JSTE ANONYMNÍ, nebo sledují i vás?

Nechcete být jako ovce, které o sobě všechno a všem prozradí, navíc zdarma? Surfujte na internetu anonymně!

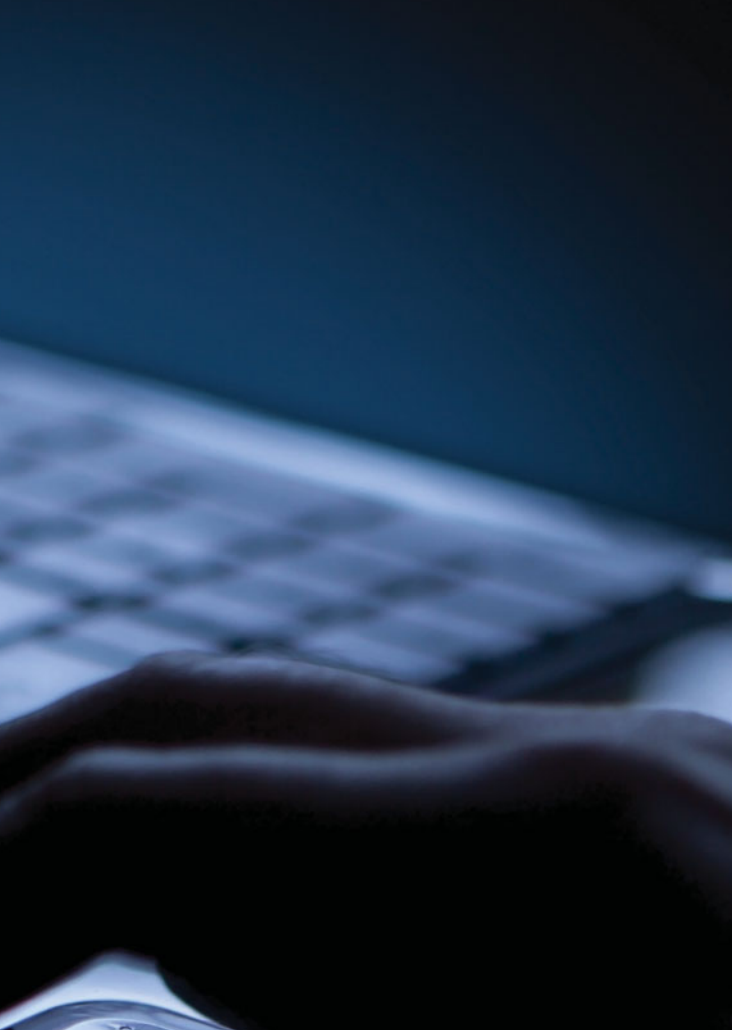
PETR KRATOCHVÍL

Bizarním trendem posledních let je totální absence soukromí. Stovky milionů lidí o sobě na sociálních sítích prozrazují téměř vše – od politických názorů přes záliby až po seznamy přátel, a ve většině případů nechybí ani fotografie či videa. Na základě těchto dat je možné uživatele poznat lépe, než se zná on sám. I když si odmyslíme různé konspirační teorie (z nichž některé ale nemusí být tak šílené, jak se na první pohled zdají – viz → **str. 36**), většina uživatelů by určitě nebyla ráda, kdyby tato data byla volně k dispozici. Byla by totiž nejen ideálním materiálem pro bytové zloděje, ale také pro potenciální zaměstnavatele nebo mediální agentury zabývající se různorodými druhy manipulací. Smutné ale je, že celá řada uživatelů toho o sobě prozradí hodně i bez odhalování na sociálních sítích.

Co o vás ví internet

Není to tak dávno, co se v několika médiích objevila aféra založená na skutečnosti, že vás Facebook sleduje a má vytvořený váš profil, i když na něm nemáte účet (viz „Jak vás sleduje Facebook“ na → **str. 127**). Celá řada lidí byla šokována množstvím informací, které je možné o komkoliv shromáždit, aniž by on o sobě cokoliv prozrazovat chtěl. Realita je ale ještě nepříjemnější. Množství stop, které se na vašem počítači ukládají, je enormní, a to i především proto, že většina webů, které navštívíte, toho o vás chce vědět co nejvíce.

