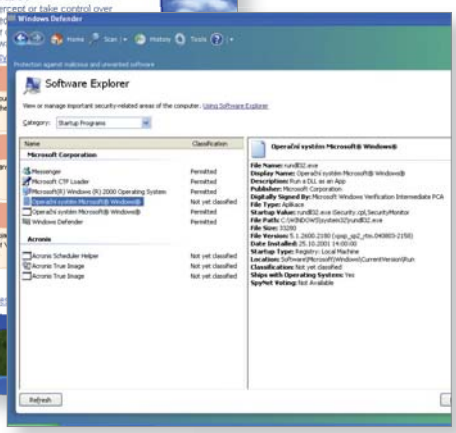
# Windows Defender systém neubrání

Všichni ho znají, všichni ho mají, ale nikdo ho nebere vážně. Je **WINDOWS DEFENDER** vážně takový outsider, nebo se najde alespoň jeden důvod, proč se mu nesmát?

PETR KRATOCHVÍL

Již v roce 2004 Microsoft pochopil, že nechat Windows XP nezabezpečená před malwarem je nebezpečný risk, a rozhodl se jednat. O tom, že bylo „za pět minut dvanáct“, svědčil i fakt, že nevyvinul vlastní produkt, ale na konci roku 2004 koupil společnost GIANT Company Software. Ta totiž „stála“ nejen za známými programy GIANT Spam Inspector a GIANT Popup Inspector, ale především za produktem, který Microsoft potřeboval – GIANT AntiSpyware. V roce 2005 tak mohl Bill Gates světu představit další krok k bezpečnějším Windows – Microsoft AntiSpyware. O rok později byl program přejmenován na Windows Defender, aby zdůraznil „ochranu Windows nejen před spywarem“. Pojďme se podívat, jak se mu to daří...


**Náhradník:** Ultimate Defender se spouští při startu Windows a nahrazuje Windows Defender.




**Bezzubý:** Sekce Startup Programs v Software Exploreru zařadila škůdce mezi produkty Microsoftu...

## Klapka, akce, jedeme...

Ačkoliv toho Windows Defender dokáže více, jeho primárním úkolem je bojovat proti malwaru. Podívali jsme se tedy zblízka na jeho „akční schopnosti“. Prvním zarážejícím faktem bylo, že při nedávném testu on-line skenerů (a naší „zavirovávací“ návštěvě webů) program téměř neprotestoval. Na potenciální riziko nás upozornil pouze jednou a téměř okamžitě byl odstaven malwarem.

Vyzkoušeli jsme tedy, jak jsou na tom jeho dezinfekční schopnosti. Pomocí zálohovacího programu jsme uvedli počítač do stejného stavu, v jakém se k němu dostaly i on-line skenery. Po updatu definic jsme spustili rychlý sken. Pouhé tři nalezené chyby nás přesvědčily o tom, že „máme problém“. Skutečnost však byla mnohem horší...

## Pomáhat a chránit…

I když program nalezl pouhé tři malwary, alespoň se tvářil, že si s nimi poradil. Po chvilce se však na obrazovce objevilo okno s informací, že některé programy (pravděpodobně byly myšleny i viry) běží a že máme vše vypnout (i browser) a kliknout na OK. Jelikož jediným spuštěným programem byl Windows Defender, klikli jsme na OK rovnou. Jaké však bylo naše překvapení, když se po restartu objevil znovu. Navíc se na nás z lišty „systray“ (tam, kde je standardně Windows Defender) vesele zubil náš „nový ochránce“ – Ultimate Defender. To nás neodradilo a rozhodli jsme se pro druhé kolo: důkladný „sken“ systému. Tentokrát bylo nalezeno osm vetřelců a opět se opakovala komedie s „úspěšným odstraněním

## SHRNUTÍ

V naší zkoušce propadl Windows Defender na celé čáře. Je sice možné, že by proti jiným škůdcům uspěl lépe, ani tak ale o pocitu bezpečí nemůže být ani řeči…

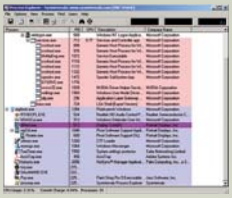
Z mála pozitiv stojí za zmínku snad jen přehledné zobrazení důležitých základních informací a naděje, že u menších problémů může pomoci (pravděpodobně ve spolupráci s dalšími programy). Na první pohled by se tedy mohlo zdát, že jeho odstranění (a nahrazení schopnějším programem) je dalším logickým krokem k bezpečnějším Windows. Náš názor je překvapivě opačný – Windows Defender se s ostatními bezpečnostními programy snáší dobře, a tak v tomto případě není důvod, proč se bránit dvojité kontrole. Navíc může v počítači sloužit i jako „návnada“. Pokud ze systému zmizí, pak víte, že máte opravdu problém…

