



TEST: Zastavte spyware!

Srovnávací test softwaru pro boj proti zákeřným programům (CD)

DAVID ČEPIČKA, MARY LANDESMAN

Napadení některým z programů, které mají sledovat vaši aktivitu na počítači, je ve své podstatě otázkou okamžiku. Zato odstranění takového slídila může být až nesnesitelně obtížné a hlavně časově náročné. V tomto článku vám nabízíme test podle našeho názoru nejlepších programů určených pro boj se spywarem a adwarem.

není tomu zas až tak dávno, kdy největšími nepříteli uživatelů pracujících s počítači byly viry šířící se prostřednictvím internetu a elektronické pošty. Jenže zatímco viry a červi způsobují škody tím, že mažou důležitá data nebo poškodí celý operační systém, novější hrozba, běžně nazývaná spyware, je daleko rafinovanější, neboť doslova krade uživateli možnost něco tvořit a takzvaně být v klidu. Nálepku s označením spyware můžeme za prvé přiznat každému legitimnímu, byť otravnému programu, který se souhlasem uživatele (i když možná nevědomky) pronikl do po-

čítače. Za druhé do kategorie spywaru zařazujeme i skupinu daleko nebezpečnějších programů, které se do počítače instalují zcela bez našeho vědomí. Obě skupiny aplikací spotřebovávají výkon vašeho systému, zpomalují internetové připojení, sledují, které stránky na internetu prohlídíte anebo dokonce násilím přesměrovávají kupříkladu domovskou stránku vašeho prohlížeče. První zmíněnou skupinu budeme nadále nazývat adware, druhou skupinu pak spyware. Adware většinou o sobě dává jasně vědět, tzn. oznámí uživateli, že se do systému instaluje a seznámí ho

se vším, co bude v systému vykonávat. Většinou obsahuje možnost odinstalace a dá se z počítače bez problémů kompletně odstranit. Naproti tomu spyware se instaluje tajně a jeho odstranění může být v některých případech bez odborné pomoci takřka nemožné.

Na základě tohoto konstatování se nelze divit, že se na trhu záhy objevila celá řada antispywarových programů. V našem článku popisujeme vyhodnocení deseti v současné době dostupných antispywarových utilit, vyvinutých za účelem vyhledání a odstranění spywaru či adwaru z počítače. U jednotlivých utilit jsme se zajímali o účinnost při detekci a odstraňování spywaru, dále o rychlost skenování systému, schopnost zabránit samočinné instalaci nechtěných aplikací a konečně o snadnost či obtížnost jejich používání. Již předem můžeme prohlásit, že jsme byli mile překvapeni, protože řada testovaných aplikací odvedla při pokusu vyčistit infikovaný počítač a zabránit průniku nové infekce pomocí ochrany v reálném čase skutečně kus dobré práce.

Otestovali jsme sedm produktů v ceně od 20 do 40 USD, a to od velkých i malých prodejců: In-

ternet Cleanup od firmy Allume Systems (dříve Aladdin Systems), Spyware Eliminator od firmy Aluria Software, ETrust PestPatrol Anti-Spyware od firmy Computer Associates, Spy-Subtract Pro od firmy InterMute, McAfee Anti-Spyware od firmy Network Associates, CounterSpy od firmy Sunbelt Software a nakonec Spy Sweeper od firmy Webroot Software. Kromě toho jsme testovali i dvě velmi známé utility dostupné zdarma – Ad-Aware SE Personal od firmy Lavasoft a Spybot Search & Destroy od firmy Safer Networking. Posledním sledovaným programem (pracujícím sice na zcela odlišném principu, přitom však neméně účinně) byl Hijack-This od firmy Merijn.org. Všechny tři poslední zmiňované utility naleznete **NA NASEM CD**. Do našich testů jsme však HijackThis nezahrnuli, a to proto, že na rozdíl od ostatních systém neskenuje a nevyhledává v něm nákazu. Také jsme testovali jeden produkt v beta verzi, konkrétně Microsoft Windows AntiSpyware, který byl až do konce loňského roku znám jako antispywarový program od firmy Giant Software (viz rámeček **Microsoft Windows Antispyware má šanci stát se nejlepším antispywarovým programem**).

Testované antispywarové utility jsme vystavili 45 adwarovým a spywarovým programům, s nimiž se lze při běžné práci na počítači setkat. Těchto 45 aplikací představovalo po instalaci celkem 81 jednotlivých souborů a procesů, které měly antispywarové programy kompletně odstranit.

