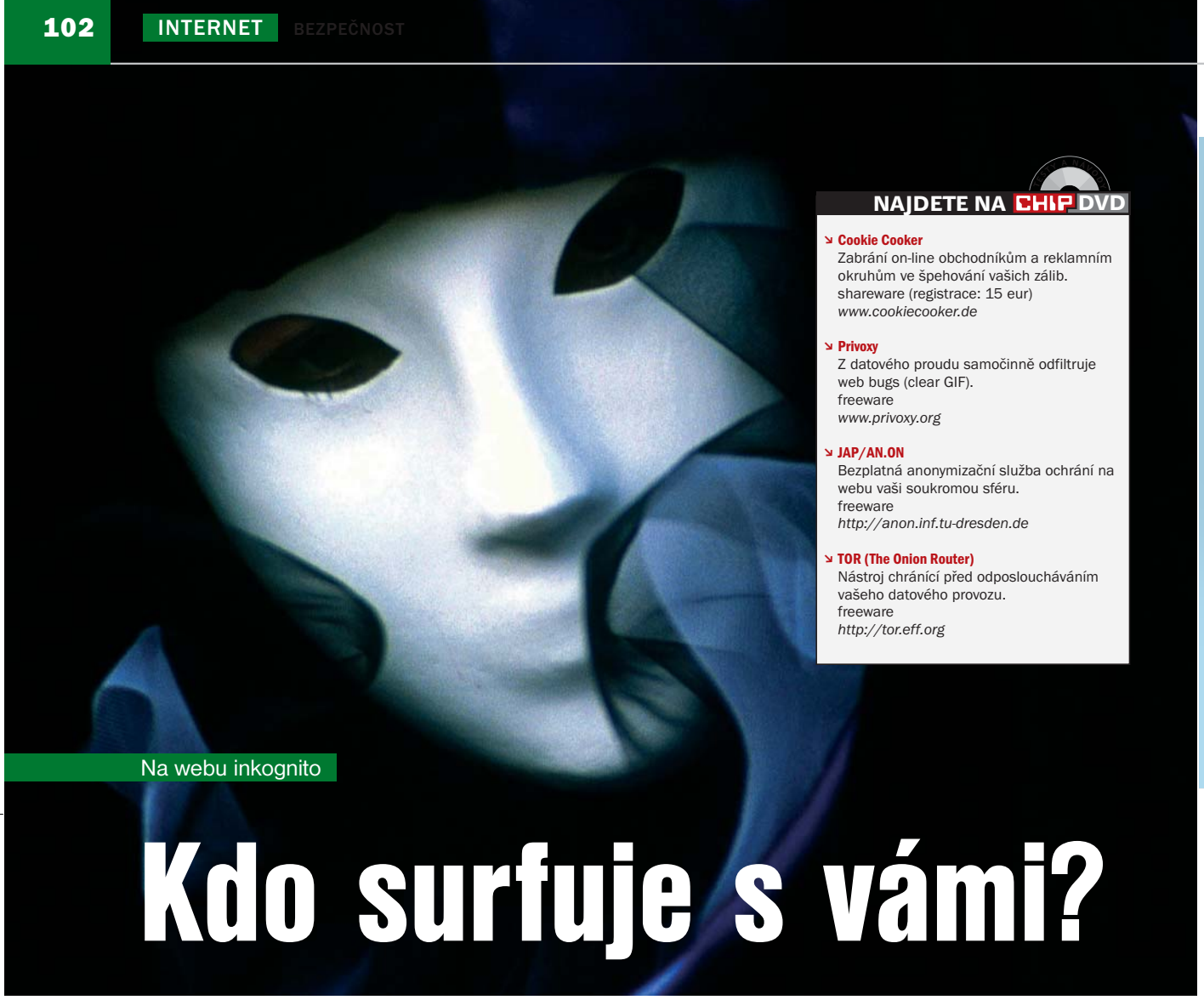


NAJDETE NA CHIP DVD

- **Cookie Cooker**
  Zabrání on-line obchodníkům a reklamním okruhům ve špehování vašich zálib.
  shareware (registrace: 15 eur)
  www.cookiecooker.de
- **Privoxy**
  Z datového proudu samočinně odfiltruje web bugs (clear GIF).
  freeware
  www.privoxy.org
- **JAP/AN.ON**
  Bezplatná anonymizační služba ochrání na webu vaši soukromou sféru.
  freeware
  http://anon.inf.tu-dresden.de
- **TOR (The Onion Router)**
  Nástroj chránící před odposloucháváním vašeho datového provozu.
  freeware
  http://tor.eff.org

Na webu inkognito

Kdo surfuje s vámi?

