JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Přírodovědecká fakulta

ANALÝZA DARKNETU SE ZAMĚŘENÍM NA FORENZNÍ ZKOUMÁNÍ

Bakalářská práce

Tomáš Rýc

Vedoucí práce: Ing. Jaroslav Kothánek, Ph.D.

České Budějovice 2019

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÉ PRÁCE

Student: Tomáš Rýc

Obor – zaměření studia: Kriminalisticko-technická činnost

Katedra: Ústav aplikované informatiky

Školitel: Ing. Jaroslav Kothánek, Ph.D.

Garant z PřF: ....
(jméno, příjmení, tituly, katedra – jen v případě externího školitele)
Školitel – specialista, konzultant: ....
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Téma bakalářské práce:
Analýza DARKNETu se zaměřením na možnosti forenzního zkoumání

Úkoly práce :

1. Provést analýzu DARKNETu zaměřenou na možné páchání protiprávního jednání
   - Nastínit způsoby identifikace trestné činnosti v rámci DARKNETu
   - Analyzovat možnosti dokumentace trestné činnosti
   - Analyzovat možnosti identifikace pachatele
   - Definovat možnosti monitoringu protiprávního jednání

Hlavní cíl práce:

1. Vytvořit metodiku řešení kybernetické kriminality v rámci DARKNETu pro použití orgánů činných v trestním řízení.

   Základním kritériem pro splnění či nesplnění hlavního cíle práce bude použitelnost navržené metodiky v praxi. Metodika musí být dostatečně konkrétní a musí obsahovat všechny eventuality, které mohou při vyšetřování páchání trestné činnosti v prostředí DARKNETu nastat. Zároveň metodika musí být dostatečně robustní na to, aby nebylo možné (nebo extrémně obtížné) na základně procesních či technických pochybení napadnout předložený důkazní materiál v rámci soudního řízení.

   Pokud z teoretické části práce vyplyne potřeba tvorby metodiky pro každý typ trestné činnosti zvlášť (tj. nebude možné aplikovat navrženou metodiku na všechny typy trestných činů páchaných v prostředí DARKNet), pak bude pro každý typ či kategorii trestných činů vytvořena metodika samostatně (tzn. „per use case“)

se zohledněním, že mohou vycházet ze stejného základu (např. zabavení zařízení, ze kterého byla s největší pravděpodobností trestná činnost v prostředí DARKNET páchána).

Základní doporučená literatura :

1. Fratepietro F., Rossetti P., DEFT User Guide, http://www.deftlinux.net/
2. Carrian B., File Systém Forensic Analysis, Addison Wesley Professional, ISBN: 0-32-126817-2
3. Digvijaysinh Rathod, Darknet Forensics, Institute of Forensic Science, Gujarat Forensic Sciences University, Inida, ISSN 2278-6856
4. https://www.dataforensics.org/tor-browser-forensics/

Financování práce: ....

Vedoucí práce: ....podpis: ....

U externích vedoucích fakultní garant práce..podpis: ....

Vedoucí katedry, kde proběhne obhajoba ....podpis: ....

Případný souhlas vedoucího ústavu AV ....podpis: ....

V Českých Budějovicích dne 27. 2. 2019 Podpis studenta: ....

BIBLIOGRAFICKÉ ÚDAJE

Rýc T., 2019: Analýza DARKNETu se zaměřením na forenzní zkoumání [Analysis of DARKNET with focus on forensic research. Bc. Thesis, in Czech] – 33 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic

Anotace

Bakalářská práce se zaměřuje na analýzu DARKNETu se zaměřením na forenzní zkoumání. V práci jsou popsána protiprávní jednání vyskytující se v síti DARKNET a jejich možný způsob forenzního zkoumání. Jsou navrženy způsoby identifikace trestné činnosti, možnosti její dokumentace a analyzována možnost identifikace pachatele. Pomocí navržené metodiky je navrženo řešení kybernetické kriminality pro použití orgánů činných v trestním řízení.

Klíčová slova

Darknet, Tor, forensic research, cybercrime

Abstract

This bachelor thesis aims to analyse the DARKNET with focus on forensic research. This paper describes a variety of illegal actions which occur in the DARKNET and possible form of their forensic research. A forms of identification of the illegal actions, possibilities of their documentation and analysis of the identification of the perpetrator are suggested. By the suggested methodology is designed a cybercrime solution, which can be used by the authorities active in the criminal proceedings.

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Analýza DARKNETU se zaměřením na forenzní zkoumání" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce nebo v poznámce pod čarou.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb., v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nekrácené podobě (nebo v úpravě vzniklé vypuštěním vyznačených částí archivovaných Přírodovědeckou fakultou) elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejich internetových stránkách, a to se zachováním mého autorského práva k odevzdávanému textu této kvalifikační práci. Souhlasm dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb., zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne . dubna 2019 ____________________________

Poděkování

Touto cestou bych rád poděkoval vedoucímu bakalářské práce *Ing. Jaroslavu Kothánkovi, Ph.D.* za odborné vedení, cenné rady, připomínky, náměty, konzultace a svědomité metodické vedení v průběhu zpracování bakalářské práce. *Paní doc.RNDR. Ivě Dostálkové Ph.D* za pomoc a konzultaci práce. Panu *Ing. Petru Břehovskému* za konzultační hodiny k možnostem identifikace pachatele. Panu Ing. *Jiřímu Pokornému* za konzultaci z pohledu policejních složek. Panu Ing. *Rudolfovi Vohnoutovi* za připomínky a podněty k dokončení práce. Také děkuji své *rodině* a *přítelkyni* za trpělivost, morální podporu a rodinné zázemí v průběhu bakalářského studia.

Obsah

ÚVOD

Tématem bakalářské práce je analýza DARKNETu se zaměřením na možnosti forenzního zkoumání. Definuje pojem DARKNET a jeho umístění v kyberprostoru včetně rozdílů mezi DARKNETem, Deepwebem a Surfacewebem a zaměřuje se na možnosti forenzního zkoumání DARKNETu. Téma práce jsem si vybral z důvodu mého zájmu o anonymní prohlížeče v kyberprostoru a to nejen DARKNETu a také z hlediska zájmu o možnostech identifikace uživatele.

V současnosti informační a komunikační technologie a na ně navázané telekomunikační služby zažívají obrovský rozvoj. S tímto obrovským rozvojem je spojena vyšší konkurence na trhu, snižování cen informačních a komunikačních technologií a s tím dostupnost technologií pro širokou veřejnost. S touto dostupností technologií a služeb výrazně narůstá znalost ovládání nových technologií a softwaru uživateli. Uživatelé postupně zjišťují, že kyberprostor a v něm konkrétně internet není pouze Surfaceweb, ale i DARKNET a Deepweb. S rostoucím uměním ovládání technologií a softwaru je spojena jak legální tak také nelegální činnost uživatelů v kyberprostoru.

Práce je rozdělena na teoretickou a praktickou část. V praktické části předkládá metodiku řešení kybernetické kriminality v rámci DARKNETu pro typy trestné činnosti. Závěrem práce vyhodnocuje přínosy metodiky, a zda je možné aplikovat navrženou metodiku na všechny typy trestných činů páchaných v prostředí DARKNETu, nebo je nutné na každou trestnou činnost vytvořit metodiku samostatně.

Obsah práce je členěn do devíti kapitol, které představují hlavní okruhy DARKNETu. Kapitoly jsou dále členěny do podkapitol, ve kterých je pak daný problém podrobněji rozebrán. **První kapitola** řeší otázky cílů a použitých metod při zpracování bakalářské práce. Ve **druhé kapitole** je rozebrán kybernetický prostor se zaměřením na surfaceweb, deepweb a darkweb. **Třetí kapitola** popisuje trestnou činnost v kybernetickém. Shrnuje trestné činy proti utajování, integritě a dostupnosti dat a systémů, trestné činy související s počítači, obsahem a porušováním autorských a souvisejících práv. Způsob identifikace trestné činnosti v Dakrnetu je obsažen ve **čtvrté kapitole**, která popisuje technologie, komunikaci v síti Tor, výhody a nevýhody Toru, analýzu informací a nastavení routerů uvnitř Tor sítě. **Pátá část** je zaměřena na analýzu možnosti dokumentace. **Šestá část** klade důraz na zabezpečení při vstupu na Darknet pro orgán činný v trestním řízení. Analýza možností identifikace pachatele uvedená v s**edmé části** a popis forenzního software pro získání informací je uveden v **osmé části**. Výsledkem práce je vytvoření metodiky řešení kybernetické kriminality pro použití orgánů činném v trestním řízení uvedena v **deváté části**.

1 Cíl práce a metodika

Cílem práce je vytvořit metodiku řešení kybernetické kriminality v rámci DARKNETu pro použití orgánů činných v trestním řízení. Vzhledem k tomu, že v práci je řešena kybernetická kriminalita v trestním řízení dle zákona č. 40/2009 Sb., trestní zákoník, není v práci řešena z hlediska zákona č. 500/2004 Sb., správní řád a zákona č. 89/2012 Sb., občanský zákoníku. Tím ale není řečeno, že v rámci těchto zákonů nemůže v síti DARKNET dojít k protiprávnímu jednání. Dále popisuji způsoby jak se připojit k tomuto prostoru s důrazem na bezpečnost připojení a nastiňuji způsoby identifikace trestné činnosti, možnosti její dokumentace a analyzuji možnosti identifikace pachatele. V neposlední řadě popisuji možnosti monitoringu protiprávního jednání v tomto prostoru.

