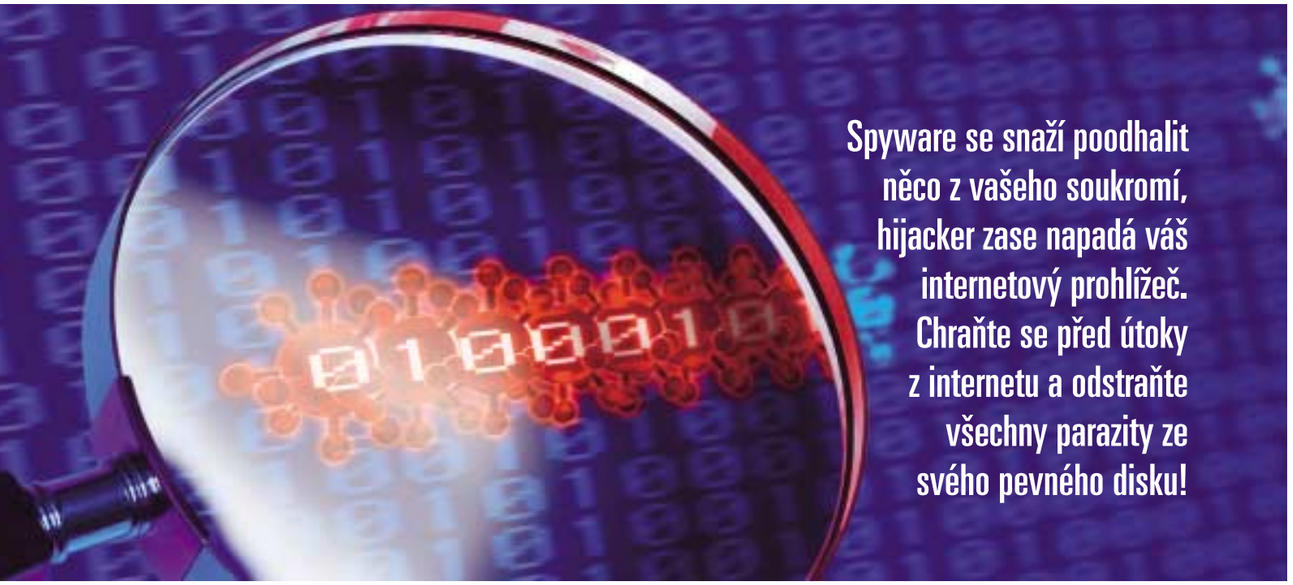
Spyware a hijackery



Spyware se snaží poodhalit něco z vašeho soukromí, hijacker zase napadá váš internetový prohlížeč. Chraňte se před útoky z internetu a odstraňte všechny parazity ze svého pevného disku!

Ochraňte svůj počítač a soukromí před útoky z internetu! (CD)

DAVID ČEPIČKA,
CHRISTIAN BÜTIKOFER

Pomoc, můj počítač dostal chuť na sex! Toto zvolání v žádném případě není vtip – přesně takové potíže začal řešit jeden čtenář našeho časopisu. Jeho počítač při každém bootování začal na pozadí pracovní plochy přehrávat v Media Playeru erotická videa, v Internet Exploreru se mu neustále objevoval proužek s nápisem Sex is great! a domovská stránka internetového prohlížeče se automaticky nastavila na adresu s pornografickými snímky. Náš čtenář se pokusil všechny podezřelé položky odstranit, ale bez úspěchu. Byl snad jeho počítač začarovaný? To určitě ne.

V polovině roku 2003 se internetem začala šířit nová počítačová epidemie, tzv. **hijackery**. Hijackery (z anglického „*to hijack/highjack*", což česky znamená unést nebo zmocnit se) přesměrovávají váš internetový prohlížeč na WWW stránky, které nechcete. Najednou máte mezi svými oblíbenými odkazy úplně neznámé stránky. Když v prohlížeči zadáte nějakou adresu, dostanete se někam úplně jinam, než jste chtěli, domovská stránka je rovněž náhle nastavena na úplně jinou adresu než dosud. Prostě se někdo úplně cizí hrabe ve vašem operačním systému a snaží se vás dostat do blázince.

