Anti-spyware: nejlepší obránci

Mary Landesmanová, Michal Bareš

Ne, nemusíte se smířit se spywarem, který blokuje váš osobní počítač a porušuje vaše soukromí. Přinášíme přehled nových nástrojů a prostředků, jejichž pomocí se můžete spywaru účinně zbavit.

Spyware je stále chytřejší. Představuje nová nebezpečí, dnes ještě větší než před několika měsíci: napadá prohlížeč, sleduje vás, jak surfujete po webu, vykrádá vaše data. Váš současný anti-spyware možná již na tyto hrozby nestačí.

Ale naštěstí ani ti, kdo se spywarem bojují, nijak nezahálejí a vyvíjejí nové prostředky ochrany. Za účelem přehledu, který zde přinášíme, jsme testovali celou škálu aktualizovaných i zcela nových produktů. Naši testovací skupinu tvoří jednak pět placených samostatných nástrojů: McAfee AntiSpyware 2006, Spyware Doctor 3.2 v rámci PC Tools, Counter-Spy 1.029 od firmy Sunbelt Software, AntiSpyware 3.0 od firmy Trend Micro a Spy ;Sweeper 4.0 od firmy Webroot Software dále tři integrované bezpečnostní balíčky (tyto soupravy jsou dražší než samostatné spywarové aplikace, obsahují však ještě antiviry, firewall, antispam a programy na ochranu soukromí): Panda Platinum Internet Security 2005, Symantec Norton Internet Security 2005 Antispyware Edition a ZoneAlarm Internet Security Suite 6.0 firmy Zone Labs. Nakonec jsme ještě otestovali bezplatné produkty: Ad-Ware SE Personal Edition 1.06 od Lavasoftu, veřejně přístupnou betaverzi Windows Antispyware (Beta 1.0.615) od Microsoftu a Spybot Search & Destroy 1.4 společnosti Safer Networking.

Zatímco adware dokáže člověka nanejvýš otravovat, spyware může být opravdu nebezpečný, a proto jsme se zaměřili právě na něj. Spyware se nejen sám tajně instaluje do systému, ale může bez vašeho vědomí také stáhnout a nainstalovat další nežádoucí aplikace. Shromáždili jsme desítky spywarových programů včetně jejich nejnovějších verzí, které uvízly v našich sítích při posledním zátahu na spyware, nevyhýbali jsme se přitom ani nejnovějšímu malwaru.

Spywarové programy přidaly na náš testovací počítač celkem 73 nežádoucích souborů. Právě na nich jsme pak zjišťovali schopnost antispywaru detekovat je a vyčistit všechny komponenty. Všimněme si nyní, jak jednotlivé produkty při této zkoušce obstály.

Výsledky

Naši favorité: Spy Sweeper 4.5 firmy Webroot, který lze pořídit za 30 dolarů, odstranil 90 procent spywarových prvků, čímž dosáhl nejlepšího skóre a vyhrál tak v kategorii samostatných aplikací. Tento produkt můžeme doporučit každému, kdo už má nějaký antivirový a antispamový software i firewall. Z tří testovaných balíčků můžeme dále doporučit Platinum Internet Security 2005 od firmy Panda Software, který pořídíte za 50 dolarů. Naše konečná volba toho, co je nejlepší možný nákup v rámci integrovaných souprav, padla právě na tento software, neboť dosáhl nejlepšího výsledku, pokud jde o celkovou účinnost při odstraňování spywaru, a druhého nejlepšího výsledku ze všech testovaných utilit, neboť dokázal odstranit 86 procent spywarových prvků. Panda rovněž odstraňovala spyware, aniž nás ale přitom nutila schvalovat každý krok.

Mezi produkty, které lze získat zdarma, nevynikl žádný. Nechce-li se vám za odstraňovače spywaru platit, doporučujeme ;vám, abyste alespoň používali více než jen jeden program tím zvýšíte svoji bezpečnost.

Nejvýraznější zlepšení jsme zaznamenali u McAffee AntiSpywaru 2006 (cena 30 dolarů), který v našich testech dokázal lapit 79 procent všech spywarových prvků. Loni tentýž

software odstranil pouze 22 procent testovaného spywaru. Spywary i antispywary se od posledních testů hodně změnily, taková míra zlepšení je však přesto pozoruhodné.

Souprava od Symantecu rovněž odstranila 79 procent veškerých ;testovaných spywarových prvků ale občas nabízela uživateli poněkud pochybná doporučení. Například nám doporučila, abychom umožnili internetový přístup trojskému koni FXAgent, tedy keyloggeru aktivovanému přes vložený e-mailový odkaz, který se tváří, jako by vedl k nástroji od firmy Symantec. Během instalace se výsledný soubor *dlhost.exe*, který se posléze snaží připojit k internetu, přidal do adresáře systému Windows. Symantec říká, že nyní již poskytuje update tohoto softwaru, který dokáže tohoto trojského koně identifikovat a zneškodní ho ihned, jakmile na něj narazí.

Nejvíc nás zklamal CounterSpy od firmy Sunbelt Software (cena 20 dolarů), někdejší vítěz naší soutěže. Vymazal totiž pouze 66 procent veškerých spywarových prvků, a to je opravdu málo, vzhledem k 85procentní účinnosti, které dosáhl v dřívějších testech. Microsoftem zdarma poskytovaná betaverze Windows AntiSpyware odstranila také pouze 66 procent veškerých spywarových prvků. Tato podobnost nepřekvapuje, jelikož oba produkty používají technologii od Giant Company Software, antispywarové firmy, kterou Microsoft koupil loni v prosinci.

