Horváth Dávid

A kiberbiztonság kihívásai Európában és Magyarországon
Dark Net: az érem két oldala

Tartalomjegyzék

1. Bevezető

Dolgozatom témája a Dark Net, melyre egységes definíció a szerző ismeretei szerint jelenleg nem áll rendelkezésre. Hogy megértsük, fontos ismerni, de legalábbis elképzelni az Internetet, ami nem más, mint olyat hálózatok hálózata, amely emberek milliárdjai által elérhető egy közös szabvány által (Internet Protocol – IP). A gyakorlatban ez úgy néz ki, hogy egy adott Internet szolgáltató (Internet Service Provider – ISP, pl. Telekom, Digi, UPC stb..) elérést biztosít a hálózathoz a felhasználónak, amit leggyakrabban egy böngészőn keresztül ér el (80-as illetve 443-as portokat használva). Modern felhasználók többsége fejből ismer egy-két weboldalt, pontosabban azoknak az URL-ét (Uniform Resource Locator), de ahhoz, hogy teljes egészében böngéssze valaki az Internetet, szükséges egy keresőmotor (search engine) használata (pl. Google), amely segíthet megérteni a Dark Net-et. Itt szükséges bevezetni a kliens-szerver modellt, mely két csoportra bontja az Internet felhasználókat. Szemléltetés végett egy rövid példával fogom bemutatni:

Egy „x” hírportál üzemeltetője szerverként funkcionál, míg a weboldalról letöltött híreket elolvasó „y” egyén pedig a kliens. A keresőmotor nem csinál mást, mint a nyilvános IP tartományon végig menve megkeresi a tartalommal rendelkező weboldalakat, majd azokat indexeli a saját adatbázisában, amit felhasználva bárki képes böngészni az Interneten. A fenti példánál maradva, az „x” hírportálnak érdeke, hogy elérhető legyen a külvilág számára, ám vannak olyan szerverek, amelyek különböző technikákkal (melyeket majd részletesen kifejtek) szándékosan rejtve maradnak, és csak nem hagyományos módszerekkel érhetőek el.

1.1 Dark Net fogalma

Ezeknek a tartományoknak az összefoglaló neve a Dark Net. A terület annyira megfoghatatlan és tudományos téren kevéssé feldolgozott, hogy magával a fogalommal kapcsolatban is viták folynak. Sokan úgy vélik, hogy a fent kifejtett terület helyes elnevezése a Deep Web, és ezen belül annak illegális tevékenységet folytató része a Dark Net, vagy sok helyütt egybeírva Darknet, esetleg Dark Web.[i] A dolgozatkiírásnak megfelelően munkám során a Dark Net kifejezést fogom használni.

1.2. Dark Net elérése

A fenti bevezetőből kitűnik, hogy a Dark Net legfontosabb kritériuma, hogy hagyományos úton nem érthető el (pl. keresőszoftverrel). Továbbiakban bemutatok két eljárást, amivel elérhetőek az ilyen hálózatok.

1.2.1. Elérés Tor-on keresztül

Az utóbbi évek buzzword-jévé vált a Tor (The Onion Ring), különösen Snowden 2013-as kiszivárogtatásai után. A Tor-t legtöbben anonim böngészés céljából használják, de ami a téma szempontjából ennél is fontosabb, az ún. hidden service-ek üzemeltetésére.

A Tor működési elve az onion routing-on alapul, melynek lényege, hogy a csomagok relay-eken keresztül több rétegnyi titkosítással (mint a hagyma rétegei) mennek keresztül az Interneten, és mindegyik relay csak egy rétegnyi titkosítást tud visszafejteni, úgyhogy nem tudja kitől jött a csomag, csak hogy merre kell továbbítani. Ezáltal a felhasználó anonim módon böngészheti az Internetet.

Két módszer van a Tor-on keresztül böngészésnek. Egyrészt elérhető a Tor saját böngészője (Tor browser – a Firefox-nak egy módosított változata) minden operációs rendszerre. Kifinomultabb felhasználók maradhatnak a megszokott böngészőjüknél (pl. Chrome), csak futtatni kell a tor-t, mint programot (pl. Linuxon „*service tor start*” paranccsal), a böngészőnél pedig be kell állítani, hogy a 9050-es portot használja proxy-ként.