Nákaza systému spywarem může začít například jednoduchou instalací programu podporovaného reklamou. Často je uživatel upozorňován samotným adwarem na jeho přítomnost a instalace adwaru je pak jakýmsi výměnným obchodem za to, že může program, jehož součástí adware je, používat zdarma (často uživatel nevědomky nainstaluje adware i tak, že si vůbec nepřečte licenční ujednání). Je smutnou skutečností, že i když mnoho adwarových programů se před samotnou instalací uživatelů ptá, zda je chtějí nainstalovat, ne všechny se chovají takto čestným způsobem. A dokonce i zdarma dostupná aplikace, jež slibuje pouze omezené množství reklamy, může celý systém doslova zamořit spywarem tím, že začne stahovat a instalovat spyware a adware jiných firem.

Adware se však liší i způsobem, jak se do vašeho počítače dostane. Dva známé panely nástrojů poskytující vyhledávání na internetu – Slotchbar a WinTools – při instalaci neobsahovaly v licenčním ujednání (EULA), v němž se obvykle upozornění na adware vyskytuje, žádnou zmínku o tom, že budou do počítače stahovat nějaké další komponenty. Tyto dva programy nainstalované v našem systému používaly při svém běhu bez našeho souhlasu spoustu dalších procesů a ukázalo se, že jejich odinstalování je krajně obtížné, jelikož při pokusu některý proces ukončit nebo příslušný soubor smazat se procesy vzájemně reinitializují.

Na druhou stranu známé adwarové aplikace WhenUSearch (panel nástrojů pro vyhledávání na internetu) a Bonzi Buddy (jakýsi interak-

tivní virtuální pomocník na pracovní ploše, který mimo jiné dokáže prohledávat internet) zobrazují při instalaci snadno srozumitelné licenční ujednání (EULA) a pro jejich pozdější odinstalování disponují odinstalačním programem, který lze spustit přes ve Windows standardně dostupnou funkci *Přidat nebo odebrat programy*.

Vyčištění systému

Nejprve jsme testovali, jak účinně dokáže každý program odstranit aktivní komponenty spywarových programů, dále jsme testovali úroveň ochrany systému v reálném čase se zvláštním zřetelím na schopnost zabránit instalaci nežádoucích programů do počítače.

Jako nejschopnější se ukázal CounterSpy od firmy Sunbelt Software, jelikož dokázal najít a zastavit 93 procent všech běžících procesů, spuštěných našimi 45 testovanými spywarovými a adwarovými programy. CounterSpy byl v našich testech jediným produktem, který byl schopen zastavit a odstranit ze systému skutečně houževnatý spyware WinTools. Spy Sweeper od firmy Webroot Software byl v testu na druhém místě pouze s nepatrným odstupem, neboť zachytil 89 procent všech aktivních procesů (bohužel nedokázal odstranit tak odolný spyware jako WinTools a Scotchbar). Nejméně účinné pak byly McAfee Anti-Spyware od firmy Network Associates a Internet Cleanup od firmy Allume Systems, které zachytily v prvním případě 33 procent a v druhém případě pouhých 11 procent spywaru.

Spyware často ovládne uživatelské nastavení domovské stránky a funkce pro vyhledávání na internetu tak, že veškeré pokusy o surfování nebo vyhledávání na internetu se díky spywaru auto-

mi těžkým oříškem. Internet Cleanup, McAfee Anti-Spyware, ETrust Pest Patrol Anti-Spyware od firmy Computer Associates a SpySubtract Pro od firmy InterMute nedokázaly žádné z těchto změn ani detekovat, Spyware Eliminator od firmy Aluria Software zvládl opravit pouze 7 procent přesměrování. Zvítězil opět CounterSpy, i když i ten dokázal opravit pouhých 53 procent přesměrování.

Browser Helper Object (BHO) jsou dalším typem problematických objektů. Zaměřují se na modifikování Internet Exploreru a ostatních prohlížečů, i když jsou často jejich důvody zcela legitimní. Například velmi často používaný *Google Toolbar* je rovněž BHO. Tvůrci adwaru a spywaru však zneužívají BHO k tomu, že vytvářejí takové komponenty pro panely nástrojů, které se spouštějí společně s Internet Explorerem a zneužívají prvky ActiveX ke stahování a instalaci BHO do vašeho počítače. Je to totiž velmi snadný způsob, jak v prohlížeči vytvořit často nechtěné panely nástrojů, které uniknou firewallům založeným na nutnosti schválit každý pokus o přístup do systému. Tímto způsobem se firewall obejde a další vrátka pro odesílání a příjem dat z internetu jsou otevřena.

Když jsme testovali schopnost detekovat potenciálně podezřelé objekty BHO, jak CounterSpy, tak Spy Sweeper zapracovaly na 100 procent. Ad-Aware, ETrust Pest Patrol Anti-Spyware, Spybot a SpySubtract dosáhly každý hodnoty 62 procent v porovnání s AntiSpywarem od McAfee a Spyware Eliminatoru, jejichž výsledkem bylo pouhých 31 procent. Internet Cleanup nezachytil ani jeden BHO nebo panel nástrojů.