Bakalářská práce je zpracována s použitím systémového přístupu (*nashromážděním nezbytného množství teoretických podkladů pro zpracování práce a způsobu uspořádání práce*) a aplikací metod:

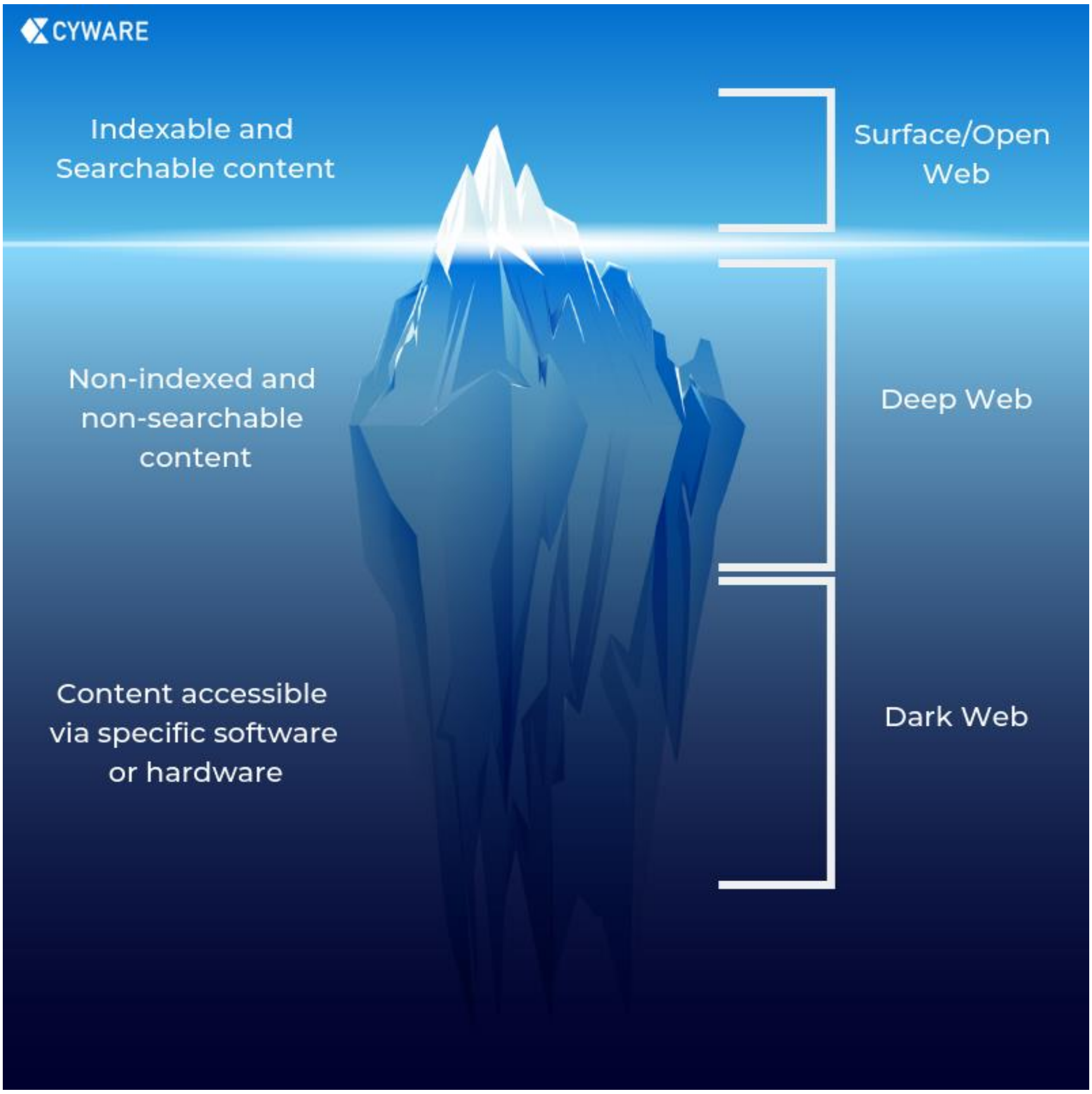
- analýza - k hodnocení kybernetického prostoru,
- syntéza - ke shrnutí jednotlivých kapitol v dílčím závěru v jeden celek,
- indukce - pro stanovení obecných závěrů trestné činnosti v kybernetickém prostoru,
- deskriptivní (*popisný způsob poznávání*) a historické metody (*heuristika - shromáždění relevantních zdrojů, bibliografie*) pro popis dosavadních poznatků z dané oblasti,
- dedukce - při vyvozování závěru na základě obecných a známých skutečností, předpokladů a tvrzení.

Z vlastních poznatků získaných studiem byla použita metoda zobecnění problému a snaha upozornit na důvody zabezpečení při vstupu na Darknet včetně nastavení prohlížeče a sociální inženýrství. Dále byly využity poznatky a připomínky expertů činných v trestním řízení, vědomosti získané při řádném studiu a ostatní praktické zkušenosti spojené v rámci využívání sociálních sítí.

2 Kybernetický prostor

Ještě do roku 2014 nebyl v České republice pojem kybernetický prostor legislativně definován. To se změnilo dnem 23. července 2014, kdy byl schválen zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen ZKB). Pojem kybernetický prostor je vymezen v §2, písm. a), ZKB takto: „*Kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikac*í."

Z výše uvedené definice si je nutné uvědomit, že kybernetickým prostorem jsou všechny informační systémy s jejich službami a sítěmi elektronických komunikací, které zabezpečují jejich propojení. V praxi se můžeme setkat s informačními systémy nepřipojenými do globální sítě Internet (dále jen Internet). Zpravidla se jedná o utajované sítě (státní, ale i nestátní) či privátní sítě společností, které z hlediska jimi definované bezpečnostní politiky nepřipouští fyzické připojení do Internetu. Pak jsou informační systémy, které jsou připojeny do Internetu. Tyto informační systémy můžeme chápat podle velikosti od minimálních (např. domácí PC a chytrý mobilní telefon) připojených pomocí wifirouteru do internetu až po složité informační systémy (desítky či stovky PC se servery a službami) připojených komplexními demilitarizovanými zónami s bezpečnostními prvky k Internetu. Všechny tyto informační systémy tvoří neomezenou, v čase se měnící síť Internet, která nezná mezinárodní hranice. Množství informací a dat, které je obsaženo v Internetu má obrovský ekonomický potenciál. To přináší zájem uživatelů a s tím spojenou jak legální tak nelegální činnost uživatelů v tomto kybernetickém prostoru. Některé publikace přirovnávají kybernetický prostor k ledovci [13], který je rozdělen na tři části Surfaceweb, Deepweb a Darkweb a to podle aplikační vrstvy v rámci sítí a služeb. Často se uvádí, že Deepweb a Darkweb společně tvoří Darknet. Úmyslně píši Darknet nikoliv DARKNET, protože takto chápaný pojem Darknet je mnohem obsáhlejší než DARKNET, který definuji ve své práci v bodě 2.3.



Obrázek 1 Kybernetický prostor [33]

2.1 Surfaceweb

Deepweb jsou vyhledávačem neindexované stránky, které jsou přístupné prostřednictvím standartních vyhledávačů, ale přístup k nim je nějakým způsobem omezen. Pojmy surface a deep web jako první uvedl Michael Bergman ve studii The Deep Web: Surfacing Hidden Value [14] v roce 2001. Jedná se o různé stránky, které nejsou z jakýchkoli technických příčin indexovány nebo se jedná o soukromé stránky, kde si vlastník nepřeje indexaci anebo o speciální stránky, kam je možné se dostat jen po splnění určitých podmínek například autentizačních např. účet na stránce (Facebooku, Youtube), e mail účet (gmail, seznam), fotka přidaná na Facebooku. Deepweb tvoří odhadem 96% veškerého obsahu Internetu.

2.2 Deepweb

Darkweb jsou stránky nepřístupné pomocí klasických prohlížečů (Google Chrome, Mozilla Firefox, Opera, Internet Explorer). Jde o anonymní šifrované sítě fungující uvnitř Internetu, na kterých běží vlastní služby. K přístupu na Darkweb je zapotřebí použít speciální software - prohlížeč (Tor, I2P, Freenet, DN42).[1]

2.3 Darkweb

Darkweb jsou stránky nepřístupné pomocí klasických prohlížečů (Google Chrome, Mozilla Firefox, Opera, Internet Explorer). Jde o anonymní šifrované sítě fungující uvnitř Internetu, na kterých běží vlastní služby. K přístupu na Darkweb je zapotřebí použít speciální software - prohlížeč (Tor, I2P, Freenet, DN42).[1]

Pojem DARKNET je v této práci chápán jako podmnožina Darkwebu, kdy se jedná o prostředí Internetu, do kterého je možný přístup pouze prostřednictvím speciálního softwaru – TOR.

3. Trestná činnost v kybernetickém prostoru

Úmluva rady Rady Evropy č. 185 ze dne 8. listopadu 2001 (dále jen Úmluva) o kyberkriminalitě sjednocuje národní právní úpravy v oblasti kyberkriminality. Česká republika ratifikovala Úmluvu 22. srpna 2013 s platností k 1. prosinci 2013. Na základě této Úmluvy byly do právních řádů České republiky implementovány takové nástroje, aby bylo možné postihovat kybernetické trestné činy. Tato kapitola vychází z [35].

Úmluva definuje čtyři základní skupiny trestných činů v kyberprostoru:

3.1 Trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů

Jedná se o trestný čin, který pachatel způsobí úmyslně s cílem neoprávněně přistoupit k celému počítačovému systému nebo k jeho části. Tento trestný čin je definován v §230 odst. 1 TZK **neoprávněný přístup a zásah do počítačového systému** a nosiče informací a jedná se zpravidla o hacking, cracking nebo computer trespass.