Visszatérve a hidden service-ekhez, a korábban említett szerver-kliens modellnél maradva, valaki dönthet úgy, hogy az általa üzemeltett szolgáltatás csak a Tor-on keresztül legyen elérhető. Ilyen esetben a felhasználó az alkalmazást telepítve rövid konfigurálás és minimális üzemeltetési ismeretekkel könnyedén beállíthat egy hidden service-t (két sor beírása a Tor konfigurációs fájljában). Ekkor a rendszer generál számára egy URL-t, melynek első tagja számok és az angol ABC betűiből álló random sorozat, míg a vége minden esetben -*.onion (pl. http://32rfckwuorlf4dlv.onion).

Innentől kezdve az adott szolgáltatás csak a Tor-on keresztül érhető el, ami biztosítja, hogy ne lehessen megállapítani honnan, és milyen IP címről üzemeltetik. Minden más szempontból ugyanolyan, mint bármilyen más szerver szolgáltatás, üzemeltethető az ismertebb rendszerekkel (pl. Apache2), csak fontos, hogy a Tor 9050-es portját fogja használni a szolgáltatás. Mivel egyedi *.onion URL-eket használ a rendszer, a keresőmotorok nem index-elik őket, a felhasználóknak ismerni kell a pontos URL-eket, hogy elérjenek szolgáltatásokat.

Itt jegyezném még, hogy vannak elérhető listák az *.onion címtartományról is, a szerző ismeretei szerint a legteljesebb a Pastebin oldalon közzétéve. [ii] Nagy különbség pl. egy

Google keresőmotorral szemben, hogy míg előbbinek az algoritmusa heti rendszerességgel az IP tartományt végigböngészi, addig a Pastebin-en közzétett és hasonló listák manuálisan vannak szerkesztve, semmiféleképpen sem teljesek vagy átfogóak, továbbá nem frissített (megfigyelhető, hogy sok link már nem él, vagy eleve nem is volt élő).

1.2.2. Elérés I2P-n keresztül

Az I2P (Invisible Internet Project) egy a Tor-hoz hasonló platform, amivel elérhető a Dark Net. Néhány különbség az I2P szempontjából a Tor-hoz képest:

- Kisebb hálózat, kevesebb felhasználó, kevésbé ismert és dokumentált
- Java-ban van megírva, ami kevésbé gépközeli, mint a C-ben megírt Tor
- Jobban van optimalizálva a hidden service-ekre, gyorsabban elérhetőek
- Teljesen megosztott a hálózat, semmilyen központi irányítása nincsen

Utolsó lényeges különbség pedig, hogy valós idejű rangsorolás van a peer-ek között, aszerint, hogy milyen valós adatátviteli kapcsolattal rendelkeznek. Tor relay esetén a felhasználó a konfigurációs fájlban megad egy adott sávszélességet (pl. 10 Mb/s), amit enged a rendszernek felhasználni, és ez automatikusan valid-nak van elfogadva, függetlenül attól, hogy ez a gyakorlatban megvalósul-e vagy sem.

2. Példák

2.1. Negatív példák

Mivel a Dark Net nehezen elérhető és lekövethető, sokan használják illegális tevékenységre (innen a Dark elnevezés, illetve a rosszhíre a kifejezésnek). A teljesség igénye nélkül az alábbi szolgáltatások érhetőek el különböző weboldalakon:

- Fegyverkereskedelem
- Kábítószer kereskedelem
- Lopott bankkártyák, hitelkártyák értékesítése
- Pénzmosás
- Bérgyilkos szolgáltatások
- Illegális szerencsejáték
- Hamis igazolványok, útlevelek készítése
- Hacker szolgáltatások bérbeadása
- Illegális pornográfia
- Szélsőséges gondolatok terjesztése
- Könyvek, folyóiratok illegális terjesztése

- Szervkereskedelem

A listában szándékosan említek kifejezetten ijesztő példákat (pl. bérgyilkos szolgáltatások), és morális szürke zónába tartozó példákat is (pl. könyvek, folyóiratok terjesztése).

2.2. Pozitív példák

Itthon, és a nyugati országokban természetesnek veszik az állampolgárok a szólásszabadság intézményét, de kevésbé demokratikus országokban (pl. Kínai Népköztársaság) mai napig erős cenzúra működik többek között az Interneten is (pl. a kínai cenzúrát „viccesen" csak *Chinese Great Firewall*-ként említik). Napjainkban is vitatott Julian Assange tevékenysége, mindenesetre az általa alapított WikiLeaks jelenleg üzemel hagyományosan elérhető URL-n (https://wikileaks.org), illetve vélhetőleg biztonsági okokból üzemeltet egy *.onion weblapot is (http://jwgkxry7xjeaeg5d.onion). Ezen kívül több ismert folyóirat is üzemeltet hidden service-t (Wired, New Yorker, Sun, Guardian, Washington Post), ahol whistleblower-ek, újságírók, állampolgárok szivárogtathatnak információkat (pl. a New Yorker által üzemeltett Project Strongbox, http://strngbxhwyuu37a3.onion).

