E-Bezpečí 2016, 1(1): Page 35-39. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1136

ZÁKOUTÍ „TEMNÉHO“ INTERNETU

Vojtěch BEDNÁŘ

Jsou věci, které na běžném internetu nekoupíte. A naopak místa, kam se běžný uživatel internetu nedostane. O „temném“ internetu se ví, ale pro mnoho těch, kteří o něm slýchají je stejně nepochopitelný, jako dříve býval internet jako celek.

Z pohledu dnešního, gramotného člověka je Internetu ne už pouze zajímavou technologickou věcí určenou nadšencům a zasvěceným, ale naprosto běžnou součástí jejich života, s jejíž pomocí je možné dělat téměř vše.

Současný internet je nicméně také médiem, které je sledováno, regulováno a řízeno státy, jejich zákony a autoritami. Také některé jeho vlastnosti, které jej kdysi dělaly tak atraktivním, jsou pryč. Současný internet například již dávno není anonymní a také ani zdaleka tak nezávislý a decentralizovaný, jako tomu bylo v počátcích jeho používání. A tak lidé, kterým to z různých příčin vadí, hledají alternativy. Mezi ně patří něco, čemu se souhrnně říká „temný“ internet, angl. ***darknet***.

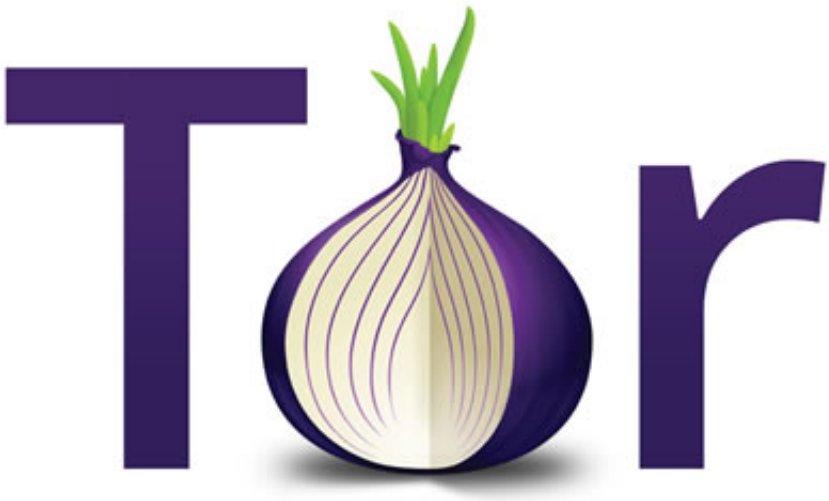
Když o darknetu hovoří mainstreamová média, mají většinou na mysli pro běžného uživatele „neviditelný“ web s využitím sítě Tor, ve skutečnosti se ale jedná o poměrně pestrý svět různých technologií a nástrojů majících společný cíl: maskovat komunikaci a zajistit uživatelům možnost výměny informací nezávisle na tom, aby je mohl někdo kontrolovat, sledovat anebo vůbec identifikovat.

Cibulové řešení

Způsobů, jak to udělat, je, jak už bylo řečeno, mnoho. Všechny v zásadě využívají toho, že technologická infrastruktura internetu je stále postavená na otevřených základech a že je možné na ní provozovat v podstatě libovolné služby, které splňují jeho základní standardy.

Jak už bylo řečeno, nejznámější (pokud se v případě skrytých technologií o něčem takovém dá vůbec mluvit), je směrovací systém Tor. Jeho princip spočívá ve vytvoření komunikační vrstvy nad standardní internetovou infrastrukturou, ve které jsou požadavky jednotlivých uživatelů směřovány přes náhodně zvolené uzly, a stejným způsobem je organizována doprava odpovědí serverů na ně (celý systém běží v režimu klient – server). Principu se říká „cibulové směrování“, odtud také cibulka, kterou má tato technologie ve znaku. Informace, která je přenášena sítí, se obalí do předdefinovaného počtu vrstev šifrování, kdy po dekódování každé z nich je směrovači (prvku, který provádí transport dat) zobrazena adresa dalšího uzlu na cestě zprávy, ale ne zpráva samotná. Každý prvek tedy „odloupne“ jednu vrstvu šifrované informace a jakmile jsou odstraněny všechny, znamená to, že zpráva dorazila do svého cíle.