V případě, že pachatel využije k přístupu do systému malware, jako prostředek útoku, lze tento neoprávněný přístup přiřadit k § 230 odst. 2 TZK.

Trestným činem je i skutek kdy pachatel úmyslně provádí odposlech neveřejných zpráv. Tento trestný čin je definován v §182 TZK **porušení tajemství dopravovaných zpráv**, metodou sniffingu.

Dalším trestným činem je zásah do dat a to úmyslným **poškozením nebo vymazáním** za předpokladu že došlo k závažné škodě. Trestný čin je definován v § 230 odst. 2 písm. a) a b) TZK a je způsobován útoky malware, DoS a hackingem.

V případě **výroby, prodeje zařízení případně i softwaru vytvořeného za účelem úmyslného spáchání trestných činů** uvedených v bodě 3.1 je možné tyto činnosti postihnout dle § 230 odst. 2 a odst. 3 TZK.

3.2 Trestné činy související s počítači

Tyto trestné činy souvisí s **paděláním** a podvodem (pozměňováním) dat uložených v počítači. Musí být vykonány úmyslně pachatelem. Padělání dat uložených v počítači je postihováno dle § 230 odst. 2 písm. c) TZK.

U **podvodu** musí jít o úmysl s cílem získat sobě nebo jinému majetkový prospěch, kdy se zpravidla jedná o phishing, pharming a spear phishing. Podvod v případě podvržení stránek s cílem získání majetkového prospěchu je možné řešit § 209 TZK.

3.3 Trestné činy související s obsahem

Do těchto trestných činů v kybernetickém prostoru spadá držení, výroba a šíření nezákonných materiálů prostřednictvím Internetu. Z hlediska obsahu se z velké většiny jedná o trestné činy související s dětskou pornografií. Trestné činy související s dětskou pornografií jsou postihovány především dle § 192 výroba a jiné nakládání s dětskou pornografií.

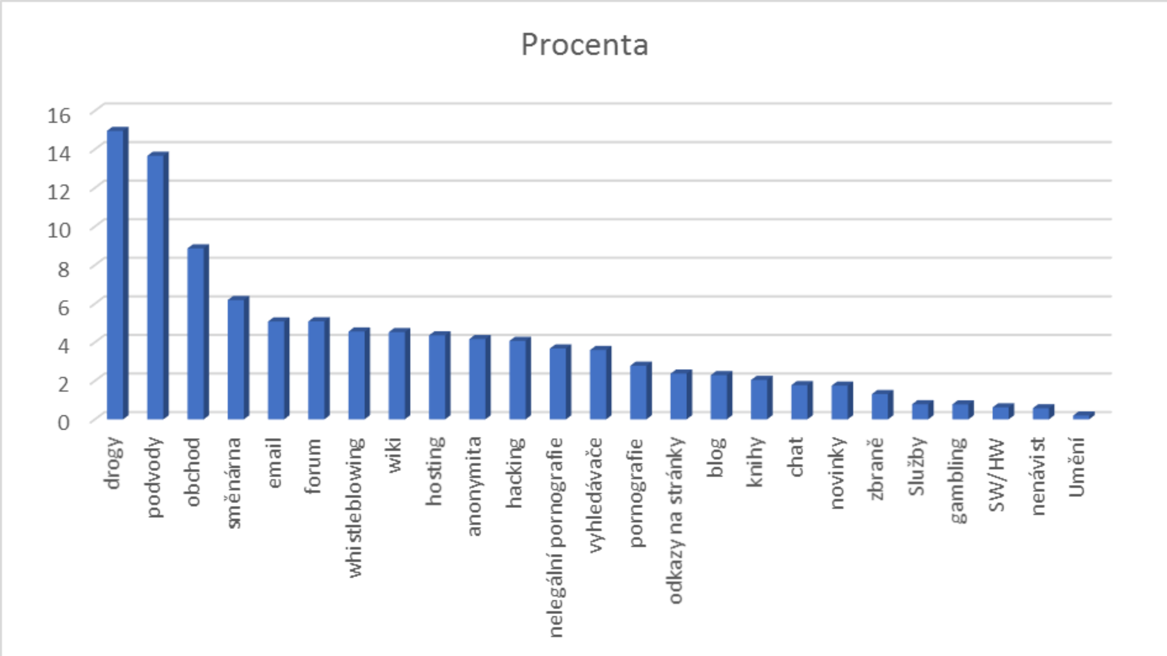
Do trestných činů souvisejících s obsahem dále spadá problematika šíření rasismu a xenofobie. V případě rasisticky a xenofobně motivované pohrůžky je uplatněn § 352 TZK, při rasisticky a xenofobně motivované urážce § 355 TZK. Šíření rasistických a xenofobních materiálů v kybernetickém prostoru je postiženo v § 356 a 403 TZK. Samostatnou kapitolou je popírání, hrubé snižování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti, které je postihováno dle § 405 TZK.

3.4 Trestné činy související s porušením autorských práva a práv souvisejících

V kyberprostoru je velmi rozšířeným trestným činem porušování autorských práv formou internetovým pirátstvím, crackingem a warezem. Trestní právo postihuje tyto činnosti podle § 270 TZK porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. U těchto trestných činů je nutné vyhodnotit účinek, tedy jak bylo zasaženo do chráněných práv a nikoliv nepatrně. Zásah do chráněných práv tedy musí být nikoli nepatrný, aby byl trestným činem.

3.5 Trestné činy vyskytující se na DARKNETu

V oblasti DARKNETu, jehož rozsah jsem pro tuto práci objasnil v bodě 1.3, je četnost činností ať již legálních či nelegálních uvedena v procentuálním vyjádření na grafu 1. Ke zjištění činností, vyskytujících se na Darknetu jsem použil pět prací[2][3][4][5][6] ve kterých jsou statistické údaje o činnostech v DARKNETu. V těchto pracech se v podobě grafu objevují hidden services (dále jen HS), což jsou vlastně servery v DARKNETu. Tyto HS v těchto pracech jsem zprůměroval, abych došel ke zjištění kolik procent HS s určitým obsahem se vyskytuje uvnitř TOR sítě. Z tohoto důvodu je možné, že se některé HS se mohou opakovat. Dohromady se vyskytovalo 53 412 HS. Některé z těchto prací neměli přesný počet serverů, takže jejich počet byl stanoven podle procentuálního grafu. Jedná se pouze o přibližný procentuální počet, ale pro představu o obsahu činností v DARKNETu je postačující.



Graf 1 - odhadovaný procentuální výskyt HS uvnitř Tor sítě

Z grafu je patrné, že na DARKNETu se vyskytuje tato trestná činnost:

a) Trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů, konkrétně – hacking, prodej nelegálního SW a HW určeného k úmyslnému spáchání trestných činů.

b) Trestné činy související s obsahem v podobě nelegální pornografie a šíření rasistických a xenofobních materiálů – forum, blogy atd.

c) Trestné činy související s porušováním autorských práv a práv prodejem nelegálního softwaru – obchod.

4. Způsob identifikace trestné činnosti v DARKNETu

Před samotným popsáním způsobu identifikace trestné činnosti v DARKNETu je nutné zvládnout technologii TOR včetně komunikace v síti a zabezpečení technologie před případným útokem na vlastní technologie.

Následně při dostatečném zabezpečení vlastních technologií je možné přistoupit do sítě DARKNET a provádět identifikaci trestné činnosti v postupných krocích. Nejdříve je nutné provést vyhledání maximálního počtu serverů v síti. Po jejím vyhledání následuje vyhodnocení obsahu podle stanovených závadných slov na jednotlivých serverech. Díky tomuto kroku se podaří snížit počty serverů s možným závadným obsahem a tyto vyfiltrované servery budou podrobeny hloubkové analýze, která odhalí servery s aplikacemi na prodej nezákonného materiálu, fora, blogy s nezákonným obsahem apod. Tato hloubková analýza by zároveň měla odhalit, zda informace na serveru naplňují skutkovou podstatu trestných činů a to jednoho či více skutků. Poté je možné zahájit dokumentaci trestné činnosti, která bude popsána v kapitole 5.

4.1 Technologie Darkentu – TOR

Pro přístup do sítě DARKNETu musíme použít speciální software nebo konfiguraci. Jedná se o speciální prohlížeče jako např. Freenet, I2P a TOR. Tato práce je zaměřena na nejrozšířenější speciální prohlížeč TOR. TOR byl vytvořen za účelem uchránění anonymity uživatele.

4.1.1 Technologie Darkentu – TOR

Komunikace po sítí funguje pomocí Onion Routeru (dále jen OR), každý OR funguje jako user level process (má svoji adresu a fyzickou paměť). OR komunikuje s dalšími OR v síti přes TLS protokol. Uživatel, když chce navázat spojení, spustí software, který se nazývá Onion Proxy (dále jen OP). OP slouží k načtení adresářů, vytvoření obvodu skrze síť a zpracovává spojení. OP přijímají Transmition control protocol (dále jen TCP), díky kterému můžou mezi sebou vytvořit spojení.

Každý OR poté podepíše TLS certifikaci, router descriptor (souhrn klíčů, adres, šířek pásma a další) a adresáře. Tyto podpisy jsou podepsány dlouhým identifikačním klíčem. OR používá ještě krátký onion klíč, který slouží k dešifrování žádosti, vytvoření obvodu a vyjednání ephemeral klíče (z důvodu komunikace mezi OR pomocí Diffie-Hellman handshake).

