ALMA MATER SOROZAT AZ INFORMÁCIÓ- ÉS TUDÁSFOLYAMATOKRÓL 10.; 2006/1; 9-30. O.

Anonim-e az anonim böngésző? Technológiák és szolgáltatások elemzése

Gulyás Gábor György

Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék
1111 Budapest, Sztoczek u. 2. St. ép. I. em. 117.
Telefon: (36 1) 463-1832, Fax: (36 1) 463-4035
e-mail: gaborgulyas@gmail.com

Absztrakt

Az Internet egyre szélesebb körű elterjedése megnövelte a benne rejlő üzleti potenciált és új eszközök bevezetését tette lehetővé. Az új eszközök használatával a felhasználó anonimitása veszélybe kerül, számára ellenőrizhetetlen módon kerülnek adatai mások birtokába, és válnak felhasználhatóvá, tudta és beleegyezése nélkül. Az anonim böngészők megoldást kínálnak a webes tevékenységek anonimitásának megóvására. E tanulmány a megoldások lehetőségeivel és korlátaival, illetve a konkrét megvalósítások elemzésével és értékelésével foglalkozik.

Kulcsszavak: anonimitás, web, anonim böngészők, proxy, (anti-)profilozás

1. Bevezető

Az anonim böngészők olyan proxy szolgáltatást nyújtó webes, vagy valamilyen programon keresztül konfigurálható proxyk[1], amelyek a felhasználó IP címének[2] az elrejtésén túl további szolgáltatásokat nyújtanak az egyszerű anonim változathoz képest, mint például titkosítás, tartalomszűrés. A különböző szolgáltatások felkínált lehetőségei, és azoknak a minősége igen széles skálán mozog, mind az ingyenes, mind a fizetős kategóriában.

Anonim böngészőt használni számtalan okból lehet előnyös. Olyan helyeken, ahol szűrik az elérhető weboldalakat IP, domén vagy tartalom alapján (ezeket a problémákat például

[1] Olyan szerver, amely valamilyen weboldalak elérhetőségét biztosítja felhasználói felé, például azokról gyorsítótárat készít és adott esetben lekéri helyettük a lap tartalmát. Egy anonim proxy anonimitási szolgáltatásokat is nyújt.
[2] IP cím: Internet Protokoll azonosító, egy számnégyes, számonként 0-255 értékekkel.

egyből megoldja egy SSL[3]-en keresztül elérhető webes felületű anonim böngésző), esetleg megfigyelik az internetezési tevékenységünket, levelezésünket (egyes szolgáltatók egész érdekes példákat gyűjtöttek össze [1]). Ez lehet a munkahelyünkön, egy könyvtárban, vagy egyéb más nyilvános számítógépen. Egy teljesen nyilvánosan hozzáférhető gép használata után előnyös lehet, ha a böngészett oldalak nem maradnak meg a böngésző előzményeiben, illetve a gyorsítótárban sem; erre is talán a legjobb megoldás egy webes anonim böngésző lehet, hiszen a használata még külön program feltelepítését, a beállítások megváltoztatását sem igényli.

Amikor valaki meglátogat egy oldalt, akkor az érintett lap tudomást szerez például a számítógép bizonyos paramétereiről, az aktuális IP címéről, és esetleg sütiket[4] használhat, hogy későbbi azonosításra előkészítse azt. A sütiket más, együttműködő oldalak is felismerhetik, majd ahogy egyre több információ birtokába kerülnek, az adatbázisukban egy profil készül a felhasználó különböző böngészési szokásairól, vásárlási preferenciáiról. Az is elképzelhető, hogy ez a profil nem csupán egy pszeudonim aktát jelent, hanem valós név, lakcím vagy más adatok is szerepelnek benne.

Az így felállított profilt sokféle marketing célra fel lehet használni, mint például célzott hirdetések küldésére a webes felületeken, email-ben, postai levelek formájában, vagy dinamikus árak generálására. Manapság már több webes bolt alkalmazza ez utóbbi funkciót; az áraikat annak megfelelően állítják elő, hogy a felhasználó mit kedvel és mit nem.

Használatuk otthon is előnyös lehet, hiszen vannak olyan esetek, amikor családtagjaink elől szeretnénk elrejteni böngészésünk összes nyomát; ilyen, amikor például valakinek ajándékot rendelünk egy webes boltból (itt már a cím jelenléte az előzmények között veszélyeztetheti a meglepetésünket).

2. A „sötét” oldal és az adatalany

Ebben a fejezetben arról lesz szó, hogy kik azok a szereplői a felhasználóval szemben álló oldalnak, akiknek érdekében áll a felhasználó anonimitását semmissé tenni. Továbbá röviden azt is körbejárjuk, hogy a szereplőknek általánosan hogyan fogalmazhatóak meg a céljaik.

[3] Secure Socket Layer, biztonságos kommunikációt megvalósító protokoll két fél között.
[4] A sütik (cookie) a böngésző által tárolt információk, amelyeket a weboldalak állítanak be. Részletesebben a 7. fejezetben foglalkozunk velük.

2.1. A felhasználó

Az első és legfontosabb szereplő. Elsődleges szempontja, hogy amikor meglátogat egy oldalt és nem akar személyre szóló kapcsolatot teremteni a szolgáltatóval, akkor megőrizze az anonimitását, a lehető legkevesebb információt áruljon el magáról. Ideális esetben ezen információk láthatósági köre, élettartama, vagy az épp megjelenő pszeudonim alany megfelelően szabályozható és ezen adatokról kizárólag maga a felhasználó dönt (léteznek erre irányuló, fejlesztés alatt álló rendszerek, mint például a PRIME [2]). Általában ez az anonim böngészők esetében nem mondható el, inkább a tartalmi elemek szűrésének kombinálásával érvényesítheti akaratát az adatalany.

2.2. Hirdetők

A hirdetők nem akarnak az adatalany információhoz hozzáférni önmagában, legfeljebb egy vásárolt (vagy saját készítésű, de itt csak a hirdetőkkel foglalkozunk) profilt használnak fel és azonosítani szeretnék valahogy a hirdetést letöltő felhasználót, hogy azután a megfelelő hirdetésekkel bombázzák. Mivel a hirdetés célja, hogy minél többen elolvassák és minél többen rákattintsanak, így a hirdetések legtöbbször nem csak feltűnőek és animáltak, hanem sokszor felbukkanó ablakként kerülnek előtérbe, vagy a nekik szánt keretből előugorva a weboldal hasznos tartalmát eltakarják, amíg a felhasználó közbe nem lép. A legrosszabb esetben még bezárni se lehet az ilyen előugró hirdetéseket, hanem csak megvárni, míg a reklám a végére ér. A felbukkanó ablakok tipikus, régebbi trükkje hasonló volt – amikor egy felbukkanó ablakban megjelent egy hirdetés, és azt be szerettük volna zárni, akkor további ablakokat nyitott meg.

