CTI elemzés

Az internet sötét oldala

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

Bevezetés
A dark web helye a modern kiberbiztonságban

A digitális tér fejlődése egyre bonyolultabb kockázati környezetet teremtett, amelyben a hagyományos hálózatvédelmi eszközök és stratégiák önmagukban nem elegendők a támadások megelőzésére. A dark web – a rejtett internetes szegmens – mára a kibertámadások és az illegális szolgáltatások szervezett, professzionális hátországává vált. A közbeszéd gyakran egysíkúan, a bűnözés szinonimájaként hivatkozik rá, pedig technológiai értelemben semleges infrastruktúráról van szó, amelyet politikai aktivisták, újságírók és civil jogvédők is használnak az anonimitás megőrzésére. A kiberbiztonsági szakemberek szemszögéből azonban a dark web stratégiai jelentőségű hírszerzési tér, ahol a támadók eszközöket, módszertant, hozzáféréseket és információkat értékesítenek vagy cserélnek.

Az elmúlt évtized során a dark web piacterei és fórumaiból olyan ökoszisztéma fejlődött ki, amely a kiberbűnözés ipari méretű szolgáltatásaival támogatja a támadások előkészítését, lebonyolítását és monetizálását. A „Ransomware-as-a-Service", „Phishing-as-a-Service" vagy éppen a hitelesítő adatok kereskedelme mind azt mutatja, hogy a fenyegetések ma már modulárisan vásárolhatók, akár technikai tudás nélkül is.

A védelmi oldal szempontjából ez a folyamat kettős kihívást teremt. Egyrészt a támadási kapacitások demokratizálódása miatt szinte bárki számára elérhetővé váltak profi eszközök. Másrészt a fenyegetési hírszerzés (Threat Intelligence) szempontjából soha nem látott lehetőségek nyíltak a támadók motivációinak, célpontlistáinak, működési

logikájának és taktikáinak megismerésére.

Ennek a tájékoztató dokumentumnak az a célja, hogy átfogó képet adjon a dark web működéséről, struktúrájáról, kiberbűnözési ökoszisztémájáról, a monitoring módszereiről és a védekezési stratégiákról. Az elemzés során kitérünk a technológiai alapokra, a támadási trendekre, a szektorális célpontképzésre, valamint a dark web-felderítés etikai és jogi dilemmáira is. A részletes esettanulmányok pedig rávilágítanak arra, hogyan lehet a láthatatlan térből származó információkat a gyakorlatban védelmi előnnyé alakítani.

A dark web technológiai architektúrája
Anonimitás és elosztott infrastruktúra

A dark web technológiai alapjai elsősorban azon a törekvésen nyugszanak, hogy a kommunikációs és tárolási folyamatok visszakövethetetlenek, decentralizáltak és titkosítottak legyenek. Bár a fogalom legtöbbször a Tor hálózattal azonosul, a valóságban több különböző architektúra működik párhuzamosan, amelyek mind más-más technológiai megközelítést alkalmaznak az anonimitás biztosítására.

A Tor (The Onion Router) a legismertebb rendszer, amely több ezer reléből és ún. „rejtett szolgáltatásból" áll. A Tor kliens forgalmat többrétegű titkosítással burkolja be, majd véletlenszerűen választott útvonalon küldi tovább. Az adatok három relén haladnak át, ahol minden relé csak a következő célállomás információját ismeri, így a küldő és a fogadó fél kiléte technológiai szinten szétválik. A Tor .onion végződésű domaineket használ, amelyeket a hagyományos DNS-rendszer

nem tud feloldani. Egy szolgáltatás eléréséhez a kliens lokálisan generált „descriptor” fájlt használ, amely megadja a kapcsolódási információkat.

A Freenet más modell szerint működik: egy tartalom-orientált peer-to-peer hálózat, amelyben a fájlok töredezett, redundáns formában, titkosítva tárolódnak a csomópontok gépein. Az I2P (Invisible Internet Project) szintén anonim kommunikációt tesz lehetővé, de rövid távú, egyirányú alagutakat (tunnels) használ, ahol a kapcsolatdinamika folyamatosan változik.

Egyre gyakoribbak az alternatív megoldások, amelyek kifejezetten az ipari méretű illegális kereskedelem és támadás-előkészítés igényei szerint fejlődnek. Ilyenek például a Toron belüli privát hálózati szegmensek vagy a decentralizált piacterek, amelyek blokklánc-alapú reputációs rendszerekkel párosulnak. Az új generációs dark web szolgáltatások kiegészültek olyan funkciókkal, mint:

- AI-vezérelt keresők és ajánlórendszerek, amelyek tematikusan rangsorolják a termékeket,
- kriptovaluta escrow rendszerek (pl. Monero vagy ZCash integráció),
- többfaktoros autentikáció,
- automatikus titkosított chatmodulok.

Technológiai szempontból a dark web egy állandóan változó, dinamikus ökoszisztéma, ahol a szolgáltatások nagy része csak rövid ideig él. Egy .onion piactér vagy fórum akár néhány hét alatt eltűnhet, átköltözhet új címre, vagy több klónoldalon is megjelenhet.

A skálázhatóság és anonimitás kombinációja teszi lehetővé, hogy a támadók professzionális szolgáltatásokat nyújtsanak: a ransomware kampányok adminfelületeitől a hitelesítő adatok kereshető adatbázisáig minden infrastruktúra rejtve marad a hagyományos monitoring eszközök elől.

A dark web támadási ökoszisztémája
Szereplők, piacok és szolgáltatások

A dark web önálló, iparszerűen szervezett támadási ökoszisztémát hozott létre, ahol világosan elkülöníthetők a különböző szereplők és az általuk kínált szolgáltatások. Az itt működő környezet sokkal fejlettebb, mint amit a kívülállók gyakran feltételeznek róla: jól kiépített piacterek, professzionális ügyfélkiszolgálás és reputációs rendszerek alkotják azt az üzleti logikát, amely révén a

kiberbűnözés gyakorlatilag kiszervezhető folyamattá vált. A támadási láncban megjelennek olyan specializált csoportok, amelyek kizárólag a kártékony szoftverek fejlesztésére koncentrálnak, más szereplők a már feltört hálózatokhoz kínálnak hozzáféréseket, míg egy harmadik réteg az adatok értékesítésére vagy a zsarolási folyamat lebonyolítására szakosodik. Az így létrejövő moduláris modell lehetővé teszi, hogy akár technikai tudással alig rendelkező személyek is komplex támadásokat rendeljenek meg egyetlen platformon, előre összeállított csomagok formájában.

A dark web kereskedelmi infrastruktúrája ennek megfelelően nem véletlenszerű fórumok gyűjteménye, hanem egyre inkább strukturált piacok rendszere, ahol a szereplők reputációját vásárlói visszajelzések, hitelesítő mechanizmusok és escrow szolgáltatások erősítik meg. Egy tipikus piactér lehetőséget ad arra, hogy egy érdeklődő akár szektor, régió vagy támadástípus szerint válogassa ki a célpontját, miközben részletes statisztikákat lát az eladó megbízhatóságáról és múltbeli tevékenységeiről. Ez a professzionalizálódás egyúttal azt is jelenti, hogy a támadási ökoszisztéma minden részfolyamata pénzre váltható termékké vált: a hozzáférés-értékesítés, a ransomware bérbeadása, a phishing kampányok előkészítése és a kompromittált adatok eladása mind egymástól független, de szorosan együttműködő szereplők közreműködésével zajlik.

A dark web platformokon a szolgáltatások minőségét részletes útmutatók, demonstrációs videók és garanciák is alátámasztják, ami tovább csökkenti a belépési korlátokat azok számára, akik akár egyetlen sikeres támadást is üzleti lehetőségként kezelnek. Ez a közeg azonban nemcsak technikai infrastruktúrát, hanem oktatási és kapcsolati hálót is kínál. A fórumokon folyamatosan zajlik a tapasztalatok megosztása, a legújabb sérülékenységek és exploitok bemutatása, valamint a sikeres kampányok részletes elemzése. A dark web így egyszerre funkcionál piactérként, tudásbázisként és közösségi platformként, amely folyamatosan fejleszti saját szereplőinek szakértelmét.