OP vyjedná s každým OR v obvodu symetrický klíč, s každým jednotlivě. Pro vytvoření obvodu OR pošle create cell šifrovanou onion klíčem za použití polovičního Diffie-Hellman handshake prvnímu uzlu v obvodu. Pro zvýšení obvodu OP klienta pošle za použití poloviční Diffie-Hellman handshake router extend cell přes první uzel v obvodu OR1. OR1 poté zkopíruje poloviční Diffie-Hellman handshake a pošle create cell přes druhý uzel OR2. OR2 zná pouze OR1, klient ho nepotřebuje znát. Jakmile OR2 odpoví OR1 s vytvořením cell. OR1 poté přepošle pomocí router extended cell klientovi. Pro vytvoření OR3 stačí klientovi, aby řekl poslednímu uzlu, ať vytvoří jeden hop navíc. Obvod se tvoří defaultně 3 OR, z důvodu bezpečnosti klienta, ale je možné zvýšit počet routerů.

Každý OR (OR1, OR2a a OR3) v obvodu má svůj onion klíč, kterým může šifrovat nebo dešifrovat komunikaci, OR1 zašifruje svým klíčem a pošle OR2, OR2 zašifruje svým klíčem a pošle OR3, OR3 zašifruje a pošle dál. Při odpovědi nazpět OR3 dostane odpověď a dešifruje ji svým klíčem a přeposílá OR2, OR2 dešifruje svým klíčem a pošle OR1, OR1 dešifruje svým klíčem a přepošle klientovi.[10]

Klient, když chce navázat spojení s HS vytvoří obvod 3 OR, 3. OR kontaktuje Directory server (dále jen DS), aby mu sdělil informace o HS včetně adres introduction pointů (dále jen IP). IP jsou serverem vybrané routery, které znají jeho adresu. Klient poté vybere router, aby se choval jako Rendezvous point (dále jen RP), který bude fungovat jako spojka mezi klientem a serverem (Klient se připojí k RP přes OR1 a OR2, RP se poté chová jako OR3. Server se připojí k RP pomocí svých vytvořených OR). Poté RP kontaktuje IP, aby server věděl, že klient se s ním chce spojit přes RP. IP přepošlou tuto zprávu serveru, který se rozhodne, jestli naváže s RP spojení nebo ne. Pokud ano, tak server kontaktuje RP, že chce navázat spojení. RP poté přepošle žádost klientovi. Nyní může klient komunikovat se serverem. [28]

Dešifrování komunikace při spojení se serverem probíhá v 7 krocích:

1. R1 dešifruje pomocí K1 a předá tuto zprávu dál na R2, tato zpráva je stále šifrovaná.
2. R2 dešifruje pomocí K2 a pošle na R3.
3. R3 dešifruje zprávu pomocí K3 a může přečíst co se v ní nachází, protože už není šifrovaná. R3 přečte zprávu, která bude obsahovat např. „spoj mě se serverem X“. R3 se může spojit se serverem X. Nyní pošle odpověď zpět pomocí opačného postupu.
4. R3 zašifruje pomocí K3 a pošle R2.
5. R2 zašifruje pomocí K2 a pošle R1.
6. R1 zašifruje pomocí K1 a pošle ji zpět klientovi.

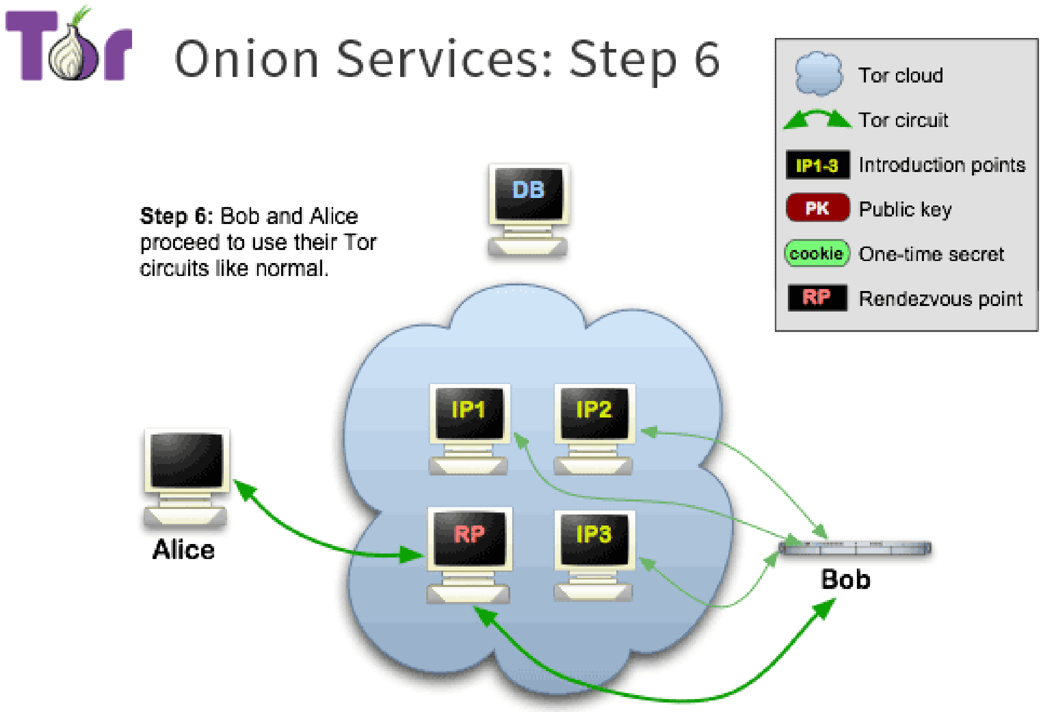
7. Klient má všechny 3 klíče, takže může dešifrovat zprávu. [8]

Poté kdyby chtěl útočník napadnout komunikaci, věděl by na prvním hopu, že se uživatel přihlásil do sítě, to je vše. Pokud by zaútočil na druhém hopu viděl by že pouze probíhá nějaká komunikace. Pokud by zaútočil na posledním hopu věděl by, že se někdo přihlašuje na server, ale nebude vědět kdo.

4.1.2 Stránky - Hidden services

V rámci TOR sítě se vytváří hidden services (dále jen HS) což jsou stránky uvnitř této sítě s koncovkou .onion. K těmto stránkám je možné se připojit jedině tak, že budeme uvnitř této sítě. Spojení mezi klientem a stránkou se vytvoří následovně:

1. Server vytvoří 3 náhodné onion routery, které se nazývají Introduction pointy (dále je IP).
2. Klient posílá žádost na onion adresu, která se skládá z 16 písmen odvozených z veřejného klíče.
3. Pokud chce klient navštívit server, musí znát jeho onion adresu. Po zadání adresy onion serveru, klient bude znát veřejný klíč a sestavení IP. Klient vytvoří pomocí náhodného routeru v síti tzv. Rendezvous point (RP) a dostane jednorázové cookie.
4. Klient sestaví přivítací zprávu, ve které bude obsahovat RP a jednorázové cookie, zašifruje pomocí veřejného klíče a zašle na náhodný IP.
5. Dešifruje se klientova přivítací zpráva a vytvoří se obvod do RP na kterou zašle jednorázové cookie.
6. Klient a server mohou pomocí svého obvodu navázat komunikaci přes RP. [8][9]



Obrázek 2 Konečná komunikace serveru a klienta [7]

4.1.3 Výhody a nevýhody TORu

Výhodou je, že jde o úplnou anonymitu, jelikož informace jde přes 3 routery v síti útočník nemá možnost tyto data napadnout (výjimky budou popsány dále v této práci).[11]

Nevýhodou je, že za cenu anonymity je komunikace pomalá, vždy, když chci navštívit nějaký server musím projít přes 3 routery, což samozřejmě zpomalí komunikaci.[11]

4.2 Vyhledávání v TOR síti

Orgán činný v trestním řízení může na TČ narazit pomocí vyhledávačů uvnitř Darknetu. Nahlášením oběti nebo svědka. Informace se dají získat pomocí routerů uvnitř sítě. Vstupní a výstupní routery jsou největším ziskem informací. Vstupní router získá informaci o uživateli, který se připojil do Tor sítě. Výstupní router získává nešifrovaný dotaz na vstup do serveru .onion. Je možné vytvořit více výstupních routerů a monitorovat tak stránky, které se na Darknetu objevují.

4.2.1 Analýza informací

Po získání .onion stránek je možné stáhnout obsah webu do počítače (viz dokumentace stránek), poté vypsat klíčová slova TČ. Je možné použít software Mallet[29] nebo uClassify[30] (text classifier) pro automatické rozdělení témat stránek [4]. Je možné použít Support Vector Machine (SVM) [5], neuronová síť, která rozpozná, co se na stránce objevuje pomocí text classifier. Darknet Usage Text Addresses (DUTA) obsahuje pouze HS, získává informace ze stránek pouze s portem 80 (http) [6].

4.2.2 Nastavení routeru uvnitř Tor sítě

Router se může nastavit buď jako vstupní/středním nebo výstupní. Vstupní router je router mezi klientem a středním routerem. Střední router je mezi vstupním a výstupním routerem. Vstupní routery potřebují mít stabilní rychlost připojení alespoň 2 MB za sekundu jinak z nich budou střední routery. Výstupní router je mezi druhým routerem a serverem. Výstupní router potřebuje mít připojení více než 100 Mb za sekundu. Podrobný způsob nastavení vstupního nebo výstupního routeru viz [28].

5. Analýza možnosti dokumentace

5.1 Dokumentace TČ

Při nalezení stránky, na které se nachází nelegální obsah je zapotřebí tuto stránku nahlásit orgánu činným v trestním řízení, který potřebuje tuto stránku uložit lokálně. Pokud by se útočník pokusil smazat nebo změnit obsah stránky, bude uložená na počítači a může sloužit jako důkazní materiál. K tomuto účelu slouží software pro stažení http a https stránek.

