Antispywarové programy by měly ochránit váš počítač před špiony i internetovou mafií. Náš test však ukázal, že žádný nástroj nesplňuje to, co slibuje. Přečtěte si vše o tomto skandálu. Chip vám prozradí, jaká ochrana je skutečně účinná.

Text: Valentin Pletzer, Vratislav Klega, vratislav.klega@vogelburda.cz

Antispyware

Testy antispyware produktů

Vetřelci ve vašem počítači jsou nebezpeční jako nikdy dříve. Hluboko v systému číhají, až zadáte heslo nebo číslo účtu nebo až otevřete soukromý dokument. Pečlivě zapisují každý pohyb myši, každé stisknutí klávesy. „Žádný problém," řeknete si. „Nainstaluji si antispyware a můj systém bude zase čistý a bezpečný." To ale bohužel není pravda. Problematika internetové bezpečnosti je velice široká a ani nejnovější, nej-dražší a nejlepší nástroj na ochranu vám nedokáže vždy pomoci.

ZKLAMÁNÍ

Nejistá obrana

Spolu s virovými experty jsme otestovali nejznámější antispywarové programy a zkontrolovali jsme, jak účinně dokáží ochránit váš počítač. Výsledek byl otřesný – žádný nástroj nedokáže zcela ochránit váš počítač před spywarem! Důvod, proč se objevují stále nové a promyšlenější špionážní programy, je jen jeden – za data od tisíců uživatelů internetu získá internetová mafie obrovské peníze.

Dříve hackeři vytvořili program, který se snadno nainstaloval, ale bylo také velice snadné ho najít. Dnešní programy jsou ukryté daleko lépe. Prostřednictvím různých technologií se schovají až do jádra systému, kde jsou pro bezpečnostní programy zcela neviditelné.

Pokud je již zhoubný software aktivovaný, máte štěstí, jedná-li se „jen" o adware. V 99 % případů postihuje jen Internet Explorer, protokoluje chování na internetu a zahlcuje počítač vyskakovacími okny. To je sice velice nepříjemné, ale není to tak nebezpečné jako druhá skupina – špionážní software. Ten vyhledává především hesla, čísla účtů a soukromé dokumenty. A zatímco přítomnost adwaru lze velice rychle odhalit, především díky vyskakovacím reklamním oknům, při napadení počítače spywarem neprojevuje systém žádné symptomy, a vy tedy vůbec netušíte, že někdo krade vaše důvěrné informace. Spyware odhalíte jedině díky pomalému připojení k internetu (stane se ještě pomalejším), nevysvětlitelným pádům aplikací a pádům operačního systému. Většina uživatelů však těmto symptomům nevěnuje zvláštní pozornost.

Záchranou „z nebes" se zdají nová Windows Vista. Lze totiž očekávat, že nová Windows budou oproti současné verzi daleko odolnější proti spywaru. Podle vzoru současných antivirů by mělo být vyhledání a odstranění spywaru stejně jednouché, jako je tomu dnes v případě virů. Náš test ukazuje, že v současnosti je to jen vysněné přání.

ROZPOZNÁNÍ

Hledání a čištění – opravdová katastrofa

Aby byl výsledek co nejvěrohodnější, budou všechny nové nástroje testovány ve virové laboratoři. Zde budou podrobeny tvrdému testu. Po dobu dvou týdnů prováděli spywaroví experti pečlivé testování všech účastníků našeho testu. Prvním tes-

CHIP ZÁVĚRY TESTU

Nákup antispywaru se skutečně nevyplatí. Žádný z testovaných programů nedokázal spolehlivě odstranit veškerý spyware. Nejlepší produkt, AntiSpyware od McAfee, sice rozpoznal 100 % aktivního spywaru, odstranil ovšem pouze 70 %, freewarový Spybot Search & Destroy pak dokonce pouze 45 %. Jediným řešením je tak kombinace více antispywarových nástrojů. Jen tak bude váš počítač dostatečně zajištěný. Lepší tedy bude, vsadíte-li na prevenci pomocí různých bezpečnostních balíků. Ty stojí samozřejmě daleko více peněz, v boji proti nebezpečné internetové mafii jsou však maximálně účinné.

