DOI: 10.38146/BSZ-AJIA.2024.v72.i9.pp1599-1607

Az Europol szerepe a kiberbűnözés elleni küzdelemben

Europol's role in the fight against cybercrime

Europol European Cybercrime Centre
Europol
O3@europol.europa.eu

Szabó Csaba ✉
Dr. PhD, főszerkesztő-helyettes, egyetemi docens, rendőr alezredes
Belügyminisztérium,
Belügyi Szemle Szerkesztősége
Széchenyi István Egyetem,
Deák Ferenc Állam- és Jogtudományi Kar
csaba.szabo3@bm.gov.hu

Absztrakt

Cél: A tanulmány célja, hogy bemutassa az Europol Európai Kiberbűnözés Elleni Központjának (Europol European Cybercrime Centre – EC3) szerepét és tevékenységét a kiberbűnözés elleni küzdelemben, különös tekintettel a legmodernebb technológiai megoldásokra és együttműködési mechanizmusokra.
Módszertan: A kutatás során az EC3 által alkalmazott stratégiák és eszközök elemzésére került sor. A szerzők az adatok gyűjtése és elemzése során az Europol belső jelentéseit, nyilvánosan elérhető forrásokat, valamint esettanulmányokat használtak fel, hogy átfogó képet nyújtsanak az EC3 tevékenységéről és hatékonyságáról.
Megállapítások: Az EC3 kiemelkedő szerepet játszik a kiberbűnözés elleni küzdelemben, különösen a transznacionális bűnszervezetek és a fejlett kiberfenyegetések kezelésében. Az EC3 három fő részlegből áll, melyek közé tartozik az operatív egység, a digitális támogató egység és a szakértelemmel foglalkozó egység. Az operatív egység négy állandó analitikai projektet tart fenn, amelyek mindegyike különböző kiberbűnözési területekre koncentrál.
Érték: A tanulmány értékes betekintést nyújt az EC3 működésébe, és a központ kiberbűnözés elleni globális küzdelemhez nyújtott tevékenységébe. Kiemeli az Europol hatékony együttműködési modelljét, amely segíti a nemzetközi

Magyar nyelvű utánközlés. Jelen cikk angol változata megjelent a Belügyi Szemle 2024. évi 9. számában. DOI link: https://doi.org/10.38146/BSZ-AJIA.2024.v72.i9.pp1707-1714

✉ Levelező szerző az EUROPOL hozzájárulásával.

összefogást a kiberfenyegetések elleni harcban. Az EC3 tevékenységei jelentősen hozzájárulnak a tagállamok közötti információmegosztáshoz és operatív együttműködéshez, növelve ezzel a kiberbűnözés elleni védekezés hatékonyságát.

Kulcsszavak: kiberbűnözés, Europol, kiberbiztonság, transznacionális bűnszervezetek

Abstract

Aim: The aim of the study is to present the role and activities of Europol's European Cybercrime Centre (EC3) in combating cybercrime, with a particular focus on the latest technological solutions and cooperation mechanisms.
Methodology: The research involved analysing the strategies and tools employed by the EC3. Data collection and analysis utilised Europol's internal reports, publicly available sources, and case studies to provide a comprehensive overview of EC3's activities and effectiveness.
Findings: The EC3 plays a crucial role in the fight against cybercrime, particularly in dealing with transnational criminal organisations and advanced cyber threats. The EC3 is divided into three main divisions: the operational unit, the digital support unit, and the expertise unit. The operational unit maintains four permanent analytical projects, each focusing on different areas of cybercrime.
Value: The study provides valuable insights into the functioning of the EC3 and its contributions to the global fight against cybercrime. It highlights Europol's effective cooperation model, which aids in international collaboration against cyber threats. EC3's activities significantly enhance information sharing and operational cooperation among member states, thereby increasing the effectiveness of defences against cybercrime.

Keywords: cybercrime, Europol, cybersecurity, transnational criminal organisations

A kiberbűnözés az elmúlt évtizedekben

Ahhoz, hogy megértsük az Europol szerepét a kiberbűnözés elleni küzdelemben, először is meg kell értenünk, hogyan fejlődött maga a kiberbűnözés jelenség az elmúlt évtizedekben, és milyen veszélyeket rejt magában.

Az ezredfordulón a világ már online volt, ami azt jelentette, hogy a világhálóhoz csatlakozó emberek ki voltak téve a kiberbűnözés korai formáinak.