5.2 Možnost dokumentace

Existuje více programů, které jsou schopny zadokumentovat stránku na internetu. Tyto programy fungují i uvnitř Darknetu, ale je potřeba, aby tyto programy věděli, že budou komunikovat přes proxy server, přes který komunikuje Tor software. Při nastavení proxy serveru na 127.0.0.1:8080 je možné dokumentovat stránku pomocí těchto programů.

Je možné pořídit si zadarmo nebo koupit program do PC, správně ho nastavit a nakonec zadokumentovat stránku, např. httrack. Je potřeba si nainstalovat do Linuxu httrack.

Poté je potřeba v terminálu použít příkaz: polipo socksParentProxy=localhost:9050, díky které se Tor proxy nastaví na http. Použít příkaz httrack, kde je potřeba poté napsat jméno projektu, vybrat cestu projektu, zadat adresu serveru xyz.onion vybrat akci 0-5 (1 – Mirror stránky, 2 – Mirror stránky s Wizardem, 3 – Pouze označit soubory, 4 – Mirror všech linků v URL, 5 – Testovat linky v URL, 0 – exit), nastavit Proxy na localhost:8080, definovat další nastavení, a nakonec zadokumentovat stránku.

Linux má přímo příkaz v terminálu, který dokáže zadokumentovat stránku, pomocí příkazu torify wget --mirror xyz.onion je také možné zadokumentovat stránku.

6. Zabezpečení při vstupu na Darknet pro orgán činný v trestním řízení

Pohybovat se v Darknetu znamená být také neviditelný pro ostatní. Toho musí být samozřejmě schopni i vyšetřovatelé, kteří hledají v dané části Internetu osoby páchající protiprávní jednání.

6.1 Důvod zabezpečení

Tor síť je jedna z nejlepších anonymních sítí, vyskytují se v ní však chyby, které snižují její bezpečnost. Útočník může zaútočit a zjistit IP adresu. Také může napadnout účet, popřípadě napadnout počítač pomocí viru. Ze všech těchto důvodů je důležité k Darknetu přistupovat anonymně a chránit si své soukromí a bezpečí.

Základním předpokladem pro to být neviditelný je skrytí IP adresy, která je viditelná i v Darknetu.

K tomu lze využít následující varianty:

a) Pořízení veřejné IP adresy přes prostředníka (firmu)
b) Pořízení a připojení přes VPN službu
c) Připojení přes vlastní server

6.2 Pořízení veřejné IP adresy

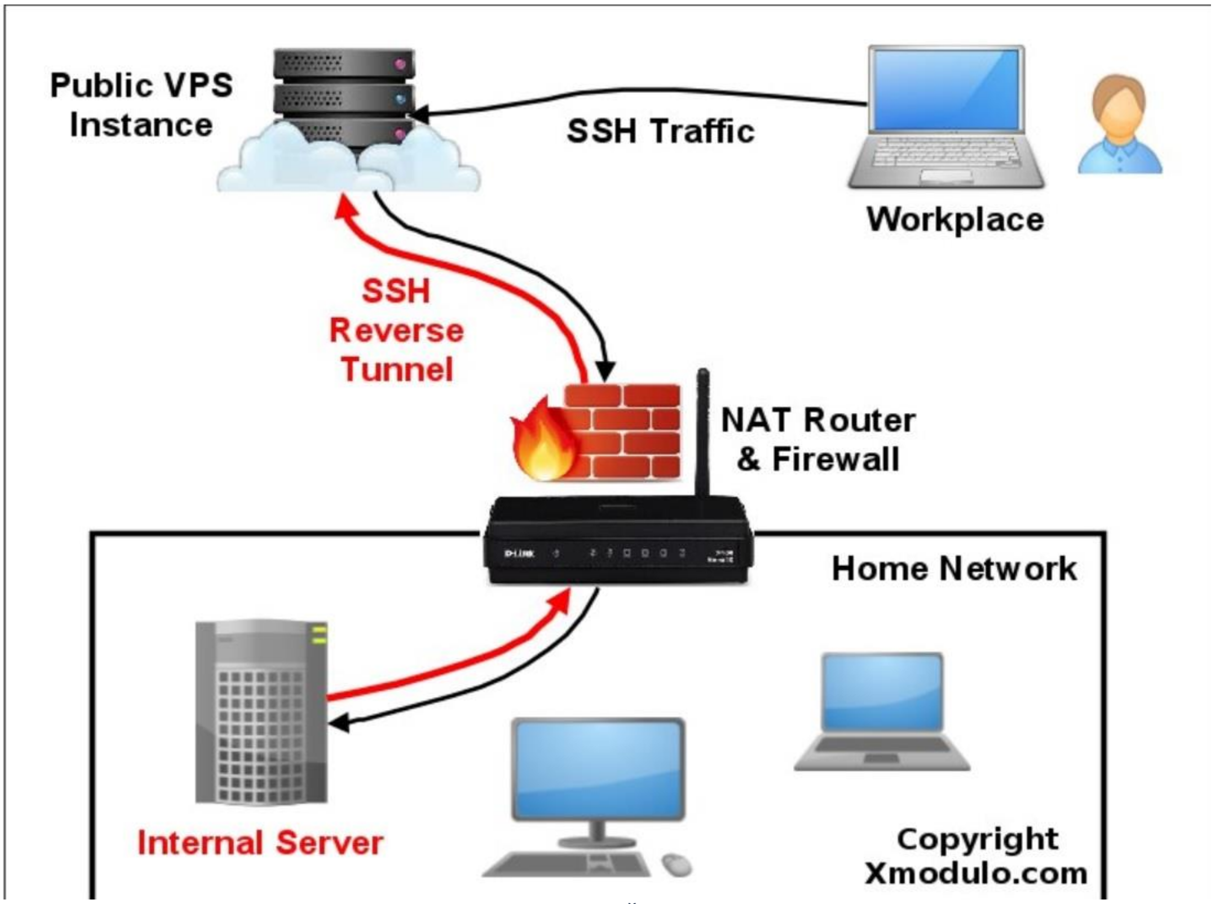
Jedná se o nejjednodušší způsob, jak zakrýt svou identitu v rámci Darknetu. Pokud se totiž využije a zaregistruje jiná osoba, než ta která dané připojení používá, pak v rámci služby whois bude dohledatelná pouze tato osoba. Jako příklad můžeme uvést doménu pcr.cz, kdy se dozvíme výpisem whois, že je zaregistrována na Pavla Smrže, k registraci došlo 10. 8. 2001 a doména je vedena pro ministerstvo vnitra. Z výše pospaného vyplývá, že používanou IP adresu PČR by si mohl prověřit kdokoliv z prostředí Darkentu a následně vyvinout sadu otázek a při nich by mohl odhalit, že se nejedná o osobu, která je vedená pod výpisem whois. Proto je tato metoda asi nejméně bezpečná z hlediska zakrytí identity, ale zároveň nejrychleji realizovatelná.

6.3 Pořízení a připojení přes VPN službu

V dnešní době existuje mnoho služeb, které nám pomohou s přístupem na Internet a také nám pomohou na něm bezpečně a zakrytě surfovat. Jednou z takových služeb je VPN, kdy k přístupu na Internet dochází tzv. přes prostředníka, v tomto případě VPN službu. VPN služby nabízí dnes mnoho společností a ceny se liší dle počtu serverů, na kterých daná služba běží, ale i taky za kolik zemí se lze schovat. V tomto případě se z výpisu whois osoba z prostředí Darkentu nedozví nic víc, než že používáme VPN od daného poskytovatele. To se samozřejmě jeví z pohledu identifikace ideálně, ale má to také svá úskalí. Jako největší vidím to, že veškerá komunikace je vedena skrz prostředí o kterém PČR nic neví, takže lze provést na dané spojení tzv. man-in-the-middle útok. Spojení mezi klientem (PČR) a serverem (služba VPN) je sice zašifrované a zároveň i dál je komunikace šifrovaná, ale certifikát, kterým došlo k zašifrování vydala a vlastní firma, která nám spojení realizuje. Je důležité si uvědomit, že v rámci Darkentu se dlouhou dobu buduje důvěra, někdy trvá i roky než se člověk dostane k osobě, která je hlavním pachatelem a proto bych ani tuto variantu neviděl jako nejvhodnější, protože právě čas může způsobit, že služba přestane fungovat, případně dojde k narušení integrity dat a tím pádem veškerá posbíraná data budou dále nepoužitelná v rámci důkazního břemene.

6.4 Připojení přes vlastní server

Asi nejbezpečnější, avšak také nejvíc časově náročné, je připojení přes vlastní prostředky, ideálně server. Na něm jsme schopni spouštět další virtuální servery a s nimi i spojené služby, tudíž nám dává relativně velkou volnost. Základním předpokladem je, že server bude připojen v rámci infrastruktury, ke které má přístup pouze omezený počet lidí z PČR. Ideální pro tyto potřeby by se hodil pronajatý byt s připojením od místního poskytovatele služby internet. Tento server by sloužil jako prostředník mezi klientem a přístupem do Darknetu. Nejprve by se na něm samozřejmě musela spustit služba VPN, tak aby byla vždy komunikace šifrována a nemohla být narušena integrita dat. Další služba, které by na daném serveru měla být spuštěna, by pak byl bnc bouncer, případně server, který bude realizovat spojení do Darknetu. Výhoda bnc bounceru je, že si můžete zvolit libovolný dns název místo IP adresy, tudíž při výpisu whois nikdo neví, přes co jste připojen. Připojení pak probíhá tak, že uživatel se přihlásí nejprve na vlastní server (v pronajatém bytě), kde si spustí virtuální PC, které se následně přihlásí do požadované části Darkentu, viz. obr. 3 níže.