NAJDETE NA CHIP DVD

- **Spybot Search & Destroy 1.4**
  freeware
  www.safer-networking.org
- **Ashampoo Anti-Spyware 1.4**
  trial
  www.ashampoo.com
- **ZoneAlarm Anti-Spyware 6.5**
  trial
  www.zonelabs.com
- **Windows Defender beta 2**
  freeware
  www.microsoft.cz
- **SpySweeper 4.5.9**
  trial
  www.webroot.com
- **Ad-Aware SE PE 1.06**
  freeware
  www.lavasoft.com

v testu tvrdosti

ROOTKIT SEM, ROOTKIT TAM

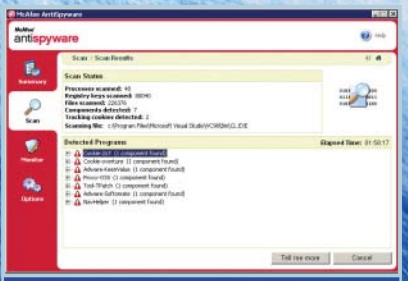
Neustále zde probíráme, zda program dokáže odhalit aktivní či neaktivní rootkit. Co to ale vlastně je? Zkráceně řečeno se jedná o program, který maskuje svoji přítomnost v systému, aby nebyl pokud možno vůbec odhalen.

V praxi narážíme na dva typy rootkitů, podle toho, jaký způsob maskování používají. Může to být buď modifikací cest, nebo modifikací struktur.

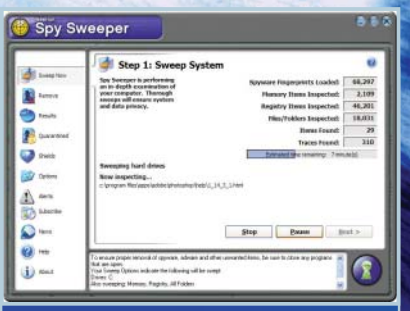
Při modifikaci cest dochází k zamaskování důležitých funkcí v systému rootkitem. Při volání běžné funkce (knihovny) dojde ve skutečnosti k zavolání škodlivého rootkitu. Ten sice poskytne stejná data, ale přitom vykonává i nekalou činnost.

Rootkity využívající modifikaci systémových struktur bývají zavrtané hluboko v systému. Mají takovou moc, že dokáží skrýt procesy před vybraným softwarem (antispywarem).

Pokud se o rootkitech chcete dozvědět více, doporučujeme navštívit server *www.rootkit.cz*, kde kromě informací naleznete také výborné diskusní fórum o této problematice.



McAfee AntiSpyware: **Ačkoliv program nabízí nejlepší rozpoznávací schopnosti a stal se vítězem našeho testování, kvůli extrémně dlouhému skenování nelze produkt pro praxi příliš doporučit.**



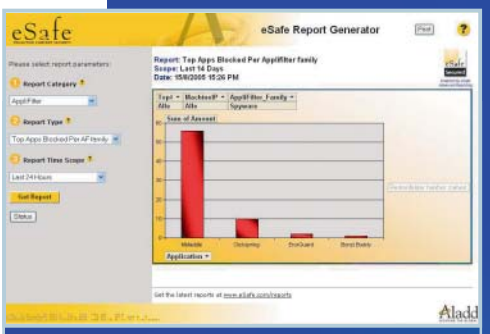
Webroot Spy Sweeper: **Rozpoznání aktivního spywaru proběhlo docela dobře, při vyhledávání aktivních rootkitů však program zcela pohořel.**

tem byl „on-demand“ test, ve kterém je spyware ještě neaktivní. Programy musely škodlivý software rozpoznat ještě předtím, než se stihne nainstalovat. Ani jeden z testovaných kandidátů neprošel tímto povinným testem s čistým štítem. Nejlépe si vedl McAfee AntiSpyware 2006. Dokázal však rozpoznat pouze 82 % spywaru – téměř 1/5 spywaru tedy projde sítí toho nejlepšího lovce zcela bez povšimnutí. Zbytek testovaných nástrojů dopadl ještě daleko hůř. Spybot Search & Destroy, AntiSpion od firmy Data Becker a ZoneAlarm skončily dokonce pod 10 %! Skutečná katastrofa. Přitom kdyby tato ochrana fungovala dokonale v reálném čase, byl by spyware odhalen už během stahování a nikdy by nemusel být aktivován.

O něco lépe dopadl „on-access“ test. Ten ukazuje, jak dobré jsou programy v hledání aktivního spywaru. Naši testeři používali k testu desítky nejrozšířenějších spywarových programů a desítky jiných škodlivých kódů. Na čele se i tentokrát drží McAfee. Jeho engine, který je známý jako výborný antivirus, našel jako jediný v testu všechny spywarové programy. Na konci testovaného pole skončily nástroje od firem ZoneLabs a Data Becker, které odchytily pouhých 55 % spywaru.

