Malí akční pomocníci

S rostoucím počtem virů a malwaru roste i **RIZIKO INFEKCE.** Jak se s ním vypořádat, nechcete-li používat nejnovější bezpečnostní nástroje?

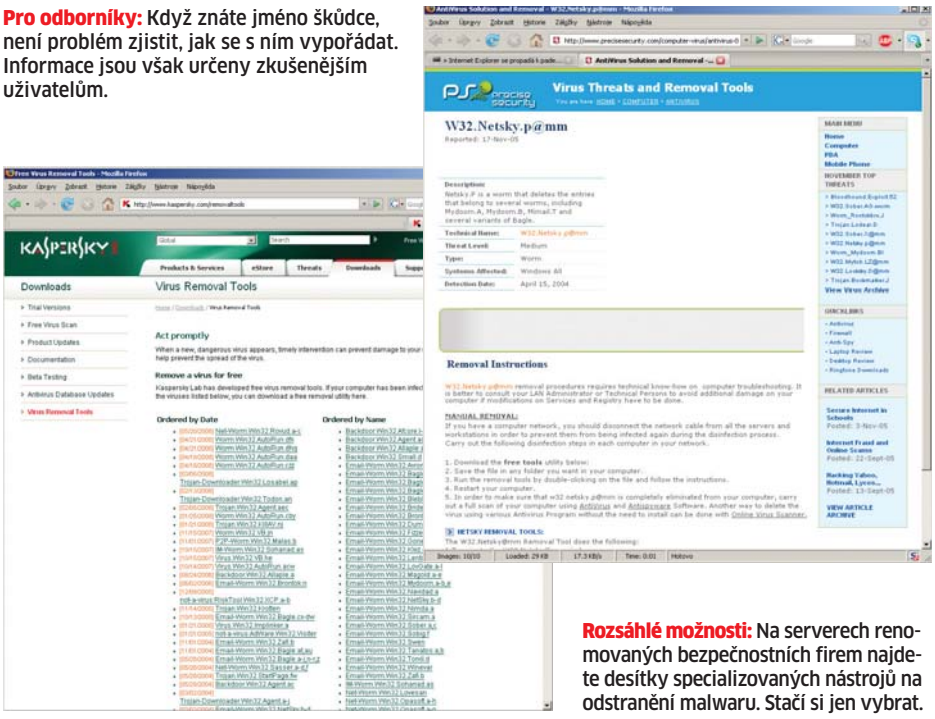
PETR KRATOCHVÍL

Pro majitele výkonných počítačů není bezpečnost žádným problémem – stačí jen trocha opatrnosti a kvalitní bezpečnostní balík. Uživatelé s pomalejšími „stroji“ obvykle své bezpečnostní nástroje shánějí, kde se dá, což v některých případech končí poměrně tragicky. Většina bezplatných nástrojů si se sofistikovaným malwarem neporadí, a tak potom bývá jediným řešením reinstalace. Jde to však i jinak.

Detekce

Prvním krokem na cestě za „čistým počítačem“ je detekce problémů. Výhodou komplexních bezpečnostních balíků je zjištění infekce již při průniku do počítače (při kopírování z USB disku nebo čtení e-mailu). U horších bezpečnostních nástrojů však obvykle nezbývá nic jiného než hledat problémy přímo na disku počítače. Nouzovým řešením je instalace jiného bezplatného antiviru, tu však dokáže šikovnější malware zablokovat. My doporučujeme alternativní cestu – internetové skenery, jejichž test jsme vám nabídli v Chipu č. 4 (najdete ho i na DVD). Pomocí těchto nástrojů naleznete většinu běžných škůdců, kteří se vám v počítači uhnízdili.

Na prvním místě se v testu umístil nástroj od firmy Eset, z hlediska detekce by však vaší pozornosti neměly uniknout ani nástroje firem F-secure a Kaspersky. Je sice pravda, že ani ten nejlepší skener nedokáže nalezený malware odstranit, v tomto kroku je ale pro nás nejdůležitější detekce. A to je oblast, ve které internetové skenery vynikají...



Pro odborníky: Když znáte jméno škůdce, není problém zjistit, jak se s ním vypořádat. Informace jsou však určeny zkušenějším uživatelům.

Rozsáhlé možnosti: Na serverech renomovaných bezpečnostních firem najdete desítky specializovaných nástrojů na odstranění malwaru. Stačí si jen vybrat.

Diagnóza

Poté, co už víte, kdo vám v počítači dělá „neplechu“, je situace veselejší. Zkušenější uživatelé teď mohou zadat do Googlu jméno škůdce a snadno najít postup, jak se ho zbavit. Na celé řadě stránek najdete návody na vyčištění registrů, smazání souborů nebo odstranění procesů. Tento postup sice také vede k cíli, má však několik drobných vad. Prvním problémem bývá to, že ho dokáží použít jen zkušenější uživatelé, kterým nedělá problémy práce s procesy nebo pohyb v registrech. Druhou „drobností“ je nebezpečí „chyby“. Stačí kliknutí na špatný klíč, odstranění jiného procesu nebo smazání důležitých systémových souborů, a i zkušený „opravář“ může nadělat více škody než užitku. Návody a informace na odstranění škůdce je tak lepší brát pouze jako nástroj na potvrzení diagnózy – s nimi už si můžete být jisti, že jste malware identifikovali správně.

