Magyar Rendészet 2024/4. 163–187. DOI: 10.32577/mr.2024.4.9

A kiberbűnözés jelene és jövője

CSIZNER Zoltán[1]

Az információtechnológia fejlődése hatással van a kiberbűnözés alakulására is. A mesterséges intelligencia elérhetősége, a földrajzi távolságok és határok megszűnése, a virtuális világ biztosította személytelenség vagy a megszerzett vagyonok kriptovalutákba menekítésének lehetősége mindmind új távlatokat nyit a bűnelkövetők számára. A bűncselekmények egy része kizárólag az informatikai eszközökhöz és rendszerekhez kötődik, de nagyobb részük a valós térben is elkövethető deliktumok sajátos végrehajtási módja.

A kibervilág fejlődése az elkövetési magatartások folyamatos megújulását eredményezi, amit a bűnüldözés és a kiberbiztonsági intézkedések, előírások a legtöbb esetben csak követni tudnak. A hatékony megelőzéshez nélkülözhetetlen a várható veszélyforrások és trendek feltárása, aminek egyik alapja az aktuális bűnügyi helyzet és a bűnözőket segítő körülmények megismerése. Ehhez nyújtanak segítséget azok az éves értékelések, amelyeket az FBI, a BKA és az Europol évek óta rendszeresen elkészít. A három értékelő jelentésben szereplő megállapítások, az újszerű jelenségek és a várható kihívások bemutatása irányt mutat a kiberbűncselekményekkel foglalkozó szakembereknek, és talán az átlagos internethasználók számára is hasznos információkkal szolgál az áldozattá válás elkerülése érdekében.

Kulcsszavak: internet, kiberbűnözés, kriptovaluta, online csalás, adathalászat, gyermekpornográfia

Mielőtt sok szakember felkapná a fejét, hogyan lehet a kiberbűnözés jövőjét elemezni, leszögezem az elején, hogy nem vállalkozom a lehetetlenre. Osztom azt az álláspontot, hogy egy olyan dinamikusan fejlődő és sok ismeretlenes tényezővel rendelkező területről beszélünk, amelynek pontos alakulását, fejlődését még csak jósolni is felelőtlenség. De ahhoz, hogy valamiféle választ tudjunk adni erre a kihívásra, mégis csak elkerülhetetlen előre tekinteni.

A kibertérben elkövetett bűncselekmények száma rohamosan nő, mint ahogyan azok típusai, a veszélyeztetett értékek, a lehetséges sértettek vagy az elkövetési magatartások is folyamatosan változnak, bővülnek.

A jelen helyzet megismeréséhez három nemzetközi tanulmányt hívok segítségül, az Europol,[2] az amerikai FBI IC3,[3] illetve a német BKA[4] egy-egy értékelő elem-

[1] R. ezredes, mb. tanszékvezető, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Kiberbűnözés Elleni Tanszék, e-mail: csizner.zoltan2@uni-nke.hu

[2] Europol: European Police Office, Európai Rendőrségi Hivatal, az EU-n belüli rendőrségi együttműködés legfontosabb intézménye.

[3] FBI IC3: Federal Bureau of Investigation Internet Crime Complaint Center, Szövetségi Nyomozó Iroda Kiberbűncselekmények Elleni Panaszközpont (USA).

[4] BKA: Bundeskriminalamt, német Szövetségi Bűnügyi Hivatal.

zését. Mindhárom tanulmány olyan, évek óta működő rendszerek adatait elemzi, amelyek a kiberbűnözéssel foglalkozó szakmai egységek tapasztalataira és megállapításaira épülnek.

A kibertérben megvalósuló bűncselekmények bemutatása mellett hasznos információ az érdeklődők számára a nemzetközi szakirodalomban egységesen alkalmazott angol kifejezések bemutatása is, amelyek ismerete és használata elengedhetetlen a kiberbűnözés vizsgálata során.

IOCTA 2024 (Europol)

Az Europol 10 éve, 2014-től évente készíti el a kiberbűnözéssel kapcsolatos kiadványát, amely az egyik legátfogóbb elemzés Európában. A legújabb IOCTA, az internetes szervezett bűnözés fenyegetésértékelése 2024. július 22-én került ki az Europol honlapjára.[5]

A tanulmány egy bevezető elemzés és az elmúlt év változásainak rövid összefoglalása után négy fejezetben mutatja be az aktuális kihívásokat, míg egy ötödikben a várható fejlődési irányokat és a szükséges intézkedéseket részletezi.

Kriptovaluták és a dark web

A kriptovaluták jelenléte az elmúlt évben is érzékelhető volt mind a valós térben megvalósuló bűncselekmények esetében, mind a kiberbűnözésben. Közülük is a befektetési csalásoknál és a pénzmosásoknál volt meghatározó a szerepük.

Ugyan a legelterjedtebb kriptovaluta továbbra is a bitcoin, de a bűnözők ezt már sok esetben egyéb *altcoinra*[6] is átváltják, és előnyben részesítik az áringadozásnak kevésbé kitett *stablecoinokat*.[7] Az árfolyam stabilitásával szemben a bűnözők szemszögéből nézve ugyanakkor ezeknél hátrány, hogy a szolgáltatók sok esetben – a szerződésben foglaltak szerint – bűncselekmény gyanúja esetén lehetővé teszik a bűnüldöző hatóságoknak a pénztárcák befagyasztásának kezdeményezését. Például az eljárások során a nyomozók több Tetherrel (USDT[8]) találkoztak a Tron blokkláncon, mint az Ethereumon, aminek az alacsony tranzakciós díj is oka lehet.

---

5 Europol 2024a.

6 *Altcoin:* a Bitcoinon kívül minden más kriptovalutára alkalmazott kifejezés, amelyek kialakítása és funkciója megegyezik, és számuk folyamatosan gyarapodik.

7 *Stablecoin:* olyan kriptovaluta, amelynek értéke stabilabb, mivel az egy másik referenciaeszköztől (pl. tőzsdén kereskedett áru, arany, másik kriptovaluta) függ.

8 Az USDT kriptovalutát a Tether Limited hozta létre azzal a céllal, hogy az internet minden időben stabil árfolyamú, digitális dollárja legyen. Minden token 1.00 USD értékű, amely mögött 1.00 USD fizikai dollárfedezet van.

A zsarolóvírus-támadások elkövetői jellemzően továbbra is bitcoinban kérik a váltságdíjat (ennek egyik oka lehet, hogy az áldozat is könnyebben fér hozzá), de egyéb *altcoin* (például Monero) is megjelent már.

A bűnös forrásból származó kriptovaluták tisztára mosására egyre elterjedtebbé váltak a feketegazdaság illegális bankrendszereinek *(underground banking)* igénybevétele. Nőtt a kriptohitel- és -betéti kártyák (például Coinbase, Crypto.com, Wirex) használata is, amivel az ATM-nél gyorsan készpénzre tudják váltani a kriptovalutát.

A bűnös eredetű kriptovaluták tisztára mosásának egy másik módja a csereszolgáltatások igénybevétele, amelynek növekedését észlelték is 2023-ban. Ennek során az ismertebb – és jellegükből adódóan könnyebben nyomon követhető vagy instabilabb – kriptovalutákat az értékmegőrzés érdekében *stablecoinra* vagy a titkosság megtartása érdekében *privacycoinra*[9] (például Monero) váltják át.

A kriptovaluta-szolgáltatók (CASP – *crypto-asset service providers*) egy része az Európai Unió (EU) joghatóságán kívül működik, így irányukba az adatkérések továbbra is nehézkesek, és gyakran csak elhúzódó jogsegélykérelmek útján teljesíthetők.

A kriptovalutákkal való visszaélések ellen az EU jogalkotással válaszolt, így 2023. május 31-én rendelet született a pénzátutalásokat és egyes kriptoeszköz-átruházásokat kísérő adatokról és az (EU) 2015/849 irányelv módosításáról.[10] Ennek értelmében többek között már a kriptovaluta-szolgáltatók is kötelesek lesznek jelenteni a gyanús tranzakciókat és azonosítani ügyfeleiket. A Rendelettel összefüggésben, 2024. januárban az Európai Bankhatóság (EBA – European Banking Authority) kiterjesztette a pénzmosás és terrorizmus finanszírozási kockázati tényezőkről szóló iránymutatását a kriptovaluta-szolgáltatókra is,[11] ami segít azonosítani számukra a gyanús és jelentésre kötelezett tranzakciókat.

A jogalkotók az intézkedésektől hatékonyabb fellépést és gyorsabb adatszolgáltatást várnak, feltéve persze, ha az elkövetők az EU joghatósága alá tartozó területen kereskednek.

A dark web továbbra is a legelterjedtebb fóruma az illegális kereskedelemnek és kommunikációnak. 2023-ban is a TOR[12] volt a dark web uralkodó elérési módja, de mellette ismert az Invisible Internet Project (I2P) is, amelyről azt hirdetik, hogy a legbiztosabb védelmet nyújtja a bűnüldöző hatóságok elől.

A dark web piactereinek adminisztrátorai egyre rövidebb ideig működtetnek egy-egy marketet, ezzel igyekeznek elkerülni, hogy a bűnüldöző szervek látókörébe kerüljenek.

---

[9] *Privacycoins* (adatvédelmi érme): olyan kriptovaluta, amely az átlagosnál sokkal jobban garantálja a használattal kapcsolatos adatok védelmét, titkosságát, ami miatt egyes országban illegális is. Ehhez a kriptovalutákkal való kereskedéshez használt alapvető funkciókat további biztonsági rétegekbe csomagolják, és így anonimizálják a tranzakciókat és/vagy az egyes pénztárca-tulajdonosok személyazonosságát.

[10] Az Európai Parlament és a Tanács (EU)2023/1113. rendelete a pénzátutalásokat és egyes kriptoeszköz-átruházásokat kísérő adatokról és az (EU) 2015/849 irányelv módosításáról.

[11] A pénzmosási és terrorizmusfinanszírozási kockázati tényezőkről szóló iránymutatásokat módosító EBA/GL/2024/01. számú iránymutatások. (2024. 01. 16.)

[12] TOR: *the onion router,* hagyma elosztó, a dark web eléréséhez szükséges speciális böngészők egyike.

A nagyobb piactereket egyre gyakrabban váltják fel a kisebb, egyszállítós (egyszemélyes) üzletek *(single-vendor shop)*. Ezek egyrészt speciálisabbak, másrészt az eladóknak így nem kell tranzakciós díjat fizetniük, és egyszerre több piactéren is jelen lehetnek.