Stopy, které po sobě zanecháte na internetu, je nejlepší rychle zahladit. Nemusí hned každý vědět, kde jste surfovali – ať jsou to úřady, obchodníci s adresami, spammeři, nebo telefonní agenti.

Text: Matthias Kremp, *autor@chip.cz*

V TOMTO ČLÁNKU NAJDETE

V domnělé anonymitě na webu si surfaři troufají dělat věci, jakých by se ve skutečném životě těžko odvážili. Jedná se například o prohlížení erotických nabídek, návštěvu herny či hackerské stránky anebo veselé „nasávání“ chráněných skladeb, filmů apod. Vždyť o tom přece nikdo neví!

Chyba lávky! Stopy webových surfařů může sledovat skoro každý – a docela snadno. Všude po sobě zanecháváme IP-adresy, identifikace prohlížečů, informace z cookies – a k nim se stát může kdykoli dostat. Jakmile začne nová směrnice EU o ukládání dat platit i v České republice, budou muset poskytovatelé internetu tato data uchovávat dokonce po dobu několika měsíců. Státní kontrolní orgány takové stopy vyhodnocují už nyní – například aby usvědčily hudební nebo filmové piráty. Ale i tomu, kdo nemá co skrývat, hrozí příval spamu, phishingových mailů a telefonátů dotěrných agentů, a měl by se na něj tedy včas připravit. Zejména šiřitelé reklamy a pololegální internetoví obchodníci se velice zajímají o to, co všechno na internetu děláme. A aby zjistili naše záliby, zájmy a surfařské počínání, využívají čím dál tím vytříbenější metody. Máme však pro vás dobrou zprávu: existuje také spousta triků, jak datovým špionům uniknout.

COOKIES

Čárový kód uživatele

Že jsou návštěvníci webových stránek „značkováni“ pomocí cookies, ví dnes snad už každý. Avšak o jaká data jde a co se s nimi vlastně děje? Provozovatelé webových stránek si jednotlivé uživatele během jejich návštěvy na stránce označují prostřednictvím tzv. Session-ID, tedy dočasných cookies. Využívají je v prvé řadě k tomu, aby návštěvníko-

CHIP PŘEHLED:
Soukromí na netu

Jak se bránit

■ Chraňte si soukromí
Nejdůležitější opatření: neprozrazujte své údaje. Informace, které se nikdo nedozví, nelze zneužít. Buďte proto velmi zdrženliví při poskytování svých telefonních čísel, data narození, povolání atd.

■ Omezte záplavu spamu
Používejte „zahazovací" mailové adresy pro různé výherní akce, newslettery nebo pro přihlášky bezplatných služeb, do internetových fór a mailing listů.

■ Umlčte browser
Ve svém webovém prohlížeči nastavte vysokou úroveň ochrany dat.

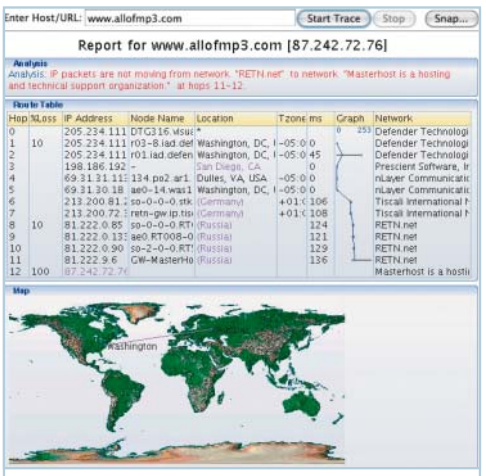
■ Používejte anonymizér
Anonymizační nástroje nebo služby zabrání datovým špionům ve vytváření kompletního uživatelského profilu o vašich surfařských zvyklostech.

vi ještě během jeho procházky on-line shopem dokázali předložit nákupní tipy šité jemu „přímo na míru".

