Technicky a srozumitelně – jak funguje vládní cenzura webů přes DNS? Jaké další cenzury přicházejí? Jak to obejít?

- CZ24 News | 28. února 2022

ČESKO: Angažovaní aktivisté z CZ.NIC a vlády SPOLU se rozhodli, že zavedou cenzuru internetu. Naštěstí se zatím neodhodlali k likvidaci webů, ale pouhému schování DNS záznamů, které slouží pro překlad srozumitelných názvů webů na IP adresy. Zde je i laikům srozumitelné vysvětlení, jak jejich cenzura technicky funguje, návod na obejití – a zároveň řešení typických uživatelských problémů a otázek. A náhled co za cenzuru technicky přijde dál, protože už na tom pracují.

Vsuvka – liberální vzkaz CZ.NIC a cenzorům

Ale nejdřív malá vsuvka a vzkaz cenzorům (ostatní čtenáři přeskočí odkazem zde až na popis cenzury a protiopatření). Vládo a CZ.NIC, my dva bychom měli jakože být na té samé straně konfliktu. Jak vidno z mých postů, jsem od začátku proti ruské invazi na Ukrajinu. Ohromně fandím Ukrajincům, kteří proti přesile útočníků brání svou domovinu, a zejména obráncům Kyjiva. Jenže vy pokrytecky taháte do ČR pod záminkou boje proti Putinovi přesně Putinovu represi, netoleranci a nesvobodu.

Ruská média mají povinnost informovat pouze v souladu s ruskými vládními zdroji a vaše pojetí „boje proti dezinformacím“ je limitně stejné. I neformální „dobrovolnou“ cenzuru internetu kopírujete od Putina. „Zavádět Putinismus proti Putinovi“ je chucpe.

Základní lidská práva a svobody jsou univerzální a proto mnohem důležitější, než dočasné krize. Přesně naopak – právo a svoboda musejí být bráněny *zejména* v době krize, kde se každý ničema snaží pod praporem „inter arma enim silent leges“ prosadit ničemnosti, které by mu jinak neprošly.

Navíc ve svých zdůvodněních výslovně lžete, že blbá ruská propaganda údajně nějak „ohrožuje bezpečnost ČR“. Ne neohrožuje – nikoho nevyzývá např. sabotovat dodávky zbraní na UA (k čemuž by opět nebyla třeba cenzura, protože to by byl nezávislý TČ). Jen to jen konkurence vašich názorů, která je třeba nehorázná a nechutná – ale to vám nedává žádné právo zakroutit krkem pluralismu, svobodě slova či opozici.

Jste nezápadní neliberálové, kteří kopírují represivní, autoritářské či totalitní režimy a pošlapáváte veškerou filosofii svobody slova, právního státu i lidských práv. Jste stejní jako čínští a ruští cenzoři a navrch lháři a pokrytci, a to vám nebudu tolerovat!

Jak funguje systém DNS a cenzura založená na DNS?

Každý server v internetu má tři pomyslné adresy.

- Fyzickou adresu své síťové karty (MAC), která je však schovaná a vy ji nepotřebujete.
- IP adresu, což je série 4 číslic (nebo 8×4 znaků v případě málo využívaného protokolu IPv6) která skutečně zajišťuje síťové spojení se serverem.
- Lidsky zapamatovatelnou písemnou adresu, kterou zadáváte do prohlížeče. Ta se technicky jmenuje „plně specifikované doménové jméno počítače“ – plně proto, že se jedná o více jmen

oddělených tečkami. Zkratka je FQDN, zapamatujte si ji.

Nepřesně a zjednodušeně řečeno překlad z FQDN na IP adresu řeší tzv. DNS servery – Domain Name Translation. Ty – což je pro cenzuru zásadní – fungují hierarchicky. Protože IP adres vázaných na domény jsou na světě miliardy, kdyby měl každý server znát všechny, zhroutil by se. Když tedy vezmete adresu např. www.novinky.cz, překlad začne od konce. Takzvanou doménou 1. a nejvyššího řádu, TLD, což je to „.cz“.

