Nemilosrdně proti spywaru

Největší hrozby

Zákeřný spyware se ve vašem počítači zahnízdí jako vetřelec ze stejnojmenného filmu. Naší soustředěné palbě, kterou vám zde předvedeme, však neodolají ani ti nejvzdornější diverzanti.

Text: Valentin Pletzer, *autor@chip.cz*

Že svůj počítač chráníte antispywarovým programem, který pravidelně aktualizujete? V pořádku. A věříte, že jste tím imunní proti spywaru a rootkitům? Chyba lávky! Srovnávací test v předchozím článku totiž ukázal, že žádný z těchto programů neposkytuje dostatečnou ochranu. Pokud se o ni nepostaráte sami, bude váš počítač brzy infiltrován vetřelci, jakými jsou SpyFalcon a CoolWebSearch. A nezvaní hosté jsou čím dál tím rafinovanější.

Noční můra z Microsoftu

Už před delší dobou stvořil Microsoft v laboratoři ultimativní rootkit, nový rozměr malwaru. Na univerzitě v Michiganu vypěstovali vědci spolu s výzkumníky Microsoftu trojského koně „Subvirt“ – jeho maskovací technika je tak dokonalá, že dokonce i jeho samotní tvůrci měli potíže s jeho zpětným odhalením. Tento trojský kůň má jednu specialitu: Subvirt nahradí kompletní operační systém a jeho originál spustí v kontrolovaném virtuálním prostředí. Při bootování počítače se nejprve potají zavede trojský kůň, a až potom operační systém. A tak zatímco člověk poklidně pracuje ve svém jen zdánlivě netknutém světě Windows, ve druhém, virtuálním světě může nepozorovaně operovat trojský kůň – Matrix nechá pozdravovat. Antispywarové programy, které se zavádějí pod Windows, pak samozřejmě nemají sebemenší šanci.

Co nás nemine

Svůj „superrootkit“ sice vědci i Microsoft zatím drží pod pokličkou, je však jen otázkou času, kdy mazaní hackeři vyvinou svou vlastní variantu. Od té doby, co bylo pojednání o Subvirtu zveřejněno, o superrootkitu hojně a intenzivně diskutuje celá hackerská komunita. A to i přesto, že ani aktuální spyware a trojské koně využívající techniku rootkitů se už takřka nedají odhalit, a tím méně zlikvidovat. Je-li jimi počítač infikován, zbývá →

postiženému uživateli často jediné východisko: naformátovat pevný disk a nově nainstalovat Windows.

Problém má však ještě jiné řešení. Ukážeme vám je na příkladech nejrozšířenějších spywarových programů a rootkitů. Následující návody lze ovšem považovat pouze za konkrétní příklady, neboť cesty k souborům a položky v systémovém registru se mění prakticky denně. Přesto s našimi nástroji a tipy dokážete odhalit a odstranit dokonce i neznámý spyware.

ZATYKAČ: VANQUISH

Cesta infekce: různé

Škody: havárie počítače

Krycí názvy souborů: *různé (mj. vanquish.exe)*

Pomocné DLL soubory: *vanquish.dll*

Skrýše v registru:

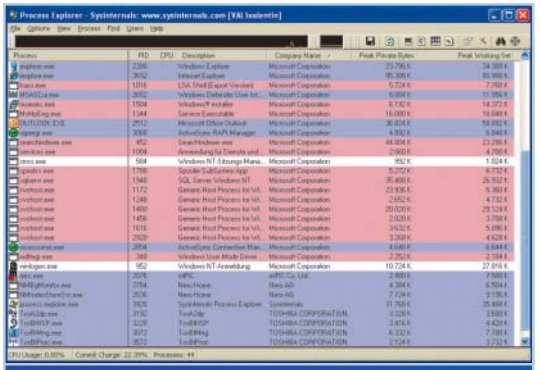
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SpyFalcon