Toto řešení je ve srovnání s běžnými postupy přenosu informací na internetu pomalé a problematická je také jeho efektivita. Na druhé straně ale velice komplikuje odposlech komunikace po cestě, a to ať už formou útoku typu *man in the middle*, anebo pasivním náslechem datového provozu po cestě. Z pohledu koncového uživatele přitom nemusí být nijak komplikované.



Jestliže je „temná“ strana internetu postavena, stejně jako třeba běžný web, na principu klientů a serverů, pak obě tyto strany jsou otevřeny, tj. může se do nich zapojovat v podstatě každý, kdo má o to zájem. Standardní (výchozí) klient na straně uživatele má podobu běžného webového prohlížeče a krom znalosti adresy cílové služby nejsou k jeho obsluze potřeba žádné zvláštní dovednosti. Také na straně serveru není mnoho odlišností oproti klasickému webovému serveru, a tak mnoho „temných“ služeb vychází z klonů anebo adaptací běžných webových serverů. Počáteční investice nutné k používání této služby jsou nulové pokud jde o finance a velmi střídmé pokud o práci a úsilí.

Alternativy

Tor a jeho skryté služby samozřejmě není jedinou „temnou“ technologií. Na obdobném principu pracuje celá řada dalších nástrojů. Všechny mají společné to, že tvoři anonymizační vrstvu nad transportní infrastrukturou klasického internetu a všechny jsou vzájemně odděleny. Patří sem třeba semi P2P sít **I2P** (také známá jako „neviditelný internet“), **Freenet** a nebo nástroje, které se vyvinuly z původně P2P technologií pro decentralizované sdílení souborů. Existují také nástroje (pocházející rovněž původně ze světa výměnných sítí pro sdílení souborů, které umožňují přemosťovat různé služby, tj. přenášet obsah, který je sdílen v jedné z nich do druhé, a to včetně přeložení adres. Tím se přenos

komplikuje, nicméně může se takto zvyšovat dostupnost informací. Efekty na základní účel, tj. ochranu soukromí jsou obojaké – pozitivní i negativní.

Použití

Když se řekne „temný internet“, vybaví se laikovi kombinace zbraně-drogy-násilí. Pravdou je, že anonymizační systémy jsou využívány těmi, kteří mají důvod chránit se před dohledem ruky zákona, ale nikde není řečeno, že to musí být pouze gangsteři. „Temný“ internet je místem, které víceméně musí používat třeba politická opozice v zemích, kde je perzekuována, ale například také specifické skupiny lidí, kteří se ničeho amorálního či nezákonného nedopouštějí, ale prostě a jen chtějí mít své informace chráněny a anonymní. Sem patří také technologičtí „geeci“, pro které jsou skryté služby vlastně tím, čím býval původně celý internet a o co byl připraven v důsledku svého komerčního úspěchu. Na bázi darknetu vznikají celé subkultury, novodobé kmeny. Pro většinového uživatele ale nemá průzkum této části internetu, snad kromě naplnění potřeby zvědavosti, žádný větší význam.

(Zdroj obrázku: Cyberwarzone.net)

Soukromí?

Anonymizační nástroje jsou sofistikované, ale ne nepřekonatelné nástroje, a je potřeba říct, že jak samotná existence darknetu, tak

jeho jednotlivé technologie jsou trvale v hledáčku nejlépe vybavených bezpečnostních služeb světa. Slabým místem jsou chyby v softwarových komponentách, postavených často na opensource modelu – v generátorech pseudonáhodných čísel, které tvoří základ, v šifrovacích knihovnách, v OpenSSL, které je otevřeně či skrytě mnoha anonymizačními technologiemi využíváno. Existuje také podezření, že některé servery, routery, a možná i protokoly jsou cíleně vytvářeny jako „honeypot“ s cílem přilákat zájem těch, které je lépe sledovat, než nechat být. To jsou ale spíše spekulace, než něco, co by mělo ověřený základ.

Pro E-Bezpečí,
PhDr. Vojtěch Bednář