Hijackery využívají trhlin v zabezpečení Internet Exploreru, aby do WWW stránek nebo různých aplikací (nejčastěji se jedná o rozšíření možností internetového prohlížeče, o tzv. *Browser Helper Objects – BHO*) dostaly takové funkce, které vás nalákají k využívání některé z internetových služeb nebo se snaží vysledovat vaše zájmy, záliby či třeba činnost při surfování na internetu. Všechny programy, skripty nebo prvky, které mají za úkol v počítači provádět nějakou nekalou činnost, se jedním slovem označují jako tzv. malware (odvozeno ze slovního spojení „*malicious software*" – škodlivý program). Kromě již popsaných nekalostí patří mezi další praktiky malwaru provádění změn v registru Windows. Často se do systému mohou dostávat i tzv. trojské koně – programy, které váš počítač zpřístupní tak, aby se do něj po síti mohl kdokoliv dostat. Hijackery jsou tedy vlastně jen další skupinou malwaru.

Hlavní příčinou úspěchu hijackerů či spywaru jsou špatná nebo špatně provedená nastavení Internet Exploreru. V tomto článku se budeme věnovat v první části hijackerům, v druhé části spywaru. Dozvíte se zde vše potřebné pro to, abyste svůj počítač dokázali proti všemožným útokům z internetu úspěšně bránit.

Hijackery

Nejefektivnějším prostředkem proti hijackerům je prevence. Možnosti, jak předejít poškození systému, začínají konfigurací prohlížeče a končí u pravidelného provádění instalací updatů Windows. Pokud se budete řídit dále uvedenými tipy, ušetříte si spoustu nepříjemností.

1) Utěsněte Internet Explorer

Přejděte v Internet Exploreru do menu *Nástroje/Možnosti internetu* a stiskem tlačítka *Vlastní úroveň*, které najdete na záložce *Zabezpečení*, si nastavte úroveň zabezpečení zóny Internet. V poli *Obnovit vlastní nastavení* vyberte možnost *Vysoká*. V poli *Nastavení* byste pak měli mít následující položky nakonfigurovány takto (viz obrázek na vedlejší straně):

- *Inicializovat a skriptovat ovládací prvky ActiveX, jež nejsou označeny jako bezpečné:* **Zakázat**
- *Spouštět ovládací prvky ActiveX a moduly plug-in:* **Dotázat se**
- *Stahovat nepodepsané ovládací prvky ActiveX:* **Zakázat**
- *Nastavení jazyka Java (pokud je tato volba k dispozici):* **Vysoká úroveň zabezpečení**

Všechny provedené změny pak potvrďte stiskem tlačítka *OK*.

Nyní použijte skript **IE-Spyads**, který najdete NA NAŠEM CD nebo na internetu na **https://net-files.uiuc.edu/ehowes/www/resource.htm** (IE-SPYAD-1.EXE, 258 KB). Tento skript zapíše v Internet Exploreru do zóny *Servery s omezeným přístupem* celou řadu serverů hostících podezřelé webové stránky. Pro všechny servery, které leží v této zóně, platí automaticky vysoká úroveň zabezpečení.

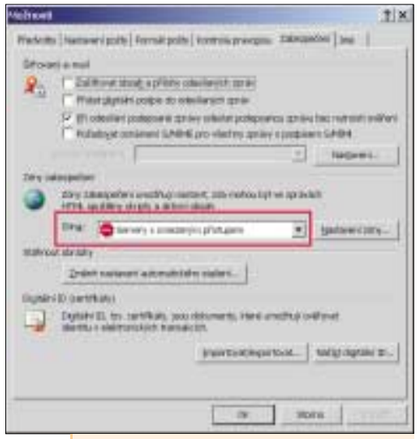
▲ **Internet Explorer: nastavení úrovně zabezpečení.**

Instalaci skriptu provedete takto: Poklepejte na soubor IE-SPYAD-1.EXE a rozbalte ho do libovolné složky. V této složce se bude mimo jiné nacházet i soubor INSTALL.BAT. Poklepáním jej spusťte. V okně programu MS-DOS nyní vyberte stiskem klávesy *2* položku *Install the New IE-Spyad List*. Poté tuto volbu ještě jednou potvrďte klávesou *1*, odpovídající položce *Yes – install IE-Spyad*. Skript nyní do zóny serverů s omezeným přístupem zapíše stovky nechvalně známých WWW stránek. Nyní by žádná z těchto stránek neměla způsobit ve vašem počítači nějakou neplechu.

