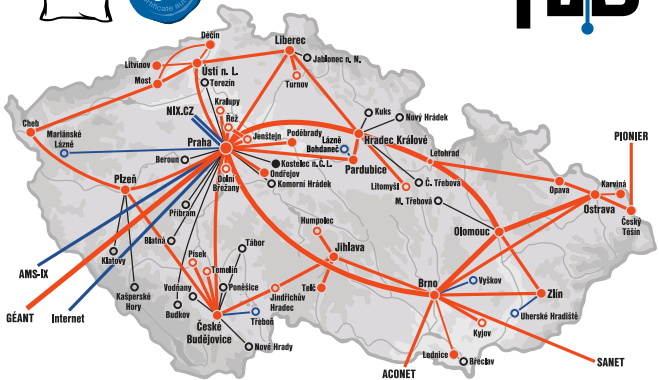
Stránka, doména, URL, adresa…

Ondřej Caletka

16. ledna 2017

O sdružení CESNET



Motivace

Zákon 186/2016 Sb.

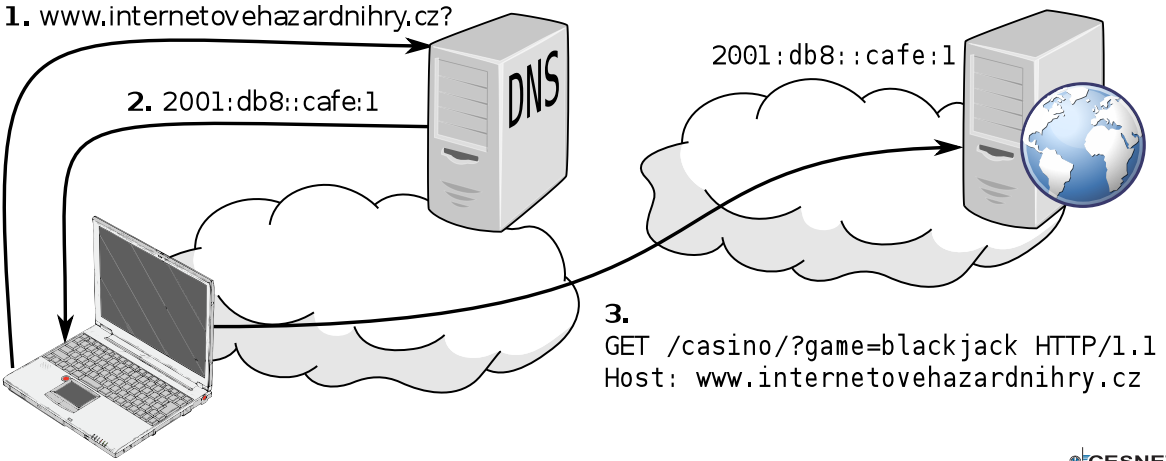
§ 82 Blokace nepovolených internetových her
(1) Poskytovatelé připojení k internetu na území České republiky jsou povinni zamezit v přístupu k internetovým stránkám uvedeným na seznamu internetových stránek s nepovolenými internetovými hrami.

- kdo je poskytovatel připojení k internetu?
  - připojení = jednorázový akt zprovoznění koncového bodu sítě
  - přístup = kontinuální služba
  - je to kdokoli s přístupem k internetu?
- co je to internetová stránka?
  - zřejmě webová stránka, tedy protokol HTTP/S
- jak to má být **technicky provedeno**?

Webová adresa, neboli URL

- kompletní URL zná pouze prohlížeč
- internetová adresa je pouze částí URL
- blokování internetové adresy při požadavku na blokování URL může být v rozporu s jinými předpisy

Webový prohlížeč s protokolem HTTP



Blokování na úrovni DNS resolveru

- DNS server nevrátí odpověď, nebo ji pozmění
- nelze blokovat konkrétní URL cesty nebo dotazy
- nenákladná metoda, ve světě velmi rozšířená