Dalším oblíbeným umístěním pro adware či spyware jsou klíče v registru a systémové složky, jejichž obsah se načítá při spouštění Windows.



▲ **Náš vítěz: CounterSpy z hlediska vyhledávání a odstraňování spywaru vyhrál.**

maticky přesměřují na stránky s pornografickými materiály nebo na stránky s jiným nevyžádaným obsahem. A co je horší, zrušení takového automatického přesměrování je velmi obtížné, neboť všechny takové pokusy jsou monitorovány spuštěnými procesy, které je okamžitě vrací zpět. Odstranění spywaru způsobujícího změnu nastavení domovských stránek a funkce pro vyhledávání na internetu bylo pro všechny testované utility vel-

Z tohoto důvodu jsou pro uživatele tato místa skutečně kritická. Bohužel antispywarové programy v této oblasti ukázaly pouze nadprůměrné výsledky. CounterSpy detekoval 86 procent, na druhém místě se umístil Spy Sweeper s 82 procenty a na třetím místě Ad-Aware se 77 procenty. Internet Cleanup detekoval pouze 5 procent.

Testovali jsme rovněž schopnost detekovat uměle vytvořené položky v menu internetových



▲ Ochranný štít Spy Sweeperu zablokuje celou řadu pokusů o průnik do Windows.

prohlížečů. Tyto změny sice automaticky neznamenají, že se nainstaloval spyware, ale pokud uživatel na takovou položku klepne, může tuto infekci snadno spustit. CounterSpy a Spy Sweeper detekovaly 100 procent takových tlačítek a položek menu. SpySubtractPro a Ad-Aware dosáhly 75 procent. Internet Cleanup, ETrust Pest Patrol a McAfee AntiSpyware nezachytily ani jeden takový objekt.

Alternativní cesta k úspěchu

Desátý program v našich testech, **HijackThis** od firmy *Merijn.org* (najdete jej ve verzi 1.99.1 **NA NAŠEM CD**), popřípadě na internetu na adrese jako soubor HIJACKTHIS.ZIP o velikosti 207 KB), není žádným klasickým prohledávacím systémem. HijackThis vám poskytuje zprávu o všech aktivních procesech, klíčích v registru, v nichž se uchová-

vají všechny položky, které se spouští při startu Windows, dále ukazuje obsah všech složek, jejichž obsah se načítá při spouštění systému, zobrazí všechny BHO či služby existující v systému. S tímto protokolem pak můžete snadno určit všechny podezřelé položky a pak je odstranit. I když identifikování podezřelých objektů vyžaduje zkušeného a věci znalého uživatele, je samotný program hravě ovladatelný i pro naprostého laika. Méně zkušený uživatelé tak mohou poslat své protokoly se záznamy do různých internetových fór, kde se jim může podařit nalézt kvalifikovanou pomoc pro identifikaci nevyžádaných procesů.

My jsme použili HijackThis společně s funkcí *Přidat nebo odebrat programy*, dostupnou v Ovládacích panelech Windows XP. Byli jsme velmi mile překvapeni, když se ukázalo, že prakticky všech 45 adwarových či spywarových aplikací mělo odpovídající položku pro odinstalování právě ve funkci *Přidat nebo odebrat programy*.

(K tomu, abyste zmiňované položky pro odinstalování mohli efektivně používat, potřebujete vědět, ke kterým programům patří, což není vždy zrovna jednoduché). Když jsme všechny položky pro odinstalování navržené utilitou HijackThis použili a dále jsme s pomocí stejné utility identifikovali a odstranili všechny ostatní aktivní komponenty, které odinstalátory nedokázaly odebrat, dosáhli jsme doposud nevidaného výsledku – podařilo se nám totiž odstranit 100 procent adwaru či spywaru, jímž byl náš počítač nakažen. Stejněho výsledku jsme dosáhli i tehdy, když jsme použili CounterSpy společně se zmiňovaným HijackThis. Žádnou jinou kombinací testovaných programů se nám stejného výsledku dosáhnout nepodařilo – procesy ovládané spywarem WinTools, které žádný jiný anti-spyware nedokázal odstranit, zmařily naše snahy dosáhnout kompletního vyčištění systému. HijackThis samotný (už z principu jak je postaven) běžící procesy zastavit nedokáže.