A 2000-es évek eleje volt a számítógépes férgek[1] aranykora, amelyeket e-mail mellékletekben és fertőzött weboldalakon keresztül osztottak meg, miközben az alkalmazások sebezhetőségeit kihasználva terjedtek el más felhasználók között. Bár a leghírhedtebb ilyen tevékenységek némelyikének (például LoveBug, URL1) szándéka nem volt egyértelmű, a fertőzött rendszerekben okozott károk hatalmasak voltak. Ugyanez mondható el a hackerek által indított elosztott szolgáltatásmegtagadási (Distributed Denial-of-Service – DDoS) támadásokról, amelyek számos nemzetközi kereskedelmi weboldalt, például a Yahoo-t, az Amazont, a CNN-t és másokat is képesek voltak működésképtelenné tenni (URL2).

Nem tartott sokáig, mire a bűnözők elkezdték keresni azokat a módokat, amelyekkel pénzzé tehetik ezeket az újszerű bűnözési formákat, ami az online csalások és olyan banki trójai vírusok (például Zeus, URL3) elterjedéséhez vezetett, amelyek célja az emberek pénzének és személyes adatainak ellopása. Történetesen a Zeus banki trójai a szolgáltatásként kínált kiberbűnözés egyik legismertebb úttörője is lett, mivel a művelet mögött álló szereplők elkezdték licencezni kódjukat más kiberbűnözők számára, hogy azok végrehajthassák támadásaikat. A trójai vírussal megfertőzött számítógép teljes hozzáférést biztosított a rendszerhez, ami az áldozat hitelkártyaadatainak ellopása mellett azt is lehetővé tette, hogy rosszindulatú szoftvereket juttassanak a rendszerbe és/vagy az eszközt hozzáadják a bothálózatukhoz.[2]

A zsarolóvírusok első verziói is a Zeusszal egy időben jelentek meg, de csak 2013-ban, a CryptoLocker megjelenésével kezdte a világ megérteni a modern zsarolóvírus-tevékenységek pusztító hatásait. A CryptoLocker ransomware 2048 bites RSA titkosítást használt, és a hagyományosabb terjesztési módszerek mellett bolthálózatokat (Gameover Zeus bothálózat) is igénybe vett, hogy növelje a hatókörét (URL4). Ekkorra már megjelentek a piacon az első kriptovaluták, amelyekkel a bűnözők visszaélhettek a tiltott bevételeik elrejtésére. Ezek a fejlemények megalapozták a szervezett, szolgáltatásalapú kiberbűnözés modern korszakának nevezhető időszakot.

Bűnüldözési válasz

A felmerülő fenyegetésekre válaszul 2013-ban létrehozták az Europol Európai Kiberbűnözés Elleni Központját (Europol European Cybercrime Centre – EC3).

1 Önterjesztő rosszindulatú számítógépes program (azaz malware).
2 Fertőzött eszközök hálózata, amely malware terjesztésére és/vagy DDoS-támadások indítására használható.

Az EC3 ma három részlegből áll: az operatív, a digitális támogatással foglalkozó, valamint a szakértelemmel és az érdekeltek kezelésével foglalkozó egységekből. Az operatív egység négy állandó analitikai projektnek (AP) ad otthont, amelyek mindegyikét egy adott kiberbűnözési területnek szentelt:

- AP Cyborg – a kiber-függő bűnözés;
- AP Terminal – online csalási rendszerek;
- AP Twins – gyermekek online szexuális kizsákmányolása;
- AP Dark Web – keresztbűnözést elősegítő kiberbűnözés (például tartalomfelügyelet nélküli tárhely, vírusirtó-ellenes szolgáltatások, a dark web bűnös felhasználása).

Emellett az EC3 ad otthont a kiberbűnözés elleni közös munkacsoportnak (Joint Cybercrime Action Taskforce – J-CAT) is, amely 13 uniós tagállam és hét nem uniós együttműködési partner kiberkapcsolati tisztviselőit tömörítő állandó operatív csoportból áll. A J-CAT együttműködik az EC3 operatív csoportjaival azért, hogy hírszerzésen alapuló, összehangolt fellépést vezessen be a legfontosabb kiberbűnözési fenyegetések és célpontok ellen.

Modern kiberbűnözési veszélytérkép

Az elmúlt tíz év során a kiberbűnözéssel kapcsolatos fenyegetések a transznacionális bűnszervezetek és (infra)struktúrák magasan specializált feketegazdaságává fejlődtek (URL5).