Prohlížeč tedy vezme z požadované FQDN segment „.cz“ a obrátí se na kořenový server DNS. Těch je na světě pouze těchto 13. A zeptá se – koho se mám zeptat ohledně domény s TLD „.cz“?

Odpověď zní – zeptej se sdružení CZ.NIC, které spravuje národní doménu nejvyššího řádu „.cz“. Adresa jeho DNS serverů je „a.ns.nic.cz“ a IP adresa tohoto DNS serveru je „194.0.12.1“.

Takže prohlížeč pošle druhý dotaz na DNS server „a.ns.nic.cz“: jakého DNS serveru nižší úrovně se mám zeptat na IP adresu doménu 2. řádu „novinky“ na TLD „cz“?

A odpověď zní třeba – zeptej se „ans.seznam.cz“, jehož IP adresa je „77.75.74.80“. Protože Novinky provozuje na svých serverech Seznam, který vlastní stovky domén – a proto právě jejich organizace a její servery udržuje mapu, které jím vlastněné domény mají aktuálně jakou IP adresu.

Takže se prohlížeč konečně zeptá DNS serveru „ans.seznam.cz“ – jakou IP adresu má váš server vašeho webu „www.novinky.cz“? DNS server odpoví IP adresu 77.75.74.173. A to je adresa serveru, na kterém běží web, který si chcete zobrazit. K němu se potom připojí váš počítač.

(Pokud si s tímto chcete hrát, můžete si rozběhnout svůj vlastní DNS server např. od Technitia a pak sledovat DNS frmol na síti programem Wireshark.)

Cenzura pak funguje nesmírně jednoduše: správce domény nejvyššího řádu prostě zablokuje, resp. smaže záznam, jakého dalšího serveru v hierarchii se máte zeptat pro danou doménu.

Takže na a.ns.nic.cz přijde dotaz „koho se mám zeptat na ‚novinky.cz‘“? A DNS server odpoví – nevím, žádná taková doména neexistuje a nikdo ji nezná! Takže není možné se zeptat DNS serveru daného webu, kam se máte připojit, a vše skončí neúspěchem ještě než to začalo.

Serveru se nic nestane, funguje dál jako předtím – ale nikdo na něj netrefí přes doménu, protože ta se tváří že najednou neexistuje. Případně se přesměruje na nějaké parazitické stránky typu „tento web je blokován a znamenáme si váš nekalý zájem, bu bu bu.“

Nestačí zadat IP adresu? Nestačí – kvůli přepisům domén na adresáře na sdíleném serveru

Mohlo by se zdát, že si stačí zapsat na papírek IP adresy a máte vyhráno. Jenže je to složitější. Ukažme si to názorně. Dotazovat se DNS serverů na IP adresy můžete nástrojem NSLOOKUP, který je součástí snad každého operačního systému.

Spusťte si příkazovou řádku (na Linuxu alt+F2, na Windows start > spustit > napište CMD a odklikněte).

V příkazové řádce pak napíšete „nslookup novinky.cz“ (bez uvozovek) a odklepnete Enter. Výsledek vypadá takto:

```
C:\Users\mrcas>nslookup novinky.cz
```

```
Server: localhost
Address: ::1

Non-authoritative answer:
Name: novinky.cz
Addresses: 2a02:598:3333:1::3
2a02:598:4444:1::3
77.75.75.173
77.75.74.173
```

Znaky s dvojtečkami jsou adresy typu IPv6, tu tu nebudeme řešit. Relevantní je čtyřčíslí oddělené tečkami. To si zkopírujeme.

Zkuste si do prohlížeče zadat jako adresu webu 77.75.75.173 a zobrazit jej. Nefunguje to! Namísto zpravodajství Novinek se IP adresa přesměrovala na FQDN „media.novinky.cz“ a objevila se chyba HTTP403, která znamená „Nejste oprávněni číst tento soubor“. Proč?

