VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

DARKNET: FENOMÉN ANONYMNÍ KRIMINALITY

Autor práce: Petr Pluhař

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: JUDr. Milan Kocík, MBA

Katedra: Právních oborů a bezpečnostních studií

2024

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Petr Pluhař

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Darknet: fenomén anonymní kriminality

Název bakalářské práce v anglickém jazyce: Darknet: The Phenomenon Of Anonymous Crime

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):
JUDr. Milan Kocík, MBA
Datum zadání bakalářské práce (měsíc, rok): květen, 2023

Cíl bakalářské práce:
Hlavním cílem bakalářské práce bude teoreticko-popisně charakterizovat online prostor darknetu a vymezit jeho základní kriminologická specifika, která z darknetu vytváří globálně využívané kriminální prostředí. Vedlejším cílem bude provést analýzu statistických dat kyberkriminality. Druhým vedlejším cílem bude realizace a popis experimentálního vstupu do darknetu, včetně návrhu možných opatření směřujících ke ztížení vstupu do tohoto kriminálního prostředí.

Student: Petr Pluhař	10.6.2023 *datum*	*podpis*
Vedoucí práce: JUDr. Milan Kocík, MBA	10.6.2023 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	12.6.2023 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	14.6.2023 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	26.6.2023 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí(mu) bakalářské práce JUDr. Milan Kocík, MBA za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

PLUHAŘ, P. *Darknet: fenomén anonymní kriminality: bakalářská práce.* Příbram: Vysoká škola evropských a regionálních studií, 2024. 67 s. Vedoucí bakalářské práce: JUNDr. Milan Kocík MBA

Klíčová slova: darknet, dark web, darknetové tržiště, kyberkriminalita, Tor, opatření

Bakalářská práce se zaměřuje na fenomén dark webu, jehož anonymní platformy se staly útočištěm pro různé nelegální a neetické aktivity, včetně obchodování s drogami, prodeje zbraní a distribuce materiálu CSEA. V první, teoretické, části práce je představena historie a technologická struktura dark webu, včetně síti Tor a jejích skrytých služeb, a jsou diskutovány klíčové bezpečnostní aspekty a výzvy, které dark web přináší. Popsána je především problematika darknetových tržišť. Dále se práce zaměřuje na specifické kryptoměny. Část práce je stručně věnována také obecnému tématu kyberkriminality.

Cílem praktické části práce je realizace vstupu do darknetu, který je popsán s ohledem na jeho technickou nenáročnost a doložen screenshoty jednotlivých obrazovek. Popisujeme zde příklady možností získat nelegální zboží a služby. Závěrečná část je věnována návrhu možných opatření směřujících ke ztížení vstupu do prostředí darknetu.

ABSTRACT

PLUHAŘ, P. *Darknet: The Phenomenon OF Anonymous Crime: Bachelor Thesis.* Příbram: The College of European and Regional Studies, 2024. 67 pgs. Supervisor: JUDr. Milan Kocík MBA.

Key words: darknet, dark web, darknet marketplace, cybercrime, Tor, measures

The bachelor's thesis focuses on the phenomenon of the dark web, whose anonymous platforms have become a haven for various illegal and unethical activities, including drug trafficking, weapons sales, and the distribution of CSEA material. The first, theoretical part of the thesis introduces the history and technological structure of the dark web, including the Tor network and its hidden services, and discusses the key security aspects and challenges that the dark web presents. It primarily describes the issue of darknet marketplaces. Furthermore, the work focuses on specific cryptocurrencies. A part of the thesis is also briefly devoted to the general topic of cybercrime.

The aim of the practical part of the thesis is the realization and description of entering the darknet, which is described with regard to its technical simplicity and documented with screenshots of individual screens. Here we describe examples of opportunities to obtain illegal goods and services. The final part is devoted to the proposal of possible measures aimed at making it more difficult to enter the darknet environment.

Obsah

Úvod

V digitálním věku, kde internet otevírá nekonečné množství možností pro komunikaci, vzdělávání a obchod, existuje paralelní vesmír známý jako darknet. Tato bakalářská práce se věnuje prozkoumání tajemného a často nesprávně pochopeného světa darknetu, jehož existence vyvolává zájem i obavy. Darknet, často chybně zaměňován s deep webem, je unikátním segmentem internetu, který je nedostupný prostřednictvím běžných vyhledávačů a vyžaduje speciální software pro přístup. Jeho skrytá povaha a šifrovaná komunikace lákají široké spektrum uživatelů, od těch, kteří hledají anonymitu z legitimních důvodů, po ty, kteří se zapojují do nelegálních aktivit.

Cílem této práce je popsat nelegální prostředí darknetu, aby bylo možné lépe pochopit jeho strukturu, funkce, sociální dynamiku a přesah do kriminality. Tento výzkum se nesoustředí pouze na technologické aspekty darknetu, ale také zkoumá etické, právní a sociální otázky, které s ním souvisejí. Metodologicky se práce opírá o kombinaci kvalitativních výzkumných metod, především pak případové studie, aby poskytla komplexní pohled na toto skryté prostředí.

Volba tématu mé bakalářské práce se týká darknetu, a to pramení z mého dlouhodobého zájmu o informační technologie a prostředí internetu, který se u mě vyvinul během studia na střední škole s IT zaměřením. Fascinuje mě, jak rychle se digitální svět vyvíjí, a zvláště mě zaujalo tajemné a skryté prostředí darknetu. Darknet, často vnímaný jako nezmapovaná část internetu, je pro mě oblastí, kde se stýká vysoká technická sofistikovanost s etickými a právními dilematy. V posledních letech jsem pozoroval, jak se darknet stává stále více využíván k nelegálním činnostem, od prodeje zakázaných látek, až po šíření malwaru a provádění kybernetických útoků. Tento trend vnímám jako významný sociální a bezpečnostní problém, který si žádá hlubší pochopení a analýzu.

Darknet je komplexní a často nesprávně chápaný aspekt internetu. Přestože je často spojován s nelegálními aktivitami, má i řadu legitimních použití[1]. Těmito se však v naší práci podrobněji nezabýváme.

[1] MIREA, Mihnea; WANG, Victoria a JUNG, Jeyong. The not so dark side of the darknet: a qualitative study. *Security Journal*, 2019, 32. s. 102-118.

V teoretické části práce se zaměřuji na vymezení základní terminologie spojené s jednotlivými částmi internetu, tedy běžný internet, dark a deep web. Dále se zaměříme na přístupy k darknetu, tj. Tor a I2P, popíšeme stručně téma kyberkriminality a to především opět ve vztahu k darknetu, kde se specificky zaměříme na popis tržišť. V praktické části se pak pomocí exploratorního výzkumu v kombinaci s případovou studií zaměříme na dostupnost darknetového zboží a služeb pro běžné laické uživatele internetu a s ohledem na výsledky doporučíme limitující opatření.

1 Cíl a metodika bakalářské práce

Hlavním cílem teoretické části práce bude podat základní kriminologicko-technický popis online prostoru darknetu a vymezit jeho základní kriminologická specifika, která z darknetu vytváří globálně využívané kriminální prostředí. Cílem praktické části práce bude realizace a popis vstupu do darknetu, včetně návrhu možných opatření směřujících ke ztížení vstupu do tohoto kriminálního prostředí.

Popis cesty a praktického použití darknetu může být považován za kombinaci několika výzkumných metod, kterou lze klasifikovat jako exploratorní výzkum, který je doplněn prvky případové studie. Tento typ výzkumu se zaměřuje na zkoumání nových oblastí nebo jevů, o kterých není mnoho známo. V případě darknetu může jít o průzkum neznámých nebo málo prozkoumaných aspektů. Explaratorní výzkum může zahrnovat sběr informací, analýzu dostupných dat a procházení darknetu za účelem získání hlubšího porozumění. Cíl tohoto typu výzkumu je zjistit nové informace nebo vygenerovat hypotézy pro další výzkum. Exploratorní výzkum hledá a popisuje, jak se systém chová, či jaké jsou v něm závislosti. Exploratorní výzkum je prováděn za účelem získání lepšího povědomí o tom, co se děje a proč se to děje, čili provádí se za účelem stanovení hypotéz. Základem je popis a utřídění problému či situace, tedy deskripce a klasifikace, který obyčejně začíná „zeširoka“, ale jak průzkum postupuje, tato deskripce a klasifikace se zpřesňuje[2].

Případová studie je výzkumná technika, která se často používá v oblastech jako jsou psychologie, sociologie, politické vědy a antropologie. Základem této metody je důkladné zkoumání a analýza konkrétní sociální entity nebo jednotky, která může být například jednotlivec, rodina, skupina s konkrétním zájmem, etnickou příslušností, místní komunita nebo nějaká instituce. Tento "případ" je poté předmětem pozornosti studie, která jej zkoumá a zpracovává v celé šíři sociologicky relevantních aspektů. Často se setkáváme s komunitními studiemi jako typickým příkladem případové studie. Tato metoda využívá kombinaci různých technik shromažďování dat, přičemž preferuje dokumentární analýzu (jako jsou historické zdroje nebo statistiky) spolu s přímým pozorováním nebo rozhovory. Využívají se i audiovizuální záznamy. Případová studie obvykle upřednostňuje

[2] CRESWELL, John W. a CRESWELL, J. David. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017. ISBN: 978-1452226101.

kvalitativní metody a techniky, ačkoliv mohou být výjimečně využity i kvantitativní metody. Na rozdíl od statistického průzkumu, který shromažďuje omezené množství dat od mnoha jedinců, případová studie shromažďuje rozsáhlé množství informací od jednoho nebo několika málo subjektů. Vychází z předpokladu, že hluboký výzkum jednoho případu může pomoci porozumět ostatním podobným situacím. Nicméně si z podstaty svého charakteru neklade nárok na statistickou generalizovatelnost[3]. V tomto kontextu se jedná o podrobný popis a analýzu specifických aspektů darknetu, jako jsou konkrétní weby, komunity nebo technologie. Cílem metody je hluboce porozumět specifickým aspektům darknetu.

[3] HENDL, Jan. *Kvalitativní výzkum: základní metody a aplikace*. Praha: Portál, 2005. s.303.022. ISBN 80-7367-040-2.

2 Základní části internetu

2.1 Surface web

Surface web, známý také jako viditelný web nebo Clearnet, je ta část internetu, která je přístupná a indexovatelná běžnými vyhledávači jako je Google, Bing nebo Yahoo. Stránky na surface webu jsou snadno přístupné komukoliv s připojením k internetu a standardním webovým prohlížečem, bez potřeby speciálního softwaru nebo konfigurací. Jedním z klíčových rysů surface webu je, že jeho obsah je indexován běžnými vyhledávači. To znamená, že když zadáte dotaz do vyhledávače, výsledky, které se objeví, pocházejí z surface webu[4]. Obsah na Surface Webu zahrnuje většinu běžných webových stránek, jako jsou korporátní stránky, blogy, zpravodajské portály, e-commerce stránky, atp. Většina aktivit na Surface Webu je zcela legální a odpovídá běžnému používání internetu. Surface Web je ta nejviditelnější a nejběžnější část internetu, kde se odehrává většina online aktivit běžných uživatelů. Surface web tvoří zhruba 4 % celkového objemu internetu, což je stejně šokující jako povědomí o tom, že člověk využívá pouze 10 % svého mozku. Pro každý počítač připojený k běžnému internetu existuje specifická internetová protokolová adresa (IP). Poskytovatel internetových služeb (ISP) poskytuje internetové služby, jako jsou internetová protokolová adresa (IP) a doménové jméno. Pro zjištění polohy jakéhokoli zařízení připojeného k internetu můžeme použít IP adresu tohoto zařízení[5].

[4] LIU, Yizhi; LIN Fang Yu; AHMAD-POST, Zara, EBRAHIMI, Mohammadreza; ZHANG Ning et al. Identifying, collecting, and monitoring personally identifiable information: From the dark web to the surface web. In: *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 2020. p. 1-6. Dostupné z: https://doi.org/10.1109/ISI49825.2020.9280540

[5] LEWIS, M. (2018). *What Is the Dark Web – Who Uses It, Dangers & Precautions to Take* [online]. Dostupné z: https://www.moneycrashers.com/dark-web/. [citováno 2024-04-01].

2.2 Darknet a deep web

Darknet je termínem pro část internetu, která není přístupná prostřednictvím standardních vyhledávačů a vyžaduje speciální software, konfigurace nebo autorizaci pro přístup. Uživatelé darknetu často vyhledávají anonymitu, ať už pro ochranu osobních údajů nebo pro skrytí nelegálních aktivit. K tomu slouží nástroje jako Tor a I2P, kterým se budeme podrobněji věnovat dále. Většina obsahu na darknetu není indexována standardními vyhledávači, což znamená, že není (snadno) dostupná nebo viditelná pro běžné uživatele internetu. Darknet je často spojován s nelegálními aktivitami, jako je prodej drog, zbraní, krádež identity a další zločiny. Nicméně, ne všechny aktivity na darknetu jsou nezákonné; někteří lidé jej používají také k diskuzi o citlivých tématech, jako jsou politika nebo osobní problémy, ve větší anonymitě. Darknet může být také použit pro legitimní účely, jako je ochrana whistleblowrů, obcházení cenzury nebo pro komunikaci v represivních režimech. Transakce na darknetu jsou obvykle prováděny pomocí kryptoměn, kvůli jejich relativní anonymitě a obtížnému vysledování. Používání darknetu přináší určitá rizika, včetně možnosti napadení malwarem, krádeže identity a právních důsledků za účast na nelegálních aktivitách[6].

Mnoho osob spojených s darknetem si zachovává anonymitu nebo používá pseudonymy. Uvedená anonymita je výraznou podmínkou kriminálního jednání, což komplikuje identifikaci konkrétních "zakladatelů" nebo klíčových osob. Vývoj a historie darknetu jsou tedy spíše výsledkem kolaborativního a evolučního procesu, než dílem jednotlivých zakladatelů. Známý je nicméně Ross Ulbricht (vytupující pod pseudonymem Dread Pirate Roberts), zakladatel a správce Silk Road, jednoho z prvních a nejznámějších darknetových tržišť. Jeho případ byl medializován a zdůraznil existenci darknetových tržišť a jejich potenciál pro nelegální aktivity.

Za zmínku stojí dále Gary Davis (alias "Libertas"), jeden z administrátorů Silk Road. Jeho role ukázala, jak mezinárodní komunity spolupracují na darknetových tržištích[7].

---

[6] OZKAYA, Erdal a ISLAM Rafiqual (2019). *Inside the dark web.* CRC Press. ISBN: 9780367260453.

[7] WEISER, Benjamin. *Ross Ulbricht, creator of Silk Road website, is sentenced to life in prison*. New York Times. [online]. 2015. Dostupné z: Ross Ulbricht, Creator of Silk Road Website, Is Sentenced to Life in Prison - The New York Times (nytimes.com). [citováno 2024-04-01].

Pojem darknet a deep web jsou často zaměňovány, ale ve skutečnosti představují různé části internetu. Deep web zahrnuje všechny stránky na internetu, které nejsou indexovány standardními vyhledávači, jako je Google, Bing nebo Yahoo. To znamená, že tyto stránky nelze najít prostřednictvím běžných vyhledávacích dotazů. Deep web obsahuje širokou škálu neindexovaných stránek, včetně databází, soukromých firemních stránek, akademických časopisů, vládních záznamů, ale třeba také profilů sociálních sítí a dalších informací, které nejsou veřejně dostupné. Většina obsahu na deep webu je zcela legální a obvyklá. Tento obsah je často chráněn kvůli ochraně soukromí, bezpečnostním důvodům nebo proto, že není určen pro širokou veřejnost. Obsah Deep webu z celého množství internetu tvoří asi 96 %. Darknet je část Deep Webu, ale je specifický tím, že je přístupný pouze pomocí speciálních softwarových nástrojů, jako je Tor nebo I2P, které umožňují anonymní a šifrovanou komunikaci[8].

[8] HARSH, Kumar. Darknet Market Brings Billions In Crypto World, Finds Study. In:
HE, Bin, et al. *Accessing the deep web. Communications of the ACM*, 2007, vol. 50, no. 5, s. 94-101. ISSN: 0001-0782

3 Historie darknetu

Historie darknetu je úzce spjata s vývojem technologií pro anonymní komunikaci na internetu. Koncepty, které vedly ke vzniku darknetu, se začaly objevovat v 80. a 90. letech jako součást výzkumu v oblasti kryptografie a anonymní komunikace. V tomto období vznikly nápady jako například "mix networks" od Davida Chauma. Oficiální vznik darknetu je často připisován vytvoření Tor v roce 2002. S nárůstem povědomí o ochraně soukromí a anonymitě na internetu došlo k rozšíření využívání darknetu. Nástroje jako Tor Browser učinily přístup k darknetu snazším a přístupnějším pro širší veřejnost. Vznik a popularita online tržiště Silk Road, v roce 2011, které fungovalo na darknetu a umožňovalo uživatelům anonymně kupovat a prodávat drogy a jiné nelegální zboží, významně zvýšily veřejné povědomí o darknetu. Silk Road byl nakonec uzavřen federálními úřady v roce 2013[9].

