# Ostré zbraně proti malwaru

V téměř každém Chipu vás informujeme o nových virech, trojských koních nebo jiném zákeřném malwaru. Je proto nejvyšší čas tyto poněkud depresivní zprávy vylepšit novinkami z druhé strany barikády. *Petr Kratochvíl, petr.kratochvil@chip.cz*

## V tomto článku najdete



Nové trojské koně, malware na klíč, anonymní proxy za pár dolarů – to vše hraje do karet temné straně internetu. A jaké jsou zbraně milionů obyčejných surfařů? Naprostá většina z nich používá pouze standardní výbavu (Windows Defender a firewall), která ve spojení s Firefoxem pro běžné surfování stačí. Jaké možnosti ale mají náročnější uživatelé? Co doporučit těm, kteří chtějí počítač používat i k internetovému bankovnictví nebo bezpečněji poznávat taje internetu?

### Volba nejnáročnějších

Pokud pravidelně surfujete v temnějších částech internetu, máte výkonný stroj a na monitoru nalepené heslo „Můj počítač – můj hrad“, je pro vás ideální volbou komplexní bezpečnostní balík. V Chipu č. 1/2008 jsme jich pro vás několik otestovali a i na základě tohoto testu lze doporučit dva: Norton Internet Security 2008 a (s důrazem na antiphishingovou ochranu) Kaspersky Internet Security 7. Vaši pozornost si zaslouží především prvně jmenovaný, a to díky nejlepším výsledkům v boji proti malwaru. Je vidět, že Symantec na svém produktu opravdu zapracoval – zatímco předchozí verze byla kvůli vysokým systémovým nárokům téměř nepoužitelná, verze 2008 má naše plné doporučení.

Ať už ale zvolíte kterýkoliv z dostupných „balíků“, počítejte s vyššími nároky na hardware – to je cena za komplexní ochranu. Naopak výhodou je sjednocené a integrované ovládání, což znamená, že všechny části obranného systému PC ovládáte podobnými tlačítky z jednoho místa. To vzhledem k nepraktickému rozhraní některých bezplatných nástrojů

### Na DVD tentokrát ne...

Bývá pravidlem, že nejdůležitější programy zmiňované v článku vám nabídneme na přiloženém DVD. V tomto případě je tam ale nenajdete, protože výrobní termíny jakéhokoliv časopisu nemohou soupeřit s rychlostí vývoje v oblasti bezpečnosti. A zatímco u programu pro úpravu obrázků je rozdíl mezi verzí 2.12 a 2.13 obvykle minimální, u programu pro detekci malwaru to může být otázka „existenční“. V případě zájmu vám doporučujeme stáhnout si příslušný program přímo z webu autorů...

(viz dále) určitě není k zahození. Další „nepříjemností“, se kterou je nutné při volbě komplexní bezpečnostní soupravy počítat, je potenciální zranitelnost. Pokud se totiž v programu objeví chyba (to, že nejde o výjimečnou událost, vám potvrdí i web Secunia; **www.secunia.com**), je ohrožen celý počítač. I přes výše uvedené výhrady lze obecně říci, že jde o bezpečnější řešení zabezpečení počítače.

## Cena: Zdarma

Druhou variantou, oblíbenou především kvůli „ceně“, jsou freewarové nástroje. Najít zde komplexní ochranu je nemožné, zbývá tudíž vytvoření bariéry proti malwaru z jednotlivých nástrojů. Firewall, antivir, antimalwarový nástroj, „hlídač“ systému – ve všech těchto oblastech lze sehnat kvalitní nástroje, které jsou k dispozici zdarma. Dřív než se ale začnete rozhlížet po internetu, je nutné připojit varování: při výběru programu je důležitá maximální obezřetnost – vždyť vybíráte program, který vám bude hlídat počítač. Stáhnout si z webu „Supersecurity antivir“, který vám byl doporučen bannerem na pornowebu, je pokus o počítačovou sebevraždu. V lepším případě jde o amatérský pokus na poli programování, v tom horším o „falešný nástroj“, který místo boje s malwarem ho do systému sám nahrává. Ne každý program má také rozumné systémové nároky a přívětivé ovládání. Výběr bezplatného strážce zkrátka není snadnou záležitostí. Cílem tohoto článku je vám to trochu usnadnit…