Odstranění

Většina renomovaných „bezpečnostních“ firem nabízí nejen klasické antivirové programy, nástroje proti malwaru nebo bezpeč-

INFO

Tři kroky k bleskově čistému počítači

1) DETEKCE

Nejprve zkontrolujte počítač vybranými internetovými skenery. Doporučujeme tyto:

- ► **www.eset.cz/online-skener**
- ► **http://support.f-secure.com/enu/home/ols.shtml**
- ► **www.kaspersky.com/virusscanner**

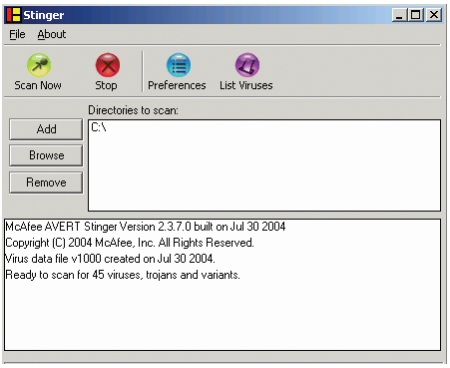
2) VYČIŠTĚNÍ

Pomocí výše uvedených skenerů odstraňte méně zákeřný malware a po restartu počítače si pořiďte seznam toho odolnějšího.

3) ODSTRANĚNÍ ZBÝVAJÍCÍCH ŠKŮDCŮ

Na serverech renomovaných antivirových firem (nebo pomocí Googlu) vyhledejte jednorázové „čisticí“ nástroje. Najdete je například zde:

- ► **www.symantec.com/business/security_response/removaltools.jsp**
- ► **www.kaspersky.com/removaltools**



Komplexnější: McAfee nabízí pokročilejší variantu nástroje proti malwaru, která si poradí s více škůdci.

nostní balíky, ale také celou řadu bezplatných služeb pro uživatele. Mezi ně lze řadit jak již zmiňované internetové skenery, tak i specializované utility pro boj s malwarem. Jde o malé prográmky, které obsahují nástroj na odstranění vybraného „problému". Uživatel jen musí vybrat ten správný a spustit ho. Nástroj už se postará o vše důležité – ukončí běžící procesy, odstraní klíče z registru a smaže infikované soubory. Jediným potenciálním zádrhelem je to, že vzhledem k velkému množství malwaru existují i desítky nástrojů na jeho odstranění.

Kde hledat

Jeden z nejrozsáhlejších archivů najdete na webu firmy Symantec **www.symantec.com/business/security_response/removaltools.jsp,** kde najdete utility roztříděné jak podle abecedy, tak i podle data přidání. Podobně rozsáhlý archiv (i se stejným tříděním) nabízí firma Kaspersky na adrese **www.kaspersky.com/removaltools.** Zajímavý postup zvolila firma McAfee. Na jejím webu **(http://us.mcafee.com/virusInfo/default.asp?id=vrt)** totiž najdete jen několik utilit proti těm nejrozšířenějším škůdcům. Na alternativním webu **(http://vil.nai.com/VIL/stinger/)** ale najdete nástroj jménem Stinger, který prohledá počítač a poradí si s celou řadou virů a malwaru. Tato varianta je vhodná především pro méně zkušené uživatele, neboť v tomto případě částečně odpadá zjišťování, co se vlastně v počítači skrývá.

Standardní nabídku jednoúčelových utilit najdete i na webech Alwilu **(www.avast.com/eng/avast-virus-cleaner.html)** a Grisoftu. **(www.grisoft.com/ww.virus-removal)**. Poněkud komplikovanější způsob zvolila firma Eset, která na svém webu také nabízí antimalwarové utility **(www.eset.com/download/free-virus-remover.php)**. Zde si musíte nejprve zvolit správný nástroj, stáhnout ho a rozbalit (archiv ZIP), což není zrovna ideální řešení. Komplexní způsob zvolila Avira, která na svém webu **(www.avira.com/en/support/support_downloads.html)** nabízí nejen nástroj na odstranění vybraných virů a malwaru, ale také záchranné CD nebo nástroj na opravu registrů.

Zkrátka, nástrojů proti malwaru je více než dost, stačí si jen vybrat...

PETR.KRATOCHVIL@CHIP.CZ

NA CHIP DVD

Na Chip DVD najdete pod indexem Malware nejen článek „Test internetových skenerů" z Chipu č. 4, ale také nástroje od firmy Symantec proti třem nejrozšířenějším škůdcům:

W32.Mytob@mm

W32.Netsky@mm

W32.Mydoom@mm

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