Málokomu přijde zábavné spouštět Správce úloh a zkoumat tu kupu záhadně pojmenovaných procesů, běžících na počítači. Pokud si vůbec nevíte rady, pak je možné položit si otázku, kolik spuštěných procesů je skutečně nezbytných pro práci, kterou na svém počítači právě děláte. Nebo jinak: zda neběží nějaký proces, který nějakým způsobem dělá neplechu.

Odhalujeme nebezpečné programy

Identifikujte malware skrytý v systémových složkách Windows! (CD)

DAVID ČEPIČKA, ANDREW BRANDT

Bohužel jen velmi málo z nás má jiné než povrchní znalosti o tom, co se děje uvnitř operačního systému Windows. Většinou se spokojíme s tím, že pokud nějaký program spustíme, tak jednoduše běží, a pokud spustíme další programy, tak ve Windows běží paralelně vedle sebe.

V tomto článku se pokusíme objasnit způsob, jak identifikovat většinu systémových souborů Windows (a jak objevit neznámé soubory), takže budete moci snadno odlišit procesy neškodné a naopak užitečné od těch, které vám škodí. Rovněž vám prozradíme, jak sledovat běh každé aplikace spuštěné na vašem počítači, včetně nejnovější hrozby, která se nyní objevila – těmi jsou skryté soubory programů umožňující napadení a následné využívání počítače útočníkem – tzv. *rootkity*.

Samozřejmě podobně jako například u přírodních katastrof ani v tomto případě nemůžete nikdy přesně vědět, kdy nebo kde se v operačním systému objeví nová bezpečnostní trhlina, která dokořán otevře bránu do vašeho systému a umožní doslova vykradení dat z vašeho počítače. Dokonce ani když používáte firewall, aktualizovaný antivir a antispywarový program, pečlivě provádíte stahování a instalaci všech bezpečnostních záplat, nejste spolehlivě chráněni před nejnovějšími a nejrafinovanějšími škodlivými programy.

Antiviry a ostatní utility na ochranu vašeho počítače se musí skutečně co nejčastěji aktualizovat co možná nejdůkladnějšími updaty, aby skutečně pracovaly účinně, přesto však nezachytí nákazu, kterou ještě nikdy nepoznaly. Jinými slovy, největší nevýhodou těchto programů je vždy určité „mrtvé" období, které uplyne mezi tím, kdy se na internetu objevil a rozšířil například nový červ, a dobou, kdy se objeví nové definice pro antivirové programy, které tuto nákazu odstraní. Zda je toto „mrtvé" období záležitostí několika minut či dní, je při těchto úvahách asi jedno, protože vrátka pro průnik do systému se budou stejně otevírat vždy s objevením nové nákazy a zavírat s vydáním záplaty tuto nákazu postihující.

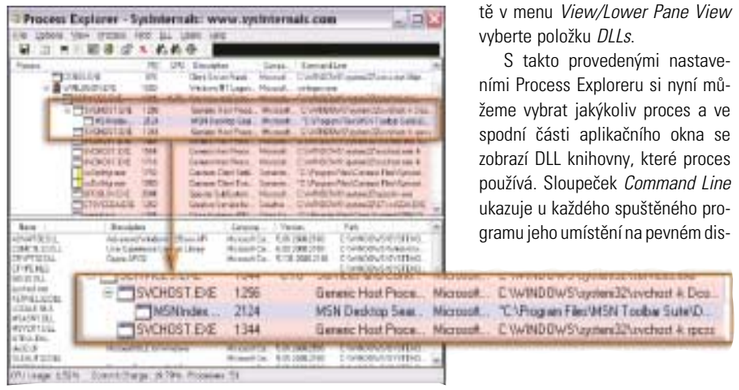
Na druhou stranu pokud je malware identifikován, je jeho odstranění obvykle docela jednoduché, třebaže velmi únavné. Proto pokud se budete řídit postupy pro detekci malwaru, uvedenými v tomto článku, pak váš počítač bude dozajista vždy v dobré kondici.

Bezpečnost především

Prvním a nejdůležitějším pravidlem, které si musíte zapamatovat, je to, že na počítači máte nainstalovaný operační systém, takže nemůžete jednoduše projít složky se systémovými soubory a ty, které se vám nějakým způsobem nezdají, smazat. Pokud byste takto postupovali, pak se snadno stane, že svůj počítač již příště nespustíte.

Za druhé, před každým důležitým krokem si nejprve udělejte zálohu operačního systému pomocí nástroje **Obnovení systému**. Zmíněný nástroj, který je k dispozici ve Windows ME a XP, spolehlivě vrátí operační systém do stavu před provedením případné změny, která se neukázala jako šťastná. Nástroj spustíte pomocí nabídky *Start/Programy/Příslušenství/Systémové nástroje/Obnovení systému*. Po spuštění programu vyberete možnost *Vytvořit bod obnovení* a následně se budete řídit pokyny průvodce. Nový bod obnovení pak vytvořte před provedením každé významnější změny v operačním systému.