NOVÉ CESTY V BOJI PROTI SPYWARU

Aby se schopnosti vašeho antispywaru ještě více zlepšily, bude nutné ho naučit nové triky. Problémem bezpečnostních nástrojů je to, že lze jen těžko definovat hranici mezi tím, co je spyware, trojský kůň, případně červ. Rozdíly mezi těmito škůdci se stírají. Jen sotva narazíte na nový spyware, který je bez rootkitu. Nový spyware se zavrtá tak hluboko do systému, že navenek lze najít maximálně vrchol ledovce – trojského koně.



Proaktivní strategie: **Techniky jako eSafe od společnosti Aladdin mohou bojovat proti malwaru, který ještě nebyl objeven.**

Zcela jednoznačné rozlišení tedy není možné. Konvenční antispywarové skeny nemají žádnou šanci a výsledek našeho testování to jen potvrzuje. Firmy vyrábějící bezpečnostní software budou muset jít novou cestou, aby proti záludnému softwaru vymyslely účinnější ochranu.

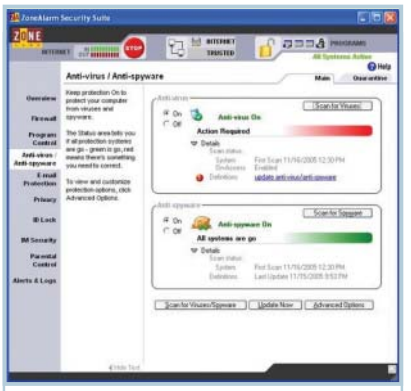
V oblasti bezpečnostního softwaru můžeme v současnosti pozorovat tři velké trendy:

Intruzní detekce: místo běžného skenování a hledání spywaru v systému bude systém podrobně monitorován. V případě, že v síti bude zjištěna podivná aktivita, bude alarmován administrátor.

Proaktivní technika: – místo hledání charakteristik malwaru v programech bude monitorována celá činnost programu. Neobvyklé nebo nežádoucí procesy budou automaticky ukončeny.

Malware Task Force: – doposud byli hackeři vždy o krok napřed před výrobci bezpečnostního softwaru. Nyní hledají viroví specialisté a programátoři účinný protijed.

Podvodník: **Drzost internetové mafie nezná mezí. Nabízený antispyware není ve skutečnosti nic jiného než obyčejný spyware.**



ZoneAlarm Anti-Spyware: **Jako jediný nabízí tento program také firewall. Ten je mimochodem velice dobrý.**

Bohužel ani uživatelé nástroje od firmy McAfee se nemohou cítit zcela bezpečně. Vysoké procento rozpoznaných škůdců ještě neznamená, že program dokáže odhalit vše. Prakticky stačí, když máte v počítači jednoho jediného špiona, a vaše data jsou v nebezpečí. Čištění také nepatří mezi jednoduché disciplíny. Program od firmy McAfee sice odstraní 70 % škodlivého kódu, ale jen polovinu záznamů v registrech, což je obzvláště málo, protože mnoho spywaru narušuje bezpečnost operačního systému právě přes registry. Program od firmy Webroot, který se na boj se spywarem přímo soustředí, je na tom o něco lépe. Odstraní 75 % souborů a 70 % záznamů z registrů. Poslední místa zaujímají SimonTools AntiSpyWare a AntiSpion, které odstraní 5, respektive 15 % spywaru.

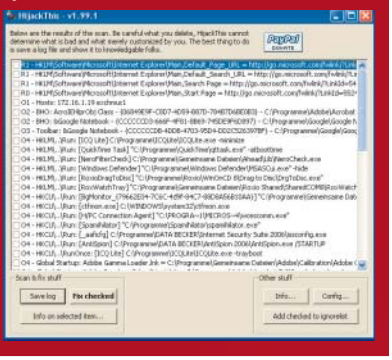
V královské disciplíně – odhalování rootkitů – se objevil ještě další extrém. Ashampoo a SimonTools na nás udělaly skutečně dojem – rozpoznaly 100 % neaktivních rootkitů, zatímco programy od Microsoftu, Data Beckeru a Lavasoftu nenašly ani jeden neaktivní rootkit! Ještě horší byla situace u aktivních rootkitů. Ty dostaly do kolen všechny programy z našeho testovaného pole. Ashampoo jich sice našel 78 %, i to je však bohužel málo.