K získání informací o uživateli se používají především cookies – malé soubory, které web pošle prohlížeči a které prohlížeč uloží na počítači uživatele. Původní myšlenka cookies nebyla špatná: měly sloužit především k ukládání informací



sloužících k personalizaci (nastavení webu, přihlašování). S přibývajícím hladem po osobních informacích se ale stále častěji využívají nejen k získávání statistických informací o chování návštěvníků, ale i ke sbíráním dat o uživatelích. Většina běžných uživatelů zná standardní HTTP cookies, které lze smazat běžně v prohlížeči. O něco obtížněji se odstraňují tzv. LSO (Local Shared Object) cookie. Ty se také někdy označují jako flash cookies, protože při jejich vytváření weby využívají doplňku Adobe Flash. Na rozdíl od klasických cookies do nich lze uložit až 100 kB dat, využívají se nezávisle na prohlížeči a jejich platnost nikdy nevyprší! Vzhledem k tomu, že se jich netýká standardní příkaz pro odstranění cookies v prohlížeči, je nutné je zlikvidovat manuálně. K tomu je možné využít například program CCleaner, případně doplněk BetterPrivacy (je k dispozici třeba pro Firefox a Operu). Zkušenější uživatelé si mohou tyto cookies odstranit sami: jde o soubory s příponou SOL, které se například ve Windows 7 skrývají ve složce »AppData\Roaming\Macromedia\Flash Player\#SharedObjects«. Ovšem pozor: LSO cookies nemusí být jen na škodu – pokud například hrajete flash hry nebo využíváte flash aplikace, můžete v nich mít uložena důležitá data.

A aby nebylo špatných zpráv dost, objevila se nedávno takzvaná evercookie (někdy také označovaná jako supercookie), která pro účely špehování nejen kombinuje ukládání klasických a LSO cookies, ale využívá i některé další unikátní techniky, díky kterým je téměř nesmazatelná. Typickou ukázkou může být například ukládání údajů v RGB hodnotách cachovaných PNG souborů. Evercookies využívají celou řadu HTML5 technik, díky kterým je běžný uživatel nemá šanci odstranit. Podrobnější informace o evercookies, včetně jejich umístění, najdete například na webu **samy.pl/evercookie/**.

CHIP NA CHIP DVD

Na Chip DVD najdete celou řadu zajímavých nástrojů, které vám umožní bezpečnější a anonymnější surfování.

Firefox Portable – Chipem speciálně upravená verze prohlížeče Firefox vám zaručí bezpečnější pohyb na internetu.

AntiPhotoSpy – Ukládáte si vlastní obrázky na internet? Odstraňte z nich nejprve citlivá metadata!

Spybot 2 - oblíbený nástroj na vyhledání a likvidaci špehovacího softwaru, se kterými si běžné antiviry často neporadí.

Hotspot Shield – Praktický nástroj pro šifrování internetové komunikace při připojení pomocí free Wi-Fi hotspotů.

TrueCrypt – Oblíbený nástroj na šifrování dat. Bude se vám hodit, pokud si například ukládáte citlivá data do webového úložiště.

JAK VÁS SLEDUJE FACEBOOK

Je to přibližně rok, co se ve Spojených státech rozvířila debata o právu na internetové soukromí. Tu odstartovala žaloba na Facebook, jejíž základem bylo tvrzení, že Facebook důkladně špehuje nejen vlastní uživatele, ale i uživatele, kteří u něj nemají účet. Výsledkem debaty bylo mohutné vysvětlování specialistů Facebooku a prý i drobné korekce v mechanismech sledování.

Nejdůležitějším faktem ale bylo potvrzení výše zmiňovaného sledování. Podle dostupných informací Facebook rozděluje sledované uživatele do tří kategorií – na aktivní a přihlášené uživatele, nepřihlášené uživatele a uživatele bez účtu na Facebooku. Sledování uživatele začíná ve chvíli, kdy ten navštíví libovolnou stránku na doméně Facebooku – stačí si jen prohlédnout fotografii v kamarádově galerii. Poté už sociální síť monitoruje uživatelovu aktivitu pomocí prvků typu „Sdílet" nebo „To se mi líbí" a k vytvořenému profilu si ukládá další identifikační údaje, související s jeho počítačem a prohlížečem (například IP adresu, verzi operačního systému a prohlížeče, používané rozlišení atd.). Tato data jsou prý po uplynutí 90 dní mazána a nahrazována novými. Pro ukládání dat jsou využívány dva typy cookies: obyčejní surfaři dostanou browser cookie, uživatelé Facebooku session cookie.