Az IOCTA 2024 az ismertebb illegális fórumok közül az Exploitot, az XSS-t, a BreachForums-ot a CryptBB-t és a Dreadet nevesíti, ahol hackelési ismereteket osztanak meg, ellopott adatokkal, hackereszközökkel és kiberbűnözési szolgáltatásokkal kereskednek.

Ezek közül például a kimondottan kiberbűnözők számára működtetett, zárt CryptBB fórum a kiberbűnözési szolgáltatások széles skáláját kínálja, így távoli asztali protokoll (RDP, *Remote Desktop Protocol*) hozzáférés értékesítését, bérbeadó hackereket, behatolási tesztelést vagy hibajelentési szolgáltatásokat különböző piactereken.

A tanulmány kiemel pár dark webes marketet is (Genesis, RAMP, WWH-Club, Russian Market), amelyek az elmúlt évben jelentős forgalmat bonyolítottak le.

Ezek közül az orosz RAMP korábban illegális gyógyszer-kereskedelemmel foglalkozott a 2017-es bezárásáig, majd 2021-ben újraéledt, és már nemcsak orosz nyelven, hanem angol és mandarin nyelven is. 2023-ban zárt, szigorú hozzáférési feltételekhez kötött piactérként működött, amely elsősorban zsarolóvírusokkal kereskedett.

Az elmúlt években újonnan megjelenő marketek közül a KKKSecforum, a Viceforum, a Germania, a Yomi no Kuni és a Kerberos voltak a leggyakrabban bejelentett dark webes kereskedői platformok. Ezeken is széles skálán elérhetők az illegális áruk és szolgáltatások, a kábítószerektől a digitális cikkeken át az ellopott adatokig. A fentiek közül a Yomi no Kuni a gyermekek online szexuális kizsákmányolására (CSE, *child sexual exploitation*) összpontosít.

Az illegális kereskedelemben egyre nagyobb szerepet kap a AI. Mind az AI-eszközök, mind a szolgáltatások jelen vannak a dark weben. Így például az Only Fake szolgáltató az IA által generált hamis identitásokat, azonosítókat árul. Ezek felhasználhatók a banki csalásokhoz, pénzmosáshoz vagy bármilyen olyan illegális cselekményhez, amelyhez személyazonosság igazolására lenne szükség.[13]

Az elkövetőkkel összefüggésben megállapítja, hogy az úgynevezett „elkövetői életciklus", azaz az egy-egy illegális tevékenységet folytató oldal (piactér, fórum) elérhetősége, működése folyamatosan csökken a bűnüldöző szervek hatékonyabb fellépéseinek eredményeként. Ez egyben töredezett, állandóan változó, nehezebben kiismerhető és utólag nehezebben felderíthető környezetet jelent.

[13] Cox 2024.

Kibertámadások

A kibertámadások közül 2023-ban is a *ransomware,*[14] azaz a zsarolóvírusos támadások jelentették a legnagyobb kihívást, és ezek okozták a legnagyobb károkat is. A ransomware-támadások 2023-ban jelentős emelkedést mutattak, az áldozatok száma 55,5%-kal nőtt meg világszerte. Ugyanakkor 2023 utolsó negyedévéhez képest az új esztendő első negyedévében 22%-os csökkenést lehetett megfigyelni, ami biztató tendencia.[15]

Ennek egyik oka, hogy a bűnüldöző szervek érzékelhető csapásokat mértek több RaaS[16] csoportra (például Hive, LockBit), míg a másik ok a kiszivárgott ransomware-forráskódok volt, amelyek együttesen érzékelhető hatást gyakoroltak a *ransomware* szolgáltatásának piacára.

Egy-egy RaaS-csoport elleni hatósági fellépésben az egyik legérzékenyebb pont az informatikai infrastruktúrájuk eltávolítása, elérhetetlenné tétele. Ez egyben azt is jelenti, hogy a velük kapcsolatban álló leányvállalatok[17] is elvesztik a hozzáférést a szolgáltatáshoz, azaz megszűnik a befolyásuk a zsarolt vállalatok felett. A forráskódok kiszivárgásával pedig a támadott szervezetek gyakorlatilag váltságdíj fizetése nélkül is hozzáférhetnek az addig zárolt adataihoz.

A ransomware-támadások során az elkövetők elsősorban a kis- és középvállalkozásokat veszik célba, mivel a nagyobb vállalkozások többsége már megfelelő szintű és minőségű kibervédelmi rendszerrel rendelkezik. A támadások előtt a célvállalkozás mérete mellett feltérképezik a várható fizetési hajlandóságot és a támadott rendszer kompromittálásához szükséges erőforrásokat is, és ezek figyelembevételével döntenek.

A támadásokhoz sok esetben alkalmaznak olyan hackereket is, akik kimondottan hálózatok védelmi rendszerének feltörésére szakosodtak, amivel jogosulatlan hozzáférést szereznek, majd az így megismert belépési adatokat jellemzően a dark weben értékesítik. Ezeket a nemzetközi szakirodalom kezdeti hozzáférési brókereknek, ügynököknek (IAB, *initial access broker*) nevezi.

Az elkövetők többrétegű zsarolási taktikát alkalmaznak, azaz több fenyegetési pontot igyekeznek alkalmazni az áldozataiknál a fizetési hajlandóság fokozásához. A zsarolások során – a biztonsági másolatokból eredő védettség miatt – csökken

---

[14] A *ransomware* a *malware-ek* egy fajtája, amely az informatikai rendszerbe települve az ott tárolt adatok zárolásával (illetve újabban már az illegális megszerzésével is) olyan helyzetbe hozza az elkövetőt, hogy a támadott rendszer üzemeltetőjét fenyegetni és zsarolni tudja. A *malware* ezzel szemben magába foglalja az összes olyan káros programot, amely az üzemeltető tudta nélkül az informatikai rendszerre települ, így például ide tartoznak a kémprogramok, a kéretlen reklámok vagy a vírusok, férgek.

[15] The Drop in Ransomware Attacks in 2024 and What it Means 2024.

[16] RaaS: *ransomware-as-a-service* – az erre szakosodott bűnözői csoportok tevékenysége, amikor a ransomware-támadáshoz szükséges forráskódokat üzleti alapon, quasi szolgáltatásként értékesítik, miközben a támadások fontos adatait saját maguk tárolják. Egy-egy RaaS-csoport jellemzően 10–30%-os jutalékot kér az általa átadott *ransomware-ek* felhasználásával befolyt váltságdíjakból.

[17] Azok a bűnözői csoportok, amelyek a RaaS szolgáltatását igénybe véve magát a zsarolóvírus telepítését és a zsarolást ténylegesen elkövetik, és akik a háttér-infrastruktúrán tárolt adatok (különösen a megfertőzött rendszerek visszafejtési kódjai) miatt erős függőségben állnak a RaaS-sal.

a tartalmak zárolása, helyette sokkal inkább a megszerzett adatokkal való visszaélések, azok nyilvánosságra hozatala jelentik a hatásos fenyegetést. Ezek mellett előfordul a szolgáltatásmegtagadásos (DoS, *denial-of-service*), illetve elosztott szolgáltatás-megtagadásos (DDos – *distributed denial-of-service*) támadásokkal való fenyegetés is, amely szintén érzékenyen érinti a vállalatokat.

2023-ban a legnagyobb ransomware-forráskódok (például Conti, LockBit és HelloKitty) kiszivárgása és a hatóságok eredményes műveleteinek hatására töredezetté vált a piac, és ebből adódóan át is alakult. Felértékelődött az IAB-k szerepe, és egyes leányvállatok az önállósodás útjára lépve már önálló ransomware-változatokat fejlesztettek ki. Ezzel függetlenítették magukat a RaaS-csoportoktól, így sem a forráskódok kiszivárogtatásától vagy a háttér-infrastruktúra elvesztésétől nem kell tartaniuk, és az egyedi változat miatt jobban védettek a bűnüldöző hatóságokkal szemben is. Az önállósodások miatt nagyobb harc indult el az RaaS-csoportok részéről a szolgáltatásukra még mindig igényt tartó leányvállalatokért. Ennek egyik példája, hogy a 2023 januárjában felszámolt Hive[18] volt ügyfeleinek elcsábítására a BlackCat hajlandó volt az általánosan elfogadott 70%-os részesedés helyett 80–90%-os kifizetést is megadni az általa biztosított *ransomware* felhasználásával beszedett váltságdíjakból a vele szerződő leányvállalatoknak.[19]

2023-ban a *LockBit* volt a legtermékenyebb ransomware-szolgáltató a piacon, amelyet 2024 februárjában egy 10 országot (Egyesült Királyság, Hollandia, Németország, Finnország, Franciaország, Svájc, Ausztrália, Egyesült Államok, Lengyelország és Ukrajna) érintő nemzetközi együttműködés eredményeként felszámoltak a hatóságok. A Cronos fedőnevű művelet az Egyesült Királyság nyomozására épült, amelyet az Europol és az Eurojust koordinált. A Cronos eredményeként 34 szervert iktattak ki, 2 személyt fogtak el és további három ellen elfogató parancsot adtak ki, valamint több mint 200 kriptovaluta-fiókot fagyasztottak be.[20] A kiberbűnözés elleni harc sajátossága, hogy egy-egy felderítés leggyakrabban csak átmeneti sikereket eredményez. Sajtóhírek szerint a megzavart LockBit öt nappal a műveletet követően új infrastruktúrán újraindította tevékenységét, és ismételt támadásokat helyezett kilátásba.[21]

A *ransomware-ekkel* zsaroló csoportok közül 2023-ban a Play, a Royal, a Rhysida, Cl0p és a 8base merült fel a leggyakrabban, amelyek közül a Play és a Royal már 2022-ben is felbukkantak, a Rhysida 2023 közepén jelent meg, és valószínűsíthetően korábban felszámolt ransomware-csoportok reinkarnációi.