Egy másik történet 2011-ben, az Arab Tavasz kezdetén bontakozott ki. Az egyiptomi tüntetések idején Mubarak elnök erős cenzúrát üzemeltett és rengeteg weboldalt elérhetetlenné tett országában (pl. a Twitter-t). Ezt megkerülve sok tüntető telepítette a Tor-t, mely egyrészt biztosította a felhasználó anonimitását, másrészről elérhetővé váltak az eddig elérhetetlen weboldalak.[iii]

Érdekességként egy harmadik példa: a népszerű social media, a Facebook is üzemeltet hidden service-t (https://facebookcorewwwi.onion/). Amennyiben valaki Tor böngészővel lépett be Facebook-ba, sokszor kapott figyelmeztetéseket, hogy felhasználófiókját esetleg feltörték, hiszen a Tor automatikusan 10 percenként változtatja az általa használt kilépőpontot. A gyakorlatban ez azt jelenti, hogy a Facebook rendszere észlel egy belépést pl. Norvégiából, fél órával később az USA-ból, egy óra múlva pedig Ausztráliából. Ilyenkor a log rendszere flag-gel jelzi a gyanús tevékenységet, ami rontja a felhasználói élményt. A *.onion oldalát látogatva ellenben megszűnik ez a kellemetlenség, továbbá a felhasználó anonim marad (legalábbis ami a kapcsolódást illeti, ellenben a Facebook az általa gyűjtött egyéb meta adatok és a böngészési stílus alapján nem kizárt, hogy továbbra is tudja deanonimizálni a felhasználót). Mindenképpen pozitív példával jár elől a Facebook, remélhetőleg más oldalak is követik, hogy teljes anonimitást biztosítsanak felhasználóinak.

2.3. Hidden service-ek megoszlása

Az előbbiekben bemutattam pozitív és negatív példákat is, most igyekszem konkrét adatokkal felmérni a hidden service-ek megoszlását. Pályamunkám megírása előtt nem sokkal jelent meg egy átfogó tanulmány, Daniel Moore és Thomas Rid közös munkája, *„Cryptopolitik and the Darknet”* címmel.[iv] A szerzők egy alapos vizsgálatot folytattak az elérhető *.onion weboldalakat, illetve az abból nyíló további weboldalakat felhasználva, hogy pontosan milyen arányban oszlanak meg a tartalmak. Felhívnám a figyelmet a cikk részletes tanulmányozására, mivel jelen műben csak a végeredményt mutatom be:

- Összesen üzemelő hidden service-ek száma: 5205
- Tartalommal rendelkező hidden service-ek száma: 2723
- Beazonosíthatatlan tartalommal rendelkező hidden service-ek száma: 155
- Legális tartalommal rendelkező hidden service-ek száma: 1021
- Illegális tartalommal rendelkező hidden service-ek száma: 1547

Fenti összesítés sajnos elég sötét képet fest: még optimistán feltételezve a beazonosíthatatlan oldalakról a legális tartalmat, akkor is messze nagyobb az illegális oldalak száma. Még valósabb lehetne kapni, ha elérhetőek lennének adatok az egyes szolgáltatások időben eloszló felhasználóinak számáról, de technikailag ez kivitelezhetetlen. Fontos kiemelnem, ahogy már korábban is említettem, nem lehetséges az összes hidden service-t áttekinteni, a szerzők is két nyilvánosan elérhető listát vettek alapul (továbbá az arról nyíló további oldalakat).

3. Gyakorlati megvalósulása a Dark Net-nek

3.1. Anonim fizetés

A negatív példáknál feltűnhet az olvasónak, hogy sok szolgáltatást biztosítanak, ahol felmerül az ellenszolgáltatás módja. Nyilván hagyományos bankszámlára utalva könnyen lekövethetővé válik bármilyen tranzakció és megszűnik a Tor nyújtotta anonimitás, a készpénz esetén pedig a személyes találkozó ténye miatt veszne el a felhasználók anonimitása. Ennek elkerülése végett használnak különböző cryptocurrency-ket (pl. Bitcoin, Litecoin, Faircoin, stb..). A rendszer lényege, hogy minden felhasználónak van egy anonim tárcája (wallet) ami teljesen egyedi, és amelynek segítségével tud utalni vagy fogadni másoktól utalásokat egy titkosított rendszeren keresztül. Kívülről annyi látszik, hogy két véletlenszerű azonosítóval rendelkező egyén között adott összegű tranzakció zajlott le. Bár

több szolgáltatás is épül az adott rendszerre, az első és mai napig legnépszerűbb a Bitcoin, így a továbbiakban ezt fogom említeni.