Na darknetu je českého obsahu a uživatelů málo. Nejvýraznější vzestup v denních přístupech byl zaznamenán koncem září 2013, kdy překročil hranici 40 000. Od té doby však došlo k výraznému poklesu a počet denních přístupů se stabilizoval lehce pod 15 000. Tento náhlý nárůst byl zapříčiněn kombinací botnetových útoků, které se běžně používají k útokům na webové stránky, vedoucí k jejich přetížení a pádu, a změnou smluvních podmínek Googlu, který začal více sledovat uživatelské chování. V důsledku těchto změn se mnoho uživatelů přesunulo na anonymní a nekontrolovaný darknet. V porovnání s jinými zeměmi je Česká republika v užívání darknetu poměrně malým hráčem, s denním přístupem, který se umisťuje někde mezi Řeckem a Saudskou Arábií. Na vrcholu tohoto žebříčku jsou Rusko, Německo a především Spojené státy americké s až 400 000 denními přístupy. Přestože se Česko z hlediska těchto statistik může jevit jako marginální účastník, ve skutečnosti je to významný hráč ve využívání technologií spojených s darknetem. Zejména v síti Tor, která je celosvětově využívána pro anonymní přístup k informacím jak na darknetu, tak mimo něj, Česká republika vyniká počtem

[9] IdentityIQ. (n.d.). (2023). The Origins and History of the Dark Web. Cit. 2023. Dostupné z: https://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/#:~:text=Early%202000s%20%E2%80%93%20Present%3A%20Tor%E2%80%99s,people%20began%20to%20take%20advantage. [citováno 2024-04-01].

hostovaných tzv. „exit nodů“. Pokud jde o obsah, česká darknetová komunita má spíše charakter nadšenců pro moderní technologie než zločinců s IT zálibami[10].

Podle kvalitativní studie Mirea, Wang, Jung (2021) někteří z jejích účastníků uvedli, že se o darknetu dozvěděli z konvenčních otevřených zdrojů, včetně škol, zpravodajských médií a dalších diskusních fór na Surface Webu. Dnes jednoduché vyhledávání na Google nabízí nespočet webových stránek s návody, jak se dostat na darknet, jak stáhnout Tor, atp.[11]

V současné době je Tor nejpoužívanějším softwarem pro vstup na Dark Web[12]. Většina Dark Web stránek je přístupná pouze prostřednictvím sítě Tor. Nejsnazším způsobem, jak se připojit k síti Tor, je použití prohlížeče Tor.[13]

[10] Česko v datech. (n.d.). (2015). Odvrácená strana internetu: Český Darknet v číslech. Dostupné z: https://www.ceskovdatech.cz/clanek/28-odvracena-strana-internetu-cesky-darknet-v-cislech/. [citováno 2024-04-01].

[11] MIREA, Mihnea; WANG, Victoria a JUNG, Jeyong. The not so dark side of the darknet: a qualitative study. *Security Journal*, 2019, 32. s. 102-118.

[12] WOOLLASTON, Victoria. How To Access The Dark Web: What Is Tor And How Do I Access- Dark Websites?. In: *Alphr* [online]. 2020. Dostupné z:
world-finds-study-news-183428. [citováno 2024-04-01].

[13] KOBIE, Nicole. What is the dark web? How to use Tor to access the dark web. In: *Wired* [online]. 2019. Dostupné z: https://www.wired.co.uk/article/what-is-the-dark-webhow-to-access. [citováno 2023-24-12].

4 Tor

Tor, zkratka pro The Onion Router, je volně dostupný software a síť, která umožňuje anonymní komunikaci na internetu. Byl vyvinut v námořní výzkumné laboratoři Spojených států a později se stal projektem s otevřeným zdrojovým kódem. Za autory, vývojáře jsou považováni Paul Syverson, Rogere Dingledin a Nick Mathewson. Tor používá techniku zvanou „onion routing“, kde data procházejí přes síť serverů, nazývaných uzly Toru, které je šifrují a přeposílají. Tímto způsobem se skryje původní zdroj informací a jejich konečný cíl, čímž se zvyšuje anonymita uživatelů. Data jsou předávána mezi uzly ("nodes") v síti. Každý uzel odstraní jednu vrstvu šifrování, což je metaforicky přirovnáváno k odstraňování vrstev cibule (odtud název „onion routing“). Tento proces zajišťuje, že žádný jednotlivý uzel nezná jak původ, tak konečný cíl dat. Poslední uzel v řetězci, známý jako „exit node“, odstraňuje poslední vrstvu šifrování a předává data do jejich cílové destinace v běžném internetu[14]. Mosty mohou být nastaveny i ručně, což je zvláště užitečné v zemích, kde vláda blokuje Tor provoz, jako je například Turecko. Tyto mosty, tvořené nezveřejňovanými a neindexovanými uzly, se šíří diskrétně mezi uživateli. Důvodem je, že jakmile se o nich vláda dozví, obvykle je zablokuje. To vede k vytváření nových mostů, díky kterým je celá Tor síť znovu dostupná[15].

Tor je často používán pro ochranu identity a zajištění soukromí na internetu. Umožňuje uživatelům procházet internet, aniž by odhalili svou fyzickou polohu nebo další identifikační informace. Tor je také nástroj pro obcházení cenzury internetu v režimech, kde je přístup k informacím omezen nebo kontrolován. Mimo darknet se používá také pro zabezpečenou komunikaci, například novináři pro komunikaci se zdroji, politickými aktivisty. Ačkoliv Tor zvyšuje anonymitu, není stoprocentně bezpečný. Útoky prostřednictvím exit nodů a pokročilé sledovací techniky mohou ohrozit anonymitu uživatelů.

[14] OWEN, Gareth a SAVAGE, Nick. *The tor dark net.* Published by the Centre for International Governance Innovation and the Royal Institute of International Affairs. 2015. Bez ISBN.

[15] STROUKAL, Dominik. *Dark Web: Sex, drogy a bitccoiny*. Praha: Grada Publishing, a.s., 2020. ISBN 978-80-271-2934-8.

Speciální prohlížeč postavený na bázi Mozilla Firefox, který automaticky používá síť Tor pro veškerou internetovou komunikaci, se nazývá Tor browser.[16]

Pixel Privacy (2023) popisuje, že Tor Browser je upravenou verzí prohlížeče Mozilla Firefox a obsahuje rozšíření jako TorButton, TorLauncher, NoScript a HTTPS Everywhere, spolu s Tor proxy. Tor Browser lze spouštět i z přenosných médií, například z USB klíčenky. Mezi známé vyhledávače patří DuckDuckGo (verze pro Tor), notEvil a Candle. Tyto vyhledávače jsou navrženy tak, aby usnadnily navigaci na darknetu a umožnily uživatelům nalézt relevantní obsah[17].

Odhad počtu uživatelů Tor činil v roce 2015 tři miliony[18], v roce 2018 čtyři miliony a od té doby data nemáme.

Používání VPN (Virtual Private Network neboli Virtuální privátní síť je vhodným bezpečnostním doplňkem. Bez VPN mohou poskytovatelé internetových služeb (ISP) a webové stránky zjistit, že uživatel používá Tor, protože IP adresy Tor uzlů jsou veřejně dostupné. Avšak ISP pak již nemůže dešifrovat uživatelovu komunikaci a webové stránky nemohou určit, kdo k nim přistupuje. Samotný přístup k síti Tor je ve většině zemí zcela legální. Nicméně připojení k síti Tor může přitáhnout nechtěnou pozornost, například ze strany vlády. Čína zakázala služby poskytující anonymitu a prostřednictvím velkého firewallu blokuje provoz sítě Tor. Některé další země, jako Írán, Rusko nebo Saudská Arábie, intenzivně pracují na tom, aby zabránily občanům v přístupu k síti Tor[19].

[16] MACRINA, April a Eric PHETTEPLACE. The Tor browser and intellectual freedom in the digital age. *Reference and User Services Quarterly*. 2015, vol. 54, no. 4, s. 17-20. ISSN: 1094-9054.

[17] Pixel Privacy. (2023). *The Ultimate 2023 Guide to The Tor Browser – Explained*. [online]. Dostupné z: https://pixelprivacy.com/resources/tor-browser-guide/#:~:text=How%20Does%20the%20Tor%20Browser,a%20USB%20stick%2C%20for%20example. [citováno 2023-12-23].

[18] EVERETT, Cath. *Should the dark net be taken out?*. Network Security, 2015. vol. 2015, no. 3, s. 10-13. ISSN: 1353-4858. Dostupné z: https://doi.org/10.1016/S1353-4858(15)30018-0

[19] ILIADIS, Lazaros Alexios a KAIFAS, Theodoros. Darknet traffic classification using machine learning techniques. In: *2021 10th international conference on modern circuits and systems technologies (MOCAST)*. IEEE, 2021. p. 1-4.

5 I2P

I2P, zkratka pro Invisible Internet Project, je anonymizační síť, která umožňuje bezpečné a anonymní internetové komunikace. I2P je navržena tak, aby poskytovala silnou ochranu soukromí a anonymitu pro své uživatele. Podobně jako Tor, I2P využívá technologii podobnou onion routing pro zajištění anonymity. Místo toho, aby však data posílala přes vnější internet, I2P data udržuje uvnitř své vlastní sítě. I2P je primárně zaměřena na interní komunikaci mezi uživateli ve své síti. Má schopnost posílat a přijímat zprávy, provádět anonymní webové procházení, chat a další komunikační funkce uvnitř své sítě. I2P vytváří to, co se nazývá "tunely", které jsou jednosměrné a umožňují šifrovaný přenos dat. Každá komunikace je rozdělena do několika cest, což zvyšuje bezpečnost a anonymitu. I2P je silně decentralizovaná, což znamená, že nemá žádný centrální bod kontroly nebo selhání, což zvyšuje její odolnost vůči útokům a cenzuře[20].

I2P je populární mezi uživateli, kteří hledají vyšší úroveň anonymity pro své internetové aktivity. Díky své decentralizované struktuře je I2P odolná vůči pokusům o cenzuru. Uživatelé mohou hostovat webové stránky a služby v I2P, což se nazývá "eepsites". Zatímco I2P poskytuje silnou anonymitu, uživatelé by měli být opatrní, aby neodhalili svou identitu prostřednictvím chybného používání nebo konfigurace. Podobně jako u jiných anonymizačních sítí, existuje riziko využití I2P pro nelegální aktivity. I2P je dostupné jako software, který si uživatelé mohou stáhnout a nainstalovat na své počítače, aby se připojili k síti. Celkově I2P poskytuje robustní platformu pro anonymní komunikaci a je často používána pro ochranu soukromí a svobody projevu online. Jde o důležitý nástroj pro ty, kteří hledají alternativu k tradičnímu internetu nebo k sítím jako je Tor.[21]

[20] ZANTOUT, Bassam a HARATY, R. I2P data communication system. In: *Proceedings of ICN*. Singapore: ICN, Springer, 2011. p. 401-409.

[21] GEHL, Robert W. *Weaving the dark web: Legitimacy on Freenet, Tor, and I2P*. MIT Press, 2018. ISBN 9780262038263.

6 Kyberkriminalita

Kyberkriminalita je rychle se rozvíjející oblast zločinu, která zahrnuje širokou škálu nelegálních aktivit prováděných prostřednictvím počítačů nebo sítí. V současném digitálním věku, kde je většina společnosti stále více propojena s internetem, se kyberkriminalita stala významnou hrozbou pro jednotlivce, organizace i státy. Zločinci využívají anonymitu, rychlost a globální dosah internetu k provádění různých druhů protiprávních činností.

Kyberkriminalita je široký pojem, který zahrnuje mnoho různých forem nelegálních aktivit provedených pomocí počítačů nebo sítí. Rozsah kyberkriminality je rozmanitý a neustále se rozšiřuje s novými technologickými vývoji. Níže uvádíme přehled některých klíčových forem kyberkriminality:

- **Krádeže Identity**: Zahrnuje neoprávněné shromažďování a využití osobních údajů, jako jsou čísla sociálního zabezpečení, kreditní karty a další finanční informace. Zahrnuje se mezi kriminalitu odehrávající se v online prostředí, ale s možnými účinky v běžném prostředí.

- **Phishing**: Tato technika zahrnuje zasílání podvodných e-mailů nebo zpráv, které se snaží uživatele přimět k poskytnutí citlivých informací, jako jsou hesla nebo bankovní údaje. Zahrnuje se mezi kriminalitu odehrávající se v online prostředí.

- **Malware**: Zahrnuje škodlivý software, jako jsou viry, červi, trojské koně a ransomware, který je navržen tak, aby poškodil nebo získal přístup k systémům bez vědomí uživatele. Zahrnuje se mezi kriminalitu odehrávající se v online prostředí.

- **Útoky Ransomware**: Specifická forma malware, která šifruje data oběti a požaduje výkupné za jejich odemčení. Zahrnuje se mezi kriminalitu odehrávající se v online prostředí.

- **Kyberšpionáž**: Zahrnuje hacking prováděný s cílem získat důvěrné informace, obvykle pro politické, vojenské nebo průmyslové účely.[22]

- **Nelegální Obchodování na Darknetu**: Použití anonymních sítí, jako je Tor, pro prodej nebo distribuci nelegálního zboží a služeb, včetně drog a zakázaných materiálů.[23]

- **DDoS Útoky (Distributed Denial of Service)**: Tyto útoky zaplavují webový server nebo síť velkým množstvím dat, což vede k jejímu selhání.

- **Kreditní Kartové Podvody**: Zahrnují neoprávněné použití kreditních karet k provedení transakcí.

- **Sociální Inženýrství**: Manipulace lidí do provádění určitých akcí nebo zveřejnění důvěrných informací.[24]

S rozvojem technologií, jako jsou cloudové služby, umělá inteligence a Internet věcí (IoT), se objevují nové příležitosti pro kyberzločince. Například, IoT zařízení často trpí nedostatečnými bezpečnostními opatřeními, což je činí snadnými cíli pro hackerské útoky.[25]

Důsledky kyberkriminality jsou rozsáhlé a mohou zahrnovat finanční ztráty, poškození reputace, narušení osobního soukromí a dokonce ohrožení národní bezpečnosti. Případy, jako byl útok WannaCry ransomware v roce 2017, ukázaly, jak rozsáhlé mohou být důsledky těchto útoků.[26]

Boj proti kyberkriminalitě vyžaduje koordinované úsilí na několika frontách. Zahrnuje vzdělávání uživatelů, vývoj pokročilých bezpečnostních technologií a mezinárodní

---

[22] KASPERSKY, I. C. S. *Threat landscape for industrial automation systems. Statistics for H2*, 2021. [online] Dostupné z: https://ics-cert.kaspersky.com/publications/reports/2022/03/03/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2021/. [citováno 2024-04-01].

[23] UNODC. (2020). World Drug Report 2020. United Nations Office on Drugs and Crime.

[24] Cisco. (2020). *Annual Internet Report (2018–2023) White Paper*. Cisco Systems, Inc.

[25] Symantec. (2019). *Internet Security Threat Report.* Symantec Corporation. [online]. Dostupné z: https://www.insight.com/en_US/content-and-resources/brands/symantec/internet-security-threat-report.html. [citováno 2024-04-01].

[26] BBC News (2017). *'WannaCry ransomware cyber-attacks slow but fears remain'.* BBC News [online]. Dostupné z: https://www.bbc.com/news/technology-39920141 [citováno 2023-12-12].

spolupráci ve vymáhání práva. Přístupy zahrnují zvyšování povědomí o kybernetické bezpečnosti, používání šifrování a pravidelné aktualizace softwaru [27].

[27] Europol (2020) *Internet Organised Crime Threat Assessment (IOCTA).* The Hague: Europol. [online]. Dostupné z: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020. [citováno 2024-04-01].

6.1 Kybernetická kriminalita a ostatní kriminalita páchaná v kyberprostoru za rok 2023

Kriminalita páchaná v kyberprostoru v roce 2023 stále tvoří 10,8 % celkové registrované kriminality. Dle statistických dat je tento trend setrvale stoupající (meziročně +0,6 %, +1 038 skutků), přesto však oproti předchozím rokům jde o vzestup podstatně nižší. Objasněnost v této oblasti kriminality poklesla meziročně o 1,3 %. Opakovaně jsme zaznamenali pokles případů tzv. hackingu (-939, -33 %). Lze předpokládat, že skutky spáchané v dané oblasti jsou i tzv. souběhové s majetkovou trestnou činností.

V oblasti podvodů páchaných v online prostředí se stále setkáváme s provázanou sériovou trestnou činností. Typický je nábor legalizátorů výnosů z trestné činnosti na sociálních sítích a dalších online platformách. Phishing probíhá skrze e-mailovou komunikaci, sociální sítě a placenou inzerci na webových stránkách. Speciální variantou je phishing v podobě podvodných telefonátů a SMS zpráv. V podvodných telefonátech významně převažuje legenda falešného bankéře ve spojení s legendou napadeného bankovnictví. V těchto případech je často využíván vzdálený přístup k zařízení oběti a následný vklad peněz oběti do vkladomatů na virtuální měny. Přetrvává rozesílání podvodných SMS zpráv, které předstírají, že jsou zasílány institucemi nebo přepravními společnostmi. Cílem je vylákat přístupové údaje do internetového bankovnictví oběti a neoprávněně odčerpat její finanční prostředky. V současnosti zaznamenáváme nárůst případů s velmi nebezpečným modem operandi, a to kombinací podvodné SMS zprávy a podvodného telefonátu[28].

Dalším znepokojivým jevem je vzestup nových forem sociálního inženýrství, včetně tzv. callback phishingu. Tato technika kombinuje tradiční emailový phishing s telefonním podvodem (vishing) a často vede k instalaci škodlivého softwaru, jako je ransomware. Ransomware samotný zůstává významnou hrozbou, přičemž počet útoků ransomwaru se zdvojnásobil mezi lety 2020 a 2021[29]. Kromě toho je významným faktorem vzdělávání a zvyšování informovanosti v oblasti kybernetických rizik, zejména mezi malými a středními podniky, které často čelí obavám z virů, malwaru, ransomwarových a DDoS

[28] Policie České republiky. (2023). *"Statistické přehledy kriminality za rok 2023".* [online]. Dostupné z : www.policie.cz. [citováno 2023-12-23].