Na jednom serveru a IP adrese běží typicky více webů. V našem případě nejen „www.novinky.cz“ ale i „media.novinky.cz, „special.novinky.cz“ a další. (Tip: chcete odhalit, co všechno kohabituje na nějaké IP adrese? Do vyhledavače jako DuckDuckGo zadejte speciální klíčové slovo ip:, jako ip:77.75.75.173.)

Ty se liší pouze tím, v jaké složce serveru každá webová prezentace žije. To má každý server jinak, například na Wedosu se jedná o adresáře jmenné konvence „www/domains/domena.tld“. Tzn. kdyby byly novinky hostované na Wedosu, jejich skutečná adresa by byla „77.75.75.173/www/domains/novinky.cz“ (IP by samozřejmě byla jiná).

Když tedy zadáte jen IP adresu, server neví, kterou složku chcete. Takže vám hodí nějakou výchozí chybu a končíte.

Oproti tomu pokud zadáte do prohlížeče FQDN, prohlížeč si nejprve z DNS serverů zjistí IP adresu serveru a naváže s ní kontakt – ale potom prohlížeč předá serveru na uvítanou i FQDN ze své adresní řádky.

A server poté na své straně provede složitou magii překladů a přesměrování, které se říká „HTTP rewrite rules“, a v jejímž důsledku se adresní řádek tváří, že je v něm třeba „novinky.cz/aktuality“, ačkoli reálně je v něm soubor třeba (vařím z vody) „server.seznam.cz/www/novinky/dennitisk/skript.aspx?id=19983“. Tohle si každý server může dělat jak chce.

Takže vám nestačí jen IP adresa – musíte i říci serveru, jenž na té IP adrese běží, jakou FQDN po něm chcete. Jen na základě této informace vás potom server podle toho patřičně přesměruje do té správné složky, kde běží požadovaný web.

V políčku „adresa“ prohlížeče tedy musí být FQDN, nikoli IP adresa. Ovšem zároveň potřebujete s touto FQDN chcete propojit IP adresu, kterou vám oficiální DNS servery drze cenzurují. Jak na to?

Soubor HOSTS – když oficiální DNS server cenzuruje, uděláme si primitivní vlastní

Každý operační systém má soubor HOSTS. Je to primitivní ekvivalent DNS serveru, který se skládá pouze z tabulky o dvou sloupcích. V levém sloupci je IP adresa. V pravém sloupci je FQDN, která se

na danou IP adresu má přeložit.

Na Linuxu je cesta k němu „/etc/hosts“ a na Windows je odnepaměti v adresáři systému Windows, podsložce“system32\drivers\etc\hosts“.

Snadno si v HOSTS souboru můžete vyrobit vlastní jakoby DNS záznam. Struktura souboru je takováto:

```
#Copyrightové kecy na začátku
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
```

Mřížka na začátku řádku je tzv. zakomentovaná – tzn. systém ji celou ignoruje. Pokud mřížku smažete, řádka se aktivuje.

Syntaxe je IP adresa – mezery nebo tabulátory – FQDN. A pozor, už tady je jsou dvě drobné zrady. Zaprvé, FQDN neobsahuje znaky jako „http://“, který vám zobrazí prohlížeč. To je totiž identifikace protokolu pro prohlížeč, ale nikoli součást FQDN.

Zadruhé – je zásadní rozdíl mezi „www.novinky.cz“ a „novinky.cz“. Novinky jsou doména druhého řádu, ale „www“ je zcela samostatná subdoména třetího řádu pod doménou „novinky“ pod TLD „.cz“! Na serveru by FQDN s „www“ a bez „www“ mohly být samostatné složky, a tedy i samostatné rozdílné weby. Že to servery často maskují a pro vaše pohodlí automaticky přesměrovávají subdoménu „www“ na stejný obsah jako doménu 2. řádu je sice hezké, ale když si děláte vlastní DNS záznam, musíte tento rozdíl respektovat.