Jedna pozitivní zpráva – plané poplachy se objevují velice zřídka. Některé programy klopýtají během skenu o AOL-Toolbar pro Internet Explorer – ptají se na další postup. Instalaci však neodepřel žádný.

JAK NAJÍT JEŠTĚ VÍCE SPYWARU

LOVEC PROFESIONÁL

Freewarový „HijackThis“ pomáhá při ručním vyhledávání spywaru. Program vám vypíše všechny možnosti, kde se může spyware skrývat. Nezřídka se ovšem stává, že program mezi spyware zařadí i regulérní software. Než se tedy pustíte do úklidu, je lepší si ověřit, zda se jedná o škůdce, nebo o běžný software. Nejjednodušší je, prozkoumáte-li fóra o virech nebo zadáte-li název souboru do Googlu. Pak už snadno zjistíte, zda mazat, či nikoli.



VÝKON

Spywarová ochrana žere čas a operační paměť

Bezpečnost stojí peníze – v podobě spotřebovaných zdrojů. To platí pro antispyware stejně jako pro firewall nebo antivirový štít. Antispyware ale vytváří ochranu ve dvou vrstvách – respektive se o to snaží. První vrstvu celého mechanismu tvoří štít. Ten běží na pozadí, skenuje v reálném čase otevírané soubory, kontroluje nová data a změny provedené v systému. To samozřejmě významným způsobem ukrádá ze zdrojů systému, což je možné si ověřit v Taskmanageru ve Windows, kde jsou vidi- →

telné všechny procesy, které má antispyware spuštěné. Ten ovšem nenabízí takové možnosti sledování zákulisí, jaké bychom si představovali, a proto jsme sáhli po programu „Process Explorer“ od firmy Sysinternals (*www.sysinternals.com*), který dokáže podrobně zobrazit obsazení paměti a další detaily.

Velice zajímavý je pohled do položky, která udává, kolik místa zabírá rozpoznávací software v paměti. Spy Sweeper od společnosti Webroot si zabere 83 MB operační paměti. V případě systému, který má jen 512 MB operační paměti, to znamená, že jen antispyware si zabere jednu šestinu paměti. Také SimonTools a Ashampoo Anti-Spyware spolknou nezanedbatelných 69 MB. Skutečně spokojeni jsme byli jen s nástroji Spybot Search & Destroy a Windows Defender od Microsoftu: 7, respektive 12 MB v operační paměti je velice příjemná hodnota.

JAK FUNGUJE INTERNETOVÁ MAFIE

Willie Sutton, známý bankovní lupič, dostal v roce 1952 dotaz, proč přepadal banky. Odpověděl: „Protože tam jsou peníze.“ Z téhož předpokladu vychází i kyberkriminalita. I na internetu se povalují miliardy. Stále více bankovních transakcí se provádí on-line. V tomto případě pochopitelně nikdo nečeká před bankou s nastartovaným motorem. Místo toho, aby lupiči nutili on-line obchodníky dávat ruce za hlavu a lehat si na zem, hackují servery a rozesílají phishingové maily.

Struktura internetové mafie je postavena velice podobně jako Cosa Nostra. Všechny akce řídí muži v pozadí, kteří ve většině případů sídlí ve státech východního bloku, takže „západoevropští“ úředníci jsou na ně krátcí. Odsud koordinují své hackerské skupiny a zde se také vyvíjí většina phishingových mailů či spywarů.

Na tato místa se dostávají nejen informace o vašich kontech, ale také kontakty, historie surfování, čísla platebních karet a prakticky vše, co do počítače zadáváte. Odsud míří do vašich schránek i nechvalně známé maily, oznamující, že vám někdo chce dát hromadu peněz, pokud pošlete na jeho účet drobný obnos. Doufáme, že mezi čtenáři Chipu už není nikdo, kdo by takovým zprávám věřil!

Druhá vrstva mechanismu odhaluje brzdy v systému. Při „on-demand“ testu, který ideálně probíhá každý den, je systém prohledáván na přítomnost spywaru, a to například během přestávky na oběd nebo před vypnutím počítače. Zde opět platí, že čím je test intenzivnější (lepší), tím více systémových zdrojů je spotřebováno.