[29] ESET. (2023). *Trendy a výzvy v kyberbezpečnosti v roce 2023.* Digital Security Guide. [online]. Dostupné z: https://digitalsecurityguide.eset.com. [citováno 2024-04-01].

útoků[30]. V roce 2022 došlo v České republice k výraznému nárůstu některých forem kriminality, včetně majetkové a násilné kriminality. Byl zaznamenán výrazný nárůst majetkových trestných činů, jako jsou podvody a krádeže. Násilná kriminalita také zaznamenala nárůst, stejně jako mravnostní kriminalita, včetně případů týkajících se dětské pornografie[31]. Tyto statistiky a trendy naznačují, že kyberkriminalita je v České republice stále významnou a rostoucí hrozbou, která vyžaduje neustálou pozornost a inovativní přístupy k prevenci a ochraně.

[30] Prevence Kriminality. (2023). *Fenomén zvyšující se kybernetické kriminality byl hlavním tématem aktivit ke Dni bezpečnějšího internetu 2023.* [online]. Dostupné z: http://prevencekriminality.cz. [citováno 2023-12-23].

[31] Policie České republiky. (2022). *"Vývoj registrované kriminality v roce 2022"*. [online]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx. [citováno 2023-12-23].

6.2 Role darknetu v kybernetické kriminalitě

Darknet hostí tržiště, kde se prodávají drogy, zbraně, ukradené údaje, falešné doklady a další nelegální zboží. Kromě fyzických variant zboží se na darknetu prodávají i nástroje pro kybernetickou kriminalitu, jako jsou malware, ransomware, a služby pro DDoS útoky. Darknetová fóra slouží jako místa, kde se kyberzločinci scházejí, sdílejí informace, prodávají ukradená data (jako jsou osobní údaje, bankovní informace a další citlivé informace) a diskutují o metodách kybernetického útočení. Anonymita a decentralizovaná povaha darknetu komplikují snahy vymáhat právo a sledovat kyberzločince. Účinné řešení kybernetické kriminality na darknetu vyžaduje obvykle komplexní a expertní mezinárodní spolupráci a koordinaci[32]. V oblasti kybernetické bezpečnosti existují určité mezinárodní dohody, ale neexistuje jednotný, globálně přijímaný "mezinárodní zákon o kybernetické bezpečnosti". I na národní úrovni je situace zdaleka nejednoduchá. Podle nedávné zprávy britského ministerstva vnitra o kyberkriminalitě je hlášeno pouze 2–3 % takové aktivity a navíc mezi policejními složkami neexistuje konzistence v tom, jak provádějí vyšetřování. Podle Tima Watsona, ředitele Centra pro kybernetickou bezpečnost na Warwick University, je alarmující, že celých 80 % všech návštěv darknetových webů směřuje na stránky hostící dětskou pornografii. V důsledku toho se zdá, že zaměření na pedofilní aktivitu jako výchozí bod při řešení zločinu na darknetu, s nebo bez nevyhnutelných prvků politické expediencie, dává smysl[33].

[32] BYRNE, James M. a KIMBALL, Kathryn A. Inside the Darknet: techno-crime and criminal opportunity. In*: Criminal justice technology in the 21st century.* 2017. s. 206-232. ISBN: 978-0398091514

[33] EVERETT, Cath. *Should the dark net be taken out?.* Network Security, 2015. vol. 2015, no. 3, s. 10-13. ISSN: 1353-4858. Dostupné z: https://doi.org/10.1016/S1353-4858(15)30018-0.

6.3 Darknetová tržiště

Online tržiště je virtuální místo, kde dochází ke střetávání nabídky od mnoha dodavatelů s poptávkou od mnoha odběratelů. Podobně jako na tradičním trhu mezi dodavateli a odběrateli dochází k různým jednáním, která vedou k uzavírání obchodů. Darknetový trh lze rozdělit do dvou základních kategorií: nezávislé weby, které často provozuje jednotlivec nebo malá skupina a mohou být podvodné, a více strukturovaná tržiště podobná tradičním online portálům jako je například Aukro.cz. Tyto tržiště nabízejí širokou škálu produktů, včetně zbraní, hacknutých účtů, platebních karet s odcizenými údaji, padělaných dokladů, kreditních karet, falšovaných bankovek a pornografie. Dominantním zbožím na těchto trzích jsou však drogy a nově syntetizované psychoaktivní látky. Podle odhadů Evropského monitorovacího střediska pro drogy a drogové závislosti (EMCDDA) tvoří prodej drog asi dvě třetiny celkového objemu obchodů na darknetu. Na rozdíl od samostatných webových stránek, darknetová tržiště často nabízejí dodatečnou úroveň zabezpečení obchodu, obvykle prostřednictvím důvěryhodného prostředníka nebo escrow služby. Tato tržiště také implementují opatření proti podvodům, jako je placená registrace a hodnocení prodejců, a z tržeb si odvádějí určitý procentuální podíl. Dalším charakteristickým rysem těchto tržišť je použití kryptoměn pro transakce, což zajišťuje větší anonymitu než běžné bankovní převody[34]. V roce 2021 dosáhly tržby na tržištích darknetu celkem 2,1 miliardy dolarů v kryptoměnách. Tržišti Hydra Marketplace, které bylo toho času největším darknetovým tržištěm na světě, je připisováno přes 75 % celosvětových tržeb na darknetových tržištích za rok 2020[35]. Hodnocení na darknetových tržištích mají důležitou roli. Ačkoliv je možné najít hodnocení přímo na konkrétním tržišti, doporučuje se prověřovat prodejce i na dalších tržištích nebo na portálu Recon nebo na fóru Dread.

Životnost nelegálních tržišť na darknetu bývá omezená, často kvůli problémům jako je silná konkurence, nedostatek zákazníků a zásahy orgánů činných v trestním řízení[36].

---

[34] KRUITHOF, Kristy; ALDRIDGE, Judith; HÉTU Décary David; SIM Megan; DUJSO, Elma a HOORENS Stijn. *The role of the'dark web'in the trade of illicit drugs*. RAND, 2016. [online]. Dostupné z: https://www.rand.org/pubs/research_briefs/RB9925.html. [citováno 2023-24-12].

[35] HARSH, Kumar. Darknet Market Brings Billions In Crypto World, Finds Study. In:
HE, Bin, et al. *Accessing the deep web. Communications of the ACM*, 2007, vol. 50, no. 5, s. 94-101. ISSN: 0001-0782

[36] KRATINA, Tomáš a PITSCHMANN, Vladimír. Dostupnost vybraných syntetických opioidů a analgetik na darknet markets. *New Approaches to State Security Assurance*, 2021, 108.

Tržiště na darknetu obvykle končí jedním ze čtyř způsobů.

Bust / Takedown je forma ukončení provozu ze strany státu nebo mezinárodních organizací. Když stát nebo mezinárodní organizace ukončí provoz tržiště, vyšetřovatelé získají přístup k základní infrastruktuře tržiště a uzavřou jej.

Silk Road - jednoho z prvních a nejznámějších darknetových tržišť v roce 2013. Aby se předešlo velké pozornosti ze strany států a mezinárodních organizací, některá tržiště zakazují prodej určitých položek – například zbraní, fentanylu nebo dětské pornografie[37].

exit-Scam – únikový podvod. Při únikovém podvodu dojde k ukončení provozu tržiště bez předchozího varování kupujících a prodávajících, přičemž provozovatelé tržiště uniknou s penězi svých zákazníků. K tomuto podvodu může dojít i pouze ze strany prodejců, kteří ukradnou kupujícím peněžní prostředky a zakoupení zboží či službu nikdy nedodají. Tato forma ukončení tržiště byla velmi rozšířená v minulosti, avšak v posledních letech začala být tržiště ukončována oznámením o ukončení provozu. Mezi příklady únikového podvodu patří například tržiště Empire Market, které koncem srpna roku 2020 ukončilo svůj provoz únikovým podvodem s tím, že ukradlo zhruba 30 milionů USD38.

Poslední variantou ukončení provozu je oznámené ukončení. V tomto případě mají všichni kupující i prodejci možnost dokončit své obchody a vybrat své finance, než dojde k organizovanému ukončení tržiště. Existuje několik důvodů, proč tržiště ukončují svůj provoz touto cestou. Jedná se o vydělání dostatku peněz, **příliš vysoké riziko odhalení**, **vydírání nebo útoky jinými kyberzločinci** a další. Některá tržiště na darknetu slouží jako platformy pro svobodu projevu, umožňují diskuzi a obchod v represivních režimech, kde je přístup k informacím a zboží omezen. Po uzavření Silk Road se v následujících osmi letech otevřelo 87 tržišť na Darknetu. Obchod s drogami online rychle rostl,

[37] CAESAR, Ed (2021). The Takedown of a Dark-Web Marketplace. The New Yorker. [online]. 2021. Dostupné z: https://www.newyorker.com/news/news-desk/the-takedown-of-a-dark-web-marketplace.

[38] REDMAN, Jamie. Sources Say World's Largest Darknet Empire Market Exit Scammed, $30 Million in Bitcoin Stolen. In: *Bitcoin.com* [online] 2020. Dostupné z: https://news.bitcoin.com/sources-say-worlds-largest-darknet-empire-market-exit-scammed-30-million-in-bitcoin-stolen/. [citováno 2023-09-04].

například podíl Američanů, kteří kupovali drogy online, se téměř zdvojnásobil od roku 2014 do roku 2017 a s odhadovanými příjmy 14,2 milionu dolarů pouze v lednu 2016[39].

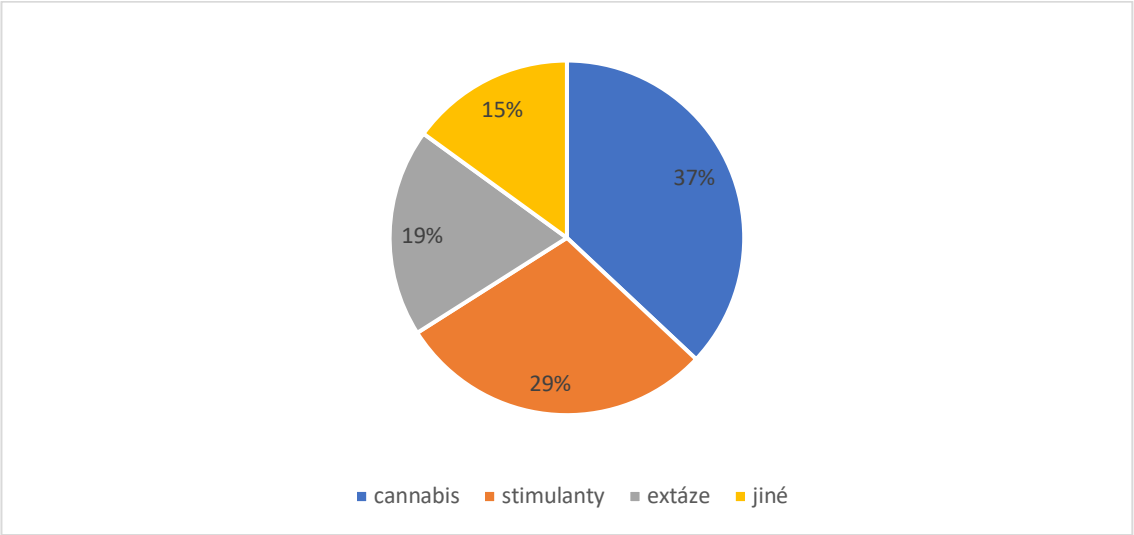
Nelegální drogy tvoří přibližně 85 % příjmů a 60 % celkového počtu nabídek na tržištích na Darknetu. Nejprodávanějšími látkami jsou cannabis (37 % celkových příjmů), stimulanty (29 % celkových příjmů) a extáze (19 % celkových příjmů). Tržiště na darknetu slouží jak velkoobchodu, tak maloobchodu. To lze usuzovat z rozmanitosti prodávaných množství, kdy některé nabídky prodávají malé množství jasně určené pro maloobchod a nabídky prodávající množství, která jsou příliš velká pro maloobchod. Velkoobchodní transakce představují přibližně 25 % celkových příjmů z drog prodávaných online[40]. Mezi další položky, které se prodávají na tržištích na Darknetu, patří psychiatrické léky, a během pandemie COVID-19 tržiště na Darknetu zaznamenala stále více nabídek osobní ochranné výbavy, léků a podvodů v oblasti lékařství – například falešné očkovací certifikáty.[41]

[39] KRUITHOF, Kristy, et al. *The role of the'dark web'in the trade of illicit drugs*. RAND, 2016. Bez ISBN.

[40] KRUITHOF, Kristy; ALDRIDGE, Judith; HÉTU Décary David; SIM Megan; DUJSO, Elma a HOORENS Stijn. *The role of the'dark web'in the trade of illicit drugs*. RAND, 2016. [online]. Dostupné z: https://www.rand.org/pubs/research_briefs/RB9925.html. [citováno 2023-24-12].

[41] BRACCI, Alberto; NADINI, Matthieu; ALIAPOULIOS, Maxwell; McCOY, Damon; GRAY, Ian; TEYTELBOYM, Alexander; GALLO, Angela a BARONCHELLI, Andrea. *Dark web marketplaces and covid-19: before the vaccine.* EPJ Data Science. 2021, vol. 10, no. 1, s. 6. ISSN: 2193-1127.

Graf 1: Procentuální přehled příjmu z darknetu[42]



Prodejci působící na tržištích na darknetu jsou obvykle prodejci, kteří dříve prodávali drogy osobně, a kteří se rozhodli přejít – úplně nebo částečně – k prodeji online. Hlavní motivací, která vede prodejce k přechodu na online prodej, je vnímání nižšího rizika odhalení policií, menší pravděpodobnost vystavení se násilí nebo podvodu ze strany zákazníků a vyhlídka na větší finanční zisky.[43]

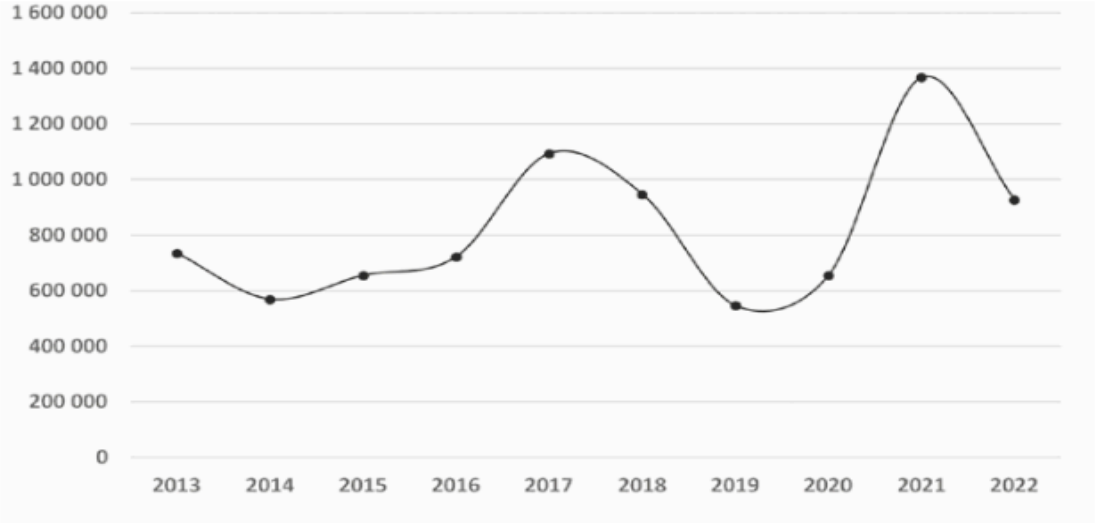
Většina zásilek z tržišť je odesílána prostřednictvím běžné pošty. V roce 2017 popisuje Agentura pro potírání drog (DEA), jak agent zakoupil čtyři různé typy drog od několika prodejců na platformě Dream Market a obdržel je všechny prostřednictvím Priority Mail. Látky odeslané poštou čelí riziku, že budou zabaveny. To však nevede k automatickému odhalení odesílatele a nepředstavuje dostatečný důkaz pro prokázání, že si kupující látku zakoupil na internetu. Prodejce nemusí na běžné zásilce uvádět svou adresu, kupující může vždy tvrdit, že mu byla látka doručena omylem. Prodejci v USA tvrdí, že dosáhli 100procentní úspěšnosti doručení ve více než 4 000 zásilkách. Navíc pravděpodobnost, že budou látky zabaveny, není tak vysoká, jak by se mohlo zdát, protože pošta obsahující

[42] KRUITHOF, Kristy; ALDRIDGE, Judith; HÉTU Décary David; SIM Megan; DUJSO, Elma a HOORENS Stijn. *The role of the'dark web'in the trade of illicit drugs*. RAND, 2016. [online]. Dostupné z: https://www.rand.org/pubs/research_briefs/RB9925.html. [citováno 2023-24-12].

[43] MARTIN, James; MUNKSGAARD, Rasmus; COOMBER, Ross; DEMANT, Jakob a BARRATT, Monica J. (2020). *Selling drugs on Darkweb cryptomarkets: Differentiated pathways, risk and rewards.* British Journal of Criminology, vol. 60, no. 3, s. 559-578. ISSN 0007-0955. Dostupné z: doi:10.1093/bjc/azz075.

drogy obvykle vypadá stejně jako běžná pošta a ne všechna běžná pošta je kontrolována bezpečností. Když je však produkt zabaven, kupující neví, zda prodejce produkt neodeslal, nebo byl produkt zabaven[44].

