VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

DARKWEB A KONEC HEDVÁBNÉ STEZKY

DARKWEB AND END OF SILK ROAD

SEMESTRÁLNÍ PROJEKT
TERM PROJECT

AUTOR PRÁCE **DAVID HUDÁK**
AUTHOR

VEDOUCÍ PRÁCE **Mgr. Ing. PAVEL OČENÁŠEK, Ph.D.**
SUPERVISOR

BRNO 2021

Abstrakt

Tato práce se zabývá bývalým webovým černým trhem zvaným Hedvábná stezka. Práce se zabývá jak kontextem teoretické problematiky dnešního temného internetu (darkwebu), tak právě tímto konkrétním černým trhem.

Abstract

This thesis deals with past web black market known as Silk Road. This thesis also deals with with theoretical problematics of today's darkweb in context of black markets.

Klíčová slova

darkweb, temný web, kryptoměny, Bitcoin, Silk Road, Hedvábná stezka, drogy, černý trh

Keywords

darkweb, cryptocurrencies, bitcoin, Silk Road, drugs, black market

Citace

HUDÁK, David. *Darkweb a konec Hedvábné stezky.* Brno, 2021. Semestrální projekt. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Mgr. Ing. Pavel Očenášek, Ph.D.

Darkweb a konec Hedvábné stezky

Prohlášení

Prohlašuji, že jsem tuto semestrální práci vypracoval samostatně pod vedením pana Pavla Očenáška. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
David Hudák
20. dubna 2021

Poděkování

Rád bych poděkoval panu Očenáškovi za vedení této práce a jeho práce při vedení předmětu IBS.

Obsah

1 Úvod **2**

2 Fungování temného webu (darkwebu) **3**
2.1 Hluboký web . . . 3
2.2 Temný web . . . 3
2.2.1 Darknet . . . 3
2.3 Prohlížeč Tor . . . 4
2.3.1 Besa Mafia . . . 4
2.3.2 Narušení anonymity . . . 4
2.3.3 Přínosy Toru (a darknetu) . . . 4
2.4 Kryptoměny . . . 5
2.4.1 Obchodování měny . . . 5
2.4.2 Princip fungování blockchainu . . . 5

3 Hedvábná stezka **7**
3.1 Nabízené služby . . . 7
3.2 Způsob zabezpečení klientů, PGP . . . 8
3.2.1 Způsob využití . . . 8
3.2.2 Výhody a rizika PGP . . . 8
3.2.3 Platby . . . 8
3.3 Právní stránka . . . 9
3.4 Pád Hedvábné stezky . . . 9
3.5 Dopady Hedvábné stezky a závěr . . . 10

Literatura **11**

Kapitola 1

Úvod

Od počátečního vojenského záměru vzniku internetu uběhlo již více než 50 let a za tu dobu ušel velmi dlouhou cestu. Od původního užívání pro čistě akademické účely v rámci sítě zvané ARPANET se jeho možnosti nepředstavitelně rozšířily a jeho dostupnost je tu už prakticky pro kohokoliv, kdo má o něj zájem[10]. S rostoucími možnostmi samozřejmě vznikly nejen člověku přínosné a zcela legální činnosti, jako je rychlá a snadná dostupnost informací, nákup zboží a služeb, kontaktování se s přáteli a rodinou a tak dále, ale i ne zcela legální použití, jako je sdílení ilegálního obsahu (dětské pornografie, explicitního násilí, softwaru s licencí zamezující šíření...) a především prodej a distribuce zboží, které není dle státních norem vůbec možné na území většiny států vůbec možné prodávat. Tato práce se pak zabývá právě jedním z průkopnických serverů zaměřeným tímto směrem. Hedvábnou stezkou.

Kapitola 2

Fungování temného webu (darkwebu)

V této kapitole budou vysvětleny základní principy fungování temného webu.