Nejděsivější je ale to, že tato data lze díky kontaktním údajům na Facebooku (pokud jsou pravdivé) přiřadit ke konkrétní osobě – včetně propojení na její rodinu či přátele. Tímto způsobem lze například snadno sledovat aktivity vybrané skupiny lidí – od politických aktivistů až po „problémové občany". Z tohoto úhlu pohledu je možnost zneužití těchto dat k reklamním účelům jen zanedbatelným a druhořadým problémem. Pokud vás tato problematika zaujala, doporučujeme podrobnější studium odhalení Facebooku na zpravodajském webu USA TODAY (**usatoday30.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1**).

Sleduje i vás: Tlačítka z Facebooku najdete dnes na obrovském množství www stránek, včetně známých zpravodajských webů.

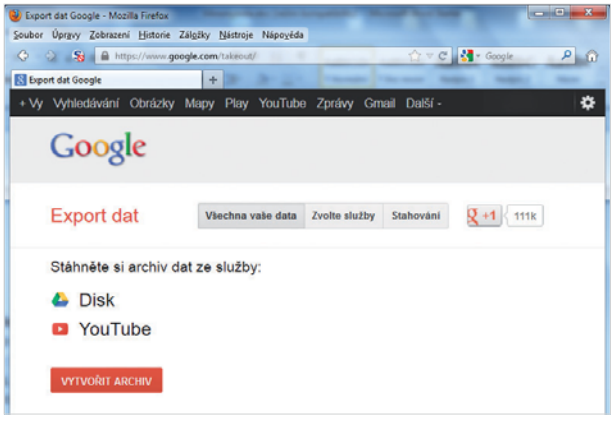
PRAKTICKÝ TIP

Pokud se přihlásíte na webovou stránku pomocí kombinace uživatelského jména a hesla, mohou vás administrátoři webu sledovat nezávisle na tom, zda používáte anonymizační službu či nikoliv. V případě, že se chcete k takovémuto webu přihlásit anonymně, bez registrace, zkuste využít služby, které tento přístup usnadňují. Například na webu BugMeNot (**bugmenot.com**) lze najít obrovské množství kombinací uživatelských jmen a hesel. Pokud žádné vhodné nenajdete, zkuste se zaregistrovat a místo svého e-mailu využijte „desetiminutový e-mail" (**10minutemail.com**). Bezplatná služba vám vygeneruje anonymní e-mailovou schránku, která po pár minutách zmizí. Stačíte tak bez problémů ověřit registraci, bez následných otravných spamových zpráv.

Webové stránky BugMeNot nabízí možnost přístupu na celou řadu webů bez nutnosti registrace. Naleznete na něm totiž kombinace uživatelských jmen a hesel.

EVROPSKÉ PRÁVO NA VLASTNÍ DATA

I když se Evropská unie angažuje v celé řadě bizarních záležitostí typu „jak má vypadat pravý špekáček", čas od času má snahy k aktivitám, kterým tleskáme. Poslední takovouto aktivitou je právo na zapomnění (right to be forgotten), které by mělo uživatelům například zaručit, že pokud se z Facebooku odhlásíte, pak tato služba skutečně smaže veškerá data o vás uložená. Druhou aktivitou je tzv. právo na přenositelnost, které by vám mělo umožnit přenést si veškerá svá data z jedné služby na druhou – například z Facebooku na sociální síť Google+. To je zatím kvůli neexistujícím jednotným normám na ukládání soukromých dat spíše fantazie, ale i tak má tato aktivita jednu světlou stránku. V rámci ní jsou totiž firmy tlačeny k tomu, aby od nich zákazník (na vyžádání) mohl získat veškeré informace, které o nich firma vlastní. Pravdou je, že některé služby či weby už něco podobného nabízí. Například na Facebooku najdete možnost exportu uložených dat v nastavení (**www.facebook.com/settings**). Pro většinu uživatelů ale může být zajímavější, co si o nich ukládá Google, což lze zjistit pomocí funkce Export Dat Google (**www.google.com/takeout**).



Google uživateli nabízí možnosti exportu vlastních dat.