Graf 2: Množství zajištěné sušiny marihuany (g) v ČR[45]



Při nákupech na darknetových tržištích by měli kupující věnovat zvýšenou pozornost bezpečnostním opatřením. Je vhodné se chránit různými metodami – používat k platbám kryptoměny, využívat operační systém Tails, šifrovat data individuálně, objednávat nelegální zboží v menších množstvích, dávat přednost objednávkám z vlastní země a odhalovat o sobě pouze nezbytné informace. Někteří uživatelé mohou mít dojem, že nákupy na darknetu jsou zcela anonymní. Ačkoli plná anonymita může být dosažena při nákupu virtuálních položek, při objednávce fyzického zboží je často nutné poskytnout skutečné osobní údaje (jméno, příjmení, adresa). Pro nákup na některých tržištích je také nutná registrace a často se vyžaduje vklad určité částky pro ověření totožnosti kupujícího[46].

[44] The Washington Post. *Postal Service the preferred shipper for drug dealers.* [online]. 2018. Dostupné z: https://www.washingtonpost.com/politics/2018/10/16/postal-service-preferred-shipper-drug-dealers/. [citováno 2024-04-01].

[45] Policie České republiky. (2023). "Výroční zpráva NPC za rok 2022". Získáno z www.policie.cz

[46] VOLEJNÍK, R. (2016). *Darknet – fikce či realita anonymity skrytých služeb Tora systému bitcoin.* Brno. Bakalářská diplomová práce. Masarykova univerzita. Vedoucí práce Mgr. Viktor Pantůček. Dostupné také z: https://is.muni.cz/th/px96p/Darknet-fikce-ci-realitaanonymity-skrytych-sluzeb-Tor-a-systemu-bitcoin.pdf.

6.3.1 Novinky ze světa darknetových tržišť

Hydra byl největší darknetový trh na světě, dokud německá policie nezabavila jeho servery současně s označením OFAC v dubnu 2022, což efektivně ukončilo provoz tržiště. Hydra, se sídlem v Rusku, nejenže usnadňovala prodej drog, ale také nabízela služby praní peněz kyberzločincům, včetně útočníků ransomwaru. Hydra se pyšnila zákaznickým servisem s výhodami a uvážlivostí, kterou by člověk očekával spíše od legitimního podniku než od online drogového trhu. Hydra měla například službu, kde uživatelé mohli poslat drogy k testování na čistotu. Měli také Telegram bota, se kterým mohli uživatelé kontaktovat pro informace o první pomoci v případě předávkování. Pomáhali prodejcům spojit se se službami právní pomoci v případě, že byli vystaveni policejní razii. Hydra měla rovněž interní mixer nazvaný Bitcoin Bank Mixer, který mohli prodejci používat k výběru Bitcoinů z Hydry, které se na řetězci jevily jako čisté.

Uzavření Hydry vedlo k celkovému poklesu tržeb na darknetových trzích, průměrné denní tržby všech trhů klesly ze 4,2 milionu dolarů těsně před jejím uzavřením na 447 000 dolarů bezprostředně poté. I když tržby kolektivních drogových trhů nejsou zcela obnoveny, pomalu se vrátily k předchozím úrovním ve druhé polovině roku 2022[47].

[47] THOWSEAF, S. a SATHISH Kumar. Cryptocurrency May Prove Financial Crime: A Conceptual Analysis. In: *Emerging Insights on the Relationship Between Cryptocurrencies and Decentralized Economic Models*. IGI Global, 2023. s. 110-121. ISBN: 9781668456910.

7 Kryptoměny a darknet

Kryptoměny představují fascinující vývoj v oblasti digitálních financí. Jsou definovány jako decentralizované digitální nebo virtuální měny, které využívají kryptografii pro zajištění bezpečnosti transakcí a kontrolu vytváření nových jednotek. Bitcoin, zavedený v roce 2009 Satoshi Nakamotem, je považován za první a nejznámější kryptoměnu[48]. Od té doby bylo vytvořeno tisíce dalších kryptoměn, každá s unikátními vlastnostmi a zaměřením. Kryptoměny nabízejí řadu výhod, včetně decentralizace, což znamená, že nejsou kontrolovány žádnou centrální autoritou, což může přinášet vyšší úroveň finanční svobody a soukromí. Další výhodou je jejich globální dosah; kryptoměny mohou být odesílány nebo přijímány kdekoli na světě, kde je připojení k internetu. Však také přinášejí rizika, jako je volatilita cen, regulační nejistota a potenciální zneužití pro nelegální aktivity[49]. Nedávný vývoj v oblasti blockchainové technologie, která je základem mnoha kryptoměn, otevírá nové možnosti pro inovace v mnoha odvětvích, od financí po zdravotnictví a vládní služby[50]. K získání přehledu o nejpoužívanějších kryptoměnách je třeba se podívat na několik faktorů, jako jsou tržní kapitalizace, obchodní objem, uživatelská základna a technologický vývoj. K dubnu 2023 patřily mezi pět nejpoužívanějších kryptoměn následující:

- **Bitcoin (BTC)**: Jako první a nejznámější kryptoměna, Bitcoin drží vedoucí pozici z hlediska tržní kapitalizace a uznání. Je široce používán jako prostředek ukládání hodnoty a je často považován za "digitální zlato".
- **Ethereum (ETH)**: Ethereum je nejen kryptoměna, ale i decentralizovaná platforma, která umožňuje vývoj a provoz tzv. chytrých kontraktů a decentralizovaných aplikací (dApps). Její flexibilita a široké využití ji činí jednou z nejdůležitějších kryptoměn na trhu.

[48] NAKAMOTO, Satoshi. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* [online]. Dostupné z: https://bitcoin.org/bitcoin.pdf. [citováno 2024-04-01].

[49] CATALINI, Christian a S. GANS Joshua. *Some Simple Economics of the Blockchain.* NBER Working Paper No. 22952. 2016. Cambridge, MA: National Bureau of Economic Research. Dostupné z: doi:10.3386/w22952.

[50] IANSITI, Marco a Karim R. LAKHANI. *The Truth About Blockchain*. Harvard Business Review. 2017, vol. 95, no. 1, s. 118-127. ISSN: 0017-8012

- **Binance Coin (BNB)**: Vyvinutý společností Binance, jednou z největších kryptoměnových burz na světě, Binance Coin je používán k získání slev na poplatky za obchodování na burze Binance a pro řadu dalších účelů.
- **Cardano (ADA)**: Cardano se zaměřuje na poskytování vysoce bezpečného a udržitelného blockchainu, a je známé svým vědeckým přístupem k vývoji. Nabízí pokročilé funkce, jako jsou chytré kontrakty, které přitahují pozornost ve světě kryptoměn.
- **Solana (SOL)**: Solana je známá svou vysokou propustností a nízkými transakčními poplatky. Je oblíbená mezi vývojáři dApps, zejména v oblastech jako jsou decentralizované finance (DeFi) a decentralizované burzy (DEX)

I když kryptoměna bitcoin v minulosti na darknetu zaznamenala výrazný úspěch, nedávno došlo k jejímu postupnému poklesu a přesunu zájmu směrem k méně monero. Kriminální subjekty začaly hledat alternativní digitální měny, hlavně monero a ethereum. Odborníci tuto změnu přičítají technologii blockchain, na které je bitcoin založen. Když někdo získá bitcoin z bankomatu a použije ho k nákupu nelegálního zboží, je možné vysledovat původ peněz. Přestože u malých transakcí v bankomatu nemusí uživatel uvádět své jméno, policie může v případě potřeby zjistit totožnost pachatele pomocí kamer v okolí. Blockchain funguje na principu veřejného záznamu všech transakcí, což je v podstatě účetní kniha přístupná komukoliv. To znamená, že uživatelé musejí pro přijímání plateb použít veřejnou adresu složenou z čísel a písmen, což může vést k odhalení jejich identity. Tím jsou zpravodajské agentury schopny sledovat finanční pohyby na určených adresách a potenciálního zločince identifikovat, jakmile se pokusí vybrat peníze přes více regulovaný subjekt[51].

Monero (XMR) je populární kryptoměna, která byla vytvořena v dubnu 2014 s cílem poskytnout větší anonymitu a soukromí svým uživatelům než mnoho jiných kryptoměn. Zatímco Bitcoin a většina jiných kryptoměn mají transparentní blockchainy, Monero používá různé technologie, aby zajistilo, že transakce a částky jsou skryty a nelze je vysledovat. Kromě vysoké úrovně soukromí, které nabízí, je Monero také decentralizované a funguje na principu proof-of-work, což znamená, že je těžitelné.

[51] STROUKAL, Dominik. *Dark Web: sex, drogy a bitcoiny*. Praha: Grada, 2020, 207 s. ISBN 978-80-271-2934-8.

Jelikož není potřeba žádný speciální hardware, je oblíbené mezi jednotlivci, kteří chtějí těžit kryptoměnu doma pomocí běžných počítačů[52].

[52] AKCORA, Cuneyt Gurcan; GEL, Yulia R.; KANTARCIOGLU, Murat. *Blockchain networks: Data structures of bitcoin, monero, zcash, ethereum, ripple, and iota*. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2022, 12.1: e1436.

8 Tor browser

Nyní přestoupíme do empirické časti práce, kde bude cílem přiblížit reálné prostředí darknetu, od stažení prohlížeče až po jednotlivé stránky, portály a e-shopy.

- **Stažení Tor Browseru**

Otevřeme svůj běžný webový prohlížeč a přejdeme na oficiální stránku Tor Browseru: https://www.torproject.org/. Vybereme verzi Tor Browseru, která odpovídá našemu operačnímu systému (na výběr je Windows, macOS, Linux). Klikneme na tlačítko ke stažení a počkáme, až se instalační soubor stáhne na náš počítač.

- **Instalace Tor Browseru**

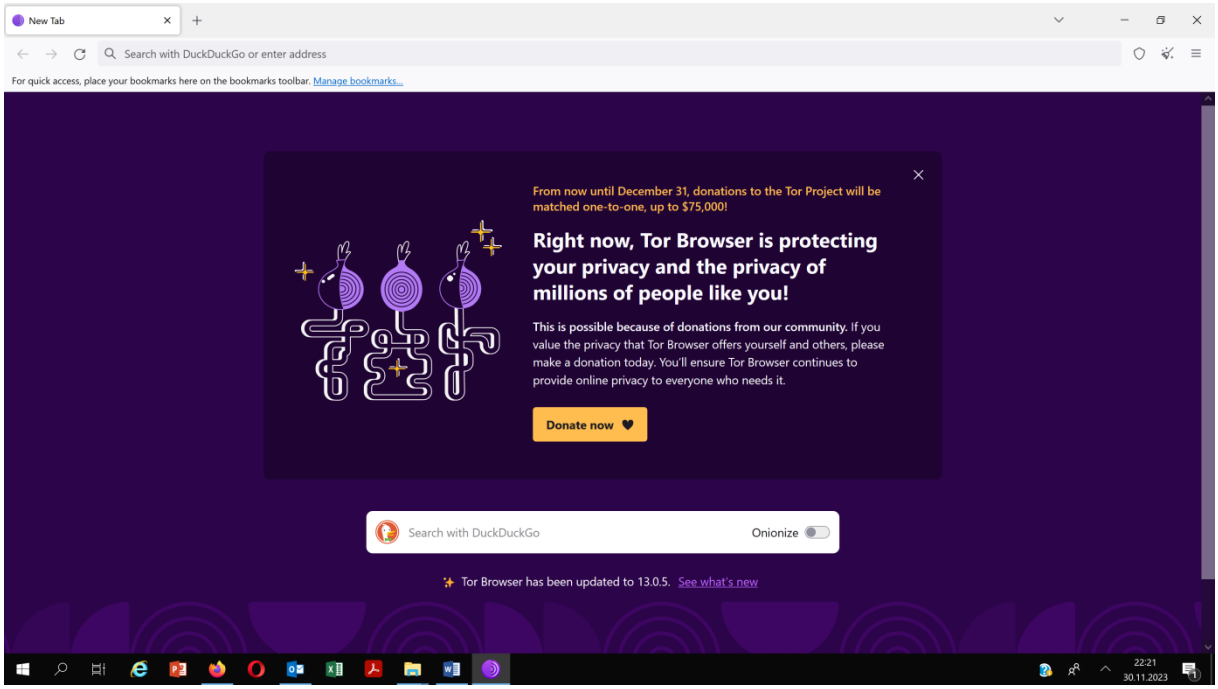
Najdeme stažený instalační soubor ve složce Stahování a spustíme jej. Postupujeme podle pokynů na obrazovce pro dokončení instalace. Po dokončení instalace otevřeme Tor Browser.

- **Používání Tor Browseru**

Při prvním spuštění Tor Browseru se zobrazí okno, které nás provede procesem připojení k Tor síti. Po připojení k Tor síti můžeme začít bezpečně a anonymně procházet internet jako s běžným prohlížečem. Můžeme navštěvovat běžné webové stránky nebo přistupovat k onion webovým stránkám, které jsou specifické pro darknet.

Obrázek 1 níže ukazuje stránku, která se zobrazí po otevření Toru.

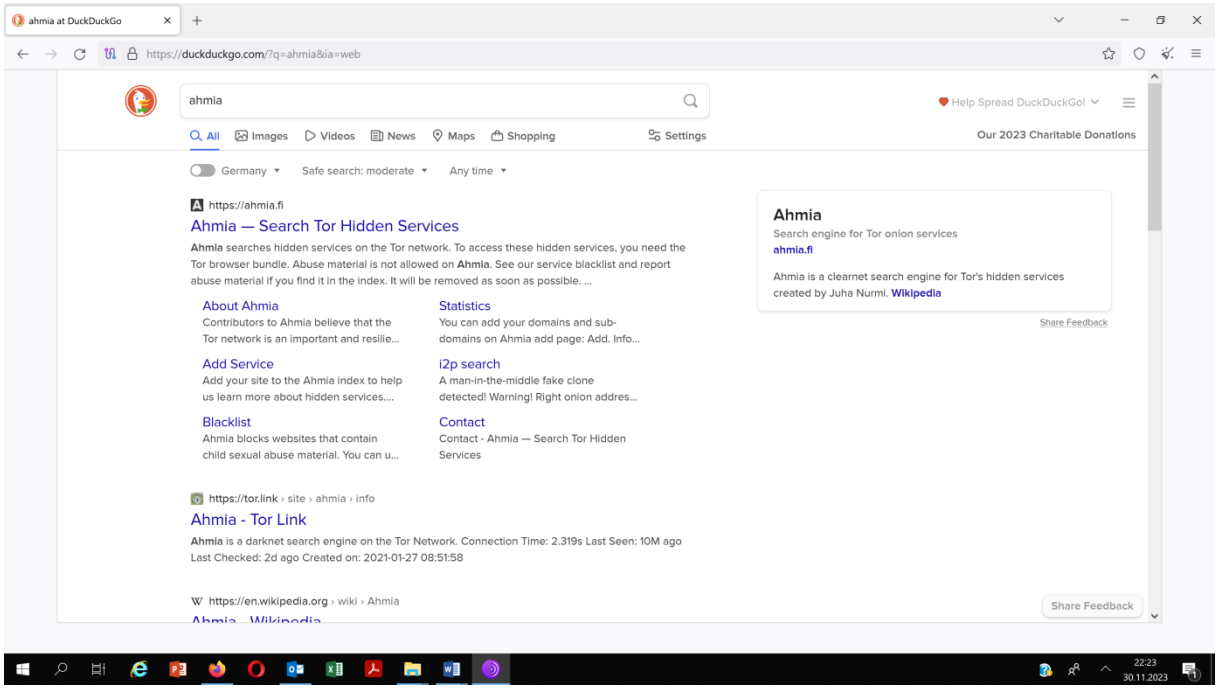
Obrázek 1: Úvodní stránka[53]



Webové stránky na darknetu často používají speciální doménové jméno končící na ".onion". Tyto adresy nelze nalézt pomocí běžných vyhledávačů jako Google. Existují vyhledávače určené speciálně pro darknet, jako je DuckDuckGo pro Tor, not Evil, nebo Torch, které umožňují hledání .onion stránek. Na obrázku 2 níže přikládáme ukázku úvodní stránky vyhledávače DuckDuckGo. Přes tento vyhledávač je možné navštívit i „nedarknetové“ stránky. Existují adresáře, jako například dark.fail nebo onion.live. Na tyto webové stránky se lze dostat i přes běžné prohlížeče, jako jsou Google Chrome, Firefox a další. Na těchto stránkách pak lze nalézt .onion adresy. Jedná se ale pouze o vybrané adresy a to ty nejznámější.