Pro účely tohoto článku jsme rovněž testovali komerčně nabízený ;CounterSpy 1.029 novější verze 1.5, kterou jsme v době testu měli k dispozici pouze jako betaverzi (betaverze placených programů do testů nezařazujeme), však podle Sunbeltu již obsahuje přebudovaný engine.

Podíváme-li se na naše poslední dvě hodnocení, mezi nimiž uběhlo pouhých sedm měsíců, můžeme zaznamenat přesuny na prvních i ;posledních místech žebříčku to ukazuje, jak důležité je v této oblasti neustále držet krok s vývojem a znát aktuální nebezpečí i případné možnosti ochrany.

Odstranění nepořádku: Jedním z klíčových kritérií anti-spywarového softwaru je schopnost likvidovat spywarové ;procesy, jež aktivně probíhají v paměti tyto procesy představují pouze část činnosti spywaru, o níž jsme se zmínili výše. Panda byla jediným programem, který dokázal probíhající procesy odstranit stoprocentně. Těsně následoval McAffee, který zneškodnil 96 procent. Na třetí příčce se umístil Spy Sweeper s 88 procenty.

Některé spywarové prvky zkoumané v našem testu změnily domovskou stránku Internet Exploreru, vyhledávací stránku, pomocné objekty prohlížeče (BHO) a nástrojové lišty (panely nástrojů), jakož i oblast důvěryhodných serverů. U anti-spywarových produktů jsme sledovali jejich schopnost detekovat tyto nežádoucí změny a vrátit pak vše do původního stavu.

Spy Sweeper detekoval a následně čistil nejlépe ze všech: dokázal nejen eliminovat 100 procent objektů BHO a nástrojových lišt (toolbars), vložených do prohlížeče našeho testovacího počítače, nýbrž rovněž odstranit již proběhlé změny na úvodních a vyhledávacích stránkách prohlížeče a vrátit vše do původního stavu. Panda a McAffee odstranily 100 procent nástrojových lišt a BHO, ale nedokázaly vrátit do původního stavu již existující změny na úvodních a vyhledávacích stránkách prohlížeče. Soupravy Trend Micro a ZoneAlarm rovněž nedokázaly opravit změny na těchto stránkách, přesto však odstranily v prvním případě 50 procent a ve druhém 86 procent nástrojových lišt (toolbars) a BHO. Symantec sice stoprocentně odstranil změny na všech stránkách, ale poradil si jen s 79 procenty nástrojových lišt a BHO.

Spy Sweeper firmy Webroot nejen odstranil všechny nástrojové lišty a BHO, ale byl také jedinou anti-spywarovou aplikací, která odhalila a zlikvidovala zvláště zákeřnou variantu

Look2Me. Tento program se uloží do přihlašovací procedury Windows a pak bedlivě sleduje webové stránky, které navštívíte a z nichž se do vašeho počítače natahuje spyware nebo adware.

Dozor nad chováním

Mnoho anti-spywarových produktů se snaží nejen očistit počítač od známého spywaru, ale rovněž zabránit tomu dosud neidentifikovanému, aby se usadil na vašem počítači. Anti-spywary přitom fungují tak, že sledují ty části systému, na které zákeřný software obvykle útočí, všímají si podezřelého chování a pak se ho snaží zastavit. Abychom u anti-spywaru mohli hodnotit jeho schopnost všimnout si podivného chování, vytvořili jsme aplikaci, která generuje právě takové typy chování, jimiž se vyznačují nejrůznější spywarové a adwarové instalace: např. přidává spouštěcí hesla registru, přidává soubor do adresáře Startup, pozměňuje úvodní a vyhledávací stránky prohlížeče a přepisuje hostitelský soubor, tedy první místo, kam se obracejí Windows při vyhledávání webových adres, na které se chcete dostat. Spyware může modifikovat soubor Hosts takovým způsobem, že vás přesměruje na určitá místa (např. na servery s adwarem) nebo vám naopak zabrání se někam dostat (např. na stránky firem nabízejících antiviry).

CounterSpy, McAffee, Spybot, Spy Sweeper, Spyware Doktor, Windows AntiSpyware a souprava ZoneAlarm - všechny tyto prostředky a nástroje poskytují ochranu monitorující chování počítače. Jednoznačně se ukázalo, že nejúčinnější je Spy Sweeper.

Z hlediska jednoduchosti ovládání se na nejvyšší příčce umístila souprava od firmy Panda: odstraňuje totiž nalezený spyware a adware, nevyžaduje však zásahy uživatele. Standardní nastavení lze ovšem změnit tak, aby bylo možné rozhodovat případ od případu. Souprava ZoneAlarm zobrazuje řadu výstražných hlášek, které vyžadují vaši reakci, což může být poměrně náročné, nerozumíte-li do hloubky problematice bezpečnosti.

Ani rozhraní McAffee nás právě nenadchlo. Ikona, která se objevuje v oznamovací oblasti systému Windows (vedle hodin), ;totiž nespustí anti-spywarový skener místo toho spouští a napojuje se na McAffee SecurityCenter, kde se inzerují další produkty McAffee, avšak McAffee AntiSpyware mezi nimi nenajdete.

Bitva pokračuje

Jak již bylo řečeno, spyware se neustále mění a spolu s ním se mění i nástroje na jeho potírání. V době, kdy čtete tento článek, se pět výrobců - Sunbelt, Symantec, Webroot a Microsoft - chystá svůj software aktualizovat. Jakmile nové produkty uvolní, znovu prověříme, nakolik jsou proti nejnovějším a nejzákeřnějším hrozbám účinné.