Odstraňte špínu v počítači

V minulém čísle jsme vám představili nejlepší on-line skenery, které zčásti dokáží **ODSTRANIT INFEKCI** z libovolného počítače. Nyní vám poradíme, jak zatočit se zbytkem škůdců…

PETR KRATOCHVÍL

Odvirování počítače je ve většině případů náročná „operace“, a to jak z hlediska znalostí, tak z hlediska času. Problémem je, že část škůdců může být provázána se systémem, nebo se alespoň za systémové procesy vydávat. Jak tedy postupovat?

Zákeřní pomocníci

Nemalou část zavirovaných počítačů mají na svědomí „zákeřní pomocníci“ a falešný antimalware. V prvním případě jde o různé přehrávače, nástrojové lišty nebo jiné „pomocníky“, které si uživatel do počítače nahraje v dobré víře, že jde o neškodné utility. Druhou variantou jsou škodlivé programy vydávající se za nástroje proti škůdcům (často bývají označovány jako rogue antispyware). Informace o nich najdete na celé řadě stránek, k těm lepším patří námi již několikrát zmiňovaný web Spyware Warrior (**www.spywarewarrior.com/rogue_anti-spyware.htm**).

Jedno však mají obě kategorie programů společné: jakmile se dostanou na váš disk, začnou zde úřadovat. Deaktivují standardní ochranné prostředky Windows (firewall

a Windows Defender) a snaží se vyřadit z provozu i „externí“ bezpečnostní nástroje (antiviry, bezpečnostní balíky). Problém spočívá v tom, že jen málokterého takto nainstalovaného „falešného pomocníka“ lze odstranit antimalwarovými nástroji. Uživatel si ho totiž do systému nainstaloval sám (se všemi důsledky z toho plynoucími) a snaha odstranit ho nemusí být zcela bez postihu. Někteří autoři těchto zákeřných nástrojů měli dokonce tu drzost soudit se s jistou bezpečnostní firmou, která si „dovolila“ označit jejich program za malware...

Prvním krokem při dezinfekci počítače by mělo být odinstalování všech nežádoucích a podezřelých nástrojů. Počítejte s tím, že tyto programy nenabízí svoje odinstalování přímo v nabídce Start. Musíte se proklikat do Ovládacích panelů a nabídky Přidat nebo odebrat programy. Lišty a pomocníky v Internet Exploreru (pouze ve verzi 7) odstraníte přes nabídku »Nástroje | Spravovat doplňky | Povolit nebo zakázat doplňky«...

Nám se z testovacího počítače podařilo odstranit všechny tři „dobrovolně“ nainstalované škůdce, byť některé až na druhý pokus. Ve chvíli, kdy už jsou tyto problematické nástroje z počítače odstraněny, je čas na druhý krok.

Vyzbrojení

První část následující akce nebude neznámá všem milovníkům akčních filmů – důkladné vyzbrojení. Na rozdíl od Arnolda Schwarzeneggera a jeho „nákupu“ bagrem v obchodě se střelnými zbraněmi vám bude stačit na-

On-line skenery pomohou jen zčásti...

hrát si na USB disk doporučené nástroje (nebo přímo použít Chip DVD) a k nim přidat instalaci libovolného antivirového nástroje nebo bezpečnostního balíku.

Poté se připojte k internetu a vyzkoušejte dva nebo tři on-line skenery. V ideálním případě nástroj od Esetu (**www.eset.cz /online-skener**), Bit Defenderu (**www.bitdefender.com/scan8/ie.html**) a od firmy Kaspersky (**www.kaspersky.com/virusscanner**). Je téměř jisté, že nástroje neodstraní všechen malware, ale v této fázi je důležité zjistit, kteří škůdci se na počítači skrývají a kde. Doporučujeme si seznam škůdců vytisknout, nebo alespoň exportovat do souboru pro pozdější kontrolu. Ve chvíli, kdy skenery dokončí svou práci, je ta pravá chvíle na experiment. Pokud se skenerům podařilo odstranit většinu nebezpečného malwaru, můžete zkusit na počítač nainstalovat antivir nebo bezpečnostní balík (třeba AVG 8 z Chip DVD). Jestliže se instalace zdaří, máte již zčásti vyhráno – okamžitě antivir aktualizujte a proveďte kontrolu počítače. Nástroj od renomované firmy by si měl bez problémů poradit s většinou škůdců.