Webové proxy nabízí uživateli snadnou cestu k alespoň částečné anonymitě na internetu.

Proč a jak anonymně?

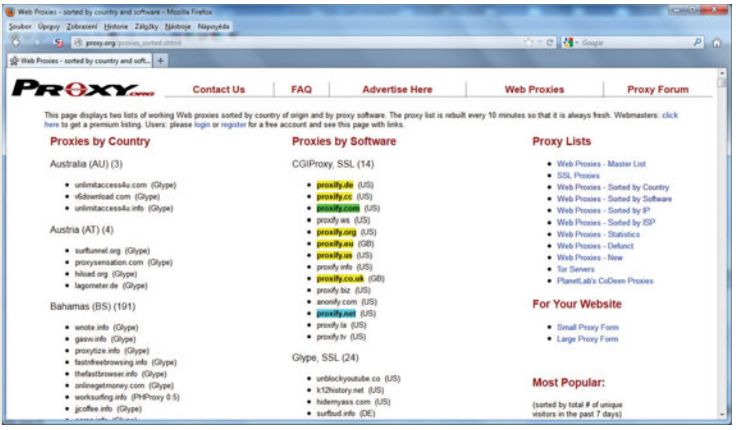
Hned v úvodu je nutné zdůraznit, že slovo anonymní je zde nutné brát s rezervou. Pokud provedete něco „ošklivého" a příslušné orgány vás budou chtít vypátrat, s největší pravděpodobností se jim to podaří. Ukryjí se před nimi jen skuteční profesionálové se znalostí prostředí. Běžným uživatelům ale zcela postačí, když se skryjí před stovkami zvědavých firem, které chtějí získat informace o jejich soukromí a surfovacích návycích. Díky tomu se především zbaví spousty zbytečného spamu (firmami často označovaného jako newsletter). Další výhodou anonymního surfování může být například přístup ke službám, které mají určitá omezení (typicky pro přístup z určité domény či geografické lokace).

A kudy tedy vede cesta k alespoň částečné anonymitě? Ještě před několika lety bylo základním krokem mazání cookies. S rozvojem modernějších technologií (viz zmiňované flash cookies a evercookies) to ale bohužel neplatí. Celá řada stránek se navíc snaží přistupovat k datům ukládaným plug-iny a doplňky prohlížeče, kde hledají další osobní informace. Řešením je tak využívání upravených verzí prohlížečů a speciálního softwaru zaměřeného na odstraňování stop.

Například pokud běžně surfujete v Google Chrome, upravte si pro anonymní surfování Firefox: připravte si jeho mobilní verzi a přidejte doplňky specializované na zlepšení soukromí – BetterPrivacy, NoScript a DoNotTrackMe. Vzhledem k tomu, že i některé anonymizační služby umožňují webovým stránkám automaticky na počítač ukládat cookies, pokud byste používali stejný prohlížeč pro běžné a pro anonymní surfování, mohly by webové stránky teoreticky využít tyto cookies k vaší identifikaci. Proto byste měli u alternativního prohlížeče nastavit automatické mazání cookies při každém ukončení prohlížeče. Dalším krokem k lepší anonymitě je využití programů pro zametání internetových stop – například již zmiňovaného CCleaneru.

Na internet s maskou

Základním kamenem identifikace uživatele na internetu je IP adresa. V dobách minulých byla většina uživatelů připojena k internetu prostřednictvím tzv. dynamické IP adresy, což znamenalo, že prakticky při každém připojení k internetu (po zapnutí routeru) jim byla přidělena nová adresa. V současnosti už má velký počet uživatelů pevnou (neměnnou) IP adresu a s nástupem IPv6 toto číslo i nadále poroste. To bude mít za následek téměř naprostou ztrátu anonymity. Ať už na internetu uděláte cokoliv (prohlédnete si web, navštívíte diskusní fórum, zahrajete si hru), na příslušném serveru o tom budou v tzv. logu uloženy záznamy: čas přístupu, IP adresa



V seznamu proxy serverů si můžete vybrat i například podle země, v níž je server umístěn.

počítače, typ a cíl události. Jediným způsobem, jak si zachovat alespoň částečnou anonymitu, tak bude využití proxy serverů či proxy sítí.