[53] Vlastní zdroj

Obrázek 2: Vyhledávač DuckDuckGo[54]



[54] Vlastní zdroj

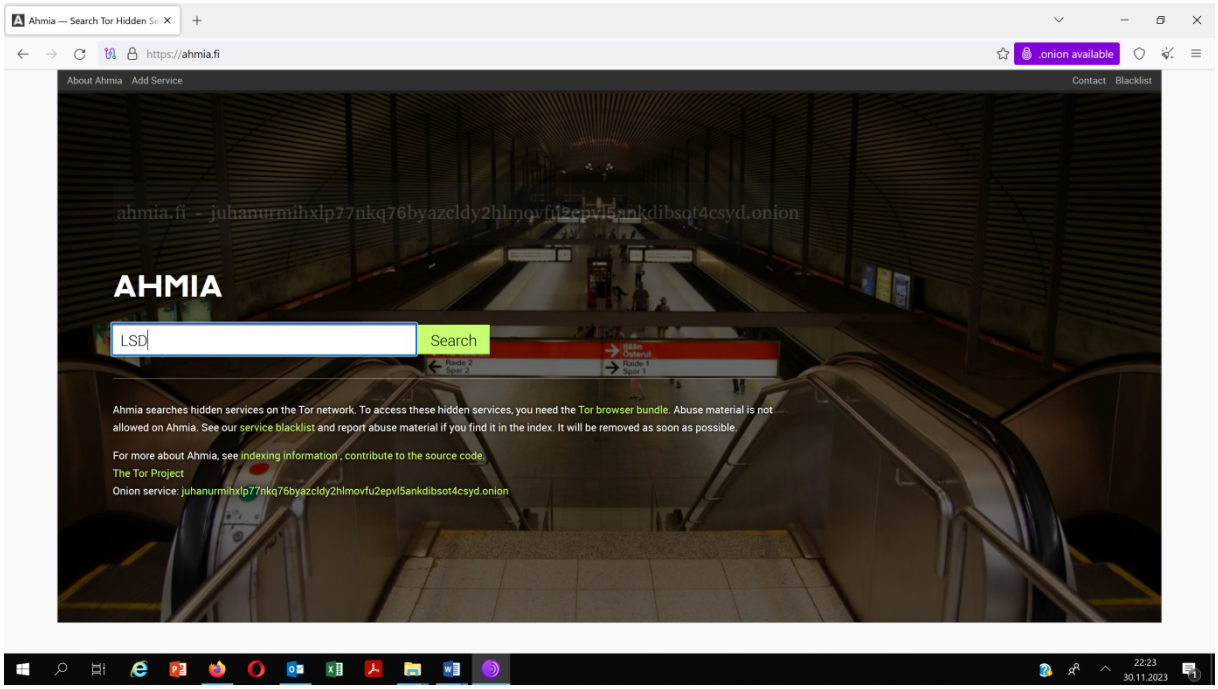
9 Ahmia a nákup drog na darknetu

Ahmia (viz obrázek 3 níže) je asi nejznámější vyhledávač speciálně navržený pro prohledávání obsahu na Tor síti. Hlavním cílem Ahmia je poskytnout přístup ke skrytým službám dostupným prostřednictvím sítě Tor a usnadnit vyhledávání v prostředí, které nelze prozkoumat pomocí běžných vyhledávačů. Ahmia se specializuje na indexaci webových stránek s koncovkou - onion, Ahmia se snaží filtrovat nelegální obsah ze svých vyhledávacích výsledků, ale i tak lze tyto stránky nalézt v hojné míře. Příkladem je náš pokus zakoupit na darknetu drogu LSD. Jak ukazuje obrázek č. 4, po zadání klíčového slova „LSD“ se zobrazí široká nabídka darknetových prodejců. Stejným způsobem lze samozřejmě sehnat v podstatě jakoukoli drogu. Na darknetu jsou eshopy specializující se na psychedelika, stimulanty, nebo třeba jen kanabinoidy, stejně jako eshopy poskytující celou škálu návykových látek, či třeba steroidy nebo léčiva.

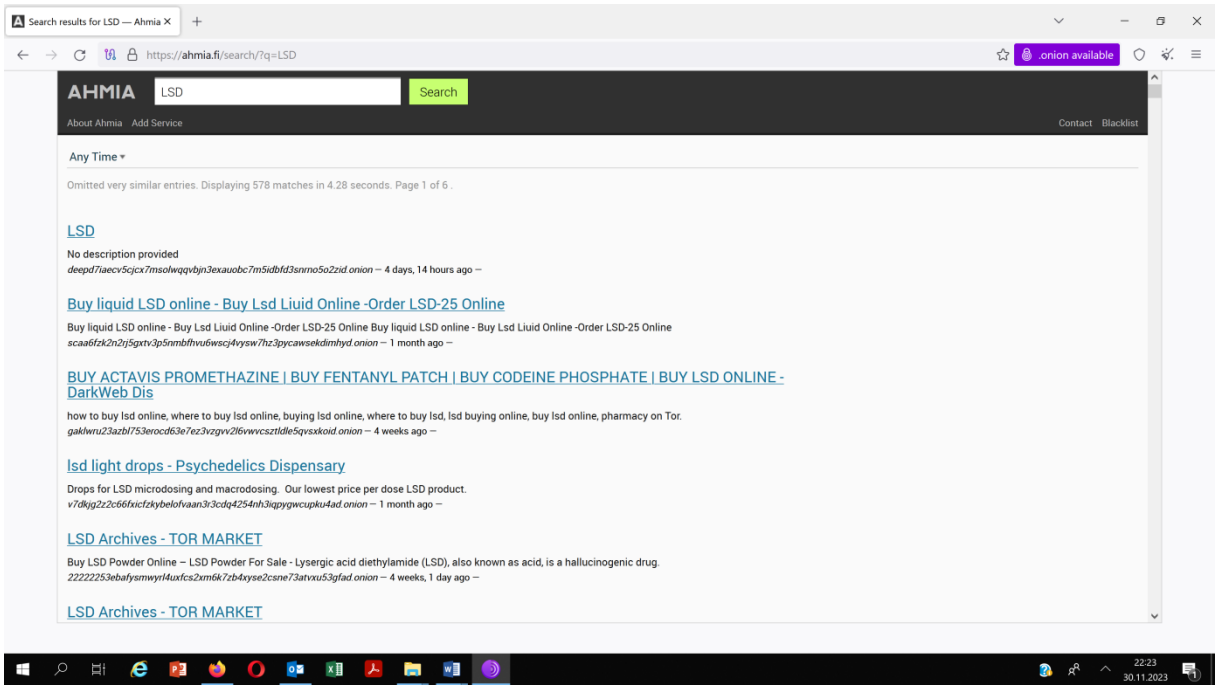
Ahmia poskytuje čisté a snadno použitelné rozhraní, které je podobné běžným vyhledávačům, což usnadňuje uživatelům procházení skrytého internetu. Ahmia je vyvíjen a podporován komunitou, která podporuje svobodu informací a anonymitu na internetu.

Je tedy zřejmé, že po jednoduchém nainstalování Toru, na které jsou hojně dostupné návody na běžném internetu, včetně různých youtuberů, a znalosti existence Ahmia, bez nutnosti znát přímo link, je velmi snadné proklikat se k prodejcům nelegálních /tvrdých/ drog.

Obrázek 3: Ahmia vyhledávač, titulní strana[55]



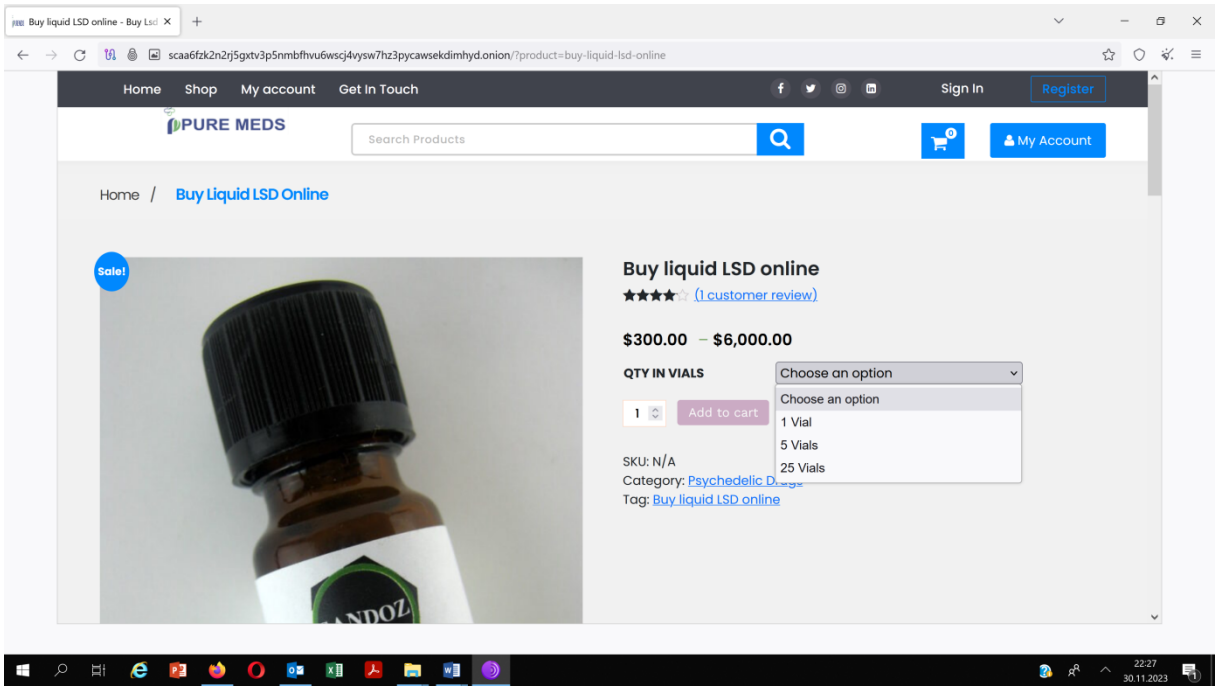
Obrázek 4: Výsledky vyhledávání klíčového slova na vyhledávači Ahmia[56]



[55] Vlastní zdroj
[56] Vlastní zdroj

Po rozkliknutí namátkově druhého linku se zobrazí eshop prodejce s názvem Pure meds a konkrétně odkaz na LSD v kapalné podobě (jak ukazuje printscreen obrázek 5). Tu lze zakoupit v různých objemech za cenu od 300 dolarů za jednu lahvičku, po šest tisíc dolarů za lahviček 25, které lze tedy nakoupit s množstevní slevou, a jsou určené velkoodběratelům. Do eshopu je potřeba se před nákupem zaregistrovat a vytvořit si tak uživatelský účet. To vyžadují všechny podobné eshopy. Dále se pak obchod chová jako klasický eshop. Na printscreenu můžeme dokonce spatřit jednu uživatelskou recenzi. Po objednání můžeme sledovat stav zboží, od přípravy po odeslání na zvolenou adresu.

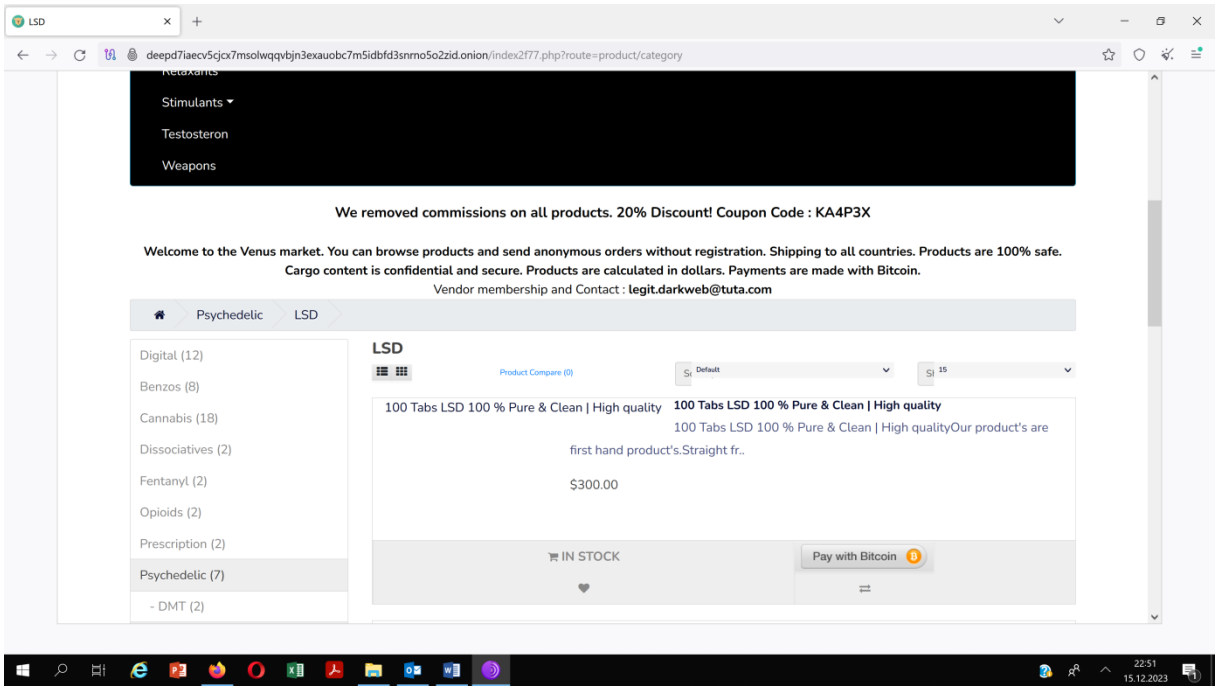
Obrázek 5: Nákup LSD online [57]



[57] Vlastní zdroj

Na obrázku 6 je příklad eshopu pod prvním Ahmia odkazem, kde není nutné ani vytvářet registraci a prodejce nabízí aktuálně 20% slevu po zadání kódu. V případě vytváření registrací se používají emaily na darknetu, kde je rovněž výběr z několika poskytovatelů.

Obrázek 6: Slevy na drogy na darknetu [58]



[58] Vlastní zdroj

10 Fóra na darknetu

Dark web fórum (DWF) je platforma, kde členové mohou svobodně diskutovat o nelegální činnosti. Tyto kriminální aktivity často zahrnují prodej osobních identifikačních informací (PII), nelegálního zboží nebo drog; korporátní špionáž; plány fyzického násilí; zranitelnosti a sady pro phishing; a dokonce obchodování s lidmi nebo dětskou pornografií. Dark web fóra mohou být také místem dark web tržišť pro transakce nelegálních nebo nezákonných akcí.

Provozovatelé kryptomarketů často nabízejí uživatelům (jak prodávajícím, tak kupujícím) diskusní fóra. Tato fóra zahrnují většinu témat souvisejících se zbožím a službami obchodovanými na kryptomarktech. Fórum je však obvykle věnováno drogám a zahrnuje vlákna vytvořená prodejci, kteří propagují své zásoby a komunikují se zákazníky. Existují také fóra, která nejsou spojena s určitým kryptomarketem, ale nabízejí obchodní sekci uvnitř fóra. Tato fóra často nemají nástroje běžné pro funkčnost kryptomarketů, jako jsou standardizované hodnotící systémy, služby escrow a lístky podpory. V důsledku toho jsou taková fóra ještě více závislá na vláknech prodejců (např. pro reklamu prodeje na straně prodejců a zveřejňování recenzí nebo hodnocení na straně kupujících) a na účasti správců a moderátorů (např. údržba fóra a reagování na požadavky uživatelů)[59].

Některá fóra jsou nicméně obecná. Podobně jako fóra ve stylu Redditu, dark web fóra obvykle sestávají z řady podsajtů pro konkrétní témata. Jedná se většinou o málo moderované komunity s mezinárodními předplatiteli nebo účty. Orgány činné v trestním řízení se mohou pokusit monitorovat tato fóra, ale často nedokážou stíhat obrovské množství informací, které jsou na nich denně zveřejňovány.

Úrovně členství a systémy důvěry jsou základními prvky online darknetových komunit. Tyto systémy jsou navrženy tak, aby budovaly důvěru, zajišťovaly bezpečnost a rozlišovaly mezi uživateli na základě jejich účasti a historie na konkrétní platformě. Mnoho fór, ale i tržišť na darkwebu má různé úrovně členství, z nichž každá nabízí odlišná privilegia. Čím vyšší úroveň, tím více přístupu a důvěry uživatel má. Tyto úrovně

[59] KAMPHAUSEN, Gerrit; WERSE, Bernd. *Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums*. International Journal of Drug Policy, 2019, vol. 73, no. 1, s. 281-287. ISSN: 0955-3959.

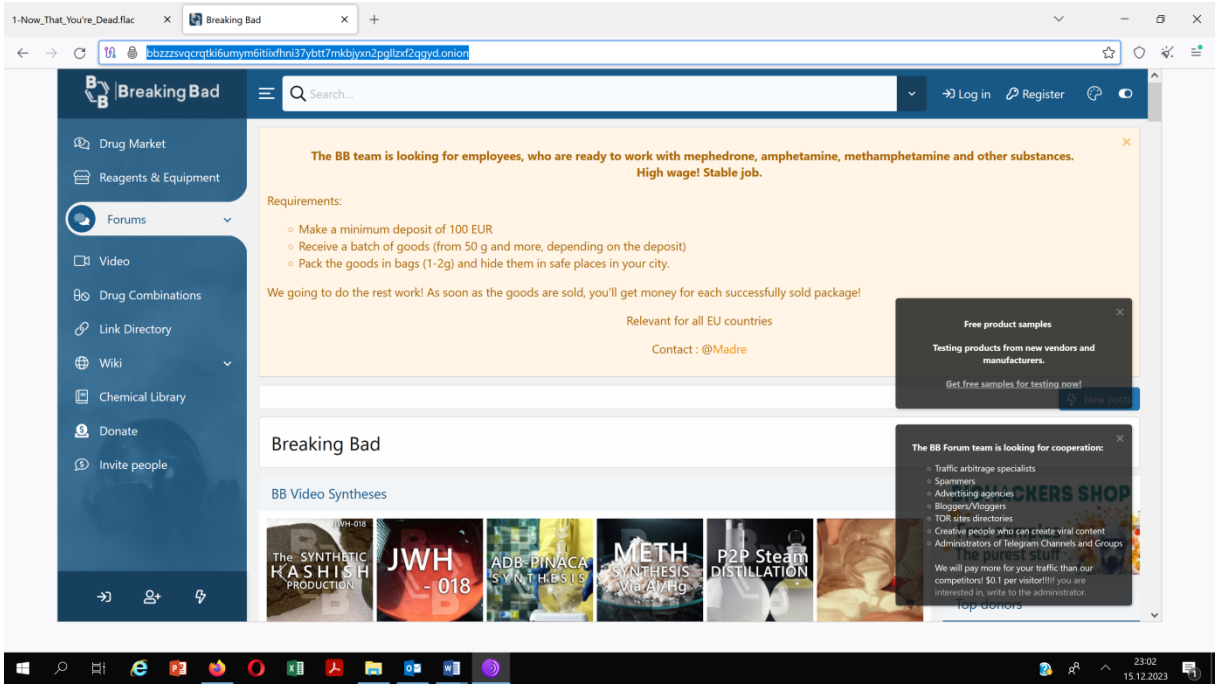
mohou sahat od základních členů po pokročilé uživatele, moderátory a administrátory. Důvěra může být získána pozitivními interakcemi, příspěvky a dodržováním pokynů komunity. Některé platformy implementují systémy reputace, kde si uživatelé mohou vzájemně hodnotit a recenzovat na základě svých interakcí. Tento zpětnovazební mechanismus pomáhá budovat důvěru a umožňuje ostatním uživatelům posoudit spolehlivost konkrétního jednotlivce před zapojením do transakcí nebo diskusí.