## Staří známí

V počátcích boje proti spywaru patřily mezi špičku – na svém počítači je měla většina zkušenějších uživatelů. Jenže s přibývajícími léty jejich kvality klesaly a nakonec je konkurence převálcovala. Nyní jsou zpět i s novými funkcemi…

### SPYBOT-SEARCH&DESTROY

**Zaměření:** detekce malwaru
**Web:** www.safer-networking.org

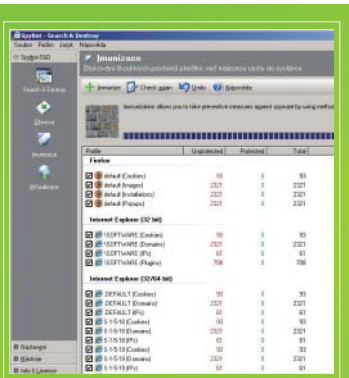
**Proč instalovat:** Už několik let nás pánové z firmy Safer-Networking Limited zásobují novými verzemi praktického nástroje proti malwaru. Po delší odmlce byla loni na podzim představena nová verze 1.5, která konečně vrátila program zpět mezi elitu. Nyní je k dispozici verze 1.5.2, ve které jsou vyřešeny i drobné problémy „nové“ verze. Jako bonus dostanete s programem výborný nástroj TeaTimer, který dokáže ochránit nastavení systému a na potenciální změny vás upozorní. Když ke všem uváděným výhodám přidáte ještě ovládání v českém jazyce, je logické, že Spybot lze více než doporučit!

**Co je nového:**

- Vylepšené detekční schopnosti: Jednou z velkých slabin předchozí verze byla nekvalitní detekce. Schopnosti nové verze jsou už opět na úrovni profesionálních nástrojů.
- Imunizace pro Firefox a Operu: Nyní už jsou seznamy nebezpečných webů a signatury škůdců k dispozici pro tři nejrozšířenější browsery. Proti nejznámějším internetovým hrozbám by tak měli být „imunní“ i začátečníci.
- Automatická kontrola „stahovací“ složky: Ať už ukládáte data stažená z internetu kamkoliv, program si potenciální škůdce ohlídá.
- Varování před ztrátou administrátorských práv ve Vistě: S rostoucím počtem uživatelů Visty roste i zájem hackerů o tento systém. Řešením problému může být i Spybot.
- Obnovená kompatibilita pro Windows 95 a 98: Máte doma starší počítač pro občasnou návštěvu webu a stažení pošty? Spybot vám ho ochrání…

**Slabiny:** O něco horší je schopnost odstraňovat nalezené škůdce. Při „nepovedeném“ odstranění malwaru lze doporučit použití alternativního nástroje (například jednoúčelové utility od profesionálního výrobce). Za ideální také nelze označit fungování ve Windows Vista…

**Další zajímavosti:** Na webu autorů Spybotu jsou k dispozici i další nástroje



**SPYBOT:** Verze 1.5 konečně vrátila program zpět mezi elitu.


**AD-AWARE:** Nyní si zdarma můžete stáhnout verzi Plus...

usnadňující detekci malwaru. Run Analyzer umí měnit a kontrolovat programy spouštějící se při startu počítače, RegAnalyzer slouží ke kontrole a úpravě registrů. Profesionálové ocení FileAnalyzer, umožňující zkoumání jednotlivých souborů (mimo jiné i jejich kódu).