A C10P 2023 májusában a MOVIEit felügyelt fájlátviteli szoftver (MFT, *managed file transfer*[22]) nulladik napi sebezhetőségeit[23] használta ki, miután nem sokkal ko-

[18] Europol 2023a.
[19] What Is BlackCat Ransomware? 2023.
[20] Europol 2024b.
[21] Ilascu 2024.
[22] MFT: az adatok biztonságos, automatizált átvitele egy központi megoldáson keresztül, amely segít a szervezeteknek kiküszöbölni a duplikált, nem biztonságos eszközöket.
[23] A gyártó által telepített szoftverek még fel nem fedezett hibáinak és védelmi hiányosságainak összefoglaló neve.

rábban sikeres támadást hajtott végre a GoAnywhere MFT ellen is.[24] A C10P-ről azt feltételezik, hogy technikailag fejlett, és olyan csúcskategóriás IAB-kal áll kapcsolatban, akik képesek a nulladik napi sebezhetőségek feltárásával lehetővé téve számára, hogy kifinomult és időigényes MFT elleni támadásokat hajtson végre. Az értékelés alapján mindenképp olyan bűnözői csoport, amely potenciális fenyegetést jelent a jövőben is.

A fejlődésük mellett több ransomware-csoport ellen is sikerült eredményesen fellépni. Így például nemzetközi bűnügyi együttműködés keretében 2023 februárjában a DoppelPaymer,[25] októberben a RagnarLocker[26] csoport prominens tagjait fogták el.

A *ransomware-hez* hasonlóan a *malware-ek* világában is egyre elterjedtebb a bűnözői csoportok részéről a szolgáltatás jellegű (MaaS – *malware-as-a-service*) tevékenység. 2023-ban ezek között a QakBot leépítése volt az egyik legjelentősebb eredmény. A QakBot malware 2007 óta volt ismert, és mintegy 700 000 számítógépet fertőzött meg. A széles körű elterjedését jellemzi, hogy közel 30 országban észleltek olyan fertőzött szervereket, amelyek lehetővé tették a *malware-ek* globális szintű működését. A QakBot infrastruktúráját 2023 nyarán sikerült egy nemzetközi művelet eredményeként kiiktatni, amit az Europol számítástechnikai bűnözés elleni közös akciócsoportja (J-CAT, Joint Cybercrime Action Taskforce[27]) is támogatott. A műveletben 7 ország (Franciaország, Németország, Lettország, Hollandia, Románia, Egyesült Királyság, Egyesült Államok) bűnüldöző hatóságai vettek részt, és az informatikai háttér leépítése mellett 8 millió euró értékű kriptovaluta lefoglalását is eredményezte.[28]

2023 végére az IcedID, a Pikabot, a SmokeLoader, a SystemBC és a Danabot lett a QakBot elérhető és széles körben használt alternatívája, míg töretlen népszerűségnek örvend a 2020 óta piacon lévő Redline Staler is. Utóbbi képes többek között a bejelentkezési és hitelesítő adatok kinyerésére, begyűjti a böngészőkben, csevegési naplókban és helyi fájlokban tárolt hitelesítési *cookie-kat* és kártyaszámokat. Az Europol adatai szerint a szolgáltatáshoz a bűnözők havi 140 euró, illetve évi 740 euró díj megfizetésével férhetnek hozzá.

A kiberbűnözők másik elterjedt elkövetési módszere a legális behatolásteszt-keretrendszerekkel *(penetration testing frameworks)* való visszaélés. A legális tesztelés esetén ezek segítenek a rendszer gyenge pontjait azonosítani, amivel fejleszthető a hálózat és a környezet ellenálló képessége. A bűnözők ugyanúgy a rendszer gyenge pontjait keresik az illegális behatolás érdekében. Ehhez leggyakrabban a Cobalt Strike, Metasploit, Mimikatz programokat használják. Ráadásul ezeknek a legális teszteknek a legújabb verziója már az AI által támogatott, így például a PentestGPT

[24] Gihon–Tayar 2023.
[25] Europol 2023b.
[26] Europol 2023d.
[27] Lásd: www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce
[28] Europol 2023e.

képességei már sokkal többre képesek, mint a hagyományos verziók, és sokkal hatékonyabban felhasználhatók az információs rendszerek kompromittálására.

A Cobalt Strike a Fortra (korábban HelpSystems) által, több mint egy évtizeddel ezelőtt kifejlesztett, népszerű szimulációs és behatolásvizsgálati eszköz, amely az IT-biztonsági szakértők számára lehetőséget kínál a biztonsági műveletek és az incidensekre adott válaszok gyenge pontjainak azonosítására. A bűnözők feltört másolatokat szereztek a szoftverből, így az egyik legszélesebb körben használt eszközzé vált az adatlopásban és ransomware-támadásokban.

Az Europol 2024. június végén hajtotta végre a Morpheus fedőnevű nemzetközi műveletet, amely során közel 600, a bűnözők által üzemeltett Cobalt Strike szervert iktattak ki. Az Egyesült Királyság által 2021-ben indított közös nyomozásban Ausztrália, Kanada, Németország, Hollandia, Lengyelország, Németország, az Egyesült Államok, Bulgária, Észtország, Finnország, Litvánia, Japán és Dél-Korea hatóságai, tisztviselői vettek részt, miközben hatékony segítséget kaptak a magánszektor (a BAE Systems Digital Intelligence, a Trellix, a Spamhaus, az abuse.ch és a Shadowserver Foundation) képviselőitől is.[29]

A *malware-ek* egyik sajátos területe a kriptojacker-tevékenység, amely során az elkövető azért támad meg informatikai eszközöket, hogy azokat – a tulajdonos tudta nélkül, de az ő költségén – kriptovaluta-bányászatára használja. Az IOCTA 2024 megemlíti az Europol és az ukrán nemzeti rendőrség közös akcióját, amelyben egy kriptojackert fogtak el, aki közel 1,8 millió euró értékben bányászott illegálisan kriptovalutát. A gyanúsított és tevékenységének felderítéséhez nélkülözhetetlen volt a magánszektorral való együttműködés. A gyanús tevékenységet ebben az esetben az érintett felhőszolgáltató észlelte, aki ezt megosztotta az Europollal, és így sikerült az érintett nemzeti hatóságnak a szükséges intézkedéseket eredményesen végrehajtania.[30]

A gyermekek szexuális kizsákmányolása

Az interneten megjelenő (CSAM, *child sexual abuse material*[31]) növekvő mennyisége folyamatos kihívás elé állítja az ezzel foglalkozó bűnüldöző hatóságokat.

A CSAM-ek nagy részét saját előállítású, közvetlen forrású tartalomként (SGEM, *self-generated explicit material*)[32] azonosítják. Ezeket a fiatalkorú szereplők saját magukról készítik önszántukból, vagy szexuális célú, hamis tartalmú kapcsolatépítést, behálózást *(sexual grooming)* követő zsarolás eredményeként. Az IOCTA 2024 érté-

[29] NCA 2024.

[30] Europol 2024c.

[31] CSAM: a gyermekek szexuális zaklatását bemutató, ábrázoló tartalmak, amelyek lehetnek hagyományos készítésű képek vagy videók, illetve a AI által generált tartalmak.

[32] Nemzetközileg elfogadott kifejezés, amely a Luxembourgi Irányelvek (Terminológiai Iránymutatások a gyermekek szexuális kizsákmányolással és szexuális zaklatással szembeni védelmére) jelenleg is zajló felülvizsgálata során változhat.

kelésében a fiatalkorúak által önmagukról önkéntesen készített tartalmak akkor minősülnek CSAM-nek, ha a társak kölcsönös beleegyezésén alapuló cseréken túl harmadik félnek is továbbítják, azaz terjesztik azokat.

(Meg kell jegyezni, hogy gyermekpornográfiát tiltó és szankcionáló hazai jogszabály[33] nem ismer olyan kivételt, amely a 18 év alatti személyről készült pornográf felvétel készítését, megszerzését vagy annak készítésére való felhívást bármely körülmény esetén büntetlenné minősítené. Még abban az esetben sem, ha ezt például két 17 éves, érzelmi alapokon nyugvó, rendszeresen szexuális életet élő fiatal, kölcsönös beleegyezéssel, saját felhasználásra követné el.)

A határokon átnyúló gyermekbántalmazások elkövetői (TCSO, *transnational child sex offenders*) előszeretettel utaznak a leendő áldozataik lakó- vagy tartózkodási országaiba – ahol a helyi viszonyok miatt kisebb a lebukásuk és az áldozatok azonosításának a kockázata –, és helyi segítők közreműködésével kerülnek kapcsolatba áldozataikkal. Ezek az elkövetők gyakran állnak összeköttetésben egymással, chatszobákban és fórumokon információkat, tapasztalatokat cserélnek, megvitatják az elkövetett visszaéléseket és fantáziákat, és a saját maguk által készített CSAM-eket egymás között terjesztik, hozzáférhetővé teszik. Az ilyen tartalmak között kiemelkedően magas az úgynevezett ismeretlen vagy első generációs[34] CSAM-ek száma.

Az utazások előkészítéseit, a helyi áldozatok felkutatását és bántalmazásuk megszervezését, a bántalmazásokról készített tartalmak megosztását jellemzően bűnszervezetben követik el, egyes mozzanatai mind a szervezői, mind a bántalmazói oldalról mélyen konspirált, többnyire zárt és szigorúan ellenőrzött chatszobákban zajlanak.

A közvetlen fizikai kontaktus mellett hasonlóan veszélyes és ártalmas az úgynevezett élő közvetítéses távoli gyermekbántalmazás (LDCA, *live-distant child abuse*), amely során ellenszolgáltatásért egy távoli helyen lévő gyermeket valós időben bántalmaznak szexuálisan az ott jelen lévő közreműködők, az őket online összeköttetésben megfigyelő megrendelő kérése szerint. Ezen cselekmények rögzítése, majd az így készített tartalmak megosztása, értékesítése is gyakran előfordul.

A fórumokon belül külön figyelmet fordítanak a bántalmazásokkal kapcsolatos információkon túl az egyes technikai védelmi intézkedésekre (OpSec, *operational security*), konspirációs szabályokra is. Megfigyelhető, hogy az illegális oldalak, fórumok hatósági eltávolítására készülve adminisztrátorok tükörwebhelyeket hoznak létre, és így egy intézkedést követően rövid időn belül új helyen képesek visszaállítani a hatóságok által eltávolított tartalmat. Az elkövetők egymás közötti kommunikációjára és a CSAM-ek cseréjére egyre gyakrabban alkalmazzák a végpontok közötti titkosítást biztosító E2EE-platformokat.

A CSAM-mel való kereskedéssel párhuzamosan gyakori bűncselekmény a pénzfizetésre kényszerítő zsarolás, amikor a képen szereplő fiatalkorú szégyenérzetből tel-

[33] A Büntető Törvénykönyvről szóló 2012. évi C. törvény 204. §-a.