Pravděpodobně budete potřebovat, aby se v systému zobrazovaly standardně skryté systémové soubory. To zařídíte tak, že spustíte program Průzkumník Windows, zde v menu *Nástroje* klepnete na položku *Možnosti složky* a přesunete se na záložku *Zobrazení*. Zde umístěte zatržítko před položku *Zobrazovat skryté soubory a složky* a ujistěte se, že naopak nejsou aktivní položky *Skrýt příponu souborů známých typů* a *Skrýt chráněné soubory operačního systému (doporučeno)*. Pokud se zobrazí nějaké dialogové okno, vyžadující potvrzení některé z prováděných akcí, stiskněte tlačítko *Ano* (o dalších varováních bude řeč později). Nyní spusťte aktualizovaný antivirový a antispywarový program. Nakonec případně smažte soubor, o němž jste si takřka stoprocentně jisti, že je součástí nějaké malwarové infekce. Nepoužívejte ale například následující postupy pro odstranění starých DLL souborů ze systémových složek.



▲ **Process Explorer pomůže identifikovat programy asociované s procesy běžícími ve vašem počítači.**

Zjistěte, které procesy jsou spuštěny

Nyní jste připraveni k tomu, abyste zjistili, které programy a procesy máte na svém počítači právě spuštěny. Aplikace *Správce úloh systému Windows* bohužel nedokáže zobrazit úplně všechny běžící procesy a aplikace, proto musíte použít program jiný. Velmi vhodným je například zdarma dostupný **Process Explorer**, který naleznete na internetové adrese **www.sysinternals.com/Utilities/ProcessExplorer.html**, popř. NA NAŠEM CD jako soubor PROCESSEXPLORERNT.ZIP o velikosti 553 KB.

Není nutná instalace, stačí pouze rozbalit soubor archivu a poklepat na soubor PROCEXP.EXE. Process Explorer je skutečně velkolepou náhradou Správce úloh. Možná se někomu nemusí jeho vzhled zamlouvat, nicméně je to program velmi spolehlivý a účinný. A navíc je dostupný zdarma.

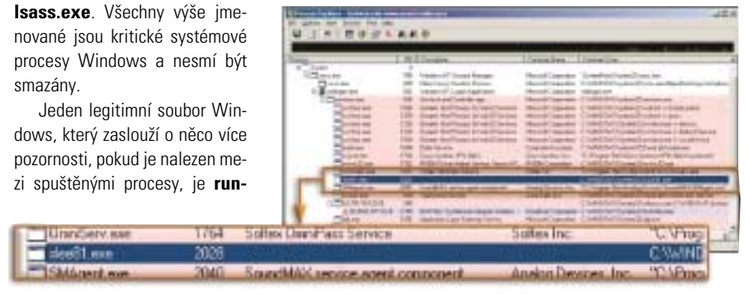
Řada informací, které může Process Explorer poskytnout, je však standardně skryta. Pokud je chcete zobrazit, klepněte pravým tlačítkem myši na název sloupečku a z kontextového menu vyberte příkaz *Select Columns*. Položky *Process Name* i *Description* by měly být zatrženy vždy, ale ujistěte se, že jsou aktivní i položky *Company Name* a *Command Line*. Nyní se přesuňte na záložku *DLL*, zkontrolujte, že je zatržena položka *Path* a stiskněte tlačítko *OK*.

Nyní se přesuňte do menu *View* a ověřte, zda je aktivní volba *Show Lower Pane*. Nakonec ještě v menu *View/Lower Pane View* vyberte položku *DLLs*.

S takto provedenými nastaveními Process Exploreru si nyní můžeme vybrat jakýkoliv proces a ve spodní části aplikačního okna se zobrazí DLL knihovny, které proces používá. Sloupeček *Command Line* ukazuje u každého spuštěného programu jeho umístění na pevném disku, nebo v případě spuštěných procesů (jelikož některé běží pod procesem **svchost.exe**) identifikuje, která instance procesu **svchost.exe** tuto službu používá.

Všechny procesy, jejichž cesta ukazuje do dočasné složky *Temp*, by vás měly okamžitě upozornit, že něco zřejmě nebude v pořádku. Spyware má totiž tendenci se sám instalovat a spouštět z takových nestandardních umístění, jako je právě složka *Temp*. Podobně pokud nějaký spuštěný proces ukazuje na DLL knihovnu ve složce *Temp*, pak je opět třeba se mít na pozoru. Jedinou možností, kdy může být nějaká aplikace či proces spuštěn ze složky pro dočasné soubory, je případ, kdy instalujete nějaký program, který používá instalátor, například *InstallShield*. Kromě procesu **Explorer.exe** pravděpodobně uživatelé Windows XP naleznou ještě i jiné běžící procesy jako například **smss.exe**, **winlogon.exe**, **services.exe**, **alg.exe** či **lsass.exe**. Všechny výše jmenované jsou kritické systémové procesy Windows a nesmí být smazány.

