Tor připomíná spíše projekt zpravodajců než nástroj vytvořený komunitou, cenící si hodnot zodpovědnosti a transparentnosti.

Autor: Yasha Levine

Jak bezpečný je vlastně Tor?

Je s podivem, že Dingledina důkazy o útoku NSA na Tor nijak neznepokojily – v neposlední řadě proto, že už poměrně dlouho byl útok ze strany mocné vládní organizace pokládán za jednu ze zásadních slabin sítě.

V roce 2011 na diskusi na oficiálním serveru Toru jeho vývojář Mike Perry přiznal, že Tor nemusí být tváří tvář mocným a organizovaným „protivníkům“ (čti vládám), schopným monitorovat obří sekce internetu, kdovíjak účinný.

„Protivníci s bezednými kapsami, schopní kontrolovat velké částí internetu, pravděpodobně mohou prolomit některé prvky Toru a zbavit uživatele anonymity. Proto má současný hlavní program Toru označení verze 0.2.x a jeho součástí je varování, že není určen pro ‚silnou anonymitu‘. (I když sám nevěřím, že by nějaký protivník mohl spolehlivě zbavit anonymity *všechny* uživatele toru... ale napadení anonymity bývají ze své povahy subtilní a kumulativní).

A skutečně – loni pracoval Syverson ve výzkumném týmu, který *de facto* prokázal, že na Tor už nelze pro dlouhodobou ochranu uživatelů spoléhat.

„Je známá slabost Toru proti protivníkovi, který dokáže monitorovat pohyb uživatele při vstupu a výstupu z Toru**.** Vcelku jednoduché a účinné techniky umí korelovat datový provoz (*traffic*) v těchto jednotlivých oblastech využíváním identifikace struktury datového provozu. Následkem toho lze určit uživatele a jeho cíl, čímž dochází k úplnému rozvrácení smyslu bezpečnostního protokolu.“

Výzkumníci uzavírají: „Tato zjištění jsou poněkud skličující pro bezpečnostní situaci Toru.“

I když Syverson naznačil, že některé ze slabin, na něž výzkum poukázal, řeší novější verze Toru, zjištění se přidala k prodlužujícímu se seznamu jiných materiálů a jednotlivých případů, které ukazují podstatně slabší Tor, než o jakém by se vás jeho tvůrci snažili přesvědčit – zvlášť když čelí odhodlaným bezpečnostním službám.

Jeden příklad za všechny: V prosinci 2013 zjistil jeden vyděšený premiant z Harvardu, Edlo Kim, jak malou ochranu poskytuje Tor potenciálním teroristům.

Aby se vyhnul zkoušce, na niž nebyl dostatečně připraven, přišel Kim na myšlenku vyvolání falešného bombového poplachu. Pro skrytí své identity použil Tor – údajně nejlepší na webu

dostupný nástroj k poskytnutí anonymity. Před odhodlaným Strýčkem Samem ho však Tor neskryl na dlouho. Společné vyšetřování FBI, Tajné služby a místní policie falešný bombový poplach vystopovalo ke Kimovi za necelých 24 hodin.

Jak osvětlila žaloba FBI: „Harvardova univerzita byla schopna určit, že během několika hodin před obdržením potvrzení o přijetí výše popsaného e-mailu, se ELDO KIM připojil přes univerzitní bezdrátovou síť na TOR.“ Kvůli Toru to tedy měla policie jen o trochu složitější – ne však složité; nic s čím by se pár lidí s plnou zákonnou pravomocí k přístupu k záznamům o vstupech na síť snadno nevypořádalo. Vyšetřování neuškodilo ani to, že harvardská síť schraňuje veškerá metadata o přístupech na ni – tak trochu jako NSA.

Během několika posledních let převzaly americké orgány činné v trestním řízení kontrolu nad – aby je následně zrušily – několika středisky obchodu s dětskou pornografií a drogami, operujících na domněle nevystopovatelných, hyperanonymních serverech běžících na počítačovém cloudu Toru.

V roce 2013 byl odstavena webhostingová firma Freedom Hosting, obviněná z poskytování masívního prostoru stránkám s dětskou pornografií – ale ne předtím, než FBI převzala všechny její servery a odposlechla veškerou komunikaci se zákazníky. Téhož roku potkal podobný osud ze strany FBI i online drogový supermarket Silk Road, který také své služby provozoval z Tor cloudu. I když odhalit identitu Dread Pirate Robertse pomohly FBI začátečnické chyby, zůstává záhadou, jak se jim povedlo zcela převzít a ovládat – a dokonce i zkopírovat – server běžící na Tor cloudu, což má být zcela neproveditelné.