A rendszernek köszönhetően az üzemeltetőnek nincs más dolga, mint megadni a nyilvános azonosítóját és egy Bitcoin-ban megadott összeget, amit a szolgáltatásaiért cserébe vár, majd a Bitcoin-okat beváltva hagyományos valutába, anonim módon juthat hozzá pénzéhez. Ha figyeli is valaki a felhasználóhoz tartozó pénzmozgást, csak azt tudja megállapítani, hány alkalommal és mekkora összeget fizettek ki, de az kinyomozhatatlan, hogy ki(k)hez tartozik a tárca.

3.2. Anonim levelezés

Előfordulhat, hogy az anonim fizetés mellett felmerül az igény levelezésre is a Dark Net felhasználóinak. Ilyenkor két elterjedt lehetőség áll rendelkezésre

3.2.1. Eldobható e-mail címek

Az eldobható e-mailek rendszere arra épül, hogy a weblap megnyitásakor a felhasználónak generálódik egy e-mail cím (általában random karakterekből), amelyet egy bizonyos ideig (általában 1 óra) használhat, utána megszűnik. A fiók alkalmas e-mailek küldésére és fogadására, mint bármilyen más szolgáltatónál, viszont nem követel meg semmilyen regisztrációt vagy azonosítást, Tor hálózatról is elérhető. Legismertebb a GuerillaMail (http://www.guerillamail.com).

Érdekességként a Gmail szolgáltatás elérhető Tor-ról, ám ha új felhasználót akar valaki regisztrálni, és a Gmail észleli, hogy egy Tor kilépő pontról érkezett a kapcsolat, akkor megkövetel egy telefonszámot, aminek hitelességét egy SMS-ben érkező kód megadásával kell igazolni.

Fentihez hasonló rendszerek kijátszására (hasonlóan az eldobható e-mailekhez), egyes szolgáltatók üzemeltetnek nyilvános telefonszámokat SMS-ek fogadására, különböző országokban. A felhasználó regisztrációkor megad egy ilyen nyilvános telefonszámot, majd a szolgáltatás honlapján leolvassa az érkezett SMS-ben található kódot. A fenti Gmail esetében ez a rendszer nem működik, mivel a Google figyeli, ha több regisztrációkor használják ugyanazt a telefonszámot, viszont más szolgáltatóknak nincs mindig ilyen kifinomult védelmi rendszerük.

3.2.2. Titkosított levelezés

Az online levelezés (e-mail) 3 portot használ, a POP3 (port 110), az IMAP (port 143), és az SMTP (port 25) portokat. Az e-mailezés részletei nélkül annyit érdemes tudni, hogy mindhárom port alapjáraton titkosítatlan. Egyes szolgáltatók használják az SSL/TLS (Secure Sockets Layer/Transport Layer Security) technológiát (POP3S – port 995, IMAPS – port 993

és STMPS – port 465), amelynek segítségével a felhasználó és az e-mail kiszolgáló (pl. Gmail) között a kapcsolat titkosított lesz. Ez hasznos lehet, ha pl. a későbbiekben említett exit relay üzemeltetésével, vagy épp egy man-in-the-middle támadással akarja valaki a felhasználó e-mailjeit elolvasni, de fontos tudni, hogy az e-mail szolgáltatók között a világhálón titkosítatlanul megy át az üzenet. Köznapibb nyelven ez annyit tesz, hogy az e-mail szolgáltató belelát a felhasználó levelezéseibe. Kevesen tudják, de a Google 2014 óta nem titkolja, hogy beleolvas a felhasználó e-mailjeibe:

„Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored."[v]

Ennek megoldására találta ki Philip R. Zimmermann 1991-ben a PGP-t (Pretty Good Privacy), egy számítógépes programot, amely alkalmas a titkosításra és a hitelesítésre. A rendszert és variánsait (OpenPGP, GPG) a mai napig használják, mivel a titkosításhoz használt kriptográfiai eljárás (RSA) a mai napig biztonságos és megbízható (megfelelő kulcsmérettel). A legnépszerűbb e-mail szolgáltatónál, a Gmail-nél, egy plugin segítségével (*Mymail-Crypt for Gmail*) érhető el a rendszer, míg Linuxon pl. gyárilag telepített a GNU Privacy Guard (GPG). Fontos, hogy a rendszer Nyilvános Kulcsú Infrastruktúrán (PKI) alapul, tehát minden felhasználó rendelkezik egy nyilvános-privát kulcspárral, és amennyiben valaki ismeri egy személy nyilvános kulcsát, úgy lehetősége van számára titkosított üzenet küldésére. A PGP rendszer mai napig biztonságosként van számon tartva, nincs ismert matematikai módszer, amellyel támadható volna, 1024 bites verzióját napjainkig nem sikerült még brute froce segítségével feltörni (bár egyes szakértők szerint éveken belül ez megtörténhet), míg 2048 bites verzióját még a pesszimistább kriptográfusok sem jósolják belátható időn belül.[vi]