A kiberbűnözés valamennyi területén a bűnszervezetek gyakran földrajzilag szétszórt szereplőkből állnak, és műveleteiket a világ különböző pontjain elhelyezett komplex infrastruktúrán végzik, ami ellenállóvá teszi őket a bűnüldözői lekapcsolásokkal szemben. A kiberbűnözés határok nélküli jellege miatt a bűncselekmények áldozatai szinte mindig nemzetköziek, több joghatóságon, régión, sőt kontinensen is átívelnek.

A szolgáltatásalapú kriminális gazdaság emellett csökkentette a belépési korlátot mind a szükséges technikai készségek, mind a műveletek létrehozásához szükséges idő- és erőforrás-befektetés tekintetében. A zsarolóprogram-szolgáltatásként (Ransomware as a service – RaaS) működő szolgáltatók például más kiberbűnözőknek adják kölcsön rosszindulatú kódjukat, cserébe a bűncselekményből származó bevételük egy százalékáért.

A kiberbűnözés valamennyi területén tevékenykedő elkövetők online tevékenységük során kihasználják a tárhely- és anonimitási szolgáltatásokat, hogy elkerüljék a bűnüldöző szervek általi felderítést és azonosítást. A leggyakoribb

példák erre a bűnözők számára nyújtott tartalomfelügyelet nélküli tárhelyszolgáltatások (Bulletproof Hosting – BPH) és virtuális magánhálózati (Virtual Private Network – VPN) szolgáltatók, amelyek lehetővé teszik számukra, hogy infrastruktúrájukat kiépítsék, valamint proxykon keresztül kapcsolódjanak áldozataikhoz és egymáshoz.

A kriptovaluták szintén hatalmas szerepet játszanak a kiberbűnözésből származó bevételek tisztára mosása révén. Amellett, hogy nem kötődnek központi pénzügyi intézményekhez, vagy a tárcák tulajdonosainak személyazonosságához, a blokkláncon végrehajtott tranzakciók nyomon követése megnehezíthető a kriptopénzkeverő[3] és -cserélő[4] szolgáltatások használatával.

A dark web fórumok és piacterek a bűnözők rendelkezésére bocsátják a támadások végrehajtásához szükséges eszközöket, szolgáltatásokat és lopott adatokat, miközben a tudásmegosztás és a toborzás platformjaként is szolgálnak.

Ezek az átalakulások a modern kommunikációs technológiák által kínált növekvő anonimitással együtt hozzájárulnak a kiberbűnözés új és régi formáinak folyamatos növekedéséhez.

Küzdelem a kiberbűnözés modern formái ellen

A kiberbűnözés transznacionális jellege miatt csak egy nemzetközileg koordinált bűnüldözői válaszlépés lehet hatékony az elkövetők azonosításában és műveleteik megszakításában. E célból az EC3 egyedülálló szerepet játszik a nagy értékű célpontok azonosításában, a nemzetközi bűnüldözői műveletek koordinálásában, valamint az uniós tagállamok és az Europollal operatív együttműködési megállapodást kötött országok számára nyújtott technikai támogatásban.

Az EC3 operatív csoportjai és a J-CAT megkönnyítik a kulcsfontosságú kiberbűnözési fenyegetések és célpontok elleni határokon átnyúló nyomozások közös azonosítását, rangsorolását, kezdeményezését és végrehajtását. Ezek a fellépések hírszerzésen alapulnak, mivel az Europol képes azonosítani a nemzeti bűnügyi nyomozások kereszthivatkozásait és átfedéseit, és koordinálni a számos ország bűnüldöző szerveit érintő nemzetközi műveleteket. Ez a megközelítés kulcsfontosságú a nemzetközi bűnszervezetek elleni küzdelemben, mivel – amint azt korábban már említettük – a szereplők, áldozataik és infrastruktúrájuk több joghatóságban is szétszóródnak.

3 A potenciálisan azonosítható kriptovaluta-alapok keverése más alapokkal, hogy elfedjék eredeti forrásukat.

4 Egy kriptovaluta cseréje egy másikra.

Ez a megközelítés vezetett többek között az EMOTET (URL6), azaz az elmúlt évtized egyik legjelentősebb bothálózata, a RaidForums (URL7), a világ egyik legnagyobb hacker közössége, a Genesis Market (URL8), az egyik legveszélyesebb olyan piac, ahol lopott fiókok hitelesítő adatait értékesítették hackerek számára világszerte, valamint az olyan kiemelkedő zsarolóprogram-szolgáltatások, mint a LockBit (URL9) és a Hive (URL10) felszámolásához.