A támadások iparszerű szervezettsége és az infrastruktúra kifinomultsága miatt a dark webet nem lehet egyszerű feketepiacként kezelni. A modelljét sokkal inkább a professzionális szolgáltatóipar logikájához lehet hasonlítani, amelyben a reputáció, a hatékonyság és a gyors reagálás mind versenyelőnyt jelent. Ez a komplexitás és átláthatatlanság az egyik legnagyobb kihívás a védekezés és a hatósági fellépés számára.

Kiberfenyegetési trendek a dark weben

A támadási módszerek evolúciója

A dark weben megfigyelhető kiberfenyegetési trendek világosan mutatják, hogy a támadók nem csupán eseti alapon próbálnak ki új módszereket, hanem stratégiai, folyamatosan fejlődő támadási modelleket építenek ki. A legnagyobb változást az elmúlt években az jelentette, hogy a klasszikus adathalászat és egyszerű malware-terjesztés mellett megjelentek a ransomware-ökoszisztémára épülő szolgáltatásalapú konstrukciók, amelyek szorosan integrálódnak a dark web platformjaihoz. A Ransomware-as-a-Service (RaaS) modellben külön entitások felelnek a kód fejlesztéséért, az infrastruktúra biztosításáért, az áldozatok feltérképezéséért, sőt a zsarolási folyamat adminisztrációjáért is. A támadások ezen formája gyakorlatilag franchise rendszerként működik, ahol a kiberbűnözés résztvevői

fix jutalékért cserébe vehetnek részt a kampányokban.

Ezzel párhuzamosan a zero-day exploitok piaca is erőteljesen bővült, és ma már nem kizárólag állami vagy felső kategóriás APT-csoportok privilégiuma. Egy jól dokumentált sérülékenység értékesítése sok esetben száz- vagy akár több százezer dolláros bevételt is jelenthet az eladónak, ami hozzájárul a támadások minőségi javulásához és a védekezésre fordított erőforrások gyorsabb amortizálódásához. A dark web tehát a sérülékenységek elsődleges elosztóközpontjává vált, ahol a vásárlók gyakran előre összeállított támadási csomagokhoz is hozzáférhetnek.

A trendek között egyre nagyobb hangsúlyt kapnak az AI-alapú eszközök, amelyek a phishing és social engineering támadások sikerességét növelik. A gépi tanulás segítségével előállított tartalmak, például személyre szabott hamis e-mailek vagy deepfake videók, olyan szintű meggyőzőerőt képesek biztosítani, amely korábban elképzelhetetlen volt. Ez különösen aggasztó a vállalati környezetekben, ahol a támadók belső kommunikációt imitálva téveszthetnek meg alkalmazottakat és juttathatnak hozzáférést rendszerekhez.

Emellett a Phishing-as-a-Service (PhaaS) konstrukciók is professzionálisabbá váltak. Már nem csupán eszközöket kínálnak, hanem teljes szolgáltatásláncot: a célpontlisták beszerzését, a kampányok lebonyolítását, a sikeres hitelesítő adatok begyűjtését és értékesítését egyetlen csatornán keresztül. Az automatizált folyamatok miatt a támadók egyszerre képesek nagy volumenű és nagy pontosságú műveleteket végrehajtani.

A fenyegetési trendek másik jelentős területe a credential stuffing és az identitásalapú támadások elterjedése. A dark web fórumokon és piactereken naponta több ezer kompromittált hozzáférési adat kerül értékesítésre, amelyekből a támadók automatikus szkriptek segítségével próbálnak bejelentkezni különféle szolgáltatásokba. Ezek a támadások kifejezetten gyorsak és nehezen detektálhatók, különösen akkor, ha a támadó böngésző fingerprintet, session cookiet vagy VPN-proxy szolgáltatást is vásárol a sikeres beolvadás érdekében.

A dark web folyamatosan megújuló támadási repertoárja azt mutatja, hogy a kiberfenyegetések nem egyszeri, hanem folyamatosan adaptálódó és finomodó jelenségek. Az elemzésük és időbeni felismerésük elengedhetetlen ahhoz, hogy a szervezetek valóban ké-

pesek legyenek proaktív védekezést kialakítani, mielőtt a támadások éles szakaszba lépnek.

Veszélyeztetett szektorok

A célzott támadások logikája

A dark web felületein zajló kereskedelem és kommunikáció világosan kirajzolja, hogy a támadók soha nem véletlenszerűen választanak célpontokat. A célpontok szegmentációja tudatos gazdasági, technológiai és pszichológiai megfontolások mentén történik, amelyek a támadási stratégiák alapját képezik. A leggyakrabban érintett szektorok közé tartozik a pénzügyi iparág, ahol a kompromittált hozzáférések, banki belépési adatok és kriptovaluta-wallet kulcsok különösen magas értéket képviselnek. A támadók számára a pénzügyi intézmények nem csupán közvetlen pénzszerzési lehetőséget jelentenek, hanem átjárót biztosítanak további pénzmosási és csalási tevékenységekhez.

Hasonlóan kiemelt célpont az egészségügyi ágazat, ahol a támadások motivációja már nem kizárólag anyagi természetű. Az orvosi adatcsomagok olyan maradandó és nehezen megváltoztatható információkat tartalmaznak, amelyek egyaránt alkalmasak zsarolásra, biztosítási csalásra és identitáslopásra. A dark web fórumain rendre felbukkannak teljes egészségügyi adatbázisok, amelyek ára sokszor magasabb, mint egy banki credential csomagé. Ez jól mutatja, hogy az adatok piaci értéke nem feltétlenül a pillanatnyi eladhatóságtól, hanem a hosszútávú felhasználhatóságtól függ.

Az oktatási és kutatási intézmények is egyre gyakrabban válnak célpontjává, különösen a felsőoktatási szektor. Az egyetemek rendszerint nagy mennyiségű kutatási és szellemi tulajdont kezelnek, miközben informatikai védelmük sok esetben alulfinanszírozott vagy széttagolt. A támadók ezt a sebezhetőséget kihasználva olyan dokumentumokat és hozzáféréseket kínálnak eladásra, amelyek akár államilag támogatott ipari kémkedéshez is felhasználhatók. A dark web felületein rendszeresen felbukkannak kompromittált egyetemi VPN-konfigurációk, kutatási anyagok vagy teljes e-mail archívumok, amelyekre kormányzati és versenyszférabeli szereplők egyaránt licitálnak.

A kis- és középvállalkozások különösen sebezhetőnek számítanak, hiszen gyakran nincsenek felkészülve arra, hogy oldalsó kapuként váljanak egy nagyobb ellátási lánc támadásának részévé. A dark web aktivitások között számos olyan példa található, amikor a támadók kifejezetten KKV-k infrastruktúráját kompromittálták, hogy onnan belépési pontot nyissanak egy nagyvállalat vagy kormányzati szervezet hálózata felé. Ezeket a támadásokat jellemzően alacsony technikai belépési küszöb és gyors monetizációs lehetőség jellemzi.

A kritikus infrastruktúrát üzemeltető iparágak, különösen a logisztikai, energia- és ipari termelő szektor szintén folyamatosan jelen vannak a dark webes kommunikációkban. Az ipari vezérlőrendszerekhez tartozó hozzáférések, SCADA konfigurációk és szoftverkulcsok időről időre kifejezetten célzott kampányok tárgyát képezik, amelyek hátterében gyakran geopolitikai indíttatású csoportok állnak. Ezek a támadások nemcsak anyagi kárt okoznak, hanem ellátási lánc zavarokat és társadalmi pánikot is kiválthatnak.

A célpontok szegmentációja tehát sosem véletlenszerű, hanem összetett döntési folyamat eredménye, amelyben egyszerre jele-

a támadók stratégiai érdeke. A szervezeteknek ezt a logikát felismerve kell felkészülniük arra, hogy a dark weben zajló előkészítő műveletek egy nap közvetlen támadás formájában csapódjanak le a saját környezetükben.

Dark web monitoring mint védekezési módszer

A proaktív kiberhírszerzés alapjai

A dark web figyelése mára a kiberbiztonsági gyakorlat egyik legfontosabb pillérévé vált, hiszen egyedül ez a tér képes korai, kontextusban értelmezhető jelzéseket adni a támadások előkészítéséről. A monitoring lényege, hogy a szervezet képes legyen a számára releváns, gyakran széttagolt és rejtett információk összegyűjtésére, majd azokat hitelesen és gyorsan értelmezni. A folyamat során a szakértők és az automatizált eszközök célja nem pusztán az adatszerzés, hanem a fenyegetési aktivitások korai detektálása, amely lehetőséget ad a megelőző intézkedések kidolgozására.

