Autor: Yasha Levine

Tor, the Best Internet Anonymity Tool the Government Ever Built

„Americká vláda prostě nemůže provozovat anonymizační síť a pak ji využívat jen pro svou potřebu. Pak by si totiž lidi pokaždé, když by se odtud někdo připojil, řekli: ‚No jo, další agent CIA,' pokud by tu síť využívali jen oni."

— Roger Dingledine, spoluzakladatel sítě Tor, 2004

***

Na začátku června zveřejnil hacker Jacob Appelbaum a další dva bezpečnostní experti, zároveň s německým tiskem, senzační zprávu. Dostali se k přísně tajným dokumentům National Security Agency (NSA) a zdrojovému kódu dokazujícím, že tato sledovací agentura se zaměřila a potenciálně prolomila síť Tor, široce užívaný anonymizační nástroj, považovaný za svatý grál online anonymity.

Aktivisté za internetové soukromí i podobné organizace reagovali zděšeně. Po celé uplynulé desetiletí propagovali Tor coby problematickou, ale extrémně účinnou široce dostupnou technologii, která dokáže ochránit novináře, disidenty a „whistleblowery" před mocnými vládami, snažícími se monitorovat jejich veškerou aktivitu. Tor byl pokládán za nejlepší existující prostředek – šlo o nedílnou součást příručky EFF „Sebeobrana před sledováním" od Electronic Frontier Foundation (EFF). Mezi jeho přesvědčené uživatele patřili Edward Snowden a také Glenn Greenwald, podle něhož Tor „umožňuje lidem surfovat, aniž by je vlády či tajné služby mohly sledovat."

Ale německé *exposé* ukázalo pravý opak: používání Toru zvýrazňuje uživatele pro totální sledování NSA, potenciálně zaznamenává a archivuje jeho veškerou online aktivitu.

Pro mnoho lidí v komunitě online soukromí se útok NSA na Tor rovnal velezradě: fašistické porušení základního a posvátného práva na soukromí a svobodu slova.

Nadace EFF považuje Tor za zásadní nástroj „umožňující svobodu projevu". Appelbaum – dobrovolník Wikileaks a vývojář Toru – pokládá dobrovolnickou práci na Toru za akt statečnosti srovnatelný s Hemingwayem nebo Orwellem, kteří „odešli do Španělska bojovat s Frankovými fašisty" po boku anarchistických revolucionářů.

Pěkný příběh, stavící na jednu stranu bojovnou hrstku technoanarchistů proti všemocné mašinérii amerického impéria na straně druhé. Ale fakta o Toru nejsou tak zřejmá nebo

jednoduchá, jak tito lidé tvrdí...

Začněme od začátku: Tor byl vyvinut, vytvořen a zaplacen americkým vojensko-průmyslovým a špionážním komplexem. Původním – i současným – účelem Toru je skrýt online identitu vládních agentů a jejich spolupracovníků v poli: při získávání informací, plánování operací, poskytnutím způsobu informátorům, jak se hlásit svým řídicím zpravodajcům a podobně. Toto je sice známo, ale nepříliš široce, a propagátory Toru to samozřejmě nijak zdůrazňováno není.

Stačí rychlý pohled pod pokličku Toru, abychom se přesvědčili, že prakticky všichni lidé zapojení do vývoje této technologie byli, či stále jsou, placeni Pentagonem nebo jiným spřízněným chapadlem amerického imperiálního leviathana. To platí i pro Rogera Dingledina, který vytvořil technologii díky různým vojenským a federálním kontraktům. Dingledine dokonce strávil celé léto na praxi v NSA.

Pokud si přečtete obligátně malým písmem psané podmínky použití na webu Toru, zjistíte, že americká vláda jej stále aktivně využívá:

> „Složka amerického námořnictva využívá Tor pro získávání zpravodajských informací z otevřených zdrojů a jeden z jejích týmů využil sítě během nedávného nasazení na Středním východě. Bezpečnostní složky jej užívají, aby při návštěvách webů nezanechaly vládní IP adresy v jejich lozích a pro bezpečnost při zpravodajských provokačních operacích (sting operation – operace s agenty-provokatéry, pozn. DP).“

NSA? Ministerstvo obrany? Americké námořnictvo? Policejní sledování? Co se to sakra děje? Jak mohl být nástroj na ochranu soukromí vytvořen stejnými vojenskými a bezpečnostními agenturami, před nimiž nás měl chránit? Je to trik? Podvod? Návnada? Možná jsem jen paranoidní...