Stejně vznikají také typické vzory pohybů a z nich odvozené profily zákazníka, například ve stylu úvahy „Kdo si v oddělení campingu prohlíží stany, bude mít zájem i o sprej proti komárům". Ale ani s „osobním nákupním poradenstvím" potenciálním klientům se už komerční nabízeči pomalu nechtějí spokojit. Nejraději by se dozvěděli všechno o zvycích a zálibách zákazníků, a značkují si je proto trvale uloženými cookies – nejlépe hned na dobu několika let. Obrazně řečeno tak spotřebitel dostane jakousi „nálepku s čárovým kódem".

Takový „cejch" sestává výlučně z textových údajů a neobsahuje žádný spustitelný kód. Viry ani jiný škodlivý software se tedy touto cestou do domácího počítače nedostanou. Často se cookies uživateli dokonce starají o pohodlí, když na často navštěvovaných webových stránkách samočinně zadávají uživatelské jméno a heslo. Bezpečnostním rizikem se však cookies mohou stát, dostanou-li se do nepovolaných rukou. Normálně může webový server číst jenom cookies pro vlastní doménu. Pokud se však hackerovi prostřednictvím útoku typu Cross Site Scripting podaří přístup k cizím cookies, mohl by se vydávat za cizího člověka a využívat jeho účet.

Takové surfařské profily ale v prvé řadě ohrožují soukromí. Cookies totiž nejsou zakládány jenom webovými stránkami, ale také reklamními bannery, umístěnými dnes na tolika stránkách. Tyto zdánlivě nevinné reklamní proužky jsou vlastně „stránkami ve stránce" a jako takové rovněž mohou zapisovat cookies. Prostřednictvím bannerových cookies pak reklamní firmy pilně shromažďují údaje o surfařích. Vedle jednoznačné identifikace uživatele bývají v těchto cookies často také údaje o tom, kdy dotyčný webovou stránku naposled navštívil a co konkrétně si prohlížel. Prostřednictvím nevelkého počtu různých webových nabídek je tedy uživatele možno jednoznačně identifikovat. Profil vytvořený pomocí „Cross Site Tracking" pak využívají marketingové firmy k tomu, aby bezbranného surfaře bombardovaly „personalizovanou" reklamou.

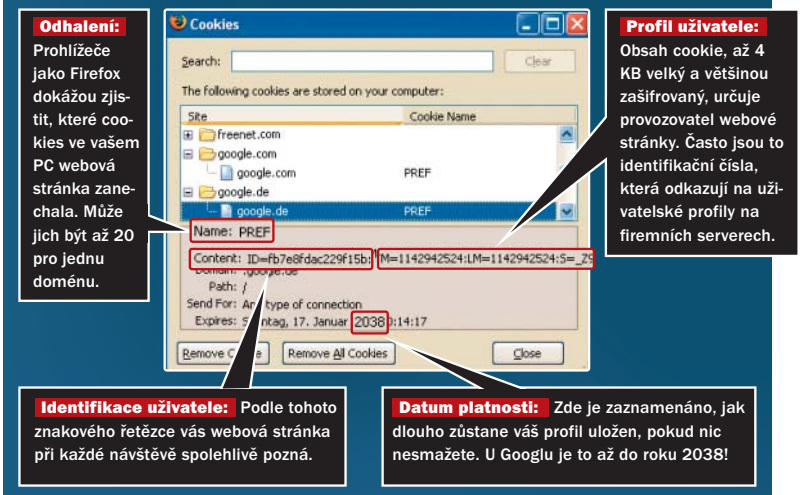


Dopaden: **Cestu stahovaného souboru, zde například z ruského hudebního serveru, dokáže Trace Router snadno vystopovat.**