V HOSTS souboru si můžete přidat i falešné FQDN pro své lokální adresy. Například pokud máte síťovou tiskárnu na adrese 192.168.1.52 a síťový disk Synology na adrese 192.168.1.101, můžete do HOSTS souboru přidat řádky
`192.168.1.52 printer.lan`
`192.168.1.100 disk.lan`
A odpříště namísto IP adres napříště do nastavení a prohlížeče zadávat uživatelsky mnohem přívětivější „printer.lan“ a „disk.lan“ jako kdyby to byly domény na internetu. Nám se ale samozřejmě jedná o obcházení cenzury.

Praktický návod – zjišťujeme (necenzurované) IP adresy a zálohujeme si je v HOSTS

Pokud už je nějaký server cenzurovaný, máte problém. Protože jsou totiž DNS servery hierarchické, jejich údaje se propagují od autoritativních po ty méně. Takže když se DNS servery CZ.NIC začnou tvářit, že „zlobivé dezinformační weby“ nikdo nezná, aby je zcenzuroval… Ostatní DNS servery si řeknou „aha, tak to asi vypli“ a smažou si své lokální kopie.

To trvá až několik hodin, což nesmírně pohoršilo naše cenzurychtivé spoluobčany. Ale nakonec jsou vyzmizikované odevšud. IP adresu by vám někdo musel říci offline ze svých před-cenzurních poznámek.

Proto se bavíme o preventivním scénáři, kdy si zjistíte IP adresu požadované domény a uděláte si kopii jejího DNS záznamu do souboru HOSTS. V každém operačním systému jsou k tomu předpřipravené nástroje.

Chcete-li zjistit IP adresu serveru, máte dvě možnosti. Buď si na internetu vyhledáváte tzv. WHOIS službu, např. www.who.is nebo mnohem schopnější DNSchecker.org, která vám ukáže přímo DNS záznamy pro daný web.

Nebo použijete výše zmíněný program NSLOOKUP. Jak zjistíme novinky víme, co jiný server – už potenciálně zcenzurovaný?

```
C:\Users\mrcas>nslookup dfens-cz.com
Server: localhost
Address: ::1

Non-authoritative answer:
Name: dfens-cz.com
Addresses: 2a02:2b88:1:4::99
46.28.106.34
```

Znaky s dvojtečkami jsou adresy typu IPv6, tu tu nebudeme řešit (ač sama o sobě někdy umí cenzuru DNS obejít.) Relevantní je čtyřčíslí oddělené tečkami. To si zkopírujeme.

Teď otevřeme soubor hosts. Zádrhel: soubor nemá příponu, takže operační systém se dožaduje nápovědy, jak jej otevřít. Nejsnazší řešení: neproklikáváme se, ale použijeme tento příkaz:

```
notepad %windir%\system32\drivers\etc\hosts
```

Takový příkaz se dá zadat buď do dialogu spustit. Nabídka Start > Spustit > zkopírujte tam příkaz viz výše a odkliknete. Nebo můžete použít klávesovou zkratku WinKey+R (WinKey je klávesa s logem Windows mezi levým Alt a Ctrl), která vám také zobrazí dialog Spustit. Nebo můžete příkaz zadat do příkazové řádky CMD. To bude nejlepší řešení.

Co příkaz udělá? Jen to, že vezme program Notepad – „poznámkový blok“, který je primitivním editorem textových souborů, a přikáže mu otevřít soubor hosts.

Z příkazového řádku či dialogu spustit totiž můžete programy spouštět s tzv. parametry. To znamená, že pokud za jménem programu uděláte mezeru a něco připíšete, program si „to něco za mezerou“ vezme jako úokol pro sebe a něco s tím udělá. A jmenovitě program Notepad udělá s prvním parametrem za mezerou to, že jej zkusí otevřít jako cestu k souboru.