2.3. Webes boltok

A webes boltok célja, hogy minél több (visszajáró) vásárlójuk legyen. Ezt – a megfelelő reklámkampányon túl – úgy lehet egyszerűen elérni, ha személyre szabott árakkal gondoskodnak a felhasználók elégedettségéről. A profilhoz illő termékek árát csökkentik, míg a kevésbé passzentosokét növelik, így hosszú távon ugyanannyit költ a vásárló (mivel nem szükségszerűen csak a legolcsóbb termékekből választ), de elégedettebb lesz az árakkal, a szolgáltatással. A boltoknak egyszerű dolguk van, a dinamikus árazáshoz bonyolult profilra sincs szükség, egyszerű azt megfigyelni, hogy a vásárló milyen hirdetések után érdeklődött korábban.

2.4. Adatgyűjtők

Az adatgyűjtők nem használják fel közvetlenül a megszerzett adatokat, hanem csupán kereskednek velük – eladják a megszerzett adatokat, profilokat például webes boltoknak. Az ő céljuk különböző statisztikák, profil vagy email cím adatbázisok készítése, vagy egyéb adatoknak az összegyűjtése, amelyek nagy mennyiségben kereskedésre alkalmassá válnak. Tipikus eszközeik közé tartoznak például a web bugok (webpoloskák)[5], a reklámok forgalmának megfigyelése és rögzítése, különféle weboldalak belső statisztikáinak összegzése.

2.5. Szolgáltatók

A szolgáltatók roppant fontos szerepet játszanak, ugyanis a szolgáltatás igénybevételéhez a többi résztvevőnek adatokat kell szolgáltatnia a számára, továbbá lehetőséget adnak web bugok, reklámok elhelyezésére. Ennek ellenére megjegyzendő, hogy sokszor a szolgáltató nem tud róla, hogy a felületén elhelyezett reklámmal valaki visszaél – például több szolgáltatónál elhelyezett reklámokkal nyomon követi a felhasználókat.

Az előbbi kategóriák előfordulása önmagukban nem jellemző. Tipikusan egy résztvevő több funkciót is képvisel; általában aki hirdet, maga is végez adatgyűjtést. Ezen túlmenően van egy külön kategória, amely cenzúrával, adatok manipulálásával, az információszabadság csonkításával operál.

2.6. Cenzúrázó szervek

Ebbe a kategóriába tartoznak a munkahelyek, könyvtárak, ingyenes hozzáférést biztosító szolgáltatók, kormányok és általában véve az információ áramlásával kapcsolatos szolgáltatást üzemeltetők (például elektronikus könyvtárak üzemeltetői, keresőmotorok, Internetes újságok). Ezen kategóriába eső szervek tiltását sok esetben meg lehet kerülni az anonim böngészőkkel[6].

[5] Apró, helykitöltésre használt, vagy elrejtett képek, amelyek más oldalról töltődnek be, ez által lehetőséget adnak harmadik félnek a felhasználó nyomonkövetésére ld. még [3]. A reklámok is hasonló lehetőségekkel rendelkeznek.

[6] Például ilyen eset volt, amikor a Google a kereséseit a kínai felhasználóknál cenzúrázni kezdte egy a kormánnyal kötött egyezség alapján. A felhasználók anonim módon férhetnek hozzá a nem cenzúrázott szolgáltatáshoz anonim böngészőkön keresztül. [13]

3. Milyen információk vannak veszélyben? A visszaélés lehetőségei

Ebben a fejezetben néhány olyan tipikus információt vizsgálunk meg, amelyek felfedése hasznos lehet az információgyűjtőknek. Nem csak az anonimitás kompromittálódását okozó információkról van szó, hanem statisztikák, felmérések, profilkészítés alapanyagaként szolgáló adatokról is.

A jelenlétünket első sorban egy IP cím bizonyítja, ez általában egy bennünket egyértelműen azonosító számsor (kivéve néhány esetben, mint például amikor NAT[7] mögül kapcsolódunk). Az IP címet statikus vagy dinamikus mivoltától függetlenül (hiszen ez csak a felhasználhatóság időtartamát korlátozza) lehet használni az oldalak közötti nyomon követésre. Ennek az előnye, hogy különösebb technológiát nem igényel, a rosszindulatú félnek mindössze fel kell jegyezni ezt a címet egy olyan adatbázisban, amelyet a szövetségeseivel megoszt. Ebből a közös adatbázisból később ki lehet nyerni a felhasználói profilt. Ezt a technikát más jellegű azonosítókra is lehet alkalmazni, például web bugokon keresztül feltöltött sütiben tárolt kódokra is.

A sütiben tárolt azonosítók és egyéb adatok halmozhatók, és ezekből profil készíthető. A profilt a különböző oldalakon megadott adatok alapján állítják össze. Ha email címeket is használtunk, akkor ezt is hozzácsaphatják, de ennél súlyosabb adataink is kiszivároghatnak, mint például a lakcímünk egy vásárlás során.

A profilokat adatbázisokban gyűjtik. Ha több ilyen adatbázis létezik, akkor ezek között elég gyakori is lehet a csere, a felhasználók profiljai pénzért vagy más profilokért cserélnek gazdát. A profilokat azután marketing célokra felhasználhatják, például reklámmal bombázzák az illető email postafiókjait, vagy a különböző weboldalakon a profil szerinti preferenciáinak megfelelő hirdetéseket nyújtanak elé.

Manapság nagyon sok oldalon megfigyelhetőek célzott hirdetések. A legelterjedtebbek a társkeresős hirdetések, amelyek általában kitalálják, hogy honnan böngészünk és ennek megfelelő ál-társkereső hirdetésekkel próbálnak érvényesülni. Ezek az információk, mint például az előnyben részesített nyelvek listája, ha egy oldal több nyelven is elérhető, vagy a

[7] Network Address Translator: több számítógép egy publikus IP című számítógépen keresztül fér hozzá az Internethez.

böngésző által használt felbontás, minden oldal számára elérhetőek[8] (az előbbire például az IP cím alapján is lehet következtetni[9]).

Egyes oldalak felhasználhatják az ún. URL-Referer karakterláncot is, amely az előző weboldal címét adja meg a látogatott weboldalnak[10]. Így szintén sütik nélkül követni lehet, hogy valaki melyik weboldalon kattintott egy hirdetésre.

Vannak olyan helyben tárolt tartalmak is, amelyek kompromittálására általában a hálózaton keresztül nincs lehetőség. Ilyenek a böngészőben eltárolt előzmények és a gyorsítótár. Ezeket általában vírusok, férgek vagy hasonló információgyűjtő programok (tipikusan spyware programok) analizálják profilkészítés szempontjából. A modern böngészőkben beállítható az ilyen tartalmak készítésének kiiktatása, rendszeres törlése, bár ha ezt a beállítást nem szeretnénk minden weblapra kiterjeszteni, akkor kényelmesebbnek bizonyulhat csak a titkolni kívánt weboldalakat anonim böngészőben megtekinteni.