Ve většině případů se však on-line skenerům podaří odstranit jen méně nebezpečné záškodníky, a ti, kteří zůstali, obvykle úspěšně blokují pokusy o nainstalování jakýchkoliv bezpečnostních nástrojů.

Stojí za zkoušku

Pokud tedy pokus o instalaci selhal, je ta pravá chvíle nasadit těžkou techniku. Prvním krokem by ale mělo být odpojení počítače od internetu (a sítě), což zabrání některým typům malwaru v aktivní obraně.

Prvním nástrojem, který doporučujeme použít, je KillBox. Postup je snadný: ze seznamu škůdců (získaných od on-line skene-

NAJDETE NA CHIP DVD

Nástroje proti malware

Killbox ► Nástroj, který dokáže ukončit běžící proces, nebo smazat systémem blokovaný soubor patřící malwaru.
Web autorů: **http://killbox.net/**

The Avenger ► Alternativa k programu killbox určená zkušenějším uživatelům. Program vykonává činnost, která je popsána pomocí skripů
Web autorů: **http://swandog46.geekstogo.com/**

HijackThis ► Utilita sloužící k získání komplexních systémových informací o počítači. Jeho výstup je v současnosti standardem v diskuzních fórech o malwaru.
Více informací: **www.spywareinfo.com**

Process Explorer ► Pokročilejší varianta správce úloh umožňující detekci malwarových procesů. Původně nástroj firmy Sysinternals, nyní k dispozici u Microsoftu.
Více informací: **http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx**

Spybot Search&Destroy ► Program nabízející jak detekci malwaru, tak i kvalitních ochranu. Dokáže počítač ochránit před známými škůdci a upozornit na změny v systému.
Více informací: **www.safer-networking.org**

► **NA DVD:** Programy pro tento článek najdete pod DVD indexem: **ODVIROVÁNÍ PC**

INFO

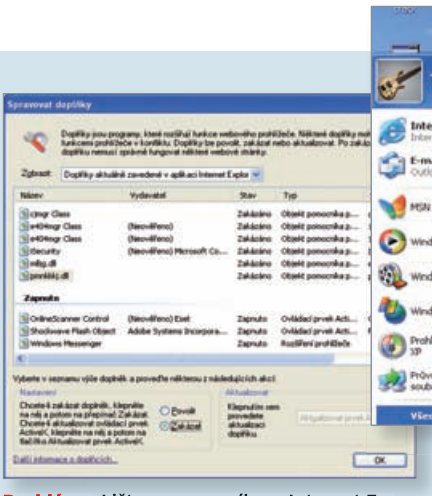
Dvakrát měř, jednou... maž

Zatímco Windows se snaží tvářit jako uživatelsky přítulný program a varují vás i před „odhozením“ souboru do koše, nástroje pro boj s malwarem si na nic nehrají. Jejich autoři předpokládají, že víte co děláte a nepovažují za nutné vás za „vodit za ruku“. Stačí jedno špatné rozhodnutí, jedno kliknutí vedle a místo odstranění malwaru „poškodíte“ operační systém. Proto víc než kdy jindy doporučujeme „konzultovat“ každý krok s „Googlem“. Pokud si nejste stoprocentně jisti, že soubor patří malwaru (a internetová diskuzní fóra také mlčí), raději soubor nemažte. Problémem je, že některé ze škůdců nedokáží odstranit ani známé bezpečnostní nástroje. To především proto, že téměř denně mění svou tvář – tedy „krycí“ jméno souboru a úkryt v systémovém registru.