Znaky za mezeru příkazu jsou cesta k souboru HOSTS, který má Poznámkový blok otevřít. %windir% je tzv. systémová proměnná, protože složka Windows se může jmenovat různě a být na různém písmenu disku (třeba „C:\Windows“, ale i „C:\OldWindows“ nebo „D:\WindowsXPSP2“). Pokud použijete systémovou proměnnou %windir%, automaticky se místo ní doplní disk a cesta k momentálně aktivnímu systému Windows. Takto to funguje všude a neřešíte odlišnosti.

Pak do souboru HOSTS vložíme IP adresu, spoustu mezer (nebo dva tabulátory – klávesa „TAB“ nad CAPSLOCK) a naše FQDN. Pro případ novinek a DFENSu bude upravený soubor HOSTS vypadat takto:

```
# 127.0.0.1 localhost
# ::1 localhost
77.75.74.173 novinky.cz¨
77.75.74.173 www.novinky.cz
46.28.106.34 dfens-cz.com
46.28.106.34 www.dfens-cz.com
```

Uložit a máte hotovo. (Tip: můžete si do HOSTS přidat i jiné stránky pod vlastním aliasem a ten pak používat v prohlížeči. Např. pro naši vládu „82.117.137.222 banda-pokryteckych-cenzoru.cz“).

Ovšem pokud je server již cenzurován a IP adresu vám poslal kamarád, je potřeba ještě jeden krok. Váš operační systém si totiž může držet „otrávený“ DNS záznem od cenzorů v mezipaměti. Ten je nejprve nutné smazat, aby se namísto toho podíval do souboru hosts. (Totéž platí, pokud jste soubor hosts předělávali.)

Na Linuxu by mělo stačit restartovat prohlížeč (nebo službu DNS, přinejhorším celý systém.) Na Windows také restartujte prohlížeč, ale napřed vymažte dočasnou mezipaměť DNS příkazem

```
ipconfig /flushdns
```

A dostanete potvrzení ve smyslu

```
Successfully flushed the DNS Resolver Cache.
či
Mezipaměť DNS byla úspěšně vymazána
```

Nebojte se, ničím z tohoto nic nemůžete rozbít. Soubor HOSTS je normálně úplně prázdný, jediné dva předpřipravené řádky jsou zakomentované a tedy ignorované. Nejhorší co se může stát je, že byste do HOSTS zadali špatnou kombinaci adresy a FQDN a tím si danou FQDN omylem zablokovali. (Tip: takto si můžete snadno zablokovat nežádoucí servery – stačí jim v HOSTS souboru vytvořit řádky jako „127.0.0.1 nechteny-server.cz“).

A příkaz „ipconfig /flushdns“ smaže jen dočasnou mezipaměť výsledků dotazů na DNS servery, která se však okamžitě znovu zaplní úplně sama prostě tím, jak v prohlížeči (či HOSTS) dotazujete internetové adresy.

Možná potřebujete zvýšení oprávnění k úpravě souboru HOSTS

Další problém je, že v závislosti na vašem nastavení systému můžete potřebovat si zvýšit oprávnění. Systém se totiž snaží soubor HOSTS chránit před neoprávněnými úpravami – představte si, že by do něj např. nějaký virus zadal IP adresu phishingového serveru a k ní lživě přiřadil FQDN vašeho internetového bankovnictví!

K úpravě tohoto souboru jsou tedy potřeba administrátorská práva. Pokud nepoužíváte počítač pod administrátorským účtem, ale máte k němu heslo, můžete použít tento příkaz:

```
runas /user:administrator "notepad C:\windows\system32\drivers\etc\hosts"
```

Ten spustí výše uvedený příkaz pod uživatelem administrator a interaktivně se zeptá na heslo administrátorského účtu. Na Linuxu dostanete stejný výsledek příkazem
`sudo nano /etc/hosts`

Většina uživatelů novějších systémů Windows (vše od XP nahoru) ale má jediný účet, který má administrátorská oprávnění ale tváří se, že je nemá. Musíte mu říct a potvrdit, když a že je opravdu chcete použít.