Už v roce 2007 švédský hacker/výzkumník Dan Egerstad ukázal, jak pouhým spuštěním přenosových relací Toru (vstupních/výstupních uzlů – entry/exit nodes) dokáže „odčerpat“ a přečíst veškerý nezašifrovaný pohyb skrz jím provozovanou část sítě Tor. Dostal se k přihlašovacím jménům a heslům účtů nevládních organizací, společností a indického a íránského velvyslanectví. Zprvu se Egerstad domníval, že zaměstnanci se svými daty nakládali neopatrně, ale rychle si uvědomil, že ve skutečnosti narazil na hackerskou/sledovací operaci, využívající Toru k tajnému přístupu k těmto účtům.

I když Egerstad zůstal příznivcem Toru a stále věří, že při správném užití dokáže zajistit anonymitu, po svých zkušenostech se stal mnohem opatrnějším.

Listu *Sydney Herald* řekl, že podle jeho mínění velkou část největších uzlů Toru provozují zpravodajské služby nebo jiné subjekty, které by rády naslouchaly komunikaci přes Tor.

> „Nechci o tom spekulovat, ale lidem říkám, že je to možné. Pokud se opravdu podíváte, kde se tyto uzly Toru nachází a jak jsou velké, některé z nich stojí tisíce dolarů měsíčně jen na hostingu, protože spotřebovávají spoustu přenesených dat, jde o vysoce výkonné servery atd. Kdo by za to platil a zůstal anonymní? Pět nebo šest z nich se například nachází ve Washingtonu, D.C…“

Tor prudí?

Příznivci Toru poukazují na balík dokumentů NSA vynesený Snowdenem, aby prokázali, jak se agentura Toru bojí a nesnáší ho. Článek *Guardianu* – čerpající z těchto dokumentů – z roku 2013 Jamese Balla, Bruce Schneiera a Glenna Greenwalda se snaží ukázat, že NSA je proti nástroji na ochranu anonymity *de facto* bezmocná.

> ...dokument naznačuje, že základní bezpečnost služby Tor nebyla narušena. Z jedné supertajné prezentace, nazvané ‚**Tor Stinks**' se dovídáme: „ Nikdy se nám nepodaří trvale odanonymizovat všechny uživatele Toru" a pokračuje: „Analýzou manuálu toho můžeme docílit u velice nízkého procenta uživatelů," a prohlašuje, že NSA neměla „sebemenší úspěch v deanonymizaci uživatele v odpovědi" na specifický požadavek.

Jiná supertajná prezentace označuje Tor „králem vysoce bezpečné internetové anonymity s nízkou mírou zpoždění."

Dokumenty NSA však jen stěží lze pokládat za průkazné, obsahují protichůdné důkazy a nacházíme v nich oporu pro četné interpretace. Faktem zůstává schopnost NSA a GCHQ proniknout do Toru – i když si to může žádat trochu zvýšeného úsilí.

Jedna věc by nám měla být jasná: NSA se Toru rozhodně nebojí a není ani pravda, že jej nesnáší. Některé jeho prvky dokonce rozhodně vítá, zčásti i proto, že se jí díky němu potenciální „cíle" shromažďují na jednom místě.

Tor prudí... ale mohlo by to být horší

> Tor užívá kritické množství cílů. Jejich vystrašení by se mohlo prokázat jako kontraproduktivní.
> Můžeme zvýšit naši úspěšnost a jednotlivým uživatelům poskytnout více klientských IP adres.
> Nikdy se nedostaneme na 100%, ale nemusíme každému cíli poskytnout skutečnou IP adresu pokaždé, když využívá Tor.

Převzít kontrolu nad sítí Tor je snazší než by se mohlo zdát...

V roce 2012 Roger Dingledine odhalil, že síť Tor je nastavena na preferenci rychlosti a směřuje pohyb přes nejrychlejší dostupné servery/uzly. Díky tomu drtivá většina pohybu přes Tor běží skrz několik tuctů nejrychlejších a nejspolehlivějších serverů: „na dnešní síti si klienti volí jeden z pěti nejrychlejších výstupních přenosových relací v 25-30%, z toho 80% jejich voleb pochází z množiny 40-50 relací."

Komunita kolem Toru Dingledina pochopitelně kritizovala, že směrování provozu přes pár

rychlých uzlů usnadňuje sledování a subverzi Toru. Každý může spustit uzel Toru – student výzkumník v Německu, chlápek z Victorville s připojením FIOS (můj případ po několik měsíců), utajené pracoviště NSA na Havaji nebo zaměstnanec čínské internetové policie.

Nelze zjistit, jestli lidé provozují nejrychlejší stabilní uzly z dobré vůle nebo protože tak lze nejsnáze odposlouchávat síť Tor. Zvláště znepokojivé Snowdenovy úniky jasně prokázaly, že NSA a GCHQ provozují uzly Toru a mají zájem zprovoznit další.

Spustit 50 uzlů Toru se nezdá pro kteroukoliv světovou rozvědku – ať už americkou, německou, ruskou, čínskou nebo íránskou – být příliš velkou výzvou. A pokud jste zpravodajská služba, proč byste vlastně Tor uzel *ne*vytvořili?