2.1 Hluboký web

Základní rozdíl mezi hlubokým webem (mezi který patří i temný web) a povrchovým spočívá v tom, že u klasického povrchového internetu dochází k indexaci stránek webovými vyhledávači, zatímco u hlubokého ne. V praxi to znamená, že zatímco stránky různé zájmové, publicistické, sociální, úřední a zkrátka jakékoliv běžné jsme schopni vyhledat webovým vyhledávačem jako Google.com, ty z hlubokého internetu ne. Samo o sobě je to naprosto očekávatelné, jelikož součástí hlubokého webu jsou například naše e-mailové schránky, námi užívané části fakultního informačního systému, ale i náš vlastní profil na Facebooku. Tím zásadním rozdílem tedy je, že na přístup k takové stránce potřebujeme nějaké puštění zevnitř, ať už heslo, speciální odkaz či jiný způsob autentizace[10]. Jedná se o zcela legální formu internetu

2.2 Temný web

Temný web v některých ohledech oproti hlubokému webu zachází dál, ale opět je nutné zdůraznit, že se stále jedná o formou zcela legální činnost[4]. Oproti hlubokému webu je však zapotřebí prohlížeč, který jednak podporuje doménovou koncovku „.onion“ (tato pseudodoména se nenachází v klasických kořenových DNS serverech) a který umí pracovat se speciálními darknetovými protokoly.

2.2.1 Darknet

Výklady toho, co je přesně darknet, se mohou různit, avšak především se dá říct, že se jedná o komunikační systémy, které cílí na anonymizaci uživatele a patří do nich například Freenet, který slouží jako necenzurovaná platforma pro šíření informací, BitTorrent, který slouží pro peer-to-peer sdílení obsahu (primárně pirátského), a nebo obecně prohlížeč Tor, který slouží k přístupu na takové platformy[5].

2.3 Prohlížeč Tor

Prohlížeč Tor klade oproti klasické internetové komunikaci velký důraz na anonymitu. Oproti klasickému TCP/IP spojení pak přidává výrazně více vrstev šifrování (při každém síťovém skoku; z tohoto důvodu se objevuje často termín onion, cibule, který značí množství vrstev) a při každé paketové transakci volí náhodně novou cestu. Při každém skoku navíc server zná pouze lokaci dalšího serveru, nikoliv celou cestu. Právě tímto způsobem se pak Tor snaží znemožnit zjištění lokace uživatele ze strany serverů a webových stránek, zabránit odposlouchávání od nevyžádaných subjektů (policie) a také znemožnit odposlouchávání komunikace přímo internetovými providery[15].

I přes tuto míru ochrany existují (nebo alespoň jsou aktivně vyhledávány) způsoby, jak Torovské protokoly přelstít a získat informace o uživateli. Navíc tyto protokoly nezaručují, že někde neudělá chybu sám uživatel takovéto sítě. Navíc právě kvůli snaze o anonymitu není možné zjistit, kdo se skrývá na druhé straně. Může to být klidně policie, ale i podvodník, co se na ilegálních službách snaží vydělat peníze.

2.3.1 Besa Mafia

Jedním takovým zajímavým případem se stala služba nabízející nájemné vraždy zvaná Besa Mafia. Ve skutečnosti se jednalo o podvod, který se pouze snažil působit dojmem takové organizace a z toho důvodu, že klienti takových služeb pravděpodobně nechtěli zajít na policii s nevyplněnou zakázkou, tato služba nějakou dobu žila a zůstávala. Důvěryhodnost navíc byla doplněna vytvořením stránky na Wikipedii (kterou však může upravovat každý). K tomu byly doplněny falešné recenze a krvavé fotky fiktivních obětí a kritikům poukazujícím na možnost podvodu byly zasílány agresivní komentáře včetně záběrů na hořící auto s nápisy jejich jména a výhružkou, že následovat může jejich dům. Nakonec však celý podvod padl na úniku interních údajů zaměstnanců v roce 2016[3].

2.3.2 Narušení anonymity

K tomuto se samozřejmě přidávají snahy jak akademiků, tak i policistů a tajných služeb (například NSA), které se snaží tuto anonymitu narušit. Zajímavý je přímo postoj organizace spravující webový prohlížeč Tor, který se například vyjadřuje k možnému odposlouchávání (eavesdroppingu) na síti a poukazuje na to, že pro co největší omezení možných odposlouchávaných informací je vhodné využívat jak Torovské protokoly, tak šifrované HTTPS protokoly, jinak může docházet k poskládání prakticky veškeré informace díky sdílenému odposlouchávání uvnitř této sítě. Dalším problémem, na kterou Tor upozorňuje je, jak již bylo v podstatě zmíněno v jedné z předchozích sekcí 2.3, že osoba na druhé straně nemusí být tou, za kterou se vydává a i tato osoba může být přímo odposlouchávána[2].