Našemu vítězi testu, nástroji McAfee, trvalo skoro hodinu, než proběhl standardní test. Přitom optimalizaci prohledávání budete hledat marně. Detailní nastavení, které například dovolí vynechat vybrané adresáře či data, není bohužel k dispozici. U produktu společnosti McAfee chybí i volba pro rychlý test, který by zkontroloval jen systémové oblasti. Na druhou stranu – jiné programy sice mají i bohatší možnosti nastavení, přinášejí však mizerné výsledky.

FUNKCE

Záblesk naděje v oblasti podpory a informace o spywaru

Bezpečnostní nástroj by měl být velice jednoduše ovladatelný. Zrovna náš vítěz testu však dělá v této kategorii psí kusy. McAfee AntiSpyware působí jako nevlastní dítě balíku Security-suite. Engine a prostředí programu jsou stejné jako u antiviru. Při instalaci balíku se nainstaluje ikona do system tray, což je obvyklé, při poklepání na ikonu však paradoxně chybí možnost spustit antispyware. Ostatní součásti balíku odsud pochopitelně spouštět lze.

McAfee je naštěstí v tomto ohledu výjimkou. Všechny ostatní nástroje mají ovládání skutečně jednoduché. Kromě ovládání jsme se však zaměřili ještě na jednu část – na podporu ze strany výrobce. Hodnotili jsme e-mailovou podporu, hotline a podporu na webových stránkách. Pouze Zone Labs mírně propadá: firma totiž nabízí placenou hotline (1,5 eura za minutu). I zde však mají uživatelé bezplatnou alternativu – e-mail a informace o spywaru na stránkách výrobce.

Na druhou stranu musíme uznat, že nástroj Zone Labs je velice štědrý, co se týče výbavy. K antispywaru nabízí navíc firewall, který měl při našem posledním testování bezpečnostních suit nejlepší výsledek. Je to určitě lepší cesta než přídavné utility v podobě blokování vyskakovacích oken nebo skartovačky dat.

Na závěr ještě jeden důležitý detail. Mnoho uživatelů má sice nastavený admi-

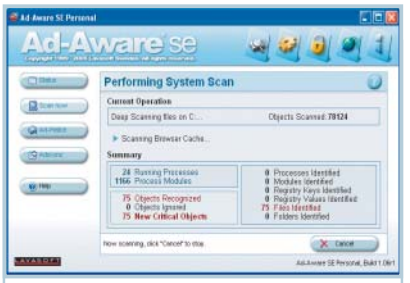
	1	2	3	4
Produkt	**AntiSpyware 2006**	**SimonTools AntiSpyWare**	**Spybot Search & Destroy**	**Ashampoo Anti-Spyware**
Výrobce	McAfee	S.A.D.	Safer Networking	Ashampoo
Cena	880 Kč	18 eur	freeware	30 eur
Internet	*http://cz.mcafee.com*	*www.s-a-d.de*	*www.safer-networking.org*	*www.ashampoo.com*
Celkové hodnocení	**65**	**59**	**59**	**58**
Rozpoznání (60 %)	69	58	39	57
Výkon (25 %)	49	47	89	60
Funkce (15 %)	78	82	87	59
Poměr cena/výkon	uspokojivý	uspokojivý	dobrý	dostatečný
Shrnutí	Uspokojivé rozpoznávání aktivního a neaktivního spywaru, avšak extrémně zdlouhavé testování.	Uspokojivé rozpoznávání; nedokonalý při odstraňování aktivního spywaru z registrů.	Velice špatný při rozpoznávání rootkitů, nedokonalé čištění.	Odstraňování dělá problémy, rozpoznávání aktivního spywaru výborné.
Rozpoznání				
Rozpoznání neaktivního spywaru (868 nástrah)	82%	63%	1%	27%
Rozpoznání aktivního spywaru	100%	95%	90%	95%
Odstranění aktivního spywaru (soubory)	70%	60%	45%	40%
Odstranění aktivního spywaru (registry)	50%	5%	25%	40%
Rozpoznání neaktivních rootkitů	89%	100%	11%	100%
Rozpoznání aktivních rootkitů	44%	55%	0%	78%
Plané poplachy během instalování toolbaru	žádný	žádný	žádný	žádný
Plané poplachy během skenování toolbaru	1	1	žádný	1
Počet škůdců v databázi (podle výrobce)	53 657	313 527	nedostupná informace	365 313
Výkon				
Operační paměť zabraná rezidentní ochranou	40 MB	69 MB	7 MB	67 MB
Doba skenu, standardní mod (min:s)	55:46	20:05	4:45	7:03
Potřebné místo (přibližně)	16,7 MB	23,5 MB	19,7 MB	23,8 MB
Funkčnost				
Plánovač	•	-	•	-
Volby pro sken	silně omezené	detailně nastavitelný	detailně nastavitelný	detailně nastavitelný
Informace o nalezeném spywaru	jen na webu	jen krátká informace	v programu, dobře srozumitelné	jen jméno a umístění
Rezidentní ochrana	•	•	•	•
Podpora browseru	Internet Explorer	Internet Explorer	Internet Explorer	Internet Explorer
Podpora více uživatelů	•	•	•	-
Prostředí	matoucí	přehledné	přehledné	přehledné
Update	automaticky	automaticky	automaticky	ručně
Podpora	fórum, chat, hotline	e-mail, placená hot-line	fórum	fórum, e-mail
Další funkce	blokování vyskakovacích oken, ničení stop	automatické startování, ničení stop	imunizace, automatické startování, skartovačka dat	automatické startování, ničení stop, skartovačka