Pokud si nevíte rady, zkuste poslat svůj log z programu Hijackthis do fóra na webu **www.viry.cz**, nebo nám napište do redakce.

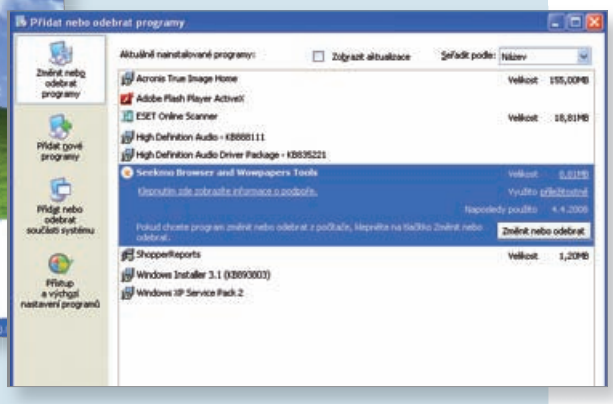
Přeinstalování Windows je sice obvykle účinná metoda vedoucí k odstranění malwaru, měla by být až posledním východiskem kdy všechny ostatní prostředky selžou...

ZDROJE INFORMACÍ A CENNÝCH RAD PRO ODSTRANĚNÍ ŠKŮDCŮ:
http://forum.chip.cz/
www.rootkit.cz/forum/



Problém: Lišty a pomocníky v Internet Exploreru lze snadno odstranit pouze ve verzi 7.

Test: Některé programy lze odebrat přímo z nabídky Start.



Pryč s nimi: Prvním krokem by mělo být odinstalování všech nežádoucích nástrojů.

rů) v KillBoxu vybírejte procesy (klikněte na »Processes>>>«) a soubory (kliknutím na žlutý symbol složky) a pokuste se je odstranit. Ve většině případů nebude stačit základní volba »Standard File Kill«, a to ani s použitím varianty spuštění Killboxu s administrátorskými právy »File | Run as System Task«. Zákeřnější malware se těmto pokusům o odstranění (obvykle úspěšně) brání. Mnohem úspěšnější bývají varianty »Delete on Reboot« a »Replace on Reboot + Use Dummy«. V těchto případech můžete označit více souborů (nebo procesů), které má program při restartu (nebo několika restartech) smazat.

V některých případech se však nepodaří KillBox ani spustit. S jeho rostoucí popularitou se bohužel určitý malware naučil tento praktický program blokovat. Tehdy je tedy nutné použít jeho alternativu.

Těžký kalibr

Relativní novinkou na poli boje proti malwaru je The Avenger. Zjednodušeně lze říci, že jde o alternativu k programu KillBox, určenou především zkušenějším uživatelům. Tomuto „zařazení“ odpovídají nejen rozsáhlejší schopnosti programu, ale především komplikovanější ovládání. Zde totiž nestačí jen klikat – program vyžaduje zadávání příkazů pomocí skriptů. Na internetu sice existuje několik stránek s předpřipravenými skripty, většina infekcí však vyžaduje individuální nastavení. Pomocí skriptů programu určíte, které soubory nebo drivery chcete odstranit či nahradit, a po restartu se o to program pokusí.

Jako bonus program nabízí detekci rootkitů, která je na velmi dobré úrovni (více se o rootkitech dozvíte v příštím čísle Chipu).