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Vanquish

SPYFALCON

Odstranění falešného antispywaru

Na nejvyšší příčce pomyslného žebříčku nejdrzejších vetřelců dnes nepochybně stojí SpyFalcon – údajný antispyware, který je však ve skutečnosti spywarem. Na pochybných webových stránkách, například s ilegálními sériovými čísly, je návštěvníkovi nabízena kontrola počítače na přítomnost spywaru. Za tím účelem má uživatel spustit bezplatný skener SpyFalcon. Pokud tak učiní, obdrží zprávu, že jeho počítač je napaden. A je tomu skutečně tak – původcem však není údajně identifikovaný spyware, nýbrž samotný SpyFalcon. A zatímco program přebírá kontrolu nad počítačem, pokouší se pachatel naprosto bezostyšně svůj zcela bezcenný antispywarový nástroj dokonce ještě prodávat! Raději ani nedomyslet, co se pak stane s údaji z kreditních karet důvěřivých surfařů...



Lepší než od Microsoftu: Process Explorer poskytuje mnohem více informací a funkcí než Správce úloh ve Windows.

1. Rozpoznání spywaru

Dokud je aktivní třeba i jen jeden proces SpyFalconu, trojského koně z počítače nedostanete. Prvním a nejdůležitějším krokem při odstraňování jakéhokoliv malwaru je proto deaktivace procesů v operační paměti. Poněvadž Správce úloh ve Windows nemusí vždy ukázat všechny probíhající procesy, doporučujeme Process Explorer (*www.sysinternals.com*) – ten také používáme u všech tipů. Tento obohacený správce úloh totiž také disponuje užitečnými přídavnými funkcemi, které se při honu na malware mohou hodit.

Můžete tak po kliknutí pravým tlačítkem myši a volbě *Google...* vyhledat na internetu název podezřelého souboru a dozvědět se, jaký úkol soubor plní. Pod jakými názvy spustitelných (exe) souborů se SpyFalcon takto ukrývá, se dozvíte z jeho „zatykače“. Důležitá poznámka: Poněvadž se trojský kůň průběžně proměňuje, mohou k seznamu přibýt názvy další. Ve virových lexikonech jako např. *www.2-spyware.com* a téměř u všech výrobců antivirových programů najdete aktuální seznamy spywarem a trojskými koňmi používaných názvů souborů.

2. Ukončení procesů

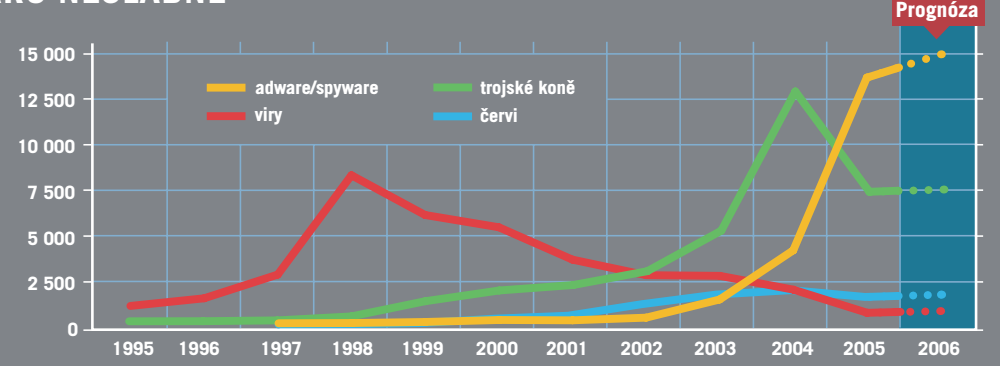
Nejlepší a nejjednodušší cestou, jak eliminovat spywarové procesy, je nastartovat PC z bootovatelného CD či DVD a pak soubory a položky registru odstranit. Pokud takový disk po ruce nemáte, v Process Exploreru nejprve všechny spywarové procesy přerušte kliknutím pravým tlačítkem myši a volbou *Suspend*, abyste je pak mohli jeden po druhém eliminovat dalším kliknutím pravým tlačítkem a aktivací *Kill Process Tree*. Bez okliky přes *Suspend* by se mohlo stát, že jakmile byste ukončili první proces, druhý spywarový proces by jej znovu oživil. V režimu „suspend“ je totiž proces sice pozastaven, není však považován za deaktivovaný.