Moderátoři darkwebových fór jsou jedinci zodpovědní za udržování pořádku, prosazování pravidel a řízení diskusí na skrytých nebo anonymních online fórech, které se běžně nacházejí na dark webu. Moderátoři jsou obvykle vybíráni administrátory fóra nebo stávajícími moderátory. Mohou mít zkušenosti s tématy diskutovanými na fóru, jako je hacking nebo kyberzločin. Někteří mohou pracovat jako dobrovolníci, zatímco jiní mohou být různými způsoby odměňováni. Moderátoři darkwebových fór provádějí různé úkoly, jako je:

- **Prosazování pravidel**: Darkwebová fóra mají pravidla a pokyny, ačkoli se mohou lišit od tradičních internetových fór. Moderátoři tato pravidla prosazují monitorováním diskusí, odstraňováním nevhodného obsahu, zákazem rušivých uživatelů a podnikáním kroků proti těm, kteří porušují politiky fóra.
- **Monitorování obsahu**: Moderátoři aktivně sledují diskuse na fóru pro jakýkoli obsah, který porušuje pravidla fóra nebo zákon. To zahrnuje nelegální prodeje, explicitní obsah, hrozby nebo jakoukoliv aktivitu, která by mohla přitáhnout nechtěnou pozornost orgánů činných v trestním řízení.
- **Komunikace**: Moderátoři mají často komunikační kanály s ostatními moderátory a administrátory. Diskutují o problémech, koordinují akce a sdílejí informace o problematických uživatelích nebo potenciálních hrozbách pro bezpečnost fóra.
- **Balancování**: Moderátoři musí najít tenkou hranici mezi udržováním pořádku a umožněním pokračování diskusí. Snaží se zabránit tomu, aby se fórum stalo centrem nelegální aktivity, která by mohla přitáhnout pozornost orgánů činných v trestním řízení, zároveň udržují prostředí, kde se uživatelé cítí, že mohou diskutovat o svých zájmech.
- **Bezpečnostní opatření**: Aby chránili svou anonymitu, moderátoři často používají šifrování, anonymní metody komunikace a přijímají další opatření k ochraně své identity.

Níže přikládáme ukázku jednoho ze známých darknetových fór Breaking Bed. Jedná se o platformu o drogách a chemikáliích, kde se můžeme naučit metody výroby drog doma. Obsahuje také seznamy dodávek, které si člověk může koupit, aby si založil laboratoř u sebe doma. Jak ukazuje obrázek 7, aktuálně jsou na fóru i nabídky brigád v oblasti distribuce drog.

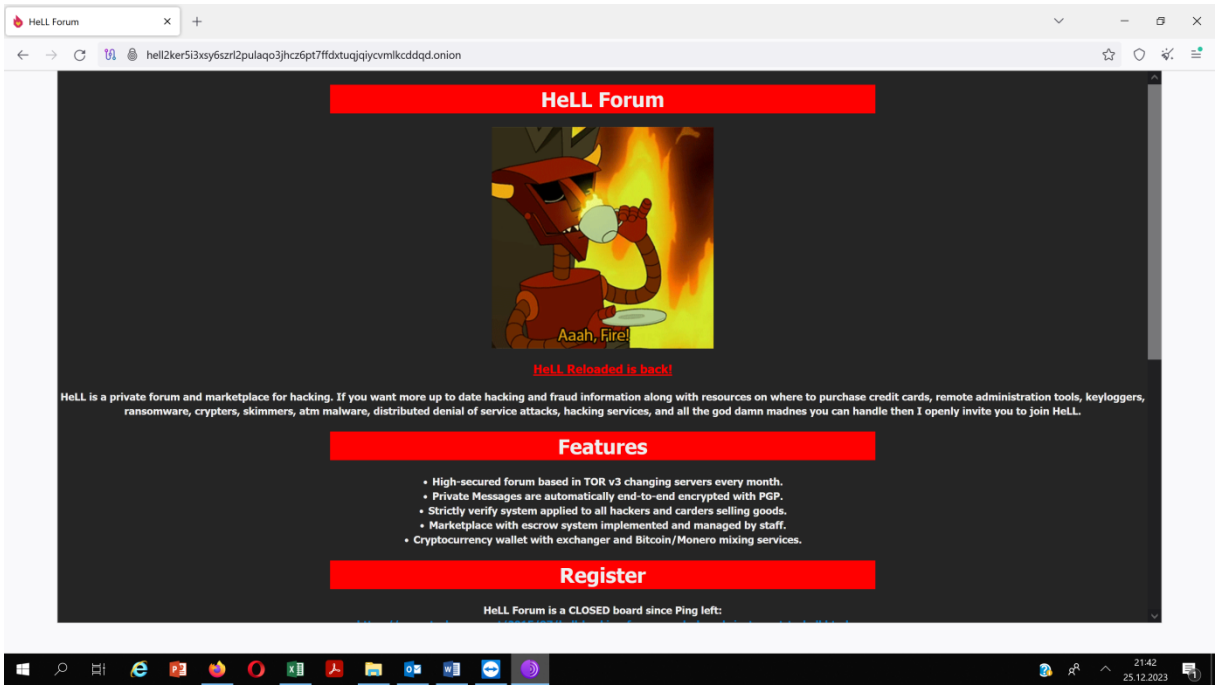
Obrázek 7: Ukázka fóra o drogách Breaking Bad na darknetu [60]



Mezi další známá fóra patří **XSS[.]is**. Jedná se o převážně ruské fórum s velkou komunitou zemí SNS. Je známé jako hackerská komunita, jejíž členové ovládají širokou škálu škodlivých nástrojů, technik hackingu, brokeringu počátečního přístupu, exfiltrace dat, ransomwaru atd. Jedná se o jednu z nejrespektovanějších platforem v podzemní hackerské scéně. Podobnou roli splňují i některá placená fóra jako například Hell, viz obrázek níže.

[60] Vlastní zdroj

Obrázek 8: Ukázka fóra s placeným přístupem zaměřeného na hacking na darknetu [61]



[61] Vlastní zdroj

11 Darknet a prodej dalšího ilegálního zboží a služeb

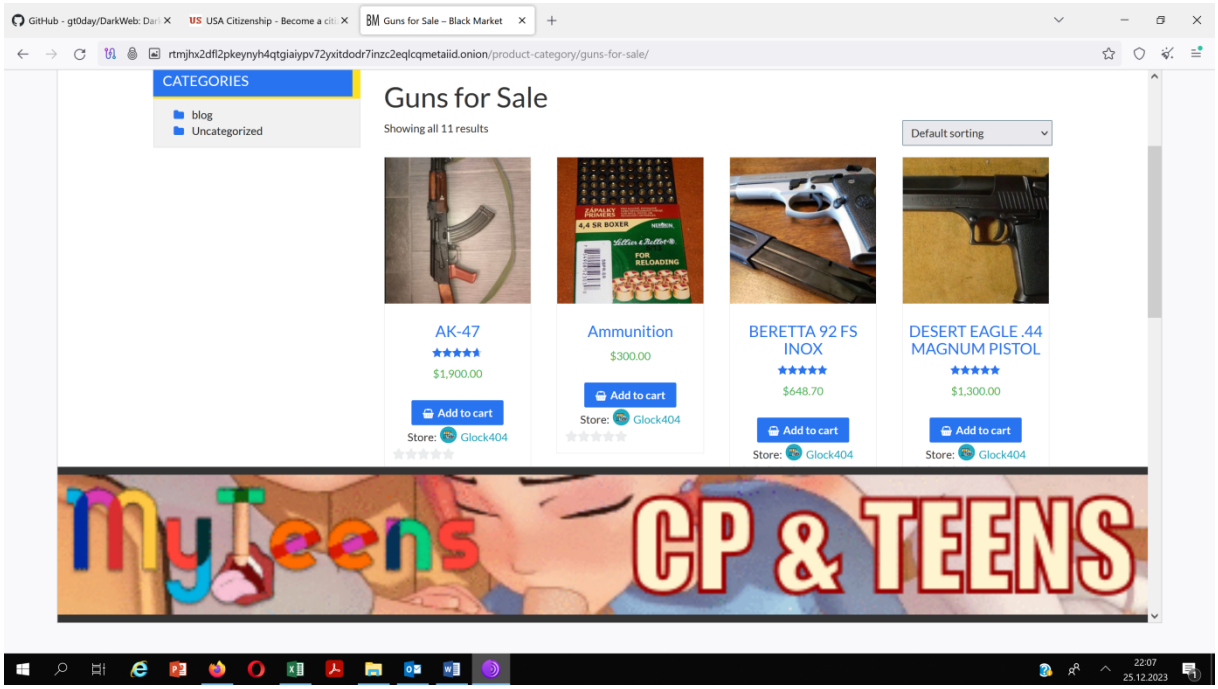
Pro příklad jsme vyhledali několik dalších objektů, které se (vedle drog) nabízí na darknetu.

11.1 Zbraně

Darkweb je známým prostředníkem pro oběh nelegálních zbraní, které jsou již na černém trhu, stejně jako potenciálním zdrojem odvedení legálně držených zbraní. Dark web zvyšuje dostupnost lepších, modernějších zbraní za stejnou nebo nižší cenu, než by bylo možné na ulici na černém trhu. Jak zjistil průzkum Paoli et al. (2018), USA se zdají být nejčastější zdrojovou zemí pro zbraně, které jsou na prodej na darkwebu. Téměř 60 % seznamů zbraní souvisí s produkty, které pocházejí z USA. Následuje výběr evropských zemí, které tvoří přibližně 25 %, zatímco nespecifikovaná místa původu tvoří přibližně 12 %. Evropa však představuje největší trh s obchodem se zbraněmi na darkwebu enerující příjmy, které jsou asi pětkrát vyšší než v USA. Seznamy zbraní (42 %) byly nejčastějšími seznamy na darkwebu, následované digitálními produkty souvisejícími se zbraněmi (27 %) a dalšími, včetně munice (22 %). Pistole byly nejčastěji uváděnou zbraní (84 %), následované puškami (10 %) a samopaly (6 %). V darknetových fórech se dále můžeme dočíst návody, které poskytují tutoriály pro širokou škálu nelegálních akcí, od přeměny replik/ poplašných zbraní na ostré zbraně, po kompletní výrobu domácích zbraní a výbušnin, a také zahrnují modely, které lze přeměnit na plně funkční zbraně pomocí 3D tisku. Celková hodnota obchodu se zbraněmi na darkwebu na základě 12 analyzovaných kryptotržišť ve studii se odhaduje na 80 000 dolarů měsíčně, přičemž zbraně generují téměř 90 % veškerých příjmů. Kvůli obchodu se zbraněmi na darkwebu by každý měsíc mohlo být až 136 nevysledovaných zbraní nebo souvisejících produktů ve skutečném světě. Odhady hodnoty a objemu obchodu se zbraněmi na darkwebu mohou zahrnovat určité procento falešných nabídek nebo transakcí, zejména mezi prodejci zbraní. Nicméně, je obtížné zjistit rozsah podvodů na darkwebu obecně a objevuje se vedle zbraní i ve všech dalších oblastech prodeje zboží a nabídky služeb.

Obrázek níže je ukázkou prodeje zbraní. Jedná se o „typického prodejce“ s nabídkou jedenácti různých zbraní. Větší obchody o větším počtu stejného zboží nejsou příliš časté. Nalezli jsme nabídku i různé munice, ale také třeba protiletadlové střely.

Obrázek 9: Nabídka zbraní na darknetu [62]



Pozn. v dolní části je k povšimnutí banerová reklama na pornografické obsahy (i na darknetu se reklamě nevyhneme)

Darkweb má potenciál stát se preferovanou platformou pro jednotlivce (např. osamocené teroristy) nebo malé skupiny (např. gangy) k získání zbraní a munice za anonymitní clonou. Kromě toho by mohl být darkweb využit psychiatrickými jednotlivci k nákupu zbraní a jejich zneužití k vraždě či sebevraždě.

[62] Vlastní zdroj

11.2 Kradená a padělaná identita

Osobní informace jednotlivce mohou mít na darkwebu hodnotu více než 1 000 dolarů v důsledku nárůstu kybernetické kriminality a krádeže identity. Studie Dark Web Price Index od Privacy Affairs[63], která shromažďovala data z darkwebových tržišť, fór a webových stránek, zjistila, že přihlašovací údaje k online bankovnictví, informace o kreditních kartách a přihlašovací údaje k sociálním médiím lze zakoupit online za šokující nízké ceny:

- Přihlašovací informace k online bankovnictví stojí v průměru 100 dolarů
- Úplné informace o kreditní kartě a související data stojí mezi 10 a 100 dolary
- Kompletní sadu dokumentů a informací o účtu, která umožní krádež identity, lze zakoupit za přibližně 1 000 dolarů

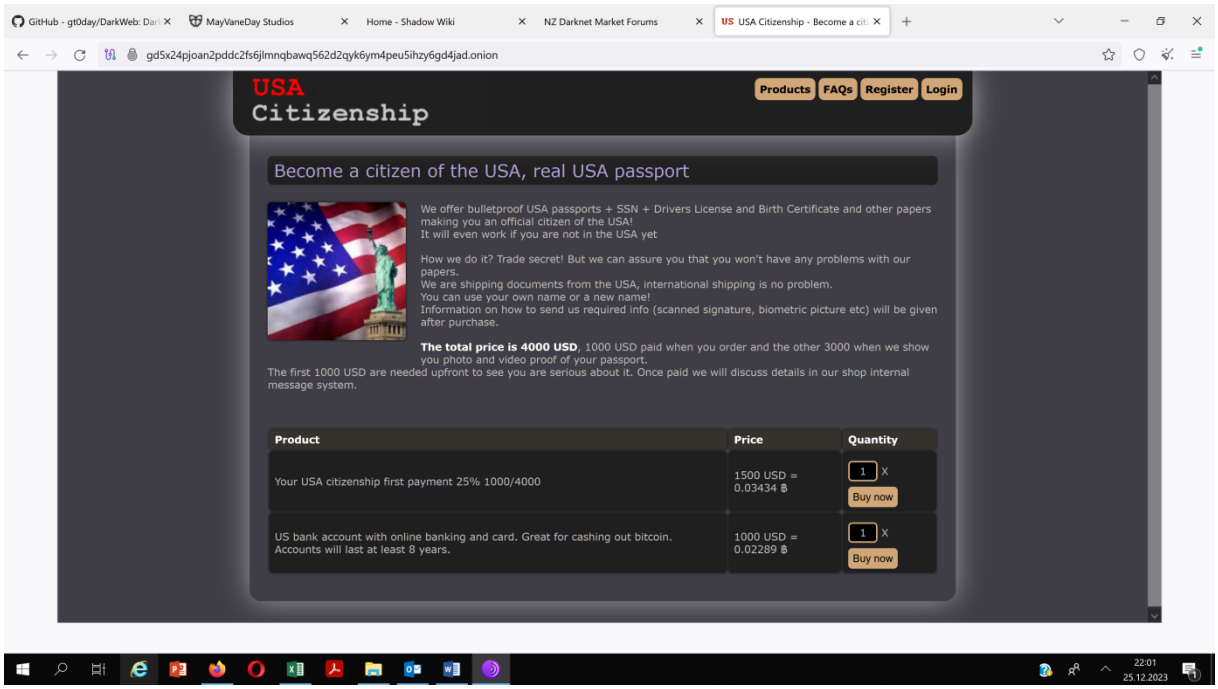
Studie uvedla, že ukradené údaje o kreditní kartě jsou obvykle formátovány jako jednoduchý kód, který zahrnuje číslo karty, datum expirace a CVV, stejně jako údaje o držiteli účtu, jako je adresa, e-mailová adresa a telefonní číslo.

Za přibližně 1 000 dolarů mohou zločinci získat dostatek dokumentace, aby úspěšně ukradli identitu osoby.

Padělané dokumenty, jako jsou řidičské průkazy, pasy a pojistné karty, lze objednat tak, aby odpovídaly ukradeným informacím, tak jak ukazuje naše ukázka, kde lze zakoupit USA cestovní mas za 4000 amerických dolarů. Následně lze dokoupit i bankovní účet včetně platební karty k této nově získané identitě.

[63] SMITH, Ryan. *Revealed: how much is personal information worth on the dark web* [online]. 2022. Dostupné z: https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx. [citováno 2023-09-04].