Történet „érdekessége", hogy Zimmermann bíróság elé került, mivel a kriptográfiai eljárását a törvényszék „munition"-ként kezelte, így a vád hadianyag illegális exportja volt vele szemben. A pert végül ejtették és Zimmermannt felmentették, ezzel egy lépéssel közelebb kerültek az emberek a mindennapokban használható privacy-hez.

Napjainkban a legnépszerűbb platform a titkosított e-mail-ezéshez a Protonmail. Újítása abban rejlik, hogy automatikusan implementálja a PGP rendszerét, és amennyiben mind az üzenet küldője és fogadója is Protonmail-t használ, a levél automatikusan titkosítva megy át. Nagy előnye, hogy a felhasználójának nem kell ismernie a saját kulcsát, a titkosítási eljárást,

vagy akár a PGP-t magát se, egyszerűen használható, mint bármelyik másik nem titkosított levelező szolgáltatás.

4. Kihívások leküzdése

4.1. Dark Net felszámolása

A Dark Net esetleges felszámolása több okból is problémákhoz vezethet. Ahogy korábban is említettem, morális okokból is kérdéses, hiszen nem feltétlenül „rossz" a rendszer, csupán vannak, akik visszaélnek vele.

Az erkölcsi részétől eltekintve, gyakorlati problémák is felmerülnek. A hidden service-ek megszüntetéséhez a Tor-t magát is meg kellene szüntetni, ami körülményes, tekintve, hogy egy szabványról, egy protokollról beszélünk, és nem fizikai gépekről. A gyakorlatban ez úgy néz ki, hogy véges számú Tor relay-ek üzemelnek, amik közvetítik a titkosított kapcsolatot keresztül a világon, és ezáltal válik lekövethetetlenné a felhasználó. Ezeknek egy speciális fajtája az exit relay vagy exit node, a kilépési pont, amelyen keresztül a felhasználó eléri a látogatni kívánt weboldalt. Az exit relay-ek nyilvánosak, hiszen ez az utolsó stádiuma a kapcsolódásnak, ezek jellemzően önkéntesek gépén futó szolgáltatások, melyekről lehet tudni, hogy csak kilépési pontként szolgálnak (olyannyira, hogy a Google pl. detektálja, hogy a felhasználó Tor-on keresztül böngészik). Ezek a kilépő pontok könnyen beazonosíthatóak IP cím és szolgáltató által, viszont üzemeltetésük beszüntetése két szempontból is indifferens lenne.

Egyrészről egyből feltűnnének helyettük mások, akik saját gépükön folytatják a kilépőpont üzemeltetését. Egy Tor exit relay bekonfigurálása nem bonyolultabb a korábban már említett hidden service-nél, egy 1Mb/s-os Internet eléréssel stabil kilépőpontot lehet üzemeltetni. Érdemes megjegyezni, hogy napjainkban 1 Gb/s-os Internet előfizetési csomagokat kínálnak lakossági ügyfeleknek, a havi magyar átlagkereset ~5%-áért, vagyis elérhető áron.

Másrészről, aki érti a rendszer felépítését, az tudja, hogy a kilépési pont üzemeltetőjén keresztül se az esetleges illegális tevékenységet folytató egyént, se az azt igénybe vevő egyént nem lehetne elérni, tehát a valódi probléma megoldásához nem vezetne közelebb. Érdekességként az éppen aktuálisan üzemelő Tor kilépő pontok listája elérhető az alábbi weboldalon: https://torstatus.blutmagie.de/

4.2. Csapda állítása

A Dark Net felszámolása mellett alternatíva lehet az ott nyújtott illegális szolgáltatások igénybe vevőit csapdába csalni és beazonosítani.