Ide sorolhatjuk a sütiket is, amelyek analizálása egy olyan szoftver lehetőségeivel, amely mindent lát (hiszen a weboldalak csak a hozzájuk tartozó sütiket látják) átfogó profil készítéséhez vezethet. Ez a profil lényegesebben átfogóbb jellegű, mint az előbb felsorolt technikákkal készültek, hiszen – ha nem gondoskodunk az efféle melléktermékként képződő adataink rendszeres szűréséről, törléséről – a felhasználható alapanyagok nem korlátozottak, gyakorlatilag minden rendelkezésre áll.

4. Lehet ezt jogszerűen, etikusan is?

A felsorolt technológiák többsége etikus célokat is szolgálhat. Vegyük először a különböző azonosításra szolgáló technikákat. Ezek a technikák szolgálhatnak tényleges statisztika-készítési célokat, de jogszerűen csak akkor, ha a felhasználó ehhez hozzájárul. Hasznos és etikus lehet, ha például valaki a saját weboldalát monitorozza és ez alapján készít statisztikát a felhasználók ízléséről, preferenciáiról. Ezeket az adatgyűjtési és egyéb megfigyelő tevékenységeket belefoglalván az oldal adatvédelmi nyilatkozatába[11], s a szolgáltatásokhoz csak akkor férhet hozzá a felhasználó, ha elfogadja azt.

[8] Érdekes megfigyelni, hogy az elárult információk böngészőnként különböznek. A [4] weboldalon kipróbálhatjuk, hogy milyen információk elérhetőek a weboldalak számára.

[9] Például, próbáljuk lehívni a www.google.com keresőt egy anonim böngészőből és azon kívülről: más nyelven fog megjelenni (ha böngészőnkben magyar nyelv az alapértelmezett).

[10] Az URL a Uniform Resource Locator rövidítése. URL-ekkel weblapokat, webes és általános interneten elérhető szolgáltatásokat lehet azonosítani a protokoll, hely, port, lokális fájl és további paraméterek megadásával.

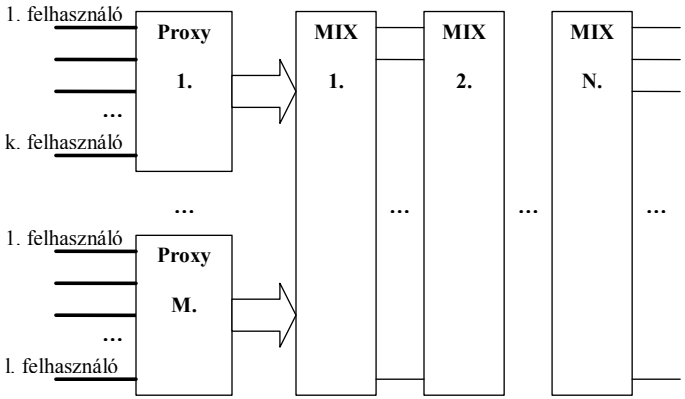
[11] Erre jó példa a Gmail adatvédelmi nyilatkozata, amely elérhető az [5] címen.

Ez nem mindig járható út. Hiszen ha például egy oldal tartalma tipikusan kilinkelhető külső oldalakra, akkor meg kell oldani, hogy ha a felhasználó külső weblapról érkezik, előbb el kell fogadtatni vele, hogy a weblap az érkezési címet rögzíti, vagy felhasználja egy statisztikához. Ez gyakran nem praktikus, a kényelmetlenség kihathat a felhasználók számára.

Egyes technikákat azonban nem lehet etikusan használni. Ilyen a dinamikus árazás. Ezzel a technikával az a probléma, hogy akármilyen formában is használják, megfosztja a vásárlókat az esélyegyenlőségtől, hiszen akármilyen céllal is működik ez a rendszer, az árak elosztása sosem lehet igazságos a felhasználók között.

5. A szolgáltatások technológiai háttere

Egy jó minőségű szolgáltatást nyújtó anonim böngésző működését láthatjuk az 1. ábrán. A felhasználók csoportjai különböző proxy szervereket érnek el (akár hagyományos proxy, vagy webes proxy alapon), a szerverekig a kapcsolat titkosított. Ez SSL protokollon keresztül történik. A proxy (esetleg webszerver is) és a felhasználó között titkosított a kapcsolat, a proxy tartalomszűrést végez, majd a külső szakaszon MIX-eken keresztül megy a forgalom.



1. ábra: Egy jó minőségű szolgáltatást nyújtó anonim böngésző

Mind a bejövő és mind a kimenő üzeneteket a proxy szerver dolgozza fel, a kommunikáció a weboldalakat kiszolgáló szerverek felé egy MIX rendszeren keresztül zajlik. A MIX

rendszer állomásokból épül fel, amelyek között a kommunikáció általában egy meghatározott sorrendben történik (MIX lánc), kódolt formában. A MIX-ek akár földrajzilag lényegesen különböző helyen is lehetnek (más városokban, országokban).

Egy megfelelő MIX struktúra lehetne például a JAP rendszeré: onion routing alapú MIX technikát használ[12]. A szimmetrikus kódolás AES (128 bites kulcs) algoritmussal, az aszimmetrikus pedig RSA kódolással (1024 bites kulcs) történik. Ez a mai kriptográfiai követelmények eleget tesz.

A MIX-ekkel szemben fontos kritériumokat kell támasztani, különben értelmüket vesztik. Az ideális MIX hálózat véletlen csomagokat szúr be a forgalomba, amelyeket véletlenszerűen generál és nyel el, továbbá a forgalmat kiegyenlíti, hogy a csomagok számából és az időben változó terheltségből ne lehessen a MIX állapotára következtetni. A kísérletezések kizárása érdekében az is fontos, hogy egy személy ne tudjon egyszerre sok klienst futtatni, hiszen így ismételten következtetéseket vonhat le a rendszerről. Ez utóbbi kritériumot érdemben csak a fizetős szolgáltatások tudják garantálni, ugyanis csak ezen hálózatokban nem elég kifizetődő ez a támadási módszer.

A bejövő forgalmon a proxy komplex tartalomszűrést végez, a lekért oldalt átalakítja, a nem kívánatos elemeket eltávolítja belőle: ez tipikusan a különféle szkript nyelvek kódjainak[13] (pl. JavaScript), és különböző aktív elemeknek (pl. Flash, Java) a szűrését és törlését jelenti.

A proxy szerveroldali sütikezelést nyújt, a felhasználó felé nem továbbít egyet sem. Adott esetben ez a funkció kikapcsolható, vagy némely oldalak sütijei engedélyezhetőek a felhasználó felé is. Bár jelenleg nincs olyan szolgáltatás, amely ezeken a lehetőségen túlmutatna, a cél egy teljes adminisztrációs felület, ahol a hozzáértő felhasználók a szerveroldali sütikkel bármilyen műveletet elvégezhetnek.