Példaként említhetjük emellett a magyar bűnüldöző szerveket is érintő kiemelkedő nemzetközi operatív akciókat is, például a FluBot kémprogram infrastruktúrájának felszámolását, amely az egyik leggyorsabban terjedő mobil kártevő volt. (URL11),A VPNLab elleni fellépést is (URL12), amely védett kommunikációt és internet-hozzáférést kínált – például váltságdíjfizető programok telepítését – súlyos bűncselekményeket elkövető kiberbűnözőknek.

További példák az EC3 által koordinált és a többi részt vevő ország mellett Magyarországot is érintő, ismétlődő, hírszerzés által irányított akciókra:

- **Kártyás Akció** (URL13) – a lopott hitelkártyaadatokat értékesítő weboldalakon veszélyeztetett kártyaadatokat értékesítő és vásárló csalók elleni művelet, amelynek célja a pénzintézetek és a kártyabirtokosok veszteségeinek mérséklése és megelőzése. 2020-ban több mint 90 000 kártyaadatot elemeztek, amivel mintegy 40 millió euró veszteséget sikerült megelőzni.
- **Európai Pénzcsempész Akció** (URL14) – a pénzcsempészek és beszervezőik elleni küzdelemre irányuló művelet. 2023-ban több operatív szakaszban 10 759 pénzcsempészt és 474 beszervezőt azonosítottak, ami világszerte 1013 személy letartóztatásához vezetett.
- **Áldozat Azonosítási Munkacsoport** (URL15) – kezdeményezés a gyermekek szexuális zaklatását bemutató anyagokban ábrázolt áldozatok és elkövetők azonosítására. 2021-ben a szakértők mintegy 580 olyan képsorozatot és videófájlt elemeztek, amelyeken gyermekek szexuális zaklatásának ismeretlen áldozatai szerepelnek, és 18 gyermeket tudtak azonosítani, két elkövetőt pedig letartóztatni. Ezenkívül 211 esetben sikerült meghatározni a valószínűsíthető gyártó országot, és hírszerzési csomagokat küldtek az érintett országoknak vizsgálat céljából.
- **Kiber-járőrözés Hete** (URL16) – kezdeményezés a dark web piactereken működő nagy értékű célpontokkal (eladók és vevők) kapcsolatos hírszerzési információk gyűjtésére.

Mint már említettük, a kiberbűnözők jól kihasználják a modern, adatvédelmet fokozó technológiákat, ami kihívást jelenthet a bűnüldözés számára a tevékenységük nyomon követése és a zárolt és titkosított eszközökről történő digitális bizonyítékok megszerzése tekintetében. A bűnözők operatív biztonsági

intézkedéseinek ellensúlyozására léteznek eszközök és technikák, de ezek költségesek, és alkalmazásuk magas szintű szakértelmet igényel. Ezen kívül az új technológiák gyors fejlődése miatt folyamatos kutatásra és fejlesztésre van szükség ahhoz, hogy lépést tartsanak a piaccal. Az összes uniós tagállam számára nehéz fenntartani ezeket a képességeket, ezért az EC3 létrehozta a digitális támogató egységet (Digital Support Unit – DSU), hogy megerősítse a veszélyes bűnözői hálózatok és a nagy értékű célpontok elleni kollektív bűnüldözői reakciót. A DSU néhány kiemelkedő képessége a következő:

- Helyszíni forenzikus támogatás nyújtása nemzetközi műveletek során a gyanúsítottak eszközeiről származó bizonyító erejű adatok lefoglalása és rögzítése érdekében.
- Az Europol dekódolási platformjának működtetése (URL17), amely segít a bűnügyi nyomozás során jogszerűen megszerzett információk dekódolásában.
- Kriptokövetési támogatás nyújtása a kiberbűnözők tiltott bevételeinek nyomon követése érdekében.
- Az Europol Kártevő Programok Elemzési Megoldásának (Europol Malware Analysis Solution – EMAS) üzemeltetése, amely a rosszindulatú szoftverek (például zsarolóprogramok) viselkedésének vizsgálatára szolgáló, bűnüldözői korlátozás alá eső dinamikus elemzési platform, melynek célja az üzemeltetők elleni, határokon átnyúló nyomozások gazdagítása.