Jak se bránit

„Utěsnění" Internet Exploreru: Proti zvídavému slídění pomocí cookies a spol. se dá leccos podniknout už s „palubními" prostředky Internet Exploreru. Chcete-li mít úplnou jistotu, zakažte automatické zpracování cookies tak, že aktivujete *Nástroje* | *Možnosti Internetu* | *Osobní údaje* | *Upřesnit*. Při tomto nastavení musíte každý cookie jednotlivě manuálně přijmout, nebo odmítnout. To je ovšem jako trvalé nastavení velmi zdlouhavé. Proto je lepší nastavit ochranu osobních dat v prohlížeči na úroveň *Střední* nebo

CO O VÁS PROZRADÍ COOKIES



Vysoká. Cookies, které už jsou v počítači uloženy, můžete odstranit na kartě *Obecné*. Zdá-li se vám to příliš radikální, můžete vymazat jen jednotlivé cookies tak, že pod *Obecné* | *Nastavení* zvolíte *Zobrazit soubory*. Vzhledem k tomu, že mnoho cookies žije mimořádně dlouho, měli byste kromě toho pravidelně čistit složku *C:\Documents and settings\jméno_uživatele\Cookies*.

Použití „anticookie“ nástrojů: Komfortněji se proti sběratelům dat a profilů můžete bránit s programem Cookie Cooker *(www.cookiecooker.de)*. Tento shareware (registrace: 15 eur) vám při surfování umožní zaujímat různé identity, a přesto přitom využívat výhod cookies, například přihlašování včetně uživatelského jména a hesla. Je dokonce možné, aby jeden cookie sdílelo více uživatelů, kteří tak navenek vystupují jako jediná osoba – což de facto znemožňuje smysluplné shromažďování osobních údajů. Zuřivou sběratelskou vášeň reklamních firem lze ovšem nejlépe zchladit tak, že je uživatel sám zasype daty, která se nedají nijak zařadit.

Před cookies chrání také bezplatný webový filtr Privoxy *(www.privoxy.org)*. K začátečníkům však tento nástroj není tak přívětivý jako Cookie Cooker a před nasazením je nutné jej vhodně nakonfigurovat.

WEB BUGS

Digitální štěnice

Mnohem vynalézavěji a zákeřněji pracují tzv. web bugs, známé rovněž pod názvem Clear GIF. Tyto digitální „štěnice“ ve formě miniaturních grafických souborů se mohou skrývat v každé webové stránce nebo v e-mailu ve formátu HTML. Za takovými, často jen jeden pixel velkými, transparentními, a tedy neviditelnými obrázky vězí většinou na serveru uložený skript, spojený s nějakou webovou stránkou. Jakmile takto upravenou stránku otevřete, ze serveru se spustí web bug. Tímto způsobem si také například internetové portály zjišťují počty uživatelů. To je však ještě to nejmenší zlo. K vyšpehování surfařského chování uživatelů však nejen samotné internetové portály, ale často také komerční šiřitelé reklamy rozmísťují štěnice – většinou kombinované se skriptem, který z prohlížeče vybírá informace a odesílá je. V tomto případě web bug ovšem uživatelské údaje neposílá provozovateli navštívené stránky, nýbrž sběrateli dat, který štěnici nasadil. Takoví sběratelé se pak dále sdružují v informační alianci a vyměňují si nashromážděná data – například vaši IP-adresu, URL stránek, které si právě prohlížíte a na kterých jste byli předtím, vždy s přesným časovým údajem. Na webových štěnicích je dále nepříjemné to, že jimi získaná data lze kombinovat s informacemi obsaženými v cookies. A poněvadž se web bugs dnes už skrývají v mnoha komerčních stránkách, ze všech těchto informací vzniká zájmový profil uživatele – čím déle surfuje, tím detailnější.

V souvislosti s elektronickou poštou používají web bugs především šiřitelé spamu. Ti se prostřednictvím sdílných miniobrázků dozvědí, kdy byla jejich zpráva přečtena, a tím také to, zda je uvedená adresa vůbec platná.