Obrázek 10: Nabídka padělaných cestovních pasů a bankovní identity na darknetu[64]

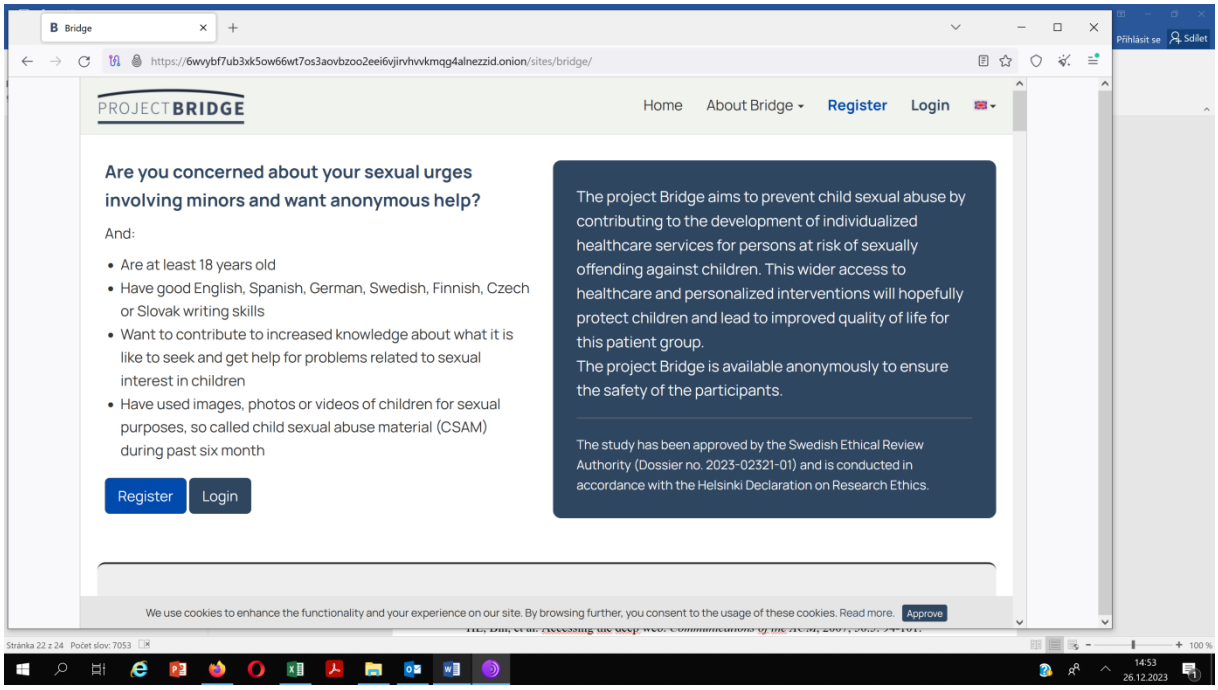


[64] Vlastní zdroj

11.3 Dětská pornografie

Dětská pornografie byla odjakživa s darknetem spojována. Aktuálně dochází k tomu, že při snaze vyhledat stránky s takovýmto materiálem na klasických darknetových vyhledávačích neuspějeme. Naopak – budeme přesměrováni na stránky, které nabízejí odbornou pomoc osobám s pedofilními sklony, viz obrázek níže.

Obrázek 11: odborná pomoc, na kterou je uživatel vyhledávající dětskou pornografii přesměrován [65]



Data z odborných zdrojů ale hovoří jinak. V nedávné době mezinárodní policejní orgány zaznamenaly nárůst využívání darknetu jednotlivci za účelem zapojení se do tématu CSEA (zneužívání dětí pro sexuální účely) a souvisejícího materiálu[66]. Citovaný zdroj z Europolu uvedl, že jak počet dark web fór věnovaných pedofilii a CSEA, tak i objem materiálu, který se na nich vyměňuje, rostl. Spolu s nárůstem frekvence se obsah zobrazovaný v materiálu CSEA stává stále extrémnějším a násilnějším. Členství na dark web fórech věnovaných CSEA není nevýznamné. Web-Iq[67] uvedl, že na sedmi takových fórech, které indexovali, bylo více než dva miliony jedinečných uživatelských ID. I když

[65] Vlastní zdroj

[66] Europol (2020) *Internet Organised Crime Threat Assessment (IOCTA).* The Hague: Europol. [online]. Dostupné z: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020. [citováno 2024-04-01].

[67] Web-Iq. *Web-IQ newsletter.* Amsterdam: Web-IQ, 2018.

se někteří uživatelé registrují na více fórech, odhaduje se, že tento počet odpovídá mezi 300 000 a 1 milionu uživatelů napříč sedmi fóry.

Došlo tedy pravděpodobně k tomu, že se dříve běžně vyhledatelná dětská pornografie přesunula do adres distribuovaných pouze ve specializovaných fórech.

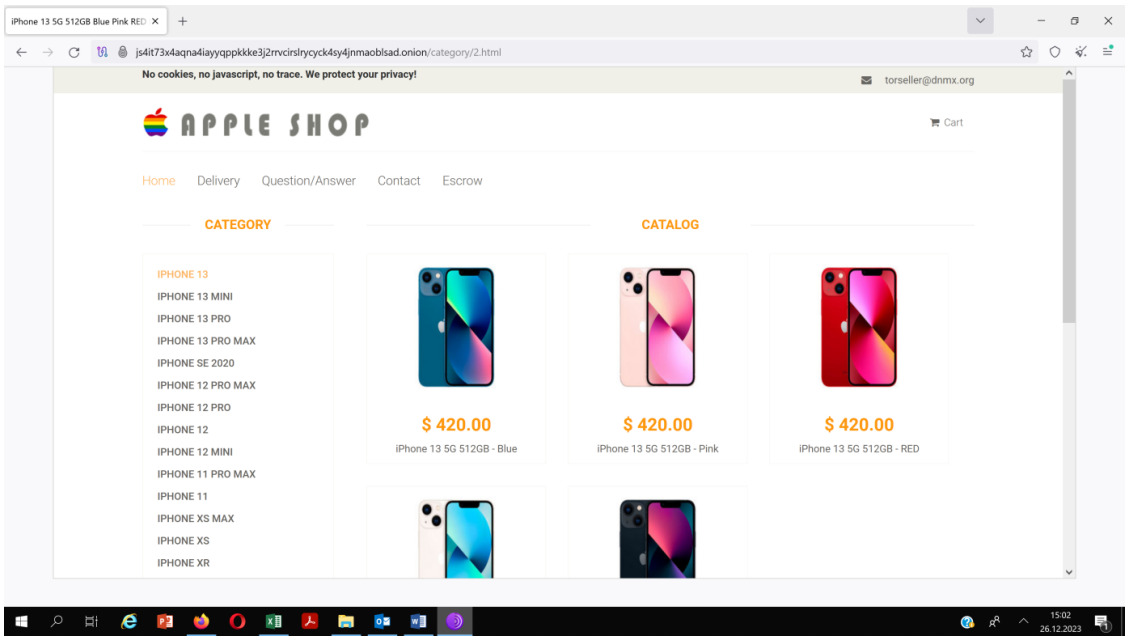
11.4 Elektronika

Prodej elektroniky, zvláště mobilních telefonů, na darknetu je součástí širšího trhu s nelegálním zbožím a službami, se kterými se obchoduje na těchto částech internetu.

Často jsou na darknetu prodávány kradené nebo zablokované telefony. Tyto telefony mohou být někdy "odblokovány" nebo "odemykány" pro další použití, ale často jsou prodávány tak jak jsou, ovšem za velmi nízké ceny. Falšované nebo replikované modely populárních značek jako Apple nebo Samsung jsou také běžné. Tyto telefony mohou vypadat téměř identicky jako skutečné, ale často mají nižší kvalitu. Některé telefony jsou prodávány s předinstalovaným softwarem pro zvýšení anonymity a bezpečnosti, často zaměřené na zákazníky, kteří chtějí zůstat v utajení. Z našich zkušeností je nejčastěji nabízená značka Apple. Od této značky se dají na darknetu sehnat nejen mobilní telefony (viz obrázek 12), ale i sluchátka, tablety či počítače.

Specialitou jsou nabízená zařízení, která ruší signály mobilních telefonů, GPS a další komunikaci a zařízení schopná kopírovat bezpečnostní informace z RFID čipů, jako jsou ty v platebních kartách nebo identifikačních průkazech.

Obrázek 12: Nabídka apple výrobků na darknetu [68]

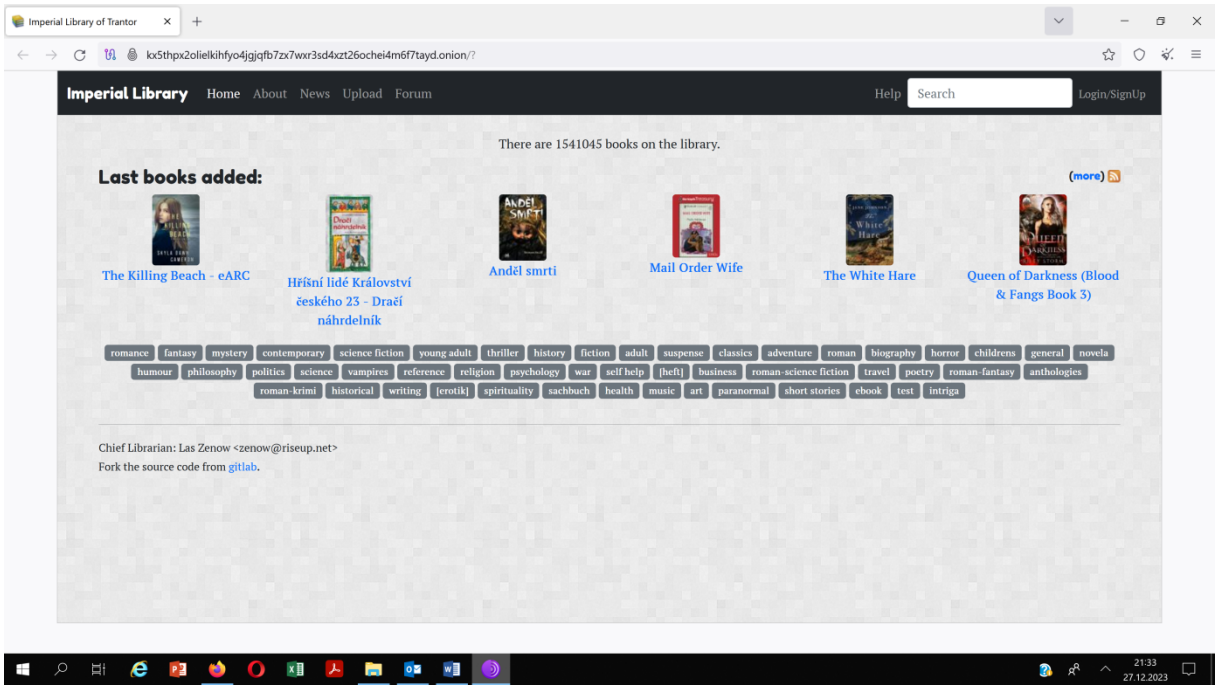


[68] Vlastní zdroj

11.5 „Pozitivní“ části darknetové nabídky

V některých zemích je přístup k vědeckým článkům, knihám a dalším edukačním materiálům omezen. Darknet může poskytovat přístup k těmto materiálům, což umožňuje vzdělávání a šíření informací. K tomuto lze využít pestrou nabídku stránek, kde mezi nejznámější patří Imperial Library. Ta obsahuje přes milion a půl knižních titulů ke stažení a to i v českém jazyce, viz obrázek 13.

Obrázek 13: Imperial library – nabídka knih na darknetu[69]



Podobně Sci-Hub, původně darknetový nástroj, který je aktuálně, byť s různými výpadky dostupný i na klasickém internetu, poskytuje bezplatný přístup k vědeckým pracím, s miliony dokumentů. Vědecké časopisy často umisťují své články za placenou zeď nebo účtují vysoké poplatky za přístup, ale Sci-Hub nabízí otevřený přístup k čtení nebo stahování výzkumných prací. V mnoha zemích je technicky nelegální, protože porušuje autorská práva.

ProPublica je nezisková, Pulitzerovou cenou oceněná zpravodajská organizace, která se zaměřuje na zneužívání moci a otázky veřejné důvěry. Investigativní žurnalistika ProPublicy z nich činí terč mocných, proto se připojili k dark webu, aby jejich novinářům a čtenářům pomohli přistupovat k jejich obsahu a vyhnout se sledování. Být

[69] Vlastní zdroj

na darkwebu také umožňuje whistleblowerům posílat materiál ProPublice bez obavy z odvetných opatření.

BBC a další známé zpravodajské služby jsou v některých částech světa blokovány. Lidé však stále mohou přistupovat k nezávislým médiím prostřednictvím BBC Tor Mirror a podobných portálů zpráv na dark webu. BBC Tor Mirror je mezinárodní verze BBC, která se zaměřuje na světové události, a je nesmírně užitečná pro ty, kteří žijí pod přísnými zákony o cenzuře.

Na darknetu lze rovněž využít běžné sociální sítě jako je Facebook, což může být přínosné opět pro občany těch zemí, kde je klasický Facebook zakázán a blokován.

Všechny výše uvedené stránky nalezneme klasicky přes prohlížeče uvedené v úvodu praktické části.

12 Podvody na darknetu

Pokud se uživatel rozhodne nakupovat na darknetu, může se setkat s řadou podvodů. Je důležité si uvědomit, že kvůli anonymní a nelegální povaze mnoha transakcí na darknetu je zde vyšší riziko podvodů než na běžném internetu. Zde jsou některé z nejběžnějších podvodů, na které mohou uživatelé darknetu narazit:

1. **Falešní obchodníci a prodejci**: Někteří prodejci mohou vypadat důvěryhodně, ale ve skutečnosti nemají v úmyslu dodat zboží. Po obdržení platby jednoduše přestanou komunikovat. Prodejce může také požadovat předplacení za zboží nebo služby, které nikdy neplánuje dodat.
2. **Podvody s escrow službami**: Escrow služby na darknetu by měly být způsobem, jak chránit kupujícího i prodejce, ale některé z těchto služeb jsou samy podvodné a uživatele mohou připravit o peníze.
3. **Podvržené nebo škodlivé produkty**: I když uživatel obdrží produkt, může se jednat o nekvalitní nebo dokonce škodlivé napodobeniny. Toto je obzvláště nebezpečné v případě, že se jedná o léky nebo jiné citlivé materiály.
4. **Phishingové útoky a malware**: Uživatelé mohou narazit na stránky nebo prodejce, kteří se snaží získat osobní informace, jako jsou hesla nebo bankovní údaje, prostřednictvím falešných stránek nebo škodlivého softwaru. Dočetli jsme se ve fóru i případy, kdy bylo přislíbeno zajistit hackerský útok na ex partnerku klienta, ale nakonec tento klient se stal útokem hackera a musel zaplatit navíc za službu, že mu hacker nesmaže data v počítači.
5. **Podvody s kryptoměnami**: Vzhledem k tomu, že transakce na darknetu jsou obvykle prováděny v kryptoměnách, existují podvody, jako jsou falešné směnárny nebo investiční schémata, které slibují vysoké výnosy.
6. **„Red rooms"** jsou předmětem mnoha mýtů a legend na internetu. Jsou popsány jako tajné online místnosti na darknetu, kde diváci mohou za úplatu sledovat, a někdy i diktovat, mučení nebo vraždu v reálném čase. Ačkoli je obtížné ověřit věrohodnost většiny příběhů o red rooms, rozsáhlý konsenzus mezi experty na kyberbezpečnost a právních odbornících je, že většina těchto příběhů jsou podvody. Skutečné důkazy o existenci red rooms jsou minimální nebo neexistují, a mnoho takzvaných red rooms se ukázalo být podvody, které si cílí vylákat peníze od zvědavých nebo naivních uživatelů. Najít red room na darknetu není podle našich zkušeností zas tak obtížné, uživatel musí

pro vstup zaplatit poměrně vysokou částku (podle míry zapojení se v red roomu se jedná v přepočtu o desítky až sta tisíc korun) a výsledek je nejistý. Stránky po určité době zmizí a otázkou je, zda proto, že se jednalo o podvod nebo že skutečně nějaký red room proběhl. S přihlédnutím k diskusním fórům se spíše jedná o první variantu.

7. **Nájemní vrazi**: Podobně jako v případě red rooms, existují i stránky na darknetu, které tvrdí, že nabízejí služby nájemných vrahů. Tyto stránky často slibují, že dokážou za peníze organizovat vraždy nebo jiné těžké zločiny. Je však třeba mít na paměti, že mnoho, pokud ne většina, těchto stránek je široce považováno za podvody. Některé z nich byly dokonce odhaleny jako pasti provozované vymáhacími orgány k chycení lidí, kteří se pokoušejí najmout vraha. Z našich zkušeností opět není problém stránky nalézt, ačkoli je zakazují provozovatelé tržišť ve většině případů. Částky za domnělou vraždu se pohybují řádově ve stovkách tisíc korun.

13 Návrh opatření omezení dostupnosti darknetu

Omezení nebo ztížení přístupu na darknet je komplexní výzvou, která vyžaduje koordinované úsilí na několika frontách, včetně technologických, legislativních a vzdělávacích iniciativ.

V rámci technologických opatření bychom zdůraznili rozvoj a implementace sofistikovanějších sledovacích technologií, které mohou efektivněji detekovat a monitorovat darknetový provoz. Je rovněž možné (spolu)pracovat s ISP (poskytovateli internetových služeb) na identifikaci a blokování přístupu k darknetovým sítím. V neposlední řadě je možná implementace bezpečnostních protokolů, které by omezovaly nebo kontrolovaly přístup k darknetovým aplikacím a službám. Podstatné je také poskytnutí rozšířeného školení pro policisty v oblasti technologií a metod používaných na darknetu, včetně rozšíření počtu policejních specialistů kteří se této problematice věnují. Orgány činné v trestním řízení společně s výzkumníky byly v průběhu let úspěšné ve zrušení celé řady darknetových tržišť a rozbití sítí dealerů a provozovatelů.