A technikai eszköztár kulcsszerepet játszik ebben a munkában. A speciális crawler rendszerek és indexelő motorok képesek a Tor hálózat .onion című oldalait, piactereit, fórumait és chatcsatornáit pásztázni, miközben folyamatosan új forrásokat fedeznek fel. Ezek az eszközök azonban önmagukban csak nyers adatot szolgáltatnak, amelyet strukturálni és verifikálni kell. A hamis pozitív találatok kiszűrése és az értelmezési kontextus megteremtése egyre inkább emberi szakértelmet igényel, különösen a célzott támadások előkészületeit rejtő zárt közösségek esetében.

A dark web monitoring során a szervezetek elsődleges célja az, hogy a kompromittált hitelesítő adatokat, a hozzáférési listákat, a belső dokumentumokat vagy a szervezet nevére vonatkozó említéseket időben felismerjék. Az ilyen találatok gyakran hetekkel vagy hónapokkal előzik meg a tényleges támadásokat. Emellett a monitoring lehetőséget ad arra is, hogy a szervezet figyelemmel kísérje az iparági trendeket, a zero-day exploitok kereskedelmét, valamint a riválisvagy beszállító cégek kompromittációját, ami ellátási lánc szintű kockázatokra is fényt deríthet.

A dark web monitoring tehát nem egyszerű technológiai feladat, hanem stratégiai hírszerzési képesség, amely a gyorsaságra, az elemzési pontosságra és a felelős döntéshozatalra egyaránt épül. A

szervezeteknek azt is el kell fogadniuk, hogy a teljes lefedettség illúziója helyett a siker kulcsa az arányos, célzott, kontextusban értelmezett adatgyűjtés. Aki képes ezt a folyamatot jól integrálni a biztonsági működésébe, nemcsak reagál, hanem proaktívan alakítja a kockázati környezetét.

Technikai és etikai kihívások

A láthatatlan tér látható korlátai

A dark web monitorozásának és elemzésének gyakorlata számos olyan akadályt és dilemmát rejt, amelyek túlmutatnak a technológiai eszközök hatékonyságán. A legnagyobb nehézséget sok esetben nem a hozzáférés vagy a gyűjtés jelenti, hanem a releváns adatok hiteles elkülönítése a zajtól és a szándékos dezinformációtól. A támadók egy része tudatosan épít be hamis szivárogtatásokat, félrevezető dumpokat és provokatív állításokat a piacterek és fórumok tartalmába, hogy reputációs vagy stratégiai kárt okozzon a célpontnak. Egy szervezet domainjének vagy márkanevének említése tehát nem jelenti automatikusan a tényleges kompromittáció tényét. Az információ értelmezéséhez kontextus, időbeli összevetés és tapasztalt elemzői kontroll szükséges, különben téves riasztások alapján születhetnek pánikszerű döntések.

Technikai oldalról a legfontosabb kihívás a dark web gyorsan változó, fragmentált szerkezete. Egy piactér vagy fórum akár órák alatt megszűnhet, átköltözhet másik címre vagy rebrandelheti magát, miközben az elérhető tartalmak nagy része örökre elveszhet. Ez a dinamika megköveteli a crawler és indexelő rendszerek folyamatos frissítését és rugalmas működését, sőt sok esetben manuális

utánkövetést, amely idő- és erőforrás-igényes feladat. Különösen nagy nehézséget jelentenek a többfaktoros vagy reputációhoz kötött belépési rendszerek, ahol a hozzáférés csak hosszú ideig épített bizalmi kapcsolatok révén történhet. Ilyen környezetekben az automatizált feltérképezés gyakorlatilag lehetetlen, ezért a szervezeteknek el kell dönteniük, milyen mértékig hajlandók erőforrást fordítani az emberi hírszerzői jelenlét kiépítésére.

Nem elhanyagolható szempont, hogy a dark web figyelése során a szervezetek számos jogi és etikai korlátba ütközhetnek. A passzív megfigyelés és az aktív részvétel határvonalai sok esetben elmosódnak, hiszen sok közösség csak regisztráció vagy interakció ellenében enged betekintést, amely egyes joghatóságokban könnyen minősülhet együttműködésnek, bűnpártolásnak vagy informatikai visszaélésnek. Mindez különösen érzékeny, ha a monitoring során folyamatban lévő bűncselekményre utaló bizonyítékok vagy személyes adatok kerülnek elő, amelyek jogszabályi bejelentési kötelezettséget idézhetnek elő. A vállalati és kormányzati szabályozások egyaránt megkövetelik, hogy a monitoring kizárólag olyan módszerekkel történjen, amelyek nem minősülnek bűnsegélynek vagy jogsértő együttműködésnek. Az ilyen helyzetek kezelése csak világos felelősségi keretekkel, előre definiált és szervezeti szinten jóváhagyott etikai protokollokkal lehetséges, amelyek pontosan meghatározzák a döntési folyamatokat, valamint azt, mikor és hogyan reagál a szervezet egy konkrét információra.

Emellett a privátszféra védelme is központi etikai kérdéssé vált. A dark weben rengeteg kiszivárgott, személyes adatot tartalmazó információ kering, melyekhez való hozzáférés sértheti a jogi előírásokat vagy a szervezet etikai normáit. A védekezés során ezért kulcsfontosságú a célhozkötött adatgyűjtés és a minimális szükséges mérték

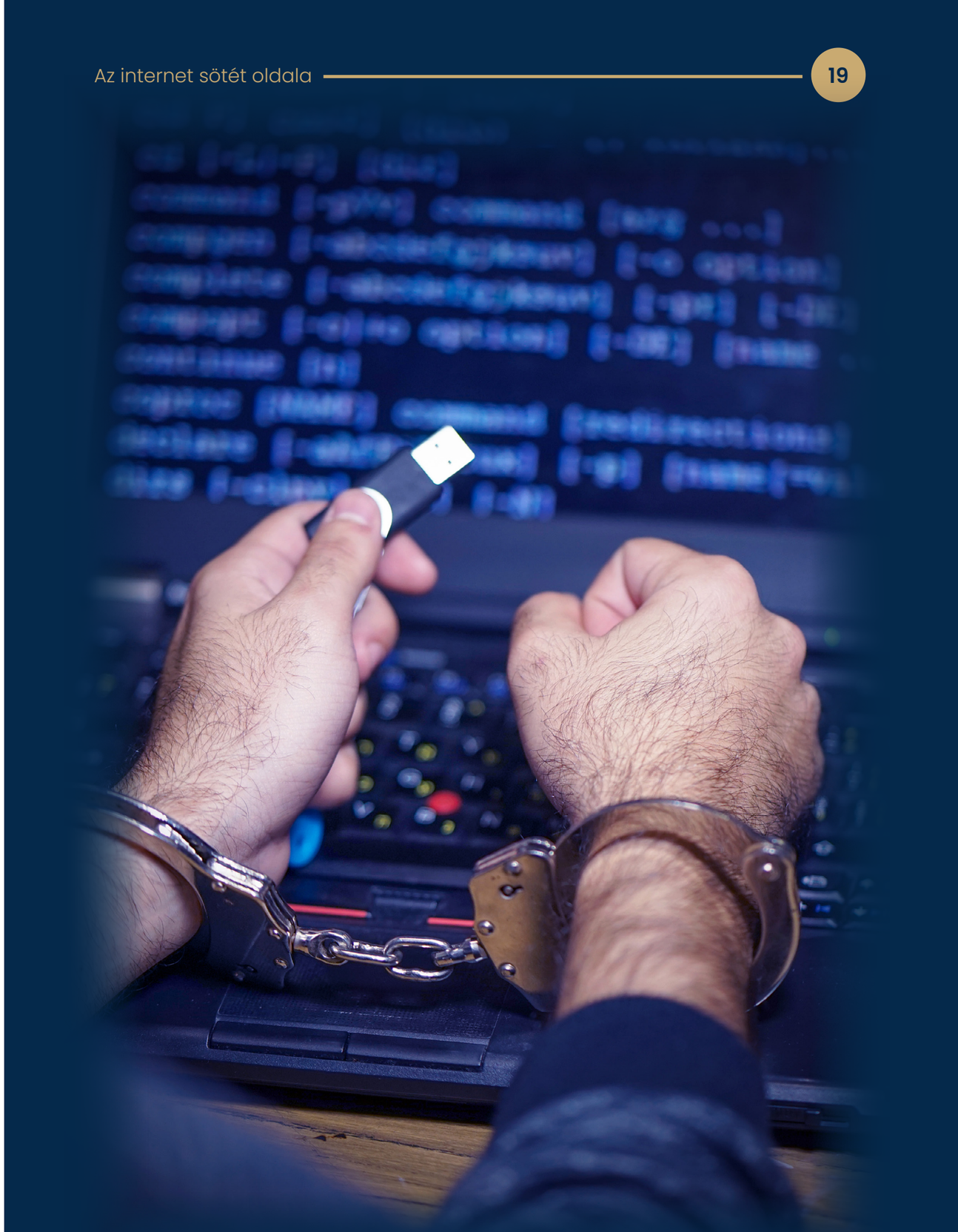
elvének érvényesítése. Mindez azt jelenti, hogy a dark web-monitoring sikeres és felelős megvalósításához nemcsak technológiai kapacitásokra van szükség, hanem érett szervezeti kultúrára, jogi tájékozottságra és etikai érzékenységre is.