## NÁHRADNÍCI

Rozhodnete-li se poslat Windows Defender do věčných lovišť, měli byste se poohlédnout po kvalitnějších náhradách. To kupodivu není nijak velký problém. V každé kategorii najdete celou řadu náhradníků, kteří disponují lepšími schopnostmi než Windows Defender. My vám doporučíme staré známé, kteří své kvality již několikrát prokázali…

### KONTROLA PROCESŮ

**Náhradník:** Process Explorer
**INFO: http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx**
Je to paradox, ale o třídu lepší produkt nabízí zdarma i sám Microsoft. Process Explorer (původně z dílen Sysinternals) dokáže vše, o čem mohou uživatelé Windows Defeneru jen tajně snít. Na první pohled vlastní gól Microsoftu…

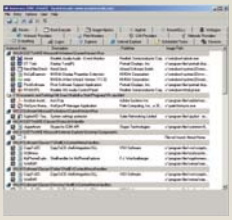


### OCHRANA SYSTÉMOVÝCH NASTAVENÍ

**Náhradník:** Spybot
**INFO: www.safer-networking.org**
Programů nabízejících ochranu systémových nastavení Windows je celá řada. Jako nejdůvěryhodnější se nám jeví několikrát zmiňovaný Spybot, respektive jeho součást Tea Helper.

### DETEKCE PROCESŮ SPOUŠTĚNÝCH PŘI STARTU

**Náhradník:** Autoruns
**INFO: http://technet.microsoft.com/cs-cz/sysinternals/bb963902(en-us).aspx**
Ve srovnání s aplikací Autoruns (také původně produkt firmy Sysinternals) působí nabídka Windows Defenderu jako Škoda 120 vedle Audi A8. Ve chvíli, kdy zjistíte, že je program k dispozici zdarma na webu Microsoftu, neexistuje důvod, proč dále váhat. Že by další vlastní gól?



### ODSTRANĚNÍ MALWARU

**Náhradník:** AVG Chip Edition 8
**INFO: www.chip.cz**
Pokud vám nebude stačit nový bezpečnostní balíček AVG Chip Edition 8, naprosté většiny škůdců se zbavíte i trojkombinací „on-line skener + The Avenger + Gmer“.

škůdců“ – tentokrát dokonce bez upozornění, „že se něco nepovedlo“. Alespoň nás ale nepřekvapilo, že po restartu bylo vše při starém, včetně našeho věrného ochránce – Ultimate Defenderu. Pokud bychom tedy měli uzavřít kapitolu „Ochrana a odvirování počítače“, bylo by skóre pro Windows Defender hodně nepříjemné.

## Další pomocník

Druhou silnou stránkou Windows Defenderu byl měl být monitorovací program „Software Explorer“ (SE). Uživatelé zvyklí na asketického Správce úloh určitě zajásají, protože ve srovnání s ním je SE mimořádně sdílný. Kromě pojmenování procesů a roztřídění podle „výrobce“ dokáže prozradit i celou řadu dalších zajímavých informací. V boji proti virům může pomoci například datum instalace, cesta k souboru nebo údaj o automatickém spouštění. Jenže je tu jedno velké ALE. Ty samé informace (plus desítky dalších) najdete i v bezplatném Process Exploreru, který nabízí sám Microsoft. Jediným bodem ve prospěch SE je jeho přehlednost – po kliknutí na proces hned vidíte základní informace důležité pro jeho základní identifikaci. Process Explorer nabídne informací téměř o řád více, ale musíte se k nim „proklikat“. I když zapomeneme na obrovské množství informací, kterými nás může tento program doslova zavalit, nad SE vítězí především proto, že nabízí tři účinné zbraně proti některému malwaru: „pozastavení“ procesu, on-line identifikaci procesu a zjištění vazeb mezi procesy.

## Na startu

Další částí Windows Defenderu (respektive Software Exploreru) je zobrazování a řízení programů spouštěných při startu Windows. V sekci „Startup programs“ byste měli najít tento seznam roztříděný podle výrobců. Je navíc doplněn tlačítky Disable a Remove, která mají spouštění položky zablokovat, případně ji z registrů odstranit. Na první pohled opět jen slova chvály – přehledné zobrazení jednotlivých položek se všemi důležitými údaji, v praxi ale opět propadák. Na našem testovacím počítači jsme našli dvě „podezřelé položky“ (později se ukázalo, že opravdu patří malwaru), které jsme se pokusili zablokovat. Program znovu nahlásil „splnění úkolu“ – a po restartu byly ony podezřelé položky opět na svém místě. Stejný výsledek měl i pokus o odstranění.