V rámci legislativních opatření je možné vytvoření nebo zpřísnění legislativy, která se zaměřuje na používání anonymizačních nástrojů a sítí jako Tor v závislosti na regionálních a národních právních rámcích. Nezbytné je také posílení mezinárodní spolupráce v boji proti kyberkriminalitě spojené s darknetem. Kybernetická bezpečnost je složitá a dynamická oblast, a různé země mají své vlastní zákony a předpisy. **Budapešťská úmluva o kyberkriminalitě (**Úmluva Rady Evropy o kyberkriminalitě), je prvním mezinárodním smluvním nástrojem zaměřeným na kyberkriminalitu. Úmluva se snaží usnadnit mezinárodní spolupráci a harmonizaci zákonů v oblasti kyberkriminality.

Součástí budou i investice do kybernetické obrany a bezpečnostních technologií pro detekci a obranu proti hrozbám vycházejícím z darknetu a podpora výzkumu a vývoje v oblasti kybernetické bezpečnosti.

Jiný pohled pak může pracovat na posílení odpovědnosti uživatelů darknetu a to vytvořením mechanismů, které by zvýšily odpovědnost uživatelů za používání darknetu, včetně možných právních důsledků pro nezákonné aktivity. V rámci tohoto pohledu zabránění lidem ve snadném stahování a používání Toru (což se jeví na první pohled jako nejsnazší a nejúčinnější řešení) není praktické a ani eticky vhodné. Tor je nástroj, který

byl původně vyvinut k poskytování online anonymity a soukromí, a má mnoho legitimních použití. Namísto snahy o zamezení přístupu k Toru je lepší se zaměřit na vzdělávání veřejnosti o bezpečném a zodpovědném používání internetu, včetně nástrojů jako Tor. Je důležité si uvědomit, že omezování přístupu k nástrojům jako je Tor by mohlo mít negativní dopady na svobodu projevu a právo na soukromí. Proto je vhodnější se soustředit na osvětu a zvýšení povědomí o bezpečnosti a etice v kyberprostoru.

Vstupní zabezpečení pro osoby mladší 18 let na darknet je úplně stejně obtížné. Navíc je potřeba vzdělávání, poučit mládež o možných rizicích a důsledcích používání darknetu. Vhodné je také použít pokročilé rodičovské kontrolní nástroje na všech zařízeních, která mladiství používají. Nastavit filtry, které blokují přístup k známým nástrojům pro anonymní procházení, jako je Tor nebo I2P. Rodiče by měli monitorovat online aktivity svých dětí, včetně historie procházení, aplikací a komunikace. To by mělo být provedeno s respektem k soukromí dítěte a s důrazem na otevřenou a důvěrnou komunikaci. Je důležité si uvědomit, že žádné technické nebo vzdělávací řešení nemůže být 100% účinné a nejlepší obrana vždy zahrnuje kombinaci monitorování, vzdělávání a otevřené komunikace mezi rodiči a dětmi. Ochrana mladistvých na internetu vyžaduje neustálou pozornost a přizpůsobení se novým výzvám a technologiím.

Závěrem bychom rádi poznamenali, že jakékoli omezení přístupu na darknet by mělo být vyváženo respektem k právům na soukromí a svobodu projevu, protože ač my bereme darknet z kriminologického a patologického pohledu, pro mnoho lidí především pak v zemích s totalitním režimem, se jedná o jednu z mála cest k sebevyjádření, získání informací, ale také například léků nutných k řešení zdravotních problémů.

Závěr

V této práci byl prozkoumán složitý a často nejasný svět darknetu a jeho vztah k kyberkriminalitě. Přestože darknet nabízí anonymitu a může být využit pro legální účely, jako je ochrana soukromí a svobody projevu, jeho zneužití pro nelegální aktivity vyvolává vážné obavy. Vývoj v oblasti kyberkriminality, včetně nových forem sociálního inženýrství a ransomwaru, poukazuje na neustálou potřebu vzdělávání a prevence.

Dostat se na darknet může být relativně snadné pro kohokoli, kdo má základní pochopení pro používání internetu a stahování softwaru. Prostřednictvím nástrojů jako Tor Browser, který je navržen pro snadné použití, může být přístup k darknetu získán během několika minut. Tato snadnost přístupu však přináší značná rizika, zejména pro zranitelnější uživatele, jako jsou děti.

Pro děti, které jsou často zvídavé a mají tendenci experimentovat s technologiemi, může být relativně snadné dostat se na darknet, pokud narazí na správné informace nebo návody, které mnohdy poskytují oblíbení youtubeři a které jsou k dohledání velmi jednoduše na klasických internetových stránkách. Tato skutečnost může být znepokojivá pro rodiče a pedagogy, protože darknet hostí řadu nebezpečných a nelegálních aktivit, které jsou nevhodné a potenciálně škodlivé (pro mladé uživatele). Na druhou stranu zaplatit za službu či zboží na darknetu se jeví být pro tuto cílovou skupinu skoro nemožné, s ohledem na nutnost vlastnictví peněženky na kryptoměny, kryptoměn, atp.

Pozitivní zprávou je, že pro neznalé uživatele je značně obtížné dostat se aktuálně na darknetové stránky s dětským pornografickým materiálem, respektive obecně s jakoukoli nekonvenční pornografií. Pornografie je omezována i většinou marketů.

Závěrem bychom rádi zmínili, že je nezbytné, aby jednotlivci, organizace i státy pokračovaly ve společném úsilí o zvýšení kybernetické bezpečnosti a etiky v digitálním prostoru, a zároveň zachovávaly rovnováhu mezi bezpečností a svobodami.

Seznam použitých zdrojů

Literární zdroje

1. BYRNE, James M. a KIMBALL, Kathryn A. Inside the Darknet: techno-crime and criminal opportunity. In*: Criminal justice technology in the 21st century.* 2017. s. 206-232. ISBN: 978-0398091514
2. CRESWELL, John W. a CRESWELL, J. David. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017. ISBN: 978-1452226101.
3. GEHL, Robert W. *Weaving the dark web: Legitimacy on Freenet, Tor, and I2P*. MIT Press, 2018. ISBN 9780262038263.
4. HENDL, Jan. *Kvalitativní výzkum: základní metody a aplikace*. Praha: Portál, 2005. ISBN 80-7367-040-2.
5. OZKAYA, Erdal a ISLAM Rafiqual (2019). *Inside the dark web.* CRC Press. ISBN: 9780367260453.
6. STROUKAL, Dominik. *Dark Web: Sex, drogy a bitccoiny*. Praha: Grada Publishing, a.s., 2020. ISBN 978-80-271-2934-8.
7. THOWSEAF, S. a SATHISH Kumar. Cryptocurrency May Prove Financial Crime: A Conceptual Analysis. In: *Emerging Insights on the Relationship Between Cryptocurrencies and Decentralized Economic Models*. IGI Global, 2023. s. 110-121. ISBN: 9781668456910.
8. MARTIN, James; MUNKSGAARD, Rasmus; COOMBER, Ross; DEMANT, Jakob a BARRATT, Monica J. (2020). *Selling drugs on Darkweb cryptomarkets: Differentiated pathways, risk and rewards.* British Journal of Criminology, vol. 60, no. 3, s. 559-578. ISSN 0007-0955. Dostupné z: doi:10.1093/bjc/azz075.
9. IANSITI, Marco a Karim R. LAKHANI. *The Truth About Blockchain*. Harvard Business Review. 2017, vol. 95, no. 1, s. 118-127. ISSN: 0017-8012
10. HE, Bin, et al. *Accessing the deep web. Communications of the ACM*, 2007, vol. 50, no. 5, s. 94-101. ISSN: 0001-0782.
11. BRACCI, Alberto; NADINI, Matthieu; ALIAPOULIOS, Maxwell; McCOY, Damon; GRAY, Ian; TEYTELBOYM, Alexander; GALLO, Angela a BARONCHELLI, Andrea*. Dark web marketplaces and covid-19: before the vaccine.* EPJ Data Science. 2021, vol. 10, no. 1, s. 6. ISSN: 2193-1127.
12. KAMPHAUSEN, Gerrit; WERSE, Bernd. *Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums*. International Journal of Drug Policy, 2019, vol. 73, no. 1, s. 281-287. ISSN: 0955-3959
13. EVERETT, Cath. *Should the dark net be taken out?.* Network Security, 2015. vol. 2015, no. 3, s. 10-13. ISSN: 1353-4858. Dostupné z: https://doi.org/10.1016/S1353-4858(15)30018-0.
14. MACRINA, April a Eric PHETTEPLACE. The Tor browser and intellectual freedom in the digital age. *Reference and User Services Quarterly*. 2015, vol. 54, no. 4, s. 17-20. ISSN: 1094-9054.
15. OWEN, Gareth a SAVAGE, Nick. *The tor dark net.* Published by the Centre for International Governance Innovation and the Royal Institute of International Affairs. 2015. Bez ISBN.
16. NAKAMOTO, Satoshi. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* [online]. Dostupné z: https://bitcoin.org/bitcoin.pdf. [citováno 2024-04-01].

17. VOLEJNÍK, Robert. (2016). *Darknet – fikce či realita anonymity skrytých služeb Tora systému bitcoin*. Brno. Bakalářská diplomová práce. Masarykova univerzita. Vedoucí práce Mgr. Viktor Pantůček. Dostupné z: https://is.muni.cz/th/px96p/Darknet-fikce-ci-realitaanonymity-skrytych-sluzeb-Tor-a-systemu-bitcoin.pdf.

Elektronické zdroje

1. BBC News (2017). *'WannaCry ransomware cyber-attacks slow but fears remain'*. BBC News [online]. Dostupné z: https://www.bbc.com/news/technology-39920141 [citováno 2023-12-12].
2. AKCORA, Cuneyt Gurcan; GEL, Yulia R.; KANTARCIOGLU, Murat. *Blockchain networks: Data structures of bitcoin, monero, zcash, ethereum, ripple, and iota*. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2022, 12.1: e1436.
3. HARSH, Kumar, 2022. Darknet Market Brings Billions In Crypto World, Finds Study. In: Outlook India [online]. [cit. 2024-02-26]. Dostupné z: https://www.outlookindia.com/business/darknet-market-brings-billions-of-revenues-incrypto-world-finds-study-news-183428
4. CAESAR, Ed (2021). The Takedown of a Dark-Web Marketplace. The New Yorker. [online]. 2021. Dostupné z: https://www.newyorker.com/news/news-desk/the-takedown-of-a-dark-web-marketplace.
5. CATALINI, Christian a S. GANS Joshua. *Some Simple Economics of the Blockchain.* NBER Working Paper No. 22952. 2016. Cambridge, MA: National Bureau of Economic Research. Dostupné z: doi:10.3386/w22952.
6. Cisco. *Annual Internet Report (2018–2023).* White Paper. 2020. Cisco Systems, Inc.
7. Česko v datech. (n.d.). (2015). Odvrácená strana internetu: Český Darknet v číslech. [online]. Dostupné z: https://www.ceskovdatech.cz/clanek/28-odvracena-strana-internetu-cesky-darknet-v-cislech/. [citováno 2024-04-01].
8. ESET. (2023). *Trendy a výzvy v kyberbezpečnosti v roce 2023.* Digital Security Guide. [online]. Dostupné z: https://digitalsecurityguide.eset.com. [citováno 2024-04-01].
9. Europol (2020) *Internet Organised Crime Threat Assessment (IOCTA).* The Hague: Europol. [online]. Dostupné z: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020. [citováno 2024-04-01].
10. IdentityIQ. (n.d.). (2023). *The Origins and History of the Dark Web*. [online]. Dostupné z https://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/#:~:text=Early%202000s%20%E2%80%93%20Present%3A%20Tor%E2%80%99s,people%20began%20to%20take%20advantage. [citováno 2024-04-01].
11. ILIADIS, Lazaros Alexios a KAIFAS, Theodoros. Darknet traffic classification using machine learning techniques. In: *2021 10th international conference on modern circuits and systems technologies (MOCAST)*. IEEE, 2021. p. 1-4.
12. KASPERSKY, I. C. S. *Threat landscape for industrial automation systems. Statistics for H2*, 2021. [online] Dostupné z: https://ics-cert.kaspersky.com/publications/reports/2022/03/03/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2021/. [citováno 2024-04-01].
13. KOBIE, Nicole. What is the dark web? How to use Tor to access the dark web. In: *Wired* [online]. 2019. Dostupné z: https://www.wired.co.uk/article/what-is-the-dark-webhow-to-access. [citováno 2023-24-12].
14. KRATINA, Tomáš a PITSCHMANN, Vladimír. Dostupnost vybraných syntetických opioidů a analgetik na darknet markets. *New Approaches to State Security Assurance*, 2021, 108.

15. KRUITHOF, Kristy; ALDRIDGE, Judith; HÉTU Décary David; SIM Megan; DUJSO, Elma a HOORENS Stijn. *The role of the'dark web'in the trade of illicit drugs*. RAND, 2016. [online]. Dostupné z: https://www.rand.org/pubs/research_briefs/RB9925.html. [citováno 2023-24-12].
16. Kunovice. Bakalářská práce. Evropský polytechnický institut, s. r. o. Vedoucí práce Ng. René Nábělek.
17. LEWIS, M. (2018). *What Is the Dark Web – Who Uses It, Dangers & Precautions to Take* [online]. Dostupné z: https://www.moneycrashers.com/dark-web/. [citováno 2024-04-01].
18. MITRE. (2020). *Common Attack Pattern Enumeration and Classification.* MITRE Corporation. [online]. Dostupné z: https://r.search.yahoo.com/_ylt=AwrEoUIdWApmT.cOjphXNyoA;_ylu=Y29sbwNiZjEEcG9zAzMEdnRpZAMEc2VjA3Ny/RV=2/RE=1713163549/RO=10/RU=http%3a%2f%2fmsm.mitre.org%2fdocs%2fcapec-intro-handout.pdf/RK=2/RS=1GsG7BPTS0mWxMajKDQfKiWo2H8-. [citováno. 2024-04-01].
19. PAOLI Giacomo Persi; ALDRIDGE, Judith; RYAN, Nathan a WARNES, Richard. The sale of illegal weapons on the dark web and the impact on international security [online]. 2018. Dostupné z: https://www.weforum.org/agenda/2018/12/the-sale-of-illegal-weapons-on-the-dark-web-and-the-impact-on-international-security/. [citováno 2023-12-23].
20. Pixel Privacy. (2023). *The Ultimate 2023 Guide to The Tor Browser – Explained*. [online]. Dostupné z: https://pixelprivacy.com/resources/tor-browser-guide/#:~:text=How%20Does%20the%20Tor%20Browser,a%20USB%20stick%2C%20for%20example. [citováno 2023-12-23].
21. Policie České republiky. (2022). *"Vývoj registrované kriminality v roce 2022"*. [online]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx. [citováno 2023-12-23].
22. Policie České republiky. (2023). *"Statistické přehledy kriminality za rok 2023".* [online]. Dostupné z : www.policie.cz. [citováno 2023-12-23].
23. Prevence Kriminality. (2023). *Fenomén zvyšující se kybernetické kriminality byl hlavním tématem aktivit ke Dni bezpečnějšího internetu 2023.* [online]. Dostupné z: http://prevencekriminality.cz. [citováno 2023-12-23].
24. REDMAN, Jamie. Sources Say World's Largest Darknet Empire Market Exit Scammed, $30 Million in Bitcoin Stolen. In: *Bitcoin.com* [online] 2020. Dostupné z: https://news.bitcoin.com/sources-say-worlds-largest-darknet-empire-market-exit-scammed-30-million-in-bitcoin-stolen/. [citováno 2023-09-04].
25. SMITH, Ryan. Revealed: how much is personal information worth on the dark web [online]. 2022. Dostupné z: https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx. [citováno 2023-09-04].
26. Symantec. (2019). *Internet Security Threat Report. Symantec Corporation.* [online]. Dostupné z: https://www.insight.com/en_US/content-and-resources/brands/symantec/internet-security-threat-report.html. [citováno 2024-04-01].
27. The Washington Post. *Postal Service the preferred shipper for drug dealers.* [online]. 2018. Dostupné z: https://www.washingtonpost.com/politics/2018/10/16/postal-service-preferred-shipper-drug-dealers/. [citováno 2024-04-01].

28. UNODC. (2020). *World Drug Report 2020.* United Nations Office on Drugs and Crime.
29. Web-Iq. *Web-IQ newsletter.* Amsterdam: Web-IQ, 2018.
30. WEISER, Benjamin. *Ross Ulbricht, creator of Silk Road website, is sentenced to life in prison*. New York Times. [online]. 2015. Dostupné z: Ross Ulbricht, Creator of Silk Road Website, Is Sentenced to Life in Prison - The New York Times (nytimes.com). [citováno 2024-04-01].
31. WOOLLASTON, Victoria. How To Access The Dark Web: What Is Tor And How Do I Access-Dark Websites?. In: *Alphr* [online]. 2020. Dostupné z: world-finds-study-news-183428. [citováno 2024-04-01].
32. ZANTOUT, Bassam a HARATY, R. I2P data communication system. In: *Proceedings of ICN*. Singapore: ICN, Springer, 2011. p. 401-409.

Seznam zkratek

IT - Informační technologie

Tor - The Onion Router

I2P - nvisible Internet Project

ISP - Internet Service Provider

IP - nternet Protocol

VPN - Virtual Private Network

HTTPS - Hypertext Transfer Protocol Secure

IoT - Internet of Things

SMS - Short Message Service

DDoS - Distributed Denial of Service

OFAC - Office of Foreign Assets Control

dApps - decentralized applications

XMR - kryptoměna Monero

SOL - kryptoměna Solana

ADA - kryptoměna Cardano

BNB - kryptoměna Binance Coin

ETH - kryptoměna Ethereum

BTC - kryptoměna Bitcoin

DWF - Design Web Forma

PII - Personally Identifiable Information

SNS - Social Networking Service

Seznam tabulek a grafů