Esettanulmányok

Valós támadások tanulságai a dark webről

A dark web működésének megértéséhez elengedhetetlen, hogy valós példákon keresztül lássuk, miként szerveződnek a támadások, hogyan zajlik a zsarolási folyamat, és milyen hibák vezetnek végzetes következményekhez. Az egyik legismertebb incidens a Hydra Market felszámolása, amely éveken át a legnagyobb forgalmú piactérként működött, és kiterjedt pénzmosási hálózatot tartott fenn. Bár elsősorban drogkereskedelemről vált hírhedtté, a Hydra infrastrukturális mintája számos kiberbűnözői szereplő számára szolgált példaként. A hálózat lebuktatását követően a dark web gazdasági egyensúlya átmenetileg megingott, hiszen a szolgáltatók és a vásárlók egyaránt piac nélkül maradtak. Ez az eset egyértelműen bizonyította, hogy a központosított szerverarchitektúra sebezhetősége komoly kockázati tényezőt jelent, még a legnagyobb bűnözői platformok számára is.

Egy másik súlyos incidens a Genesis Market története, amely nem csupán kompromittált hitelesítő adatokkal kereskedett, hanem komplett böngészőprofilt biztosított a vásárlók számára. Ez a technológiai újítás lehetővé tette, hogy a támadók a hitelesítés folyamatát valós felhasználói viselkedés szimulációjával kerüljék meg, így gyakran a többtényezős védelmet is kijátszották. A piactér több mint másfél mil-



lió eszköz adatait kínálta, és az ügyfelek számára rendkívül kényelmes, kereshető felületet biztosított. Az esettanulmány egyik legfontosabb tanulsága, hogy a támadók üzleti szemlélettel fejlesztett platformjai egyre inkább eltüntetik a technológiai küszöböt a bűnözés és a kíváncsi próbálkozás között.

Szintén figyelemre méltó a Conti Leak esete, amely egy rendkívül szervezett ransomware-csoport belső működését tárta fel a nyilvánosság előtt. A szivárogtatás során több ezer oldalnyi chatnapló, pénzügyi elszámolás és stratégiai terv került napvilágra, amelyek bemutatták, milyen professzionális struktúrával, prémiumrendszerrel és belső hierarchiával dolgoznak ezek a csoportok. A Conti működésének feltérképezése hozzájárult számos más támadási minta azonosításához, és világosan megmutatta, hogy az emberi tényező – legyen az árulás vagy belső konfliktus – bármely szervezet gyenge pontja lehet, még akkor is, ha bűnözői szervezetről van szó.

Egy kevésbé ismert, ám tanulságos példa egy kelet-európai kisvállalat elleni zsarolási támadás története, amelyben a támadók egy olyan jelszóval jutottak be a vállalat VPN-hálózatába, amely hónapok óta elérhető volt dark webes listákon. Az incidens során a cég partnerei is érintettek lettek, mert a támadók minden kapcsolt webshop infrastruktúráját titkosították. Mivel nem volt offline mentés és előre kialakított válságkommunikációs terv, a vállalat kénytelen volt váltságdíjat fizetni, a reputációs kár azonban így is visszafordíthatatlanná vált. Az eset rámutatott arra, hogy a dark web monitoring hiánya egyenesen üzleti összeomláshoz vezethet, különösen akkor, ha a fenyegetések hónapokkal korábban már nyilvánvalóvá váltak.

Bár Magyarország mérete és digitális piacának volumene messze elmarad a nagy nemzetközi szereplőkétől, a dark web jelensége hazánkban is jelen van, és az elmúlt években számos ügy, sajtómegjelenés és rendőrségi akció bizonyította, hogy a rejtett hálózatok magyar felhasználói körében is ismert és alkalmazott eszközök. A hazai közeg sajátossága, hogy a felhasználók motivációja, nyelvi közössége és az elérhető tartalmak jellege gyakran szorosan kapcsolódik a nemzetközi platformokhoz.

A magyar internethasználók egy részét elsősorban az adatvédelem és az online megfigyelés elkerülése motiválja a dark web elérésére. Jellemző, hogy újságírók, aktivisták, kutatók vagy adatvédelmi tudatossággal rendelkező felhasználók a Tor hálózatot nem feltétlenül illegális céllal, hanem a nyílt interneten való böngészés során is alkalmazzák, például hogy elrejtsék IP-címüket, vagy hogy hozzáférjenek a cenzúrázott külföldi oldalakhoz. Emellett megfigyelhető egy szűkebb kör, amely érzékeny témák, politikai vagy társadalmi diskurzusok miatt választja a sötét web zárt fórumait. Ezek a közösségek legygyakrabban angolul kommunikálnak, és többnyire nem önálló magyar platformokat építenek, hanem nemzetközi oldalakon jelennek meg.

A hazai illegális felhasználás egyik legismertebb formája a dark webes drogkereskedelem, amely a globális darknet piacterekhez kötődik. A Nemzeti Nyomozó Iroda tapasztalatai szerint Magyarországon elsősorban kiskereskedelmi jelleggel történik ilyen típusú vásárlás: egyes fogyasztók külföldi eladóktól szereznek be különféle szereket, amelyeket postai úton rendelnek meg. Bár a nagy volumenű drogkereskedelem továbbra is inkább hagyományos csatornákon zajlik, a darknet piacterek kedvező ár-érték arányuk miatt bizonyos fogyasztói rétegek számára vonzó alternatívát jelentenek. A hatóságok beszámolói alapján különösen jellemző, hogy fiatal felhasználók kriptovalutával fizetve kísérelnek meg vásárolni, és sok esetben nincsenek tisztában a lebukás reális kockázatával.

Az elmúlt években több hazai nyomozás és sikeres akció is rávilágított arra, hogy a magyar rendőrség aktívan részt vesz a nemzetközi együttműködésekben. 2021-ben nagy port kavart ügyben számolták fel azt a pedofil fórumot, amelyet magyar állampolgárok működtettek a dark weben. A Készenléti Rendőrség Nemzeti Nyomozó Irodája több éves felderítést követően, nemzetközi kooperációval tárta fel a szerverek helyét, és hat személyt tartóztattak le gyermekpornográfia terjesztése miatt. Egy másik ismert esetben – amely 2024-ben került nyilvánosságra – az FBI jelzése alapján a magyar rendőrök elfogtak egy darknet-drogkereskedőt, aki három év alatt közel százmillió forint értékű tiltott szert közvetített külföldi eladók és európai vásárlók között, teljesen digitális csatornákon. A férfi kriptovalutában bonyolította a tranzakciókat, és olyan infrastruktúrát épített, amely első ránézésre egy legális e-kereskedelmi modellre hasonlított. Az eset jól mutatja, hogy a darkneten történő kereskedelem nemzetközi jellege és az anonimitás miatt a hazai hatóságok önállóan nehezen tudnának eredményesen fellépni, ezért kulcsfontosságú a külföldi partnerekkel való szoros együttműködés.