Rychlost skenování systému a výsledné zprávy

Během testů jsme zaznamenali i značné rozdíly v rychlosti skenování systému. Nejúčinnějším a zároveň i nejrychlejším programem byl CounterSpy, kterému kompletní skenování systému s 2,7 GB dat trvalo pouhou minutu. Rychlé byly i utility Spybot a SpySweeper, jež stejný systém skenovaly něco málo přes dvě minuty. Na druhou stranu Spyware Eliminator byl z hlediska rychlosti skenování systému nejpomalejší a jeho chování bylo poněkud zvláštní, neboť při opa-

Microsoft Windows Antispyware má šanci stát se nejlepším antispywarovým programem

I firma Microsoft se snaží nezůstávat v boji proti spywaru v pozadí. V polovině února vydala betaverzi svého produktu **Microsoft Windows Antispyware**, založeného na technologii firmy *Giant*, kterou Microsoft koupil v prosinci 2004. V našich testech si tato utilita vedla velmi dobře. Vzhledem k tomu, že její definiční soubory byly daleko aktuálnější než definice ostatních programů, rozhodli jsme se tuto utilitu nakonec do srovnávacích testů přímo nezařadit. Nicméně Microsoft AntiSpyware se po všech stránkách jeví jako produkt útočící na nejvyšší příčky z hlediska výkonnosti a je prakticky připraven k tomu, aby mohl být uveden na trh.

Při našich testech se mu podařilo odhalit a odstranit celkem 91 procent veškerého adwaru či spywaru. Odstranil 96 procent všech procesů běžících v operační paměti, 67 procent spywaru modifikujícího domovskou stránku nebo funkce pro vyhledávání na internetu, 100 procent BHO a panelů nástrojů, 95 procent spywaru usazujícího se v registrech a 100 procent ostatních druhů spywaru, jako jsou kupříkladu podezřelá tlačítka či nabídky v menu v nejrůznějších aplikacích. Naši sadu dat o velikosti 2,7 GB otestoval za necelé tři minuty. Funkce sledování systému v reálném čase u Microsoft AntiSpyware dokáže zastavit možnosti nákazy tím, že zabraňuje všem pokusům o modifikaci do-

movské stránky prohlížeče a funkce pro vyhledávání na internetu, identifikuje neznámé procesy běžící v operační paměti, blokuje neautorizované pokusy o editaci souboru *Hosts* a zabraňuje změnám v registru, které ovlivňují spuštění aplikací při startu Windows.

Aby Microsoft AntiSpyware dokázal bránit internetový prohlížeč proti hijackerům měnícím funkci vyhledávání nebo domovskou stránku, má v sobě integrovanou funkci, která dokáže tyto stránky resetovat na výchozí stránky definované operačním systémem. Pomocí menu *Advanced Tools/Browser Hijack Restore* však můžete určit i svoji výchozí domovskou stránku a stránky zprostředkovávající vyhledávání na internetu. Microsoft AntiSpyware vás pak okamžitě varuje při jakýchkoliv pokusech o jejich změnu. Je to daleko účinnější ochrana oproti té, kterou známe kupříkladu ze Spy Sweeperu od firmy Webroot, která obnovuje stránky do stavu, v němž byly v době, kdy byl Spy Sweeper poprvé instalován.

Pokud máte zájem dozvědět se o Microsoft AntiSpywaru více, přesuňte se na stránky Microsoftu, konkrétně na www.microsoft.com/athome/security/spyware/software/default.msp, kde si jej v souladu s politikou Microsoftu můžete zdarma stáhnout, pokud použijete legální kopii Windows, protože budete vyžadováni k ověření pravosti vašeho operačního systému. Skutečností je, že popisovaná validace



▲ Windows AntiSpyware se ve své betaverzi s naší testovací sadou adwaru a spywaru vypořádal velmi zdatně.

vaší kopie Windows není povinná, takže produkt lze stáhnout i bez ní.

Windows AntiSpyware se může pyšnit jasným, intuitivním rozhraním, jež je téměř identické co se týče funkcí a jejich rozvrstvení v rozhraní programu CounterSpy od firmy Sunbelt Software, tj. aplikaci, která rovněž používá technologii firmy Giant Software. Na rozdíl od utility CounterSpy ignoruje Windows AntiSpyware při skenování systému automaticky cookies, což je příjemná zpráva pro všechny, kteří oceňují možnosti automatického přihlašování ke službám a personalizaci obsahu na některých stránkách, což jsou právě vymoženosti, jež se dají využívat právě díky cookies.

Counter Spy a Spy Sweeper na předních místech

CounterSpy od firmy Sunbelt Software a Spy Sweeper od firmy Webroot identifikovaly a odstranily více než 80 procent adwaru a spywaru, čímž se umístily na předních místech našeho testu.