To se dá udělat buď přes příkazovou řádku PowerShell, máte-li ji v systému, nebo klikáním přes grafické rozhraní.

Pokud je na vašem počítači nainstalován PowerShell (měl by být všude od Windows 7 později),

spustíte jej příkazem „powershell“ (opět ze Start>Spustit, nebo Winkey+R, nebo z příkazové řádky). Poté stačí zadat:

```
start-process notepad -argumentlist $env:WINDIR\system32\drivers\etc\hosts -verb RunAs
```

To dělá úplně totéž jako příkaz viz výše, akorát v prostředí PowerShell a s příkazem zeptat se uživatele, že chce povolit použití administrátorských práv.

Klikací alternativa je, že v nabídce Start ve vyhledávacím poli napíšete CMD, ale na výsledek hledání kliknete pravým tlačítkem, vyberete „Spustit jako administrátor“ a až na takto spuštěné příkazové řádce zadáte příkaz

```
notepad %windir%\system32\drivers\etc\hosts
```

Může stát cenzurovat i jinak, brutálněji? Může a už na tom pracuje. Co s tím?

Přes kolaboraci správce národní domény CZ.NIC dosáhne vláda jen na domény s koncovkou „.cz“, takže například servery na doménách „.info“ nebo „.com“ nedosáhne metodou blokace DNS.

Může ale přímo udeřit na provozovatele serverů a natvrdo je vypnout. S vydatnou podporou pokryteckých bolševických prý „bojovníků za svobodu internetu“ z Pirátské Strany si totiž vláda prosadila bezprecedentní zákon, že Policie smí kdykoli komukoli naprosto svévolně sestřelit stránky na 90 dní bez schválení soudem. Je to další z vládních pokusů o Putinizaci Česka, Putin si zavedl přesně totéž.

Tomu se prozměnu vyhne ten server, který je hostován v zahraničí a čeští Putinističtí cenzoři na něj nedosáhnou.

Takže ještě zbývá „jaderná varianta“ Velkého Čínského Firewallu. Blokovat přímo jakékoli spojení z ČR na dané servery nebo dokonce kusy internetu.

K tomu už vláda reálně sáhla. Oslovila s žádostí o cenzuru ISP a Peeringové uzly. ISP je váš poskytovatel připojení k internetu – ten zablokuje přímo vytvoření spojení na cílovou IP adresu, i když obejdete DNS blokaci.

Peeringový uzel pak znamená propojky jednotlivých ISP – takže i kdybyste byli u svobodného ISP, který odmítne kolaborovat s nelegálními Putinovskými cenzory… Nebude mu povoleno navázat spojení přes sítě jiných ISP. Žádný ISP totiž nemá spojení všude na všechny servery, ale navzájem si dovolují používat své sítě. „Přestupní stanice“ mezi sítěmi ISP a potom i mezi ISP a mezinárodním internetem jsou pak Peeringové uzly, a ty mohou efektivně zablokovat „nežádoucí“ přestupy a spojení.

Takto lze zařízнout nejen servery, ale třeba i všechno co se geograficky nachází v Rusku – prostě by byl na úrovni sítě Peeringů v CZ odříznut veškerý internetový provoz, který směřuje na protějšky-Peeringy v RU. I to někteří digitální bolševici otevřeně požadují právě v těchto dnech.

Na takto brutální blokaci na všech frontách po vysloveně Čínském komunistickém a Ruském Putinovském vzoru už nestačí žádné obcházení. Jedině síť Tor.

Proxy síť TOR – americký systém, jak obejít cenzuru čínských, ruských a nejnověji i českých digitálních bolševiků

Když Čína začala cenzurovat internet a nejrůznější bolševici po celém světě začali nahánět, zavírat a mučit nezávislé bloggery a internetové novináře, americká vláda a programátoři si sedli a vytvořili systém TOR – The Onion Router. Cílem bylo vytvořit nezablokovatelný, svobodný a anonymní internet pro disidenty.