A magyar sajtó figyelme a dark web felé az utóbbi években fokozódott, ugyanakkor a médiamegjelenések többsége inkább szenzációhajhász narratívát követ, és kevésbé törekszik a jelenség árnyalt bemutatására. A vezető hírportálok jellemzően a nagy nemzetközi ügyek – Silk Road, AlphaBay – fordításait közlik, vagy a hazai rendőrségi sikerek kapcsán írnak cikkeket, miközben a darknet valós szerkezete, működése és társadalmi kontextusa ritkán kerül részletes elemzésre. A közvélemény körében emiatt a dark webről kialakult kép többségében torz, félelemmel és tévhitekkel átszőtt, sokan például a mélywebet és a dark webet tévesen ugyanannak gondolják, vagy minden rejtett szolgáltatást automatikusan bűnözői tevékenységhez kötnek.

A magyar kormányzat részéről időről időre elhangzanak figyelmeztető üzenetek a sötét web veszélyeiről, különösen az adatlopás, a fiatalkorúak kiszolgáltatottsága és a kábítószer-kereskedelem kapcsán. Az NBSZ Nemzeti Kiberbiztonsági Intézet rendszeresen publikál tájékoztató anyagokat, amelyek a darknet kockázataira hívják fel a figyelmet, és tanácsokat adnak a megelőzéshez. Ugyanakkor egy összefogott, országos stratégia vagy állandó monitoringprogram kialakítása mindezidáig várat magára, így a felhasználók tudatossága és a szervezetek felkészültsége nagyon eltérő szinten mozog.

Magyarországon tehát a dark web jelenléte nem tömegjelenség, de egyre több szervezet, magánszemély és bűnözői kör fedezi fel a lehetőségeit. Ez a folyamat a jövőben várhatóan fokozódik, és mind a nyomozóhatóságoknak, mind a társadalomnak fel kell készülnie arra, hogy az anonimitás és a digitális pénzügyek összefonódása új kihívásokat teremt a bűnüldözés, a jogalkotás és a kiberbiztonsági védekezés területén.

Ezek a példák egyértelműen bizonyítják, hogy a dark web tevékenységét nem lehet csupán technológiai kuriózumként kezelni. A piacterek, fórumok és szivárogtatási portálok olyan strukturált támadási archívumként működnek, amelyek időbeli kontextust és konkrét mintázatokat nyújtanak a védekezéshez. Ha egy szervezet képes ezeket az adatokat időben elemezni és a saját kockázati térképéhez igazítani, a támadások döntő része még a végrehajtás előtt felismerhető és elháríthatóvá válik.

Védelmi javaslatok és ajánlások

Proaktív biztonsági válaszok a dark web kihívásaira

A dark web megfigyelése során nyert tapasztalatok egyértelműen bizonyítják, hogy a védekezés soha nem szorítkozhat pusztán technológiai intézkedésekre. A támadók professzionális szervezettsége, szolgáltatásként működő kiberbűnözési modelljei és a pszichológiai manipuláció eszközei olyan komplex kihívásokat teremtenek, amelyekre csak többrétegű, szervezeti és stratégiai válasz adható. Mindenekelőtt kiemelkedő jelentősége van a hitelesítő adatok védelmének, mivel a kompromittált jelszavak és session tokenek a leggyakoribb termékek közé tartoznak a dark weben. A többtényezős hitelesítés bevezetése önmagában sem jelent garanciát, ha nem párosul rendszeres rotációval, erős jelszóhigiéniai programmal és a hozzáférési események folyamatos auditjával.

Ezzel párhuzamosan megkerülhetetlen a szervezeti szintű threat intelligence stratégia kialakítása, amely nemcsak a nyers adatgyűjtésre, hanem a kontextusértelmezésre és a döntéstámogatásra is kiterjed. Az incidensek jelentős része abból fakad, hogy a vállalatok nem képesek a dark weben felbukkanó jeleket megfelelő súllyal értékelni, vagy egyáltalán nem tudnak a kompromittációról, amíg annak következményei a felszínre nem törnek. A jól működő hírszerzési folyamat keretet ad a gyűjtött információk validálásához, összefésüléséhez és priorizálásához. A threat intelligence nem egy szoftverfunkció, hanem szervezeti képesség, amely kifejezett kompetenciát, kijelölt felelőst és világos folyamatot igényel.

Szintén kulcsfontosságú a rendszerszintű hardening, amely a támadók által előszeretettel kihasznált gyenge pontok lezárását célozza. A tapasztalatok szerint a legtöbb sikeres támadás nem kifinomult 0-day exploitokra, hanem egyszerű, be nem foltozott sérülékenységekre vagy felügyelet nélküli hozzáférésekre épül. A frissítési folyamatok és a hozzáférési jogosultságok rendszeres felülvizsgálata éppúgy nélkülözhetetlen, mint a naplózás és a detekciós képességek fejlesztése. A honeypotok alkalmazása emellett lehetőséget ad a támadási mintázatok megismerésére és az elkövetők korai azonosítására.

A védelmi stratégiát csak akkor tekinthetjük teljesnek, ha abban a szervezeti tudatosság és az emberi tényező kezelése is hangsúlyos szerepet kap. A social engineering támadások a legtöbbször a munkavállalók hiányos ismereteit célozzák, miközben a támadók a dark weben könnyedén beszerezhetik a vállalat működésére vonatkozó belső információkat. Ezért elengedhetetlen a célzott oktatás, amely valódi példákon keresztül mutatja be a veszélyeket, és felkészíti a munkatársakat a felismerésre és a megfelelő reagálásra.

Összességében a dark web adta kockázatokra adott válaszok akkor válnak hatékonnyá, ha technológiai, szervezeti és emberi szinten egyaránt integrált, proaktív védekezési képességgé állnak össze. Az incidensek következményeinek mérséklése nem csupán a detekció gyorsaságán, hanem a döntések sebességén, a kommunikáció felkészültségén és a tanulságok beépítésén is múlik.

Dark web és mesterséges intelligencia

A fenyegetések új generációja

A dark web fejlődése napjainkra egyre szorosabban összekapcsolódott a mesterséges intelligencia megjelenésével, amely a kiberbűnözés automatizálását és méretezését minden korábbinál hatékonyabbá teszi. Bár az AI alkalmazása sokáig elsősorban védekezési célokra, például anomáliadetektálásra vagy prediktív kockázatértékelésre összpontosult, a bűnözői közösségek gyorsan felismerték, hogy ugyanazok az algoritmusok új típusú támadási képességekhez is vezethetnek. A dark web fórumain és piacterein már megjelentek azok a szolgáltatások és eszközök, amelyek AI-támogatással képesek a társadalmi manipuláció, a phishing kampányok vagy épp a deepfake tartalmak előállítására.

Az egyik legfontosabb trend a phishing automatizáció. Míg korábban a megtévesztő e-mailek kézi előállítást és célzott kutatómunkát igényeltek, ma már olyan mesterséges intelligenciával támogatott csomagok érhetők el, amelyek képesek a nyilvánosan elérhető információk alapján személyre szabott levéltartalmat generálni. A támadó néhány kulcsszó vagy LinkedIn-profil megadásával percek alatt olyan szöveget hozhat létre, amely nyelvileg kifinomult és pszichológiailag meggyőző. Az AI ezen túl automatikusan optimalizálja a tárgymezőt, a megszólítást és a szöveg szerkezetét, növelve a megtévesztés sikerességét.

Szintén aggasztó fejlemény a deepfake technológiák integrációja a támadásokba. A dark weben már hirdetnek olyan

szolgáltatásokat, amelyek viszonylag alacsony áron vállalják videó- vagy hangklónok elkészítését, például vezetők vagy kulcspozícióban lévő alkalmazottak utánzására. Ezek a megoldások egyre gyakrabban jelennek meg átverési kísérletek, zsarolási kampányok és reputációs támadások eszközeként, ahol a manipulált tartalom célja a bizalom megszerzése vagy a célpont megfélemlítése.