ANTISPYWARE	Účinnost skenování*	OCHRANA V REÁLNÉM ČASE					OSTATNÍ CHARAKTERISTIKY			Poznámky
		Detekce podezřelých procesů běžících v operační paměti	Ochrana proti změnám klíčů v registru (ty ukryjící informace o spuštění položek při startu Windows)	Ochrana proti změně domovské stránky a funkce vyhledávání na internetu	Ochrana proti změně souboru Hosts	Další**	Podpora plánování skenování systému/ skenování po spuštění systému	Možnost automatických nebo plánovaných aktualizací		
CounterSpy 1.0 (Sunbelt Software), 20 USD www.sunbelt-software.com/CounterSpy.cfm	★★★★★	85 %	●	●	●	●	●	●	Nejúspěšnější detekce spywaru. Rozsáhlé možnosti ochrany systému v reálném čase včetně blokování skriptů a ochrany před nákazou přes Browser Helper Objects (BHO).	
Spy Sweeper 3.2 (Webroot), 30 USD www.webroot.com	★★★★★	81 %	●	●	●	●	●	●	Druhá nejúspěšnější detekce spywaru. Je vybaven štítem blokujícím službu Windows Messenger, která je často zneužívána k zaslání cílené reklamy.***	
Ad-Aware SE Personal 1.0 (Lavasoft), zdarma, www.lavasoftusa.com/software/adaware a NA NAŠEM CD (aawsepersonal.exe, 2.51 MB)	★★★★★	65 %	●	●	●	****	●	●	Zdarma dostupná utilita s nadprůměrnou schopností detekce. Ochrana systému v reálném čase je možná pouze u verze Plus (cena 27 USD) nebo Professional (40 USD).	
SpySubtract Pro 2.6 (InterMute), 30 USD www.intermute.com	★★★★★	56 %	●	●	●	●	●	●	Nepatrně nadprůměrná úroveň detekce. K dispozici je možnost mazání historie v internetovém prohlížeči a bezpečné odstraňování souborů.	
Spybot Search&Destroy 1.3 (Safer Networking), zdarma, www.safer-networking.org a NA NAŠEM CD (spybots13.exe, 4,15 MB)	★★★★★	54 %	●	●	●	●	●	●	Poskytuje průměrnou úroveň detekce, navíc nabízí ochranu systému v reálném čase jako prevenci proti napadení systému.	
ETrust PestPatrol Anti-Spyware 5.0 (Computer Associates), 30 USD, home.ca.com	★★★★★	48 %	●	●	●	●	●	●	Detekce na úrovni mírně pod 50 % a omezené možnosti použití – tento produkt se nijak zvlášť nevyznamenal.	
Spyware Eliminator 3.5 (Aluria Software), 30 USD www.aluriasoftware.com/homeproducts/spyware	★★★★★	32 %	●	●	●	●	●	●	Podprůměrný antispywarový program, obsahuje databázi mírně řečeno problematických webových serverů a prvků ActiveX. Ta má chránit uživatele před nákazou systému.	
McAfee AntiSpyware 1.0 ***** (Network Associates), 40 USD us.mcafee.com	★★★★★	22 %	●	●	●	●	●	●	Tento produkt má velmi slabou úroveň detekce, ochrana systému v reálném čase v našich testech naprosto selhala.	
Internet Cleanup 4.0 (Allume Systems), 30 USD www.allume.com/win/cleanup/index.html	★★★★★	5 %	●	●	●	●	●	●	V testech se projevil jako prakticky nefunkční při ochraně proti spywaru a jeho odstraňování. K dalším funkcím patří blokování pop-up oken, cookies, reklam, rovněž dokáže vyčistit historii.	

Vysvětlivky: ● = Ano, ○ = Ne
* Vyjadřuje celkovou úspěšnost při odstraňování celkem 81 vzorků adwaru a spywaru. Podrobnosti najdete v tabulce **Uklid balastu**.
** Nejedná se o program Windows Messenger.
*** Zahrnuje další možnosti detekce podezřelých objektů v reálném čase, jako například pop-up okna či prvky ActiveX.
**** Ad-Aware uzamkne soubor Hosts až poté, co jej opraví.

kovaných testech mu jednotlivé testy trvaly v rozsahu 10 minut až 1 hodinu. Zbylým programům trvala prohlídka systému 4–5 minut.

Jednotlivé programy také odlišně interpretovaly jednotlivé nalezené infekce. Například pokud jsme nainstalovali panel nástrojů WhenUSearch, CounterSpy jej viděl jako dva odlišné spywarové programy – WhenUSearch a SaveNow. Naopak Ad-Aware detekoval stejný panel nástrojů jako souhrn 73 objektů. Když jsme pak dovolili programu CounterSpy odstranit všechny aktivní komponenty panelu WhenUSearch, AdAware stále ještě hlásil pět kritických objektů – těmi pak byly tři prázdné klíče v registru a dvě prázdné složky. Takové výstrahy jsou však zbytečné a mohou pouze přispět k tomu, že problém spywaru se pak v některých případech jeví jako daleko závažnější, než skutečně je.