### AD-AWARE 2007

**Zaměření:** detekce malwaru
**Web:** www.lavasoftusa.com

**Proč instalovat:** Jeden z nejoblíbenějších detekčních nástrojů. Svého času populární především díky výborné detekci dialerů. Programu ale příliš neprospěla poněkud kontroverzní politika upgradů. Většina uživatelů obvykle nezaregistrovala, že je k dispozici nová verze, a po několikátém neúspěšném stažení „aktualizací“ (v horším případě dokonce došlo k pádu systému) program odinstalovala. Tento „problém“ se týkal i přechodu z verze Ad-Aware SE na verzi 2007. To je ale škoda, protože nová verze nabídla celou řadu revolučních vylepšení, která pomáhají zabezpečit počítač.

**Co je nového:**

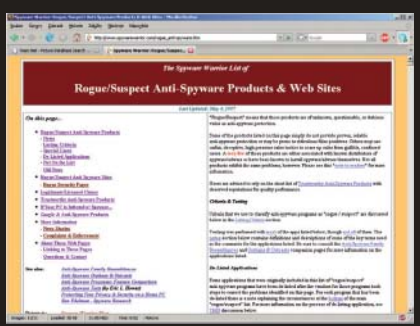
- Ad-watch: Celá řada hlídačů, kteří monitorují vaši činnost a pomáhají zabránit nežádoucím změnám v systému.
- Výkonnější jádro: Ve srovnání s předchozími verzemi jednoznačně schopnější…
- Zásuvné moduly: Nyní je možné rozšířit schopnosti programu pomocí zásuvných modulů.

**Slabiny:** Pouze detekce malwaru. Realtimový štít je k dispozici až ve „vyšších“, placených verzích. K dispozici je pouze neoficiální čeština, s jejíž instalací mají méně zkušení uživatelé problémy. Ve srovnání s předchozí verzí (SE) poněkud vyšší hardwarové náro- →

## Zdaleka se vyhněte...

Kromě programů s problematickým chováním nebo ovládáním existuje ještě jedna skupina nástrojů, které je lepší se zdaleka vyhnout. Jde o tzv. „false/rogue antispyware" programy, které místo boje se zákeřnými škůdci je naopak do systému nahrávají nebo jinak ohrožují váš počítač. Mezi ty nejnebezpečnější patří:

- AdwarePunisher
- AntiSpyware Soldier
- AntiSpyZone
- ExpertAntiVirus
- MyNetProtector
- Privacy Champion
- PSGuard
- SlimShield
- SpyBan
- Spy-Shield
- SpywareCleaner
- Spyware Soft Stop
- Winhound Spyware Remover
- ZoneProtect AntiSpyware




**NENECHTE SE NAPÁLIT:** **Aktualizovaný seznam podezřelých programů nabízí web www.spywarewarrior.com.**

Pokud patříte mezi důvěřivější jedince a bojíte se, že nedokážete odolat lákavé nabídce 80procentní slevy na „nový" úžasný nástroj proti malwaru, přidejte si do záložek stránku SpywareWarrior (**www.spywarewarrior.com/rogue_anti-spyware.htm**). Zde totiž najdete poměrně často aktualizovaný seznam podezřelých programů, který vám může ušetřit čas i peníze...

ky. Snaha o nalákání uživatelů na placené verze (Plus a Pro) vedla k mírnému znevýhodnění bezplatné verze (výkon, funkce).

**Další zajímavosti:** Výkonnější a schopnější verze Plus stojí jen 27 USD, což při současném kurzu dolaru není moc. V českých obchodech (například na Sw.cz) ji najdete za necelých 600 Kč, takže nákup už není jen otázkou mezinárodní platební karty…

### HijackThis

**Zaměření:** získání informací o systému

**Web:** http://www.spywareinfo.com/~merijn/programs.php

**Proč instalovat:** Nejpoužívanější program pro vytváření „logů". Pokud budete potřebovat poradit s odstraněním malwaru, na většině diskusních fór (např. spyware.cz) vás požádají právě o log programu HijackThis. Program dokáže zaznamenat spuštěné procesy v paměti, nejdůležitější položky v registrech nebo nainstalované ActiveX programy. Navíc lze některé „problematické" položky přímo zablokovat…

