Ad-Aware 2008

Alexandr Radecký

Ad-Aware je známý a oblíbený program k ochraně počítače před škodlivými programy, které se často nainstalují bez vědomí uživatele, občas i s jeho vědomím (to se vydávají za něco jiného, obvykle užitečného). Následně zobrazují nevyžádanou reklamu (adware), popřípadě odesílají soukromá data uživatele neznámo kam (spyware). PC World svým čtenářům exkluzivně nabízí 90denní možnost vyzkoušet program ve verzi Pro, jež je běžně dostupná výhradně na komerční bázi.

Instalace programu

Spusťte instalaci poklepáním na soubor *aaw2008trial_159.exe*, vyberte vhodný jazyk, v další části budeme předpokládat, že je to angličtina. Pokračujte tlačítkem **OK**.
Dále stiskněte tlačítko **Next**, zvolte **I accept the licence agreement**, pokračujte dalším **Next**, zadejte jméno a organizaci (není to ovšem nutné), opět **Next**, ponechejte první volbu standardní instalace, **Next**, zadejte cílový adresář, **Next**, **Next**. Ke konci instalace spustí program automatickou aktualizaci svých součástí, tedy nic, čeho byste se měli obávat. Proces dokončete klávesou **Finish**.
Pokud jste zvolili standardní instalaci, ihned po jejím skončení se spustí program a aktualizace definičních souborů, tedy těch, v nichž se uchovávají informace o závadných aplikacích. Po jejím ukončení se zobrazí hlavní okno Ad-Aware 2008.

Hlavní funkce

Okno programu se skládá ze dvou částí, a to z levého panelu se všemi programovými volbami a z hlavního informačního okna, které zároveň obsahuje i nejdůležitější a nejčastěji používané funkce: **Update** (aktualizace), **Scan Now** (hledání závadných programů v počítači) a **Upgrade** (zakoupením licence lze program natrvalo přeměnit na profesionální verzi).

Ovládací panel v levé části je rozdělen na tyto části:
Status:

- **Main Status**: zobrazí hlavní informační okno.
- **Statistics**: statistika dosavadních vyhledávání.
- **Log Files**: podrobné informace o všech hledáních a nalezených škodlivých programech.

Scan:

- **Scan Mode**: prohledávání počítače, podrobněji rozebírané v další části textu.
- **Quarantine & Ignore**: seznam souborů v karantnéně, tedy těch, které byly shledány podezřelými a odklizeny do zvláštního adresáře. Vpravo dole jsou tlačítka **Delete** a **Restore**. První volba vybraný soubor smaže, druhá ho pak obnoví do původního místa v počítači. Druhá záložka (**Ignore List**) ukáže seznam souborů, u nichž uživatel stanovil, že nemají být prohledávány a nemají být mazány či izolovány, i když u nich existuje podezření na škodlivý obsah.
- **Sheduler**: tady lze naplánovat pravidelná prohledávání počítače, a to kliknutím na tlačítko **Add**. Zvolíte typ skenování, jeho četnost a čas, kdy má začít.

Ad-Watch: zde můžete spustit součást programu Ad-Aware, která je stále aktivní a chrání počítač proti infekcím, podrobněji dále.

Web Update: aktualizace definičních soborů programu.

Tools & Plug-Ins:

- **Tools**: v této složce se nacházejí dva nástroje. První, **Process Watch**, je obdobou Správce úloh systému Windows, zobrazuje tedy podrobnosti o aktuálně spuštěných programech a jejich provázanost. Každý proces lze také nechat zkontrolovat či ukončit. Tento nástroj doporučujeme pouze zkušeným uživatelům. Pro zkušené uživatele je určen i **Host File Editor**, v němž lze měnit adresu serverů s aktualizačními soubory.
- **TrackSweep**: jde o nástroj určený k rychlému vyčištění dočasné paměti webového prohlížeče či prohlížečů, dále cookies, historie navštívených stránek, prostě všech informací, které by cokoli vypovídaly o vaší nedávné aktivitě na internetu. Podporovány jsou všechny tři nejrozšířenější prohlížeče. Stačí jen u každé položky zaškrtnout, že ji chcete vymazat, a pak kliknout na **Clean**.
- **Settings**: položka nastavení se dále dělí na pět záložek. Obecně se jedná o nastavení pro pokročilejší uživatele. Za pozornost stojí ve druhé záložce - **Scanning** - položka **Skip files larger than**, kde je možné zadat, jak velké soubory již nebudou prohledávány. Vhodné je to zejména pro případ, kdy na počítači máte například datově objemnější počítačové hry či filmy.