3. Odstranění souborů

Jakmile z operační paměti zmizí všechny spywarové procesy, v dalším kroku je třeba vymazat všechny soubory SpyFalconu. Jen tak lze zabránit opětovnému spuštění procesů. Tyto soubory najdete většinou v adresářích *C:\Program Files\SpyFalcon* a *C:\Windows\System32*. Pro jistotu byste však měli

PŘÍVAL SPYWARU NESLÁBNE

Dramatický nárůst: Spywarových napadení přibývá, klasických virů ubývá, trojské koně setrvávají na vysokých hodnotách. Počet nových červů zůstává na stejné úrovni jako v minulých letech.



BEZPEČNOSTNÍ „SUPERSOUPRAVA“ CHIPU

Jestliže se Windows jednou osvobodí od malwaru, mělo by to tak zůstat i nadále. S naším bezpečnostním balíkem to také není žádný problém. Sedm nástrojů, které jsme do něj zahrnuli (na Chip DVD), už nedá šanci k infikování vašeho počítače ani obávanému „superrootkitu".

F-Secure Antivirus: Dobré nástroje odhalí nejen viry, ale také spyware. Patří k nim i skener od F-Secure. Tento hlídač ihned kontroluje každý nový soubor, a blokuje dokonce i rootkity.
www.f-secure.com

Kerio Firewall: Ačkoliv firewall nepředstavuje žádnou neproniknutelnou hráz, nainstalovat byste si jej měli. Běžným útokům čelí bezplatný firewall firmy Kerio tak dobře jako snad žádný jiný.
www.sunbelt-software.com

Spamihilator: Internetová mafie se pokouší ukrást vaše data i prostřednictvím e-mailu. Těm nejhorším útokům zabrání Spamihilator. Je nezávislý na poštovním programu, ovládá všechny protokoly a dá se dále vylepšovat pomocí plug-inů.
www.spamihilator.com

Privoxy: Reklamní „pop-upy" nepředstavují ve většině případů žádné nebezpečí, dokážou však pěkně otrávit. I přes blokování integrované v prohlížečích nacházejí stále nové cesty, jak se vnutit vaší pozornosti. I těm nejzarputilejším dotěrům však Privoxy učiní přítrž.
www.privoxy.org

Adblock: Nejčastějším objektem útoků spywaru je Internet Explorer. Používejte proto raději Firefox. Adblock jako filtr ohlídá, aby se malware vůbec nezavedl. Díky tomu si počítač nemůžete „zaneřádit" ani omylem.
http://adblock.mozdev.org

Process Explorer: Na kvalitní detekci a likvidaci spywaru „palubní“ prostředky Windows nestačí. Řešním je Process Explorer.
www.sysinternals.com

Killbox: Metody spywaru jsou čím dál tím záludnější. Jakmile ukončíte jeden proces, jiný jej znovu nastartuje. S tím však rázně skoncuje Killbox.
www.killbox.net

prohledat celý pevný disk, zda se v něm nevyskytují spywarové DLL soubory.

Kromě toho ještě vymažte DLL soubory, abyste tak z počítače odstranili kompletní spyware. Aby chybějící DLL soubory později nevyvolávaly chybová hlášení, musíte je ještě před odstraněním odhlásit z Windows. Chcete-li například odhlásit soubor *C:\Windows\System32\appmagr.dll*, prostřednictvím *Start | Spustit | cmd* vyvolejte režim příkazového řádku a v něm se příkazem *cd c:\windows\system32* přepněte do uvedeného adresáře. Odhlášení pak zařídí příkaz

```
regsvr32 /u appmagr.dll
```

V dosovém okně hned také můžete příkazem *del appmagr.dll* soubor odstranit. Lze to ale samozřejmě učinit i v Průzkumníku.

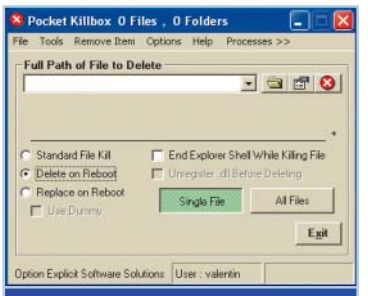
Další soubory SpyFalconu (typu INI a dočasné), které sice nejsou nebezpečné, ale zbytečně zabírají místo na pevném disku, jsou pojmenovány *ld????.tmp*, *hp????.tmp* a *sf.ini*, kde *????* znamená libovolnou čtyřmístnou kombinaci znaků.