Viděli jste někdy nějaký film o hackerech? Policisté tam vždy ukazují, jak sledují hackerovo připojení skákající mezi kontinenty – udeřil ve Washingtonu a oni jej sledují do Ria a odtamtud do Chartůmu a odtamtud do Moskvy a odtamtud do Pekingu až jej vysledují… Spojení ukončeno, zase nám unikl! No tak to je umělecká licence, ale přesně takto funguje TOR.

Vytvoří virtuální síť, kde si pokaždé zcela náhodně vybere několik prostředníků-uzlů, přes něž postupně proskáčete ze svého cenzurovaného a sledovaného internetu, až vypadnete na prostřednikovi-uzlu na opačné straně světa a teprve odtamtud se připojíte na požadovaný server. Z pohledu vládních fízlů se tedy nepřipojujete na nějaký zlolajný dezinfo server, nýbrž na jednoho z prostředníků sítě TOR. Tím se může stát kdokoli. A tudíž se vždycky dá vybrat nějaký uzel, který ještě není blokovaný. Ani Číňani to nezvládnou blokovat všechno.

TOR začnete používat prostě tak, že jdete na stránky TorProject.org a stáhnete si uživatelsky přívětivý balík systému TOR a k němu přimontovaného, lehce upraveného prohlížeče Firefox. Ten se nainstaluje na váš počítač „vedle“ normálního prohlížeče a internetu, po spuštění si vybere nějaký vstupní uzel, přeskáče přes půlku světa a dál jej používáte jako normálně.

Jakkoli TOR teoreticky slibuje nejen porážku cenzury, ale i anonymitu, v praxi na to nespoléhejte.

1. Zaprvé je značné množství uzlů vlastněné vládami a jejich tajnými službami s cílem odhalit ty, kteří se přes ně připojují. Hlavně čínskými, ale i americkými.
2. Zadruhé platí, že než aby se fízlové snažili porazit síť TOR, je mnohem snazší porazit IT bezpečnost uživatele TORu. Nasadit mu virus, nebo využít zranitelnost prohlížeče.
3. Zatřetí vlády vynalézají geniální metody, jak TOR deanonymizovat nepřímo. Europol a Interpol takto několikrát úspěšně deanonymizovaly uživatele TORu celoevropskou kolaborací ISP.
4. A začtvrté je směšně snadné někodo deanonymizovat zkorelováním unikátních stop, které za sebou zanechává. Například pokud je někdo tak hloupý, že se v TORu přihlásí do svého oficiálního mailu nebo ještě hůře sociální sítě. Nebo i jen využitím tzv. „fingerprintingu“ – kombinace všech měřitelných parametrů vyšeho počítače od údajů o baterii přes údaje o klávesnici, nainstalovaných fontech a zásuvných modulech, detailní verze všeho softwaru na počítači, až po rozlišení obrazovky a údaje o pseudonáhodném HTML5 Canvasu. Schválně si fingerprinting názorně vyzkoušejte, jak moc jste unikátní.

Nám však jde o poražení cenzury a to funguje vždy, dokud není trestné samotný TOR používat (jako v komunistické Číně a Putinově Rusku).

TOR se umí snadno dostat přes cenzuru ISP a Peeringových uzlů – prostě proto, že se nepřipojuje na

jimi blokovaný server, nýbrž na uzel TORu na opačné straně světa a až odtamtud na odříznutý server.

Klient TOR neřeší vše. Cenzurované servery se musí přesunout na darknet skrze VPS se službou .onion

Potíž je, že TOR ignoruje server HOSTS – je to proxy síť, takže DNS se řeší až na výstupním uzlu někde v Tramtárii. TOR má sice své vlastní mechanismy pro robustnější DNS ochráněné proti cenzuře, ale nejsou všemocné proti cenzuře národních správců DNS TLD jako náš Putinovský CZ.NIC. Ti fungují jako otrávená studna.