Pokud používáte ve Windows několik uživatelských účtů, je potřeba pro každý z nich skript spustit zvlášť.

2) Ochrana v programech pro práci s elektronickou poštou

Vedle internetového prohlížeče musíte patřičně nastavit ochranu svých programů pro práci s elektronickou poštou. V Outlooku 2003 si zvolte v menu *Nástroje/Možnosti* na záložce *Zabezpečení* v poli *Zóny zabezpečení* položku *Servery s omezeným přístupem*. Na stejném místě naleznete tuto položku i v Outlook Expressu 6. I zde zvolte v poli *Ochrana proti virům* položku *Zóna serverů s omezeným přístupem* (viz obrázek).



▲ **Outlook Express/Outlook: v poli Zóny zabezpečení vyberte položku Servery s omezeným přístupem.**

Zásadně v e-mailovém programu neklepejte na žádné internetové odkazy a všechny příchozí zprávy si nechte zobrazovat pouze v textovém formátu a nikoli ve formátu HTML. Toto nastavení v Outlook Expressu 6 provedete v menu *Nástroje/Možnosti* na záložce *Čtení*, kde umístěte zatržítko před položku *Číst všechny zprávy jako prostý text*. Pro Outlook a Outlook Express 5 bohužel podobné nastavení k dispozici není.

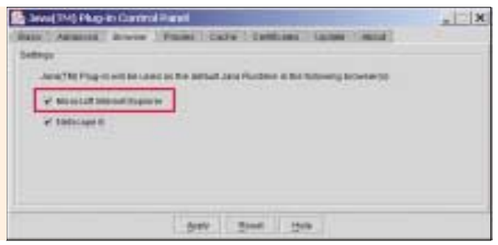
▲ **Outlook: vypnutý automatický náhled.**

Dále zrušte u e-mailů automatický náhled. V Outlook Expressu 6 postupujte následovně: Klepněte na ikonku *Doručená pošta* a z menu *Zobrazit* vyberte příkaz *Rozložení*. V poli *Podokno náhledu* zrušte zatržítko u položky *Zobrazit podokno náhledu*. V Outlooku 2003 se ujistěte, že v menu *Zobrazit* není u položky *Automatický náhled* umístěno zatržítko (viz obrázek).

3) Nahraďte aplikaci MS Java originální verzí od firmy Sun

Vzhledem k tomu, že aplikace Microsoft Java již není delší dobu podporována, nejsou pro starou verzi MS Javy vytvářeny žádné záplaty ošetřující problémy se zabezpečením. Prostě nejvyšší čas pro přechod k originální verzi Javy od firmy Sun Microsystems. NA NAŠEM CD, popřípadě na internetové adrese **http://java.sun.com/j2se/1.4/** naleznete nejaktuálnější verzi **Java 2 Standard Edition 1.4** (J2RE-1_4_1_02-WINDOWS-I586-I.EXE, 9,76 MB). Java se vám po instalaci automaticky zabuduje do Ovládacích panelů.

Jak zjistíte, že máte jako standardní aplikaci nastavenou Javu od firmy Sun? Poklepejte v Ovládacích panelech na ikonu Javy – vypadá jako šálek kávy – a v dialogovém okně, které se objeví, se přesuňte na záložku *Browser*. Pokud používá-



▶ **Java: definujte si pro svůj internetový prohlížeč – na obrázku pro MS Internet Explorer a Netscape – jako standardní aplikaci Sun Java.**

◀ **SpywareGuard: s nastaveními uvedenými na obrázku se postará o bezpečnost vašeho počítače a odežene pryč všechny nezvané hosty.**

te Internet Explorer, pak si zde umístěním zatržítka před položku *Microsoft Internet Explorer* definujete tuto aplikaci jako standardní.

