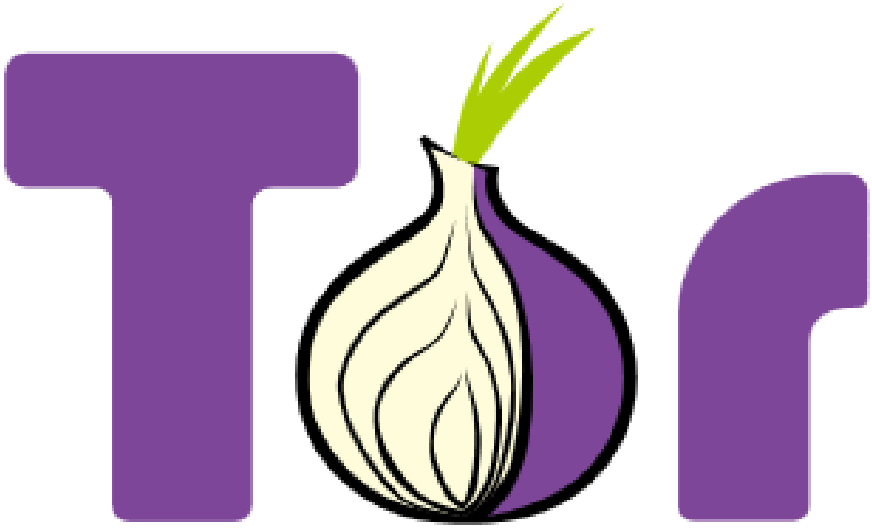
Počítačové siete - Tor sieť :)

Typ anonymizačnej siete. Najväčšia a najznámejšia.



Masová dostupnosť Internetu priniesla nový pohľad na medziľudskú komunikáciu. Väčšina používateľov si ani neuvedomuje, koľko zneužiteľných osobných údajov sprístupňuje. Na ochranu súkromia preto vznikli anonymizačné siete.

Svet sa vďaka Internetu zmenšil a komunikácia medzi ľuďmi sa neuveriteľne zintenzívnila. Spočiatku toto nové médium predstavovalo problém pre štátne zložky a ich nepružné nástroje kontroly. Domnelá aura anonymity na internete sa však vytratila pred mnohými rokmi.

Pozor na súkromie!

Štáty a štátne inštitúcie sa prispôsobili tejto relatívne novej forme komunikácie. Do platnosti vstúpili legislatívne úpravy, ktoré prikazujú poskytovateľom internetového pripojenia uchovávať údaje o aktivite používateľov a sprístupňovať ich na požiadanie štátnym orgánom. Ako internet preniká do každodennej ľudskej činnosti, štát, ale aj nežiaduce osoby či inštitúcie kontrolujú občanov omnoho efektívnejšie. Využívanie agentov a analytikov na prácne získavanie informácií v teréne, analýza odpočutých telefonátov a pošty mali v porovnaní s dátami získanými pomocou informačných technológií minimálny efekt. Už malý úsek zachytených dát stačí záujemcovi na to, aby si poskladal profil osoby, jej záujmy, preferencie alebo obchodné aktivity. Pálčivejší je problém ochrany súkromia alebo ľudskoprávnych aktivít v autoritatívnych a diktátorských štátoch.

Tak získavajú anonymizačné siete životne dôležitý význam.

Údaje zabalené do cibule

Najväčšia a najznámejšia z anonymizačných sietí je Tor. Jej funkčná verzia vznikla už v roku 2002 pod pôvodným názvom TOR (The Onion Router/ vrstvové smerovanie, metaforicky *cibuľové* balenie dát do viacerých šifrovaných vrstiev). Každodenne sa na Tor pripája približne 400 000 používateľov. Anonymizačné siete chránili vo veľkej miere aj organizátorov protestov po prezidentských voľbách v Iráne alebo počas Arabskej jari. Použitie Toru ich nielen chránilo, ale aj znemožňovalo represívnym zložkám blokovanie ich stránok.

Výhodou Toru je jednoduché použitie. Posledné verzie nevyžadujú osobitné inštalovanie lokálneho proxy servera. Používateľ si nemusí nastavovať ani prehliadač, stačí, keď si nainštaluje Tor Browser Bundle, ktorý obsahuje všetko potrebné vrátane prehliadača.

Tor aj pre mobily

Dnes sú prístupné dokonca aj mobilné riešenia ako Orweb pre Android alebo Onion Browser pre iOS (predtým známy ako iPhone OS). Program Tor oddeľuje identifikáciu používateľa podľa IP adresy a smerovanie jeho požiadaviek. Požiadavky potom zašifruje do viacerých vrstiev a odošle ich do Tor siete, kde prejdú viacerými servermi náhodných používateľov a vystúpia v niektorom zo stoviek výstupných serverov. Viacvrstvové (cibuľové) šifrovanie poskytuje bezpečnosť medzi stanicami. Poskytovateľ internetového pripojenia teda nevie, kam sa používateľ snaží pristupovať a čo je obsahom informácií. V žiadnom prípade však Tor siete nezaručujú bezpečnosť a utajenie *end to end* dát, pokiaľ to nepodporuje cieľový server.