Beze zmínky by také neměl zůstat fakt, že samotní tvůrci Toru obecně podporují pokusy o útoky na jejich program, a to z důvodu vylepšení jejich vlastního softwaru. Navíc přímo nabízí služby k pomoci při takovém výzkumu. Do tohoto výzkumu jsou pak zapojeny například výzkumné skupiny na univerzitách v Minnesotě, Londýně či Waterloo[1].

2.3.3 Přínosy Toru (a darknetu)

Byť to tak nemusí vyznít, Tor jako takový je zcela legální a dá se zdarma stáhnout na stránkách organizace TorProjectu či z webových repozitářů[1]. Jeho systém anonymity pak může

[1] Například https://github.com/torproject/tor.

jednak přinášet soukromí běžnému uživateli, který prostě nechce být sledován, jednak pomáhá v zemích, kde možnosti internetové komunikace jsou výrazně omezené. Díky němu se pak dají šířit informace o násilí, korupci, zmanipulovaných volbách či jenom informace ze světa, který je od takových uživatelů izolován[4].

2.4 Kryptoměny

Jelikož při provozování ilegálních služeb je hlavním zájmem vydělat poměrně velké peníze, a to naprosto anonymně, bylo velmi obtížné v kriminálním (ale i pokud je záměrem anonymita) světě platit běžnými měnami. Proto začaly vznikat block-chainové kryptoměny, z nichž první (a dosud také nejznámější a nejvýznamnější) byla kryptoměna Bitcoin. Tu vytvořila skupina (či jednotlivec) pod pseudonymem Satoshi Nakamoto v roce 2009. Dalšími známými kryptoměnami jsou například Litecoin, Peercoin, Namecoin, Ethereum[6].

2.4.1 Obchodování měny

Kryptoměny sice mají nějakou svoji hodnotu a někde se s nimi dá platit[2], přesto se nejedná o běžné platidlo ať už z toho důvodu, že mimo kriminální činnost se toho s ním moc nakoupit nedá, nebo z důvodu relativně vysoké nestability způsobené obecným povědomím jako investiční měny[14]. Hlavním využitím kryptoměn tedy je zajištění anonymity. Tedy pokud někdo chce pořídit nějaké zboží s libovolnou kryptoměnou, založí si účet u směnárny umožňující nákupy kryptoměn (či si stáhne aplikaci), převede běžné peníze (například eura) na danou kryptoměnu, na adresu zadanou prodejcem převede (převod je anonymní, co se týká fakturačních údajů atp.) danou částku a doufá, že mu přijde objednané zboží (záleží na kredibilitě prodejce)[17].

Další dobrý poznatek je, že i když se kryptoměny označují jako platidla, tak dle formálního hlediska se o platidlo nejedná, jelikož neodpovídá žádnému typu platby dle zákona o platebním styku (č. 284/2009 Sb.).

„*Vysvětlení Petry Petlachové, mluvčí Generálního finančního ředitelství:*
Bitcoiny (obecně všechny virtuální měny) finanční správa považuje z pohledu českého soukromého práva za věc v právním smyslu, a to za věc nehmotnou, movitou a zastupitelnou. Z dostupných stanovisek ČNB vyplývá, že bitcoiny nejsou bezhotovostní peněžní prostředky ani elektronické peníze, nákup nebo prodej bitcoinů na vlastní účet nepředstavuje žádnou z platebních služeb ani bezhotovostní obchod s cizí měnou podle zákona o platebním styku (č. 284/2009 Sb.). Směna bitcoinů za oficiální měnu nenaplňuje znaky směnárenského obchodu a bitcoiny nevykazují ani znaky investičního nástroje — nemají povahu ani cenného papíru ani derivátu.“[7]

Dále se dá zmínit, že byť banky provozující tento typ směn nemusí hlásit jednotlivé transakce, v případě podezřelých transakcí musí dle zákona proti praní špinavých peněz (č. 253/2008 Sb.) upozornit policii.