**Co je nového:**

- Detekce: Jediná a nejdůležitější schopnost programu – detekce skrýší zákeřných záškodníků byla opět vylepšena…

**Slabiny:** Uživatelské rozhraní není zrovna přívětivé a efektivní využití programu vyžaduje přiměřené počítačové znalosti. Pokud však program budete využívat pouze na vytváření „logů", jsou předchozí výtky zbytečné…

**Další zajímavosti:** Jinou alternativou zmiňovaného programu je StartupList. Ten dokáže vypsat všechny automaticky spouštěné programy ve vašem systému. Je asi zbytečné přidávat poznámku, že je podstatně lepší než MSconfig…

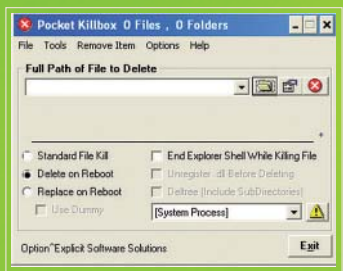
### KillBox

**Zaměření:** likvidace nežádoucích procesů

**Web:** http://killbox.net/

**Proč instalovat:** Výborný nástroj na mazání „škůdců" ze systému. Kromě obyčejného mazání dokáže zadaný soubor odstranit při restartu, soubor typu „dll" před smazáním odregistrovat, zvládne dokonce i ukončení shellu Windows a následné smazání záškodníka.

**Slabiny:** Použití programu vyžaduje dobré znalosti systému. Chybí jakákoliv možnost nápovědy nebo opravy „špatných rozhodnutí". Nezkušený uživatel může pomocí tohoto programu během několika minut nenávratně poškodit systém.




**ŠIKULA:** **Kromě obyčejného mazání dokáže zadaný soubor odstranit při restartu.**

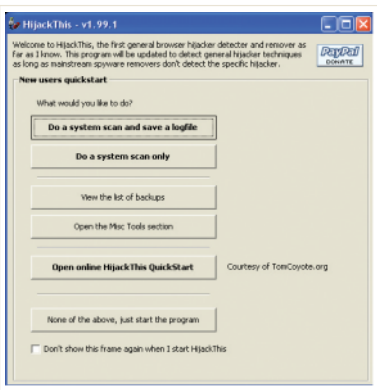
**Další zajímavosti:** Domácí stránka autorů killboxu je v nepravidelných intervalech „mimo provoz". Před jeho použitím tak doporučuji spíše navštívit server Viry.cz, kde na adrese **http://www.viry.cz/forum/viewtopic.php?t=43207** najdete nejen stručný návod k použití, ale i odkaz na alternativní web pro stažení programu.

### Spy Sweeper

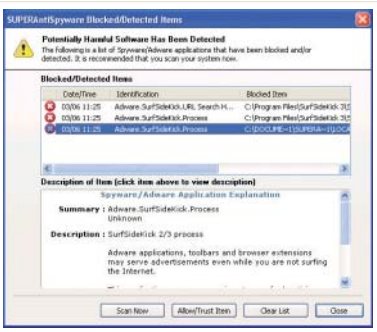
**Zaměření:** detekce malwaru

**Web:** www.webroot.com

**Proč instalovat:** Jeden z dlouhodobě nejlepších nástrojů na detekci nežádoucích „návštěv" v počítači. V celé řadě testů poráží konkurenci (Ad-Aware a spol.) rozdílem několika tříd, což z něj ve spojení s nadprůměrnou rychlostí dělá ideální nástroj na rychlou očistu napadených počítačů.