[34] Azok a gyermekpornográf tartalmak, amelyekkel a hatóság először találkozik, azaz korábban még nem vizsgálták.

jesíti a zsaroló pénzkövetelését. Természetesen a pénz mellett az áldozatoktól az elkövetők sok esetben még több CSAM saját maguk általi előállítását és megküldését is követelik.

Zsarolások elkövetői között fiatalkorúak is előfordultak olyan erőszakos, szexuális tartalmakat megosztó online csoportok tagjai között is, ahol a – jellemzően hasonló korú fiatalokból álló – társaság karizmatikus személyiségű vezetője megtévesztéssel vagy más manipulációval engedelmességre kényszeríti az új tagokat is, akik félelemből vagy az új közösségnek való megfelelési kényszerből extrém tartalmakat osztanak meg magukról. Később újabb, részben személyes információkkal kiegészült zsarolással még több hasonló tartalom megosztását érik el, aminek a végén már nyíltan szexuális tartalmú CSAM-eket is megosztanak.

Egyre fokozódik a mesterséges intelligencia (AI, *artificial intelligence*) által generált CSAM-ek előfordulása. A technológia fejlődésével a végtermék egyre élethűbb, egyre jobban hasonlít az eredeti anyagokra, és sokszor csak alapos vizsgálat útján lehet megállapítani, hogy azt mesterségesen állították elő. Ugyan ezekben az esetekben nincs szó ténylegesen bántalmazott valós gyermekről, azonban a tartalom ugyanúgy tárgyiasítja és szexualizálja a fiatalkorúakat – még ha egy fiktív személyiségen keresztül is teszi mindezt –, és így mindenképp tiltandó és üldözendő. A fiatalkorúak közvetlen védelme mellett az AI által generált tartalmak más veszélyforrások miatt sem lehet eltűrt. Mivel nehéz megkülönböztetni a valós tartalmaktól, hosszabb vizsgálatot igényel az eredetük megállapítása, és addig a mesterségesen előállított tartalom esetén olyan felesleges és elpazarolt energia a vélt sértettek, azaz az ábrázolt fiatalok azonosítására fordított munka, amelyet eredményesen lehetne a valós sértettek azonosítására és felkutatására használni. Az AI alkalmazása nem igényel magasabb szintű informatikai képzettséget vagy eszközparkot, így várhatóan mind az elkövetők száma, mind az így előállított CSAM-tartalmak mennyisége is emelkedni fog. Ez hatványozottan nehezíti majd a ténylegesen bántalmazott gyermekek azonosítását és a bántalmazók felderítését.

A fiatalok körében – a CSAM-ek újszerű módszerrel történő készítése és terjesztése mellett – az AI segítségével előállított tartalom egyszerre lehet alkalmas zaklatásra és zsarolásra is, mint ahogy erre az FBI is figyelmeztetett 2023 nyarán.[35]

Spanyolországban 2023 őszén került az ügyészség elé az az ügy, amelyben egy 15 és egy 13 éves fiú a lánytársaikról készített ártalmatlan fotókat, az AI segítségével, mintegy 20 esetben szexuális tartalmú képpé alakította át, majd ezeket a neten megosztották. Zsarolás ebben az ügyben nem történt, de a fényképen szereplő áldozatok által megélt lelki trauma jelentős volt. A spanyol ügyészség elsősorban azt vizsgálja, hogy ezzel a magatartással megvalósult-e bűncselekmény.[36]

[35] FBI 2023a.
[36] Spanish Prosecutor to Probe AI-Generated Images of Naked Minors 2023.

Online fizetési csalások

Mind az EU-n belül, mind azon kívül az egyik legdinamikusabban fejlődő fenyegetés az online csalási módszerek (OFS, *online fraud schemes*), amelyeket több elkövetési magatartás jellemez.

Ezek közül az adathalászat *(phishing)* a legelterjedtebb, amely gyakorlatilag az alapját jelenti az online térben megvalósított legtöbb csalásnak és zsarolóvírusos támadásnak is. 2023-ban a szöveges *(SMS/text phishing)* volt a leggyakoribb típus, de új fenyegetésként megjelent a QR-kódos *(quishing)* típusú adathalászat is. Utóbbinál egy hamis QR-kódot küldenek ki a szöveges hivatkozások helyett a leendő áldozatnak, aki ezt beolvasva tölti le a káros vírust.

Az adathalászat kapcsán is egyre inkább terjed annak szolgáltatásként történő értékesítése, amelynek eredményeként egyre több bűnözői szervezet kapcsolódhat be sikeresen az online csalásokba, függetlenül a tagok szakértelmétől.

Példaértékű az az ítélet, amelyet az Egyesült Királyságban szabtak ki a „iSpoof.cc" nevű, adathalász-szolgáltatást nyújtó weboldal üzemeltetetőjére. A weboldal olyan szolgáltatásokat tett elérhetővé bűnözők számára, mint például hamisított hívószámok (VoIP-hamisítások) alkalmazása, előre rögzített üzenetek küldése vagy PIN-kódok ellopása. Az Eurojust[37] által támogatott nyomozás adatai szerint a honlap 16 hónapos működése alatt közel 115 millió euró kárt okozott világszerte, amiből az Egyesült Királyságban 49 millió euró keletkezett. Az eljárásban 184 gyanúsítottat tartóztattak le, és a honlap fő adminisztrátorát a bíróság végül 13 év 4 hónapos szabadságvesztésre ítélte, ami egy kiberbűncselekményhez képest kiemelkedőnek tekinthető.[38]

Az online csalásokban is érzékelhető az AI fejlődése, amelynek egyik kiemelkedő pontja az úgynevezett nagy nyelvi modell (LLM, *large language model*). Ennek eredményeként a program – a sokszori tanítást követően – képes a közölni szánt információt több nyelven, szinte hibátlan nyelvhelyességgel közölni. Ez különösen az emberi tényezőkre épülő online csalások (romantikus, befektetési, vállalati belső levelezés) esetén jelent egyre nagyobb segítséget a bűnözőknek, hiszen a tökéletes nyelvhasználat vagy az igényes fogalmazás a kételkedést és az óvatosságot háttérbe szorítja.

Adathalászattal legegyszerűbben egyes fiókok (banki, levelezőrendszer vagy közösségimédia-felületek) feletti irányítást szerzik meg a bűnelkövetők, és sokszor a megszerzett adatokat tömegesen értékesítik. Az illegális kereskedőfelületeken hirdetett belépési adatok aztán újabb pénzszerzési lehetőségeket biztosítanak, vagy további bizalmas személyes adatok megszerzését teszik lehetővé. Sok pénzintézet emiatt már egyre sűrűbben hárítja az ilyen adatszerzések következményeit az ügyfél felelősségi körébe, amennyiben nem alkalmazott kétfaktoros vagy multifaktoros azonosítási rendszert (2FA/MFA, *two-factor authentication/multi-factor-authentication*). Ezeknél nem elégséges az adott fiókhoz tartozó belépési adatok ismerete,

[37] European Union Agency for Criminal Justice Cooperation, az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége.

[38] Eurojust 2023.

hanem igazolni kell a belépéshez használt eszköz jogosultságát is, például egy időkorlátos, egyszerhasználatos és az eszköz által generált kóddal.

Az elmúlt időszakban az egyik leginkább terjedő csalási módszer a vállalati belső levelezési csalás (BEC, *business email compromise*), ahol elsősorban pénzügyi utalásra jogosult alkalmazottat vagy gazdasági vezetőt céloznak meg valótlan információkkal. A kérésüket gyakran adathalászat útján megszerzett részinformációkkal teszik hitelessé, így például egy tervezett valós utalásnál csak a címzett számlaszámát módosítják a bűnözők a sajátjukéra, vagy a felső vezetőt megismerve, az ő nevében és stílusát utánozva adnak utasítást az utalásra.

A BEC mellett továbbra is jelentős fenyegetést jelentenek a romantikus csalások, ahol az AI fejlődése szintén az elkövetőket segíti. Ezeknél a bűncselekményeknél azonban magas a látencia, jellemző, hogy az áldozatok bejelentési hajlandóságát a szégyenérzetük csökkenti.

Az online kereskedelem térnyerésével együtt 2023-ban nőtt az ezek sérülékenységeit kihasználó skimming-támadások száma is. Ezek során az elkövetők a legális kereskedésben megjelenő ügyfelek kártyaadatait szerzik meg, és azokkal élnek vissza. Ehhez három lépésre van szükség; (1) a webáruház szerveréhez való hozzáférés, behatolás; (2) kártékony kód elhelyezése; (3) a fizetési adatok összegyűjtése. Ennek a támadásnak egyik különös veszélye, hogy az adatok másolása *(skimmelése)* huzamosabb ideig észrevétlen maradhat, hiszen az ügyfél a fizetés után a megrendelt árut megkapja, így nem észlel semmi gyanúsat.

A bankautomatákkal (ATM, *automated teller machine*) kapcsolatos bűncselekmények száma jelentősen csökkent. 2023 első félévében az előző év hasonló időszakához képest 40%-kal kevesebb csalást (5022 helyett 3021) követtek el fizetési terminál ellen, igaz az okozott kár 8%-kal volt magasabb (a 2022. évi 97 millió helyett 105 millió euró). A leglátványosabb eredmény az ATM-ek informatikai rendszere ellen intézett támadások területén tapasztalható, ahol a 2020-as csúcsérték (129 támadás és 1,1 millió euró kár) 2023-ra a töredékére (4 támadás és 2 ezer euró kár) csökkent.[39] Az ATM-ek elleni támadások számának csökkenése – a védelmi intézkedések javulása mellett – a készpénzforgalom csökkenésének is köszönhető, ami ugyanakkor a bűnözőket az online térben megjelenő kereskedelem és fizetési műveletek irányába tereli.

A bűnözők számára az online csalások esetén is kulcskérdés a megszerzett összegek legalizálása. A pénz tényleges származásának elrejtése érdekében előszeretettel alkalmazzák a digitális banki szolgáltatókat, a dark weben jelen lévő, kriptovalutákra alapuló illegális pénzügyi szolgáltatókat, illetve azokat a szolgáltatókat, ahol az ügyfél-azonosítás (KYC, *know your customer*) nem megfelelő színvonalú.

Mindezek mellett a hagyományos pénzmosási technológiák is fellelhetők, amelyek alapja a pénzintézeteknél nyitott folyószámla. Az ehhez szükséges szemé-

[39] EAST 2023.

lyek – akiket a szakirodalom pénzöszvérnek *(money mule)* nevez – adatait több lehetséges módon szerzik meg.