Proxy servery fungují jako prostředníci mezi počítačem uživatele a cílovým webem. Uživatel zadá požadavek na zobrazení určitého webu proxy serveru, ten skryje jeho IP adresu a požadavek na zobrazení webu pošle pod svou IP adresou. Po obdržení výsledků je proxy předá zpět uživateli. Důsledkem toho není cílovému serveru známa IP adresa uživatele, který požadavek zadal. Tyto servery lze označit jako otevřené proxy servery, které slouží jen pro maskování IP adresy. Lze je využít například k získání přístupu k lokalitou omezeným službám. O krůček dál jdou anonymizéry, což jsou v podstatě proxy servery, které upravují odeslané požadavky, například odstraňují cookies nebo HTTP referrer. Zásadním nevýhodou těchto služeb je jejich omezená použitelnost. Nejen že server, který funguje dnes, už zítra fungovat nemusí, ale i rychlost, se kterou vám anonymní surfování obvykle nabízí, je světelné roky vzdálená od dnešních standardů. Zkrátka – najít rychlý a stabilní proxy server je malá výhra v loterii.

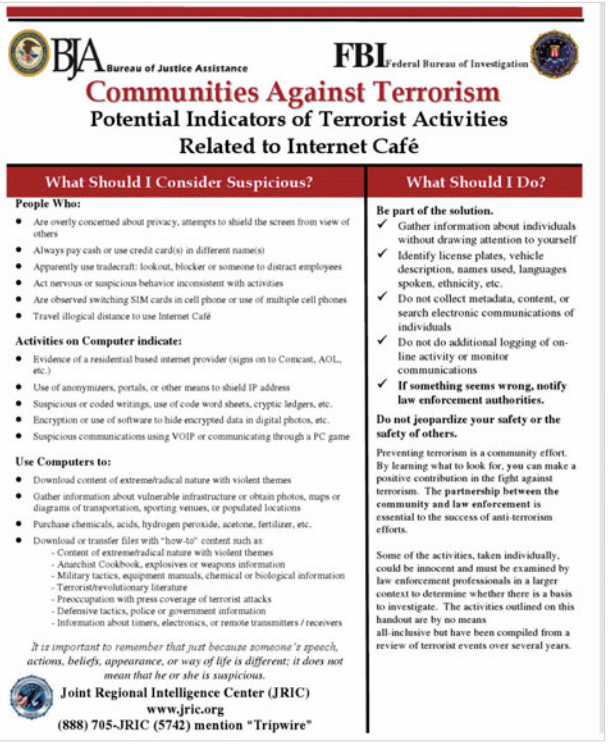
Anonymita se vším všudy

Jednou z nejdokonalejších metod, jak skrýt svoji identitu, je využití sítě TOR (The Onion Router), která umožňuje maskovat i přenášená data. Ta jsou z počítače odesílána šifrovaně, stejně jako probíhá i komunikace mezi jednotlivými routery až k cíli. Tento projekt byl původně určen pro obcházení blokády (či cenzury) internetu v celé řadě zemí, ale zpočátku velmi vysoká úroveň anonymity přitáhla i temnou stranu síly. Odborníci tvrdí, že přes TOR probíhá výměna dětské pornografie a ve velké míře ho využívá i podsvětí. Na internetu se nyní objevují zvěsti, že do sítě TOR masivně investovaly americké bezpečnostní služby, které díky správě velkého množství tzv. exit NODů mohou část dat bez problémů dešifrovat. Fakt ale je, že především v USA může být používání sítě TOR poměrně rizikové (viz například příspěvek na **toddsnotes.blogspot.cz/2009/11/because-i-ran-tor-police-took-all-my.html**).

Pokud se i přes výše uvedené informace rozhodnete pro TOR, určitě vás potěší, že má ve srovnání s proxy servery celou řadu výhod. Například jeho rychlost je znatelně lepší než u webových proxy a zároveň platí, že čím později večer surfujete (v USA začíná špička), tím více se přenos dat zrychluje (více počítačů v síti znamená vyšší rychlost). Výhodou je i možnost mobilního použití. Svoji TOR aplikaci můžete mít na flash disku a pak anonymně surfovat například z internetové kavárny. Podrobnější informace lze nalézt třeba na webu **portableappz.blogspot.cz/2012/06/tor-02237-multilingual.htm**.

