Krádež dat pomocí

Kreditní karty, bankovní účty, e-mailová konta – žádná data nejsou před spywarem bezpečná. Náš test vám prozradí, zda uživatel potřebuje k ochraně počítače speciální **ANTISPYWAROVÉ NÁSTROJE**, nebo zda mu stačí jednoduchý virový skener.

CLAUDIO MÜLLER

Co vás napadne, když na internetu narazíte na programy pojmenované XP Anti-Spyware 2009, AntiSpyCheck či Malware Alarm? Obvykle to, že jde o antispywarové programy, které ochrání vaše data před hackery. Ale pozor, skutečnost je přesně opačná – jde o maskovaný spyware.

V současné době stovky takových programů s neškodnými jmény předstírají, že naleznou a odstraní škůdce, ve skutečnosti jsou však samy speciálním typem malwaru. Jejich taktika je následující: Nejprve vás otravují varovnými zprávami, předstírají, že nacházejí spyware, a potom žádají uživatele, aby aktualizoval či instaloval plnou verzi pro odstranění červů. Skromnější nástroje „jen" stáhnou a propašují do počítače další škůdce, ty drzejší za to ještě chtějí od vás peníze. Snadné vítězství vás nečeká ani v případě, že program „odhalíte" a rozhodnete se ho odinstalovat. V některých případech mají problém odstranit tyto „bezpečnostní programy" i experti. Po pár dnech „používání" je navíc počítač prolezlý malwarem, který slídí po citlivých osobních datech a zasílá je hackerovi.

Slídicí techniky

Hackera nezajímají informace týkající se preferencí při surfování. On má především zájem o čísla kreditních karet, přístupová data k on-line bankovnictví a hesla k e-mailovým kontům (viz graf). Obchod s těmito daty mu totiž přináší spoustu peněz – podle firmy Symantec dostanete na černém trhu za bankovní konto zaplaceno až 1 000 dolarů, za číslo kreditní karty 25 dolarů a funkční poštovní adresy (megabajt dat) jsou na prodej už za 40 dolarů.

Není tedy divu, že klasický spyware, který slídí jen po informacích týkajících se chování uživatele na internetu a který otravuje vyskakovacími okny, je už jen stínem předchozí hrozby a jeho dny jsou sečteny.

Pod taktovkou internetové mafie pracují škůdci jinak. Již zmiňovaná vyskakovací okna mají především přitáhnout pozornost uživatele ke speciálně upraveným stránkám, kde návštěvník „chytí" opravdový spyware. Říkáte si, že vy se nemusíte bát, protože byste na nic neklikli? Chyba lávky. Někdy ke stažení malwaru (a instalaci na pozadí) úplně stačí i pouhé nahrání webové stránky.

Tyto metody (označované jako drive-by-downloads) jsou zvláště nebezpečné, protože skutečně nemusíte ani na nic kliknout, a přesto se ihned po navštívení stránky na vašem počítači objeví nenápadný škůdce. Ten ukryje příkazy ke svému automatickému spouštění do registrů a tím se stane vaším věrným „přítelem" při každém spuštění systému. Podobní škůdci už často dokonce fungují simultánně s dalšími paralelními procesy (škůdci), které se vzájemně monitorují. Pokud uživatel ukončí podezřelý proces, je okamžitě spuštěn proces další. Touto metodou dokáží škůdci i obnovit jednou vymazané položky v registrech.

Stále obtížnější je dokonce i samotná identifikace spywaru. Důvodem je skutečnost, že profesionální hackeři začali preferovat kombinaci spywaru a rootkitu. Rootkit používají jako kamufláž pro skutečný virus, a tak dokonce dokáží skrýt procesy či položky v registrech před systémovými nástroji. Rootkity se obvykle uhnízdí přímo v jádře operačního systému a odsud skrývají aktivity spywaru. Jejich umístění v kornelu má i další „výhody". Odsud totiž mohou ovládat i další důležité vlastnosti, jako je řízení procesorového času pro různé procesy, kontrola přístupu k souborům, prosazování přístupových práv jednotlivých aplikací k systému a řízení paměti. Všechny tyto „drobnosti" jsou pak příčinou toho, že jsou rootkity tak nebezpečné a tak obtížně odstranitelné – fungují totiž na stejné úrovni jako jádro systému a mají stejná práva.