Obrázek 3 - návrh připojení PČR do DARKNETu [34]

Díky tomu, že je vše v naší správě, pak je možné se přihlásit odkudkoliv na světě, následně se tvářit jako, že jsem doma a klidně se zájmovou osobou diskutovat, jako bych byl pořád na jednom místě. Výhoda tohoto řešení je, že navázaní důvěry, která je v tomto případě nejdůležitější pro odhalení trestné činnosti, je jednodušší, než kdybychom byli připojeni přes různé VPN služby či proxy servery. A protože pachatel bude chtít znát dřív nebo později naší identifikaci a zeptá se na něco, co si bude moc ověřit, pak je důležité být stále konstantním, což nám tento způsob připojení umožní.

6.5 Zabezpečení koncového zařízení

Při vstupu na Darknet používejte antivir, protože je to nejlepší způsob zabránění stáhnutí viru do počítače a ochránění před útočníkem. Ani antivir nezachytí všechny nové viry, je bezpečné používat také Virtual machine (dále jen VM), který zajistí, že při stáhnutí nějakého viru, stačí přeinstalovat VM a můžete pokračovat dále.

Z důvodu bezpečnosti je rovněž důležité vypnout Javascript, Flash. Zakázat vyskakovací okna a soubory cookies. Při použití Tor browser, nemějte ho přes celou obrazovku, ale snižte jeho rozlišení z důvodu otisku prohlížeče.

Poté co jste se ochránili dostatečně v softwaru, je důležité ochránit se i na Darknetu. Nikomu neříkat osobní informace, nezveřejňovat nikde heslo, nepřihlašovat se na žádné stránky, které se vyskytují na internetu (Facebook, Twitter, Youtube, Google… tyto stránky o mně mají cookie záznamy, a tudíž okamžitě co se na ně přihlásím, tak ví, jaký jsem počítač a kdo jsem.).

7. Analýza možnosti identifikace pachatele

7.1 Možnosti identifikace pachatele

Pachatel může být, jak klient, který páchá TČ (sleduje dětskou pornografii, šíří extrémistické názory), tak správce serveru, na kterém se nachází TČ. Pachatele lze dopadnout útoky na síť Tor, tyto útoky se dělí na aktivní a pasivní útok. U aktivních útoků jde o zjištění HS IP adresy. Pasivní útoky jsou ty, u kterých odposloucháváme na síti a zjistíme, klientovu IP adresu. Útoky jsou potom směřované na klienta, server nebo Tor síť.

7.1.1 Aktivní útok

1. *DoS útok* - Sniper attack – Tento typ útoku je určený k identifikaci serveru. V tomto útoku je potřeba, aby útočník kontroloval klienta a jeden z routerů mezi serverem a RP. Útočník poté potřebuje udělat z routeru, který kontroluje HS vstupní uzel, aby zjistil lokaci serveru. Aby tohoto dosáhl musí zrušit všechny HS vstupní uzly serveru, dokud server nevybere útočníkův router jako vstupní uzel. Jakmile se útočníkův router stane vstupním uzlem zná lokaci HS. Toho dosáhne tím, že posílá SENDME cell na vstupní uzel serveru, tím blokujeme čtení paketů a server si vybere jiný vstupní uzel. Sniper attack se jmenuje z důvodu, že útočník je neznámý, protože kontroluje zároveň klienta.[12]

Další DoS útoky je např. Cellflood attack.

2. Časový útok – Bandwith estimation attack – Používá šířku pásma (bandwith) ke zjištění klienta, identitu HS nebo identitu OR. Útok spočívá v podobě šířky pásma. Útočník musí ovládat server, technologii ke zjištění šířky pásma a mapu obsahující vstupní a konečné routery autonomního systému. Útočník umístí technologii ke zjištění šířky pásma poblíž vstupních a konečných routrů. Pokud se klient ze vstupního routeru připojí k serveru přes konečný router vytvoří se vzor šířky pásma. [25]

The indirect rate reduction attack – Výběr konečného uzlu lze předpovědět, jeden ze sedmi konečných uzlů byl vybrán v 20 %. Útočník pošle 3 packety se špatnou sekvencí čísel všem předpokládaným konečným uzlům. IP adresa je podvržena, takže to vypadá, že tyto packety poslal server. Konečný uzel pošle 3 ACK packety serveru. Server omezí okno přetížení, klientovo připojení k vstupnímu uzlu bude také omezeno. Opakováním tohoto útoku může útočník říci s velkou pravděpodobností, že klient se připojil k serveru. [24]

3. *Congestion attack* - Útoky směřované na zjištění OR, které se nacházejí uvnitř obvodu.

Congestion attack by modulating traffic – Tento útok není aktuální, protože v jeho době bylo uvnitř Toru pouze pár OR, nyní je tato síť mnohem větší, v této práci jen zmíním, jak tento útok funguje. Útočník kontroluje server a jeden OR. Útok je vytvořen k identifikaci OR, které tvoří komunikaci mezi serverem a klientem. Aby útok proběhl úspěšně musí se klient připojit k útočníkovu serveru. Server poté pošle klientovi specifický vzor. Útočníkem ovládaný OR poté vytvoří připojení s ostatními OR a nahraje odezvu připojení. Pokud se odezva připojení shoduje s odezvou připojení, který přišla na útočníkem kontrolovaný server, útočník bude vědět, že OR pravděpodobně navázal spojení se serverem. Tato technika může vést k odhalení všech OR v obvodu. [26]

A practical Congestion attack – Útočník kontroluje výstupní uzel. Útočník napadne kódem Javascriptu HTML odpověď na výstupním uzlu. Javascript kód nechá klienta poslat http žádost s intervalem 1 sekundy. Tato žádost bude obsahovat čas, kdy byla poslaná. Díky tomu bude moci útočník korelovat čas na konečném uzlu mezi časem, kdy přišla žádost a tím, kdy byla poslaná. Poté vypočítá průměrnou dobu odezvy připojení. Útočník bude opakovat, dokud nebude dostatek vzorků. Pokud bude odezva zpomalena bude vědět, že vstupní uzel se připojil k výstupnímu uzlu. [27]

7.1.2 Pasivní útok

1. Correlation attack - Korelační útoky jsou takové útoky, kdy útočník převážně odposlouchává na prvním uzlu (klient vstupuje do Toru) a posledním uzlu (připojení k serveru). V těchto útocích se sleduje korelaci provozu mezi prvním a posledním uzlem. Pokud zjistí korelaci bude vědět, že k serveru se připojil tento klient.

Relay early traffic confirmation attack – K tomuto útoku potřebuje útočník mít přístup k HS adresáři routeru a vstupnímu uzlu klienta. Klient při vstupu na server musí nejprve požádat IP, který se nachází v HS directory. Directory mu poté pošle název HS zašifrovaně. Útočník poté zjistí, že proběhla komunikace mezi klientem a serverem a ví, že klient se připojil k tomuto serveru. [13]

Replay attack – Útočník si vybere cell ve vstupním uzlu a zduplikuje ji. Zduplikovanou cell pošle následně na stejný druhý uzel. Útočník poté může detekovat cell na posledním uzlu, který také kontroluje. Zduplikovaná cell, způsobí, že šifrovací a Counter Encrypted data (CTR) se dostane ze synchronizace a tím vznikne šifrovací error. Útočník může tento error vidět na posledním uzlu, pro jistotu by útočník měl zkontrolovat, jestli se error objevil až poté co poslal cell a čas odpovídá cestě z prvního uzlu do posledního uzlu. Jestli se objevil error a čas odpovídá útočník ví, že klient se připojil k serveru. [14]

Cellcounter based attack – Útočník z posledního uzlu vytvoří provoz mezi klientem a serverem. Vybere náhodný signál (např. binární sekvenci). Změní cell counter klienta a nahradí ho náhodným signálem. Útočník poté rozpozná na prvním uzlu jeho náhodný signál. Pokud se objeví vzor, útočník ví, že klient se snažil kontaktovat server. [15]

Low resource routing attack – Útočník kontroluje klienta a poslední uzel k serveru. Kontrolováním klienta může zjistit jeho vstupní uzel. Útočník zaútočí na vstupní uzel (DoS útokem), tím ho udělá nedostupným. Vybere se nový vstupní uzel s možností vybrat útočníkem kontrolovaný vstupní uzel. Když je útok úspěšný a vybere se útočníkův kontrolovaný vstupní uzel má možnost zjistit log informace a tím zjistí korelaci mezi klientem a serverem

Dále existují útoky např.:

Correlation based traffic attack [16]

HTTP based application level attack [18]

Bad apple attack – Raptor attack [19].

2. Fingerprint attack - Útoky otisku využívají toho, že provoz má nějakou specifickou charakteristiku. Tyto útoky mohou identifikovat, kterou stránku klient chce navštívit nebo jestli se klient připojuje k HS.

Website fingerprint – Útočník kontroluje pouze vstupní uzel. Nejdříve útočník odposlouchává packety z různých serverů, které by mohl klient navštívit. Útočník takto získá informace, které posílá server v packetu. Útočník kontroluje klientův příchozí a odchozí provoz. Provoz proběhne a útočník poté porovná klientův packet a packety všech jeho vybraných serverů. Útok je úspěšný, když je ve vzoru shoda. [20]

Dále existují útoky např.:

Circuit fingerprint [21]

Throughput fingerprint [22]

7.2 Zastavení hidden services

Blokování HS – HS nevydrží dlouho proti technickému útoku. Je možné blokovat HS:

1. Jednotlivec za pomocí spuštění několika routerů a obsazením pozice v distribuovaném hash table odpovědí. Pokud někdo přijde k routeru a zeptá se na spojení. Jednotlivec to může pro každého, kdo to udělá odmítnout.