4. Vyčištění registru

Zbývá už jen vymazat záznamy SpyFalconu ze systémového registru, a Windows budou skoro jako nová. Prostřednictvím *Start | Spustit | regedit* proto vyvolejte editor registru a v něm položky, které najdete v našem „zatykači“ na SpyFalcon, po kliknutí pravým tlačítkem myši vymažte volbou *Odstranit*.

Samá lež: Údajně antispywarový program SpyFalcon je ve skutečnosti sám drzým datovým špionem.

Zlý bratr Googlu: Stránka vyhledávače CoolWebSearch se stala podnětem pro vznik zvláště podlých trojských koní.



Jistý výmaz: Zarputilé spywarové soubory nejlépe zlikvidujete nástrojem Killbox a následným restartem počítače.

COOLWEBSEARCH

Blokování pornografických pop-upů a hijackerů

Stačí neopatrné kliknutí na hackerské webové stránce, a vládu nad vaším prohlížečem převezme trojský kůň. Snad nejznámějšími „únosci browseru“ jsou trojské koně označované jako CoolWebSearch (nebo jen zkratkou CWS), které se do počítače vetřou skrze Internet Explorer. Jakmile se v něm jednou zahnízdí, začnou měnit domovskou stránku prohlížeče, otevírat pornografická vyskakovací okna a pozměňovat oblíbené položky. Z obyčejného vyhledávání se stanou muka, neboť namísto Googlu nebo Yahoo se pokaždé ocitnete na stránce CoolWebSearch.

A co za tím vězí? Vyhledávač CoolWebSearch nabízí peněžitou odměnu každému, kdo na jeho stránku přiláká další uživatele. Tam je ovšem návštěvník bombardován spamovými odkazy, jimiž si CoolWebSearch vydělává na živobytí. Hackeři, kteří chtějí na nabídce CoolWebSearch zbohatnout, proto vyvinuli nesčetné trojské koně, jimiž co nejvíce surfařů donucují k návštěvě této stránky.

1. Rozpoznání hijackeru

Podobně jako v případě SpyFalconu je nejlepší obranou proti CoolWebSearch rychlé rozpoznání a zrušení →

aktivních procesů. Je tu však problém: CWS se brání deaktivaci všemi prostředky a samotný Process Explorer na takový úkol nestačí. Je proto nutno se uchýlit k malému triku: Nástroj „Killbox“ nevymaže zatvrzelé soubory ihned, nýbrž až při příštím restartu počítače. Které soubory máte prostřednictvím Killboxu (*www.killbox.net*) odstranit, to se dozvíte v „zatykači“ na CoolWebSearch a pomocí Process Exploreru. Abyste nemuseli zkoušet více procesů, než je nutné, měli byste však nejprve uzavřít co nejvíc aplikací. Platí to i pro programy, které se skrývají v pravé části hlavního panelu Windows (označovaném také jako „tray“).

Dále si musíte sestavit seznam spywarových souborů. Spusťte proto Process Explorer a všechny zavedené programy zkontrolujte po kliknutí pravým tlačítkem myši pomocí *Properties*. Pozor! Nedejte se zmást například popisem (Description) a výrobcem (Company Name), neboť právě tyto údaje hackeři často falšují. Proces je skutečně bezpečný jedině tehdy, je-li opatřen platným certifikátem. Prověřte proto soubor tlačítkem *Verify*. Je-li jeho certifikát platný, vedle ikony souboru se objeví (Verified) a popis výrobce. Eventuální zpráva „Unable to verify“ však bohužel nic nevypovídá o tom, zda se jedná skutečně o škodlivý program, nebo jen o pouhé konstatování, že se ověření neuskutečnilo – což se týká skoro každého nevinného freewaru.