KDO CHCE SOUKROMÍ, TEN JE PODEZŘELÝ!

Americké ministerstvo spravedlnosti občanům vysvětlilo, že pokud chtějí mít například v internetové kavárně soukromí, jsou podezřelí a měli by být nahlášeni jako potenciální teroristé. Podezřelé je především když platíte v hotovosti, používáte kavárnu v podezřele nelogické vzdálenosti nebo využíváte anonymizéry.


BJA Bureau of Justice Assistance
FBI Federal Bureau of Investigation

Communities Against Terrorism

Potential Indicators of Terrorist Activities Related to Internet Café

What Should I Consider Suspicious?

People Who:
- Are overly concerned about privacy, attempts to shield the screen from view of others
- Always pay cash or use credit card(s) in different name(s)
- Apparently use tradecraft: lookout, blocker or someone to distract employees
- Act nervous or suspicious behavior inconsistent with activities
- Are observed switching SIM cards in cell phone or use of multiple cell phones
- Travel illogical distance to use Internet Café

Activities on Computer indicate:
- Evidence of a residential based internet provider (signs on to Comcast, AOL, etc.)
- Use of anonymizers, portals, or other means to shield IP address
- Suspicious or coded writings, use of code word sheets, cryptic ledgers, etc.
- Encryption or use of software to hide encrypted data in digital photos, etc.
- Suspicious communications using VOIP or communicating through a PC game

Use Computers to:
- Download content of extreme/radical nature with violent themes
- Gather information about vulnerable infrastructure or obtain photos, maps or diagrams of transportation, sporting venues, or populated locations
- Purchase chemicals, acids, hydrogen peroxide, acetone, fertilizer, etc.
- Download or transfer files with "how-to" content such as:
  - Content of extreme/radical nature with violent themes
  - Anarchist Cookbook, explosives or weapons information
  - Military tactics, equipment manuals, chemical or biological information
  - Terrorist/revolutionary literature
  - Preoccupation with press coverage of terrorist attacks
  - Defensive tactics, police or government information
  - Information about timers, electronics, or remote transmitters / receivers

It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different; it does not mean that he or she is suspicious.

Joint Regional Intelligence Center (JRIC)
www.jric.org
(888) 705-JRIC (5742) mention "Tripwire"

What Should I Do?

Be part of the solution.
- ✓ Gather information about individuals without drawing attention to yourself
- ✓ Identify license plates, vehicle description, names used, languages spoken, ethnicity, etc.
- ✓ Do not collect metadata, content, or search electronic communications of individuals
- ✓ Do not do additional logging of online activity or monitor communications
- ✓ **If something seems wrong, notify law enforcement authorities.**

Do not jeopardize your safety or the safety of others.

Preventing terrorism is a community effort. By learning what to look for, you can make a positive contribution in the fight against terrorism. The partnership between the community and law enforcement is essential to the success of anti-terrorism efforts.

Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years.

Nepřipomíná vám to moderní verzi varování „Socialistickou vesnicí imperialistický agent neprojde" z dob minulých?

ODKAZY, KTERÉ SE VÁM MOHOU HODIT

DOMÁCÍ ANONYMIZÉRY:
www.anonymouse.cz/anonymizer
www.anonymizer.in/anonymizer
www.proxyserver.sk
www.katedrala.cz/anonymizer-katedrala

ZAHRANIČNÍ ANONYMIZÉRY:
www.hidemyass.com
www.anonymizer.com
proxify.com

SEZNAM PROXY SÍTÍ
www.proxy.org/proxies_sorted.shtml

JAK SE ZBAVIT FACEBOOKU?

Chcete zablokovat na svém počítači veškeré prvky Facebooku? Upravte si přímo na svém počítači DNS záznamy. Otevřte si (s právy administrátora) na svém počítači soubor hosts a přidejte do něj následující řádky:

127.0.0.1 static.ak.fbcdn.net
127.0.0.1 www.static.ak.fbcdn.net
127.0.0.1 login.facebook.com
127.0.0.1 www.login.facebook.com
127.0.0.1 fbcdn.net
127.0.0.1 www.fbcdn.net
127.0.0.1 fbcdn.com
127.0.0.1 www.fbcdn.com
127.0.0.1 static.ak.connect.facebook.com
127.0.0.1 www.static.ak.connect.facebook.com