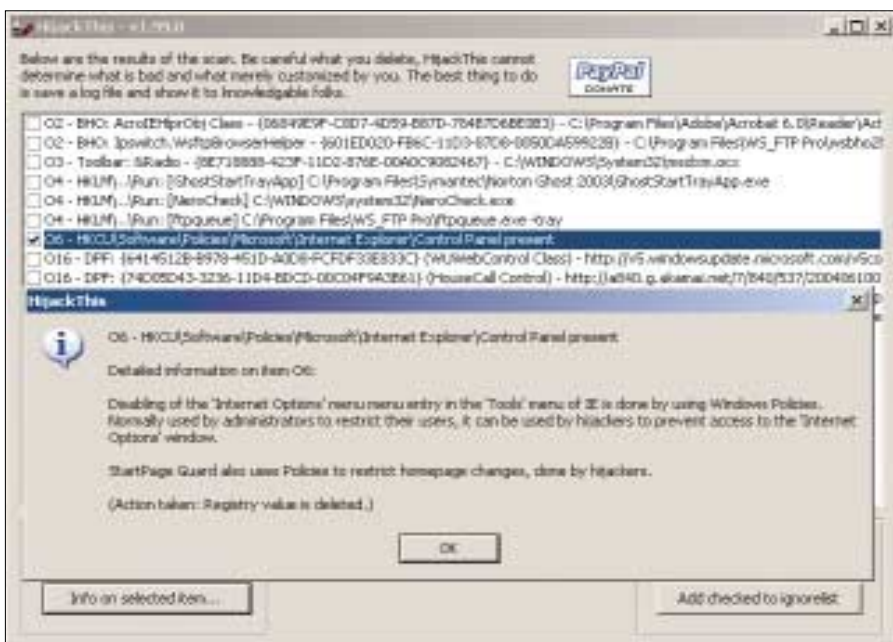
Sledování systému v reálném čase

Schopnost odstranit spyware v okamžiku, kdy je systém infikován, je sice velmi podstatná, ale určitě není pochyb o tom, že důležitější je pro nás

otázka prevence, tj. jak zajistit, aby se žádný škodlivý objekt do systému vůbec nedostal. Jedním z nejúčinnějších nástrojů se na tomto poli stal Spybot. Při použití v něm obsaženého doplňku **Resident TeaTimer** nás utilita varovala pokaždé, kdy se nějaký program pokoušel o změnu v kritických oblastech registru systému. Dokonce i procesům, které představovaly spyware a které byly schopné se samy nahrát do paměti, bylo zabráněno modifikovat registr – a tak byly okamžitě likvidovány obvyčejným okamžitým restartem systému.

Spybot dokonce disponuje i možností chránit před modifikací soubor *Hosts*. Tento soubor totiž představuje pro internetový prohlížeč jakousi mapu. Každý záznam se v něm totiž skládá z názvu webového serveru a odpovídající IP adresy, na níž se má přeměrovat. Škodlivé programy často tento soubor zneužívají k tomu, aby zabránily uživatelům v návštěvě bezpečnostně orientovaných stránek, jako jsou například stránky výrobců antivirových programů.

CounterSpy a Spy Sweeper také blokovaly pokusy o modifikaci zmíněného souboru *Hosts*, zastavovaly pokusy o editaci registru systému, zabraňovaly v internetovém prohlížeči změně na-



▲ HijackThis vypíše seznam všech procesů běžících ve vašem systému, ovšem než něco podniknete, je nutné vygenerovaný seznam konzultovat s odborníkem.

McAfee AntiSpyware má zabudovanou funkci sledování systému v reálném čase, ale vzhledem k její nízké rozpoznávací schopnosti se účinnost této funkce prakticky rovnala nule.

Co se týče programů Spyware Eliminator či Internet Cleanup, ani jeden z nich na poli sledování systému v reálném čase příliš nebyl. Spyware Eliminator má k dispozici pouze „černou listinu“ podezřelých WWW stránek a prvků ActiveX – i když samotná unikátní možnost existence takového seznamu je také velmi hezkým rysem programu. Podobně jako Spyware Eliminator i Internet Cleanup ignoroval možné změny nastavení domovské stránky a funkce pro vyhledávání na internetu, zcela propadl v testech zaměřených na detekci podezřelých procesů a chyběla mu rovněž možnost ochrany souboru *Hosts*. Na druhou stranu nabízí integrovaný blokátor pop-up oken a dále dokáže blokovat odesílání osobních dat, čímž zabraňuje jejich potenciálnímu zneužití.