Neučinné, protože…

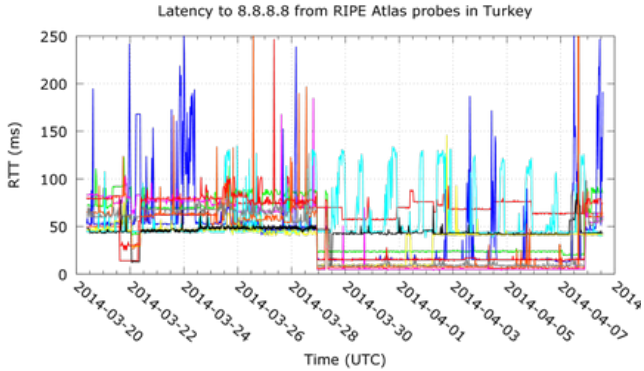
- uživatel může použít DNS server třetí strany
  - má poskytovatel *povinnost* znemožnit použití takových DNS serverů?
- provozovatel služby může používat URL s IP adresou `http://[2001:db8::cafe:1]/casino/?game=blackjack#score`
  - co dělat, až se taková URL objeví na seznamu?

Příklad z Turecka ①

21. 3. 2014 zablokován Twitter a YouTube na DNS serverech
25. 3. 2014 zablokován přístup k Google Public DNS a podobným
28. 3. 2014 nainstalován falešný DNS server na 8.8.8.8

Příklad z Turecka ②

4. 4. 2014 ukončeno lhaní o Twitteru a Youtube
7. 4. 2014 ukončen únos DNS serverů



Zdroj: `https://labs.ripe.net/Members/emileaben/a-ripe-atlas-view-of-internet-meddling-in-turkey`

Blokování na úrovni IP adres

- jakékoli spojení s danou IP adresou je v síti blokováno
- účinnější než blokace DNS
- nenákladná metoda, ve světě velmi rozšířená

Nepoužitelné, protože…

- IP adresy jsou velmi často sdíleny
- blokace by postihla i ostatní stránky hostované na stejném (proxy-)serveru; často zcela nesouvisející
  - je poskytovatel *oprávněn* blokovat jiné, nesouvisející stránky?

Sdílení IP adres

- mezi službami téhož provozovatele
- sdílené webhostingy pro malé weby
- sítě typu Content Delivery Network
  - doručování obsahu svých zákazníků

Příklad webů, které sdílí IP adresu

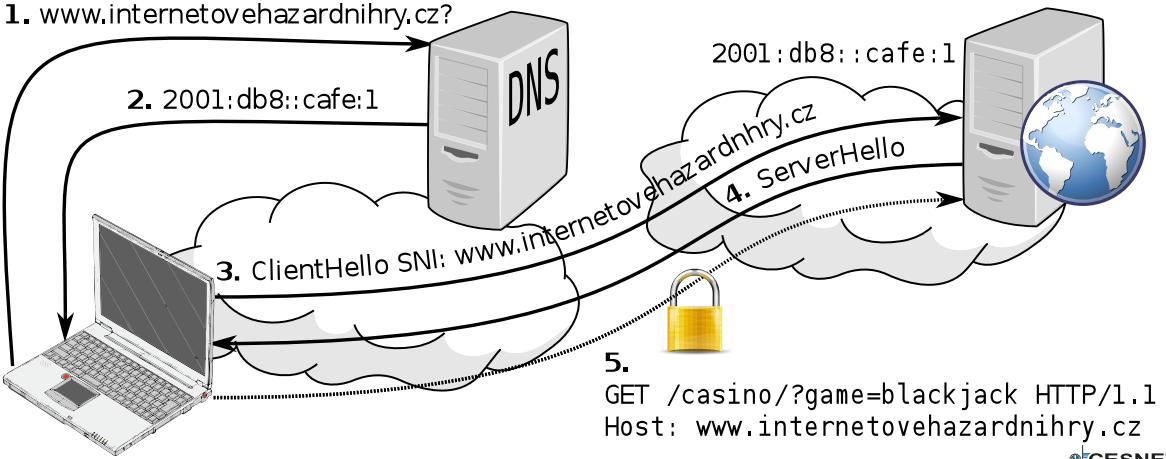
internetovehazardnihry.cz alexandranice.xyz almatyzhylu.kz angelburk.xyz asyakitty.top bez-vinta.ru cashregisterny.com diadiva.top jaytaylor.top lucar.rs nspus.com pensy.top prof.estate ricktejeiro.xyz ricusrebudma.cf roadtrain.fr secretlab.name suttoncoldfieldantiquescircle.org ultrasoundtechschoolsga.xyz unlockedseries.com wotton-firework-display.co.uk xdwqrz.loan

