Microsoft AntiSpyware

Důsledná obrana

K velkým bezpečnostním rizikům současnosti patří malware – „speciální“ programy, které se tajně instalují na váš počítač a dělají věci, jež se vám příliš nezamlouvají… Kromě narušení soukromí přináší spyware i takové nepříjemnosti, jako je ztráta výkonu a podivné chování některých programů (typicky internetového prohlížeče).

Text: Jiří Macich ml., *jirka.macich@macich.net*, *http://blog.macich.net*

V řadách široké veřejnosti je povědomí o malwaru (a „spywaru“) velmi malé. Podle průzkumu zveřejněného koncem srpna 2005 na serveru The Inquirer nemá 64 % uživatelů ponětí, co je to spyware, a 11 % uživatelů si dokonce myslí, že jde o nějaké zařízení z Hvězdných válek *www.theinquirer.net/?article=25587*).

Uživatelé mívají na svém počítači nainstalován maximálně antivir, avšak většina antivirů je na spyware krátká. Rozhodně také neplatí, že pokud nepoužíváte Internet Explorer, je váš počítač vůči spywaru imunní. Není proto divu, že existují speciální programy pro vyhledávání a odstranění spywaru a že patří k nejžádanějším programům na „stahovacích“ serverech, jako je Download.com nebo Slunečnice.cz.

Stranou nezůstal ani Microsoft, který se snaží napravit svou pošramocenou pověst v oblasti bezpečnosti svých produktů. V některých případech pak MS volí strategii kupovat hotové technologie na úkor vývoje vlastních. A to je i případ programu Microsoft Windows AntiSpyware. Koncem loňského roku koupil Microsoft malou firmu Giant Company Software, která kromě produktů Spam Inspector a Popup Inspector stála i za programem Giant AntiSpyware, jenž spadá právě do skupiny nástrojů pro boj se spywarem. Vývojáři Microsoftu ho přepracovali, a tak vznikl Microsoft Windows AntiSpyware, který je od začátku letošního roku ve fázi veřejného beta testování.

Najít a zlikvidovat

Windows AntiSpyware je komplexní řešení pro boj proti spywaru. Základem je klasický nástroj na vyhledávání spywaru, který se již zabydlel ve vašem systému. Kromě souborů na všech pevných discích jsou kontrolovány i prováděné procesy a klíče v systémovém registru.

Po dokončení vyhledávání spywaru se zobrazí okno shrnující informace o provedené akci, po jehož uzavření můžete začít řešit, co s nalezeným spywarem.

Windows AntiSpyware vám před definitivním rozhodnutím, co se špiony ve vašem počítači, předloží další důležité informace. Ke každému nalezenému objektu připraví program dostupné informace o záškodníkovi. Tyto informace lze vytisknout, nelze je však bohužel uložit do souboru. Kromě podrobného popisu je přítomen i grafický indikátor stupně závažnosti. Podle odhadnutého stupně závažnosti jsou předdefinovány volby, jak s nalezeným objektem naložit.

Objekt můžete ignorovat dočasně, nebo natrvalo a můžete ho dát do karantény, nebo rovnou odstranit. Před odsouhlasením těchto voleb je ještě možné zaškrtnout přepínač pro vytvoření bodu obnovy systému pro případ pozdějších problémů.

Sken může být také spouštěn automaticky, v určitých periodách podle vaší volby. Naplánování kontroly je pohodlné, chybí však možnost například automaticky vypnout nebo alespoň uspat počítač po jejím dokončení, což je velké minus v případě, že si potrpíte na „automatizovanou“ údržbu.

Ochrana v reálném čase

Nástroj pro nalezení spywaru pochopitelně najde jen takové špiony, kteří jsou už ve vašem počítači zabydleni. Windows AntiSpyware proto nabízí také Real-time Protection, což je systém ochrany blížící se rezidentnímu antivirovému štítu. Odhaluje totiž útoky spywaru v „reálném čase“.