Takže máme soubor HOSTS, který nám umožní porazit cenzuru DNS.
A máme systém TOR, který nám umož ní porazit cenzuru odstřižení síťového provozu ISP a Peeringy.
Ale proti kombinaci obojího máme jen částečnou obranu, a přesně na to spoléhají cenzoři Vladimir Putin i Jana Černochová úplně stejně.

A to už vůbec nemluvím o tom, že pokud vláda ví, který webhosting provozuje server – může jej zcela bezzákoně a bez soudu šikanovat svévolným vypínáním na 90 dní „protože my chceme a máme právo silnějšího“. Bez odvolání, bez soudu, bez práva na spravedlivý proces. Zase po vzoru přesně toho Putina, proti kterému údajně bojujete, šmejdi pokrytečtí.

Jediné zcela neprůstřelné řešení tedy je, aby cenzurované servery začaly aktivně podporovat síť TOR – aby si zřídily i TORový webový server s příponou .onion. Paralelní síť webů, která funguje jen uvnitř TORu a na kterou nedosáhne žádná vládní cenzura nikde. A o kterém vlády jako je ta naše nedokáží zjistit, kdo a kde ten server provozuje. Skutečně svobodný internet.

To je veškeré tajemství paralelního internetu .onion – toho strašidelného dárknetu, před kterým vás varovali novináři. Má to jediný háček. TORový .onion server nepodporují běžné webhostingy, ale potřebujete na něj celý vlastní (virtuální) server. Tzn. namísto služby „webhosting“ službu „VPS“, která bývá ca. 3x dražší. A musíte si ji sami nakonfigurovat namísto profíků, čímž se můžete stát snadným cílem „hacktivistů“. S tím ovšem opět pomohou USA – Pentagon zveřejnil své kontrolní seznamy pro zabezpečení počítačových systémů SCAP, a postupně to převzali lidé z IT firem. Výsledné dokumenty SCAP vás provedou zabezpečením takřka čehokoli na přijatelnou základní úroveň.

Lakomá varianta – zahraniční freehosting s „živými štíty“ (a jeho nevýhody)

Lakomá alternativa je zrcadlit svůj server na nějakém zahraničním free hostingu. Pokud by jej totiž vládní cenzoři chtěli shodit přes ISP nebo Peering blokaci spojení, zařízli by přístup na celý free hosting včetně všech „legálních“, nevinných stránek – a to by bylo porušení zákonů a nemohou si to dovolit. Ostatní nevinné stránky si Lakomá varianta vlastně bere za živé štíty.

Státní cenzoři mohou jen blokovat doménu 3. řádu na tom freehostingu skrze DNS – a to umíme obejít přes soubor HOSTS.

A samozřejmě by žádali provozovatele freehostingu, aby vás zrušil. S čímž nejspíše uspějí. Takže Lakomá varianta vyžaduje neustále putovat po freehostingách, měnit domény a dávat je svým čtenářům… Technicky možné, organizačně neplausibilní.

Poslední nevýhoda lakomé varianty pak je, že freehosting má velmi omezené technické prostředky. V

žádném případě by neutáhl komentáře a možná ani čtenost.

Takže nakonec je asi nejlepší, když se jakékoli weby, které po vzoru Roskomnadzoru „odporují oficiální vládní linii“ a proto mají být zcenzurovány a popraveny, připraví na náraz. Kdo nemá peníze na VPS s .onion serverem, ať si udělá offline zálohu článků v nějakém uživatelsky přívětivém formátu a dá ji svým čtenářům ke stažení, dokud může.

Ať si zřídí pár freehostingových zrcadel a včas o nich informuje své čtenáře.

A ať se připraví na to, že Putinizace českého internetu ve jménu boje proti Putinovi znamená konec svobodného internetu, konec svobody slova a konec práva si vybrat, co chce kdo číst. Bylo to pěkných 30 let svobody, nashledanou příště. Nebo na TORu.

AUTOR: Jan Mrcasik

ZDROJ