Egy másik fontos terület a zero-day sérülékenységek felkutatása és kiaknázása, amelyet egyes körökben már gépi tanulásos modellekkel támogatnak. A támadók kísérleteznek olyan eszközökkel, amelyek automatizáltan elemzik a nyílt forráskódú komponensek vagy ismert szoftverek frissítéseit, hogy azonosítsák a potenciálisan kihasználható hibákat még a hivatalos javítások megjelenése előtt. Bár ezek a képességek eddig főként államilag támogatott csoportokra voltak jellemzők, a dark weben zajló eszközkereskedelem révén fokozatosan egyre szélesebb kör számára válnak elérhetővé.

A mesterséges intelligencia térnyerése a kiberbűnözésben ugyanakkor nem csupán új támadási technikákat hoz magával, hanem növeli a támadások sebességét, volumenét és adaptív képességét. Az AI-vezérelt rendszerek képesek valós időben reagálni a védelmi intézkedésekre, dinamikusan módosítva a támadási mintákat, így a hagyományos szabályalapú védelem egyre kevésbé bizonyul elegendőnek. A jövőben várhatóan mesterséges intelligenciák harca bontakozik ki a dark weben szervezett támadások és az azok ellen bevetett védelmi eszközök között.

E fejlemények miatt elengedhetetlen, hogy a szervezetek proaktív módon építsék be az AI-alapú fenyegetések monitorozását és a mesterséges intelligencia támogatású védekezési megoldásokat a biztonsági stratégiájukba.

A dark web gazdaságtana

Bűnözői üzleti modellek és pénzmozgások

A dark web nem pusztán technológiai infrastruktúra, hanem önálló gazdasági ökoszisztéma, amelynek szereplői jól szervezett üzleti modellek mentén működnek. A platformokon zajló tranzakciók és szolgáltatások mögött kiforrott értékteremtési és haszonmaximalizálási logika rejlik, amely a klasszikus gazdasági szerepeket – termelőt, közvetítőt és végfelhasználót – szinte maradéktalanul tükrözi. A dark web gazdaságtanát éppen ezért sok szakértő nevezte „digitális bűnözői piacként", ahol a kiberbűncselekmények szürke- és feketepiacai strukturált kínálatot és keresletet generálnak.

A legsikeresebb üzleti modell az elmúlt években kétségkívül az „-as-a-Service" konstrukció lett, amely különböző formában – például Malware-as-a-Service, Ransomware-as-a-Service vagy Phishing-as-a-Service – érhető el. E modellek lényege, hogy a technikai tudás vagy az infrastruktúra birtokosa nem maga hajtja végre a támadást, hanem szolgáltatásként biztosítja az eszközt a fizető megrendelőnek. Így a támadások skálázhatók és „demokratizálhatók", hiszen a kevésbé felkészült bűnözők is hozzáférnek professzionális megoldásokhoz. Ez a jelenség jelentős mértékben növeli a kiberfenyegetések számosságát és komplexitását.

A pénzügyi tranzakciók túlnyomó része kriptovalutákon keresztül bonyolódik, elsősorban Bitcoin, Monero és Zcash felhasználásával. Bár a Bitcoin transzparens blokklánca eleinte megkönnyítette a nyomkövetést, a bűnözői körök egyre gyakrabban választják a Monero vagy más, magasabb anonimitást biztosító tokenek használatát. A fizetések gyakran a korábban említett escrow rendszeren keresztül zajlanak, amely a platform üzemeltetőjénél zárolja az összeget, és csak akkor engedi tovább, ha a vásárló visszajelzi, hogy a termék vagy szolgáltatás megérkezett. Ez a rendszer kölcsönös bizalmat teremt egy bizalmatlan környezetben, és stabil alapot ad a piac működéséhez.

Egy másik kiemelt bevételi forma a hozzáférések értékesítése, amit Initial Access Brokerage néven ismerünk. Azok a szereplők, akik sikeresen kompromittálnak vállalati hálózatokat, távoli asztali kapcsolatokat vagy VPN-fiókokat, gyakran nem maguk hajtják végre a zsarolást vagy adatlopást, hanem értékesítik a belépési pontot a magasabb szintű támadó csoportoknak. Az ilyen hozzáférések ára a célpont méretétől és a jogosultságok szintjétől függően akár a tízezer dolláros nagyságrendet is elérheti.

A dark web gazdaságtanának különleges jelensége a reputációs rendszer, amely a bűnözői piacok egyik legfontosabb bizalomépítő mechanizmusa. A kereskedők és vásárlók visszajelzéseket hagynak egymásról, értékelik a szállítás minőségét, a termék hitelességét, a support gyorsaságát. Ezek a reputációs pontok a sötétpiaci siker kulcsai, hiszen a vevők a kockázatok miatt előnyben részesítik a magas értékelésű eladókat. A reputáció elvesztése – például csalás vagy hamisított termék miatt – azonnal a forgalom zuhanásához vezet, és gyakorlatilag ellehetetleníti a további működést.

A pénzmosás szintén a dark web gazdaságtanának alapvető eleme. A bűnözői bevételek legalizálására külön szolgáltatások állnak rendelkezésre, például mixerek és coin tumblerek, amelyek szétosztják és összekeverik a kriptoeszközöket, csökkentve a visszakövethetőséget. Az összetett láncolatok, több lépcsős váltások és peer-to-peer tranzakciók szinte teljes átláthatatlanságot eredményeznek, ami nagy kihívást jelent a pénzügyi nyomozás számára.

Összességében a dark web gazdaságtana olyan önfenntartó és folyamatosan újratermelődő környezet, amelyben a támadások már ipari logikával szerveződnek. A védekezésnek ezért nem csupán technológiai, hanem gazdasági szempontokat is figyelembe kell vennie, hiszen a bűnözői motivációk alapja minden esetben a pénzügyi haszon maximalizálása.

Kormányzati fellépés és nemzetközi együttműködés

A dark web elleni küzdelem keretei

A dark web terjedése nemcsak a vállalati kiberbiztonsági szereplőket késztette reagálásra, hanem a kormányzati és bűnüldözési szervezeteket is. Az elmúlt évtized tapasztalatai alapján világossá vált, hogy egyik ország sem képes önállóan hatékonyan fellépni e globális fenyegetéssel szemben. A dark web infrastruktúrája decentralizált, a szerverek gyakran több kontinens között vándorolnak, a kriptovaluta-tranzakciók országhatárokat nem ismerve történnek, így a hatósági beavatkozásnak is transznacionális logikát kell követnie.

Az első jelentős áttörések egyike az Operation Onymous volt, amelyben 2014-ben az Europol, az FBI és több nemzeti rendőrség összehangolt akció során közel ötven dark web piacteret kapcsolt le. E művelet a Tor infrastruktúrára épülő illegális szolgáltatások ellen irányult, és jól példázta, hogy a bűnüldözés nem feltétlenül tehetetlen a titkosított hálózatokkal szemben. Később hasonló célú razziák zárták be a Hansa Market, az AlphaBay és a Wall Street Market platformjait is, amelyek közül némelyiket hosszabb ideig titokban megfigyelték, hogy bizonyítékokat gyűjtsenek a felhasználókról.

A dark webes bűnözés határokon átnyúló jellege miatt a nemzetközi bűnüldözési együttműködés kiemelt jelentőséggel bír. Az Europol és az Interpol speciális egységeket hozott létre a kiberbűnözés és azon belül a darknet monitorozására. Ennek egyik kiemelt példája a 2017-es Operation Bayonet, amelyben az FBI, a DEA, az Europol és számos ország rendőrsége összehangoltan számolta fel az AlphaBay és a Han-

sa Market piactereket. Az akció több száz letartóztatást eredményezett, és ideiglenesen visszavetette a feketepiaci forgalmat. A korábbi, 2014-es Operation Onymous-hoz hasonlóan ezek a műveletek azt mutatják, hogy a hatóságok ma már nem tehetetlenek: beépüléssel, informátorok révén vagy technikai hibák kihasználásával a legnagyobb illegális oldalakat is fel tudják deríteni.