Tételezzük fel, hogy az egyszeri „A” felhasználó kábítószert szeretne vásárolni online, és azt hallotta, hogy a Tor-on keresztül anonim módon tud böngészni. Ha egy jóindulatú „B” felhasználó szeretné beazonosítani „A” felhasználót, létrehozhat „csaliként” egy nem titkosított (80-as port-on futó) hagyományos HTTP weboldalt, mely illegális szolgáltatásokat hirdet magáról. Emellett „B” üzemeltet nagyobb mennyiségű kilépőpontot (mely se sávszélesség, se fizikai erőforrás szempontjából nem igényel különösebb eszközöket). Így van rá esélye, hogy az ő kilépő pontján keresztül csatlakozik „A” a weboldalra, és mivel nem titkosított a kapcsolata, az átmenő csomagokat könnyedén tudja szűrni és megvizsgálni (minél több kilépő pontot üzemeltet, annál nagyobb rá az esélye). Ebben az esetben „A” abban a hitben, hogy anonim a kapcsolata, megad személyes adatokat, elérhetőséget a weblapon (pl. telefonszám, postai cím, e-mail cím), mivel „B” úgy készítette el a weboldalát, hogy ezek megadása szükséges legyen. A csomagszűrést a tcpdump nevű programmal könnyedén végre lehet hajtani (Linuxon előre telepített), erre épül egyébként a népszerű és felhasználóbarát grafikus felülettel rendelkező Wireshark is (Windows-os felhasználók számára).

Amennyiben „B” sikeren „csapdába ejt” egy „A” felhasználót, az már elvezetheti egy hidden service-t üzemeltető egyénhez.

4.3. Csapda állítása 2.0

Az Interneten jelenleg is elérhető több olyan szoftver, amellyel a hidden service-ek elérhetőek a Tor böngésző használata nélkül. Példaként a Tor2web (https://tor2web.org/) használatához a *.onion site végére egy *.to domain nevet kell írni (pl. https://duskgytldkxiuqc6.onion.to/), és innentől kezdve a hagyományos böngészőn is elérhető a *.onion site.

Mivel nem Tor böngészővel irányul a felhasználó kérése a szolgáltatóhoz, ezért annak publikus IP címe ismert a szolgáltatónál. Az IP cím ezután egy adatbázisban összepárosítható a lekért *.onion site-tal. Innen már csak egy lépés, hogy a szolgáltató összeszedje a legnépszerűbb, illegális tevékenységet folytató Dark Net oldalak *.onion oldalát (Pl. a Silk Road-ét), és kiszűrje a rosszindulatú felhasználókat. Természetesen egy illegális szolgáltatást hirdető weboldal látogatása még önmagában nem illegális, de kiindulási pont lehet egy a potenciálisan illegális szolgáltatást használó egyének listája.

4.4. Deanonimizálás

Következő elképzelés egy kissé komplexebb eljárás, de elvben jó eséllyel jelenthet megoldást a kihívásokra. Adott a Dark Net, ahol a legnagyobb védelmet az anonimitás nyújtja. Ha az anonimitást nyújtó rendszert (Tor) nem is lehet megszüntetni, de az egyén anonimitását kompromittálva, egyénenként megszüntethető a fennálló helyzet.

Adott egy „A" egyén, aki valamilyen oknál fogva egy hidden service útján kezd el lopott bankkártyákat árulni egy *.onion-os weblapon keresztül, legyen ez „B". A probléma, hogy senki más nem tudja, hogy a „B" oldalt az „A" egyén üzemelteti, csak „A". A cél „A" azonosítása, anélkül, hogy bármi módon kompromittálódna a rendszer (Tor), amely összekapcsolja „A"-t a „B" weblaphoz. A deanonimizálási folyamatot a példánál maradva mutatom be.

Legyen „A"-nak egy nyilvános Facebook profilja is, „C", amely teljesen legitim és egyértelműen „A"-hoz köthető. Ha valamilyen módon sikerülne összefüggést felállítani „B" weboldal és „C" profil között, az egyértelműen igazolná, hogy „A" egyén áll a „B" weboldal mögött is. Ilyen összefüggés akkor állítható fel, ha feltételezzük, hogy mindannyiunk Internetes jelenléte olyan szinten egyéni, akár az aláírásunk.

A gyakorlatban ez úgy nézne ki, hogy egy megfelelő algoritmus végigmegy egy rendkívül nagyszámú bemeneti anyag (pl. az összes nyilvános Facebook profil) és az összes (elérhető) illegális weboldal között, és ahol összefüggést talál, azt visszadobja gyanús elemként.

Az elgondolást azért tartom megvalósíthatónak, mivel 2008-ban a University of Texas két kollégája publikált egy cikket „*Robust De-anonymization of Large Sparse Datasets*" címmel.[vii] Munkájuk során megvizsgáltak egy, a Netflix által kiadott, 500.000 felhasználójuk névtelen film értékelését tartalmazó adatbázisát. Ezt összevetették az Internet Movie Database (Imdb) adataival és sikerült beazonosítaniuk névtelen felhasználókat.