Korábban nem foglalkoztunk vele, hogy proxy vagy webes proxy szolgáltatásról van szó. Ha egy ideális szolgáltatásról beszélünk, akkor mindkét funkció elérhető, hogy mindig a szolgáltatás legkedvezőbb tulajdonságai szerint lehessen választani: otthonról, vagy a munkahelyről egy konfigurációs programmal használható, nyilvános számítógépről pedig egy webes proxy-n keresztül elérhető a szolgáltatás.

[12] Bővebb leírása a [6] -ban.
[13] A szkript kódokat tekinthetjük úgy is, mint a weboldalakba beépülő, korlátozott lehetőségekkel bíró programok.

6. A proxy funkció vizsgálata[14]

A böngészőket a proxy funkció vizsgálata szempontjából két csoportra bonthatjuk. A két csoport tagjai különböző képességekkel és lehetőségekkel bírnak, a továbbiakban ezeket vizsgáljuk. Elképzelhetőek olyan anonim böngészők, amelyek mindkét csoportba beletartoznak – hasonlóan az előző fejezetben elemzett szolgáltatáshoz. A később bemutatásra kerülő böngészők e tulajdonság alapján két különváló csoportra bonthatóak.

6.1. Webes proxy böngészők

A webes proxy böngészők szolgáltatásait egy adott URL-en keresztül lehet igénybe venni. Ehhez a terminálon, amelyen dolgozunk, semmilyen beállítást nem kell átállítani, így szembetűnő a legnagyobb előnye ennek a csoportnak: az áttetsző használat. A proxy működése bármikor igénybe vehető illetve kiiktatható, anélkül, hogy a beállításokba bele kellene nyúlnunk.

Ebből adódóan egy olyan számítógépen keresztül is igénybe vehető ez a szolgáltatás, ahol nem lehet a beállításokat módosítani, vagy nem telepíthetünk programokat, esetleg egyéb hálózati tiltások léteznek (például csak a 80-as portokra lehet kifelé csatlakozni), hiszen az általános keretprogram maga a böngésző szoftver.

Ez egyben hátrányt is jelent. Sajnos nem minden (tipikusan) alkalmazott technológiára léteznek még egységesen elfogadott szabványok (mint például a JavaScript esetében), így nagy eltérések lehetségesek a különböző márkajelzésű böngészők esetén, sőt, az adott termékek különböző verziói között is jelentős eltérések lehetnek. Mint a későbbi tesztekből is kiderül, ezen okok miatt több anonim böngésző csak néhány böngésző programmal képes együttműködni, amivel bizonyos esetekben nem csupán a többi programot, hanem majdnem az összes operációs rendszert is kizárják a lehetőségek sorából.

További hátrány az URL-en történő elérés, mivel az anonim böngészők használata könnyen gátolható az adott szolgáltatás címének, vagy a szolgáltatást nyújtó gép IP címének a blokkolásával.

A webes proxy alapú anonim böngészőknek sajátos módon kell megoldaniuk a proxyn átengedett különböző oldalak tartalmának felismerését, feldolgozását és fordítását. Mivel ezek a megoldások a legtöbb esetben nem teljesek, így különböző módszerekkel a szűrések

[14] A proxy működéséről és anonimizáló funkciójáról részletes elemzést nyújt [7]

kikerülhetők (legtöbb esetben csak az adott elemek teljes körű blokkolása jelenthet megoldást), azaz a böngészőt rá lehet kényszeríteni, hogy ne a proxyn keresztül töltsön le bizonyos elemeket. Ennek a hibának a forrása az áttetsző működésből adódik.

6.2. Valódi proxy alapú szolgáltatások

Az ilyen anonim böngészők legszembetűnőbb eltérése a másik csoporthoz képest, hogy nem képesek transzparens működésre. A használatukhoz be kell állítani a közbeiktatott proxy kiszolgáló tulajdonságait a böngészőbe, vagy egy külső programra van szükségünk.

A külső program feltelepítésével használható anonim böngészők talán legelőnyösebb tulajdonsága, hogy lehetőség nyílik mások számára proxyként megosztani a szolgáltatást. Az anonim böngészők ezen csoportja ezzel elegánsan kiküszöböl több hibát is, amely az előző csoport tagjaira jellemző. Ezek az 1. táblázatból olvashatóak ki.

A táblázatban további szempontok is láthatóak. Egy ilyen jellegű szolgáltatásnál fontos, hogy sokan használják, ugyanis ekkor nehezen lehet megfigyelésekből következtetéseket levonni (például forgalomanalízissel, ha MIX-eket is használ a proxy rendszer). A webes proxy alapú anonim böngészőket vélhetően egyszerű alkalmazhatóságuk miatt sajnos többen kedvelik.

A böngésző által a rendszerben hátrahagyott információk is szivárgáshoz vezethetnek. A böngésző a háttértárba elmenti a már látogatott lapok tartalmát, illetve a lekérdezett lapok címét is naplózza, néhány napra visszamenőleg (a tárak mérete beállításfüggő).

1. táblázat: a két böngésző-típus összehasonlítása

	Webes proxy	Valódi proxy
transzparens működés	X	
platformfüggetlenség		X
tipikusan sok felhasználó	X	
nehezen szűrhető / tiltható		X
web forgalom csak a szolgáltatáson át		X
háttértárazás és előzmények elrejtése	X	

Sajnos vannak olyan problémák, amelyek ellen egyik böngésző típus sem képes szűrő jellegű védelmet nyújtani, s csak az adott elemek blokkolásával lehet elérni a magasabb fokú védelmet. Ilyen elemek azok az aktív elemek, amelyek képesek elindulásuk után felcsatlakozni egy szerverre, felfedve előtte például az IP címünket.

7. HTTP protokoll „állapotai", a sütik

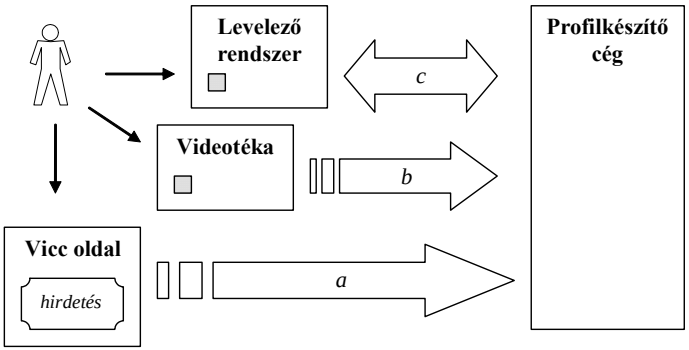
Ha a támadónak, azaz a veszélyes oldalnak nincs lehetősége valamilyen külső jel alapján azonosítani a látogatót minden látogatás alkalmával, azaz például nem elérhető számára a látogató IP címe, akkor valahogyan meg kell jelölnie a látogatót. A HTTP[15] protokoll egy állapotmentes, statikus protokoll; önmagában két kiszolgálás között nincs kapcsolat, a két igény kiszolgálása egymástól függetlenül történik.