2.4.2 Princip fungování blockchainu

Základem fungování každé kryptoměny se stala technologie blockchainu. Jedná se v podstatě o distribuovaný systém peněženky obsahující všechny informace o jednotkách dané měny. Tato peněženka se pak v průběhu času rozrůstá o další a další položky dané měny,

[2] Za zmínku v rámci legální činnosti stojí relativně nová možnost platit s ní u podniku Elona Muska, viz http://www.hybrid.cz/tesla-zacala-prijimat-platbu-bitcoiny.

přičemž každá tato položka je chráněna před zásahy jak zvenčí, tak před zásahy jednotlivých uživatelů a vlastníků uzlů obsahujících dané položky. Každá taková položka pak obsahuje data o aktuálním vlastníkovi, o vykonávané transakci, o adrese odesílatele a adresáta atd. Každý uživatel dané kryptoměny má pak nějakou (může mít i více) anonymní adresu, se kterou vykonává transakce. To vše je pak kryto asymetrickou kryptografií fungující v PKI využívající různé šifrovací algoritmy (může používat standardní RSA, ale i například algoritmy SM9). Tento princip současně řeší i možnost manipulace, jelikož pro napadení měny by musel získat k více místům, kde je uložena daná část měny[8][16].

Kapitola 3

Hedvábná stezka

Distribuce drog a jiných nepříliš legálních látek se historicky odehrávala především v ulicích a temných zákoutích měst, což ale nebylo příliš bezpečné z hlediska kupujícího. Proto se s rozmachem internetu vytvořily myšlenky prodeje zboží právě skrze něj. Průkopníkem pak v tomto ohledu byla služba texaského rodáka Rosse Ulricha (přezdívaného Dread Pirate Roberts) Silk Road, která přesně na tento problém navazovala a řešila ho právě díky funkcionalitám darkwebu (předchozí pokusy nebyly zcela úspěšné z toho prostého důvodu, že na původním internetu nebylo možné zajistit naprostou anonymitu)[13].

3.1 Nabízené služby

Server se primárně soustředil na distribuci drog. Párkrát se objevily i pokusy o distribuci zbraní (od webu Silk Road se oddělil web armory, který se tímto zabýval; nakonec ale v rámci konkurence nebyl příliš úspěšný) a pedofilního obsahu (který je ale nakonec dle základní filozofie serveru odsouzen a nepovolen). Prakticky jen na drogy se nakonec tento web zaměřoval nejspíše z několika praktických důvodů, a to jednak z důvodu obav o zahrnutí dalších policejních a vyšetřovacích složek, jednak z důvodu obav o konkurenční weby, které mohly být agresivní a v podstatě ohrozit fungování Silk Road. Dále se dokonce web Silk Road distancoval od prodeje kradených věcí a informací, ukradených kreditních karet, padělaných peněz a dokonce i atentátů, a to opět ze stejných důvodů (částečně asi i z morálního hlediska)[13].

Důvodem úspěchu této sitě ale nebyla jenom samotná podstata prodeje drog, ale i podle anonymních slov tamních uživatelů dobrá komunita, způsob hodnocení a svobodná fóra. Aby web omezil podvody, každý prodejce musel vložit nějakou zálohu do Silk Road a každý prodejce pak měl i své osobní hodnocení[1]. To vedlo k tomu, že pokud někdo často nedoručil slíbenou dodávku (nebo to prostě byl podvodník), získal negativní recenze a nikdo si od něj už nic nekoupil.

Co se týká fóra, to skýtalo velkou popularitu právě z toho důvodu, že bylo necenzurované a lidé mohli diskutovat o čemkoliv chtěli bez nějakých vnějších omezení. Navíc se většinou jednalo o lidi podobného smýšlení (protože na takový obchod nechodí každý), takže by se tato fóra dala označit jako darkwebová sociální síť. Navíc mnozí jeho uživatelé vnímali Silk Road jako vzpouru vůči autoritám a bojovníka za svobodu. Někteří také zmiňují ochranu

[1] Podobný karmický princip můžeme vidět i na dnešních běžných aukčních serverech, například na aukro.cz či ebay.com

ústavy Spojených států. Argumentace okolo ústavy pak ještě vzrostla po zatčení zakladatele Rosse Ulricha následným obviněním.[4][13].

3.2 Způsob zabezpečení klientů, PGP

Jelikož hlavním účelem takových stránek mělo být bezpečné nakupování ilegálního zboží, bylo nutné zamezit vnějším přístupům. Toho krom využívání protokolů sítě Tor sloužily i program PGP pro asynchronní šifrování.