PROHLÁŠENÍ

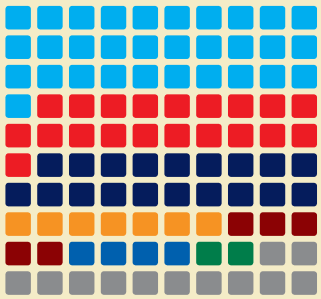
Christian Funk, virový specialista Kaspersky Lab Central Europe

Rostoucí hrozba

Zatímco klasických virů přibylo jen málo, v oblasti spywaru jsme zaznamenali raketový růst. Za poslední rok vzrostl počet škůdců o více než 400 %. Zdá se, že tento trend bude pokračovat tak dlouho, dokud si uživatelé lépe nezabezpečí počítače a nedonutí hackery k hledání jiného zdroje financí. Je především důležité, aby uživatelé nepodceňovali riziko v oblasti profesionálního počítačového zločinu.

ČERNÝ TRH S DATY

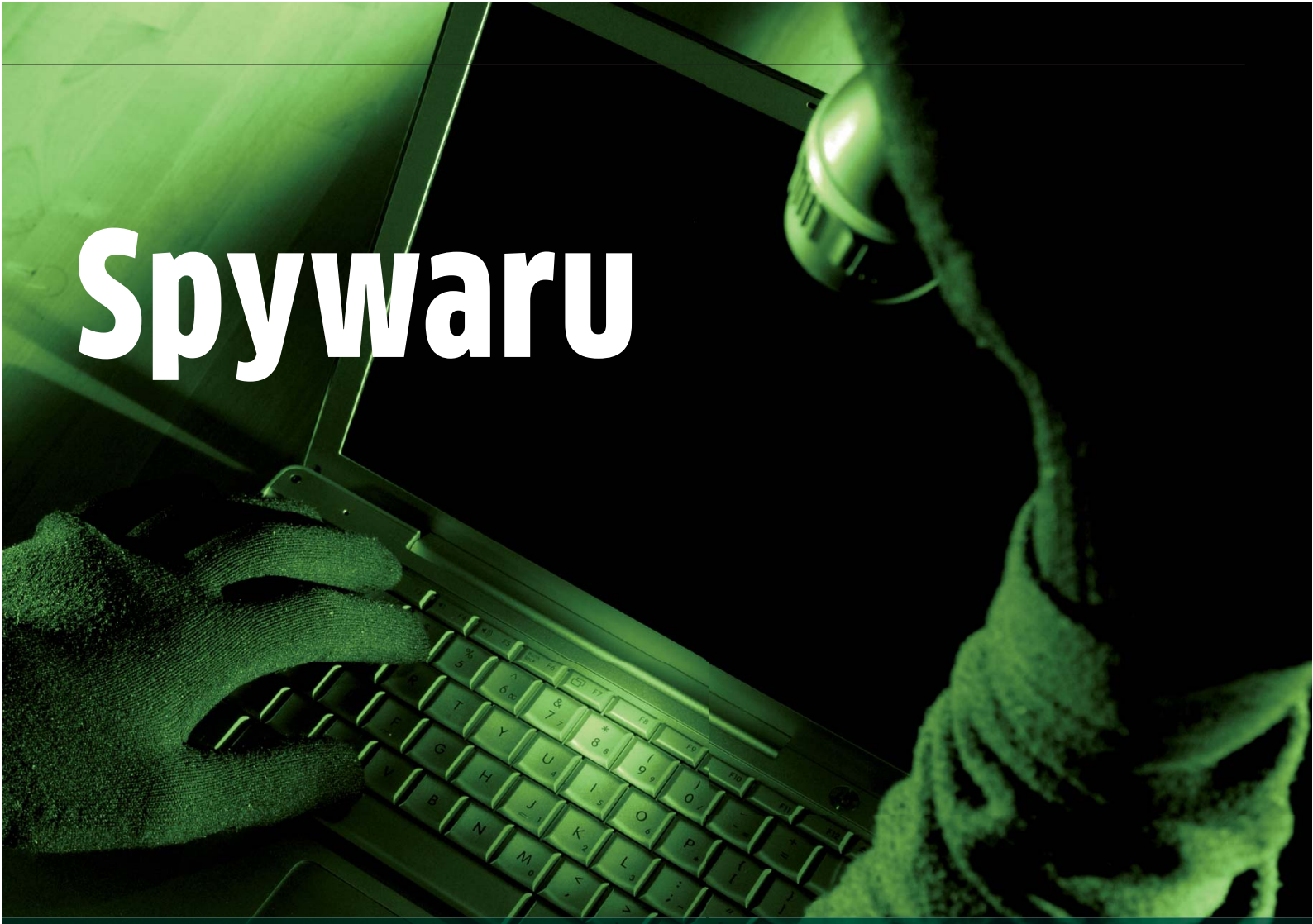
Hackeři kradou především přístupové údaje k bankovním kontům, která poté „kupci" dokonale „vyčistí"