ZATYKAČ: COOLWEBSEARCH

Cesta infekce: Internet Explorer

Škody: pop-upy a špionáž

Krycí názvy souborů:
services.exe, DownloaderEXE.exe, tmksrvu.exe

Další soubory: *update911.js, DNLDC.ocx, SexDownloader.cab*

Pomocné DLL soubory: *iekp32.dll, image.dll, mshp.dll, mslq32.dll, mssearch.dll, xplugin.dll*

Skrýše v registru:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Image

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Image

Další informace o původu souboru prozradí Process Explorer údajem o cestě k souboru (Path). Zvláštní pozornost byste přitom měli věnovat souborům v adresáři *C:\Windows\System32*. Právě tam totiž sídlí velmi mnoho systémově kritických souborů – skvělý úkryt pro spyware všeho druhu. Nejste-li si u některého souboru jisti, měli byste si jeho název vyhledat na Googlu, anebo si na některé speciální webové stránce, jako jsou *http://whatisthatfile.com* a *http://virusscan.jotti.org*, zjistit, zda se nejedná o spyware.

2. Odstranění souborů

Po sestavení seznamu spywarových souborů nastupuje do akce Killbox. Zvolte v něm *Delete on Reboot* a *All Files* a do pole *Full Path of File to Delete* zadejte název souboru včetně kompletní cesty. Obsluha nástroje je však poněkud nestandardní, a proto vám pro přidávání souborů doporučujeme v programu používat ikonu složky. Pokud byste do výmazového seznamu přidali nějaký soubor omylem, k jeho odebrání stačí klávesa *Delete*.

Pro odstranění vybraných souborů nyní klikněte na ikonu s červeným symbolem výmazu. Jakmile budou takto zlikvidovány všechny soubory CWS, je spyware deaktivován a zbývá už jen odstranit zbylý „datový šrot“. Restart počítače zařídí Killbox automaticky.

3. Úklid pozůstatků

Podobně jako u SpyFalconu zbudou po odstranění procesových souborů v počítači ještě DLL soubory a položky v systémovém registru, které zbytečně zabírají místo a rovněž by měly být odstraněny. DLL soubory je i zde nutno předem odhlásit – zařídí to příkaz

```
regsvr32 /u soubor.dll
```

Poté už můžete DLL vymazat. V „zatykači“ najdete ještě tři další soubory, které CWS založil a které můžete odstranit bez speciální přípravy. Položky v registru už po ukončení spywarových procesů také nepředstavují žádný problém – vymažte je obvyklým postupem v editoru registru.

VANQUISH

Odhalení a výmaz nebezpečných rootkitů

Na specializovaných webových stránkách si hackeři zcela legálně a otevřeně vyměňují rootkity a triky, jejichž pomocí se záškodnické programy jako spyware mohou vplížit do počítače i přes přítomnost bezpečnostního softwaru. Jak se takového malwarového narušitele zbavit, to si nyní ukážeme na příkladu mezi hackery velice oblíbeného rootkitu „Vanquish“.

1. Rozpoznání rootkitu

Rootkity narušují funkce počítače, pozměňují části operačního systému a falšují odpovědi na různé dotazy. Programům jako Správce úloh, Process Explorer nebo Tento počítač se pak rootkitem chráněný malware nedaří odhalit. Proto byly vyvinuty speciální nástroje jako „Blacklight“ (*www.f-secure.com*) nebo „RootkitRevealer“ (*www.sysinternals.com*), které k vyhledávání kompletně používají vlastní prostředky, a to, co najdou, porovnají s tím, co zjistil operační systém. Soubory, které Windows neobjeví, jsou pak soubory patřící k rootkitu. Například Vanquish při standardním nastavení zatají každý soubor, jehož název obsahuje slovo „vanquish“.

2. Odstranění

Nástroj RootkitRevealer od Sysinternals ukáže zatajené soubory a zápisy v registru. Poněvadž se však aktivní procesy rootkitu nedají ukončit, stejně jako už u výše zmíněného trojského koně CoolWebSearch je opět nejlepší použít Killbox. Kromě toho byste příkazem *regsvr32 /u* také měli všechny DLL soubory rootkitu odhlásit z operačního systému, a to dříve, než je definitivně odstraníte.

3. Ověření

Rootkit a malware mohou podle okolností operovat navzájem nezávisle. Odstraníte-li tedy samotný Vanquish, ještě to zdaleka neznamená, že jste se automaticky kompletně zbavili infiltrovaného trojského koně či spywaru. Alespoň však už nejsou chráněny rootkitem. Proto po odstranění rootkitu ještě počítač proskenujte nějakým antivirovým programem, jako je například F-Secure Antivirus, a pak se s Process Explorerem vydejte na lov neobvyklých souborů.