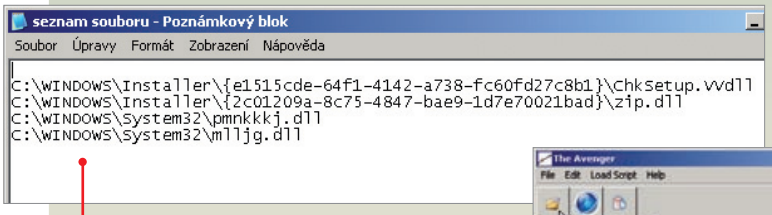
Posílení obrany

Nyní je ten správný čas nasadit další pomocníky. Následujícím krokem by mělo být nasazení programu Spybot. Po jeho nainstalování je nutné program aktualizovat a provést imunizaci. Ta zajistí, že by měl být uživatel varován před návštěvou nebezpečných stránek, rizikových domén nebo problematických plug-inů. Další výhodou

Program Spybot lze doporučit i pro obranu PC..

NÁVOD K POUŽITÍ

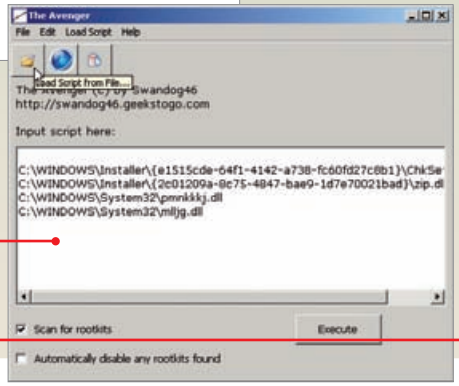
The Avenger

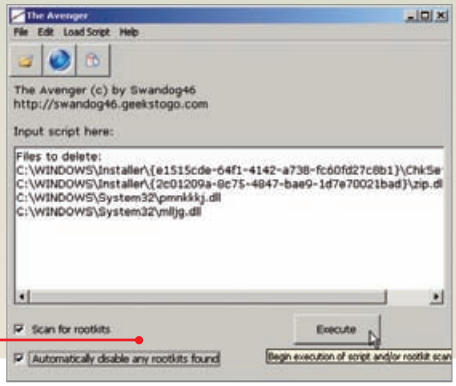


1 Vytvořte si seznam nežádoucích souborů, složek či driverů určených k odstranění a uložte si ho do textového souboru (musí mít příponu txt).

2 Klikněte na tlačítko »Load Script from file...« a vyberte textový soubor se seznamem souborů.

3 Před seznam souborů zadejte příkaz, který má program vykonat a klikněte na »Execute«.





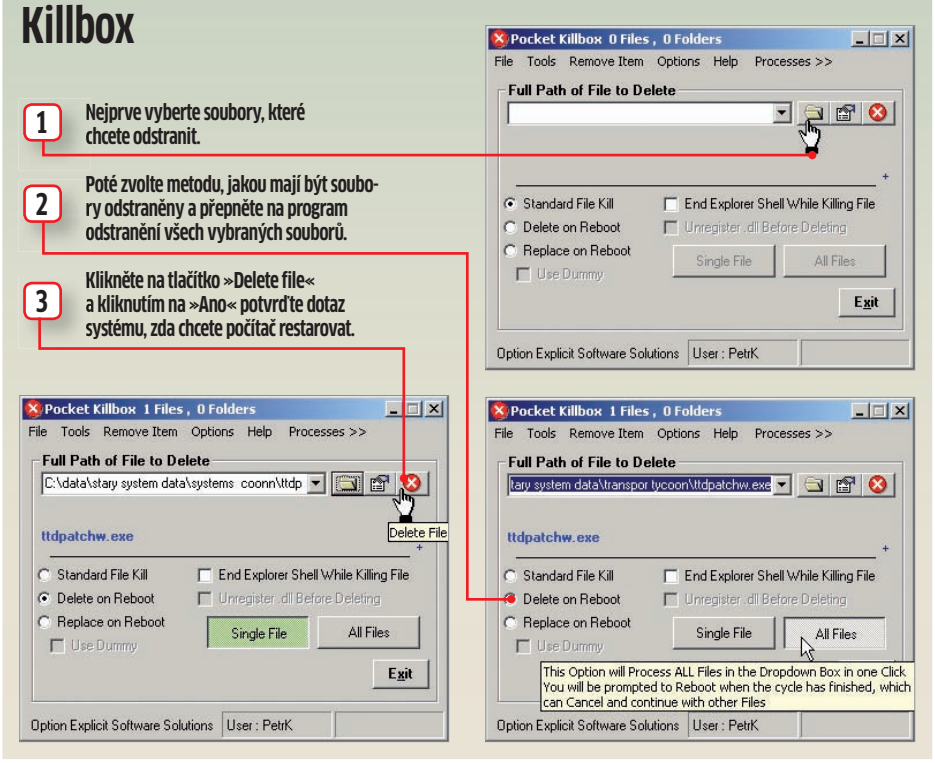
NEJPOUŽÍVANĚJŠÍ PŘÍKAZY JSOU:

