

Vítejte v Orwellově 1984! Další stupínek k nesvobodě a kontrole, salámovou metodou: Každá šifra bez zadních vrátek otevřených pro vládu včetně třeba chatů ve WhatsAppu se zakáže a kryptoměny tím pádem také!

- CZ24 News | 3. července 2020

Počátkem roku 1775 Benjamin Franklin se svým evropským kolegou Charlesem Dumasem vyvinuli tajnou metodu vzájemné komunikace.

Dumas trávil v Evropě roky sběrem zpravodajských informací, aby pomohl Američanům v jejich revoltě proti Británii. Ti dva ale potřebovali bezpečný způsob předávání těchto informací přes Atlantik.

A tak vyvinuli speciální číselnou formu šifrování, při níž se písmenka a slova nahrazovala číslicemi.

Šifrovací klíč se měnil s každým dopisem, takže např. v dopise Franklina z 2. března 1781 se slovo „MERCHANT“ (obchodník) psalo jako „23.3.4.13.6.14.24.18.“

Souběžně s tím lékař James Jay (bratr prvního šéfa Nejvyšších soudu Johna Jaye) vyvinul neviditelný inkoust, aby ti vůdci revoluce mohli tajně komunikovat.

Pro Revoluci byla šifrovaná komunikace kriticky důležitá. Dá se asi s jistotou říci, že by nebylo Spojených států, kdyby nevyvinuli bezpečné způsoby posílání informací.

Ironií je, že politici se teď pokouší moderní metody šifrování zničit.

Během několika posledních měsíců, kdy se každý krčil ve strachu doma při povinné karanténě, dospěla Země svobody až k těm několika posledním týdnům, kdy ji pohltil hněv...

A v průběhu těch časů se našlo i pár amerických senátorů, kteří zase využili to děsivé politické přikázání: „Nikdy nepromarni dobrou krizi.“

Předložili senátní návrh zákona 4051 „Zákon o zákonném přístupu k zašifrovaným datům,“ který byl potichoučku předložen minulý týden, kdy byla pozornost všech upřena k něčemu jinému.

V první řadě ty důležité věci, jako všechny zákony, co zabíjí svobodu, má i tento ošidné jméno.

Zákon o zákonném přístupu k šifrovaným datům (Lawful Access to Encrypted Data Act – zkratka LEAD), která znamená vedení a také olovo, nás zvede někam spíše do Číny. V Zemi svobody by ten LEAD měl vést ke zničení posledních zbývajících svobod občanů.“

(V tomto smyslu je to spíše jako to „olovo“, tj. vysoce toxický kov, který otravuje mozek a vytváří těžké zmrzačení intelektu.)

Zákon LEAD je v podstatě zabiják šifrování. Jeho záměrem je od technologických společností vyžadovat, aby do svých produktů zabudovávaly „zadní vrátka“, aby se tak zajistilo, že vláda může na

dálku přistupovat k vašim datům, vašim zařízením a vašim životům.

Je to prostě hodně otřesné.

Např. Apple v poslední době poskytuje šifrování na zařízení jako na jeho iPhonech a iPadech. Jakmile si zařízení zašifrujete, jenom VY ho můžete odšifrovat. Apple nemůže. Hackeři nemůžou. Ale nemůže ani vláda.

Takže když vám vaše zařízení ukradnou (nebo zkonfiskují), k vašim datům se nikdo nedostane.

Podle Zákona LEAD by ale praxe takového podlézání zájmům zákazníků byla ilegální. Apple by už nemohl nabízet šifrování zařízení a navíc by federální vládě museli poskytnout dálkový přístup k vašemu zařízení a ke všemu jeho obsahu.

To samé by platilo i pro vaše oblíbené chatové aplikace.

Např. WhatsApp, jedna z nejoblíbenějších textových appek světa. Facebook (kterému WhatsApp patří) před pár lety začal zabudovávat šifrování end-to-end (specifické vždy pro komunikující dvojice) do všech dat WhatsAppů.

