Dlouhé prsty chobotnic dat

Podobně jako chobotnice se svými dlouhými chapadly číhají **ZLODĚJI DAT** na vhodnou příležitost a pak za použití různých technik kradou data o uživatelích. Chip vám ukáže, jak se jim bránit...

MANUEL SCHREIBER

NA DVD

Nástroje na mazání stop

Adblock Plus ► blokování reklamy a vyskakovacích oken

CustomizeGoogle ► nabídka celé řady vylepšení pro vyhledávače a blokování Google trackeru

Enigmail ► GnuPG plug-in pro Thunderbird

Firefox ► alternativní prohlížeč

Gpg4win ► kompletní šifrovací balík

GPGrelay ► kompletní ochrana e-mailu

IE7pro ► rozšíření prohlížeče Internet Explorer

JAP ► anonymizace IP adresy

JonDoFox ► browser založený na Firefoxu s předkonfigurovanými bezpečnostními nastaveními

Mozilla Thunderbird ► doporučeníhodný poštovní klient

NoScript ► nástroj na deaktivaci skriptů ve Firefoxu

Password Safe ► manažer hesel

Tor + Privoxy + Vidalia ► šifrovaný přístup na internet

TrueCrypt ► vytvoří virtuální šifrovaný disk

Web assiccibility ► analýza a blokování skriptů

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **OCHRANA DAT**.

Vše pro anonymní internet. Kdokoliv, kdo v současné době používá internet, je prozkoumán chapadly nenasytných zlodějů dat. Webové stránky, vyhledávače i profesionální zloději dat hladově nasávají každou i nicotnou informaci, která pomůže identifikovat surfaře. A tato informace může být často mnohem nebezpečnější, než by si většina z nás dokázala představit. Jako příklad si vezměme Google. Jeden z největších „sběračů dat“ využívá svůj nový prohlížeč Chrome jako rafinované a nenápadné chapadlo. To zasílá data uživatele přímo serveru Googlu. A protože každý prohlížeč Chrome má vlastní ID, Google dokáže přesně vystopovat celou řadu akcí.

Měli by se tedy internetoví surfaři vyhýbat Googlu? Ne. Google není typickým zlodějem dat – je to jen jeden z největších sběračů, který díky své velikosti poskytuje i jakousi „anonymitu“. Uvedený příklad by však měl každého uživatele, kterému alespoň trochu záleží na svém soukromí, varovat před nerozvážnou instalací haldy doplňků pro surfování a před automatickým odklikáváním „podmínek použití“.

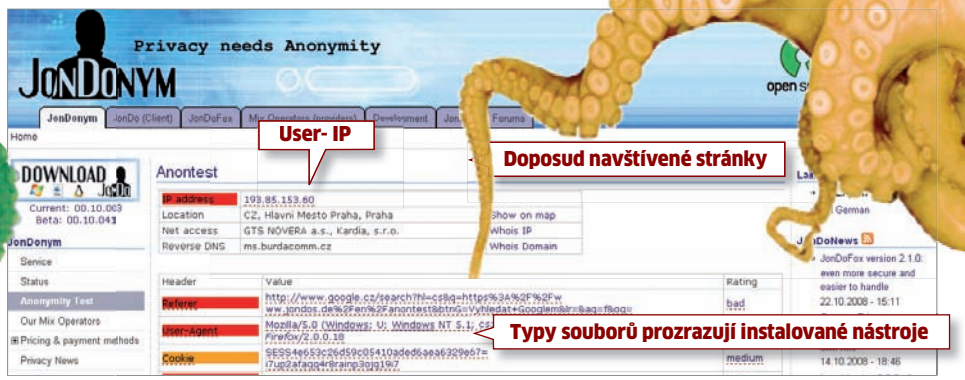
Budete-li se alespoň trochu snažit, nemusíte být na internetu bez obrany. Pomocí našich nástrojů můžete buď chapadla useknout, nebo si s „datovými chobotnicemi“ hrát na schovávanou. Chip vám ukáže, jak na to. Předvedeme vám komplexní ochranná opatření, která vám usnadní rozhodování, komu poskytnout svá cenná osobní data...

Browser: Žádné cookies pro obludy

První pravidlo zní: Držte se dál od beta verzí softwaru (a to včetně zmiňovaného Chromu nebo Internet Exploreru 8). Riziko kritických mezer je zkrátka příliš vysoké. Nebezpečí však mohou představovat i stabilní verze, protože i ony mohou skončit jako pravý ráj pro zloděje dat.