nistrátorský účet, nemálo uživatelů má však účet s omezenými právy. Zajímalo nás, zda je možné program používat, i když nemáte administrátorská práva. Je možné programy jen spouštět, nebo i nainstalovat?

Dobrou zprávou je, že u většiny programů jsme nenarazili na závažnější problém. Na skutečné problémy jsme narazili jen u antispywarů od firem Ashampoo a Data Becker. V těchto případech se jednalo o problém s omezenými konty u skenu zaměřeného na spyware. Důvodem je to, že oba programy je možné spouštět jen s administrátorskými právy. Nepomůže dokonce ani provedení druhé instalace pod omezeným účtem.

Tento nedostatek výrobci ovšem vykompenzovali v oblasti updatu. Téměř všechny programy se aktualizují automaticky. Jen u Ad-Awaru, Data Beckeru a Ashampoo musí uživatel aktualizaci povolit ručně.

Celková situace ovšem tak veselá není. Žádný antispywarový program nesplňuje to, co slibuje. Pokud to s ochranou svého počítače myslíte vážně, bude lepší investovat do kompletního zabezpečovacího balíku. ■ ■ ■



Ad-Aware SE Personal: V boji proti spyware je tento freeware neúčinný. Špatné výsledky podává ve všech kategoriích.

5	6	7	8	9
ZoneAlarm Anti-Spyware	**Windows Defender**	**Spy Sweeper 4.5**	**AntiSpion 2006**	**Ad-Aware SE Personal**
Zone Labs Security	Microsoft	Webroot	Data Becker	Lavasoft
30 eur	Beta 2	1 046 Kč	20 eur	freeware
www.zonelabs.com	*www.microsoft.cz*	*www.webroot.com*	*www.databecker.com*	*www.lavasoft.com*
54	**53**	**53**	**48**	**42**
29	28	51	27	27
64	95	36	89	64
66	82	87	67	66
dostatečný	uspokojivý	dostatečný	nedostatečný	nedostatečný
Jen díky rychlosti a firewallu je program ve středu testovacího pole.	S rootkity si neporadí vůbec, čištění je rovněž špatné.	Aktivní spyware odstranil nástroj docela dobře, s rootkity si však neporadil.	Rozpoznávání spywaru je neakceptovatelné, rootkity nezná vůbec.	Tento testovaný nástroj selhal ve všech disciplínách.
8%	23%	35%	6%	15%
55%	70%	90%	55%	65%
25%	45%	75%	35%	35%
30%	45%	70%	15%	40%
11%	0%	22%	0%	0%
56%	0%	0%	0%	0%
žádný	žádný	žádný	žádný	– (žádné sledování)
1	žádný	žádný	1	1
nedostupná informace	nedostupná informace	135 855	nedostupná informace	56 111
22 MB	12 MB	83 MB	35 MB	-(žádné sledování)
1:50	1:22	24:55	1:10	0:57
12,1 MB	10,8 MB	16,8 MB	16 MB (z toho 8 MB reklama)	3,4 MB
•	•	•	•	•
detailně nastavitelný	omezeně nastavitelný	detailně nastavitelný	detailně nastavitelný	detailně nastavitelný
krátká informace + webová databanka	v programu, dobře srozumitelné	jen webová databanka	v programu, dobře srozumitelné	krátká informace + webová databanka
•	•	•	•	– (jen ve verzi Pro)
Internet Explorer / Firefox	Internet Explorer	Internet Explorer	Internet Explorer	Internet Explorer
•	•	•	-	•
přeplácané (mnoho funkcí)	přehledné	přehledné	přehledné	přehledné
automaticky	automaticky	automaticky	ručně	ručně
fórum, e-mail, placená hotline	webová databanka	fórum, e-mail, placená hotline	fórum, e-mail, hotline	fórum, webová databanka
firewall	rozšířený Taskmanager	novinky z oblasti spywaru	XP-Tweaker	rozhraní pro bezpečnostní doplňky

