Černý trh na Internetu

Vložil/a dw [1], 2 Březen, 2015 - 22:52

- Anonymita [2]

V tomto článku vám představím tzv. deep web (někdy též darknet nebo invisible web) a krok za krokem ukážu, jak si zajistit anonymitu prostřednictvím technologie Tor a získat finanční prostředky v podobě kryptoměny zvané BitCoin, což jsou dvě věci nezbytné k přístupu a nákupu na internetovém černém trhu.

Přes internet lze dnes pořídit téměř cokoliv, od dřevěných hodinek, přes sadu 216 kusů magnetických kuliček, až po exotické suroviny k výrobě vlastního sushi, ale také drogy, cizí údaje k platebním kartám, zbraně a střelivo, nebo knihu s názvem Jak se (ne)chovat během zatčení. Pro přístup k tomuto více či méně delikátnímu zboží vám však nestačí běžný webový prohlížeč ani nekoupíte nic za běžné měny, jako jsou dolary nebo eura, v první řadě potřebujete anonymní webový prohlížeč Tor a finanční obnos v podobě kryptoměny zvané bitcoin (BTC). V tomto článku vám krok za krokem ukážu, jak si tyto prostředky obstarat.

Tor – na webu anonymně

Tor, neboli The Onion Router, je systém, který celkem spolehlivě zahalí vaší identitu, reprezentovanou vaší IP adresou, při surfování po internetu a umožní vám proniknout na tzv. deep web (darknet, invisible web). Jak to funguje? Místo abyste k serveru přistupovali přímo, Tor vaše spojení přesměruje přes mnoho dalších uživatelů sítě Tor a to tak, že každý uzel má informace pouze o uzlu předchozím a následujícím, cíl je tedy zapouzdřen do jednotlivých vrstev, podobně jako jádro cibule (onion – angl. cibule), vedlejším efektem takového spojení je občas velmi znatelný pokles rychlosti, proto je vhodné nepoužívat Tor tam, kde to není nezbytně nutné a zbytečně tak síť nezatěžovat. Black Markety, tedy internetové obchody s ilegálním zbožím, internetový černý trh, jsou pomocí této technologie také zcela anonymně připojeny do sítě, používají doménu .onion a jinak než přes Tor se na ně nedostanete.

Instalace

Tento postup je platný a otestovaný na distribuci Ubuntu 14.04 LTS. Nejprve je nutné zjistit jednoslovný název tohoto vydání, jedná se vždy o první slovo ze sloupce Code name v tabulce na této adrese:

https://en.wikipedia.org/wiki/List_of_Ubuntu_releases#Table_of_versions [3]

Zde vidíte, že verze 14.04 je označena jako Trusty Tahr, naše slůvko je tedy **trusty**. Nyní otevřete Terminál a zadejte jeden po druhém následující příkazy, pro získání přístupu k potřebným balíčkům:

```
deb http://deb.torproject.org/torproject.org trusty main
gpg --keyserver keys.gnupg.net --recv 886DDD89
gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt- key add -
sudo apt-get update
```

A tyto příkazy, pro instalaci keyringu a konečně Toru jako takového:

```
sudo apt-get install deb.torproject.org-keyring
sudo apt-get install tor
```

Nakonec stáhněte prohlížeč Tor Browser Bundle z oficiálních stránek projektu:

https://www.torproject.org/projects/torbrowser.html [4]

Stažený balíček kamkoliv rozbalte a pomocí Terminálu spusťte soubor **./start-tor-browser**. Jakmile vám prohlížeč najede, můžete na první pohled vidět, že vychází z dobře známého Firefoxu, což znamená, že v něm můžete používat jakékoliv add-ony, napsané pro běžný Firefox, např. ReloadEvery, pro automatické znovunačítání stránek.

Okruh anonymizace vašeho spojení můžete změnit ručně, kliknutím na malou ikonu zelené cibule vlevo, vedle řádku pro URL adresu, zvolení možnosti New Identity, prohlížeč Tor tak činí automaticky defaultně každých 600 vteřin, čili každých 10 minut, pokud byste chtěli aby automatickou změnu okruhu prováděl častěji, což je vhodné při podvádění v klikacích soutěžích, nebo reklamních systémech, které vám platí za unikátní zobrazení reklamních bannerů, můžete toto nastavení změnit pomocí konfiguračního souboru **torrc**, který naleznete ve složce **Browser/TorBrowser/Data/Tor** a to tak, že do něj přidáte řádek

```
MaxCircuitDirtiness 10
```

Tor bude nyní po restartování prohlížeče měnit okruh každých **10** vteřin. Dále také můžete nastavit, aby koncový bod (od toho se logicky odvíjí IP adresa pod jakou vás uvidí cílový server) byl striktně z určité země, to provedete vložením těchto dvou rádků:

```
ExitNodes {CZ}
StrictExitNodes 1
```

Cesta ke konfiguračnímu souboru torrc se čas od času s příchodem nové verze Tor prohlížeče může změnit a vy tak budete muset po stažení této nové verze, na kterou vás Tor Browser vždy upozorní, trochu hledat.

