áldozatok is célponttá válhatnak.

Mivel a különböző anonimizálást és titkosítást jelentő technológiai megoldások egyre könnyebben elérhetőek, és az elkövetők részéről történő használatuk is nő, valamint a növekvő internetsebesség és a felhőalapú szolgáltatások terjedése miatt nincs már szükség a kompromittált tartalom saját számítógépen történő tárolá-

[12] A Darknet a láthatatlan weben kialakuló olyan hálózat, ami egyaránt alkalmas tiltott és azonosíthatatlan szolgáltatások nyújtására.
[13] A peer-to-peer megosztási elven működő platformokhoz lásd: Quang HIEU VU, Mihai LUPU, Beng CHIN OOI: Peer-to-Peer Computing. Springer. 2010.
[14] Terre des Hommes: The dark side of the internet for children. Online child sexual exploitation in Kenya – a rapid assessment report, In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.20.]
[15] Netclean: Netclean Report 2017 In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.20.]
[16] Amennyiben az áldozat megunja a zaklatást és le szeretné zárni a kapcsolatot, akkor az elkövető a korábbi – sokszor az áldozat beleegyezésével – megszerzett tartalom nyilvánosságra hozatalával fenyegetőzve próbálja meg rávenni az áldozatot további tartalmak készítésére és neki történő eljuttatására.

sához, a bűnüldöző szervek felderítő munkája egyre nehezebb. Az elkövetők jellemzően a fiatalabb korcsoportokból kerülnek ki, és ismertek számukra a fentiekhez szükséges technikai megoldások. A gyermekek online történő szexuális kizsákmányolása és bántalmazása nem okvetlenül köthető definíció szerint a szervezett bűnözéshez. Az elkövetők gyakran egyedül végzik a tevékenységüket és nincs kapcsolatuk a tradicionális bűnszervezetekkel. Ugyanakkor az általuk használt online fórumok nem kizárólag a tartalmak tárolására és megosztására szolgálnak, hanem az azzal kapcsolatos ismeretátadásra is, hogy hogyan előzhető meg a bűnüldöző szervek által végzett felderítés. Ebből következően az elkövetők magányos mivolta gyakran kérdésessé válik, és az így létrejövő közösségek normalizálják és bátorítják a szélsőséges egyéni magatartásokat.

Pénzforgalmi csalások

A pénzforgalmi csalásnak két alapvető típusa létezik. Az első esetben az elkövetők megszerzik, illetve duplikálják az áldozatok bankkártyáját, és annak birtokában követnek el valamilyen visszaélést. A második esetben a kártya tényleges birtoklása nélkül követik el a csalást.

A kártya birtokában lévő csalások ugyan visszaszorulóban vannak, de továbbra is léteznek. A kártyák duplikálásához szükséges adatok megszerzése általában a közkedvelt turistacsomópontokon történik. A megszerzett adatok alapján az eredeti kártyát klónozzák, majd ezt követően egy olyan helyen használják pénzfelvétel céljából, ahol az EMV implementáció[17] még nem történt meg. Ezen túl, a megszerzett kártyaadatok sokszor továbbértékesítésre kerülnek a Darknet különböző platformjain. A jelentés idézi a European Payment Council azon véleményét, hogy mindaddig, amíg a mágnescsíkos bankkártyák nem kerülnek betiltásra Európán kívül is, a leggyakoribb pénzforgalmi csalások közé fog tartozni a kártyaadatok ATM-ek használatán keresztül történő illetéktelen megszerzése.

A pénzforgalmi csalások között továbbra is a kártya birtoklása nélküli visszaélések dominálnak. Ebben az esetben a visszaéléshez szükséges adatok a Darkneten cserélnek gazdát, a pénzhez történő hozzájutás pedig – a fentiekhez hasonlóan – olyan országokban valósul meg, ahol az EMV implementáció lassú, vagy még várat magára. Ezen felül, az illetéktelenül megszerzett bankkártya-adatokat gyakran használják fel szállásfoglalásra, repülőjegyvásárlásra, illetve termékek és szolgáltatások online beszerzésére is.