Jednoduchost použití

Rozhraní programu CounterSpy je velmi přitažlivé a snadno se s ním pracuje. Tlačítko *Scan Now* se nápadně objevuje již na uvítací obrazovce, jednotlivá menu se procházejí snadno a ukončení programu není spojeno s ukončením ochrany v reálném čase. Uživatelské prostředí programu Ad-Aware je rovněž atraktivní, ovšem jednotlivé nabídky programu jsou ukryty za nepopsanými ikonkami a je potřeba trocha odhadu, abyste zjistili, do kterého z nich se máte podívat. Pokud chcete používat Spybot, pak se pro jeho konfiguraci

stavení domovské stránky a funkce pro vyhledávání na internetu a pokoušely se detekovat podezřelé procesy běžící v operační paměti.

Ad-Aware SE Personal není vybaven funkcí sledování systému v reálném čase, i když se v něm dá nastavit ochrana proti zápisu do souboru *Hosts*. Placené verze Ad-Aware – SE Plus (27 USD) a SE Professional (40 USD) mají integrovanou funkci **Ad-Watch**, připomínající podobné funkce v pro-

gramech CounterSpy a Spy Sweeper. ETrust PestPatrol Anti-Spyware byl schopen detekovat podezřelé procesy běžící v operační paměti, ale nedokázal nás varovat, pokud byly provedeny změny v některých ze systémových nastavení. SpySubtract Pro nás varoval v případě, kdy byla provedena změna nastavení domovské stránky a funkce pro vyhledávání na internetu, a zároveň detekoval podezřelé procesy v operační paměti.

Úklid balastu

Při testování měly antispywarové utility za úkol nalézt a odstranit 45 druhů adwaru a spywaru, který vytvořil celkem 81 škodlivých procesů v různých formách. CounterSpy od firmy Sunbelt nalezl a opravil 85 % veškerého spywaru a adwaru, Spy Sweeper od firmy Webroot splnil úkol na 81 %. Tyto hodnoty je dostaly do čela všech testovaných programů. Na druhé straně Internet Cleanup od firmy Allume detekoval pouhých 5 % škodlivého softwaru.

ANTISPYWARE	Běžící procesy		Modifikace domovské stránky a funkce pro vyhledávání na internetu		Browser Helper Objects (BHO) a panely nástrojů		Modifikace registru (v klíčích, v nichž jsou údaje o tom, které aplikace se mají spustit při startu Windows)		Menu a tlačítka		Celkem	
	Nalezeno	V procentech	Nalezeno	V procentech	Nalezeno	V procentech	Nalezeno	V procentech	Nalezeno	V procentech	Nalezeno	V procentech
Množství škodlivého softwaru	27		15		13		22		4		81	
Internet CleanUp 4.0 (Allume Systems)	3	11 %	0	0 %	0	0 %	1	5 %	0	0 %	4	5 %
Spyware Eliminator 3.5 (Aluria Software)	10	37 %	1	7 %	4	31 %	9	41 %	2	50 %	26	32 %
ETrust PestPatrol Anti-Spyware 5.0 (Computer Associates)	20	74 %	0	0 %	8	62 %	11	50 %	0	0 %	39	48 %
SpySubtract Pro 2.6 (InterMute)	20	74 %	0	0 %	8	62 %	14	64 %	3	75 %	45	56 %
Ad-Aware SE Personal 1.0 (Lavasoft)	20	74 %	5	33 %	8	62 %	17	77 %	3	75 %	53	65 %
McAfee AntiSpyware 1.0 (Network Associates)	9	33 %	0	0 %	4	31 %	5	23 %	0	0 %	18	22 %
Spybot Search&Destroy 1.3 (Safer Networking)	17	63 %	7	47 %	8	62 %	11	50 %	1	25 %	44	54 %
CounterSpy 1.0 (Sunbelt Software)	25	93 %	8	53 %	13	100 %	19	86 %	4	100 %	69	85 %
Spy Sweeper 3.2 (Webroot)	24	89 %	7	47 %	13	100 %	18	82 %	4	100 %	66	81 %

Chraňte se před spywarem: aktualizujte pravidelně svůj prohlížeč nebo přejděte na jiný a bezpečnější

Jednou z možností, jak se chránit před spywarem, je možnost přejít z Internet Exploreru na jiný prohlížeč, například na Mozillu Firefox. Ale i přechod na jiný prohlížeč s sebou přináší problémy. Alternativní prohlížeče mají také své bezpečnostní trhliny, které vás mohou přivést do problémů. Navíc se můžete dostat do nepřijemností tehdy, kdy si budete potřebovat prohlédnout internetové stránky, které se korektně zobrazují pouze v Internet Exploreru.