CHIP SOUHRNNÝ PŘEHLED: Antispyware

Soupeři

1 McAfee AntiSpyware 2006
Slabé první místo. Odstranil jen 70 % spywaru.
Cena: 880 Kč

2 SimonTools AntiSpyWare
I druhý program je propadák. Dokázal odstranit jen 5 % spywaru!
Cena: 18 eur

3 Spybot Search & Destroy
Neaktivní rootkity odstranil z 11 %, aktivní vůbec.
Cena: freeware

4 Ashampoo Anti-Spyware
Rozpoznal téměř vše, odstranil jen výjimečně.
Cena: 30 USD

5 ZoneAlarm Anti-Spyware
Jen rychlost a firewall jsou pozitivní stránkou tohoto nástroje.
Cena: 30 eur

6 Microsoft Windows Defender
Tato bezplatná beta verze nedokáže rozpoznat trojské koně.
Cena: freeware (beta)

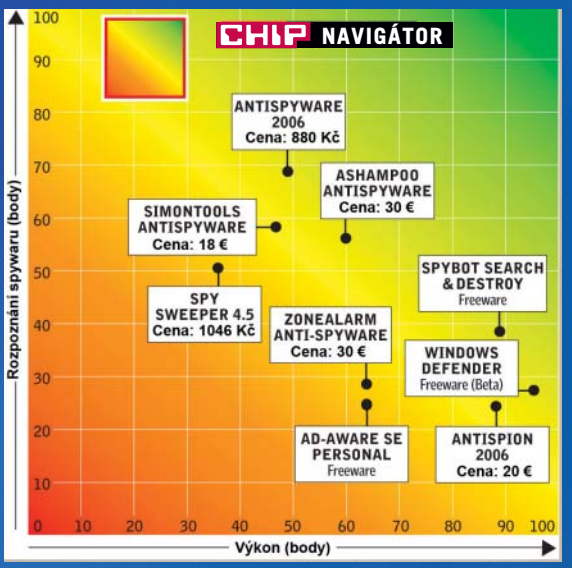
7 Webroot Spy Sweeper 4.5
Má nejlepší čisticí schopnosti, i zde však chybí 25 %.
Cena: 1060 Kč

8 Data Becker AntiSpion 2006
Rozpoznání a odstranění prakticky nefunguje.
Cena: 20 eur

9 Ad-Aware SE Personal
Jednoduše katastrofa – sice nic nestojí, ale také nic nenabízí.
Cena: freeware

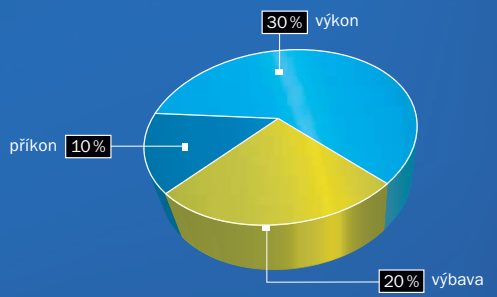
Rozpoznání versus výkon

Současné antispywarové produkty nesplnily to, co jsme od nich očekávali. Kromě toho skutečně kvalitní test trvá neúměrně dlouho. Antispyware s nejlepšími rozpoznávacími schopnostmi spotřebuje také nejvíce operační paměti. V grafu jsou znázorněny schopnosti „on-demand" skenu rozpoznat neaktivní spyware a adware v porovnání s výkonem, tedy s časem, který program k otestování potřeboval.



JAK JSME TESTOVALI

Nejdůležitějším kritériem bylo rozpoznání a odstranění spywaru. Pro získání vysokého počtu bodů musel nástroj rozpoznat a odstranit i rootkity. Měřili jsme i výkon jednotlivých nástrojů. Rychlý test a malá část zabrané paměti byly zárukou vyššího počtu bodů. Body programy získaly, pokud měly přehlednou ovládací plochu a málo chybových hlášek, pokud nabízely informace o spywaru a měly skvělou podporu a časté aktualizace. Přídavné utility celkové hodnocení neovlivnily.