4) Nainstalujte program pro sledování podezřelých objektů

Proti nezvaným hostům pomáhají programy, které ve Windows sledují na pozadí všechny prováděné aktivity. Pokusí-li se kupříkladu nějaký program o instalaci, budete okamžitě dotázáni, zda s touto instalací souhlasíte. Jako stvořené pro tento účel jsou utility **Geek Superhero** (GEEKSUPERHERO_SETUP-1.EXE, 2,01MB) nebo freewarový program **SpywareGuard** (SPYWAREGUARDSETUPMIN.EXE, 913 KB). Oba samozřejmě najdete NA NAŠEM CD, popřípadě Geek Superhero 1.1. na internetové adrese **www.geek-superhero.com/index.shtml** a Spyware Guard 2.2 na adrese **www.javacoolsoftware.com/spywareguard.html**. Geek Superhero dokáže v porovnání se SpywareGuard o něco více, například umí blokovat pop-up okna apod., ale možná i proto si jej musíte koupit za 25 USD.

Nyní se budeme věnovat zdarma dostupnému SpywareGuard. Utilitu nainstalujete poklepáním na soubor SPYWAREGUARDSETUPMIN.EXE. S nastaveními uvedenými na obrázku se pak postará o bezpečnost vašeho počítače. Nahlásí vám, pokud se nějaký program na pozadí pokusí nainstalovat nějaký nový *Browser Helper Object (BHO)* nebo když se pokusí změnit nastavení vaší domovské stránky, stránky pro vyhledávání apod. Tak získáte takřka úplnou kontrolu nad chováním svého internetového prohlížeče.

5) Omezení práv

Nikdy ve Windows NT/2000/XP nepracujte jako uživatel s administrátorskými právy, nýbrž pro běžnou práci používejte uživatelský účet, jenž má práva do nějaké míry omezena. V praxi je tato rada velmi snadno realizovatelná. Pro instalace programů, vytváření záloh, instalování updatů systému používejte účet administrátora, pro každodenní práci běžný uživatelský účet s omezenými právy. Popisované pravidlo platí dvojnásob při surfování na internetu. Pokud je uživatel přihlášen pod omezeným uživatelským účtem, má hijacker daleko méně možností, jak napáchat ve Windows nějakou škodu.

6) Radikální řez: výměna internetového prohlížeče a programu pro práci s elektronickou poštou

Internet Explorer a Outlook Express jsou nejrozšířenějšími programy používanými na internetu. Právě proto jsou vděčným terčem pro řadu hackerů, kteří se snaží pomocí bezpečnostních trhlin v těchto aplikacích ovládnout váš počítač. Jejich používání tedy není z hlediska bezpečnosti nejlepší řešení. Ten, kdo chce skutečně bezpečně surfovat po internetu, by měl zvážit použití alternativních programů. Z prohlížečů můžeme doporučit tyto aplikace:

- **Opera 7.54** – najdete ji NA NAŠEM CD jako soubor OW32ENEN754J.EXE o velikosti 16,2 MB nebo na internetové adrese **www.opera.com/download/?lng=en&ver=7.54**.
- **Mozilla 1.7.2** – NA NAŠEM CD je jako soubor MOZILLA-WIN32-1.7.2-CSCZ-INSTALLER.EXE o velikosti 12,6 MB nebo na internetové adrese **www.czilla.cz/download/**.
- **Firefox 0.9.3cs** – najdete rovněž NA NAŠEM CD jako soubor FIREFOXSETUP-0.9.3-CSCZ.EXE o velikosti 5,43 MB nebo na internetu na adrese **www.firefox-browser.de**.

Jako alternativy k Outlook Expressu mohou rovněž posloužit aplikace Mozilla či Opera, z dalších můžete vyzkoušet:

- **PMMail 2000 Professional 2.20.2717** – naleznete NA NAŠEM CD jako soubor PMMAIL2KPRO.EXE o velikosti 4,93 MB nebo na internetové adrese **www.pmmail2000.com/download.html**.
- **Mozilla Thunderbind 0.7** – NA NAŠEM CD je jako soubor THUNDERBIRD-0.7.3-WIN32-CSCZ-INSTALLER.EXE o velikosti 6,38 MB. Program naleznete též na internetové adrese **www.mozilla.org/products/thunderbird/releases/#install**.
- **AK-Mail 3.2** – nachází se NA NAŠEM CD jako soubor AKME32.EXE o velikosti 947 KB nebo na internetové adrese **http://www.akmail.com/eng/download.html**.
- **GeMail 2.2** – najdete NA NAŠEM CD jako soubor GEMAIL_EN.EXE o velikosti 2,14 MB nebo na internetové adrese **www.gemail.de/download.htm**.
- **Pegasus Mail V4.21c** – je NA NAŠEM CD jako soubor W32-421C.EXE o velikosti 4,40 MB nebo na internetové adrese **www.pmail.com/**.