PGP, Pretty Good Privacy, je snaha o zabezpečovací standard, který má být otevřený a rozšířený a sloužící k zabezpečenému předávání informace mezi komunikujícími subjekty. Využívá klasické šifry RSA, kdy subjekt 1 má svůj soukromý a veřejný klíč a své vlastní dva takové klíče má i subjekt 2. Tyto dva subjekty si pak vzájemně posílají své veřejné klíče a s pomocí soukromého klíče překládají odeslané zprávy. V případě sítě Silk Road (či jejích dnešních nástupců) má každý profil na své strácnce svůj veřejný klíč a soukromé klíče má každý své vlastní skryté [4].

3.2.1 Způsob využití

Obchod tedy může probíhat následovně – zákazník použije k zašifrování zprávy nějaký svůj nainstalovaný program PGP (například Kleopatra; zpráva obvykle obsahuje adresu doručení), pro zašifrování použije své šifrovací údaje a e-mailovou adresu (veřejný klíč protistrany) prodejce. Tuto zprávu následně přes nějaký soukromý kanál (například přes privátní zprávy daného obchodu) zašle zakódovanou zprávu příjemci, který je jediný, kdo může zprávu dešifrovat (opět s pomocí svých údajů a použití nějakého PGP programu). K tomu se samozřejmě přidávají šifrování v rámci samotné sítě[9].

3.2.2 Výhody a rizika PGP

Při zaslání takové zprávy je velkou výhodou, že použitím externího PGP programu nezískává nikdo krom obchodníka obsah zasílané zprávy, což nakonec vedlo k tomu, že žádná data, krom těch, která nebyla šifrována, při zatýkání a zabavení zařízení správcům Silk Road neunikala. Problémem této komunikace nastává v tom, že je postavena na vzájemné důvěře. Jak bylo zmíněno výše (3.1), síť Silk Road využívala recenzentský systém pro tvorbu důvěryhodných poskytovatelů služeb, přesto to nemuselo být vždy dostačující[13].

3.2.3 Platby

Platby byly původně vykonávány tak, že využívaly anonymitu blockchainových kryptoměn (konkrétně v případě Silk Road Bitcoinu), přesto však mohlo docházet k podvodům ze strany prodávajícího. Proto se zkoušely různé možnosti, kdy například zákazník zaplatil jenom zálohu atp., až se došlo k principu escrow plateb. Při nich dochází k držení úschovny kryptoměn autoritou (trhem Silk Road v tomto případě), do té převede platící subjekt potřebnou částku a peníze z něj jsou pak uvolněny jen v případě, že jsou spokojeny obě strany nákupu[13].

Dalším problémem, který se u plateb odehrává, je jen částečná anonymita obchodování kryptoměn, jelikož se jedná o distribuovanou blockchainovou databázi, ke které má přístup každý účastník daného provozu. Aby se pak zamezilo sledování velkých podezřelých toků kryptoměny, vznikly takzvané šejkry (známy spíše jako tumblery), které spojují více trans-

akcí dohromady. Nedá se pak snadno dohledat, kdo kolik převáděl peněz a současně dojde ke správné platbě[13].

3.3 Právní stránka

Byť velká část služeb, na kterých tyto stránky fungují, zůstává legální (kryptoměny, šifrování, darknet), samotný prodej a distribuce drog a jiného zboží zůstává ilegální. Například dle zákonů v české republice[2] se osoba může dopustit přestupku přechováváním drog ve vlastním vlastnictví, neoprávněným pěstováním či distribuci osobám mladším 18 let (zde se může jednat o trestný čin). Dále je zakázáno se jakkoliv podílet na distribuci návykových látek.

V některým zemích světa dnes dochází k diskuzi o tom, do jaké míry by měly být návykové látky legální či ilegální (taková diskuze se vede nějakým způsobem i u nás) a například v Kanadě je dnes (od roku 2020) možné si pořídit marihuanu nejen k lékařským, ale i rekreačním účelům[11].

Dále se Silk Road po nějakou dobu dopouštěl ilegálního prodeje zbraní, například dle zákonů České republiky[3] je neoprávněné držení zbraní přestupkem a jejich neoprávněný prodej trestným činem. Dále se Ross Ulrich, vlastník sítě Silk Road, dopustil několika vydírání a výhrůžkek vraždou.