Napjainkban a pénzforgalmi csalások a fentieken túl kiegészülnek egyéb elemekkel is. Egyrészt, az elmúlt évben a bűnüldöző szervek kiemelt figyelmet fordítottak a vámmal történő csalásokra. Előfordult ugyanis, hogy egyes bűnszervezetek illetéktelenül eltulajdonított és hamisított pénzügyi és kártyaadatokkal próbálták meg elkerülni a fizetendő vámokat. Másrészt, egyre nagyobb jelentőségre tesznek szert a több mint egy évtizede létező, de mostanában ismételten virágkorukat élő telekommunikációs csalások. Ezek közül a leggyakoribb az úgynevezett ISRF csalás (International Revenue Share Fraud), amely során az elkövetők illegális eszközöket használva hozzáférést szereznek egy hálózathoz, amelyről egy nemzetközi díjas szolgáltatóhoz kapcsolódva jelentős forgalmat generálnak. A szolgáltatónál keletkező bevételből pedig maguk is részesednek. Ez a típusú csalás a jelentés szerint összességében körülbelül évi 7 milliárd dollár kárt okozva az Unió országainak felét érinti, valamint más külső országokat (Egyesült Államok, Kanada, Svájc) is fenyeget.

Online bűnözői piacterek és egyéb bűnözési tényezők

A Darknet továbbra is megkönnyíti azoknak az illegális online piacoknak a működését, ahol olyan tiltott termékek és szolgáltatások kerülnek értékesítésre, amelyek nehezen követhetőek nyomon és további bűncselekmények elkövetésére alkalmasak. A Darknet piaci ökoszisztéma egyúttal nagyon instabil. Miután 2017-ben a hatóságok elsötétítették a Darknet három legnagyobb piacterét (az AlphaBay-t, a Hansa-t és a RAMP-ot[18]),

[17] Az EMV implementációhoz lásd EMVCo: A Guide to EMV Chip Technology, [online], forrás: EMVCO.com, [2019.06.21.]
[18] Chainalysis: The changing nature of cryptocrime, In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.21.]

további kilenc piactér zárt be önként, illetve az üzemeltetők eltűnése következtében. A jelentés kiemeli, hogy az elsötétítéséig ez a három piactér adta a teljes Darknet forgalom 87 százalékát, és egyedül az AlphaBay 200 ezer felhasználót és 40 ezer valamilyen terméket, vagy szolgáltatást nyújtó értékesítőt tömörített. Körülbelül 250 ezer drogkészítmény és vegyi anyag, illetve 100 ezer lopott, illetve hamisított dokumentum és termék került ott meghirdetésre. Bár a nagyok ellehetetlenítése a felhasználókat már létező, vagy újonnan alapított kisebb piacterek, illetve további platformok (titkosított kommunikációs alkalmazások) felé terelte, összességében csökkent az ilyen irányú aktivitás.

A Darknet piacterein a leggyakrabban továbbra is drogokkal kereskednek. A kereskedett mennyiség azonban még mindig elenyésző a hagyományos csatornákon áramló mennyiséghez képest. Az értékesített mennyiség és az abból származó bevétel alapján a legfontosabb országok közé Németországot, Hollandiát és az Egyesült Királyságot sorolhatjuk. A drogok mellett a kereskedés középpontjában lévő második legfontosabb árucikk az adat. Az illetéktelenül eltulajdonított személyes, pénzügyi és orvosi adatokkal történő kereskedés egyaránt a Darkneten történik. Hasonló a helyzet a hamisított dokumentumokkal és pénzzel is. Emellett, kevésbé gyakran, de előfordul, hogy a közbiztonságra legnagyobb veszélyt jelentő eszközök (fegyverek, robbanószerek, lőszerek) is itt cserélnek gazdát. Bár a hamisított – ruházati, elektronikai és szépségápolási – termékek kereskedelme egyaránt megjelenik a mélyben (azaz a Darkneten), ez a tevékenység elsősorban továbbra is az internet felszínén zajlik.

