Zatčen na Hedvábné stezce

Válka o virtuální anonymitu

Nedávné zadržení provozovatele webového e-shopu Silk Road, který byl zaměřen především na anonymní rozesílání drog, vzbudilo mnoho otázek týkajících se bezpečnosti a sledování internetu tajnými službami.

HONZA ŠÍPEK

Je to zdánlivě banální příběh. Ross William Ulbricht provozoval internetový obchod s drogami a druhého října ho zavřeli. Zajímavější je, že svůj e-shop zvaný Silk Road, česky Hedvábnou stezku, provozoval na síti Tor, která umožňuje skrývání identity klienta i serveru, a platilo se v anonymní měně Bitcoin (více viz A2 č. 3/2013). Oba prostředky byly do té doby považovány za skutečně anonymní a neproniknutelné.

Čtení obžaloby podané FBI k newyorskému soudu ale připomíná četbu šestákových detektivek: kdo chce spáchat dokonalý zločin, nesmí dělat chyby. A těch Ulbricht, přezdívaný Dread Pirate Roberts, nasekal vícero.

Undergroundové drogové tržiště bylo jedním z prvních míst, kde se za Bitcoiny dalo něco „rozumného" koupit

Především zcela neuhlídal oddělení své reálné a pseudonymní identity. Pod svým skutečným jménem se ptal na programátorské stránce StackOverflow na řešení problémů, které se sítí Tor souvisejí. Mnohá vodítka poskytl i na svých četných profilech v sociálních sítích a záznamy o drogových transakcích ponechával pravděpodobně archivované na serveru. Aspoň tedy podle verze obžaloby, která má důkazy spíše nepřímé a na obvinění z objednání nájemné vraždy – kterým se policie v prvních zprávách ohánělа v médiích – patrně stačit nebudou. Okolnosti zatím neprokázané vraždy jsou více než obskurní a je možné, že si Dread Pirate Roberts zaplatil vraždu vyděrače, který hrozil zveřejněním informací o uživatelích Hedvábné stezky, u něj samého. Policii v Kanadě, kde se zločin údajně stal, rozhodně žádný člověk zmíněného jména nechybí. Obvinění svůj účel ale splnilo minimálně v první vlně novinových článků, kdy se od Ulbrichta odklonila aspoň část sympatizantů – podobně, jako byl za sexuálního násilníka označen zakladatel Wikileaks Assange.

Digitální anarchisti vs. informatici

Následná diskuse v odborných kruzích se štěpila na dva tábory. Pro jedny – pracovně je nazývejme digitálními anarchisty – je hlavním nepřítelem stát a jakákoliv vláda se svými cenzurními a regulačními snahami. A kdokoliv proti nim bojuje, je spojenec, podobně jako loni v lednu zatčený Kim Dotcom, provozovatel služby Megaupload. Koho stát postihl, je oběť, a již nyní vznikají sbírky na Ulbrichtovu obhajobu. Koneckonců Dread Pirate Roberts byl libertarián, hlásící se k Rakouské škole, a v libertariánském duchu publikoval na Hedvábné stezce i politické pamflety. Stát by měl podle něj zasahovat co nejméně do záležitostí občanů a provozování digitálního tržiště se státem regulovaným zbožím je jen důsledkem těchto názorů. Druzí – nazvěme je informatiky – preferují slušnost a regulační zákony považují za nutné a funkční. Ti zánik obchodu s drogami vlastně vítají, protože prý ve špatném světle ukazoval digitální měnu Bitcoin.

První strana potřebuje Bitcoin i Tor k pocitu bezpečí před dohledem státu, kterému radikálně nedůvěřuje. Druhou stranu zajímá anonymizační technologie spíš z jakési techniciózní zvědavosti. A je pravda, že zatímco Tor i Bitcoin dlouhou dobu fungovaly bez povšimnutí širší veřejnosti, Hedvábná stezka byla tím pravým mediálním šlágrem, který na jejich existenci upozornil. Undergroundové drogové tržiště bylo jedním z prvních míst, kde se za Bitcoiny dalo něco „rozumného" koupit a kurs digitální měny byl do značné míry ovlivněn právě jeho provozem. Poslední zátah FBI pak sice radikálně srazil cenu Bitcoinu proti dolaru, ale po několika dnech se vrátila téměř k původnímu kursu a zdá se, že měna již funguje sama o sobě a nepůjde ji zastavit.