To znamená, že jakákoliv zpráva, kterou komukoliv pošlete přes WhatsApp je okamžitě zašifrovaná v okamžiku, kdy opouští váš telefon.

Ty zprávy chodí na servery WhatsApp úplně zašifrované. Takže kterýkoliv hacker (nebo Facebookový inženýr), který ty data zachytí, neuvidí nic než neuspořádaný binec znaků.

A ta zpráva se nerozšifruje, dokud se nedostane na zamýšlené zařízení příjemce. Takže jedinými lidmi, kteří tu zprávu uvidí v „jasném textu“, jsou ti dva lidé účastníci se dané konverzace.

Nikdo jiný ta data nemůže odposlechnout nebo si je stáhnout.

Ale zase i tohle by podle Zákona LEAD vstoupilo do ilegality a Facebook by měl povinnost tam pro vládu zabudovat ‚zadní vrátka‘, aby mohla vaši konverzaci na dálku kdykoliv sledovat.

LEAD vyžaduje i od vývojářů operačních systémů jako Microsoft Windows a Apple MacOS, aby i oni poskytovali zadní vrátka do svých počítačů.

Ohromující je i pomýšlení, jak dalekosáhlé efekty by tahle legislativa měla mít.

Např. používáte síťové manažery hesel jako OnePassword?

I od těch by se chtělo, aby vládě poskytli přístup k vašim datům, což by v podstatě vládě dalo přístup ke VŠEMU, co máte na síti.

Nahráváte si soubory a fotky do iCloudu? Jejda. To také. Od Applu se bude vyžadovat, aby tam vybudoval zadní vrátka a dal vládě přístup k vašim datům.

Podle té nové legislativy se jakýmkoliv šifrováním ‚s nulovou znalostí‘, ať už si ukládáte soubory, sdílíte fotky, vyměňujete s kamarády textové zprávy, provádíte video-hovory, posíláte zašifrované emaily atd., dopustíte ilegálního zločinu.

A aby to bylo průzračně jasné, co to znamená, podle tohoto Zákona LEAD v podstatě do ilegality vstoupí veškeré KRYPTOMĚNY.

Ano je to tak. Kryptoměny totiž spoléhají na šifrování dat.

Pro vaši ‚peněženku‘ je kriticky důležitá kombinace klíčů veřejný klíč / soukromý klíč. A teoreticky jenom vy byste měl mít přístup.

Ale právě tomu chtějí legislativci zabránit. Vláda chce mít přístup zadními vrátky ke všemu.

Upřímně řečeno tahle legislativa by byla hrozně legrační, kdyby nebyla opravdu navržená, protože krásně ukazuje, jak ji vymýšlí lidé, co o tom nemají ani ponětí.

Ti lidé volají po ‚zákonném přístupu‘, jako kdyby, jak tam budou zadní vrátka, do toho mohla jen vláda. Ti lidé jasně o kybernetické bezpečnosti nic nechápou.

Nic takového jako ‚zadní vrátka‘, která jsou přístupná jen pro vládu, existovat nemůže.

Jakmile technologická společnost vytvoří způsob, jak lze do zařízení na dálku vstupovat, tak budou tahle zadní vrátka přístupná KAŽDĚMU, kdo to hackne.

Není to tak, že by nějaký hacker nebo zahraniční zpravodajská agentura zkusila zadní vrátka na vašem iPhone a řekla: „Jé, promiňte, tohle je jen pro vládu USA. Myslím, že si zkusím najít jinou méně připravenou cestu dovnitř.“

Bude-li tento zákon schválen, tak nejenže vaše vláda bude schopna vstupovat do vašich zařízení, nýbrž i hackeři budou mít díky moudrému Senátu Spojených států nevyčerpatelnou pokladnici kradení dat.

To je genitální, pardon geniální.

Simon Black

Překlad: reformy.cz