Zradné výstupné servery

Ak chce napríklad používateľ pristupovať na server progressbar.sk cez Tor sieť, požiadavka sa zabalí a zašifruje už v jeho zariadení a odošle do Tor siete. Poskytovateľ pripojenia vie, že používateľ pristupuje do Tor siete, ale nepozná cieľový server a z neho vyžiadané informácie. Cez Tor sieť prejdú tieto informácie tiež zašifrované až po jeden z výstupných serverov, ktorý slúži ako brána do internetu. Tam ich už však vidno!

Výstupnú bránu si môže nainštalovať ktorýkoľvek používateľ Tor klienta. Zároveň môže slúžiť aj ako server, preto sa nedá vylúčiť, že na tomto výstupnom serveri je nainštalovaný softvér na odchytávanie komunikácie. Dotyčný *dátový pytliak* síce nebude vedieť, kto si informácie zo servera progressbaru vyžiadal, ale uvidí ich obsah. Ak používateľ pristupuje na servery, kde sa nedelí o svoje dáta, nepredstavuje to vážne riziko. Môže to byť nebezpečné, ak nepoužíva šifrované spojenie pre interaktívne služby ako napríklad e-maily alebo sociálne siete.

Https a neplatné certifikáty

Riešením je dávať si pozor a používať *end to end* šifrovanie tam, kde je to potrebné. Používateľ môže použiť adresu https://progressbar.sk, kde písmeno s za http znamená secure, teda bezpečné spojenie. Takto je spojenie medzi výstupným serverom Toru a serverom progressbar šifrované, pokiaľ správca výstupného servera nepodhodil iný certifikát. V súčasnosti, žiaľ prevádzkovatelia výstupných uzlov bežne takéto útoky vykonávajú. Na neplatný či podozrivý certifikát by mal upozorniť prehliadač, alebo by si ho mal používateľ skontrolovať sám. V prípade správneho použitia šifrovaného spojenia správca výstupného servera síce vidí, kam smeruje požiadavka, ale nevidí obsah. Poskytovateľ pripojenia teda vie, že používateľ pristupuje do Tor siete, servery v Tor sieti si však len posúvajú požiadavku a vedia identifikovať iba cestu medzi nimi. Výstupný server vie, že niekto anonymne pristupuje na server progressbar.sk, ale nevie, čo je obsahom a server progressbar nevie identifikovať používateľa, ktorý k nemu pristupuje. Tým sa značne zvyšuje anonymita a aj diskrétnosť pripojenia. No vždy treba mať na pamäti, že všetko môže obsahovať dnes ešte neznáme citlivé stránky a zohľadniť toto riziko.

Bitcoinová Hodvábna cesta

Do Tor siete boli prenesené aj ďalšie služby na bezpečné sprístupňovanie webových stránok. Ktorýkoľvek používateľ tak môže v Tor sieti zapnúť svoj server a poskytovať služby bez toho, aby bola odhalená jeho reálna lokalita alebo IP adresa. Služby sú prístupné pod pseudoadresou s koncovkou .onion. Pristupovať na ne sa dá po pripojení na Tor sieť, kde do prehliadača stačí zadať .onion adresu, alebo v prehliadači pripojenom v klasickom internete za .onion pridáme koncovku .to. Prístupných je množstvo bezpečných e-mailových služieb, wiki a obchodných aktivít. Neexistuje tu automatické vyhľadávanie stránok, je potrebné poznať presnú adresu. Zoznam stránok uvádza napríklad Hidden Wiki, http://kpvz7ki2v5agwt35.onion(.to).