Nemzetközi szinten ugyanakkor nincs a dark webre vonatkozó önálló, univerzális jogszabály. Az ott elkövetett cselekmények jellemzően a meglévő bűncselekményi kategóriák alá sorolhatók – mint a drogkereskedelem, hackertevékenység vagy gyermekpornográfia terjesztése –, így a felelősségre vonás a nyílt interneten alkalmazott törvények szerint történik. A nyomozás és bizonyítás azonban új megközelítéseket kíván, mivel az anonimitás és a rejtett infrastruktúrák sajátos akadályokat gördítenek a jogalkalmazás elé. Jogalkotási oldalról az Európai Unió és az Egyesült Államok is törekszik a kiberbűnözéssel kapcsolatos szabályozások naprakészen tartására: az EU 2013-ban fogadta el a hálózati rendszerek elleni támadásokkal foglalkozó irányelvet, az ENSZ pedig egy átfogó kiberbűnözés elleni egyezmény előkészítésén dolgozik. Egyes országok az anonimizáló technológiák korlátozásával reagálnak: Kína a „Nagy Tűzfal” révén szűri a Tor-forgalmat, Oroszország a Tor betiltását is fontolgatta, Fehéroroszország pedig 2015-ben egyenesen megtiltotta az anonim hálózatok használatát – igaz, ennek betartatása nehézkes. A demokratikus államok többsége ugyanakkor továbbra is jogszerűnek tekinti ezek használatát, elismerve, hogy számos törvényes és indokolt célra is szolgálhatnak.

Az együttműködés szerves részévé vált az információmegosztás és kapacitásépítés. Szervezetek, mint az Interpol Cybercrime Directorate, az Europol EC3 vagy a Five Eyes hírszerzési szövetség, közös erőforrásokat és szakértői csoportokat hoztak létre, amelyek célja a dark

weben zajló pénzmosás, gyermekpornográfia, kábítószer-kereskedelem és kiberkémkedés visszaszorítása. Az együttműködések fontos eleme, hogy egyre gyakrabban a magánszektor – például nagy threat intelligence szolgáltatók vagy blokklánc-analitikai cégek – is közvetlen partnerként kapcsolódik a nyomozásokhoz.

A kormányzati fellépés kritikus eszköze a blokklánc-transzparencia kihasználása. Bár a Monero és más anonim kriptók megnehezítik a tranzakciók nyomon követését, a Bitcoin továbbra is sok dark web-piactér elsődleges fizetőeszköze, és a publikus ledger elemzése révén a nyomozóhatóságok képesek pénzmozgási hálózatokat feltérképezni. Ennek köszönhetően a pénzügyi útvonal visszafejtése gyakran kulcsfontosságú bizonyítékokat szolgáltat a bűnszervezetek működéséről.

Magyarország az Európai Unió tagjaként implementálta a vonatkozó uniós irányelveket, így például a 2013/40/EU számú, a kiberbűnözés elleni fellépésről szóló irányelvet is. A Büntető Törvénykönyv rendelkezései lefedik többek között a kábítószer-kereskedelmet, a gyermekpornográfiát és az információs rendszer elleni bűncselekményeket, függetlenül attól, hogy ezek a nyílt interneten vagy a darkneten történnek. Bár a Tor vagy más anonimizáló eszköz használata önmagában nem illegális, a bírói gyakorlatban súlyosbító körülményként vehetik figyelembe, ha valaki ezek segítségével, szervezett módon követ el bűncselekményt. A Készenléti Rendőrség Nemzeti Nyomozó Irodáján belül működő kiberbűnözés elleni egység rendszeresen részt vesz nemzetközi műveletekben, és több jelentős ügyet is felderített. 2021-ben például felszámoltak egy magyarok által működtetett pedofil fórumot, míg 2024-ben az FBI jelzése nyomán lelepleztek egy magyar drogkereskedőt, aki 16 országba értékesített kábítószert a dark weben keresztül, összesen mintegy 100 millió forint értékben.

A dark web elleni fellépésnek azonban megvannak a korlátai. A Tor hálózat titkosításának feltörése rendkívül nehéz, ezért a nyomozók gyakran emberi hibákat keresnek – például Ross Ulbricht, a Silk Road alapítójának esetében egy nyílt fórumon elejtett bejegyzés vezetett a letartóztatásához. Gyakran előfordul, hogy a hatóságok infrastruktúrát – például szervereket – foglalnak le, így jutva hozzá felhasználói adatokhoz. A joghatósági kérdések, a hosszadalmas nemzetközi jogsegély, valamint a titkosított bizonyítékok rögzítésének nehézségei mind lassítják a folyamatot. A bíróságoknak új típusú bizonyítékokkal – például blokklánc-tranzakciók elemzésével – kell dolgozniuk, ami további szakmai felkészültséget igényel.

A dark web elleni küzdelem ugyanakkor komoly hatékonysági és etikai dilemmákat vet fel. A lekapcsolt piacterek helyére rendszerint új platformok lépnek, sokszor decentralizáltabb és ellenállóbb architektúrával. Az üzemeltetők tanulnak a korábbi hibákból, így a bűnüldöző szervek sikerei csak ideiglenes zavart idéznek elő az ökoszisztémában. Ugyanígy vitatott a felhasználói adatok titkos gyűjtése vagy a zárt közösségekbe történő beépülés jogszerűsége, különösen, ha ezek során a nyomozók részben aktív részvételre kényszerülnek.

Összességében a kormányzati fellépés akkor lehet hosszú távon eredményes, ha nemcsak bűnügyi eszközökre épít, hanem megelőzési, edukációs és technológiai fejlesztési stratégiákat is integrál. A dark web aktivitásainak visszaszorítása ugyanis nem kizárólag a szerverek és a pénzügyi útvonalak felderítéséről szól, hanem arról is, hogy a társadalom, a vállalatok és a felhasználók tudatosabban kezeljék az adatvédelmet és a digitális lábnyomukat.

Oktatás és tudatosságnövelés

A megelőzés emberi tényezője

A dark web fenyegetéseinek mérséklése során gyakran háttérbe szorul az a felismerés, hogy a technológiai és jogi eszközök csak részben képesek ellensúlyozni a kockázatokat. A támadások túlnyomó része ugyanis az emberi hibára, figyelmetlenségre vagy tudáshiányra épül, amelyet a dark web szolgáltatásai professzionális szintre emelt módon ki tudnak használni. Éppen ezért a megelőzés egyik legalapvetőbb eleme az oktatás és a tudatosságnövelés, amely a szervezetek minden szintjén stratégiai prioritássá vált.

A vállalatok sokáig elsősorban a technikai kontrollokra támaszkodtak, például tűzfalakra, végpontvédelmi rendszerekre vagy hálózati monitoringra. Ezek azonban nem képesek kivédeni azokat a támadási vektorokat, amelyek social engineering módszerekre, például célzott adathalászatra, hamis ügyfélkommunikációra vagy ellopott hitelesítő adatok felhasználására épülnek. A dark web ökoszisztémájában ugyanis egyre nagyobb arányban jelennek meg komplex szolgáltatások, amelyek megkönnyítik a személyre szabott támadások indítását. Az előre elkészített phishing csomagok, a lopott adatbázisok és a kifinomult manipulációs sablonok együttesen drámaian növelik a siker esélyét, ha a szervezet nincs felkészülve a felismerésükre.

Egy jól kialakított oktatási program célja nem egyszerűen az, hogy a munkavállalók évente kipipáljanak egy e-learning modult. A hatékony tudatosságnövelés akkor valósul meg, ha konkrét példákon és valós eseteken keresztül mutatja be, milyen következményekkel járhat a dark weben értékesített hozzáférések és információk kompromittálódása. Különösen fontos a közép- és felsővezetők bevonása, mi-

vel ők gyakran rendelkeznek magas szintű jogosultságokkal, amelyek megszerzése elsődleges célja a támadóknak. Az ő támadási felületük ráadásul a nyilvános szereplések és kapcsolatépítések miatt kiemelkedően nagy.

A képzési programok hatékonyságát tovább növeli, ha interaktív szimulációkat tartalmaznak, például adathalászati próbariadókat vagy váltságdíjas incidensgyakorlatokat. Az ilyen megközelítés lehetőséget ad arra, hogy a dolgozók ne csupán elméletben találkozzanak a fenyegetésekkel, hanem valósághű környezetben gyakorolják a helyes reakciókat. A tapasztalat azt mutatja, hogy a rendszeres ismétlés és a gyakorlatias, narratív alapú oktatás sokkal mélyebb tudást eredményez, mint a formális, száraz szabályzatok ismertetése.