Zvláště „lahodné“ jsou pro zájemce o soukromé informace cookies. Proto se ujistěte, že je při ukončení surfování smažete. Ukážeme vám, jak lze k tomuto účelu vhodně změnit nastavení u dvou nejoblíbenějších prohlížečů. V Internet Exploreru to můžete udělat v nabídce »Nástroje | Možnosti Internetu« . V kartě »Upřesnit« se posuňte do sekce „Zabezpečení“ a označte zatržítko u »Vyprázdnit složku...«. Ve Firefoxu najdete volbu v »Nástroje | Možnosti | Soukromí«. Zde deaktivujte volbu »Povolit serverům nastavovat cookies«.

Nikdy byste neměli dovolit, aby prohlížeč pracoval s vašimi hesly. V Internet



Test bezpečnosti: Na webu **www.jondos.de/en** můžete zjistit, jaké stopy za sebou zanecháváte.

Exploreru přejděte do karty »Nástroje | Možnosti internetu | Obsah« a v sekci Automatické dokončování klikněte na tlačítko »Nastavení«. V dalším okně deaktivujte zatržítko před volbou „Uživatelská jména a hesla na formulářích“. Ve Firefoxu najdete toto nastavení v nabídce »Nástroje | Možnosti | Zabezpečení«.

Nyní je čas na elegantní tuning. Uživatelé IE7 by měli zaměřit svou pozornost na IE7 Pro. To je výborný doplněk, který maže stopy po vašich surfařských výletech, kontroluje proxy servery a aktivuje reklamní filtr. Pokud se stane, že filtr zablokuje důležitý obsah, otevřete si nastavení IE7 Pro, klikněte pravým tlačítkem na doplněk a zvolte »Rozšířené blokování reklam | Použité filtry«. Otevře se vyskakovací okno, v němž můžete přejít na zablokovaný obsah a znovu ho kliknutím nechat zobrazit.

Ve Firefoxu je pro podobné účely ideální kombinace doplňků Adblock Plus a Noscript. Prvně jmenovaný pracuje s filtrovacím seznamem, který lze snadno upravit. Po nainstalování doplňku nezapomeňte browser restartovat. Práce s doplňkem je poté jednoduchá. Pokud některá agresivní reklama filtrem projde, klikněte na ni pravým tlačítkem myši a zvolte »Blokovat obrázek...« nebo »Blokovat rám...«. Chcete-li mít o blokovaných prvcích lepší přehled, otevřete nastavení doplňku (například pomocí klávesové zkratky [Ctrl]+[Shift]+[E]) a zde v nabídce »Možnosti« aktivujte zatržítko u položky »Zobrazit ve stavovém řádku«. Ikona, která se ve stavovém řádku Firefoxu objeví, vám prozradí všechny důležité informace o zablokovaných prvcích na navštíveném webu.

Druhým doplňkem je NoScript. Protože jsme o něm psali už mnohokrát, ve stručnosti nyní jen zmíníme, že pokud chcete sběračům dat říci jednoznačné NE, nemělo by v nabídce »Nastavení... | Zásuvné moduly« chybět zatržítko u položek „Zakázat Java“ a „Blokovat každý objekt pocházející z nedůvěryhodné stránky“.

Poté zbývá poslední krok – anonymní surfování. Bez IP adresy budou pro sběrače informací vaše osobní data jen bezcenným shlukem bajtů. Podrobně jsme se tomuto tématu několikrát věnovali v předchozích vydáních Chipu (tyto články najdete ve formátu PDF na našem DVD), proto se zmíníme jen o jednom praktickém doplňku. Pokud pro své toulky internetem používáte Firefox, je pro vás dobrou volbou Torbutton **(https://addons.mozilla.org/cs/firefox/addon/2275)**, který umožňuje snadné zapínání a vypínání surfování přes síť TOR. Pro anonymní pohyb po internetu stačí jen použít tlačítko »Start Tor«, pro vypnutí slouží »Deactivate Tor«. Surfování přes síť Tor je sice znatelně pomalejší, můžete si ale být jisti svou anonymitou.

Používáte-li pro surfování Internet Explorer, přejděte v nabídce »Nástroje | Možnosti internetu« na kartu »Připojení«. V sekci „Nastavení místní sítě (LAN)“ klikněte na tlačítko »Nastavení místní sítě« a zde aktivujte zatržítko u volby „Použít pro síť LAN server proxy“. Poté do pole Adresa zadejte „local host“ a do políčka Port zadejte 8118.

Každé kliknutí je potravou pro sběrače dat.