Kontrola počítače

Nejčastěji používanou funkcí programu je kontrola počítače na vyžádání, při níž jsou hledány potenciálně i reálně nebezpečné objekty. Pro většinu uživatelů je to vhodnější varianta než pravidelné automatické hledání, jež se může spustit ve chvíli, kdy se nám to zrovna vůbec nehodí.
Kontrolu počítače spustíte z hlavního okna tlačítkem **Scan Now**, které nabídne tři možnosti kontroly.

Smart Scan: toto je doporučená volba. Prohledá důležité části operačního systému včetně systémových registrů, místa, kde se obvykle škodlivé aplikace ukrývají. Chytré skenování je doporučenou volbou pro většinu uživatelů. Vlastnosti této volby lze měnit v nastavení programu.
Full Scan: prohledá celý systém, všechny disky a adresáře. Je to sice důkladné, avšak i velmi časově náročné skenování. Doporučujeme jen při podezření na zvláště otravné zamoření adwarem a spywarem.
Custom Scan: skenování s vlastním nastavením, jehož parametry lze blíže specifikovat kliknutím na tlačítko **Configure**.

Doporučujeme ponechat první volbu (**Smart Scan**), kliknout vpravo dole na **Scan**. Tím započne samotná kontrola. Tu lze v případě potřeby přerušit tlačítkem **Stop Scan**.
Po dokončení prohledávání se zobrazí seznam výsledků rozdělený do dvou kategorií, a to na objekty samy o sobě kritické na záložce **Critical Objects** a pak na ty obsahující soukromé informace, většinou se jedná o cookies podezřelé ze shromažďování dat o uživateli, ty jsou v záložce **Privacy Objects**. Závažnost každého rizika se určuje pomoci TAI indexu, kde 0 indikuje nulové ohrožení, 10 pak nejvyšší.

Jak vidíte, v tomto případě byl nalezen jeden případ malwaru. Není se ovšem třeba lekat, lepší je nejdříve se podívat na podrobnosti. Kliknutím na symbol plus u položky se ukáží podrobnosti, pro lepší přehlednost lze jednotlivé sloupce roztáhnout. Zde bylo jako možné ohrožení označeno nastavení domovské stránky v prohlížeči Opera na *www.seznam.cz*. Pravdou je, že škodlivé programy často samovolně nastaví domácí stránku prohlížeče, nicméně ne vždy je to hrozba. Tomu odpovídá i nízké hodnocení TAI = 3. V tomto případě tedy lze označit hrozbu zaškrtnutím čtverečku nalevo od ní a kliknout na **Add to Ignore**, čímž už na ni nebude v budoucnu upozorňováno.

Pokud by však byly nalezeny nebezpečné objekty s vyšším indexem TAI, popřípadě takové, u nichž si nevíte rady, je vhodnější je označit a odstranit pomocí **Remove**, popřípadě alespoň

přesunout do karantény. Jestliže se bojíte, že by vámi prováděné změny mohly poškodit operační systém, lze vytvořit i bod obnovení Windows.
Proces hledání ukončíte tlačítkem **Finish**.

Ad-Watch

Kromě vyžádaného prohledávání počítače disponuje Ad-Aware i na pozadí běžící součástí Ad-Watch. Je spustitelná z prostředí hlavního programu, ale i samostatně pomocí odkazu, který se po instalaci vytvořil na ploše Windows.
Ad Watch trvale sleduje změny v registrech systému, spuštěné procesy, probíhající internetový provoz, čistí dočasnou paměť webových prohlížečů a cookies, což jsou soubory, které mohou používat škodlivé weby a programy ke sledování dění na počítači. Zde je nutné zdůraznit, že ne vždy je žádoucí mít Ad-Watch spuštěn, protože spotřebovává zdroje počítače, i když nijak významně. Také někdy může dojít i k odstranění i těch cookies, které byste v počítači raději ponechali. Nicméně to vše lze podrobně nastavit ve vlastnostech Ad-Watch, jež jsou k dispozici po kliknutí na ikonu aplikace, která se zobrazí v pravém dolním rohu nástrojové lišty.