Ennek az állapotmentességnek a feloldására vezették be a sütik használatát, amelyek egy folyamattá kapcsolják össze a lekérdezéseket, mivel rajtuk keresztül a kiszolgáló emlékezhet a korábbi lehívásokra, azok eredményeire. A sütik tömör lényegüket tekintve a felhasználó gépén elhelyezett név és adat párok, amelyeket csak az adott kiszolgáló érhet el. Ezen adatok célja az is lehet, hogy a felhasználókat egyértelműen azonosítsák velük. Ezt az azonosítót eltárolják egy adatbázisban, ahol különböző adatokat gyűjtenek még emellé, azaz profilt készítenek a felhasználóról.

Az azonosító sütit csak a létrehozó oldal kérdezheti le, és előnyösebb a támadó szempontjából, ha több oldalon keresztül is követni tudja a felhasználót, s így róla színesebb profilt készíthet. Erre „megoldásként" a reklámokon keresztül szoktak megfigyelni a látogatókat: elhelyezik a hirdetéseket különböző oldalakon, majd figyelik,

[15] Hypertext Transfer Protocol, weblapok szállítására alkalmazott protokoll.

hogy honnan érkezik a lekérdezés. Nem mindenhová reklámokat tesznek, néhol a már említett apró, 1x1 méretű vagy helykitöltésre használt képek, a web bugok közvetítik a felhasználó jelenlétét.



2. ábra: Egy profilkészítő és hirdetésekkel foglalkozó cég forrásai. A felhasználót már azonosították, szerepel az adatbázisukban

A 2. ábrán egy elképzelt működés látható arról, hogy a profilkészítő cég miképp gyűjt információt sütik használatával.

1. A vicc oldal minden lapján megjelenő hirdetésen keresztül követik a barangolását.
2. A videotéka lapján egy web bug-on keresztül értesülnek, milyen filmkategóriákat kedvel.
3. A levelezőrendszer lapján is van egy web bug és az üzemeltetőkkel kapcsolatban áll a profilkészítő cég, így tudják a felhasználók ottani email címeit is a profilhoz csatolni.

Ezen információk alapján más oldalakon, esetlegesen levélben, spam[16] formájában célzott hirdetésekkel bombázzák a felhasználót. Ha a cégnek kapcsolata van webes boltokkal is, akkor ezekben az üzletekben a profiljának megfelelően dinamikus árakat tárhatnak elé.

[16] Elektronikus levél formájában érkező kéretlen hirdetés.

Miképp az jól látható, a süti-kezelés fontos részét képezi az anonim böngészőknek, ugyanis könnyen ezen áll, vagy bukhat az anonimitás kérdésének egésze. Ennek alapján a böngészőket több csoportba (osztályba) sorolhatjuk. Az alábbi sorrend a legkedvezőbbtől a legkevésbé kedvező felé halad.

sütik szűrése, blokkolása és azok szerver oldali tárolása

1. sütik szűrése és blokkolása
2. sütik szűrése vagy blokkolása
3. sütik blokkolása

A felsorolásban a sütik szűrése alatt elsősorban egy külső helyről érkező süti felkínálások kiszűrését jelenti itt (erre némely böngészőprogramok is képesek), ami a felhasználók profilozási lehetőségét korlátozza (az egy oldalon belüli profilozás a kisebb baj). Továbbá a gyanús felkínálások szűrését is jelentheti ez, bár ezt kevesebb anonim böngésző ismeri.

A legfontosabb szempont a távoli süti-kezelés. Ennek előnye, hogy az adott munkamenetben összeszedett minden süti tetszés szerint törlésre kerülhet a végén, illetve a későbbi visszalátogatás során ezekhez újra hozzáférhetünk, ha a munkamenetet a szerveren tárolja. A távoli süti-kezelés technika alkalmazásával – ha konzekvensen az anonim böngészőn keresztül látogatjuk a kártékonynak vélt oldalakat – az összes potenciálisan veszélyesnek titulált süti egy helyen, a helyben tárolt (böngészői) adatbázistól elválasztva kerül tárolásra.

8. Néhány anonim böngésző elemzése

Az alábbiakban néhány olyan nyilvános, az interneten bárki számára elérhető anonim böngésző működésének elemzését nyújtjuk, amelyek a fentiekben ismertetett technikai megoldások jellemző példái. Az elemzés alapját a szerző által végzett empirikus vizsgálatok, esettanulmányok képezik.

8.1. @nonymouse [8]

Egyszerű, gyors és ingyenes szolgáltatás webes proxy alapokon. Az anonim böngésző szolgáltatáson kívül névtelen levélküldésre és hírcsoportok névtelen megtekintésére is van lehetőség. A szolgáltatás két nyelven elérhető: angolul és németül. Bosszantó jelenség, hogy az induló és a nézett oldalakon is megjelenik egy állandó reklám (bezárására van lehetőség, de minden betöltéskor újra megjelenik).

Nincsenek beállítások és nincs navigációs panel. Ennek hátránya, hogy újabb lap lehívásához vissza kell menni a kezdőlapra, amiről igen könnyű elfeledkezni, s így a védelem tudatában a proxy hatáskörén kívülre keveredni; továbbá ha az oldal gátlón hat egy megbízható weblap működésére, azt nem tudjuk befolyásolni.

A szűrési mechanizmusa is igen egyszerű, reklámok, dinamikus elemek szűrésére nem képes. Működésében sokszor jelennek meg hibák; előfordul, hogy hivatkozásokat rosszul nyit meg, bizonyos lapok rosszul, vagy egyáltalán nem jelennek meg. Egyszerűen ki lehet csalni a szolgáltatásból a felhasználót nem proxy mögül látható lapokra[17].

8.2. beHidden [9]

Webes proxy alapú szolgáltatás. A szolgáltatások nagy részét ingyenesen is igénybe lehet venni, az ingyenes szolgáltatás egyik legerősebb korlátja a forgalomkorlátozás. A napi limit 50 megabájt forgalomra terjed ki, ami elsőre soknak tűnhet, ám néhány galéria megtekintésével könnyen felemészthető. A szolgáltatás fizetős részében továbbra is megmarad a limit, csak megnő. Ezen túl további funkciókhoz is hozzáférhetünk.

Ha szeretnénk titkosítani a böngészőnk és a szerver közötti kapcsolatot, akkor ennek az alkalmazására is csak a fizetős szolgáltatásban van lehetőségünk, és ekkor a titkosítás SSL protokollon keresztül történik. Egyébként csak az URL-ek titkosítására is van lehetőség, amely a felhasználó és a proxy közötti szakaszon a forgalom teljes megfigyelése mellett nem jelent túl sok védelmet egy komolyabb támadóval szemben. Ha szeretnénk a sütik használatát engedélyezni, ahhoz is elő kell fizetni (bizonyos oldalak csak így működnek).