2. Operátoři Toru můžou sami rozhodnout, že zablokují, co se na HS nachází, tím že vytvoří patch, který zakáže žádosti do HS. K tomuto je zapotřebí spolupracovat s operátory Toru.

Tor může zablokovat, věci nacházející se na HS jednoduše tím, že modifikují Tor program, aby určité stránky a klienti nemohli přijímat žádosti. Tor může využít svého postavení, aby zveřejnil jména klientů nebo zablokoval stránky. [2]

8. Forenzní software

Jakmile známe IP adresu pachatele, je potřeba najít důkazy na jeho zařízení. Je zapotřebí prohledat jeho PC z důvodu nalezení stop. To je možné za pomocí vytvoření bitové kopie PC pomocí forenzního softwaru.

Nejlepší forenzní software na prohledání PC je IEF, Axiom nebo Belkasoft všechny zmíněné softwary mohou vytvořit bitovou kopii a vyhledat důležité programy, uvnitř počítače, které se pojí s Darknetem.

Podle návodu Toru [31] soubor torrc vytváří HS, který ukazuje na lokální server. Uvnitř souboru torrc je napsaná cesta k lokálnímu serveru, na kterou HS ukazuje. Pokud je soubor nalezen a vyskytuje se v něm nelegální server, máme pachatele.

Defaultně:

1. V macOS se nachází soubor v ~/Library/Application Support/TorBrowser-Data/Tor/torrc
2. V Linuxu ~/[path_to_tor_browser]/Browser/TorBrowser/Data/Tor/torrc
3. Ve Windows \Desktop\TorBrowser\Browser\TorBrowser\Data\Tor\torrc[32]

Pokud nebyl nalezen soubor torrc, je možné použít forenzní software, který může nalézt tento soubor smazaný, a nebo logy serveru (v Linuxu je defaultně nastavený: /usr/local/etc/tor/tor.log).

V případě, že byl spáchán TČ pachatelem, který nevlastní HS, musí stačit pouze nainstalovaný program Tor browser.

9. Metodiky řešení kybernetické kriminality pro použití orgánu činném v trestním řízení

Žádná metodika pro odsouzení pachatele u policie, pro tento komplexní problém neexistuje, postup se může lišit případ od případu, ale nejvíce TČ uvnitř Darknetu by se dalo řešit takto:

1. Pří spáchání TČ je zapotřebí, aby trestný čin byl nalezen, toho lze docílit buďto nalezením TČ orgánem činným v trestním řízené nebo nahlášením TČ poškozeným nebo oznamovatelem.
2. Při nalezení TČ uvnitř DARKNETu je potřeba rozdělit kdo je poškozený a kdo je pachatel, popřípadě, zda se znají. Následně zjistit odhadovanou cenu, podle toho, jak velká je odhadovaná škoda je zapotřebí předat to způsobilým útvarům.
3. Určit, jak je možné dopadnout pachatele, který spáchal TČ. K dopadení pachatele, který spáchal svým konáním TČ při sledování trestné činnosti nebo šířením extrémistického názoru na HS je zapotřebí napsat žádost soudu o použití § 88 TŘ, který pojednává o odposlechu. Když se jedná o TČ, který spáchal pachatel, který vlastní HS, je potřeba poslat soudu stejnou žádost § 88 TŘ, navíc je potřeba provést DOS útoky na routery. To znamená, že oba TČ se dají dohledat pomocí odposlechu sítě. Bohužel na tento odposlech musí orgán činný v trestním řízení vytvořit velké množství rychlých routerů, které budou schopny komunikovat s Distributed hash table (dále jen DHT), nastavení routeru je detailněji popsané v kapitole 4.2.2.
4. Pokud soud vyhoví žádosti je možné poslat tyto routery do Tor sítě, aby mohli monitorovat provoz na síti, jakmile začnou komunikovat s DHT budou mít možnost přesměrovávat komunikaci na HS.
5. Při nalezení TČ, je potřeba stránku s nelegálním obsahem zadokumentovat, aby pachatel nemohl smazat nebo pozměnit obsah stránky, více popsáno v kapitole 5. Před vstupem na Darknet je potřeba postupovat podle kapitole 6.
6. V tomto okamžiku se metodika rozdělí pro výše zmíněné dva TČ.

6.1 Identifikace podezřelé osoby, která sleduje trestnou činnost nebo šíří extrémistické názory. Tento TČ je možné identifikovat jedině tak, že budeme mít router, který komunikuje s HS na kterém byl spáchán TČ, a zároveň router, který komunikuje s pachatelem, oba tyto routery spolu musí vytvořit obvod do HS, na kterém byl spáchán TČ. Poté je potřeba využít útoků, které jsou popsané v kapitole 7.1.2.

6.2 Identifikace podezřelé osoby, která vlastní HS, na kterém se nachází TČ. Tuto TČ je možné identifikovat jedině tak, že budeme mít routery, které mohou komunikovat s DHT, poté je potřeba zaútočit na router, který přímo komunikuje s HS, na kterém se nachází TČ. Použitím DOS útoku, které jsou více popsané v 7.1.1 je možné zjistit IP adresu serveru a tímto zjistit, kdo je pachatel, kterému patří HS.

7. Jakmile je pachatel vyhledán je potřeba vytvořit právní posouzení trestné činnosti, které jsou více popsané v kapitole 3.5. Dále je potřeba zakázat připojení k HS na které se vyskytuje TČ, více v kapitole 7.2.

8. Poté je potřeba povolení soudu k provedení domovní prohlídky, podle § 83 odst. 1 TŘ je potřeba podat návrh státním zastupitelem. Pro prohlídku jiných prostor je potřeba použít § 83a odst. 1 TŘ, postup je stejný jako u domovní prohlídky, navíc podle § 83a odst. 2 TŘ je možné provést prohlídku, jestliže věc nesnese odkladu, avšak poté je potřeba si dodatečně zažádat o povolení k prohlídce státním zástupcem.

9. Pokud soud vyhoví této žádosti, je potřeba využít momentu překvapení, aby nedošlo k vyplašení pachatele, který by mohl zničit stopy a důkazy. Zajistit výpočetní techniku a digitální data pachatele, více je popsáno v kapitole 8. Zjistit, kde se server nachází a zajistit ho. Pokud zajištěný server a server, který jsme stáhli pomocí dokumentace mají stejnou IP adresu, dopadli jsme pachatele.

10. Napsat otázky soudnímu znalci a posoudit v nich rizika, které mohou vzniknout. Zaslat mu nelegální materiály, které byly nalezeny na výpočetní technice u pachatele.

11. Rozebrání možností provádění úkonů v trestním řízení policejním orgánem.

12. Rozebrat, jak lze použít zákon o elektronické komunikaci a trestní řád, zákonná omezení v rámci řešení trestné činnosti (trestní řád) a povinnosti subjektů.

Závěr

Vyšetřování trestné činnosti v DARKNETu by mělo být prováděno specializovanými týmy složenými z odborníků na problematiku. V rámci DARKNETu se střetáváme s trestnými činy:

a) Trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů, konkrétně – hacking, prodej nelegálního SW a HW určeného k úmyslnému spáchání trestných činů.
b) Trestné činy související s obsahem v podobě nelegální pornografie a šíření rasistických a xenofobních materiálů – forum, blogy atd.
c) Trestné činy související s porušováním autorských práv a práv prodejem nelegálního softwaru – obchod.

Všechny výše uvedené trestné činy lze vyšetřovat pomocí jedné metodiky uvedené v kapitole 9. Není nutné vytvářet speciální metodiky pro jednotlivé trestné činy. Co je však nutné řešit, je oprávněnost provádění útoků orgány v trestním řízení v prostředí DARKNETu, tak aby nashromážděná dokumentace mohla být využita v trestním řízení. Zároveň z důvodu, že Internet je celosvětová síť, je problematické určení kde došlo k trestnému činu. Zpravidla by se měl určovat zpravidla podle toho, kde nastal následek trestného činu. Vzhledem k celosvětovosti Internetu je více než pravděpodobné, že na vyšetřování se zpravidla bude podílet více mezinárodní justiční spolupráce prostřednictvím Europolu nebo Interpolu.

Vzhledem k tomu, že vyhledávání a potírání trestné činnosti v rámci DARKNETu vyžaduje vysoce specializované odborníky, bylo by vhodné koordinovat tuto činnost i s jinými státními subjekty nejen z Ministerstva vnitra, ale i z např. Vojenského zpravodajství a útvarů Ministerstva obrany. Toto by však vyžadovalo úpravu legislativy České republiky.

Úpravu legislativy by také vyžadoval odposlech uvnitř DARKNETu (viz kapitola 4.2.2 a 7.1) je potřeba vytvořit spousty OR a následně odposlouchávat, kdo navštívil zakázané weby. Toto orgán činný v trestním řízení provést nemůže kvůli § 88 TŘ, nezískal by informace legálním způsobem, takže by je soud zamítl a musely by být zničeny. Stejně tak informace, které byly získané při odposlechu osoby, která se připojila do DARKNETu (viz kapitola 7.1.2) by byly zamítnuté soudem a musely by být zničeny. Z tohoto důvodu orgán činný v trestním řízení neřeší TČ uvnitř DARKNETu, pokud by se změnila legislativa, bylo by to možné, pomocí metodiky popsané v kapitole 9.