Rezidentní štít Windows AntiSpyware nabízí tři základní agenty – pro internet, pro systém a pro aplikace. Agent střežící systém hlídá celkem 25 oblastí systému – například neautorizované změny v kontextových nabíd- →

STAHUJTE ZDARMA

Každý zájemce si může veřejnou a už pohodlně použitelnou beta verzi zdarma stáhnout z *www.microsoft.com/athome/security/spyware/software/default.mspx*. Veřejná testovací verze je zatím pouze v anglickém jazyce a spustit ji lze výhradně pod Windows 2000/XP a pod Windows Server 2003. Rovněž potřebujete nainstalovaný prohlížeč Internet Explorer 6, ten však nemusí být nastaven jako výchozí prohlížeč.

Volba: Každému z odhalených záškodnických programů lze určit jeho osud...

Start: U programů spouštěných po startu najdete řadu zajímavých informací.

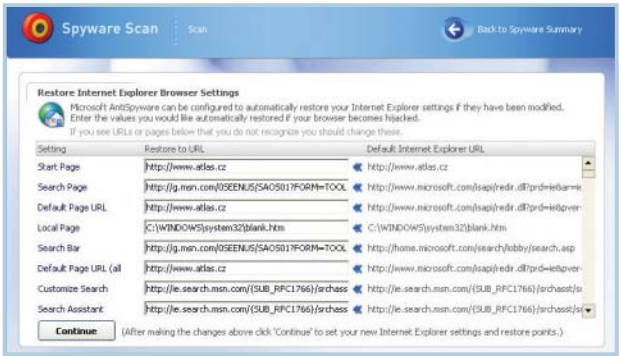
kách, úpravy klíčových souborů system.ini a win.ini nebo zásahy do nastavení systému Windows Update.

Druhý agent, hlídající aplikace, kontroluje programy spouštěné při startu Windows, běžící procesy, různé změny v nastavení Internet Exploreru, instalaci ActiveX aj. Celkem je zde opět 25 položek.

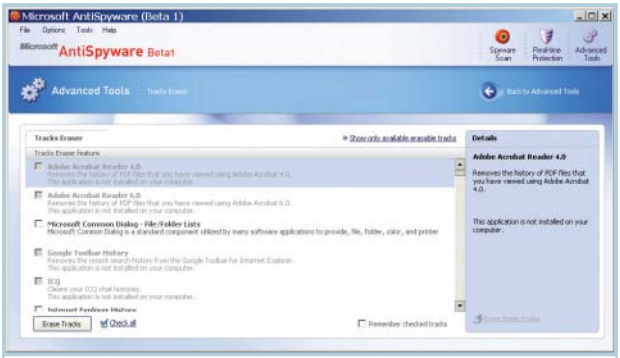
Třetí agent, chránící před nebezpečími z internetu, sleduje devět oblastí, například neautorizované aktivity vykonávané v rámci Wi-Fi připojení nebo vytáčeného připojení k internetu. Nechybí ani ochrana před tajným rozesíláním nevyžádaných e-mailových zpráv (tzv. spamu) z vašeho počítače.

Budoucnost

Windows AntiSpyware bude i po svém dokončení k dispozici zdarma, a to jako součást chystaného Internet Exploreru 7.0, ovšem pod názvem Windows Defender. Zda bude šířen i samostatně, není zatím jisté. Windows AntiSpyware, resp. Windows Defender bude i jedním z bezpečnostních pilířů



Zajímavé: Najdete zde i řadu zajímavých nastavení Internet Exploreru.



Stopy: Microsoft AntiSpyware nabízí i poměrně rozsáhlé mazání záznmů o činnosti na PC.

Windows Vista (codename Longhorn), která přijdou na trh v druhé polovině roku 2006. Je vysoce pravděpodobné, že finální verze bude oficiálně lokalizována.

Finální verze zřejmě nebude na rozdíl od verzí testovacích dostupná pro Windows 2000, ale výhradně pro Windows XP a Windows Server 2003 (Windows Vista ji budou mít předinstalovánu).

Microsoft sliboval, že Windows AntiSpyware bude spolupracovat s Centrem zabezpečení ve Windows XP, avšak zatím tomu tak není. Je možné, že k nápravě dojde buď s finální verzí Windows AntiSpyware, nebo s třetím servisním balíčkem, který by měl být k dispozici krátce po vydání Windows Vista.