A szolgáltatás kicsit bizonytalannak mondható. Ugyan nem igényli külső program telepítését, vagy használatát, de többnyire csak Internet Explorer böngészőből hajlandó működni, s az esetek egy részében az oldalak letöltése egyszerűen leáll. A tesztelés alatt néhányszor előfordult, hogy Firefox böngészőprogramból is működött a szolgáltatás, de ez kivételes esetnek tekinthető. A sebessége sem mondható túl jónak, noha a felkínált lehetőségek egészen jók (ami még hiányzik, hogy nem tudja szűrni a Flash betéteket).

A legzavaróbb elem a szolgáltatásban, hogy néha, ahelyett, hogy betöltené a kért oldalt, felajánlja a regisztráció lehetőségét. Erről a lapról ugyan lehetőség van a folytatásra, de előfordult, hogy ez sem működik.

[17] Egyszerű JavaScript trükkökkel, vagy Flash animációval.

A webes böngészővel való kísérletezés alatt a legdurvább hibának az bizonyult, hogy a JavaScript szűrés bekapcsolásakor az anonim böngésző motorja védelmet gyakorlatilag nem nyújt.

8.3. The Cloak [10]

Az előzőekhez hasonlító webes proxy jellegű anonim böngésző. Ez a szolgáltatás is két részre válik; a fizetős szolgáltatás itt azonban funkcionalitás szempontjából nem különül el az ingyenestől. Lényegében a fizetős szolgáltatás sávszélesség-növelt, az anonimitást biztosító funkciók és beállítások egyébként is hozzáférhetőek.

A szolgáltatás az előbbinél lényegesen gyorsabb és a beállítási lehetőségek lényegesen könnyebben szabályozhatóak. Itt böngészésünket nem egy állandóan látható vezérlőpult kíséri, hanem egy kis gombra kattintva hívhatjuk azt elő. Előnye, hogy nem vesz el feleslegesen felületet, de könnyen kikeveredhetünk a szolgáltatásból, ha arról megfeledkezve beírunk egy új címet.

A szolgáltatás leírása nem említi, de létezik egy kvóta határ, ami az ingyenes szolgáltatásra vonatkozik. Ennek az aktuális állapotáról szintén a vezérlőpulton informálódhatunk. Mielőtt a böngészést elkezdenénk, lehetőség nyílik arra is, hogy előre beállítsuk a böngészésre vonatkozó opciókat – minden opcióról részletes, beszédes információt lehet kérni.

Lehetőség nyílik SSL használatára a proxy és a felhasználó számítógépe között. Külön kell bekapcsolni, alapból titkosítatlan HTTP protokollon keresztül zajlik a forgalom.

A JavaScript engedélyezése átírás mellett esetlegesen túl szigorú lehet – a kódok nagy részét törli a böngésző, így előfordulhat, hogy néhány oldalt nem lehet a szolgáltatáson keresztül megtekinteni, mivel az átírásos engedélyezés mellett csak a törlésükre van lehetőség.

További érdekesség, hogy a Flash reklámok szűrését is elég jól kezeli a böngésző. A legtöbbjét helyesen kiszűri, s ha engedélyezett az objektumok megjelenítése, általában azok közül sem szűr feleslegesen.

8.4. JAP [11]

A JAP egy külső, Java technológián alapuló program feltelepítését igénylő anonim proxy alapú szolgáltatás. A feltelepítés után a böngészőnkben a proxy adatait be kell állítani,

ehhez a súgó részletes, ábrákkal illusztrált segítséget nyújt. Képes együttműködni a korszerű böngészők legtöbbjével.

Forgalomszűrésre nem képes sem a feltelepített program, sem a proxy, és emiatt, bár a szolgáltatást gyakorlatilag csak a böngészőnk átállításával tudjuk (vagy a program leállításával) elhagyni, meghagyja az oldalakba beágyazódó objektumok (pl. Java appletek) számára a lehetőséget, hogy felfedjék IP címünket. Ez ellen csak a böngészőnk védelmi beállításai, vagy más tartalomszűrő programok segítségével tudunk védekezni. A szolgáltatás proxy jellegéből adódóan a böngészőnk a szokásos módon tárolja az előzményeket és készít gyorsítótárt.

A forgalmunkról a rendszer kvótát nem tart számon, cserébe a felhasználható adatátviteli sebesség alacsony (pár száz és ezres nagyságrendű felhasználószám mellett is), ami bizonyos szempontból a forgalomanalízist megnehezíti. A forgalomanalízis további zavarása érdekében a teljes forgalmat többlépcsős MIX rendszeren vezetik keresztül. A MIX rendszer a korábban említett onion routing technológiára (5. fejezet) épít, 128 bites kulcsú AES és 1024 bites kulcsú RSA algoritmusok használatával.

A JAP szolgáltatásának egyik nagy előnye, hogy ha felcsatlakozunk egy szerverre, akkor a többi felhasználó számára lehetőséget nyújthatunk, hogy a szolgáltatást rajtunk keresztül érjék el. Ennek a funkciónak köszönhetően ha nem elérhető a központi szerver (vagy az információs szolgáltatás, ahol az elérhető szerverek listája elérhető), mert esetleg letiltották az IP címét, az ilyen felhasználókon keresztül erre lehetőség nyílik. Mivel a szolgáltatás-továbbítást nyújtó felhasználók IP címe széles skálán mozoghat, szűrésük IP cím alapján nem lehetséges.

8.5. Primedius WebTunnel [12]

A Primedius WebTunnel a JAP-hoz hasonló szolgáltatás, amely szintén csak azután használható, hogy feltelepítettük a helyi számítógépre (csak Windows és Mac OS X operációs rendszerekre érhető el). Az ingyenes verziójának használatához is regisztrálni kell, s az érvényes regisztrációt más számítógépeken is igénybe lehet venni (a szoftver feltelepítése után).

Miután elindítottuk, SSL kapcsolatot létesít a szerverrel, és automatikusan bejelentkezik. Ezen idő alatt a kiválasztott böngésző programot automatikusan beállítja, hogy rajta keresztül csatlakozzon az Internetre (kilépéskor visszaállítja a korábbi állapotot).

A beállításokat egy animált kezelőfelületen keresztül érhetjük el, témakörönként szétbontva. A legelső lapon információt kapunk a szolgáltatás állapotáról, és addigi működésének statisztikáját is meg lehet tekinteni, mint például a blokkolt sütik, felbukkanó ablakok, vagy a bejelentkezett felhasználók számát. Továbbá az az információ is itt található, hogy az ingyenes szolgáltatásban engedélyezett napi kvótából mennyit használtunk fel. A tesztelés alatt ez a számláló esetenként nem működött (sőt, volt olyan, hogy kvóta mennyiség se volt feltüntetve).

A hálózati beállítások között szerepel egy érdekes opció, amelynek segítségével akkor is fel tudunk csatlakozni a szolgáltatáshoz, ha a Primedius központi szerverei elérhetetlenek, például szolgáltató oldali tiltás miatt. Sajnos erről a beállításról a honlapon jelenleg információ nem található, és a kliensben se lehet beállítani (kipipálására a program lefagy).