E-maily: Slídilové mají smůlu

Přestože browser již máte zaopatřený, cesta ke kompletnímu zabezpečení vašich dat je ještě dlouhá. Vždy když někde zadáte své „jméno a heslo“, odhalíte o sobě zpravidla více, než by se vám mohlo zdát. Typickým příkladem jsou webmailové služby. Už jen fakt, že poskytovatel služby může „kontrolovat“ vaši příchozí poštu, je pro celou řadu uživatelů nepřijatelný vstup do jejich soukromí. Důvodů, proč poskytovatelé „čmuchají“ ve schránkách, je celá řada – od filtrování „nevyžádané pošty“ až po reklamu. Ano, například Google hledá v příchozích mailech klíčová slova, na jejichž základě poté vkládá do dopisu personalizovanou reklamu. Pokud nechcete, aby byla vaše soukromá pošta prosívána cizími filtry, používejte šifrování a klienty, které ho podporují (například Outlook nebo Thun-

NEJČASTĚJŠÍ DOTAZY

Kontrola je obtížná

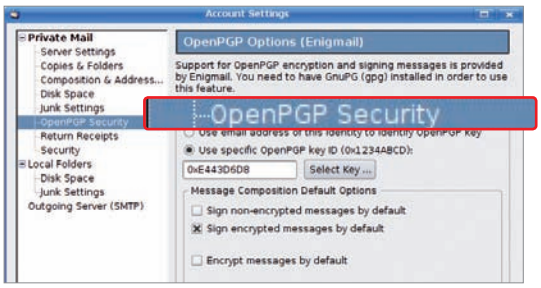
Webové stránky a obvyklá praxe při sběru důležitých osobních dat

Jaké triky používají webmasteři k získání osobních dat?
Nejprve je nutné podotknout, že celá řada webů shromažďuje data s naprostým pohrdáním zákony na ochranu dat. Nehromadí jen klasická data, ale zjišťují například i to, které produkty si na stránkách prohlížíte nebo o čem diskutujete ve fórech. Ve spojení s údaji o vyhledávaných výrazech pak dostanou komplexní informace o vašich zájmech.

K čemu jsou tato data využívána a jaké riziko hrozí uživatelům?
Je snadnější oslovit zákazníka, když znáte jeho záliby. Navíc je prodávání „zákaznických profilů“ dalším zajímavým zdrojem financí. Pro zákazníky tak existuje reálné nebezpečí zneužití těchto údajů dalšími subjekty, kde zasílání nevyžádané pošty je tou nejmenší hrozbou...

Je to legální?
Bez povolení uživatele to pochopitelně legální není, kontrola takovéhoto chování je velmi obtížná. Nebezpečné je také sdílení informací mezi jednotlivými weby. Řetězce reklamních banerů najdete už na téměř každé stránce a pomocí cookies vytváří komplexní uživatelské profily. Ovšem i zde platí, že kde není žalobce, není ani soudce...

Google Desktop: Pro větší soukromí deaktivujte prohledávání v mailu a na chatu…



Šifrování mailů: S rozšířením Enigmail můžete zašifrovat své dopisy pomocí klíče OpenPGP.

INFO

Triky čmuchalů

TRACKING:

Webmasteři používají trackingové nástroje, aby sledovali stopy a chování uživatelů za použití javasriptu. Tímto způsobem mohou vidět, zda uživatel přichází na stránku pomocí vyhledávače, odkazu nebo přímo zadáním adresy. Lze také zjistit, jak dlouho uživatel na stránce zůstane a odkud přejde na jinou stránku. Tyto informace pomáhají při optimalizaci stránek a při zjišťování počtu návštěvníků. V praxi platí, že tyto informace shromažďuje každý profesionální web.

ZAMĚŘOVÁNÍ:

Pokud se webmasteři snaží o směrování reklamy, postupy i výsledky mohou být různorodé. Jednou z cest je vnutit uživatelům používání složitých cookies, které přesně prozradí uživatelovy zájmy. Shromážděná data jsou pak používána k nabízení cílené reklamy. Další cestou je podrobná registrace již při první návštěvě webu a ukládání informací o uživatelích v centrální databázi. Nejběžnější je ale následující postup: Když surfujete po internetových stránkách, nástroj v pozadí monitoruje všechny vaše aktivity. Pokud stejný uživatel navštíví jiný portál s jiným reklamním partnerem, program na základě algoritmu odhadne vaše zájmy a nabídne vám z databáze příslušný reklamní prvek.