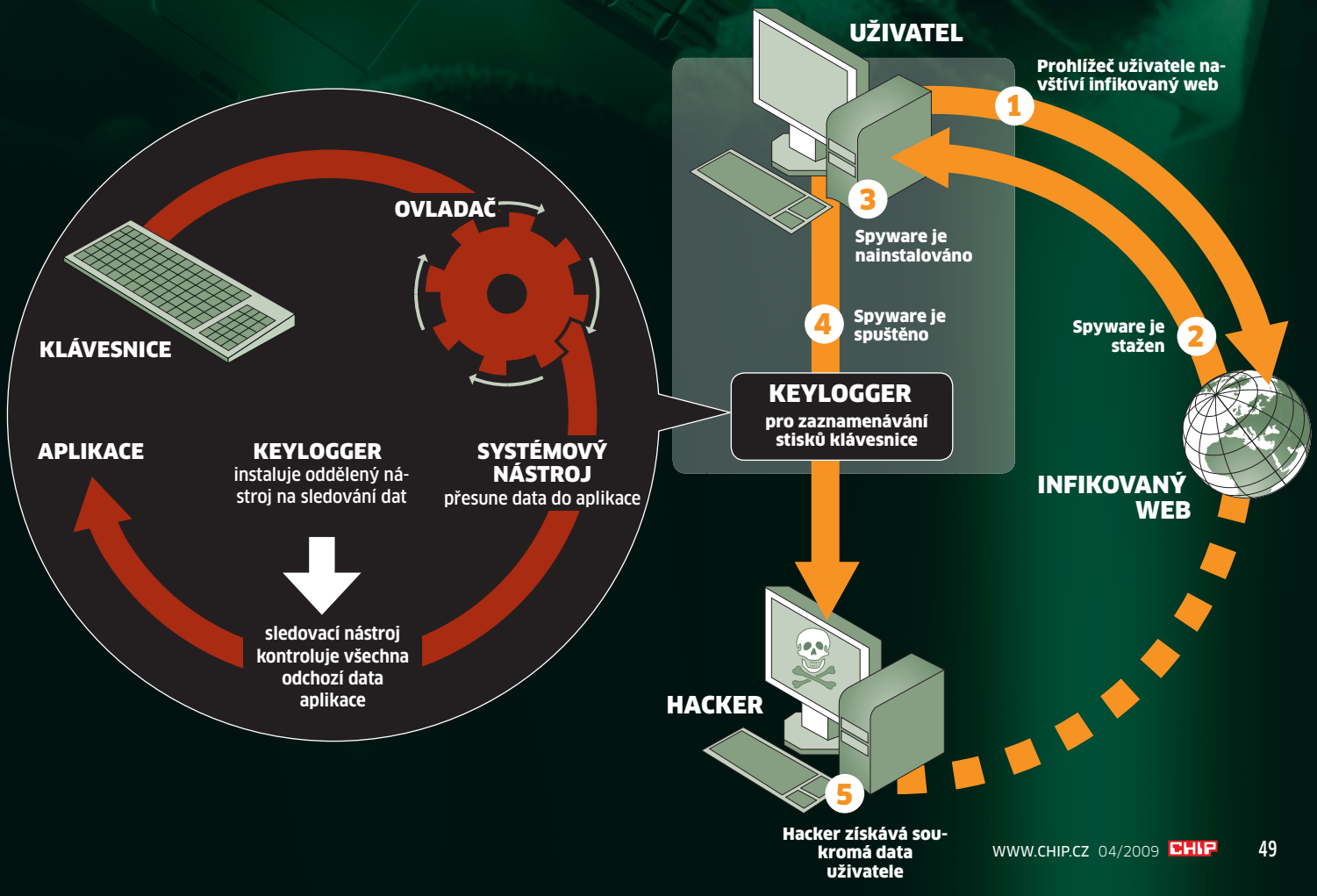
ZDROJ: SYMANTEC

31 % KREDITNÍ KARTY
20 % BANKOVNÍ ÚČTY
19 % E-MAILOVÁ KONTA
7 % SOUKROMÁ DATA
5 % ÚČTY NA SERVERECH
4 % HACKNUTÁ PC
2 % ZÁKEŘNÉ KÓDY
12 % OSTATNÍ

Spywaru

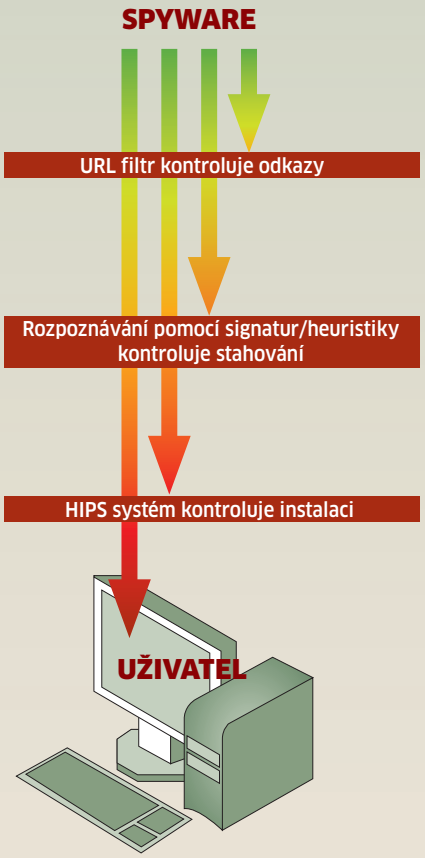


Jak funguje spyware



Třístupňová kontrola

Dobrý nástroj na obranu proti spywaru nabízí vícestupňovou ochranu, která zaručí větší bezpečnost před různými typy škůdců. Nástroj zasahuje ve třech situacích: když uživatel surfuje na nebezpečných webech, při stahování aplikací a při jejich instalaci na počítač.



Rogue antispyware: Falešné bezpečnostní nástroje obtěžují uživatele varovnými zprávami tak dlouho, dokud si nástroj nekoupí. Po nainstalování navíc program do počítače propašuje další škůdce...

Rootkit: Přestrojen za spyware

Manipulace s objekty jádra je v poslední době jednou z nejoblíbenějších metod útoku hackerů. Operační systém užívá tyto objekty k administračním a řídicím účelům, např. k registraci aktivních procesů. V praxi to funguje následujícím způsobem: Správce úloh (Task manager) vstoupí do protokolu a zobrazí zde uvedené programy. Pokud tedy kdokoliv hledá podezřelé procesy v Task manageru, rootkit protokol si procesy upraví a spyware „není vidět". Další přístup k jádru systému „umožňují" rootkitům ovladače. Windows vývojářům nabízejí možnost zlepšení funkčního rozsahu ovladačů, který má umožnit jejich snadnější úpravy. Ovladače tudíž regulují nejen přímý přístup softwaru k hardwaru, ale také umožňují přístup k souborům systému.