A szűrési lehetőségek kifinomultak: le lehet tiltani a lapokba beépülő Java programokat, a sütik kezelése három biztonsági szinten szabályozató, s végül kikapcsolható az URL-Referrer is, de ez csak a fizetős változatban. A süti szűrési szintek adják magukat: az alacsony szinten mindegyik engedélyezett, a magason mindegyik tiltott. A kettő közti fokozat választása esetén a sütik a szerver oldalon kerülnek tárolásra, és csak a látogatott oldaltól fogadja el őket, harmadik féltől nem. Továbbá reklám szűrésére is képes. A felbukkanó ablakokat lehet szimplán blokkolni, vagy a megnyitásukat felhasználói engedélyhez kötni. Utóbbi esetben a megnyitásuk előtt a program kiírja a benne szereplő oldal elérési címét és az ablak azonosítóját, és az engedélyezésre vár. Sajnos ezek mellett nagy hibája, hogy flash animációkat, így reklámokat sem képes szűrni.

A Primedius WebTunnel több böngésző programmal is képes együttműködni. A megfelelő program megnevezése mellett megadható, hogy milyen információkat tárolhat a böngésző program a felhasználó tevékenységről, s a kiválasztottak törölhetőek tetszés szerint bármikor (automatikus törlésre lehetőség nincs).

Ennek az anonim böngészőnek a beállítási lehetőségei tűnnek a legátfogóbbnak, s az ingyenes próbaverzióban is viszonylag sokat használhatunk ezek közül. Sajnos a böngészést megkeserítik a program állandó lefagyásai: a próbaverzió szinte lépten-nyomon lefagyott és állandóan újra kellett indítani (általában ez utóbbi több időt vett igénybe, mint maga a használat). E tulajdonsága mellett igen zavaró még az 1 MB forgalomkorlátozás is, ami a mai weboldalak mellett igen könnyen elhasználható a sok kép és beágyazott Flash animáció miatt, így sajnos az is még szomorúbb tény, hogy ez utóbbit nem lehet szűrni.

Használata közben további súlyos problémát jelenthet, hogy a magyar oldalak nagy hányada nem elérhető az anonim böngészőn keresztül[18].

9. A szolgáltatások összesítő értékelése

Az alábbi táblázat összefoglalja az eddig vizsgált anonim böngészők által nyújtott szolgáltatásokat.

2. táblázat: anonim böngészők összehasonlítása

@nony-mouse	beHidden	The Cloak	JAP	Primedius WT [19]	Vizsgált tulajdonság	Kategória
X				X	gyors átvitel	Sebesség
		X	X	X	kis válaszidő komplex lap esetén	
X	X	X			webes felületről elérhető (6.1.)	Kapcsolat
			X	X	külső programmal használható (6.2.)	
			X	?	MIX használata	
			X	?	nem blokkolható belépési pontok	
	X	X		X	korlátozott forgalom, sávszélesség	
	X	X	X	X	titkosított kliens-proxy kapcsolat	
S	T	ST			JavaScript Szűrés, Tiltás	Szűrés
C	A	A		A	süti kezelési osztály	
	J	JF		J	Java, Flash objektumok tiltása	
		X		X	reklámok szűrése	
	X			X	felugró ablakok gátlása	
				X	URL-referer szűrése	
		X			hibás kódok szűrése	
	X	X	X	X	navigációs és beállítási felület	Kezelhetőség
X	X			X	reklám a szolgáltatásban	
	X	X	X	X	használható szolgáltatás leírás	
X	X	X			észrevétlenül megkerülhető[20]	
X		X	X	X	böngésző-függetlenség	Egyebek
		X	X		megbízható minőségi szolgáltatás	
	X[21]			X	gyorsítótárazás és előzmények védelme	
	X	X	X		naplózó szolgáltatás	

[18] Például a www.szanalmas.hu nem, de a www.index.hu elérhető. Ez, mint később kiderült, felhasználónként eltérő lehet: némely felhasználóknál elérhetőek a lapok, míg másoknál sohasem.

[19] A Primedius WebTunnel szolgáltatása feltételezhetően tartalmaz MIX-eket és nem blokkolható belépési pontokat a szolgáltatáshoz, de erről információ nem található a honlapjukon.

[20] Ez jelenthet mind figyelmetlenségből eredő kilépést a szolgáltatásból, mind szándékos cselezést.

[21] Kikapcsolható.

Ahogy a fenti táblázatból is látszik, igazán jellegzetes minta nem adható meg a szolgáltatások típusai között (mint például a 6. fejezet csoportosítása), kivéve néhány hálózati tulajdonságot tekintve. Azonban így globálisan szemlélve is össze lehet mérni a szolgáltatások nyújtotta előnyöket, hátrányokat, hogy egységes összefoglaló képet alakíthassunk ki a vizsgált szolgáltatásokról.

Sajnos egyik vizsgált böngésző sem emelhető ki a többi közül egyértelműen pozitív összképe alapján. Sok szolgáltatás tesz hangzatos ígéreteket, s a legtöbb ezt be is váltja, de sajnos a megvalósítás a legtöbb esetben hibás. Ez a Primedius WebTunnel és a beHidden szolgáltatásaiban jelentkezik erőteljesen, amelyek rendszeresen és igen sűrűn előbukkanó hibáikkal használhatatlanná teszik a szolgáltatást.

Az @nonymouse böngésző legnagyobb hátránya és előnye is egyszerűségében rejlik. Használata ugyanis rendkívül egyszerű, viszont nincsenek beállításai, s így a beépített egyetlen biztonsági profilt vagy megfelelőnek találjuk vagy sem – választásra nincs lehetőség. A böngésző ráadásul egyszerű JavaScript kódokkal becsapható, azaz például a szolgáltatáson keresztül lehívott oldalak olyan új ablakokat tudnak megnyitni, amelyekben a böngészés már nem az @nonymouse-n keresztül folytatódik. Ezzel szemben a többi böngésző lényegesen szkeptikusabb arculatot mutatott a JavaScript kódok tekintetében, mint például a The Cloak szolgáltatása, amely a gyanúsnak tekinthető kódrészeket egyből törölte. Érdemes észrevenni, hogy a proxy csoportba tartozó szolgáltatások (6.1.) nem foglalkoznak ezzel a veszéllyel, mivel a szolgáltatás nem kerülhető meg ilyen trükkökkel.

A többi szolgáltatás az adatátviteli sebességet tekintve nem mondható jónak, a Primedius WebTunnel mondható még viszonylag gyorsnak, míg a többi csak nagy ritkán ér el használható sebességet. A web böngészése során általánosan fontos szempont, hogy a kért weblap gyorsan válaszoljon, s adott esetben fontos, hogy ehhez az anonim böngésző ne toldjon sokat. Ez a legtöbb böngészőnél jónak bizonyul, míg az @nonymouse szolgáltatásánál egyes komplex oldalak irreálisan sokáig töltődtek, vélhetően a proxy hibájából.