Jak se bránit

Vyzrát na webové štěnice není snadné. Na rozdíl od cookies se totiž v prohlížeči nedají blokovat.

Konfigurace e-mailového klienta: Příval spamu můžete alespoň trochu utlumit, jestliže v poštovním programu nepovolíte automatické zobrazování HTML mailů a tím i samočinné natahování obrazových souborů.

Použití bug filtru: Také před štěnicemi na webových stránkách vás ochrání filtr Privoxy. Tento výkonný nástroj je spolehlivě rozpozná a automaticky je z datového proudu vyloučí.

KDE ANONYMIZÉRY SELHÁVAJÍ

Nedostatečné zamaskování

Pro webové stránky už je dnes k dispozici tolik zdokonalení a plug-inů, že se mazaným hackerům závoj anonymizérů daří poodhrnout a dostat se k pravé IP-adrese.

Malý příklad: Pomocí metatagu „refresh“, zakotveného ve standardu HTML, se dá leckterý prohlížeč nechtěně zavést do anonymizační pasti. Zmíněná značka měla původně sloužit k tomu, aby návštěvníka webové stránky po uplynutí „timeoutu“ přesměrovala na jinou stránku. Pokud ovšem jako cílová adresa v tagu refresh není uvedena http adresa, nýbrž adresa Telnetu, může se stát, že Windows XP a Internet Explorer 6 automaticky sestaví telnetové spojení. Poněvadž pro ně neexistuje proxy, vytvoří se přímé spojení, které protistanici vyzradí IP-adresu oběti. Podobné triky existují i pro jiné prohlížeče a jiné operační systémy – například s novým plug-inem pro Flash 9.

Bez IP-adresy vstup zakázán

Někdy se k surfování inkognito uchýlit nelze. Například anonymní využívání některých webových služeb vůbec není možné. Také mnohá internetová fóra, jako například novinářská síť Jonet, vás anonymně nebo s falešnou adresou nevpustí dovnitř.

Příliš pomalé pro rozsáhlý download

Rovněž uživatelé, kteří obětovali hodně peněz za rychlé DSL připojení, si možná „anonymizaci“ raději odřeknou, aby si vychutnali plný požitek ze svého vysokorychlostního přístupu. V případě stahování objemných souborů totiž předřazená proxy kaskáda může dobu downloadu výrazně prodloužit. Pozor také, pokud chcete nějaký anonymizační nástroj použít na pracovišti. Systémoví administrátoři většinou velmi nelibě nesou, když zpozorují, že některý pracovník v jejich protokolech nezanechal žádnou stopu. V USA může zaměstnanec z tohoto důvodu dokonce dostat výpověď. Chcete-li se vyhnout podobným nepříjemnostem, nasazení anonymizačního nástroje si proto předem dohodněte se svým šéfem a se správcem systému.

V „maskáčích“: Anonymita na webu je vaše neoddiskutovatelné právo – odpovídající služby, zde například klient projektu JAP, jsou zcela legální.

BROWSERY

Nehorázní žvanilové

Webové prohlížeče jsou mimořádně upovídané: při standardním nastavení každému serveru ochotně prozradí, jak se jmenují a jaké mají číslo verze. A aby toho nebylo málo, ještě dodají podrobnosti o použitém operačním systému a o hardwaru, na kterém běží. A pokud ani to zvědavému serveru nestačí, nijak se netají ani s webovou stránkou, kterou naposled zobrazovaly.

Jak se bránit

Aby sběratelé údajů o surfařích z browseru vymámili jeho vědomosti, používají zpravidla špionážní JavaScripty.

Vypnutí JavaScriptů: Nejjednodušší možností obrany proti drzému odčerpávání dat z prohlížeče je tedy kompletní vypnutí podpory JavaScriptů. V Internet Exploreru k tomu aktivujte *Nástroje* | *Možnosti Internetu*. Pak na kartě *Zabezpečení* | *Internet* klikněte na *Vlastní úroveň* a pod *Nastavení* | *Aktivní skriptování* zvolte *Zakázat*. Pokud používáte jiné browsery, musíte JavaScript vypnout i v nich. Pohodlnější je to opět s Privoxy. Ten je zapotřebí nainstalovat a konfigurovat jen jednou, a pak „působí“ na všechny použité prohlížeče.