Véleményem szerint a fenti cikk csak a kezdet a témában. A problémának ketten álltak neki, különösebben kiemelkedő eszközök nélkül, ráadásul lassan tíz évvel ezelőtt. Ha pl. adott lenne egy kormányzati szerv, ahol korszerű software-ekkel és szuperszámítógépekkel felszerelt csapat tevékenykedne, jó eséllyel lehetne anonim személyeket beazonosítani.

4.4.1. DNS Leak

Amikor az Internetet böngészi a felhasználó, weboldalakat látogat meg, de ahhoz, hogy kapcsolódni tudjon a kiszolgálóhoz, ismernie kell a site-hoz tartozó URL-t (pl. www.google.com). A böngésző kapcsolódik egy Domain Name System-re (DNS), amely a kérésre visszaadja az URL-hez tartozó IP címet (pl. a Google esetén ez 216.58.217.110). Ez a

felhasználók számára észrevétlenül, általában az Internet szolgáltató saját DNS-ére kapcsolódva zajlik le. Ha a felhasználó a Tor saját böngészőjét használja, akkor automatikusan véletlenszerű DNS-ekhez kapcsolódik, ami megőrzi a felhasználó anonimitását. Ellenben, ha a felhasználó saját böngészőt használ Tor-hoz való kapcsolódáshoz, és nem megfelelően konfigurálta be a böngésző DNS beállításait, akkor a saját internetszolgáltatója DNS-éhez fog továbbra is kapcsolódni, innentől kezdve a felhasználó beazonosítható lesz.

4.4.2. Command Injection Vulnerability

Az előbbi eljárás a felhasználó módszereiben talált hibát használja ki, a következő pedig egy szerver oldali sérülékenységen alapul. Egy nem megfelelően konfigurált weblap alkalmazásnál el lehet érni, hogy bizonyos utasításokat hajtson végre. Az *Open Web Application Security Project* (OWASP) az alábbi példával szemlélteti a sérülékenységet:

http://sensitive/something.php?dir=%3Bcat%20/etc/shadow

A fenti példán látszik, hogy a rosszindulatú támadó egy lekérést hajtott végre, ami kiírja az */etc/shadow* tartalmát, ami a Linux jelszavak hash-ét tartalmazza. Ez már önmagában hasznos lehet egy hidden service deanonimizálásához, de a sérülékenységet kihasználva más parancsok is lefuttathatók. Egy egyszerű ping paranccsal bármilyen IP címre küldhető a szerverről egy csomag (megkerülve a Tor-t), pl. egy olyan címre, ahol tcpdump segítségével van figyelve a csomagforgalom. [viii]

4.5. A Silk Road története

Ahogy korábban bemutattam, rengeteg illegális tevékenység zajlik a Dark Net-en, és ahogy említettem, a Tor, mint rendszer nem szüntethető meg. Ellenben a Silk Road története talán alapot adhat jövőbeli tevékenységekhez az illegális szolgáltatások leküzdéséhez.

A Silk Road jól összegzi eddigi munkámat: Tor hidden service-t (*.onion weblapot) használva illegális szolgáltatásokat (főként kábítószer kereskedelmet) bonyolítottak le, cryptocurrency (Bitcoin) fizetőeszközzel. A Silk Road világszerte ismertté vált, de mégis lenyomozhatatlan maradt. Végleges megszüntetéséhez hagyományos módszereket kellett igénybe venni.

Az FBI azzal kezdte a nyomozást, hogy megkereste a legelső (nem Tor-on megosztott) bejegyzést, ami említi a Silk Road-ot:

„I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I'm thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it.

I found it through silkroad420.wordpress.com, which, if you have a tor browser, directs you to the real site at http://tydgccykixpbu6uz.onion.

Let me know what you think...”

Miután a poszt szerzőjének tevékenységét megfigyelték, kiderült, hogy az illető keresett egy Bitcoin technológiában jártas szakembert, és elérhetőségnek egy e-mail címet adott meg, mint később kiderült, a Silk Road tulajdonosának e-mail címét…

Az e-mail címhez tartozott egy Google+ fiók, amihez név és egyéb személyes adatok is tartoztak. Innentől a nyomozás részletei kissé homályosak, valószínűleg az FBI-nak nem érdeke minden részletet nyilvánosságra hozni, de a konklúzió egyértelmű: az emberi faktor szerepe. Bármennyire is tökéletes egy adott technológia (Tor), az emberi tényező mindig közrejátszik.