Egy részük saját elhatározásból, és az illegális tevékenység ismeretében adja meg adatait, és részesül a bevételből. Nagyobb részük azonban akaratán kívül válik részesévé a pénzmosásnak. Van, akinek kiszolgáltatott helyzetével (például az orosz–ukrán háború elől menekülő személyek esetében) élnek vissza, van, akinek idős korát kihasználva, magukat banki ügyintézőnek kiadva tévesztenek meg és nyittatnak vele számlát, de egyre gyakrabban fordul elő az ügyfél-azonosítási ellenőrzések AI alkalmazásával történő kijátszása is.

A pénzöszvérek ellen 2023-ban egy több fázisú, összehangolt fellépés is zajlott, amelynek végeredményeként 474 szervezőt és 10 759 pénzöszvért azonosítottak, több mint 10 ezer csalárd tranzakció felderítésével 32 millió euró kárt előztek meg. Az EMMA (European Money Mule Action) fedőnevű műveletben világszerte 27 ország (Európában, Észak-Amerikában, Kolumbiában és Ausztráliában) nyomozó hatóságai és a magánszektor szereplői, pénzintézetek, utazási szolgáltatók, online pénzátutalási szolgáltatók, kriptovaluta-tőzsdék vettek részt az Interpol, Eurojust koordinálása mellett.[40]

A jövő kihívásai és az azokkal kapcsolatos intézkedések

A tanulmány külön fejezetben foglalkozik a kilátásokkal, kihívásokkal és feladatokkal, amelyeket az eddigi elemzésekre építve, hét pontban sorol fel:

- a mesterséges intelligencia (AI) térnyerése a kiberbűnözésben;
- új technológiák megjelenése és elterjedése;
- az E2EE-[41] technológiák fokozott alkalmazása a bűnelkövetők között;
  - a web3 alapelv megjelenésével járó decentralizált, felhasználók által működtetett internet, aminek előnyeit saját hasznukra tudják fordítani a bűnözők is;
  - a PCI DSS[42] szabvány megújulása;
- új RaaS-márkák megjelenése;
- az uniós fizetési rendszerek fokozott védelme;
- a kriptovalutákkal kapcsolatos visszaélések elterjedése, különösen a bitcoin tőzsdén kereskedett alapok (ETF[43]) 2024. januári engedélyezése, illetve a nem helyettesíthető tokenek (NFT[44]) jelentette veszélyek miatt;
- a megelőzés szerepe.

---

40 Europol 2023c.

41 E2EE: *end-to-end encryption,* végpontok közötti titkosítás, ami lehetővé teszi, hogy az üzeneteket vagy adatokat csak a küldő és a címzett értelmezhesse.

42 *Payment card industry data security standard,* kártyatársaságok adatbiztonsági szabványa.

43 EFT: *Exchange-traded fund,* tőzsdén kereskedett alap.

44 NFT: *Non-fungible tokens,* nem helyettesíthető tokenek, amiknek egyedi kapcsolatuk van a hozzájuk tartozó online vagy offline árucikkekkel, mint például egy műalkotással. Az értékük egyedi és változhat, szemben az általános (helyettesíthető) tokenekkel.

Az elemzés felhívja a figyelmet az elkövetők jellemzően fiatal életkorára is, akik esetében nem lehet eléggé hangsúlyozni a bűnmegelőzés szerepét és jelentőségét. A bűnügyi helyzet értékelésekor egyik kockázati tényezőként azonosították a fiatalkorúak növekvő felügyelet nélküli internethasználatát. Ezek a fiatalok nem mérik fel a veszélyt, egyszerű kihívásként élik meg az egyes informatikai védelmi rendszerek kijátszását vagy az adatok megszerzését. Számukra sok esetben ez nem más, mint a kibertérben játszott játék. Nem érzékelik reálisan a valóság határát, és nincsenek tisztában cselekményük bűnös (és büntetendő) jellegével. A korosztályuk tagjai által a valós térben megvalósított jogsértésekkel szemben ezeknél hiányzik a gyors visszajelzés. Míg egy garázdaság, rongálás vagy lopás esetén közvetlenül szembesülhetnek a társadalom rosszallásával, addig a kibertérben ez szinte teljesen elmarad. Sok esetben látens marad a jogsértés, és a felismert bűncselekmények esetén is csak kis arányban tudatosul a fiatalkorú elkövetőben annak törvénysértő volta.

A megelőzésben kiemelt szerepet játszik az EU-n belül a InterCOP[45]-hálózat, amelyet 2023-ban hoztak létre, és az Európai Bizottság által biztosított hároméves Belső Biztonsági Alapból finanszírozzák. Szorosan kapcsolódik az EMPACT 2023. évi operatív cselekvési tervéhez, annak is a kibertámadásokkal foglalkozó prioritásához. A projektet Hollandia vezeti, és az InterCOP-hálózat 26 országból áll.

IC3 Internet Crime Report 2023 (FBI)

Az FBI IC3 egysége közvetlen lehetőséget ad az állampolgároknak az interneten elkövetett bűncselekmények bejelentésére. Ennek a közvetlen és kényelmes bejelentési mechanizmusnak az eredményeként az FBI folyamatosan juthat információkhoz az aktuális jogsértő eseményekről, amelyeket nyomozási és hírszerzési célból elemeznek, majd – a bűnüldöző szervek mellett – évente a közvéleményt is tájékoztatják. Az IC3 2000 májusától működik, és a tavalyi év végéig több mint 8 millió panaszt fogadott. Az egyes panaszok kivizsgálása, azok összefüggésének vizsgálata mellett fontos küldetésük a prevenciós tevékenység. A közvélemény tájékoztatása, az új elkövetési magatartásokra történő figyelemfelhívások, a megelőzés lehetőségeinek ismertetése mind-mind fontos eleme a kiberbűnözés elleni hatékony fellépésnek.

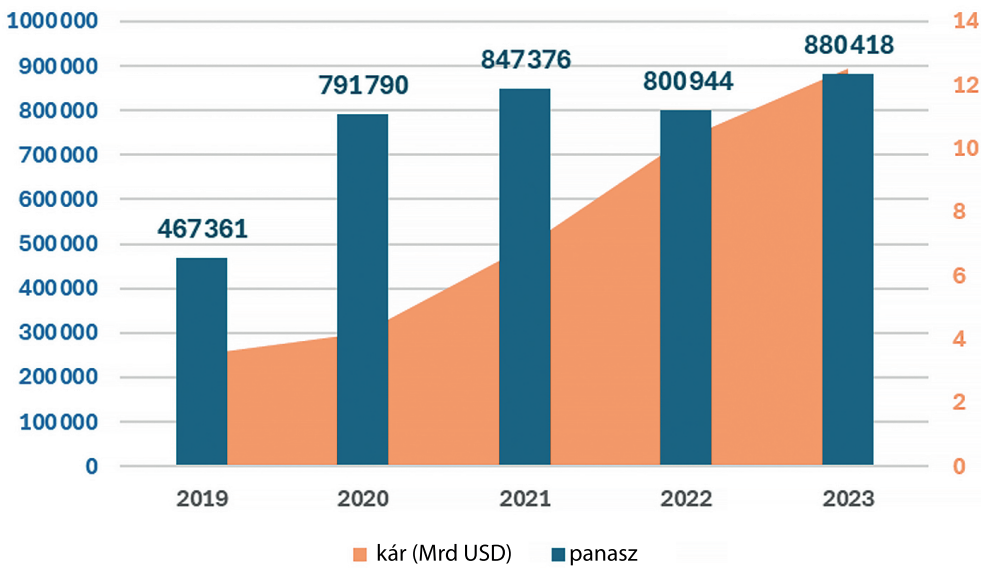
Az IC3 alapvető feladatai között a bejelentések fogadása (adatok gyűjtése), azok elemzése, a biztonságtudatosság növelése, és az ehhez szükséges ajánlások megtétele szerepel.

Az IC3 szervezetében jelentős szerep jut a 2018-ban létrehozott vagyonvisszaszerzési egységnek (RAT – Recovery Asset Team), amely központi szereplőként egyszerűsíti a pénzintézetekkel a kapcsolattartást, és kiemelkedő eredményeket ért el a kicsalt összegek továbbutalásának megakadályozásában vagy a bűnös úton szerzett pénzösszegek befagyasztásában.

[45] InterCOP: International Cyber Offender Prevention Network, Nemzetközi Kiberbűnözési Megelőzési Hálózat.

A szükséges feltételek megléte esetén a RAT a kérdéses tranzakció adatait azonnal tudja továbbítani az átutalást fogadó bank kijelölt kapcsolattartójához, akit értesít a jogellenes tevékenységről és kéri a számla zárolását. Amint a fogadó bank ezt visszaigazolja, a RAT felveszi a kapcsolatot az illetékes FBI irodával a további intézkedések érdekében. Eddigi működésük során 71%-os eredményességi mutatóval rendelkeznek, a 758 millió dolláros kárértékből 538 millió dollárt sikerült így biztosítaniuk.

A szervezet legutóbbi értékelő jelentése 2024. március 6-án jelent meg,[46] ami a 2023-as naptári évben beérkezett 880 ezer panaszra épül. Az elmúlt öt évben a panaszok száma közel a kétszeresére, míg az azokban bejelentett károsszeg a három és félszeresére (3,5 Mrd USD-ről 12,5 Mrd USD-re) nőtt. Az IC3 csak a náluk bejelentett panaszok adatait tudja értékelni, így például nem szerepelnek benne a bűnüldöző hatóságoknak közvetlenül bejelentett ügyek adatai. Ennek ellenére a kiberbűnözés tendenciái, az egyes bűncselekmények megoszlási aránya vagy az okozott kár mértékének alakulása nyomon követhető így is (1. ábra).