A korábban kizárólag hagyományos pénzügyi instrumentumokat célzó támadások ma már egyre gyakrabban kriptovaluták ellen irányulnak. Ahogy nő a kriptovaluták bűncselekményekhez történő felhasználása, úgy válnak egyre nagyobb mértékben a bűnözők célpontjaivá a kriptovaluták használói. A japán Coincheck és az olasz BitGrail kriptopénz tőzsdék elleni támadások 500 és 195 millió dolláros veszteséget okoztak a felhasználók számára.[19] A jelentés különböző beszámolókra hivatkozva azt állítja, hogy rohamosan növekvő mértékben használnak kriptovalutákat bűncselekmények finanszírozására is. A Bitcoin ugyan kezdi elveszíteni egyeduralkodó szerepét a kriptovaluták piacán, de még mindig ez az első számú eszköz, amivel a nyomozóhatóságok a különböző bűncselekmények felderítésekor találkoznak. A kriptovaluta kereskedők, a bányászati szolgáltatók, valamint az egyszerű számlatulajdonosok könnyedén rablás, zsarolás, illetve személyes adataik eltulajdonításának áldozatává válhatnak. Ezen felül, a pénzmosási tevékenység is egyre nagyobb mértékben támaszkodik a kriptovaluták használatára.

A kriptovaluták témakörének tárgyalásakor, egy gondolat erejéig érdemesnek tartjuk megemlíteni a cryptojacking jelenségét. A cryptojacking egy terjedőben lévő kiberbűnözési forma, melynek lényege az internethasználók sávszélességének kizsákmányolása annak érdekében, hogy az elkövetők mások erőforrásait a saját részükre történő kriptovaluta bányászathoz vegyék igénybe. Mivel a jelentés szerint ez a tevékenység bizonyos esetekben nem okvetlenül illegális, ugyanakkor jelentős profitot eredményez az elkövetők számára, egyre gyakoribbak a kísérletek különböző nagy látogatottságú oldalak látogatói rendszereihez történő hozzáférésre.

A kiberbűnözés földrajzi eloszlásával kapcsolatban a következők mondhatóak el. Az amerikai kontinens, különösen az Egyesült Államok, továbbra is egyaránt elszenvedője és kiindulópontja az internetes bűnözésnek. Az Egyesült Államok az első számú célpontja a különböző zsarolóprogramoknak és a mobil eszközök elleni támadásoknak, ugyanakkor itt működik a legtöbb adathalász weboldal is. Latin Amerikát tekintve pedig Brazília, amely ország a tíz legjelentősebb kiberbűnözést kezdeményező ország között van a világon, és Mexikó érintettségét érdemes kiemelni. Az európai országokat érintő fenyegetések elsősorban Európából eredeztethetőek. Néhány európai ország, beleértve ebbe Magyarországot is, a rosszindulatú programokat és adathalász elemeket tartalmazó emailforgalom alapján a világ élvonalában van. Afrika, ezen belül néhány ezzel foglalkozó bűnszervezetnek köszönhetően különösen Észak-Afrika, egyre erőteljesebb szerepet játszik a kiberbű-

[19] Mariella MOON: Coincheck loses $400 million in massive cryptocurrency heist, illetve David Z. MORRIS: Bitgrail cryptocurrency exchange claims $195 million lost to hackers, In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.21.]

nözésben is. A pszichológiai manipulációs technikákat igénylő csalások sok esetben ehhez a régióhoz kötődnek, egyre gyakoribb azonban a más technológiai elemeket igénylő támadásokban történő részvétel is. Jól érezhető, hogy az itt tevékenykedő szervezetek elkezdtek eddig számukra ismeretlen szofisztikált technológiai megoldásokat alkalmazni. A jelentés felhívja a figyelmet arra, hogy a fentiek indokán erősebb együttműködésre van szükség az Európai Unió és az észak-afrikai országok bűnüldöző hatóságai között. Ázsiában, Európával némileg ellentétben, kevésbé dominánsak a rosszindulatú elemeket tartalmazó emailek, ugyanakkor ott is jelentősek az adathalász kísérletek. Ezt mi sem bizonyítja jobban, minthogy a kiberbűnözéssel leginkább fenyegetett tíz ország között hét Ázsiában található.[20] Óceániában is létezik természetesen kiberbűnözés, az Európában létező problémák ott sem ismeretlenek, a két térség közötti kapcsolódás e tekintetben azonban nem jelentős.