3.4 Pád Hedvábné stezky

Hedvábná stezka se několikrát stala terčem kybernetických (například DDoS) útoků, kdy ke konci dochází k únikům reálných IP adres jejich serverů, a současně byla dlouhodobě sledována vyšetřovacími jednotkami Spojených států. Největší ránu Hedvábné stezce udělalo zatčení a následná výpověď Curtise Greena (známého na tehdejší síti pod přezdívkou Flush), který se nachytal na nabídku agentů v přestrojení pod přezdívkou Nob, kdy agenti DEA dostali od Států výjimku pro prodej nastrčených drog. Tyto drogy pak samotnému Greenovi dorazily, avšak vzápěti se připojila i policie.

Následkem toho byla rozplétána velká síť zločinu a samotní autoři dopadali na vlastní spáchané chyby. Například samotné založení Hedvábné stezky počínalo inzerátem, kde byl uveden Gmail email s celým jménem hlavního autora Hedvábné stezky Rosse Ulricha.

Nakonec hlavní stopa k odhalení byly objednané falešné průkazy, které měly dojít na jistou adresu v San Franciscu. Při prvním navštívení policie Ulrich namítá, že něco takového by mohl udělat kdokoliv. Následně udělal Ross Ulrich významnou chybu, kdy na Stackoverflow přidává pod vlastním jménem dotaz, jak se přes PHP připojit na TOR. Od té doby je sledován a dle odhalených skutečností byly jeho časy připojení na internet totožné, jako logy hlavního admina pod přezdívkou Dread Pirate Roberts. Při zatýkání byl navíc nalezen v knihovně jak zrovna spravuje stránky Hedvábné stezky a následně při domovní prohlídce byly nalezeny zfalšované pasy s falešnými údaji. Výsledkem bylo, že na stránky byla umístěna velmi známá obrazovka s nápisem „Tato skrytá stránka byla dopadena“[4][5][4][13].

[2] Viz zákon č. 167/1998 Sb.

[3] Zákon o střelných zbraních a střelivu č. 119/2002 Sb.

[4] O soudním líčení a důkazech se dá více přečíst zde:
https://caselaw.findlaw.com/us-2nd-circuit/1862572.html.

[5] Na tomto odkazu můžete danou obrazovku zhlédnout
https://www.justice.gov/opa/press-release/file/1210446/download

Ross Ulrich nakonec byl s ohledem na rozsáhlou ilegální distribuci drog, způsobená úmrtí předávkováním a umožnění dostání drog k lidem, kteří by se k nim jinak nedostali, roku 2015 odsouzen na doživotní odnětí svobody bez možnosti zmírnění rozsudku[12].

3.5 Dopady Hedvábné stezky a závěr

Byť se policii povedlo zatknout spoustu lidí a zavřít spoustu služeb souvisejících s původní Hedvábnou stezkou, případ napomohl k seznámení širší veřejnosti s možnostmi temného webu a nákupu drog v něm. Takže výsledkem zatýkání nebylo omezení takových služeb, nýbrž vznik mnoha nových.

V některých případech se jednalo to tzv. exit scam, kdy se objevila pro zákazníky potenciálně zajímavá stránka, na které zaplatili za požadované zboží a o pár dní či týdnů stránka zcela zmizela a převedená peněžní částka spolu s ní. Někteří provozovatelé takových podvodů nakonec byli dopadeni, například za obchod Sheep Marketplace Tomáš Jiříkovský. [13].

Míra podvodů nakonec ale neznamenala, že se celý projekt ilegálního tržiště s drogami stane neúspěšný. Spíše naopak, jak se zvedl zájem, tak vznikla i seriózní tržiště, která se věnovala a některá stále věnují tomuto ilegálnímu byznysu, včetně Silk Road 2.0 (od původních tvůrců; uzavřeno v roce 2014) či AlphaBay (uzavřeno v roce 2017)[13]. S každým zavřeným tržištěm pak přišlo několik dalších, přičemž se dá předpokládat, že spousta jich dnes ještě funguje a ještě dlouho fungovat bude.

Literatura

[1] AUTHOR anonymous. *Research* [online]. TorProject, Naposledy viděno 2021. Dostupné z: https://research.torproject.org.