IP-ADRESY

Vaše vizitka jako na dlani

Základem výměny informací na internetu jsou „Transmission Control Protocol“ a „Internet Protocol“, dohromady označované zkrat-

TAJNÁ SLUŽBA NASLOUCHÁ

Asi nejvypilovanější systém pro slídění po datových stopách uvedly do provozu tajné služby Spojených států: Echelon. Síť po celém světě rozprostřených odposlouchávacích zařízení sleduje všechny moderní komunikační cesty: fax a telefonní hovory, ale také provoz na internetu a elektronickou poštu. O tomto systému pochopitelně nejsou k dispozici žádné oficiální informace, neustále se však objevují indicie, z nichž lze usuzovat, že e-maily jsou automaticky skenovány na výskyt jistých klíčových slov. V roce 2004 musela být základna Eschelonu umístěná v bavorském Bad Aiblingu dokonce na příkaz Evropské unie uzavřena. Bylo totiž považováno za prokázané, že sloužila v první řadě hospodářské špionáži proti EU. Není jistě bez zajímavosti, že na pozemcích bývalého letiště v Griesheimu u Darmstadtu už na jaře roku 2004 zahájila činnost náhradní základna...

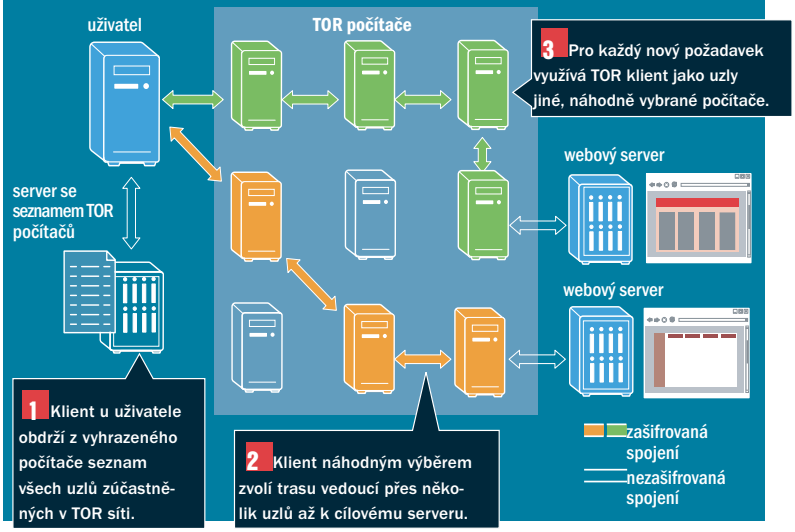
kou TCP/IP. Společně se starají o to, aby všechny datové pakety byly v pořádku doručeny svému adresátovi. Proto je také každému počítači připojenému k internetu přiděleno jednoznačné, nezaměnitelné „číslo popisné“, tzv. IP-adresa. Ovšem jenom větší organizace, jako jsou firmy nebo univerzity, nebo náročnější surfaři mají pevné, tedy statické IP-adresy. Většině těch, kdo se přes poskytovatele připojují prostřednictvím klasického modemu, DSL nebo mobilní sítě, je při každém přihlášení přidělena nová, tzv. dynamická IP-adresa. Zdálo by se tedy, že v tomto případě je uživatel vlastně anonymní – vždyť jeho momentálně používanou IP-adresu nelze jednoznačně přiřadit konkrétnímu uživateli.