Sajnos a globális, mindent látó megfigyelő elől kevés anonim böngésző nyújt védelmet. Egyedül a JAP szolgáltatásában találkozhatunk MIX rendszer használatával. Szintén csak ezen szolgáltatás keretén belül van lehetőség olyan elérési pontok használatára, amelyek tartalékként szolgálnak, ha a központi szerver le van tiltva valamilyen okból kifolyólag. A lokális forgalmat megfigyelők ellen (is) nyújt védelmet a proxy és a kliens gép közötti titkosított kapcsolat. Ez a funkció az @nonymouse kivételével mindegyik szolgáltatásban megtalálható, s általában ez elvárható egy anonim böngészőtől.

A legtöbb esetben az igénybe vehető forgalom napi kvótamennyiséggel korlátozott (néhol előfizetés esetén is). Rendszeres használatra az ingyenes változatok így a legtöbb esetben alkalmatlanok, ugyanis a kvóta néhány weboldal megtekintésével könnyen kimeríthető. A The Cloak ebből a szempontból előnyös, ugyanis a lehető legtöbb elem letiltásával ez a kvóta lassabban fogy el.

Igen vegyes képet mutatnak a szolgáltatások a reklámok kezelését tekintve is. A mai weboldalakon a reklámok főképp Flash animációk formájában, illetve szöveges formában érkeznek[22], s ezek szűrését a szolgáltatás nem képes elvégezni, csak a régebbi típusú hirdetésekét, mint reklámozó képek, felbukkanó ablakok, de erre sem mindegyik képes. Talán kiemelhetjük ismét a The Cloak böngészőt, amely képes Flash animációk (általánosan a lapokba beépülő objektumok), Java appletek és reklámok szűrésére, mind szöveges, mind kép formában.

Néhány szolgáltatás kivételesnek tűnő szűrő funkciókkal is bír. Ilyen a Primedius WebTunnel esetén az URL-Referrer letiltása, illetve a hibás kódok szűrése a The Cloak-nál. Az előbbi igen hasznos funkció lehet, mint azt a 3. fejezetben tárgyaltuk, míg a hibás kódok célként szolgálhatnak a szűrő funkciók átejtésére.

Általában elmondható, hogy kezelhetőség szempontjából a legtöbb anonim böngésző jól szerepelt. Használható navigációs felülettel rendelkezett a legtöbb, s a szolgáltatásról is jó leírást lehetett kapni (a Primedius WebTunnel szolgáltatásánál magáról a szolgáltatásról kimerítő leírás nincs, csak az opciókhoz tartozik súgó). A webes proxy-k esetében tipikus probléma, hogy a szolgáltatásból könnyen ki lehet tévedni. Előfordulhat ugyanis, hogy a webes tevékenység során véletlenül a böngésző programnak és nem az anonim böngészőnek adjuk meg a cél URL-t. Ez a The Cloak esetében könnyebben megtörténhet, hiszen ott az új cím beírásához elő kell hozni a vezérlőpanelt (ami egy aprócska ikonon keresztül elérhető), míg a beHidden szolgáltatásában az oldal tetején látható az anonim böngésző cím mezője, így inkább elkerülhető.

Az egyik legfontosabb értékelési szempont a megbízhatóság. Kevesebben fognak egy olyan szolgáltatást használni, ami rendszeresen összeomlik, vagy nem lehet tudni róla, hogy pontosan mit csinál. Két megbízhatónak mondható szolgáltatás van az elemzettek között, a The Cloak és a JAP. Egy másik hasonlóan fontos szempont az anonim böngészők szempontjából a naplózás. Több szolgáltatás is naplót vezet a felhasználói tevékenységekről, ám saját bevallásuk szerint ezeket harmadik féllel nem osztják meg és a

[22] Például Google Hirdetések.

napló a szolgáltatással visszaélő felhasználók miatt készül. A naplóbejegyzéseket néhány napon belül törlik. Ezen feltételek teljesülése mellett a naplózási tevékenység nem jelentős visszalépés az anonimitás szempontjából, bár e feltételek érvényesülését a felhasználó nem tudja ellenőrizni.

Zárszó

Az anonim böngészők jelenleg a felhasználók tömegei előtt kevéssé ismert lehetőségeket, szolgáltatásokat kínálnak. Használatukkal jelentősen korlátozni lehet internetes szokásaink illetéktelen megfigyelését, adataink általunk ellenőrizhetetlen továbbítását, felhasználását. Hiba lenne ugyanakkor vakon bízni az ilyen szolgáltatások védelmi szintjében, hiszen – mint az elemzés és értékelés kimutatta – az alkalmazott megoldásoknak és konkrét megvalósításuknak számos gyenge pontja lehet.

Az anonim böngészők elterjedését gátló tényezők közé tartoznak a túlságosan korlátozott használhatóságú ingyenes változatok, a hibás és megbízhatatlan implementációk. A szűk lehetőségekhez képest vannak azonban jól használhatóak is, amelyeket kombinálva kellemes szolgáltatást nyerhetünk: a JAP és The Cloak szolgáltatásokat együttesen használva az 5. fejezetben leírt jó minőségű szolgáltatáshoz hasonlót kaphatunk.

Egyes elképzelések szerint a jövőben már nem anonim böngészők fogják megoldani azokat a problémákat, amelyeket ma még anonim proxy-k próbálnak kezelni: olyan rendszerek fogják biztosítani a felhasználók önrendelkezését adataik sorsa felett, amelyek szabványos rétegként épülnek be az információs és kommunikációs rendszerekbe. Ilyen átfogó megoldás víziója a nemzetközi konzorcium által fejlesztett PRIME. Az átfogó, szabványos rendszerek kifejlesztése és implementálása azonban hosszú éveket igényel, addig viszont az igények egy részét az anonim böngészők megfelelően ki tudnák elégíteni. Ehhez azonban megbízhatóbb és rugalmasabb szolgáltatásokra van szükség.

Irodalomjegyzék

[1] http://www.the-cloak.com/anonymous-proxy-why.html
[2] PRIME honlap: http://www.prime-project.eu.org
[3] Hullám Gábor: A web bug technológia – barát vagy ellenség? In: Székely Iván – Szabó Máté Dániel (szerk.): Szabad adatok, védett adatok. Alma Mater sorozat, BME GTK Információ- és Tudásmenedzsment Tanszék, Budapest 2005. március.
[4] http://www.elfqrin.com/binfo.shtml
[5] http://mail.google.com/mail/help/privacy.html

[6] http://www.wired.com/news/privacy/0,1848,64464,00.html, http://anon.inf.tu-dresden.de/desc/encr_jap_en.html

[7] Tóth Csaba: Anonim kommunikáció és a proxy szerverek. In: Sokszínű e-világ. Alma Mater sorozat, BME GTK Információ- és Tudásmenedzsment Tanszék, Budapest 2002. február

[8] http://anonymouse.org/anonwww.html

[9] http://behidden.com/

[10] http://www.the-cloak.com/login.html

[11] http://anon.inf.tu-dresden.de/index_en.html

[12] http://www.primedius.com/

[13] http://index.hu/tech/net/ggle0125/