Érdemes megfigyelni a történet negatív oldalát is, egy hónappal a Silk Road bezárása után elindult a Silk Road 2.0, változatlan rendszer mellett, ugyanazokkal az üzemeltetőkkel, csak más vezető irányítása alatt. Egy év alatt azt is megszüntették, ellenben a Silk Road 3.0 a mai napig üzemel. A minta egyértelmű, ahogy azt már korábban a Tor exit relay-ek esetén is kifejtettem.

Jelenleg ami szükséges egy ilyen szolgáltatás üzemeltetéséhez egy rossz szándékú egyénnek, azt már mind kifejtettem írásomban:

- Minimális hardware igények a hidden service-hez
- Minimális sávszélesség igények a hidden service-hez
- A fenti követelmények megléte 24/7-ben
- Egy Bitcoin tárca (wallet), amely létrehozása 5 perces feladat
- … Maga az illegális tevékenység, ami felköltözne a Tor hálózatára

Amíg ezek a körülmények adottak, jó eséllyel nem szüntethetőek meg az illegális tevékenységek a Silk Road adott verziójának beszüntetésével, legfeljebb egy zuhanás érhető el a Bitcoin árfolyamában… (lásd 2013 október 2.)

5. Konklúzió

A szerzőnek nem feladata eldönteni, hogy a Dark Net létezése jogos továbbá etikus-e, ahogy azt sem, mi számít használatának, és mi visszaélésnek. Tény, hogy napról napra többen ismerik meg, használják, válik megbízhatóbbá, stabilabbá és elterjedtebbé a rendszer. Fentiekben igyekeztem bemutatni, hogy rengetegféleképpen lehet használni, visszaélni vele, továbbá azt is, hogy nem tökéletes és nem is teljesen lenyomozhatatlan.

A vita egyébként a Dark Net előtti időkre vezethető vissza. Kezdetben kormányok és szabadságjogi aktivisták között zajlott, a mérleg egyik oldalán a biztonság, a másik oldalán pedig a szabadság állt, mindkettő egyformán fontos része emberi életünknek. Napjainkban azonban az egyének szintjére is eljutott a debate, és elmondható, hogy az emberek megosztottak. Legelső nagyobb, nyilvánosság elé került ilyen esemény a Watergate ügy volt a 70-es években, majd Philip Zimmermann PGP-jével kapcsolatos court case kapcsán jött elő a kérdéskör, igaz, kevesebb nemzetközi visszhanggal. 2013-ban Snowden-nek hála megint napirendre került a téma, legutóbb pedig 2016 februárjában az *FBI-Apple Encryption Dispute* kapcsán vált ismét felkapottá. Ha valaki tehát meg akarja érteni a Dark Net körüli dilemmát, érdemes tanulmányozni a *Crypto Wars* néven elterjedt jelenséget, és annak történetét.

Véleményem szerint, bárki akar foglalkozni a Dark Net körül felmerülő biztonsági kihívásokkal, először magával a hálózatok működésének alapjaival, az Internet, a hálózatbiztonság és a sérülékenységek témakörében kell elmélyülnie, hogy reálisan felmérje az aktuálisan fennálló helyzetet. Ezek után van csak lehetőség az általam bemutatott gyakorlatban alkalmazható eljárások segítségével eredményeket elérni a témában.

6. Irodalomjegyzék

i. Daniel MIESSLER: The Internet, the Deep Web, and the Dark Web, 2016. Forrás: https://danielmiessler.com/study/internet-deep-dark-web/ (2016.08.25.)

ii. Over 5000 onion link 2016, Forrás: http://pastebin.com/hWyD5ZKP (2016.08.25.)

iii. Ingmar ZAHORSKY: Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum, 2011. Forrás: http://www.monitor.upeace.org/innerpg.cfm?id_article=816 (2016.08.25.)

iv. Daniel MOORE, Thomas RID: Cryptopolitik and the Darknet, Survival, 58:1, 7-38.

v. Google Terms of Service, Forrás: https://www.google.com/intl/en/policies/terms/ (2016.08.25.)

vi. Jeremy KIRK: Researcher: RSA 1024-bit Encryption not Enough, 2007. Forrás: http://www.pcworld.com/article/132184/article.html (2016.08.25.)

vii. Arvind NARAYANAN, Vitaly SHMATIKOV: Robust De-anonymization of Large Sparse Datasets, Oakland 2008. Forrás: http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (2016.08.29.)

viii. Testing for Command Injection (OTG-INPVAL-013), Forrás: https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013) (2016.08.29.)