1. ábra: A panaszok és a kárérték-alakulás 2019–2023 között

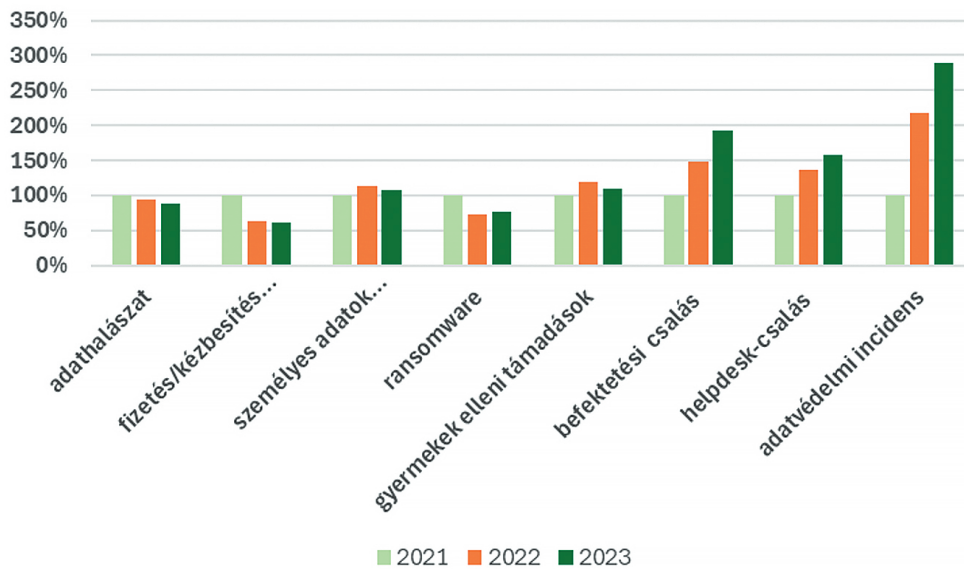
Forrás: a szerző szerkesztése FBI IC3 Internet Crime Report 2023 alapján

2023-ban a bejelentések között az adathalászat szerepelt a leggyakrabban (34%), majd ezt követte a személyes adatok megsértése, a fizetés vagy kézbesítés elmulasztásával megvalósított csalás és a zsarolás (5-6%). A panaszok között a ransomware-támadások és a gyermekek elleni bűncselekmények egyaránt 0,3%-ban jelentek meg.

[46] FBI 2023b.

Ha az elmúlt három év bejelentési adatait vizsgáljuk, akkor a 2021-es évet bázisnak (100%) tekintve megállapítható, hogy míg a klasszikusnak tekinthető bűncselekmények (adathalászat, ransomware-támadások, fizetés vagy kézbesítés elmaradásával elkövetett csalások) száma stagnáló, vagy esetleg csökkenő tendenciát mutat, addig egyes csalások (befektetési vagy a technikai segítséget színlelő), illetve az adatszivárgások ugrásszerűen megnőttek (2. ábra).

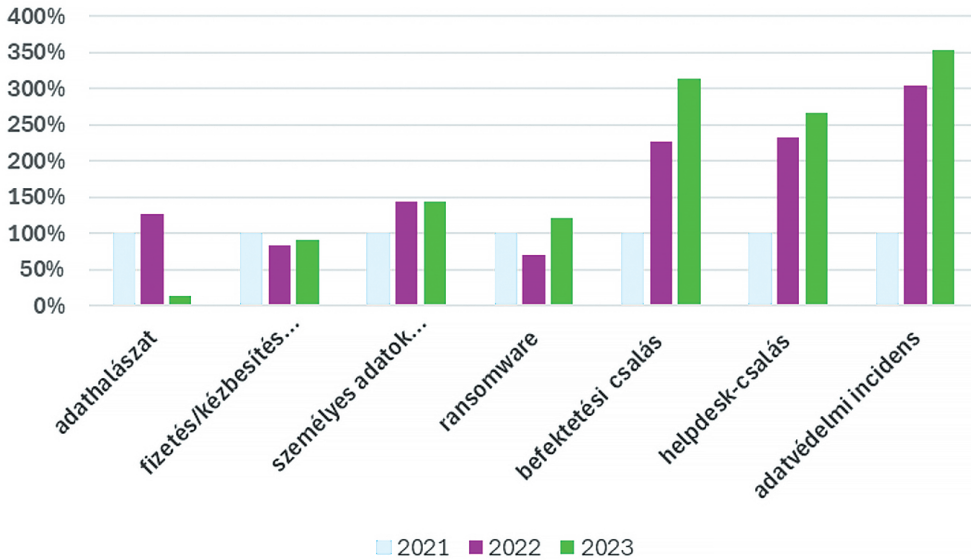
A technikai segítség színlelése (úgynevezett helpdesk-csalás) során az elkövetők az áldozatukkal egy fiktív hibajelenségre vagy üzenetre (például programhiba, vírusfertőzés) hivatkozással lépnek kapcsolatba, többek között felugró ablakon, hamis weboldalakon vagy call-centeres telefonhívásokon keresztül. Ezután az állítólagos hibajelenség elhárításáért kérnek pénzt, illetve ráveszik az áldozatukat, hogy a hamis helpdesk-támogatás keretében egy távoli elérést biztosító, ártalmas szoftvert (például AnyDask) töltsenek le. Ezzel később átvehetik az irányítást az áldozatuk eszköze felett, és szabadon rendelkeznek az azon kezelt számlák felett, illetve további vírusokat is letölthetnek arra.



2. ábra: A bejelentett jogsértések számának alakulása %-ban, 2021–2023 között, a 2021-es évet alapul véve

Forrás: a szerző szerkesztése FBI IC3 Internet Crime Report 2023 alapján

A jogsértések száma mellett az okozott kár mértéke is jellemző adat. A befektetési csalások kárértéke 2023-ra két év alatt közel a háromszorosára nőtt; 1,45 Mrd USD-ről 4,57 Mrd USD-re. Az okozott kár 86%-a (2023-ban 3,96 Mrd USD) kriptovalutában jelentkezett (3. ábra).



3. ábra: A bejelentett jogsértések által okozott kár alakulása %-ban, 2021–2023 között, a 2021-es évet alapul véve

Forrás: a szerző szerkesztése FBI IC3 Internet Crime Report 2023 alapján

Az FBI értékelésében is megfigyelhető, hogy a kiberbűncselekmények között a különféle csalások fejlődnek a legdinamikusabban, és az ezekkel okozott kár összege is folyamatosan emelkedik. Kiemelkednek ezek közül a technikai segítséget ígérő helpdesk-csalások mind az elkövetés számának, mind az okozott kárnak növekedése alapján. 2023-ban 37 ezer ilyen bűncselekményt jelentettek, és az elmúlt két év alatt a bűncselekményenként okozott átlagos kár 14 ezer USD-ről 26 ezer USD-re emelkedett.

Ugyancsak figyelemre méltó az adatvédelmi incidensek alakulása is. Az IC3 jelentésében ez alatt azokat az informatikai behatolásokat értik, amelyekkel védett adatok, információk megszerzésére törekednek, de nem számítják bele a személyi tulajdonban lévő eszközöket, rendszereket vagy felhasználói fiókokat, és nem veszik figyelembe a közösségi médiát vagy pénzügyi számlákat célzó támadásokat sem. Ezek ugyan viszonylag alacsony számban fordulnak elő (2021-ben 1287 panasz, 2023-ban 3727 panasz érkezett), de az ezzel okozott kár ehhez képest nagyon magas, 2021-ben 151 millió USD, míg 2023-ban 534 millió USD, ami bűncselekményenként 120–150 ezer USD kárt jelent átlagosan.

A hagyományosnak tekinthető kibertámadások számában jelentős változás nem érzékelhető, de ezzel együtt továbbra is ezek jelentik a leggyakrabban elkövetett bűncselekményeket. A magas elkövetési arány mellett ugyanakkor az ezekkel okozott kár alacsony szinten mozog. 2023-ban az adathalászattal okozott kár például 18 millió USD volt, ami átlagosan 60 USD-t jelent bűncselekményenként. Vélel-

mezhető azonban, hogy a jelentésben csak a közvetlenül okozott kárt vizsgálták, és az adathalászatra épülő további bűncselekmények (például zsarolások, csalások) kárértékei nem szerepelnek ebben.

Das Bundeslagebild Cybercrime 2023 (BKA)

A német BKA szintén évente teszi közzé az internetes bűnözésről szóló értékelését, amelynek aktuális verziója május közepén jelent meg.[47] A BKA értékelésének központjában az internet és az információs technológiai rendszerek elleni bűncselekmények állnak, és nem terjed ki a hagyományos módon is elkövethető bűncselekményekre (például csalások, gyermekpornográfia), függetlenül attól, hogy azok végrehajtásához alkalmaztak-e informatikai eszközt vagy internetet.

A jelentés az összefoglalásában megállapította, hogy a rendőrség célirányos fellépése – a hatékonyabb felderítés mellett – gyengítette a kiberbűnözők infrastruktúráit is. Ugyanakkor a kiberbűncselekmények számának csökkenését ellensúlyozta a külföldön elkövetett, de ténylegesen Németországban kárt okozó bűncselekmények erőteljesebb növekedése. Németországban több mint 800 vállalat és intézmény számolt be zsarolóvírusos támadásról.

A kibertámadások célpontjai között egyaránt szerepeltek közszolgáltatást nyújtó vállalatok, illetve oktatási vagy egészségügyi intézmények is. Utóbbiak különösen veszélyeztetett célpontok, miután egy kibertámadással korlátozott egészségügyi szolgáltatás nehezíti vagy megakadályozza az ellátást, adott esetben az életmentő beavatkozások végrehajtását is.

Az informatikai rendszerek ellen elkövetett támadások adatai megjelennek a német rendőrségi bűnügyi statisztikában (PKS[48]) is, amelyben 2020-tól külön megjelenítik azokat is, amelyek esetében a kár Németországban jelentkezett, de az elkövetés helyszíne külföldi vagy ismeretlen volt. A statisztikai adatokkal kapcsolatban a német helyzetértékelés is megjegyzi, hogy a kiberbűncselekmények esetében az átlagosnál magasabb a látencia, így bűnügyi statisztikai adatokon keresztül nem lehet reális képet nyerni az aktuális helyzetről.

Az adatok alapján Németországban a 2023-ban regisztrált 5,9 millió bűncselekményből 134 ezer tartozott a kiberbűncselekmény körébe, ami 2,2%-os arány. Ezekből 43 ezer bűncselekmény elkövetőjét azonosították, ami közel 32%-os felderítési arányt jelent. Az összbűnözésen belül a kiberbűncselekmények aránya évek óta minimálisan csökkenő értéket mutat, a 2020-as 3,1%-ról csökkent 2023-ban 2,2%-ra.

Ugyanakkor a külföldi elkövetés folyamatosan fejlődő képet mutat. 2023-ban az előző évhez képest 28%-os emelkedés észlelhető, és míg a belföldön elkövetett

[47] BKA 2023.
[48] PKS: Polizeilichen Kriminalstatistik, rendőrségi bűnügyi statisztika.

kiberbűncselekmények aránya 2,2%, addig a külföldön elkövetettként regisztrált bűncselekmények esetében már 26,5% ez az arány.