V roce 2005 Dingledine časopisu Wired přiznal, že jde o „ožehavou otázku designu“, ale s jasnou odpovědí, jak bude řešena, přijít nedokázal. V 2012 odbyl kritiku kompletně, když vysvětlil, že je zcela ochoten obětovat bezpečnost pro rychlost – cokoli, co Toru zajistí více uživatelů:

> Tato volba odkazuje na mou původní debatu s Mikem Perrym z před několika let… pokud se chceme dostat k rychlé bezpečné síti, dostaneme se tam skrz pomalou bezpečnou síť a naději, že se postupem času zrychlí nebo pomocí rychlé a bezpečné sítě s perspektivou nárůstu bezpečnosti? Zvolili jsme cestu „pokud nebudeme pro svět relevantní, Tor nikdy dostatečně nenaroste“.

Když jsme u „tajných“, provozujících uzly Toru…

Pokud jste mysleli, že příběh Toru už nemůže být divnější – může a je. Nejspíš nejpodivnější částí celé ságy představuje skutečnost, že Edward Snowden během své havajské práce pro NSA provozoval četné vysokorychlostní uzly Tor.

Tento fakt vešel v obecnou známost až loňského května, kdy vývojářka Toru Runa Sandviková (která také dostávala plat z peněz Pentagonu/Ministerstva zahraničí USA pro Tor) řekla Kevinu Poulsenovi z časopisu Wired, že jen dva týdny předtím, než se pokusila zkontaktovat Glenna Greenwalda, jí poslal Edward Snowden e-mail v němž vysvětloval, že provozuje významný uzel Toru a chtěl by nějaké nálepky Toru.

Nálepky? Ano, nálepky.

Edward Snowden

Následuje úryvek z článku ve Wired:

> V tomto e-mailu Snowden napsal, že osobně provozoval jeden z „hlavních tor exitů“ – 2GBps server jménem „TheSignal“ – a snažil se přesvědčit nejmenované spolupracovníky ze své kanceláře, aby zřídili další servery. Nesdělil, kde pracuje. Ale chtěl vědět, jestli by mu Runa Sandviková nemohla poslat balíček nálepek Tor. (Na některých novějších Snowdenových fotkách lze vidět nálepku Tor na zadní straně jeho notebooku, hned vedle nálepky EFF.)

Snowdenova prosba o nálepky Tor se vyvinula v poněkud intimnější interakci. Sandviková už předtím plánovala jet na Havaj na dovolenou, takže Snowden jí navrhl schůzku, kde by mohli probrat bezpečnost komunikace a šifrování.

> Sandviková tedy Snowdenovi odpověděla a nabídla mu prezentaci o Toru pro místní publikum. Snowdena to nadchlo a přišel s nápadem vytvořit pro tuto příležitost krypto-party.

A tak dvojice uspořádala v honolulské kavárně „krypto party“, na níž se asi dvacítka místních učila, jak užívat Tor a šifrovat své pevné disky. „Představil se jako Ed. Než všechno začalo, chvíli jsme spolu mluvili. Vybavuji si, že když jsem se ho ptala, kde pracuje nebo co dělá, choval se vyhýbavě,“ řekla Sandviková Wired.

Zjistila však, že Snowden provozoval více než jeden Tor uzel, a že snažil některé kolegy „z práce“ přesvědčit k založení dalších…

Hmmm… takže Snowden zakládá výkonné Tor uzly a snaží se přemluvit své kolegy z NSA, aby udělali totéž?

Zkontaktoval jsem Sandvikovou, abych získal její vyjádření – neodpověděla mi. Poulsen z Wired se domnívá, že provoz Tor uzlů a uspořádání krypto-party bylo pro Snowdena vedlejším projekt na podporu soukromí na webu. „I když myslel globálně, jednal lokálně."

Představa chlapíka s nejpřísnější bezpečnostní prověrkou – který právě plánuje ukrást ohromné množství tajných dat – riskujícího s uzlem Toru, jen aby podpořil boj za soukromí, se jeví jako poněkud absurdní. Ale kdo vlastně v tomhle všem dovede najít nějaký smysl?

Hádám, že cibulové logo Toru je velice příznačné – čím víc vrstev totiž odloupnete a čím hlouběji se dostanete, tím méně věci dávají smysl a stále více si uvědomujete, že se nejde dostat na dno či konec celé věci. Jen obtížně se nalézají přímé odpovědi – nebo dokonce jen ty správné otázky.

V tomto Tor připomíná spíše projekt zpravodajců než nástroj vytvořený komunitou, cenící si hodnot zodpovědnosti a transparentnosti.

Článek Yashi Levina Almost everyone involved in developing Tor was (or is) funded by the US government vyšel na stránkách PandoDaily.