BitCoin – virtuální kryptoměna

Bitcoiny tu s námi jsou teprve od roku 2009 a za jejich vznikem stojí člověk, nebo skupina lidí, pod pseudonymem Satoshi Nakamoto, někteří lidé věří, že se jedná o společnosti **Sa**msung, **Tochi**ba a **Naka**michi, jedná se však jen o nepodložené spekulace. Ať už tedy bitcoiny stvořil kdokoliv, stvořil úžasnou věc, díky které je možné vcelku anonymně provádět finanční transakce na globální úrovni v reálném čase (narozdíl od klasického bankovního převodu, který může na této úrovni trvat i několik dní). Lidé, kteří bojují proti zločinu by s mým tvrzením, že bitcoiny jsou úžasná věc, asi nesouhlasili, myslím že bychom se ale neshodli i na jiných věcech.

Kurz bitcoinu vůči ostatním měnám je velmi kolísavý a na těchto výkyvech lze dokonce i vydělat, podobně jako např. na výkyvech ceny ropy a jiných komodit, to nejlepší je však již za námi. V roce 2009 se totiž cena jednoho bitcoinu pohybovala okolo 40 USD (cca 900 CZK) zatímco dnes kolísá okolo 385 USD (cca 8600 CZK). Tak jen doufám, že teď nemlátíte hlavou o stůl se slovy: „kdybych já to tenkrát věděl“.

Proces, jakým jsou do oběhu uvolňovány nové bitcoiny, tzv. bitcoin mining, je velmi zajímavý, blíže ho rozebírat již přesahuje téma tohoto článku, rozhodně vám však doporučuji si o něm, dříve než se pustíte do samotného nákupu bitcoinů, vyhledat alespoň základní informace.

Pořízení bitcoinů

Vzhledem k faktu, že Bitcoiny jsou elektronickou měnou, jsou uchovávány v elektronických

bitcoinových peněženkách a to buď lokálně, přímo na pevném disku (který tak de facto může značně stoupnout na hodnotě) a nebo v cloudu. První varianta má tu nevýhodu, že pokud dojde ke ztrátě, nebo poškození vašeho zařízení, příjdete i o své bitcoiny, druhý způsob zase vyžaduje vaší absolutní důvěru k subjektu, který vaše bitcoiny uchovává. Je to jako mít peníze buď zašité do matrace, nebo uložené v bance. Předpokládejme, že máte raději své peníze pěkně u sebe, v tom případě je prvním krokem k pořízení bitcoinů stažení bitcoinové peněženky, existuje jich celá řada, mě se však velmi osvědčil program s názvem **Electum**, je multiplatformní a umoňuje mít bitcoiny uloženy dokonce i v mobilním telefonu s Androidem.

https://electrum.org [5]

Program si stáhnětě, nainstalujte, spusťte a po nastavení (doporučuji použít heslo, ale nezapoměňte ho, jinak už se ke svým bitcoinům nedostanete) přejďete na kartu Příjem, zde vidíte několik adres, které mají formát 34 náhodně vybraných čísel a malých a velkých písmen, to jsou adresy vaší bitcoinové peněženky, na které vám ostatní mohou ze svých peněženek posílat bitcoiny, při obchodování přes bitcoinové burzy (např. https://www.bitstock.com [6]) nebo některou z nich použijete při výběru z elektronické směnárny, jakou je např. VirWox – Virtual World Exchange. Nyní vám ukážu, jak si obstarat bitcoiny právě zde, otevřete tedy prohlížeč a zadejte adresu

https://www.virwox.com [7]

Zde se podle pokynů zaregistrujte a přihlašte se ke svému novému účtu. Vlevo v seznamu nadepsaném My Account (můj účet) vyberte položku Deposit (vložit) a ocitnete se na stránce, kde máte na výběr hned z několika možností, jak na svůj účet vložit peníze, já preferuji PayPal, zadal bych tedy do kolonky I want to deposit (Chci vložit) výši částky, kterou chci vložit, řekněme pro začátek takových 50€, z rozbalovacího seznamu bych tedy vybral eura (EUR) a stisknul klávesu ENTER, což mě již přesměruje na platební bránu služby PayPal. Jakmile budete mít na svém účtu nějaký finanční obnos, všimněte si pod seznamem My Account dalšího seznamu s názvem Exchange (vyměnit), zde vyberte nejprve EUR/SSL, dostanete se na stránku kde vyměníte eura za Linden Dolary (virtuální měna používaná v Second Life) a potom v SSL/BTC směňte L$ za bitcoiny, nakonec v seznamu My Accoint vyberte Withdraw (vybrat) a zde v sekci Withdraw to Bitcoin zadejte částku v bitcoinech (vlevo nahoře pod Account Ballance, stav účtu, můžete vidět kolik jich máte k dispozici) jednu z adres vaší bitcoinové peněženky a stiskněte tlačítko Request Withdrawal (Požádat o výběr). U nových účtů trvá výběr do 48 hodin, později už jsou výběry prováděny okamžitě a čeká se pouze na potvrzení tzv. block chainu, což se děje v řádech už jen několika desítek minut. Služba samozřejmě není zdarma, takže nečekejte, že dostanete bitcoiny v plné výši vašeho vkladu, proto je výhodnější netroškařit a koupit bitcoinů více najednou.