Kiemelt jelentősége van annak is, hogy a szervezetek kultúraként építsék be a kiberbiztonsági felelősséget a mindennapi működésükbe. Ehhez olyan környezetet kell kialakítani, ahol a dolgozók nem félnek jelezni, ha gyanús e-mailt kaptak, vagy hibát követtek el. A félelemkultúra ugyanis gyakran odavezet, hogy a problémákat elhallgatják, ami a dark web leak oldalakra való felkerülés után már visszafordíthatatlan reputációs kárt okoz.

A dark web fenyegetéseire adott válasz nem lehet kizárólag technológiai vagy jogi. A felkészültség emberi komponense ugyanolyan lényeges, mint az automatizált monitoring vagy a jogérvényesítés. Aki valóban csökkenteni akarja a támadások kockázatát, annak a legnagyobb hangsúlyt arra kell helyeznie, hogy minden dolgozó pontosan értse: a dark weben értékesített hozzáférések mögött legtöbbször saját figyelmetlenségük, rutinszerű kattintásaik vagy rossz jelszóhasználatuk áll. A tudás és a tudatosság ezért a leghatékonyabb és legköltséghatékonyabb védelmi réteg.

Összegzés

A dark web hírszerzési értéke és védelmi dimenziói

A dark web elemzése során világosan kirajzolódik, hogy ez a tér nem pusztán a digitális bűnözés perifériája, hanem egy komplex, önállóan fejlődő ökoszisztéma, amely mára a kibertámadások első számú inkubátorává vált. A hagyományos kiberbiztonsági megközelítések – amelyek kizárólag a periméter védelmét, a belső hálózat kontrollját és a reaktív incidenskezelést helyezték előtérbe – önmagukban már nem elegendők ahhoz, hogy a sötét térben születő fenyegetéseket időben észleljék vagy megelőzzék. A dark web ugyanis a támadók gondolkodásának és együttműködésének leképeződése, ahol az eszközök, tudás és célpontok kereskedelme a hagyományos piaci logika szerint zajlik, csak éppen rejtetten és anonim módon.

A modern szervezetek számára a legnagyobb kihívás abban áll, hogy hogyan képesek a saját kockázati profiljukhoz illeszkedő módon integrálni a dark web monitoringot a biztonsági folyamataikba, és hogyan tudják ezt a felderítési kapacitást a gyakorlatban is cselekvésre váltani. Mindez nem pusztán technikai kérdés. A hatékony védekezéshez szükséges a stratégiai hírszerzési szemlélet, a megfelelő szervezeti kultúra, a folyamatos képzés, valamint a világos etikai és jogi keretrendszer. A tapasztalatok alapján azok a szervezetek képesek proaktív módon csökkenteni a fenyegetések súlyát, amelyek nem szigetelt projektként kezelik a dark web figyelését, hanem szervesen beépítik azt a kockázatértékelési és döntéshozatali mechanizmusaikba.

A dark web jövője egyértelműen abba az irányba mutat, hogy a tá-

madási módszerek egyre kifinomultabbak, iparágra szabottabbak és automatizáltabbak lesznek. Az AI-alapú phishing támadások, a deepfake manipulációk vagy az MFA-kikerülő exploitok megjelenése új szintre emeli a kockázatot, miközben a támadók hálózatba szerveződve gyorsan adaptálódnak a védelmi innovációkhoz. Ezért a védekezés lényeges eleme, hogy a szervezetek ne csupán a támadások tüneteit próbálják kezelni, hanem előre megértsék azokat a motivációkat, üzleti modelleket és infrastrukturális mintákat, amelyek a dark web hátterében formálódnak.

A legfontosabb felismerés mégis az, hogy a dark web nem szükségszerűen legyőzhetetlen előnyt biztosít a támadók számára. Aki hajlandó energiát, szakértelmet és rendszerszemléletet áldozni a sötét tér feltérképezésére, az a támadások egy részét már a tervezési fázisban leleplezheti vagy legalább korai riasztási jeleket észlelhet. A hírszerzési előny ezért közvetlen versenyképességi tényező is, amelynek birtokában egy szervezet nemcsak védekezik, hanem a saját működését is hatékonyabbá és ellenállóbbá teszi.

A jövőre nézve a dark web monitoring és a fenyegetési intelligencia integrációja nem pusztán választható opció lesz, hanem minden nagyobb szervezet biztonsági stratégiájának kötelező alapeleme. Azok, akik képesek a technológiai, jogi és emberi tényezőket egyszerre kezelni, valódi hírszerzési fölényre tehetnek szert a támadókkal szemben. Ez pedig nemcsak a pénzügyi vagy reputációs károk mérséklésében jelenik meg, hanem abban is, hogy a digitális ökoszisztéma biztonságosabbá válik – mindenki számára.

Források

ArXiv. (2025) *Identification of malicious posts on the dark web using cyber threat intelligence.* https://arxiv.org/html/2511.23183v1 (Letöltve: 2026.01.14.)

ArXiv. (2025) *The dark side of the web.* https://arxiv.org/pdf/2504.14235 (Letöltve: 2026.01.11.)

City University of New York. (2018) *Weaving the dark web: Legitimacy on Freenet, Tor, and I2P.* https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1063&context=qb_pubs (Letöltve: 2026.01.10.)

CrowdStrike. (2025) *What is dark web monitoring?* https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-monitoring/ (Letöltve: 2026.01.12.)

Cyberint. (2025) *Initial Access Broker report 2025.* https://e.cyberint.com/hubfs/IAB%20Report%202025.pdf (Letöltve: 2026.01.13.)

EURECOM. (2017) *A comprehensive structure and privacy analysis of Tor hidden services.* https://www.eurecom.fr/en/publication/5152/download/sec-publi-5152.pdf (Letöltve: 2026.01.05.)

European Commission. (2019) *Policing the dark web: Ethical and legal issues*. https://ec.europa.eu/research/participants/documents/downloadPublic?appId=PPGMS&documentIds=080166e5c2573eef (Letöltve: 2026.01.08.)

Europol. (2017) *Internet Organised Crime Threat Assessment 2017.* https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf (Letöltve: 2026.01.06.)

Europol. (2021) *DarkMarket, the world's largest illegal dark web marketplace taken down.* https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down (Letöltve: 2026.01.09.)

Europol. (2025) *Europe-wide takedown hits longest-standing dark web drug market.* https://www.europol.europa.eu/media-press/newsroom/news/europe-wide-takedown-hits-longest-standing-dark-web-drug-market (Letöltve: 2026.01.15.)

Kaspersky. (2024) *Digital Footprint Intelligence datasheet.* https://content.kaspersky-labs.com/se/media/en/business-security/enterprise/kaspersky-digital-footprint-intelligence-datasheet.pdf (Letöltve: 2026.01.09.)

MITRE. (2024) *ATT&CK Enterprise Matrix.* https://attack.mitre.org/matrices/enterprise/ (Letöltve: 2026.01.14.)

Outpost24. (2024) *Initial Access Brokers and their links to ransomware.* https://outpost24.com/wp-content/uploads/2024/11/IAB-and-links-to-ransomware.pdf (Letöltve: 2026.01.11.)

Pivot Point Security. (2024) *Dark web monitoring use cases.* https://www.pivotpointsecurity.com/dark-web-monitoring-use-cases/ (Letöltve: 2026.01.10.)

Rapid7. (2024) *What is the dark web?* https://www.rapid7.com/fundamentals/what-is-the-dark-web/ (Letöltve: 2026.01.12.)

Rapid7. (2025) *Access Brokers report: New research reveals depth of compromise in access broker deals.* https://s29.q4cdn.com/157304370/files/doc_news/Rapid7-Access-Brokers-Report-New-Research-Reveals-Depth-of-Compromise-in-Access-Broker-Deals-with-71-Offering-Privileged-Access-2025.pdf (Letöltve: 2026.01.13.)

Reuters. (2025) *Dark web drug market busted by European and U.S. authorities*. https://www.reuters.com/world/dark-web-drug-market-busted-by-european-us-authorities-2025-06-16 (Letöltve: 2026.01.15.)

U.S. Department of Justice. (2022) *Justice Department investigation leads to shutdown of largest online darknet marketplace.* https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace (Letöltve: 2026.01.07.)

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

Kibertámadás!
podcast

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet

titkarsag@nki.gov.hu

nki.gov.hu

+36 (1) 325 7672

2025