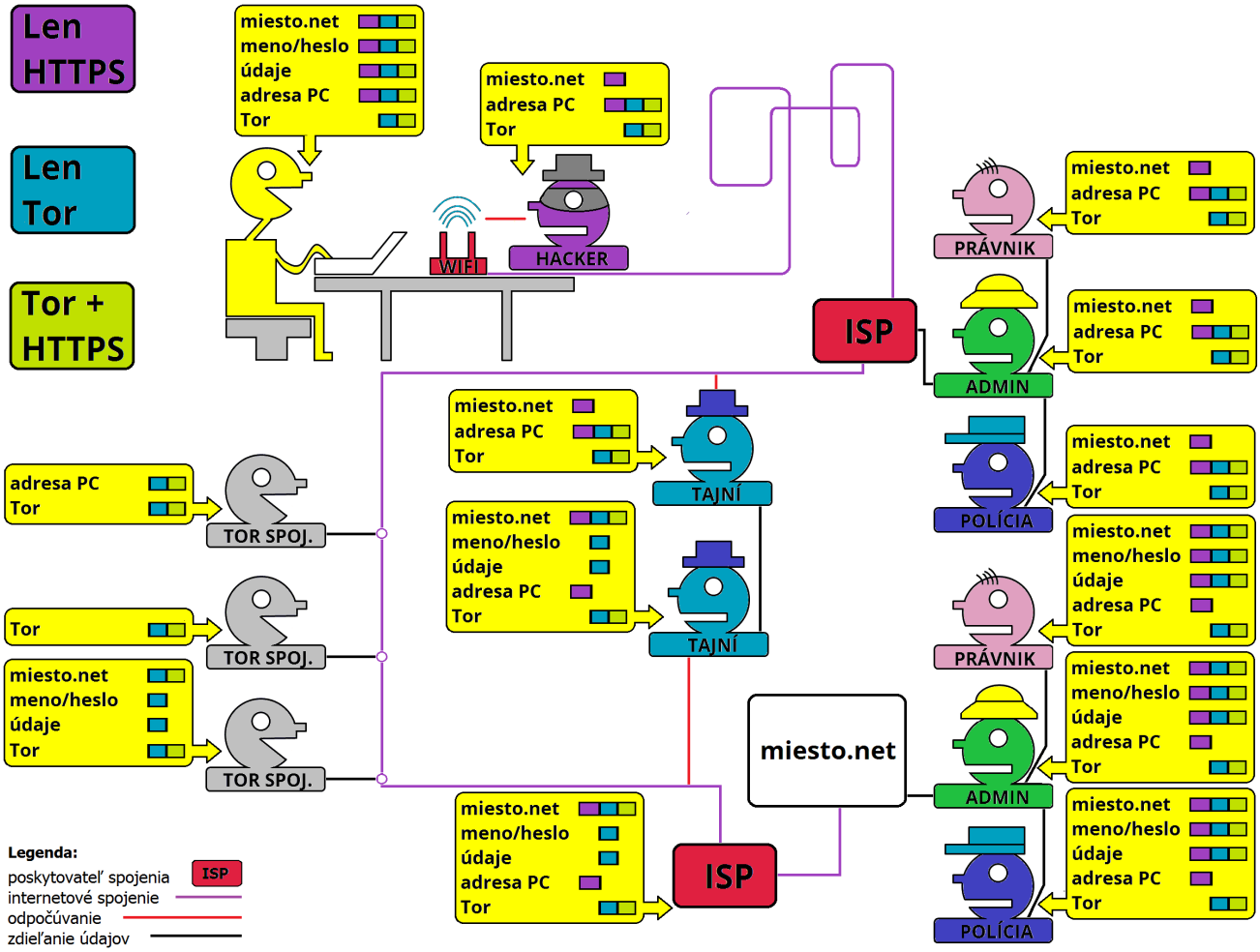
Jedna z najznámejších a aj komerčne najúspešnejších Tor služieb je tzv. Hodvábna cesta (Silk Road). Je to anonymný obchodný portál, kde si používatelia môžu vytvoriť účty a predávať tovar alebo služby. Platia za ne bitcoinmi, elektronickou menou. Kombináciou Toru a bitcoinu používatelia majú k dispozícii veľmi silné nástroje na anonymné obchodovanie na oboch stranách. Silk Road odštartovali v roku 2011 a za rok 2012 sprostredkoval obchody odhadom za viac ako 20 miliónov dolárov.

Kto používa Tor siete

Skryté služby v rámci Tor siete obľubujú a využívajú najmä rôzni hacktivisti a politickí aktivisti. Prístupné sú rozličné diskusné fóra a informačné portály. Relatívne dlho bola Tor sieť najmä doménou ľavicových aktivistov, ale v malej miere sa objavil aj pokus o prienik neonacistov a militantných rasistov. Vážnejší prienik tejto skupiny do Tor služieb však nenastal.

Služby v Tor sieti do veľkej miery chránia administrátorov a autorov, teda značne znemožňujú postih štátnym represívnym zložkám. Preto okrem ľudskoprávnych aktivistov priťahujú aj administrátorov služieb, ktoré by sme mohli označiť ako škodlivé. Zaujímavý je príklad samoregulácie, keď v roku 2011 skupina Anonymous zasiahla proti najväčšiemu úložisku detskej pornografie v Tor sieti. Cez nájdené slabšie ohnivko v PHP kóde získali prístup k serveru, ktorý odstavili a následne na internete uverejnili zoznam používateľov a ich údaje.

Keďže Tor siete vytvorili ľudia pracujúci v bezpečnostných zložkách, aby si mohli vymieňať údaje bez vystopovania, využívajú ich aj rôzne štátne rozviedky a kontrarozviedky. Predpokladá sa, že v roku 2012 pochádzali dva milióny dolárov rozpočtu Tor Project od vlády Spojených štátov amerických, švédska vláda a iné organizácie dopĺňali zvyšných 20 %.



Ukážka toho, kto a ako využíva tor siete

Zdroje

Použitá, citovaná a odporúčaná literatúra

- ***Tor siete*, Quark, apríl 2013**
- ***Anonymizačné siete TOR a I2P pod lupou***
- ***Internetová anonymita - nutnosť pre zachovanie slobody?***

Obrázky

- **Obrázok 1 - pôvodný obrázok**
- **Obrázok 2 - pôvodný obrázok a *Tor siete*, Pavol Draxler, Quark, apríl 2013**