Vnucení transparentního proxy serveru

- transparentní proxy server: aplikační server, který se chová jako skutečný server pro klienta a zároveň jako klient pro skutečný server
- dokáže filtrovat přesné konkrétní URL
- obtížně škálovatelný pro sítě poskytovatelů připojení
- obvyklé řešení: přesměrování pouze *závadných* IP adres za účelem cílené blokace konkrétní URL z dané IP adresy
- incident Wikipedie ve Velké Británii v roce 2008
  - obrázek obalu alba *Scorpions – Virgin Killer*, hostovaný na Wikipedii, se dostal na blacklist
  - poskytovatelé přesměrovali celý IP provoz Wikipedie na proxy server; ten byl přetížen
  - pro Wikipedii všichni uživatelé přistupovali z několika málo adres proxy serverů; zablokovala editace


ČT 24
A vy už jste někdy šifroval?
Ondřej Závodský náměstek pro hazard a majetek státu, MF
22:39 VEČER USTÁVÁNÍ SRÁŽEK A UBÝVÁNÍ OBLAČNOSTI.

Webový prohlížeč s protokolem HTTPS



Potíž s HTTPS

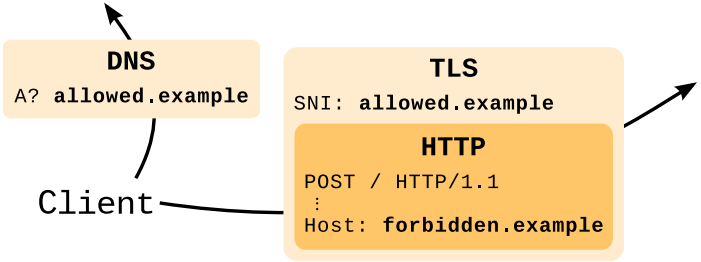
- současný standard webové komunikace
- zaručuje důvěrnost a autenticitu dat mezi klientem a serverem
- analýza přenášeného obsahu, vnucení proxy serveru **není možné**
- poskytovatel vidí pouze:
  - DNS dotaz a odpověď
  - jméno hostitele, které klient požaduje (SNI hlavička)
  - certifikát, který server poslal
- filtrovat konkrétní URL v takovém případě **nelze**

Deep Packet Inspection

- nejpokročilejší (a nejdražší) technologie filtrování obsahu
- komunikace není narušena, je pouze strojem **trvale odposlouchávána a analyzována**
- při zjištění nevhodného obsahu je do spojení injektován obsah, který způsobí jeho rozpad
- eliminuje problém s přetíženým proxy serverem
- dokáže blokovat konkrétní HTTP URL, pro HTTPS dokáže blokovat jména hostitelů

Domain fronting

- technika, která zcela znemožňuje zablokování dané komunikace bez vlivu na ostatní služby
- využívá *nedokonalosti* některých CDN sítí, které nekontrolují shodu nešifrované SNI hlavičky se šifrovanou HTTP hlavičkou `Host`
- implementováno v komunikátoru Signal



Zdroj: `https://www.bamsoftware.com/papers/fronting/`

Použití VPN

- sestavení šifrovaného tunelu někam, kde omezení neplatí
- nutno důvěřovat provozovateli VPN koncentrátoru
  - vidí komunikaci podobně jako poskytovatel internetu
- poskytovatel vidí VPN provoz, nedokáže ale určit obsah
- při správném nastavení prochází VPN i DNS provoz
- používání VPN je zcela **legitimní** a **legální**

Shrnutí

- zcela účinné blokování určitého obsahu **neexistuje**
- různé techniky jsou různě nákladné, mají různé vedlejší efekty, ale **všechny je možné triviálně obejít**
- blokování má smysl jen pro *náhodné kolemjdoucí*, nikoli pro ty, kteří předmět blokování **cíleně vyhledávají**

Pozvánka

Seminář o bezpečnosti sítí a služeb
Kdy: 7. února 2017, 9.30–17.00
Kde: FS ČVUT, posluchárna 256 (2. patro), Technická 4, Praha 6

- aktuální bezpečnostní trendy
- automatická obrana sítě
- praktická forenzní analýza
- legislativní pohled

Více informací a registrace na
`https://www.cesnet.cz/sdruzeni/akce/bss17/`

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz

Prezentace je již nyní k dispozici ke stažení.