Előretekintés

A digitalizált bűnözés fenyegetése csak tovább növekszik, mivel a bűnözők minden bűnözési területen technológiai ellenintézkedéseket alkalmaznak tevékenységük elrejtésére. Ezek közé tartozik a titkosított kommunikáció, a dark web piacainak használata illegális áruk és szolgáltatások értékesítésére, valamint a kriptovaluták mint fizetési formák alkalmazása, amellyel megnehezítik a bűncselekményből származó bevételek nyomon követését. A jelenleg a bűnözés hagyományosabb formáival foglalkozó bűnszervezetek a portfóliójukat olyan jövedelmező bűncselekményekkel kívánják bővíteni, mint az online csalási rendszerek. A szervezetek és magánszemélyek folyamatosan új technológiai megoldásokat vezetnek be, ami növeli a kibertámadások, rosszindulatú szoftvertevékenységek és behatolások potenciális támadási felületét.

Mindezen tendenciákat figyelembe véve minden eddiginél fontosabb az országok, magánvállalatok és tudományos intézmények közötti érdemi operatív együttműködés kiépítése annak érdekében, hogy ellensúlyozni lehessen a kiberbűnözők által a közös biztonságunkra jelentett fenyegetést.

A cikkben található online hivatkozások

URL1: *ILOVEYOU virus.* https://www.techtarget.com/searchsecurity/definition/ILOVEYOU-virus

URL2: *DDos attacks – one year later.* https://www.hpcwire.com/2001/02/09/ddos-attacks-one-year-later/

URL3: *The Zeus Trojan malware – definition and prevention.* https://www.crowdstrike.com/cybersecurity-101/malware/trojan-zeus-malware/

URL4: *The history and evolution of ransomware attacks.* https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/

URL5: *Internet Organised Crime Threat Assessment (IOCTA) 2023.* https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

URL6: *World's most dangerous malware EMOTET disrupted through global action.* https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

URL7: *One of the world's biggest hacker forums taken down.* https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down

URL8: *Takedown of notorious hacker marketplace selling your identity to criminals.* https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals

URL9: *Law enforcement disrupt world's biggest ransomware operation.* https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

URL10: *Cybercriminals stung as HIVE infrastructure shut down.* https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down

URL11: *Takedown of SMS-based FluBot spyware infecting Android phones.* https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

URL12: *Unhappy New Year for cybercriminals as VPNLab.net goes offline.* https://www.europol.europa.eu/media-press/newsroom/news/unhappy-new-year-for-cybercriminals-vpnlab-net-goes-offline

URL13: *Officers foil fraudsters from stealing €40 million in payment card scam.* https://www.europol.europa.eu/media-press/newsroom/news/officers-foil-fraudsters-stealing-%E2%82%AC40-million-in-payment-card-scam

URL14: *Paper trail ends in jail time for 1 013 money mules.* https://www.europol.europa.eu/media-press/newsroom/news/paper-trail-ends-in-jail-time-for-1-013-money-mules

URL15: *Global Europol taskforce identifies 18 child victims of sexual abuse.* https://www.europol.europa.eu/media-press/newsroom/news/global-europol-taskforce-identifies-18-child-victims-of-sexual-abuse

URL16: *Cyber-patrolling Week.* https://www.europol.europa.eu/operations-services-and-innovation/operations/cyber-patrolling-week

URL17: *Europol and the European Commission inaugurate new decryption platform to tackle the challenge of encrypted material for law enforcement investigations*. https://www.europol.europa.eu/media-press/newsroom/news/europol-and-european-commission-inaugurate-new-decryption-platform-to-tackle-challenge-of-encrypted-material-for-law-enforcement

A cikk APA szabály szerinti hivatkozása

Szabó Cs. & Europol European Cybercrime Centre (2024). Az Europol szerepe a kiberbűnözés elleni küzdelemben. *Belügyi Szemle*, *72*(9), 1599–1607. https://doi.org/10.38146/BSZ-AJIA.2024.v72.i9.pp1599-1607

Nyilatkozatok

Összeférhetetlenség

A szerzők nem jelentettek összeférhetetlenséget.

Finanszírozás

A szerzők nem kaptak pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Nyílt hozzáférésről szóló tájékoztatás

Jelen cikk a Creative Commons Attribution 4.0 International License (CC BY NC-ND 2.0) (https://creativecommons.org/licenses/by-nc-nd/2.0/) feltételei szerint publikált Open Access közlemény, melynek szellemében a cikk bármilyen médiumban szabadon felhasználható, megosztható és újraközölhető, feltéve, hogy az eredeti szerző és a közlés helye, illetve a CC License linkje feltüntetésre kerülnek.

Levelező szerző

A cikk levelező szerzője Szabó Csaba, aki a csaba.szabo3@bm.gov.hu e-mail címen érhető el.