A kiberbűncselekmények között legnagyobb arányban Németországban is az adathalászat fordult elő. Az elemzés felhívja a figyelmet a Telekopye eszközre, amely lehetővé teszi a kiberbűnözők számára, hogy nagyszabású adathalászkampányokat hajtsanak végre mélyreható műszaki ismeretek nélkül.

A Telekopye használatával a felhasználók a Telegramon keresztül egy leegyszerűsített felületre jutnak, ahol számos funkciót érhetnek el az adathalászkampányok lebonyolításához. A funkciók közé tartozik az adathalász-webhelyek létrehozása, az adathalász-e-mailek és SMS-ek küldése, valamint hamis képernyőképek és QR-kódok generálása. Az eszköztár különféle HTML-sablonokat kínál az adathalász webhelyekhez különböző országokban, köztük Németországban.

A német értékelés a nemzeti phishinghelyzet helyett nemzetközi adatokat mutatott be, amihez az Adathalászat Elleni Munkacsoport (APWG[49]) elemzését használta fel. A 2023/Q4 időszakra vonatkozó jelentésük szerint 2023-ban minden korábbinál nagyobb számú, közel 5 millió adathalász-támadást észleltek világszerte (4. ábra). Az év végén robbanásszerűen nőtt meg a közösségimédia-platformok elleni támadások száma, az összes támadás 42,8%-a ezeket célozta meg. Az év végére ugyancsak emelkedett a vállalati belső levelezési csalások (BEC) száma is, de az egyes esetekre kivetített átlagos kár csökkenő tendenciát mutatott az 56,195 USD összeggel.[50]

Az adathalászat területén egyre nagyobb szerephez jutnak a nagy nyelvi modellek (LLM), mint például a chatbot, a ChatGPT és az ezeknek megfelelő bűnözői variációik. A ChatGPT 2022. évi megjelenésétől óriási növekedést regisztráltak az új adathalász-e-mailek számában. Az AI által generált szövegek a hagyományos adathalász-e-maileknél személyre szabottabbak és nyelvtanilag pontosabbak lettek, így kevésbé ébresztenek kétségeket. Ezentúl az adathalász-támadások automatikusan is létrehozhatók és kiküldhetők lettek, ami a minőség mellett mennyiségi fejlődést is eredményezett.

Az így megszerzett hozzáférési adatokat üzletszerűen értékesítő brókerek, az IAB-k Németországban is elterjedtek, és csak kevés esetben lehetett megállapítani olyan képzett, professzionális csoportokat, amelyek saját készségekkel rendelkeznek a kezdeti hozzáférés területén.

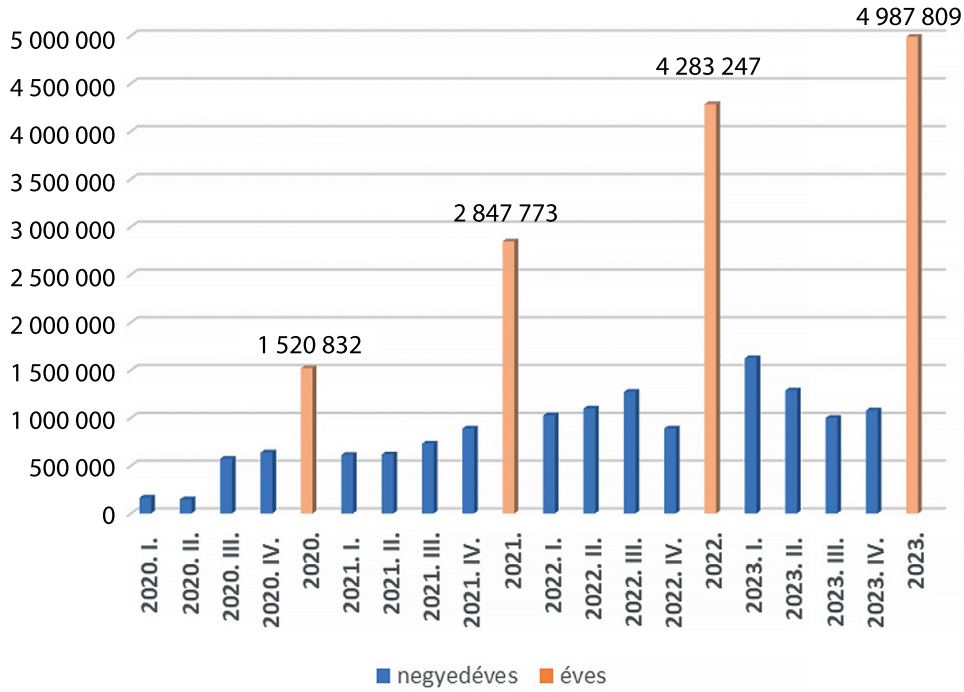
Az IAB-k Németországban is elérhető kínálatában az adathalászat mellett a nulladik napi sebezhetőségek felderítésével megszerzett belépési adatok is szerepeltek. 2023-ban az amerikai Kiberbiztonsági és Infrastruktúra Védelmi Ügynökség (CISA[51]) 187 jelentős nulladik napi sérülékenységet regisztrált, közte az ESXi, a GoAnywhere MFT, vagy a már korábban is említett MOVEit MFT hibáit.

---

[49] APWG: Anti-Phishing Working Group, 2003-ban alakult nemzetközi koalíció, amelynek közel 3200 tagja között a bűnüldöző szervek mellett gazdasági szervezetek és kiberbiztonsággal foglalkozó vállalatok is találhatók.

[50] APWG 2023.

[51] Cybersecurity and Infrastructure Security Agency.



4. ábra: Adathalász-támadások száma 2020–2023 között

Forrás: a szerző szerkesztése az APWG jelentések alapján

Ugyancsak kiemelt veszélyforrásnak tekintik a rosszindulatú zsarolóprogramok, a *ransomware-ek* előfordulását. Újszerű a *ransomware-ek* multifunkciós jellege, azaz, hogy nem egy célra alkalmazzák őket, hanem többirányú felhasználásra is alkalmasak.

Összegezve: a német BKA értékelése az általa vizsgált területen hasonló megállapításokat tett, mint az Europol és az FBI elemzése, ami megerősíti a kiberbűnözés általános megjelenését világszerte.

Összefoglalás

A bűnözés egyre inkább nemzetközivé válik, különösen olyan térségben, mint az Európai Unió, ahol a tényleges földrajzi határok már csak kivételes helyzetekben érvényesülnek. Ezen túl a kiberbűnözés – a hagyományos, fizikai térben elkövetett cselekményekkel szemben – egy olyan virtuális világban jelentkezik, ahol ezek a határok már sem elméletben, sem kivételes helyezetekben nem érvényesülnek.

Mivel a kiberbűnözés kevésbé köthető földrajzi helyszínhez, annak hatása sem szorítható országhatárok közé. Ebből adódóan a nemzetközi tapasztalatok, legyen szó amerikairól vagy európairól, előbb-utóbb hazai kihívásként is megjelennek, így

azokat a kiberbűnözéssel kapcsolatos intézkedések tervezésénél, a várható veszélyforrások meghatározásánál nem szabad figyelmen kívül hagyni.

A kiberbűnözés fejlődése, az új elkövetési magatartások és trendek, valamint azok hatásai elsősorban a gazdasági környezet, a támadással célzott személyek és szervezetek védelmi képességei, egy esetleges kibertámadással szembeni érzékenységük, valamint a kiberbiztonságra vonatkozó szabályozás függvényében térnek el az egyes országokban.

A három tanulmányt összeolvasva az elkövetkező időszakban az alábbiakat kell a kiberbűnözés területén szem előtt tartanunk hazánkban is:

- az AI folyamatos fejlődése hatással lesz az egyes bűncselekményre, különösen a ransomware-támadásokra, a gyermekpornográfiára és a csalásokra;
- eddig kevésbé ismert elkövetési módszerek elterjedésére kell felkészülni, így például a helpdesk- és a befektetési csalások nagyobb számú, kifinomultabb és nagyobb kárértékre történő elkövetésére;
- a kriptovaluták használata tovább erősödik a kiberbűnözésben és az ahhoz kapcsolódó üzleti tranzakciókban, amely során *bitcoin* mellett újfajta *altcoinok* és *stablecoinok* terjednek el;
- mind a malware-, mind a ransomware-támadásoknál meghatározó szerepet töltenek be a szolgáltató szerepet betöltő bűnözői csoportok, ami szélesebb és kevésbé képzett körben is elérhetővé teszi a támadásokat;
- a támadások tudatosabban előkészítettek és a sértettre igazítottak lesznek, amelyek során már nem a tartalom zárolása lesz az elsődleges fenyegetés, hanem a megszerzett tartalom nyilvánosságra hozatala;
- a támadások célpontjai lesznek a vállalkozások mellett a velük kapcsolatban álló – és alacsonyabb biztonsági szinten lévő – beszállítói hálózatok is;
- a bűnüldöző hatóságok fellépése időszakos eredményt hoz, mivel a bűnözői csoportok felkészülnek a tevékenységük, szolgáltatásuk újrakezdésére;
- a nyomozásoknak emiatt az elkövetők azonosítása mellett az infrastruktúrák felszámolását is eredményezniük kell;
- kiemelt feladat lesz a fiatalkorúak felelősségtudatos internethasználatának elérése, illetve az erre alkalmatlan korosztály vonatkozásában a szülői vagy technikai felügyelet nélküli internethasználat minimalizálása;
- az áldozattá válás megelőzése érdekében fontos a fiatalkorúak edukációja mellett a többi korosztály – kiemelten az idősebbek – oktatása és figyelmük felhívása a veszélyforrásokra;
- a bűncselekmények felderítésében feladattal rendelkező rendőrök képzése mellett egyre nagyobb szerepet kap az igazságszolgáltatás többi szereplőjének (ügyészek, bírók) is a felkészítése;
- a kiberbűnözéssel szembeni hatékony fellépéshez nélkülözhetetlen lesz a nemzetközi bűnügyi együttműködés, és aktív részvétel az ezzel foglalkozó nemzetközi szervezetekben.

A változó jogszabályi környezet szinkronizálása az utóbbi időben az EU területén is aktuális kérdés. Elég csak a NIS2 irányelvre[52] gondolni, amely a kiberbiztonság érdekében alakít ki egységes elvárásokat, míg a kiberbűncselekmények felderítését is olyan új szabályozások segítik, mint például 2026. augusztus 18-tól alkalmazható EU rendelet,[53] amely lehetővé teszi többek között majd a más tagállamban lévő szolgáltató közvetlen megkeresését az elektronikus adatok beszerzése érdekében.