Pro ty, kteří nechtějí přejít na alternativní prohlížeč, je tu Internet Explorer ve verzi 6 a vyšší, který má výchozí bezpečnostní nastavení nakonfigurováno tak, že poskytuje slušnou ochranu proti spywaru. Rozhodně tedy doporučujeme používat nejnovější verzi Internet Exploreru a instalovat všechny dostupné aktualizace určené pro systém Windows (viz stránky windowsupdate.microsoft.com). Dále je nutno věnovat maximální pozornost tomu, co do počítače in-

stalujeme a neinstalovat do systému neznámé programy – i to pomáhá bojovat proti spywaru.

Pokud se rozhodnete instalovat nějaký program, určitě si pečlivě přečtěte licenční ujednání (EULA); mělo by pro vás být dostatečným

► **Ani Zango nemusí být v systému vítáno, ale kdo si pozorně přečte licenční ujednání, dozví se, co všechno od něj může očekávat. Pak ho jistě nepřekvapí, když jeho internetový prohlížeč bude neustále přeměrován na WWW stránky zamořené reklamou.**



musíte nejprve přepnout do pokročilého režimu. Jak Ad-Aware, tak CounterSpy poskytují srozumitelné výsledky skenování, i když Ad-Aware označil několik cookies jako kritické objekty, což může naznačovat, že cookies jsou velmi riziková – to však nemusí být vždy pravda.

HijackThis má jednoduché textově orientované rozhraní, které poskytuje velmi dobrý přehled o všech možnostech programu a vůbec se celá aplikace neobvykle snadno ovládá. Na druhou stranu výsledná zpráva z programu je pro běžného uživatele téměř nesrozumitelná.

Spyware Eliminator je vybaven jednoduchým rozhraním s čitelným menu, ale spuštění programu trvá dlouho. Rozhraní Internet Cleanup je nepřehledné a špatně se s ním pracuje. Jednotlivá menu se měnila podle toho, v jaké sekci jsme se pohybovali, a co bylo neobvyklé – jediným výchoziskem, pokud jsme zabloudili příliš hluboko do struktury menu, bylo tlačítko Home, jehož pomocí jsme se mohli „vysvobodit“.

Uživatelské rozhraní programu ETrust PestPatrol Anti-Spyware nám připadalo neútluné a málo přitažlivé, i když orientace v něm byla dobrá. I tady byla na začátku drobná chybička. Na uvítací obrazovce bylo nejviditelnější tlačítko *Enter License Key*. Až po přečtení textu psaného drobným písmem jsme byli ujištěni, že jsme program již správně zaregistrovali.

Rozhraní aplikace Spy Sweeper bylo sice intuitivní, avšak nebylo možné ukončit program, aniž bychom současně neukončili ochranu systému v reálném čase. Jediným výsledkem byly početné dotazy, zda skutečně chceme vypnout ochranu systému nebo chceme program pouze minimalizovat. Dalším extrémem byl



▲ Jakmile jednou pochopíte podivné ikonky Ad-Awaru a porozumíte jim, bude vám již ovládání tohoto programu připadat velmi jednoduché.

McAfee AntiSpyware, nainstalovaný jako součást aplikace McAfee Security Center – ta byla představována ikonkou v pravé části Hlavního

panelu. Security Center nám totiž neumožnil se k antispywarové komponentě vůbec dostat.

Závěr

Antispywarové programy se dají sehnat zdarma, ale obáváme se, že právě toto je jedna z oblastí, kde se šetřit nevyplácí. Zdarma dostupný Spybot Search&Destroy poskytuje detekci okolo 54 procent a nabízí ochranu systému v reálném čase. Pokud přesto chcete zůstat u zdarma dostupných alternativ, pak byste měli kombinovat Spybot s Ad-Aware SE Personal, jehož schopnost detekce je v případě aktivní hrozby o něco vyšší než u Spybotu. Avšak pokud byste kombinovali Ad-Aware, Spybot a zdarma dostupný HijackThis, podobně jako my při našich testech, dosáhnete při odstraňování spywaru či adwaru 100% úspěšnosti.

CounterSpy od firmy Sunbelt Software, který se stal v našich testech favoritem, se projevil jako utilita s nejvyšší schopností detekce, nejvyšší rychlostí skenování. Cena 20 USD za roční licenci pro používání programu a technickou podporu nepředstavuje ani v našich podmínkách žádnou finanční katastrofu. Pokud se rozhodnete pro Spy Sweeper od firmy Webroot, ani tentokrát neprohloupíte, neboť je prakticky srovnatelný s programem Counter Spy: rychlost skenování systému je dostatečná, jeho použití je rovněž jednoduché. Kombinací libovolného z obou produktů s utilitou HijackThis a s dávkou rozvahy při instalaci čehokoliv do systému bez problémů udržíte svůj systém nezasazený jakýmkoliv druhem spywaru či adwaru.