7) Týdenní updaty Windows

Přenechte svoje starosti svému systému. Každý týden kontrolujte, jaké nové záplaty jsou u Microsoftu k dispozici. Ve Windows XP stačí klepnout do *nabídky Start/Windows Update*, v Internet Exploreru pak klepněte do menu *Nástroje/Windows Update*. Pak budete mít ve Windows ošetřeny záplaty všech známých bezpečnostních děr.

ODSTRANĚNÍ HIJACKERŮ

Přečetli jste si všechny naše tipy proti hijackerům a rozhodli jste se, že se podle nich budete řídit? Pak je to skvělé. Ale co dělat, pokud už v systému nějaký hijacker máme? Boj proti již zamořenému systému není vůbec beznadějný. Existuje řada použitelných programů, které vám znovu vrátí ztracenou vládu nad vaším počítačem. Stejně jako u antivirových programů i zde platí, že ne každý program skutečně najde všechny hijackery. Proto vám doporučujeme vyzkoušet všechny tyto programy:

- **Ad-Aware SE Personal Edition 1.02** – najdete NA NAŠEM CD jako soubor AAWSEPERSONAL.EXE o velikosti 2,48 MB nebo na internetové adrese **www.lavasoftusa.com/** a k němu český jazykový modul v archivu AAW6_CZ.RAR o velikosti 6,69 KB – rovněž NA NAŠEM CD nebo na internetu na adrese **http://cestiny.idnes.cz/pa/ad_aware.html**.
- **Spybot Search & Destroy 1.3** – nachází se NA NAŠEM CD jako soubor SPYBOTSD13.EXE o velikosti 4,15 MB nebo na internetové adrese **www.safer-networking.org/en/download/index.html**.
- **CWShredder 1.59.1** – je NA NAŠEM CD jako soubor CWSHREDDER.EXE o velikosti 146 KB. Naleznete jej i na internetové adrese **www.softpedia.com/public/cat/10/17/10-17-150.shtml**.

Vzhledem k tomu, že Ad-Aware a Spybot zlikvidují i spyware, čtěte návody k jejich použití v odstavci **Prověřte svůj systém off-line**.

Program **CWShredder** spustíte poklepáním na soubor SHREDDER.EXE. Stiskem tlačítka *Fix* aplikace najde a zlikviduje všechny podezřelé objekty ve vašem počítači.

Spyware

Jak již název prozrazuje, jedná se o programy, které eminentně zajímá, jaké stránky na internetu navštěvujete, které služby používáte a vůbec vše, co na počítači provádíte. Spyware se může skrývat v softwaru, který je distribuován zdarma. Spyware není pochybný jen z hlediska ochrany dat, ale je škodlivý i pro samotná Windows. Špatně se totiž odinstalovává a za určitých okolností může dokonce narušovat pravidelný běh aplikací.

Na rozdíl od hijackerů nejsou za spyware v počítači odpovědné bezpečnostní trhliny v systému. Na vině jsou tentokrát hlavně samotní uživatelé. Vzhledem k tomu, že průměrný uživatel počítače by chtěl mít nejraději vše úplně zadarmo, přešla řada programátorů sharewarových aplikací od placení za používání sharewarové aplikace uživatelem k modelu spywarovému, který nabízejí zdarma a peníze dostanou od pochybných reklamních společností za informace o uživateli tohoto softwaru. Od časů, kdy se objevila Windows 2000, se i Microsoft začíná podílet na praktikách takového sbírání dat. Např. Media Player umožňuje jednoznačně identifikovat daného surfujícího uživatele nebo vám Microsoft při zatuhnutí systému nabízí odeslání informací a výpisu z operační paměti na jeho server.

Jak se vlastně proti spywaru bránit? Jak se dozvíte, zda již nejsou ve vašem systému pilně sbírána data a následně odesílána pryč? Různé internetové společnosti měly přes dva roky času, aby vyvinuly ochranné nástroje proti spywaru. Tomu odpovídá i rozmanitost aplikací či utilit, které jsou v současnosti pro boj proti spywaru k dispozici.