Security check

Na tomto místě se běžně dozvídáte, na která kritéria si máte dát při nákupu softwaru pozor. Tentokrát vám však nedoporučíme žádný konkrétní produkt. Místo toho vám nabídneme přehled důležitých ochranných opatření.

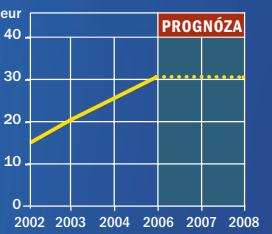
Firewall
Aby byl desktop neprůstřelný, je potřeba nainstalovat štít v podobě firewallu. Většinu běžných útoků dokáže firewall docela dobře odpálkovat.

Antivir
Dobré nástroje rozpoznají nejen viry, ale také spyware. Přesto buďte opatrní, rootkity dělají antivirům potíže.

Webový filtr
Browser bez webového filtru může být snadno napadnutelný a omylem se může do počítače dostat spyware.

Antispam
E-mail je také jednou z cest, jak se internetová mafie snaží dostat k vašim datům. Spamový filtr dokáže odstranit většinu takových mailů.

ODHAD VÝVOJE CEN



Doba samostatných produktů je pryč. Další růst cen je nepravděpodobný.

Je jen otázkou času, kdy se objeví nové typy škodlivých programů, určené přímo pro nový operační systém. V několika posledních letech je vidět velký příklon ke škodlivým programům, jejichž primárním účelem je získání peněz pro své autory či zadavatele. Ti proto nebudou váhat s investicí práce i financí, aby zjistili slabiny a možné problémy, které se v systému Vista, obsahujícím spoustu nového a poměrně komplikovaného kódu, zcela určitě budou nacházet.

Velké rozšíření škodlivých programů je hlavně sociálním problémem dneška – existuje poptávka po takových programech, existují metody, jak takové programy k uživatelům dostat a jak dostat citlivá data od uživatelů zpět. Windows Vista mohou některé cestičky zúžit či uzavřít, vyřešení celého problému se jim však rozhodně nemůže podařit... ■ ■ ■

NOVÉ BEZPEČNOSTNÍ MEZERY

WINDOWS 98/ME

11. července zastavil Microsoft podporu pro Windows 98/Me. Týká se to i bezpečnostních aktualizací pro již známé bezpečnostní mezery. Příklad: Pokud zmanipulovaná webová stránka přesměruje surfaře na vzdálený souborový server, ten může prostřednictvím upravených COM objektů (Component Object Model) spustit libovolný kód.

→ Řešení: Přestupte na jiný operační systém.

Info: *www.microsoft.com*

OpenOffice

Objevil se první makrovirus pro OpenOffice. Je více otravný než nebezpečný: skript Stardust modifikuje standardní předlohu dokumentu. Do každého nově otevřeného dokumentu pak vloží pornografický obrázek z webu.

→ Update na aktuální verze OpenOffice *(www.openoffice.org)* a StarOffice *(www.sun.com)* bezpečnostní mezeru odstraní.

Filzip

Bezplatný univerzální komprimační program Filzip *(www.filzip.de)* ve své současné verzi 3.05 uzavírá jednu bezpečnostní mezeru – a zároveň hned otevírá novou: zmanipulované archivy mohou „rozpakovat" soubory i mimo zadanou cestu a přepsat tak třeba systémové soubory. Platí to pro formáty RAR, TAR, JAR a GZ.

→ Filzipem rozbalujte archivy jen s omezenými uživatelskými právy, například pod kontem hosta.

Apple Mac OS X

Společnost Apple vydala Security Update 2006-004 pro svůj Mac OS X verze 10.3.9 a 10.4.7 včetně Server verzí. Opravy se týkají celé řady produktů, jejichž seznam a popis chyb v nich opravených naleznete v původním oznámení *(http://docs.info.apple.com/article.html?artnum=304063)*.

→ Svůj Mac OS X aktualizujte pomocí Software Update nebo přes Apple Download.

Firefox

Firefox 1.5.0.3 v PC samočinně spustí poštovní program. Stačí k tomu, aby v tagu <img src=> byla uvedena URL adresáta. Na internetu k tomu koluje JavaScript, který takto vyvolá stovku URL a simuluje tím útok typu DoS. Tomu podlehne i ten „nejsilnější" počítač.

→ Aktualizace na Firefox 1.5.0.4 problém odstraní.