A kiberbűnözés és a terrorizmus kapcsolata

A jelentés egyaránt foglalkozik a kiberbűnözés és a terrorizmus kapcsolatával. Egyes terrorszervezetek ugyanis aktívan használják az internetet propaganda terjesztésére és terrorakciókra történő buzdításra. Ez kezdetben a közösségi hálózatokon történt, a bűnüldöző hatóságok közbeavatkozása következtében azonban a Facebook és Twitter kommunikációt a terrorista szervezetek titkosított üzenetküldő alkalmazásokra cserélték. A sokszor a Darkneten futó alkalmazások használatával a kívülállók ugyanis kevésbé képesek megzavarni kommunikációs tevékenységüket.

Az elmúlt években felmerültek aggodalmak abban a tekintetben, hogy egyes terrorszervezetek képessé válhatnak a kritikus infrastruktúrák ellen elkövetett kibertámadások kivitelezésére. Igaz ugyan, hogy a terrorszervezetek esetén is egyre komolyabb mértékben beszélhetünk rendelkezésre álló informatikai szakértelemről (az „Iszlám Állam" e tekintetben kétségtelenül túltett valamennyi elődjén), a kibertámadások elkövetéséhez szükséges informatikai eszközeik és szakértelmük azonban még mindig erősen korlátozott. A jelentés szerint továbbra sem képesek az ehhez szükséges saját informatikai „fegyvereik" kifejlesztésére, ugyanakkor alacsonyabb szintű támadásokat véghez tudnak vinni.

A kriptodevizák használata lehetőséget teremt a terrorista szervezetek számára arra, hogy rendszeres banki ellenőrzés nélkül mozgathassák anyagi eszközeiket az egyes országok között. 2017 végétől az „Iszlám Állam" megpróbálta kihasználni az ebből származó előnyöket és egyúttal különböző honlapokat kezdett üzemeltetni annak érdekében, hogy a szervezetet kriptopénzekkel is támogatni lehessen. Ugyanakkor az Európában elkövetett támadások egyike esetén sem tűnik úgy, hogy azok finanszírozásában kriptopénzek is szerepet játszottak volna. Ezen szervezetek finanszírozása alapjaiban továbbra is a hagyományos csatornák használatán keresztül történik.

[20] Symantec: 'Facts and figures', Internet Security Threat Report (ISTR), In: Europol: Internet Organized Crime Threat Assessment, [online], forrás: europol.europa.eu, [2019.06.22.]

Az „SVKK Elemzések” 2003 óta a kutatóintézet munkatársainak tematikus szakpolitikai elemzéseit megjelentető időszakos kiadvány, melyben a szerzők független kutatói álláspontjukat közlik.

Az NKE Eötvös József Kutatóközpontjának Stratégiai Védelmi Kutatóintézete független szakpolitikai kutatóintézet, a kiadványaiban megjelenő elemzések, álláspontok, vélemények nem feltétlenül tükrözik a szerkesztőség vagy a kiadó véleményét. Az elemzésben foglalt információk, adatok, megállapítások tájékoztatás céljából készültek.

Kiadó: NKE Eötvös József Kutatóközpont Stratégiai Védelmi Kutatóintézet

Szerkesztés és tördelés:
Csiki Varga Tamás, Tálas Péter

A kiadó elérhetősége:

1581 Budapest, Pf. 15.

Tel: 00 36 1 432-90-92

E-mail: svkk@uni-nke.hu

2019 – : NKE Stratégiai Védelmi Kutatóintézet Elemzések (ISSN 2063-4862)

2012–2019: NKE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4862)
2011–2012: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)
2007–2011: ZMNE Stratégiai Védelmi Kutatóintézet Elemzések (ISSN 2063-4854)
2003–2007: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)