Bohužel se však nejedná o absurdní spikleneckou teorii, ale o syrovou pravdu.

Stručná historie Toru

Počátky Toru se datují do roku 1995, kdy vojenští vědci v Naval Research Laboratory začali s vývojem maskovací technologie, která by znemožňovala vystopování něčí internetové aktivity. Pojmenovali ji „onion routing“ (cibulové směrování – více informací česky zde, pozn. DP) – metoda přesměrování internetového provozu do paralelní *peer-to-peer* sítě a jeho náhodného „odrážení“ před odesláním do konečné destinace. Původní myšlenka spočívala v dostatečném pohybu s cílem zmást a ztížit odentifikaci zdroje a cíle a znemožnění případnému pozorovateli určit, kdo jste nebo kam na internetu chodíte.

Cibulové směrování se podobá skořápkám s vaším surfováním: člověk, co se vás pokouší sledovat vidí, kam jde kulička, ale nevidí, kde vyjde.

Vývoj technologie sponzoroval Office of Naval Research a DARPA. V rané fázi byli hlavními vyvojáři Paul Syverson, Michael Reed a David Goldschlag – všechno vojenští matematici a systémoví vývojaři na výplatní pásce Naval Research Laboratory, pracující uprostřed obří spojené vojenské základny Anacostia-Bolling na jihovýchodě Washingtonu, D.C.

Původním účelem cibulového směrování nebyla ochrana soukromí – přinejmenším v tom smyslu, jak si jej většina lidí představuje. Účelem bylo umožnit zpravodajcům a vojákům pohybovat se tajně online bez obav z odhalení někým, kdo by monitoroval jejich internetovou aktivitu.

„Jak komunikace na vojenském stupni ochrany stále více závisí na veřejné komunikační infrastruktuře, nabývá na důležitosti využívání této infrastruktury způsoby, které jsou odolné proti zpravodajským analýzám (traffic analysis). Může být také užitečné komunikovat anonymně, například při shromažďování zpravodajských informací z veřejných databází," vysvětlovala studie z roku 1997 v The Naval Research Labs Review, který popisoval ranou verzi cibulového směrování.

Během 90. let, jak se šířilo užívání internetu a jeho infrastruktura bytněla a narůstala – potřebovali „špioni" skrýt svou jasně viditelnou online identitu. Agent v utajení sedící v hotelovém pokoji v nepřátelské zemi nemohl jednoduše ve svém prohlížeči otevřít CIA.gov a přihlásit se, aniž by nebylo každému, kdo by monitoroval jeho připojení okamžitě jasné, o koho jde. Stejně tak nemohl vojenský rozvědčík infiltrovat možnou teroristickou skupinu, maskující se jako fórum na ochranu práv zvířat, pokud si musel vytvořit účet a hlásit se pod IP adresou z vojenské základny.

A právě tady vstupuje na scénu cibulové směrování. Jak vysvětluje Michael Reed, jeden z jeho vynálezců, prvotním cílem bylo poskytnout krytí pro vojenské a zpravodajské online operace – vše ostatní bylo druhotné:

> „Prvotní *OTÁZKA*, vedoucí k vynálezu cibulového směrování zněla: ‚Dokážeme vytvořit systém, který umožňuje dvousměrnou internetovou komunikaci, jejíž původ a místo určení nelze určit ve středních článcích řetězce?' *ÚČELEM* bylo vytvoření aplikace pro Ministerstvo obrany/zpravodajské agentury (shromažďování informací z otevřených zdrojů, krytí aktivních spolupracovníků v předpolí apod.). Nikoliv pomoc disidentům v nedemokratických zemích. Nikoliv nástroj pro zločince, aby za sebou zametli své elektronické stopy. Nikoliv prostředek pro uživatele torentů, aby se vyhnuli stíhání svazů na ochranu autorských práv MPAA/RIAA. Nikoliv poskytnutí způsobu desetiletému dítěti, jak obejít protipornografický filtr. Samozřejmě jsme nepochybovali, že nevyhnutelně dojde i k takovým způsobům využití této technologie, ale to nehrálo při řešení zadaného problému žádnou roli (a pokud by nám zmíněná využití technologie poskytly rušnější internetový provoz, v němž by se původně zamýšlené využití snáze skrylo, tím lépe… Což jsem také jednomu nepříliš nadšenému důstojníkovi řekl.)"