Avšak zdání klame. Poskytovatelé internetu totiž vedou přesné záznamy o tom, kdo, kdy, jak dlouho a pod jakou IP-adresou po síti cestoval. Z jediné IP-adresy, která tak byla uložena například při nakupování v internetovém obchodě, je možno zjistit kupce ještě i po několika měsících. Na široké frontě využívají tento postup organizace zabývající se ochranou autorských práv. Ty nechávají ve výměnných burzách systematicky vyhledávat nabídky chráněné hudby, filmů a softwaru. Je-li taková nabídka objevena, program zaprotokoluje její IP-adresu a objem nabízených dat. Na základě těchto informací podá organizace oznámení proti neznámému pachateli. Úkolem úřadů činných v trestním řízení je pak vyzvat providera k vydání osobních dat patřících k udané IP-adrese. Tento postup se už stal v zahraničí běžnou praxí. Naposledy tak státní zastupitelství v Kolíně nad Rýnem během jedné bombastické akce získalo údaje o 3500 uživatelích výměnné burzy, kteří pak byli obviněni z rozšiřování materiálu chráněného autorským právem.

Opravdu inkognito? **Pozor na bezplatné proxy servery! Nejjistější je stále ještě německá služba Anonymouse.**

JAK FUNGUJE ANONYMIZÉR TOR

Hlavní trik této bezplatné anonymizační služby spočívá v tom, že u ní cesta k cíli vede pokaždé jinudy. Počet proxy počítačů je omezen jenom počtem účastníků.



Jak se bránit

Chcete-li si zasurfovat, aniž byste dali komukoli napospas svou IP-adresu, máte k dispozici pět různých prostředků.

Bezplatný proxy server: Nejjednodušší a nejlevnější cestu nabízejí bezplatné proxy servery. Ty fungují jako zprostředkovatel mezi vámi a webovým serverem. Pak nevoláte cílovou URL přímo, ale zadáváte ji proxy serveru. Teprve ten pak kýženou webovou stránku vyvolá a její obsah zobrazí v okně prohlížeče. Vy sami přitom pro oslovený server zůstáváte neviditelní – ten totiž „vidí“ jen IP-adresu vašeho zástupce. Obsáhlý seznam takových proxy serverů najdete na *http://www.freeproxy.ru/en/free_proxy/cgi-proxy.htm*. Pro příležitostné použití je tato metoda docela vhodná.

Nutno ovšem dodat, že někteří z poskytovatelů těchto volných proxy serverů jsou sami pochybného původu. Nemůžete si proto být absolutně jisti, že vaše počínání na webu přece jen není zaznamenáváno – a předáváno bůhvíkomu. Nelze vyloučit dokonce ani pokusy o vydírání. Navíc je přitom nutno počítat s drastickým omezením výkonu. Chcete-li to přesto sami vyzkoušet, použijte raději německou službu Anonymouse *(http://anonymouse.org)*.

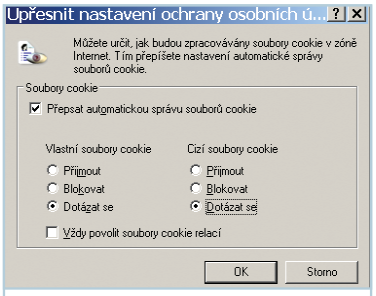
Komerční anonymizéry: Ačkoliv byl Anonymizér *(www.anonymizer.com)* původně odstartován jako bezplatná služba, dnes už přijde jeho použití ročně na 30 amerických dolarů. Podle vlastních údajů používá tento prostředek síť složenou z tisíců soukromých proxy počítačů. Jeho poskytovatel navíc slibuje, že jeho systém rychlost internetového spojení nezpomalí. Podobně funguje německá služba SaferSurf *(www.safersurf.com)*. Neviděni s ní surfujete za měsíční poplatek ve výši 5,90 eura. Lze objednat i další funkce k ochraně proti virům, spamu a ostatním útokům.

Projekt JAP: Vedle zpoplatněných služeb existuje i celá řada neplacených anonymizačních prostředků. Ty mají navíc tu velkou přednost, že své postupy a technologie nijak netají. Nadějný je výzkumný projekt JAP se svou anonymizační službou AN.ON (*http://anon.inf.tu-dresden.de*). Zde jsou s podporou Německé výzkumné společnosti a Spolkového ministerstva pro hospodářství a technologii (BMWi) vyvíjeny technologie pro maximální anonymitu na webu.