Používat?

Je patrné, že Windows AntiSpyware může být ve finální verzi špičkou v kategorii programů pro boj se spywarem. Má však smysl používat jej už teď, tedy ve stadiu veřejné beta verze? Velkou výhodou může být v tomto případě to, že nejde o nový, ale spíše o „přepracovaný“ produkt, tudíž fatální omyly nehrozí.

Spoléhat se výhradně na něj vám raději nedoporučujeme (přece jen to je zatím pouze testovací verze). Řada bezpečnostních expertů však nabádá k používání dvou antispywarových nástrojů současně, takže nebude na škodu používat ho ve spojení s jiným prověřeným freewarovým produktem (Spybot – Search & Destroy nebo Ad-Aware SE Personal Edition). ■ ■ ■

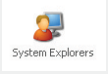
DOPLŇUJÍCÍ NÁSTROJE

Windows AntiSpyware nabízí kromě skenování a rezidentního štítu tři další, neméně zajímavé nástroje.

Browser Restore

Browser Restore slouží k návratu výchozího nastavení Internet Exploreru, které může být buď tzv. tovární (takové, které nastavil Microsoft), nebo uživatelské, tedy takové, které používáte vy. Pomocí Browser Restore lze obnovit výchozí a domovskou stránku, preferovaný vyhledávač určený k hledání přes řádku s adresou a různé chybové stránky (stránka nenalezena, přístup odepřen apod.). Celkem lze pomocí této funkce uchovávat a v případě potřeby obnovit 23 různých nastavení, která souvisí s jmenovaným okruhem voleb. Zajímavé je, že zde můžete nastavit i to, co normálně v Internet Exploreru nastavit nelze a u čeho je pro změnu nastavení nutné použít editor registrů. Jde například o preferovaný vyhledávač (IE preferuje MSN Search). Nevýhodou je to, že nelze archivovat a v případě potřeby obnovit například nastavení připojení k internetu nebo volba preferovaných programů pro prohlížení HTML kódu nebo práci s elektronickou poštou. Funkce Browser Restore je určena jen pro Internet Explorer.

Tracks Eraser



Tracks Eraser dokáže z počítače odstranit informace o vašich aktivitách. Odstranit lze obsah koše (klasické vysypání), seznamy naposledy otevřených souborů obecně i v jednotlivých vybraných programech, naposledy prohlížené internetové stránky, cookies, data zadaná do formulářů, historii konverzací na ICQ, historii hledání souborů anebo prohledávání registrů pomocí regeditu, seznam archivů, se kterými jste pracovali ve WinZIPu nebo WinRARu, historii hledání na službě KaZaa, URL zadávané do adresního řádku v IE atd.

Samozřejmě že opět nemusíte mazat vše – rozsah si můžete zvolit sami zaškrtáním jednotlivých položek z předlouhého seznamu.

System Explorers

System Explorers je souhrnný název pro řadu „průzkumníků“, kteří vám zajistí kontrolu celé řady nastavení a vlastností jak Internet Exploreru, tak i celé řady programů a samotného systému.

V části Applications můžete například spravovat programy spouštěné po přihlášení do Windows. Jejich spouštění lze zakázat, nebo je alespoň možné získat informace, jako je popis, vydavatel, verze apod. Lze zde také pohodlně spravovat právě běžící procesy nebo kontrolovat používané komponenty ActiveX v Internet Exploreru. Za zmínku stojí především to, že zde nechybí vypsání informací o jednotlivých komponentách ani jednoduché grafické znázornění toho, zda se jedná o známou, či neznámou komponentu, včetně její případné nebezpečnosti.

V části Internet Explorers lze kontrolovat jak IE toolbars, tak i samotné Browser Helper Objects, ovšem pouze ty aktivní (kompletní kontrolu nad BHO máte v IE v nabídce *Nástroje/Spravovat doplňky*...). V této sekci lze měnit i různé skryté volby Internet Exploreru, jako je třeba výchozí vyhledávač, soubory s chybovými hláškami (stránka nenalezena apod.), ale třeba i výchozí stránku. Tato funkce tedy tak trochu „leze do zelí“ Browser Restore.