Důsledek je nepříjemný – bezpečnostní programy prozkoumají aktivní soubory a zkontrolují je na podezřelé signatury, ale odhalit rootkity fungující pomocí zmiňované techniky obvykle nedokáží. Rootkit dokáže skrýt porty otevřené spywarem, a tudíž udržovat komunikační kanál s hackerem přímo „pod nosem" bezpečnostních skenerů. V porovnání s Windows XP je na tom Vista z hlediska bezpečnosti mnohem lépe – nabízí totiž zdokonalený bezpečnostní mechanismus. Vista přísně reguluje přístup k objektům jádra a instalaci ovladačů autorizuje pouze po ověření signatur kódu. Jakmile je však jednou spyware v počítači, bezpečnost dat může být zaručena jen stěží. Stálicí v žebříčku oblíbenosti jsou u hackerů stále keyloggery. Tyto programy fungují na pozadí a zaznamenávají všechny stisky klávesnice. Obvykle také zaznamenávají všechny navštívené stránky a spuštěné programy, takže bez problémů dokáží přiřadit vložená data např. ke stránkám on-line bankovnictví či kontu na Facebooku. Lepší keyloggery si dokáží poradit i s ochranou v podobě „virtuální klávesnice". Ve finále pak keylogger potom otevře port a zaznamenaná data přenese k hackerovi buď přes TCP/IP spojení, nebo pomocí samostatné rutiny přes e-mail.

Lovci spywaru

Všestranné a důmyslné metody spywaru vždy kladou na bezpečnostní programy nejvyšší nároky. V testovací laboratoři bezpečnostních expertů ze společnosti AV Test jsme srovnali šest známých antispywarových nástrojů s klasikou v podobě programu Norton AntiVirus 2009, který je také součástí Norton Internet Security (našeho vítěze testu bezpečnostních balíků v Chipu 01/2009). Protože přechod mezi spywarem a klasickým malwarem je poněkud mlhavý, chtěli jsme zjistit, zda je ochrana virového skeneru proti spywaru dostatečná, nebo zda je k zamezení špionážních aktivit ještě nutný speciální program (přímo označený jako antispyware).

Identifikace: Většina nástrojů je bezmocná

Kvalitní antispywarový program používá k zabezpečení počítače dvě metody: URL filtr s „černou listinou" (obsahující i webové odkazy) a nástroj identifikující známé viry pomocí jejich signatur. Testovací počítače (Windows XP s SP3) měly navštívit 200 webových stránek, které chtěly do počítače propašovat spyware. Jak si s tím programy poradily? Klasický URL filtr používají pouze Norton a Spy Sweeper. U druhého programu se obě metody navzájem dobře doplňují: filtr zablokoval 24 webových stránek, jejichž spyware nebylo možno identifikovat ani ze signatur. Ostatní programy, které důvěřují pouze své identifikaci pomocí signatur, se ukázaly jako zklamání: ani jeden z nich neidentifikoval víc než polovinu spywaru. Nástroje SpyBot a Spyware Doctor identifikovaly dokonce méně než jednu desetinu, a to není zrovna optimistické číslo.