Základem systému jsou tzv. mixy a klientský software JAP, který se nainstaluje na počítačích uživatelů. Mixy jsou servery fungující podobně jako proxy, přitom si však mezi sebou vyměňují zašifrovaná data. Dva až tři tyto mixy propojuje uživatel do tzv. mixových kaskád. Až poslední počítač v kaskádě data dešifruje tak, aby jim rozuměl webový server. Jeho odpověď pak celým systémem projde rovněž v zašifrované podobě, až je nakonec dešifrována v počítači uživatele.

Aby bylo nežádoucí dešifrování ještě více ztíženo, mixovými kaskádami data procházejí v předem určeném pořadí. Díky tomu jsou data v bezpečí i v případě, že by některý provozovatel mixu spolupracoval s nějakým útočníkem. Případný „vyzvědač“, který by se do řetězu vetřel, by totiž zachytil jen nesrozumitelnou hatmatilku nebo by odposlechnutá data nedokázal nikomu jednoznačně přiřadit.

Prozatím je však na systému znát, že je dosud ve fázi vývoje. A tak se třeba při surfování občas projeví zřetelné zpomalení. Navíc ještě také nejsou v systému implementovány všechny plánované funkce.



Svobodná volba: Při tomto nastavení Internet Exploreru rozhodujete sami, které cookies přijmete.

Přesto se vyplatí využívat JAP už nyní, neboť i v současné vývojové etapě efektivně chrání před mnoha „vyzvědačskými“ aktivitami.

Anonymizér TOR: Jinou bezplatnou anonymizační službu nabízí The Onion Router *(http://tor.eff.org)*. Na rozdíl od AN.ON však TOR nespoléhá na několik mix serverů – zde každý uživatel může do systému zapojit svůj vlastní počítač. Vzniká tak agregace stovek miniproxy PC. Navíc systém sám rozhoduje o cestě datových paketů. Každý počítač uvnitř stanoveného řetězu přitom ví jenom to, kterému počítači má právě obdržená data přeposlat. Za tím účelem je každý datový paket obklopen několika „slupkami", z nichž každá obsahuje zašifrovanou adresu následujícího příjemce, a tyto slupky jsou po cestě postupně odloupávány; „cibule“ v názvu a její obrázek v logu systému tedy uvedený princip docela dobře znázorňují. Za těchto okolností případný slídičský PC prakticky nemá šanci se v takovém datovém chaosu orientovat – zvláště když pro každý požadavek se volí nová trasa. A i kdyby se útočníkovi přece jen podařilo nějaký požadavek opravdu rozšifrovat a vysledovat jej až k uživateli, hned další vyvolání webové stránky by už nemohl dát do souvislosti s toutéž osobou.

Tým snů JAP a TOR: Až dosud bylo nutné rozhodnout se pro jeden z obou systémů – AN.ON, nebo TOR. V nejnovější verzi je však už služba TOR integrována v JAP softwaru anonymizéru AN.ON. Díky tomu už zájemce o webovou anonymitu není odkázán na skromné TOR rozhraní v grafickém prostředí Vidalia. Spojením obou služeb vzniká mohutný „zastírací“ potenciál, jímž může uživatel navenek utajit vedle přístupů na web také svou účast ve výměnných burzách, stahování z FTP serverů, a dokonce i chatování.

STOPROCENTNÍ JISTOTA

Surfování ve WLAN nebo v kavárně

Celý svět dnes pomalu obrůstá pletivem desetitisíců bezdrátových sítí. Mnoho jich sice provozují komerční poskytovatelé, kteří za jejich použití účtují poplatky a protokolují, stejně jako v případě pevných sítí, kdo, kdy a pod jakou IP-adresou s jejich sítí pracoval. Neustále však přibývá také volně přístupných a bezplatných WLAN, které je možné použít, aniž by bylo zapotřebí se jednoznačně identifikovat. Kromě toho provozovatelé menších bezdrátových sítí, například v kavárnách ap., často poskytují možnost uhradit zpoplatněné síťové služby po hodinách prostřednictvím předplatní karty. Poněvadž si takovou kartu jednoduše koupíte za hotové peníze u pokladny, surfujete i zde v naprosté anonymitě. ■ ■ ■