ZATYKAČ: SPYFALCON

Cesta infekce: download

Škody: havárie a krádeže dat

Krycí názvy souborů: *atmclk.exe, domcfg.exe, dfrgsrv.exe, mscornet.exe, mssearchnet.exe, nvctrl.exe, spyfalcon.exe*

Další soubory: *update911.js, DNLDC.ocx, SexDownloader.cab*

Pomocné DLL soubory: *bolnyz.dll, dxmpp.dll, fyhhxw.dll, ginuerep.dll, higjxe.dll, htey.dll, iqzv.dll, oerucu.dll, oqipt.dll, reglogs.dll, sbnudh.dll, twain32.dll, ulztc.dll*

Skrýše v registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SpyFalcon

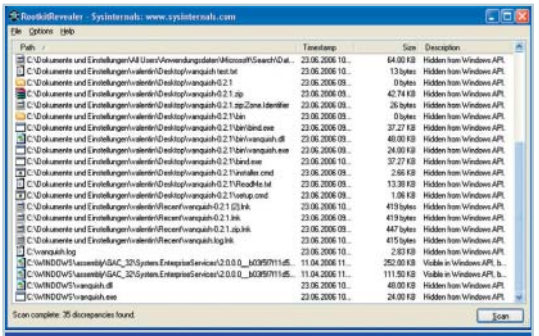
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ExplorerSharedTaskScheduler\{D1A2E7CD-F5C1-21A8-CA2C-13D0AC72D19D}

HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{D1A2E7CD-F5C1-21A8-CA2C-13D0AC72D19D}

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{244B730E-D899-4E38-9428-03D1143242E0}

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AppManagement\ARPCache\SpyFalcon

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SpyFalcon



Neviditelné: Trojské koně a spyware učiní opravdu nebezpečnými teprve rootkity, neboť je v počítači zamaskují tak, že je Správce úloh neobjeví. Pachatele však odhalí například RootkitRevealer.

SUBVIRT

Obrana před budoucím „superrootkitem“

Zatím je „superrootkit“ Subvirt ještě bezpečně uzavřen v laboratoři. Jakmile však byla jeho myšlenka zveřejněna, začali se zlí hackeři snažit o napodobení této techniky. Naštěstí pro potenciální oběti je ale velmi nesnadné a časově náročné tento druh rootkitu naprogramovat. Přesto je jen otázkou času, než se to někomu podaří. Abychom na to byli připraveni, již dnes se diskutuje o obranných opatřeních.

1. Rozpoznání „superrootkitu“

Největší výzvou pro obranné týmy bude nepochybně detekce záškodníka. Vzhledem k neobvyklému způsobu fungování Subvirtu se žádná cesta neobejde bez zavedení alternativního operačního systému – například Windows PE nebo Knoppixu. Z takového bezpečného a čistého systému pak lze kompletní pevný disk zkontrolovat různými virovými skenery a profesionálními nástroji, jako jsou diskové editory.

Příklad: Zavedl Bootmanager skutečně NT Bootloader a s ním Windows XP, nebo snad byla vyvolána nějaká jiná bootovací rutina? Pokud ano, začíná lopotná práce. Která data diverzant zavedl a kde jsou uložena? Při pátrání po rootkitu mohou hodně pomoci kontrolní součty každého souboru „čistého“ systému. Později, až se vypravíte na „odchyt“ vetřelce, porovnáte uložené kontrolní součty s aktuálním stavem. Pokud rootkit nějaký soubor změnil, lze to tímto trikem poznat. U souborů, které přibyly později, to ovšem nepomůže.

2. Odstranění

Vymazání „microsoftského“ rootkitu naštěstí nepředstavuje větší problém než u ostatních běžných rootkitů: jakmile jsou jednou všechny nebezpečné soubory identifikovány, lze je odstranit zcela normálně. Neobvyklé je jedině to, že podobně jako u bootviru je třeba opravit bootsektor. To lze ovšem provést velmi snadno díky automatické opravné funkci v instalaci XP. ■ ■ ■