NA DVD

Nástroje proti spywaru

AVG Chip ► Komplexní bezpečnostní balík ve speciální verzi

DriveImage XML ► Vytváří zálohy disků

SpyBot Search&Destroy ► Hledá spyware

F-Secure Internet Security 2008 ► Zkušební verze bezpečnostního balíku

Gmer ► Nástroj na detekci rootkitů a jejich mazání

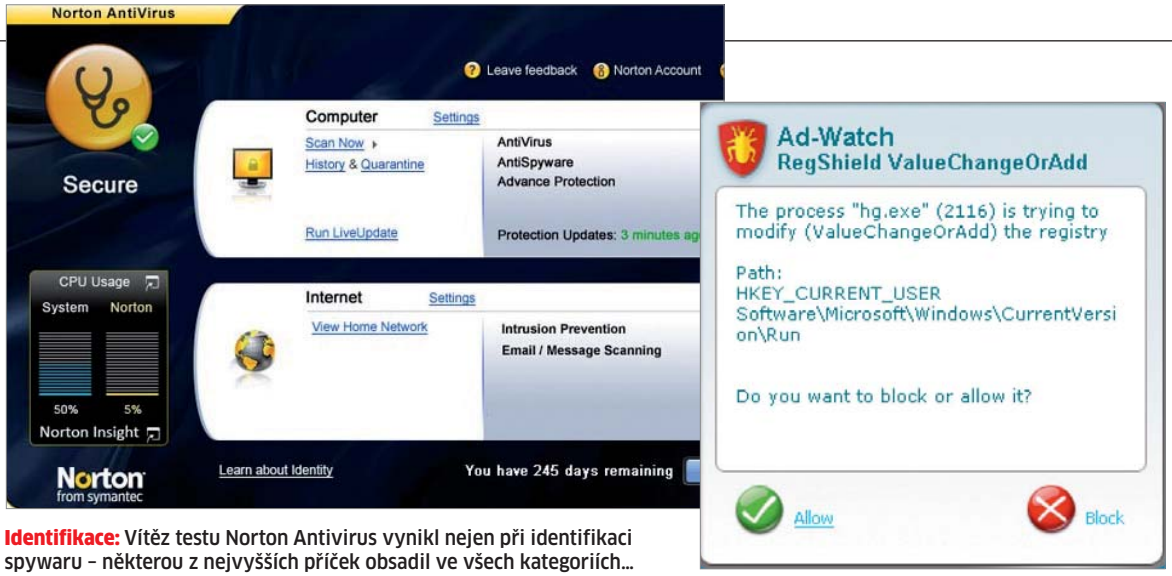
HijackThis ► Hledá v registrech malware

Recuva ► Obnovuje smazaná data

Sandboxie ► Umožňuje spouštění programů v bezpečném prostředí

VirtualKeyboard ► Jednoduchá virtuální klávesnice

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **SPYWARE**.



Identifikace: Vítěz testu Norton Antivirus vynikl nejen při identifikaci spywaru – některou z nejvyšších příček obsadil ve všech kategoriích...

Co je to? Celá řada antispywarových nástrojů uživatele „zásobuje" varovnými zprávami a nutí je rozhodovat, zda o škůdce jde, či nikoliv...

Pojďme se však podívat na další část testu. Jakmile se spyware dostane do počítače, spustí se automaticky instalační rutina a škůdce se pokusí v systému usídlit „natrvalo". Jak si bezpečnostní nástroje poradí s touto skutečností? Naši kandidáti spoléhali na signatury či další charakteristiky (jako jsou změny v registrech) vedoucí k odhalení; pouze Norton fungoval spolehlivě na základě metody detekce založené na chování. Míru detekce lze ohodnotit jako dobrou: například Norton a SpyBot identifikovaly každý z deseti instalačních pokusů. Naopak zklamáním byl Windows Defender, který zasáhl jen dvakrát. Jeho poslední místo v testu tak určitě není žádným překvapením.

Antispywarové nástroje by měly nejen zobrazit varovné zprávy, ale měly by také zablokovat instalaci a zároveň vetřelce odstranit. V tomto ohledu je nejdůslednější Norton spolu s nástrojem Spy Sweeper (k němuž jsme ale měli několik výhrad). Ostatní programy se příliš často vzdávaly a „přes varovná hlášení" přenechávaly rozhodnutí o přerušení instalace na uživateli. To ale není zrovna optimální postup – v počítači tak obvykle zůstanou spustitelné soubory a až po delší době se ukáže, že jsou opravdu zdrojem nebezpečí.

Nepříjemné také je, když to nástroje se svou podezíravostí přehánějí a obtěžují uživatele falešnými poplachy. Pro tento „scénář" bylo na testovací systém nainstalováno deset známých programů (které zahrnovaly nástroj od firmy Adobe, iTunes, specializované Daemon tools a Microsoft Office 2007), abychom si ověřili, jak na ně reaguje antispyware. Pouze programy Norton, Spyware Doctor a Windows Defender si ani jednou nestěžovaly. Naopak Ad-Aware v sedmi případech ihned zobrazil varovné zprávy.