**HIJACKTHIS:** **Nejpoužívanější program pro vytváření „logů".**




**SUPERANTISPYWARE:** „Realtimovou" ochranu najdete až u placené „profi" verze.

**Co je nového:**

- Pět štítů: Realtimová ochrana pro různé oblasti internetového nebezpečí.
- Lepší přehlednost rozhraní: Na první pohled vidíte, jaké štíty máte zapnuty…
- Snadnější ovládání: Pohodlnější a srozumitelnější detekce a odstranění malwaru i pro méně zkušené uživatele.

**Slabiny:** Zdarma k dispozici pouze 30denní verze, pro její aktivaci je navíc nutná návštěva webu autorů. Program nespolupracuje s alternativními browsery a zabere nadprůměrný objem v paměti…

## Novinky

Na webu je najdete už několik let. Začínaly jako nepovedené napodobeniny známých nástrojů a zpočátku budily jen smích. S přibývajícími roky vývoje však dospěly do stavu, kdy je lze bez problémů doporučit jako alternativu k osvědčeným nástrojům.

### SuperAntispyware

**Zaměření:** detekce a likvidace malwaru
**Web:** www.superantispyware.com
**Proč instalovat:** Z hlediska detekce malwaru současná špička. V oblasti bezplatných nástrojů navíc nabízí poměrně unikátní schopnosti při odstraňování nalezených škůdců.
**Slabiny:** Bezplatná verze nabízí pouze „prohledání" systému. „Realtimovou" ochranu najdete až u placené „profi" verze. Neexistuje oficiální česká verze.
**Další zajímavosti:** Díky výhodnému kurzu dolaru a necelým 30 USD za verzi Professional je tento program horkým kandidátem na dokonalého strážce domácího počítače.

### a-squared Anti-Malware

**Zaměření:** detekce a likvidace malwaru
**Web:** www.emsisoft.com/en/
**Proč instalovat:** Zajímavý nováček na poli boje proti červům, trojským koním a spywaru. Jde o dobrou volbu v případě doplňkového nástroje ke klasickému antiviru. Základní bezplatná verze nemá „realtimovou" ochranu, tudíž nehrozí ani konflikty se štítem antiviru.
**Slabiny:** Podobné jako u předchozího produktu: bezplatná verze nabízí pouze „sken" počítače a „nepřetržitou" ochranu najdete až u placené „profi" verze. Ani zde neexistuje oficiální česká verze.
**Další zajímavosti:** Tento program lze v „profi" verzi zakoupit na webu Sw.cz za necelých 850 Kč. *Petr Kratochvíl*

## Rozhodněte se sami...

Existuje celá řada programů, které sice dokáží proti malwaru úspěšně bojovat, přesto obsahují drobné chyby či nedodělky a nelze je jednoznačně doporučit. Zde je tip na několik z nich.

**Spyware Doctor**
Poměrně populární nástroj proti malwaru má také velkou skupinu kritiků. Ti mu vyčítají například fakt, že jeho rezidentní štít obsahuje chybu, která znemožňuje korektní fungování některých antivirů. Zatím nevyřešená je kolize s antivirem firmy Kaspersky, loňská „populární bitva" s antivirem NOD32 (**www.lupa.cz/zpravicky/spyware-doctor-bojuje-s-nod32-a-bezpecnost-trpi/**) zůstala bez vítěze a Avast! problém vyřešil upgradem...

Když k těmto problémům přidáte poněkud přehnané systémové nároky a poměrně značné zpomalení startu systému, je doporučení programu poněkud diskutabilní...
**Info: www.pctools.com/spyware-doctor**

**Spyware Terminátor**
Český produkt, který na první pohled potěší většinu uživatelů. Přívětivé ovládání, bez milionu zbytečných funkcí a s integrovaným rezidentním štítem. Na druhé straně ale poněkud rozporuplné výsledky a celá řada nevyřešených problémů. Než se rozhodnete si ho pustit na počítač, doporučuji pročíst diskusní fórum na adrese (**http://forum.spywareterminator.com**).
**Info: www.spywareterminator.com**