Seznam použitých zdrojů

[1] Darknet vs Dark Web vs Deep Web vs Surface Web — Different Parts Of The World Wide Web. *Https://techlog360.com/* [online]. Tamilnádu: Sabarinath, ©2019 [cit. 2019-04-05]. Dostupné z: https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/

[2] *OWEN, Gareth a Nick Sav. Global Commission on Internet Governance* [online]. 2015, **20**(8) [cit. 2019-04-05]. Dostupné z: https://www.cigionline.org/sites/default/files/no20_0.pdf

[3] MOORE, Daniel a Thomas RID. Cryptopolitik and the Darknet. *Survival: Global Politics and Strategy*[online]. 2016, **58**(1), 7-38 [cit. 2019-04-05]. DOI: 10.1080/00396338.2016.1142085. Dostupné z: https://doi.org/10.1080/00396338.2016.1142085

[4] BIRYUKOV, Alex, Ivan PUSTOGAROV, Fabrice THILL a Ralph-Philipp WEINMANN. *Content and popularity analysis of Tor hidden services* [online]. Washington, DC: ICDCS, 2014 [cit. 2019-04-05]. ISBN 978-1-4799-4181-0. Dostupné z: https://arxiv.org/pdf/1308.6768.pdf

[5] AVARIKIOTI, Georgia a kol. ZINDROS3. Structure and Content of the Visible Darknet. In: *Https://arxiv.org* [online]. Mountain View, 2018 [cit. 2019-04-05]. Dostupné z: https://arxiv.org/pdf/1811.01348.pdf

[6] Classifying Illegal Activities on Tor Network Based on Web Textual Contents. *EACL* [online]. 2017, **17**(1004), 35-43 [cit. 2019-04-05]. Dostupné z: https://www.aclweb.org/anthology/E17-1004

[7] Onion Services: Step 6. In: *Torproject* [online]. Seattle: The Tor Project, 2019 [cit. 2019-04-05]. Dostupné z: https://2019.www.torproject.org/docs/onion-services

[8] Onion Routing - Computerphile. *Youtube* [online]. San Bruno: YouTube, 2017 [cit. 2019-04-05]. Dostupné z: https://www.youtube.com/watch?v=QRYzre4bf7I

[9] Tor: Onion Service Protocol. *Torproject* [online]. Seattle: The Tor Project, 2019 [cit. 2019-04-05]. Dostupné z: https://2019.www.torproject.org/docs/onion-services.html.en

[10] Dingledine, Roger & Mathewson, Nick & Syverson, Paul. (2004). Tor: The Second-Generation Onion Router. Paul Syverson. 13. Dostupné z: https://www.onion-router.net/Publications/tor-design.pdf

[11] What are the Pros and Cons of Using Tor Browser?... *Deepweb-sites* [online]. ©2019 [cit. 2019-04-05]. Dostupné z: https://www.deepweb-sites.com/pros-and-cons-of-using-tor-browser/

[12] JANSEN, Rob, Florian TSCHORSCH, Aaron JOHNSON a Bjorn SCHEUERMANN. The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network. *NDSS Symposium* [online]. 2014 [cit. 2019-04-05].

DOI: 10.14722/ndss.2014.23288. Dostupné z: https://www.robgjansen.com/publications/sniper-ndss2014.pdf
[13] Tor security advisory: "relay early" traffic confirmation attack. *Torproject* [online]. Seattle: The Tor Project, 2014 [cit. 2019-04-05]. Dostupné z: https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack
[14] RYAN Pries, Wei Yu, Xinwen Fu a Wei Zhao. A New Replay Attack Against Anonymous Communication Networks. *IEEE ICC* [online]. 2008 [cit. 2019-04-05]. DOI: 10.1109/ICC.2008.305. ISSN 1938-1883. Dostupné z: http://www.cs.ucf.edu/~xinwenfu/paper/ICC08_Fu.pdf
[15] LING, Zhen a kol. A new cell counter based attack against tor. *ACM CCS* [online]. 2009 [cit. 2019-04-05]. DOI: 10.1145/1653662.1653732. Dostupné z: http://web.cse.ohio-state.edu/~xuan.3/papers/09_ccs_llyfxj.pdf
[16] YE, Zhu a kol. Correlation-Based Traffic Analysis Attacks on Anonymity Networks. *IEEE Transactions on Parallel and Distributed Systems* [online]. 2010, **21**(7), 954 - 967 [cit. 2019-04-05]. DOI: 10.1109/TPDS.2009.146. Dostupné z: https://engagedscholarship.csuohio.edu/cgi/viewcontent.cgi?article=1053&context=enece_facpub
[17] BAUER, Kevin a kol. *Low-resource routing attacks against tor* [online]. Virginia: WPES, 2007 [cit. 2019-04-05]. ISBN 978-1-59593-883-1. Dostupné z: https://cs.gmu.edu/~mccoy/papers/wpes25-bauer.pdf
[18] A potential HTTP-based application-level attack against Tor. *Future Generation Computer Systems*[online]. 2011, **27**(1), 67-77 [cit. 2019-04-05]. DOI: 10.1016/j.future.2010.04.007. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.710.6952&rep=rep1&type=pdf
[19] *YIXIN, Sun a kol. RAPTOR: Routing Attacks on Privacy in Tor* [online]. Washington, D.C.: USENIX Security, 2015 [cit. 2019-04-05]. ISBN 978-1-931971-232. Dostupné z: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sun.pdf
[20] Website fingerprinting in onion routing based anonymization networks. In: PANCHENKO, Andriy, Lukas NIESSEN, Andreas ZINNEN a Thomas ENGEL. *WPES* [online]. Chicago: ACM, ©2011, s. 103-114 [cit. 2019-04-05]. DOI: 10.1145/2046556.2046570. ISBN 978-1-4503-1002-4. Dostupné z: https://www.freehaven.net/anonbib/cache/wpes11-panchenko.pdf
[21] KWON, Albert a kol. *Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services* [online]. Washington, D.C.: USENIX Security, 2015 [cit. 2019-04-05]. ISBN 978-1-931971-232. Dostupné z: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-kwon.pdf

[22] MITTAL, Prateek a kol. Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting. In: *CCS* [online]. Chicago: ACM, 2011, s. 215-226 [cit. 2019-04-05]. DOI: 10.1145/2046707.2046732. ISBN 978-1-4503-0948-6. Dostupné z: https://arxiv.org/pdf/1109.0597.pdf

[23] BARBERA, Marco, Vasileios KEMERLIS, Vasilis PAPPAS a Angelos KEROMYTIS. CellFlood: Attacking Tor Onion Routers on the Cheap. In: *ESORICS* [online]. Springer-Verlag Berlin Heidelberg, 2013, s. 664-681 [cit. 2019-04-05]. DOI: https://doi.org/10.1007/978-3-642-40203-6_37. ISBN 978-3-642-40203-6. Dostupné z: http://wwwusers.di.uniroma1.it/~barbera/papers/barbera-esorics13.pdf

[24] Spying in the dark: TCP and tor traffic analysis. In: GILAD, Yossi a Amir HERZBERG. *PETS* [online]. Vigo: Department of Computer Science, 2012, s. 100-119 [cit. 2019-04-05]. DOI: 10.1007/978-3-642-31680-7_6. ISBN 978-3-642-31679-1. Dostupné z: https://www.freehaven.net/anonbib/cache/tcp-tor-pets12.pdf

[25] CHAKRAVARTY, Sambuddho, Angelos STAVROU a Angelos KEROMYTIS. Traffic analysis against low-latency anonymity networks using available bandwidth estimation. In: *ESORICS* [online]. Řecko: Computer Security Research, 2010, s. 249-267 [cit. 2019-04-05]. ISBN 3-642-15496-4. Dostupné z: https://www.cs.columbia.edu/~angelos/Papers/2010/esorics.pdf

[26] MURDOCH, Steven a George DANEZIS. *Low-Cost Traffic Analysis of Tor* [online]. Oakland: IEEE, 2005 [cit. 2019-04-05]. ISBN 0-7695-2339-0. Dostupné z: https://www.cs.ucy.ac.cy/courses/EPL682/papers/anon-2.pdf

[27] EVANS, Nathan, Roger DINGLEDINE a Christian GROTHOFF. A Practical Congestion Attack on Tor Using Long Paths. *USENIX* [online]. 2009, **09**, 33-50 [cit. 2019-04-05]. Dostupné z: https://www.freehaven.net/anonbib/cache/congestion-longpaths.pdf

[28] The Tor Relay Guide. *Torproject* [online]. Seattle: The Tor Project, 2018 [cit. 2019-04-05]. Dostupné z: https://trac.torproject.org/projects/tor/wiki/TorRelayGuide

[29] MALLET. *Http://mallet.cs.umass.edu/* [online]. ©2018 [cit. 2019-04-05]. Dostupné z: http://mallet.cs.umass.edu/download.php

[30] UClassify. *UClassify* [online]. Stockholm, 2008 [cit. 2019-04-05]. Dostupné z: https://www.uclassify.com/browse

[31] Configuring Onion Services for Tor. *Torproject* [online]. Seattle: The Tor Project, 2019 [cit. 2019-04-05]. Dostupné z: https://2019.www.torproject.org/docs/tor-onion-service

[32] Connecting to an authenticated Onion service. *GitHub* [online]. San Francisco, 2007 [cit. 2019-04-05]. Dostupné z:

https://github.com/AnarchoTechNYC/meta/wiki/Connecting-to-an-authenticated-Onion-service

[33] What is Surface Web and how is it different from Dark Web?. In: *Cyware* [online]. New York, 2019 [cit. 2019-04-05]. Dostupné z: https://cyware.com/educational-guides/cyber-threat-intelligence/how-is-surface-web-intelligence-different-from-dark-web-intelligence-393c

[34] Návrh připojení PČR do DARKNETu. In: *Xmodulo* [online]. USA: creative commons [cit. 2019-04-05]. Dostupné z: http://xmodulo.com/access-linux-server-behind-nat-reverse-ssh-tunnel.html

[35] KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, 2016, s. 85-133. ISBN 978-80-88168-15-7.

Seznam obrázků

Seznam grafů