Triky proti čmuchalům

CUSTOMIZEGOOGLE:

K ochraně svého soukromí použijte rozšíření pro Firefox jménem CustomizeGoogle. Tento doplněk dokáže nejen optimalizovat vyhledávání automatickou integrací dalších vyhledávačů (Yahoo, Wikipedia, Ask.com, Lycos, Altavista…), ale také dokáže po stisknutí tlačítka vypnout „tracking“ uživatele, anonymizovat cookies a blokovat statistický software Google Analytics. Podrobnější informace o doplňku najdete na adrese www.customizegoogle.com.

TRACKMENOT:

Chcete-li čmuchaly pořádně potrápit, je pro vás ideální volbou plug-in TrackMeNot. Ten dokáže zabránit vytvoření uživatelského profilu na čtyřech hlavních vyhledávacích serverech (Google, MSN, Yahoo a AOL). Domácí stránku projektu najdete na adrese **http://mrl.nyu.edu/~dhowe/TrackMeNot/.**

derbird). Pro tyto účely je ideální například balíček Gpg4Win. K šifrování používá GnuPG kombinaci privátního a veřejného klíče. Pro vytvoření spusťte program WinPT (je součástí balíčku), zvolte »Create GnuPG key pair« a zadejte jméno a e-mailovou adresu. Poté zvolte heslo (mělo by mít alespoň osm znaků) a nechte si vytvořit záložní kopii klíče, kterou uložte na externí médium. Nyní potřebujete nastavit e-mailového klienta. V Thunderbirdu doporučujeme použít nástroj Enigmail. Jeho nastavení najdete v nabídce »Tools | Addons | Install«.

Po restartování aplikace najdete v nabídce novou položku – „Open PGP“. Poté v klientovi klikněte na »Tools | Accounts | OpenPGPSecurity« a zadejte klíč. Aktivujte zatržítko u voleb „OpenPGP“ a „Use the email adress of this account to identify the OpenPGP key“. Tímto způsobem zabezpečíte e-mailovou komunikaci tak, že ji nikdo nepovolaný nebude moci číst. Integrace GnuPG do Outlook Expressu nebo Windows Mailu je o něco málo obtížnější. Například pro Outlook 2003 nabízí Gpg4Win speciální plug-in GpgOL. Pro další verze aplikací naleznete příslušné varianty nástroje GPGrelay na našem DVD. Tento nástroj je univerzálním řešením, které stojí mezi klientem a serverem.

Hraničí-li vaše touha po soukromí až s paranoiou, doporučujeme alternativní řešení založené na rychlé jednorázové výměně dat na anonymním serveru. Podobným, ale přístupnějším řešením je použití krátkodobého e-mailového účtu, jaký nabízí například server **http://10minutemail.com**.

Disk: Aby soukromí zůstalo soukromím

Vždy když si na svůj počítač integrujete nějakou webovou aplikaci (nebo alespoň aplikaci pravidelně komunikující s internetem), podstatně usnadníte práci datovým špionům. Například při standardní instalaci nástroje Google Desktop tato aplikace zaznamenává a indexuje všechny aktivity. Díky tomu mohou uživatelé hledat soubory i na různých počítačích na internetu. Zmiňovaný indexovací soubor Google ukládá na svém serveru.

Nejbezpečnější je samozřejmě vůbec takovéto služby nevpustit do svého počítače, pak se ale musíte obejít bez komfortních funkcí. Kompromisním řešením může být to, že deaktivujete vyhledávání u určitých typů dokumentů nebo služeb (mail, webové protokoly, kontakty…). V případě aplikace Google Desktop najdete všechna potřebná nastavení v nabídce „Options“.

Dodatečně byste měli svá tajná data chránit pomocí hesla. Pokud jste si již nainstalovali GPG4Win, můžete si libovolný soubor podepsat a zašifrovat pomocí svého klíče – s použitím GpGee v kontextové nabídce. Pro větší bezpečnost použijte nástroj TrueCrypt. Software se specializuje na ochranu dat – a to jak jednotlivých souborů či složek, tak i kompletních disků.

Na svém disku si vytvořte prázdnou složku a nazvěte ji například „Private“ – tato složka bude tvořit „šifrovaný disk“. Pro zašifrování dat klikněte v aplikaci TrueCrypt na »Volumes | Create new volume« a v okně, které se objeví, pak na »Create a container file«. V dalším kroku potom zvolte, zda má být složka viditelná nebo skrytá, a zadejte již zmiňovaný adresář „Private“. Nakonec zadejte jeho velikost a zvolte ochranu heslem. Ve finále ještě můžete v nabídce „Volume“ zadat, pod jakým jménem bude tento disk v systému přístupný. Nyní jsou vaše data v bezpečí nejen před slídivými pohledy datových čmuchalů. Váš počítač je bezpečný a anonymní…

AUTOR@CHIP.CZ