Řešení problému nebylo dle všeho snadné. Vývoj cibulového směrování postupoval pomalu a několik vývojových verzí bylo zavrženo. Sedm let po svém začátku, v roce 2002, se však projekt posunul do nové a aktivnější fáze. Paul Syverson z Naval Research Laboratory u něj sice zůstal, přišli však dva noví kolegové z MIT: Roger Dingledin a Nick Mathewson. Ti sice nebyli zaměstnanci Naval Labs, ale měli smlouvy s DARPA a s Center for High Assurance Computer Systems U.S. Naval Research Laboratory. Několik dalších let tito tři muži pracovali na novější verzi cibulového směrování, která později vešla ve známost pod názvem Tor (zkratka projektu The Onion Routing, pozn. DP).

Velice záhy si výzkumníci uvědomili, že vytvoření systému, anonymizujícího pohyb nestačí – ne pokud by jej využívali výhradně lidé z armády a zpravodajských služeb. Aby „špioni" snadno splynuli, museli Tor začít využívat nejrůznější skupiny obyvatelstva: aktivisty, studenty, výzkumníky z korporací, matky v domácnosti, novináře, dealery drog, hackery, šiřitele dětské pornografie, cizí agenty, teroristy – čím pestřejší společnost, tím snadněji mohli vládní agenti splynout s davem.

Tor bylo také třeba přesunout ze základny a zbavit spojení s Výzkumnou laboratoří námořních sil. Jak řekl Syverson tiskové agentuře Bloomberg v lednu 2014: „Pokud je systém určený jen námořnictvu, všechno co z něj vyjde, má očividnou spojitost s námořnictvem. Potřebujete mít síť, která přenáší internetový provoz i ostatních uživatelů."

Dingledine řekl totéž už o deset let dřív na konferenci Wizards of OS v Německu:

> „Americká vláda prostě nemůže provozovat anonymizační síť a pak ji využívat jen pro svou potřebu. Pak by si totiž lidi pokaždé, když by se odtud někdo připojil, řekli: ‚No jo, další agent CIA,' pokud by tu síť využívali jen oni."

Spotřebitelská verze Toru měla být přístupná každému a – což je neméně důležité – každému by nakonec umožnila spustit přenosovou relaci Toru (entry/exit nodes), třeba i z osobního počítače. Cílem bylo vytvoření obří crowdsourcingové sítě ve stylu torrentů s tisíci dobrovolníků po celém světě.

Na konci roku 2004, když byl Tor připraven k použití, seškrtalo americké námořnictvo většinu dotací, vydalo jej jako otevřený software a, což je divné, předalo projekt Electronic Frontier Foundation.

Dave Maas z EFF mi e-mailem sdělil: „Financovali jsme práci Rogera Dingledina a Nicka Mathewsona jeden rok od listopadu 2004 do října 2005 částkou ve výši 180 000 dolarů. Pak jsme figurovali jako sponzoři projektu, dokud za další rok či dva nezískali status nadace ve smyslu zákona 501 (c)(3). Během té doby jsme za projekt utržili méně než 50 000 dolarů."

V prohlášení z prosince 2004, v němž EFF deklarovala svou podporu Toru, se organizace jaksi náhodou zapomněla zmínit o skutečnosti, že tento anonymizační nástroj byl vyvinut v prvé

řadě pro vojenské a zpravodajské využití. Namísto toho se text prohlášení soustředil čistě na schopnost Toru ochránit svobodu projevu v éře internetu před despotickými režimy.

„Tor a EFF k sobě dokonale hodí, jelikož jedním z našich hlavních cílů je ochrana soukromí a anonymity uživatelů internetu. Tor umožňuje lidem uplatňovat jejich prvním dodatkem ústavy zaručené právo na svobodný a anonymní projev online," řekl technologický manažer EFF Chris Palmer.

Později se v online materiálech EFF začaly objevovat zmínky o původu Toru v Naval Research Lab, ale spojení bylo zlehčováno slovy, že „to je minulost." Mezitím organizace stále Tor vytrvale propagovala označením za mocný nástroj ochrany soukromí:

> „S Torem je vaše surfování bezpečnější."

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