1) Utěsněte Windows 2000/XP

Windows 2000/XP potřebují v boji proti spywaru zcela nekompromisní nástroj, neboť jsou až příliš vstřícná. Jedním z nich je utilita **XP Antispy 3.8** (XPANTISPY_EN.ZIP, 35,1 KB), kterou naleznete NA NAŠEM CD nebo na adrese **www.xp-antispy.org/**. Její instalace spočívá v rozbalení archivu do libovolné složky a v poklepání na spouštěcí soubor. V okně programu doporučujeme deaktivovat většinu položek umožňujících sbírání dat a jejich zasílání Microsoftu, a to zejména u *Windows Media Playeru*, *Internet Exploreru* a v poli *Error Reports*. U položek *Disable automatic updates* a *Disable scheduled updates* byste rozhodně měli mít červený vykřičník. U každé vybrané volby se vám ve spodní části okna objeví vysvětlení, co daná volba umožňuje. XP Antispy spouštějte v profilu, který má k počítači práva administrátora.

2) Rozpoznání spywaru

Pokud už při začátku instalace nějakého programu budete dotazováni na nějaké demografické údaje, pak je na místě nejvyšší obezřelost. Žádného obyčejného programátora sharewarových aplikací rozhodně nezajímá váš věk, co nakupujete, jaké máte zájmy a podobné marketingové údaje. Velmi známými příklady spywaru jsou například download manažer **Download Accelerator Plus (DAP)** či **Go!Zilla**. I programy pro výměnu souborů **Kazaa** a **BearShare** obsahují ve své zdarma dostupné verzi spyware. Rozvažte si proto dobře, zda není v takových případech lépe zapomenout na zdarma dostupné nástroje, které slídí po vašich osobních údajích, a zda se nevyplatí koupit si komerční verzi bez spywaru.

3) Zabraňte napadení počítače

Aplikace **SpywareBlaster 3.2,** kterou naleznete NA NAŠEM CD jako soubor SPYWAREBLASTERSETUP.EXE, 2,14 MB), nebo ji můžete stáhnout z internetové adresy **www.javacoolsoftware.com/spywareblaster.html**, váš počítač před takovými slídícími programy ochrání. Po její instalaci a při prvním spuštění už možná odhalí, že máte špatně nastavený Internet Explorer. V tom-

◀ **SpywareBlaster: hned napoprvé detekuje chybné nastavení Internet Exploreru. Pak již nezbývá než přijmout všechna opatření, která navrhne.**

to případě se objeví hlášení *Internet Explorer Security Alert!* Pak nezbývá než přijmout všechna opatření, která vám SpywareBlaster navrhne. Proto vyberte položku *Here to learn more and fix it*. Potom klepněte na volbu *Set recommended values*. V hlavním menu programu pak aktivujte ochranu v menu *Protection* tím, že klepnete na odkaz *Click here to enable protection*.

Volba *Restricted sites protection* zabraňuje přístupu na podezřelé stránky. I tuto byste měli aktivovat. Do třetice klepněte v levém sloupečku na odkaz *Updates*, kde stiskem tlačítka *Check for update* stáhnete z internetu nejnovější verzi databáze programu pro detekci nového spywaru.

Při instalaci je potřeba tuto utilitu nainstalovat pro každý uživatelský účet zvlášť.

4) Skromnost člověka šlechtí

Nejúčinnější ochranou proti spywaru je vaše chování a hlavně skromnost. Z internetu byste měli stahovat a následně instalovat pouze ty programy, které skutečně potřebujete. Pro každý typ aplikace na sto procent existuje nějaký program, který neobsahuje spyware. Na druhou stranu zase nemusí být zdarma.