Hazánkban az Országgyűlés előtt folyik a Magyarország kiberbiztonságáról szóló törvényjavaslat[54] részletes vitája, amely a kiberbiztonsággal foglalkozó korábbi normákat egységesíti. Az új jogi szabályozás megváltoztatja az egyes szervezetek és hatóságok feladatrendszerét, de olyan kötelezettségeket is ró majd a kibertérben megjelenő vállalkozásokra és állami szereplőkre is, amelyek fokozottan garantálják a biztonságot.

A kibertámadásokkal és kiberbűncselekményekkel szembeni védettség azonban alapvetően az informatikai védelem hatékonyabbá tételén és a humán kockázati tényezők minimalizálásán múlik. Míg az informatikai, technikai védelem örökös és elkerülhetetlen versenyfutás lesz a bűnözőkkel, akik mindig megtalálják az új védelmi eszközök sebezhető sérülékenységét, addig a humán oldalon a megfelelő képzés, felkészítés és érzékenyítés hosszú távon megtérülő befektetés. A két tényező csak együtt tud érvényesülni, de a leghatékonyabban kifejlesztett, legdrágább technikai védelem is alkalmatlan eszközzé válik a figyelmetlen, óvatlan felhasználók körében.

Mindezek mellett érdemes lenne megvizsgálni a kiberbűnözéssel foglalkozó hazai szervek feladat- és hatáskörét, valamint működésük feltételrendszerét az esetleges párhuzamosságok megszüntetése, a technikai eszközök és humán források hatékonyabb kihasználása érdekében.

Felhasznált irodalom

APWG (2023): *Phishing Activity Trends Reports (2020–23).* Online: https://apwg.org/trendsreports/

BKA (2023a): *Bundeslagebild Cybercrime, 2023.* Online: www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html

BKA (2023b): *Polizeilichen Kriminalstatistik (PKS)* (2023). Online: www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html

Cox, Joseph (2024): Inside the Underground Site Where 'Neural Networks' Churn Out Fake IDs. *404media.co,* 2024. február 5. Online: www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/

EAST (2023): *European Payment Terminal Crime Report, H1 2023.* Online: www.association-secure-transactions.eu/terminal-related-fraud-attacks-fall-in-europe/

[52] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv).

[53] Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról.

[54] T/9716. számú törvényjavaslat Magyarország kiberbiztonságáról.

Eurojust (2023): *Main Administrator of Ispoof Website Sentenced to 13 Years*. Online: www.eurojust.europa.eu/news/main-administrator-ispoof-website-sentenced-13-years
Europol (2023a): *Cybercriminals Stung as HIVE Infrastructure Shut Down*. Online: www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down
Europol (2023b): *Germany and Ukraine Hit Two High-Value Ransomware Targets*. Online: www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets
Europol (2023c): *Paper Trail Ends in Jail Time for 1013 Money Mules*. Online: www.europol.europa.eu/media-press/newsroom/news/paper-trail-ends-in-jail-time-for-1-013-money-mules
Europol (2023d): *Ragnar Locker Ransomware Gang Taken Down by International Police Swoop*. Online: www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop
Europol (2023e): *Qakbot Botnet Infrastructure Shattered after International Operation*. Online: www.europol.europa.eu/media-press/newsroom/news/qakbot-botnet-infrastructure-shattered-after-international-operation
Europol (2024a): *Internet Organised Crime Threat Assessment (IOCTA), 2024*. Online: www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
Europol (2024b): *Law Enforcement Disrupt World's Biggest Ransomware Operation*. Online: www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
Europol (2024c): *Cryptojacker Arrested in Ukraine over EUR 1.8 Million Mining Scheme*. Online: www.europol.europa.eu/media-press/newsroom/news/cryptojacker-arrested-in-ukraine-over-eur-1.8-million-mining-scheme
FBI (2023a): *Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes*. Online: www.ic3.gov/PSA/2023/PSA230605
FBI (2023b): *Releases Internet Crime Report, 2023*. Online: www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
Gihon, Shmuel – Tayar, Coral (2023): MOVEit Supply Chain Attack Campaign August Update. *cyberint.com,* 2023. augusztus 15. Online: https://cyberint.com/blog/research/moveit-supply-chain-attack/
Ilascu, Ionut (2024): LockBit Ransomware Returns, Restores Servers After Police Disruption. *bleepingcomputer.com,* 2024. február 25. Online: www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-restores-servers-after-police-disruption/
NCA (2024): *National Crime Agency Leads International Operation to Degrade Illegal Versions of Cobalt Strike*. Online: www.nationalcrimeagency.gov.uk/news/national-crime-agency-leads-international-operation-to-degrade-illegal-versions-of-cobalt-strike
Spanish Prosecutor to Probe AI-Generated Images of Naked Minors (2023). *Reuters.com,* 2023. szeptember 26. Online: www.reuters.com/world/europe/spanish-prosecutor-probe-ai-generated-images-naked-minors-2023-09-25/
The Drop in Ransomware Attacks in 2024 and What it Means (2024). *Thehackernews.com,* 2024. április 08. Online: https://thehackernews.com/2024/04/the-drop-in-ransomware-attacks-in-2024.html
What Is BlackCat Ransomware? (2023). *Akamai.com*. Online: www.akamai.com/glossary/what-is-blackcat-ransomware

Rövidítések

2FA/MFA: two-/multi-factor authentication – két- vagy multifaktoros azonosítási rendszer
AI: Artificial Intelligence – mesterséges intelligencia
BEC: Business Email Compromise – vállalati belső levelezési csalás
BKA: Bundeskriminalamt – német Szövetségi Bűnügyi Hivatal
CASP: crypto-asset service providers – kriptovaluta-szolgáltatók
CISA: Cybersecurity and Infrastructure Security Agency – Kiberbiztonsági és Infrastuktúra Védelmi Ügynökség
CSAM: child sexual abuse material – a gyermekek szexuális zaklatását ábrázoló tartalmak
CSE: child sexual exploitation – gyermekek online szexuális kizsákmányolása
DDoS: distributed denial-of-service – elosztott szolgáltatásmegtagadásos támadás
DoS: denial-of-service – szolgáltatásmegtagadásos támadás
E2EE: end-to-end encryption – végpontok közötti titkosítás
EAST: European Association for Secure Transactions – Biztonságos Tranzakciók Európai Szövetsége
EBA: European Banking Authority – Európai Bankhatóság
EFT: exchange-traded fund – tőzsdén kereskedett alap
EUROJUST: European Union Agency for Criminal Justice Cooperation – Európai Unió Büntetőjogi Együttműködési Ügynöksége
Europol: European Police Office – Európai Rendőrségi Hivatal
FBI IC3: Federal Bureau of Investigation Internet Crime Complaint Center – Szövetségi Nyomozó Iroda Kiberbűncselekmények Elleni Panaszközpont (USA)
I2P: Invisible Internet Project – a dark web eléréhez használatos böngésző a TOR mellett
IAB: Initial Access Broker – kezdeti hozzáférési bróker, ügynök
InterCOP: International Cyber Offender Prevention Network – Nemzetközi Kiberbűnözési Megelőzési Hálózat
J-CAT: Joint Cybercrime Action Taskforce – Europol számítástechnikai bűnözés elleni közös akciócsoportja
KYC: know your customer – ügyfél-azonosítás
LDCA: live-distant child abuse – élő közvetítéses távoli gyermekbántalmazás
LLM: large language models – nagy nyelvi modell
MaaS: malware-as-a-service – káros programok szolgáltatásjellegű értékesítése
MFT: managed file transfer – felügyelt fájlátvitel
Money mule: „pénzöszvér", a bűnös forrásból szerzett összegek legalizálásában közreműködő személyek
NFT: non-fungible tokens – nem helyettesíthető tokenek
OFS: online fraud schemes – online csalási módszerek
OpSec: operational security – technikai védelmi intézkedések
RaaS: ransomware-as-a-service – az erre szakosodott bűnözői csoportok tevékenysége, amely során a ransomware-támadáshoz szükséges forráskódokat üzleti alapon, szolgáltatásként értékesítik
RAT: Recovery Asset Team – FBI IC3 vagyonvisszaszerzési egysége
RDP: remote desktop protocol: – távoli asztal protokoll, számítógépek távoli vezérlése
SGEM: self-generated explicit material – saját előállítású, közvetlen forrású tartalom
TCSO: transnational child sex offenders – határokon átnyúló gyermekbántalmazások elkövetői
TOR: the onion router – hagyma elosztó, a dark web eléréséhez szükséges speciális böngészők egyike

Jogi források

2012. évi C. törvény a Büntető Törvénykönyvről
Az EBA/GL/2021/02 iránymutatásokat módosító iránymutatások. Online: https://bit.ly/3Wgw3P3
Az Európai Parlament és a Tanács (EU)2023/1113 rendelete a pénzátutalásokat és egyes kriptoeszköz-átruházásokat kísérő adatokról és az (EU) 2015/849 irányelv módosításáról. (2023. május 31.) Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32023R1113
Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról. (2023. július 12.) Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32023R1543
Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). (2022. december 14.) Online: http://data.europa.eu/eli/dir/2022/2555/2022-12-27
T/9716. számú törvényjavaslat Magyarország kiberbiztonságáról. Online: www.parlament.hu/irom42/09716/09716.pdf

ABSTRACT

The Present and Future of Cybercrime

Zoltán CSIZNER

The development of information technology also affects the evolution of cybercrime. Availability of artificial intelligence, the elimination of geographical distances and borders, the impersonality provided by the virtual world, or the possibility of escaping acquired assets into cryptocurrencies all open up new horizons for criminals. Some of the crimes are exclusively related to IT tools and networks, but most of them are specific execution methods of crimes that can also be committed in the real world.

The development of the cyber world results in a continuous renewal of criminal behaviour, which law enforcement and cyber security measures and regulations can only follow in most cases. For effective prevention, it is essential to explore the expected sources of danger and trends, one of the bases of which is to learn about the current criminal situation and the circumstances that help criminals. The annual reports that the FBI, BKA and Europol have been regularly preparing for years help with this. The presentation of the findings, novel phenomena and expected challenges in the three evaluation reports provides direction for cybercrime professionals and perhaps provides useful information for the average Internet user to avoid becoming a victim.

Keywords: internet, cybercrime, cryptocurrency, online fraud, phishing, child sexual exploitation