Files to delete: (smaže zvolené soubory)
Folders to delete: (smaže zvolené složky)
Drivers to delete: (smaže zvolené ovladače
Registry keys to delete: (smaže zvolené klíče v registrech)

Podrobnější návod k programu najdete na webu Chipu v sekci Tipy a triky.

NÁVOD K POUŽITÍ

Killbox



programu je zabezpečení systémových nastavení – při pokusu o jejich změnu budete varováni.

Poté přepněte program do režimu pro pokročilé »Režim | Pro pokročilé« a v levé části programu přejděte do sekce Nástroje. V části ladění IE označte zatržítko u položky »Zamknout soubor Hosts, aby byl pouze pro čtení...«. Poté přejděte do sekce Neplatné registry a v horní části programu klikněte na »Zkontrolovat«. Po ukončení kontroly vyberte neplatné odkazy a zvolte »Opravit vybrané problémy«. Nakonec v sekci »Start systému« zkontrolujte, zda zde nezůstal nežádoucí program spouštějící se při startu počítače. Při této kontrole vám pomůže barevná nápověda programu:

ZELENÁ: Známé programy, nehrozí žádné riziko.

ŽLUTÁ: Neznámé nebo nejasné programy (za jménem systémového programu se může skrývat i malware).

ČERVENÁ: Malware nebo jiné nebezpečné programy.

Pokud nechcete, aby se vybraný program spouštěl při startu Windows, stačí zde zrušit zatržítko.

Jedním z posledních kroků (po restartu počítače) by měla být kontrola pomocí programu Process Explorer. Po jeho spuštění si dejte zobrazit seznam spuštěných procesů a zkontrolujte ho. V Process Exploreru se vám může podařit i odstranit i méně zákeřné škůdce. Nejprve vybrané škodlivé procesy uspěte příkazem Suspend, poté je ukončete příkazem Kill. Pokud narazíte na podezřelou položku, klikněte na ni pravým tlačítkem a zvolte »Search online...«. V implicitním prohlížeči se objeví výsledky vyhledávání. Při rozsáhlejší kontrole doporučujeme přímou návštěvu stránek **www.liutilities.com/products/wintaskspro/processlibrary/**, kde najdete většinu známých a důležitých procesů. Další zdoje informací o podezřelých procesech jsou také:

www.processlibrary.com
www.file.net/process/

Ruční práce

Po finální dezinfekci lze ještě doporučit kontrolu registrů: zkuste vyhledat, zda v registrech nezůstaly stopy po odstraněném malwaru. Finálním testem by mohla být instalace antiviru či bezpečnostního balíku – pokud instalaci nic nebrání, dá se předpokládat, že počítač bude „čistý“. Nemáte-li k dispozici žádný takový program nebo ho na počítač instalovat nechcete, zkuste alespoň provést test pomocí on-line skeneru. Posledním krokem by měla být kontrola případného výskytu rootkitů, o které se dozvíte více v příštím čísle.

PETR.KRATOCHVIL@CHIP.CZ