[2] AUTHOR anonymous. *When I'm using Tor, can eavesdroppers still see the information I share with websites, like login information and things I type into forms?* [online]. TorProject, Naposledy viděno 2021. Dostupné z: https://support.torproject.org/https/https-1/.

[3] COX, J. *This Fake Hitman Site Is the Most Elaborate, Twisted Dark Web Scam Yet* [online]. 2016. Dostupné z: https://www.vice.com/en/article/mg77bn/this-fake-hitman-site-is-the-most-elaborate-twisted-dark-web-scam-yet.

[4] DRBOLA, V. *Darknet: mýtus a realita kybernetického prostoru*. 2016. Diplomová práce. Filozofická fakulta Masarykovy univerzity.

[5] FACHKHA, C. a DEBBABI, M. Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. *IEEE Communications Surveys Tutorials*. First. 2016, sv. 18, č. 2, s. 1197–1227. DOI: 10.1109/COMST.2015.2497690.

[6] FRANKENFIELD, J. *Cryptocurrency* [online]. Naposledy viděno 2021. Dostupné z: https://www.investopedia.com/terms/c/cryptocurrency.asp.

[7] HOVORKA, J. *Jak se daní virtuální měny? Část zisku odvedete vždy, bitcoin je pro berňák věc* [online]. Naposledy viděno 2021. Dostupné z: https://www.mesec.cz/clanky/jak-se-dani-virtualni-meny-cast-zisku-odvedete-vzdy-bitcoin-je-pro-bernak-vec/.

[8] IEEE. IEEE Standard for Data Format for Blockchain Systems. *IEEE Std 2418.2-2020*. First. 2020, č. 3, s. 1–32. DOI: 10.1109/IEEESTD.2020.9303503.

[9] KUOBIN, D. PGP E-Mail Protocol Security Analysis and Improvement Program. In: IEEE, ed. *2011 International Conference on Intelligence Science and Information Engineering*. 2011, s. 45–48. DOI: 10.1109/ISIE.2011.144. ISBN 978-1-4577-0960-9.

[10] NETOLIČKA, J. *Deep a Dark web – temná strana internetu*. 2020. Dostupné z: https://ipure.cz/archiv/magazin/deep-a-dark-web-temna-strana-internetu/#comments.

[11] SAPRA, B. *Canada becomes second nation in the world to legalize marijuana* [online]. CNN, Naposledy viděno 2021. Dostupné z: https://edition.cnn.com/2018/06/20/health/canada-legalizes-marijuana/index.html.

[12] Thielman, S. *Silk Road operator Ross Ulbricht sentenced to life in prison* [online]. The Guardian, Naposledy viděno 2021. Dostupné z: https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced.

[13] VELÍSEK, J. *Historie darknet marketů a principy jejich fungování [online]*. 2017 [cit. 2021-04-20]. Dostupné z: DostupnézWWW<https://is.muni.cz/th/emtih/>.

[14] Vávra, J. *Krypto-graf týdne: Další prudký pád bitcoinu. Velcí hráči ale hned přikupují* [online]. Naposledy viděno 2021. Dostupné z: https://www.e15.cz/kryptomeny/krypto-graf-tydne-dalsi-prudky-pad-bitcoinu-velci-hraci-ale-hned-prikupuji-1377296.

[15] Wardana, H. K., Handianto, L. F. a Yohanes, B. W. The onion routing performance using shadow-plugin-TOR. In: IEEE, ed. *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*. IEEE, 2017, s. 1–5. DOI: 10.1109/EECSI.2017.8239183. ISBN 978-1-5386-0549-3.

[16] Zhang, L. a Ge, Y. Identity Authentication Based on Domestic Commercial Cryptography with Blockchain in the Heterogeneous Alliance Network. In: IEEE. *2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE)*. 2021, s. 191–195. DOI: 10.1109/ICCECE51280.2021.9342494. ISBN 978-1-7281-8320-6.

[17] Čížek, J. *Jak fungují kryptoměny: Za oponou se odehrává perfektně organizovaný chaos* [online]. Naposledy viděno 2021. Dostupné z: https://www.zive.cz/clanky/jak-funguji-kryptomeny-za-oponou-se-odehrava-perfektne-organizovany-chaos/sc-3-a-190914/default.aspx.