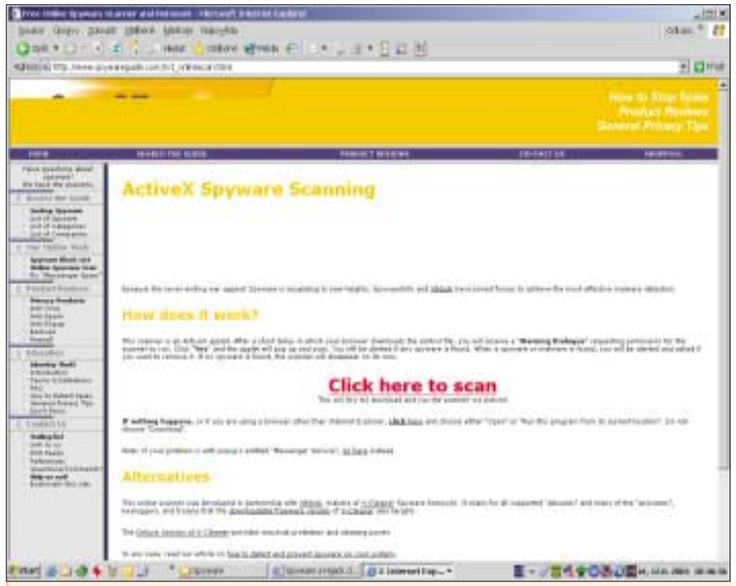
5) Otázka důvěry

Stahujte z internetu programy pouze z těch stránek, jež vám připadají důvěryhodné. Pokud se v některých aplikacích používá spyware, pak pokud se jedná o seriózní zdroj, budete na tuto skutečnost dodatečně upozorněni.

6) SpyBlocker – speciální program na blokování spywaru

Nechcete se za žádnou cenu vzdát používání programů obsahujících spyware, protože je jejich používání zadarmo? Dokonce i v tomto případě se dá zařídit, aby vaše aktivity nebyly sledovány. Takové řešení ale není zdarma. Představuje ho program **SpyBlocker 8.0** (SPYBLOCK.EXE, 3,66 MB), který sice nezabrání žádnému spywaru, aby se nainstaloval, ale znemožní mu zasílání dat o vás, takže takový spyware je pak pro svého výrobce prakticky nepoužitelný. SpyBlocker tedy nijak nemění vlastní soubory spywaru, nýbrž blokuje server spywaru tím, že mu dá do cesty svůj vlastní server. Tím si všechny programy podrží plnou funkčnost, vy neporušujete žádná licenční ujednání, ale spyware se při použití této utility naprosto mine účinkem. Pokud máte na svém počítači nainstalovaný firewall, například Zone Alarm, je potřeba v jeho nastavení povolit SpyBlockeru přístup k některým portům (např. port *80*). Program naleznete NA NAŠEM CD, popřípadě na internetu na adrese **www.spyblocker-software.com/spyblocker/index.shtm**.

▲ SpyBlocker: nasazením této aplikace „převezete“ každý spyware.



▲ On-line aplikace z internetové adresy Spyware-Guide.com najde a odstraní spyware.

JAK SE ZBAVIT SPYWARU

Myslíte si, že jste udělali naprosto vše, abyste ze svého počítače odstranili spyware a hijackery? Udělejte si test. Vsadíte se, který ze špiónů už měsíce pracuje na vašich souborech? Naštěstí jsou všechny níže popisované testovací programy schopné všechen nalezený spyware okamžitě ze systému eliminovat.

1) Prověřte svůj systém on-line

Internetová stránka **Spyware-Guide.com** vám zdarma nabízí on-line skenování vašeho systému na přítomnost spywaru. Stačí do internetového prohlížeče zadat adresu **www.spyware-guide.com/txt_onlinescan.html**. Možná budete muset dočasně deaktivovat svůj download manažer, například GetRight, pokud nějaký používáte, aby se mohlo skenování systému automaticky spustit. Tato on-line aplikace je vlastně prvek ActiveX. Internet Explorer si jej stáhne a jakmile je stažení kompletní, objeví se dialog s varováním. To naše on-line aplikace žádá o dovolení, aby se mohla spustit. Stiskem tlačítka *Yes* jí toto povolení dáte. Pokud aplikace během prohlížení systému nalezne spyware, trojského koně, keylogger, adware nebo jiný malware, zeptá se, zda jej budete chtít zlikvidovat. Malware pak odstraníte tlačítkem *Remove it*.

Když on-line aplikace nenajde nic podezřelého, po skončení kontroly se automaticky ukončí.

Používáte-li jako internetový prohlížeč jinou aplikaci než Internet Explorer, pak zvolte adresu **www.xblock.com/download/xclean_micro.exe**. Pak může prohlížeč tento soubor uložit na pevný disk. Po uložení pak poklepáním na uložený soubor spustíte skenování systému.