Hurá na černý trh

Tor máte. Bitcoiny máte. Je čas na nákupy. Upozorňují vás, že následující informace slouží již jen ke studijním účelům a autor článku ani provozovatel serveru root.cz nenesou odpovědnou za jejich případné zneužití. Pokud si objednáte půl kila kokainu a budete dopadeni, je to jen váš problém. Spusťte tedy prohlížeč Tor a přejděte na následující stránku.
http://grams7enufi7jmdl.onion [8]

To co nyní vidíte je vyhledávač nápadně připomínající dobře známý Google, krom faktu, že se jedná o vyhledávač však s Googlem nemá nic společného. Umožní vám prohledávat deep web, obsahuje ale jen omezené množství zaindexovaných stránek, proto je lepší znát a zadávat adresy přímo, tím však nechci říct, že je Grams úplně k ničemu, je rozhodně dobré ho znát, alespoň v začátcích.

Na deep webu existuje celá řada Black Marketů, nejznámější Silk Road 2 nedávno následoval svého předchůdce (Silk Road) a byl americkými úřady odhalen (server na kterém běžel se nacházel v Litvě) a zrušen, společně s dalšími více než 400 stránkami. Stále tu však zůstává celá řada dalších. Některé k registraci vyžadují pozvánku (např. Agora) a jiné jsou dostupné pro každého, jako třeba Evolution. Ten najdete na adrese

http://k5zq47j6wd3wdvjq.onion [9]

Během registrace zadáte kromě uživatelského jména a hesla také pin a získáte několik náhodně vybraných slov, které si pečlivě zapiště, pin slouží k výběru vašich bitcoinů a slova zadáváte při prvním přihlášení. Jakmile budete na úvodní stránce povšimněte si, že nikde nevidíte žádné reklamy, což trochu připomíná dobu, kdy byl internet ještě v plenkách a nikdo si nemyslel, že reklama na internetu je lukrativní obchodní odvětví. Nahoře pak vidíte stav svého účtu, tedy BTC 0.0000, kliknutím zde se dostanete na stránku, kde máte bitcoinovou adresou svého Evolution účtu, na tu pomocí Electum pošlete finanční obnos ze své bitcoinové peněženky, připsání je provedeno po dvou potvrzeních block chainu, nemělo by tedy trvat déle než několik desítek minut. Když se pak vrátíte na hlavní stránku, vlevo uvidíte kategorie a počet nabízených položek od jednotlivých prodejců (Vendors). Při výběru zboží dbejte na hodnocení vendorů a než se rozhodnete pro nákup prečtěte si odezvy (Feedback) ostatních uživatelů, u těch nejlepších prodejců s hodnocením přes 95% a velkým množstvím pozitivních ohlasů, je šance, že vám zboží nebude dodáno a přijdete o své peníze téměř nulová. Dobří prodejci také minimalizují šanci na vaše odhalení tím, že vyžadují abyste jim zaslali dodací adresu zašifrovanou pomocí technologie PGP, která k šifrování dat využíva dvojího klíče a to privátního k dešifrování a veřejného k jejich zašifrování, vendor vám tedy poskytne svůj veřejný PGP klíč a vy pomocí něj zašifrujete svojí adresu třeba na

https://www.igolder.com/pgp/encryption [10]

U citlivějších dat však doporučuji provádět šifrování pomocí utilit přímo ve vašem počítači. A to je pro dnešek vše. Pokud budete mít nějaké dotazy, obraťte se na mě prostřednictvím e-mailu, nebo svůj dotaz nasměrujte do diskuze. Máte-li zájem o pozvánku na Agoru, nepiště do diskuze, ale požádejte mě o ní přes e-mail.

URL článku: https://security-portal.cz/clanky/cerny-trh-na-internetu

Odkazy:
[1] https://security-portal.cz/users/dw
[2] https://security-portal.cz/category/tagy/anonymita
[3] https://en.wikipedia.org/wiki/List_of_Ubuntu_releases#Table_of_versions
[4] https://www.torproject.org/projects/torbrowser.html
[5] https://www.electrum.org/
[6] https://www.bitstock.com
[7] https://www.virwox.com
[8] https://security-portal.cz/grams7enufi7jmdl.onion
[9] http://k5zq47j6wd3wdvjq.onion
[10] https://security-portal.cz/https