Návrat do webové puberty

Oba tábory ale trápí myšlenka, zda jejich digitální mazlíčci nemají slabiny. Síť Tor, již může člověk využít nainstalováním specializovaného prohlížeče Tor Browser Bundle, má dvě základní funkce. Jednak umožňuje při prohlížení webových stránek skrýt IP adresu nás samých coby běžného uživatele – adresa je často spojená s naší přesnou lokalitou či identitou skutečnou, například s účtem u konkrétního telefonního operátora nebo s místností v rámci firmy či školy. Druhá funkce umožňuje skrýt síťovou adresu webové stránky, která nám poskytuje informace – tedy ideální například pro práci disidentů nepohodlných jakémukoliv režimu. Počítače dobrovolníků, které slouží jako uzly sítě Tor, každý zašifrovaný požadavek několikrát přepošlou na další náhodné uzly sítě, klidně po celém světě. Podíváte-li se na domovskou stránku Ádvojky, může si redakční systém myslet, že se díváte třeba z Filipín. Ovšem dobrovolné provozování „výstupních uzlů" sítě je spojené s jistou dávkou adrenalinu – může se stát, že u vás ve tři ráno zabuší policie a bude hledat dětské porno. Snad proto je těchto uzlů stále málo a síť je pomalá.

Kdyby byla Ádvojka undergroundovým webem provozovaným ve strachu před zásahem státní moci, měla by adresu třeba advojka5xvy2hej5.onion. Na rozdíl od „koncovek" typu .cz, .sk, .com nebo .org, které mají v rukou konkrétní organizace (a mohou také třeba na základě rozhodnutí soudu doménu zrušit nebo dát někomu jinému), fungují stránky .onion pouze v rámci sítě Tor a jejich majitel je jednoznačně definován pouze kryptografickým klíčem, který si sám vygeneroval. A hlavně – přesné umístění serveru by nemělo být možné vystopovat, a tedy ani stroj zabavit.

Servery skryté v síti .onion upomínají na rané doby webu; spíš než na jeho „akademické dětství" pak na jeho „ranou pubertu", kdy přístup k síti měla již spousta lidí, ale ještě neexistovaly výraznější „dospělácké" regulační tlaky. Na období nadšeného sdílení čehokoliv bez ohledu na autorská práva a beze strachu z právníků. Tehdy síť vzbuzovala spíše pocit jakési spiklenecké pospolitosti než veřejného média. Web byl tak malý, že k orientaci v něm stačily „rozcestníky", seznamy dostupných webových stránek; weby byly spíš nespolehlivé, někdy fungovaly, někdy ne, a digitální divočina čekala na své objevitele. Podobně dnes v .onionu nacházíme kromě matadorů typu Pirátské zátoky a Wikileaks i undergroundová rádia, která si nedělají starost s autorskými právy, politické pamflety neznámých autorů, ale samozřejmě i disidentské weby. Časopis New Yorker provozuje v Toru svou „mrtvou schránku", přes kterou je možné posílat redakci anonymní podněty k práci, jejímž spoluautorem byl legendární digitální pionýr Aaron Swartz, který byl kvůli stíhání za hromadné stahování vědeckých článků dohnán k sebevraždě. Silk Road má své následovníky v obchodech Black Market Reloaded nebo Atlantis. Atlantida ovšem zmizela krátce před zátahem na Silk Road a vyvolala spekulace, zda nebyla pouze policejní provokací.

Hackeři v FBI a NSA

„Kyberpuberťáci" a „dospěláci" dnes bojují o své území za pomoci složité matematiky a konspiračních metod. Nelze ale říct, že by v obou oborech byli FBI nebo tajná služba NSA nějakými amatéry. V srpnu policejní razie v Irsku zastavila službu Freedom Hosting, která provozovala anonymní weby pro řadu subjektů. Servery Freedom Hostingu policie pravděpodobně „hacknula" a nakazila je škodlivým kódem, který využíval neznámé díry v internetovém prohlížeči uživatelů a práskal jejich identitu. Všechny státní útoky proti Toru tedy zatím oficiálně využívaly jiných zranitelností než anonymního protokolu samotného. Ale i to vyvolává řadu pochybností, protože pro protivníka je daleko cennější neprozradit, že nějakou metodu překonat umí, a ponechat protistraně pocit falešného bezpečí.

Za druhé světové války obětoval Churchill celé Coventry, než aby prozradil, že o leteckém útoku ví díky prolomení německého šifrovacího systému Enigma. Podle bezpečnostního analytika Bruce Schneiera, který interpretoval některé ze Snowdenových dokumentů, používá NSA k útokům proti vybraným subjektům speciální servery FoxAcid, umístěné na páteřních linkách amerických internetových providerů, které automaticky „hackují" počítače uživatelů. Podle důležitosti cíle a jeho předpokládaných technických schopností se používají různé typy zranitelností. A pro cíle, u nichž se předpokládá velká míra porozumění technologiím, se používají spíše útoky banálnější a již popsané, než aby se riskovalo prozrazení zranitelnosti dosud neznámé. Stále tedy platí, že kdo se chce skrývat, musí být obezřetný po všech stránkách a hlavně nesvěřovat své bezpečí do rukou technologie, kterou dokonale nezná a neovládá.

Autor je dokumentarista.