Mimořádně nepříjemné bylo, když SpySweeper přerušil instalaci Adobe Readeru a Skypu jako podezřelých plug-inů prohlížeče a když se AntiSpyWare 2 během instalace iTunes zhroutil.

Dezinfekce: Neuspokojivý dojem

V celé řadě případů instalují uživatelé bezpečnostní program až poté, co je počítač infikován. Proto museli kandidáti smazat deset „předinstalovaných" virů, a to včetně vyčištění jejich záznamů v registrech.

Udivující výsledek: Žádný z programů nedokázal kompletně vyčistit systém; pouze Norton odstranil vše, kromě jednoho spustitelného souboru a položek v registrech. Díky tomu se stal v této části testu (poněkud rozpačitým) vítězem. Zbývající programy však předvedly ještě zoufalejší výkony – většina ostatních účastníků testu odstranila méně než pět škůdců!

Výsledek našeho testu: Zástupce virových skenerů Norton Antivirus zanechal daleko za sebou specializované nástroje na obranu proti spywaru. Z toho pro uživatele plyne i příjemná výhoda: ke svému antivirovému nástroji (nebo bezpečnostnímu balíku) nemusí dodatečně instalovat žádného lovce spywaru. Jeho instalaci lze doporučit pouze úzké skupině uživatelů, kteří používají (obvykle bezplatnou) omezenou verzi virového skeneru.

AUTOR@CHIP.CZ

Antispyware test: Antivir proti specialistům na spyware

	1. MÍSTO	2. MÍSTO	3. MÍSTO	3. MÍSTO	5. MÍSTO	6. MÍSTO	7. MÍSTO
Produkt	**Norton Antivirus 2009**	**Spy Sweeper 5.8**	**Ad-Aware 2008 plus**	**Spyware Doctor 6**	**SpyBot Search&Destroy**	**AntiSpyware 2**	**Windows Defender**
Web	www.symantec.cz	www.webroot.com	www.lavasoft.com	www.pctools.com	www.spybot.info	www.ashampo.com	www.microsoft.com
Cena (přibližně*)	850 Kč	1 000 Kč	740 Kč	1 000 Kč	zdarma	30 Euro	součást Windows
Celkové hodnocení	91 ■■■■■	67 ■■■□□	56 ■■□□□	56 ■■□□□	52 ■■□□□	50 ■■□□□	48 ■■□□□
Identifikace při stahování (URL filtr/signatura)"	**15 %/89 %**	20 %/48 %	0 %/19 %	0 %/10 %	**0 %/6 %**	0 %/29 %	0 %/38 %
Identifikace při instalaci (chování/signatura/jiné)**	**80 %/20 %/0 %**	0 %/80 %/10 %	0 %/40 %/50 %	0 %/80 %/10 %	0 %/10 %/90 %	0 %/10 %/70 %	**0 %/20 %/0 %**
Identifikace/blokování/ smazání po instalaci	**100 %/90 %/80 %**	90 %/60 %/30 %	90 %/40 %/30 %	90 %/50 %/20 %	100 %/60 %/10 %	80 %/40 %/0 %	**20 %/20 %/0 %**
Falešný poplach při instalaci softwaru (varování/zablokování)	**0 %/0 %**	30 %/20 %	**70 %/0 %**	**0 %/0 %**	50 %/0 %	50 %/10 %	**0 %/0 %**
Účinnost dezinfekce (celková/částečná)	**70 %/30 %**	50 %/30 %	50 %/20 %	30 %/30 %	**20 %/30 %**	30 %/30 %	60 %/0 %

● **Špičková třída (100–90)** ● **Střední třída (74–45)** ● **Vyšší třída (89–75)** ● **Nelze doporučit (44–0)**

Všechna hodnocení v bodech (max. 100)

***Zdroj: www.sw.cz, ** například změny v registrech, záznam firewallu**