2) Prověřte svůj systém off-line

Po otestování systému on-line restartujte počítač. Nyní přijdou na řadu již dříve jmenované utility **Ad-aware** a **Spybot**. Pro ně platí to samé, jako pro antivirové programy – ne každá utilita na odhalování spywaru nalezne všechny škůdce. Jistota je jistota. Spusťte v libovolném pořadí postupně obě utility. Po skončení každé vždy restartujte počítač.

- **Ad-aware:** je to klasika mezi programy odhalující hijackery, spyware nebo adware. Verze *Personal* je dostupná zdarma a řádění všemožného malwaru rychle ukončí. Program nainstalujete do libovolné složky klasicky poklepáním na instalační soubor. NA NAŠEM CD naleznete i český jazykový modul, který si doinstalujete tak, že rozbalíte soubor AAW6_CZ.RAR do libovolné složky a všechny rozbalené soubory přesunete do složky **Lang**, která se nachází ve složce, do níž jste instalovali Ad-aware. Potom stačí v menu *Options* vybrat v poli *Language file* položku *Czech* a stisknout tlačítko *Proceed*.

V hlavním okně programu nyní stiskněte tlačítko *Stav*. Klepnutím na položku *Aktualizovat nyní* si z internetu stáhněte nejnovější aktualizační soubor. Poté stiskněte tlačítko *Skenovat*. Jako režim skenování vyberte volbu *Vybrat soubory/adresáře* a klepnutím na odkaz *Vybrat* vyberte všechny diskové oddíly, které obsahují Windows (většinou disk C:) a dále používané programy (často disk D:). Klepnutím na tlačítko *Další* zahájíte skenování systému. Po otestování systému je nutno označit ručně všechny soubory, které mají být smazány.

Ad-aware určitě najde spoustu tzv. *tracking cookies*, které můžete bez obav odstranit. Rovněž smažte všechny EXE soubory nalezené a identifikované Ad-awarem jako spyware. Rychlá kontrola systému, která se spouští z hlavního rozhraní přes tlačítko *Skenovat* a položku *Provést rychlou kontrolu systému*, mimo jiné testuje i položky v registru Windows.

- **Spybot Search&Destroy:** při prvním spuštění vám program navrhne provedení zálohy registru, což rozhodně neodmítejte. Poté stiskněte tlačítko *Next* a dále *Search for updates*. Poté základní ošetření systému provedete opět klepnutím na tlačítka *Next* a *Immunize this system*. Konečně po stisku tlačítek *Next* a *Start using this program* se průvodce ukončí. Nyní doporučujeme celý program ukončit a znovu spustit.

Tato aplikace má zabudovaný i český jazykový modul, takže pokud klepnete do menu *Jazyk/Česky*, bude s vámi program komunikovat v češtině.

Po jeho spuštění stiskněte tlačítko *Zkontrolovat*. Po prověření systému uvidíte výsledky. Stiskem tlačítka *Opravit vybrané problémy* odstraníte ze systému všechny škůdce.

▲ Ad-aware: všechen nalezený spyware, který chcete odstranit, musíte manuálně označit.

Aby odstranění škůdců nerazilo některé aplikace takříkajíc na kolena, vytváří nejdříve Spybot bod obnovení Windows. Jestliže nemůže Spybot některé škůdce odstranit okamžitě, musí to udělat při příštím spuštění Windows. Proto mu dovolte, aby se mohl při příštím spuštění Windows automaticky spustit.

ZÁLOHOVÁNÍ SYSTÉMU

Nyní máte Windows vyčištěna od různého malwaru. Je tedy vhodná doba pro vytvoření zálohy systému. Nejrychleji to provedete prostřednictvím utility **SpywareBlaster**. Spusťte jej a v hlavním okně vyberte položku *System Snapshot*.

Vyberte možnost *Create new System Snapshot* a klepněte na tlačítko *Go*. Vložte jméno pro snapshot a klepněte na *Create Snapshot*. Po několika sekundách je vše hotovo. Pokud používáte Windows NT/2000/XP, je třeba snapshot vytvořit pro všechny uživatele.

Pokud vám někdy v budoucnu do systému vklouzne nějaký malware, vyberte v SpywareBlasteru pod volbou *System Snapshot* volbu *Restore System to Saved Snapshot Point* a klepněte na tlačítko *Go*. V dalším dialogovém okně si vyberte soubor s dříve vytvořenou zálohou a zahajte obnovu systému klepnutím na tlačítko *Next*.

4 0487/OK ❑