## Do počtu

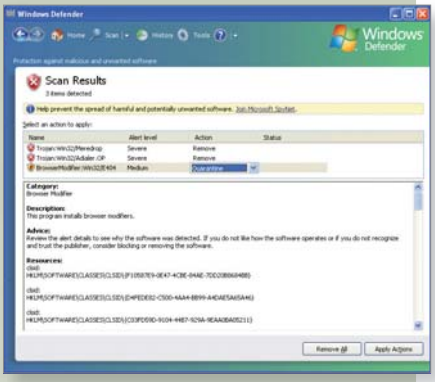
Další dva doplňky jsou ve Windows Defenderu jen „do počtu“. Sekce „Network connected programs“ patří spíše do firewallu (v tom standardním ve Windows XP nepřekvapivě chybí).

Sekci Winsock Service providers zase ocení jen zkušenější uživatelé, znalí rozhraní Winsock (a TCP/IP). Většina běžných uživatelů nad ní bude jen nechápavě kroutit hlavou...

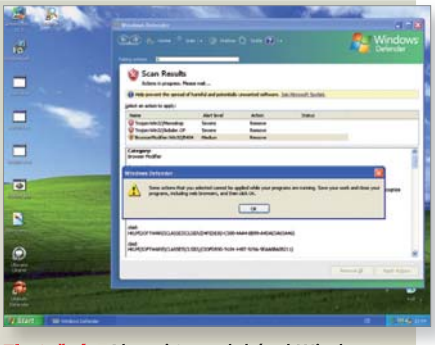
Pokud tedy shrneme schopnosti a možnosti Windows Defenderu, vyjde nám poněkud nelichotivý obrázek, který nezachrání ani uživatelská přívětivost programu. Situace je pro Defender tím horší, uvědomíme-li si, že sám Microsoft nabízí zdarma o třídu lepší alternativní programy na svém webu...

PETR.KRATOCHVIL@CHIP.CZ

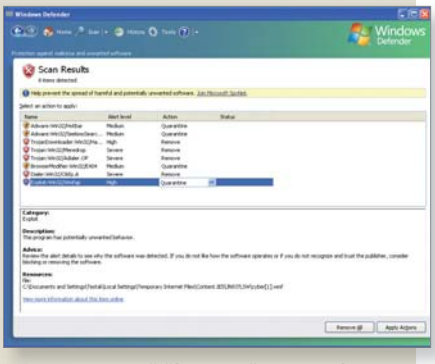
## WINDOWS DEFENDER V AKCI



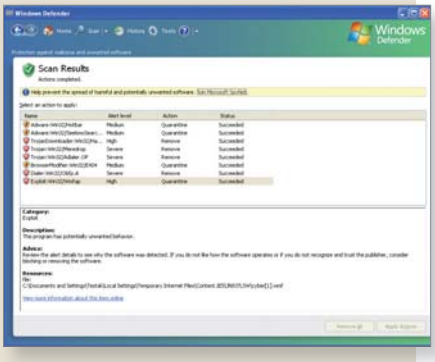
**Ubohé:** První rychlá kontrola našla jen tři škůdce.



**Zbytečné:** Ale ani ty nedokázal Windows Defender odstranit.



**Lepší:** Podrobnější sken měl na první pohled lepší výsledky.



**Lhář:** Navzdory svému tvrzení škůdci v počítači zůstali...

## INFO

### Podezřelá neschopnost

Ať už si o výtvorech z Redmondu myslíte cokoliv, nelze jim upřít snahu o zlepšení, která je ve finále oceněna vítězstvím. Proč tomu tak u Windows Defenderu není?

Celou řadu uživatelů po chvíli pozorování zoufalého tápání Windows Defenderu určitě napadne, jak je možné, že Microsoft není schopen nabídnout lepší produkt. Ať už si o jeho „tržních podílech“ myslíte cokoliv, nelze mu upřít celou řadu kvalitních produktů. Proč se tedy za čtyři roky (kdy už problém bezpečnosti pálil Microsoft opravdu palčivě) neobjevil žádný schopný program?
Je opravdu Microsoft v oblasti bezpečnosti tak neschopný, jak by naznačovala úvodní blamáž s programem Onecare:

- **www.betanews.com/article/OneCare_Deletes_Users_Outlook_Files/1173474996**;
- **www.av-comparatives.org/seiten/ergebnisse_2007_02.php**.

Nebo je nutné hledat jiné příčiny tohoto stavu? Kdyby Microsoft vylepšil Windows Defender na přijatelnou úroveň, jak by se zachovaly firmy produkující bezpečnostní software? Neopakovala by se situace jako u Media Playeru? Co si o tom myslíte vy? Napište nám svůj názor na adresu **redakce@chip.cz**.