Jeden legitimní soubor Windows, který zaslouží o něco více pozornosti, pokud je nalezen mezi spuštěnými procesy, je **rundll32.exe**. Některé druhy malwaru, rozšiřované jako soubory DLL, se skrývají právě tím, že tento program používají jako příslovečný odrazový můstek. Správce úloh ukáže pouze to, že běží program **rundll32.exe**, ovšem Process Explorer vám zobrazí i to, s jakou DLL knihovnou je **rundll32.exe** asociován. Mějte však neustále na paměti, že některé ovladače zařízení používají **rundll32.exe** pro naprosto legitimní účely, a proto dříve než takový proces ukončíte, ujistěte se, že je skutečně nežádoucí. Název složky na konci cesty k souboru by vám měl poskytnout dostatek informací o legitimnosti tohoto procesu.



▲ **Sloupeček Command Line v programu Process Explorer vám prozradí, kde se na pevném disku nachází soubor odpovídající spuštěnému procesu. Tento údaj vám pomůže v případě, kdy ve sloupečku Description chybí popis procesu.**

Identifikujte záhadné procesy

Na vašem počítači pravděpodobně běží několik programových souborů systému Windows a kromě nich je na pozadí spuštěno několik souborů aplikací a služeb, včetně ovladačů vašich hardwarových komponent. Tyto soubory se za normálních okolností spouští při startu Windows. Prozkoumejte pro každý spuštěný proces v Process Exploreru údaje ve sloupečcích *Description*, *Company Name* a *Command Line*. Na základě těchto údajů byste měli být schopni identifikovat většinu programů, s nimiž jsou spuštěné procesy asociovány. Názvy programů by měly odpovídat programům, které máte na počítači nainstalované nebo které již byly na počítači předinstalovány.

Pokud výrobce softwaru neimplementoval do svého programu položky, které se zobrazují ve sloupečcích *Description* anebo *Company Name*, budete se muset pustit do podrobnějšího testování. Klepněte pravým tlačítkem do seznamu procesů v Process Exploreru a z kontextového menu vyberte příkaz *Properties*. Pokud si budete nad informacemi na záložce *Image* příliš dlouho lámat hlavu, klepněte na záložku *Services* (tato záložka je přístupná pouze u procesů). Tady uvidíte seznam některých legitimních služeb, které jsou s tímto procesem spojeny.

Například na obrázku Process Explorer ukazuje, že na našem počítači běží dva procesy, u nichž chybí popis ve sloupečcích *Description* a *Company Name*. Jedním z nich je SLEE81.EXE. Pokud se podíváme na záložku *Services*, je tento soubor identifikován jako **Steganos Live Encryption Engine**. Vzpomínáme si, že jsme software od Steganosu skutečně nedávno instalovali, takže není žádným překvapením, že některou z jejích komponent nyní nacházíme běžet na pozadí. Tady se nejedná o žádné bezpečnostní riziko, ovšem pokud šifrování a dešifrování souborů pomocí Steganosu nepoužíváme, lze uspo-

Rootkity aneb jak na skrytý malware

Další zastávkou na naší pouti za tajemnými procesy běžícími na našem počítači bude zcela nový typ malwaru, nazývaný *kernel-level rootkit. Rootkity* jsou utility, které dovolí hackerům pronikajícím do systému skrýt na napadeném počítači po sobě všechny stopy (a soubory), takže uživatel vůbec nepozná, že se na jeho systému vůbec nějaký malware vyskytuje. Hackeři následně pomocí rootkitů pak počítač ovládnou a mohou si na něm dělat doslova co chtějí. Naštěstí existuje několik programů, které nám pomohou tyto velmi nebezpečné soubory rozpoznat a v jednom případě i odstranit.

Jednou z nejschopnějších aplikací, jež v současnosti prakticky nemá konkurenci, je **RootkitRevealer** od firmy **Sysinternals**, který v systému vyhledává soubory a klíče registru, jež by mohly být nějakým způsobem navázány na rootkity. Vyhodnocení skenování RootkitRevealeru není sice triviální a musíme upozornit na to, že ne všechny položky, které utilita odhalí, jsou nutně malware. V rámečku **Nová utilita pro odhalení rootkitů a skrytých programů používaných hackery** se dozvíte několik důležitých informací o tom, jak utilitu používat a na jakém principu vlastně funguje. Program naleznete NA NAŠEM CD, popřípadě je ke stažení na internetové adrese **www.sysinternals.com/Utilities/RootkitRevealer.html** jako soubor ROOTKITREVEALER.ZIP o velikosti 181 KB.

Další velmi jednoduchou utilitou je **BlackLight** od firmy **F- Secure**, která je známa především antivirovými programy. Nyní svoje znalosti vložila do vývoje vyhledávače rootkitů, který rovněž dokáže najít a odstranit rootkity na pevném disku. Ačkoliv je jeho design poněkud strohý, o to více je v boji proti rootkitům účinnější. Utilita je určena pro Windows 2000, XP a 2003 a je ve stadiu betaverze k dispozici zdarma NA NAŠEM CD, popř. na **www.f-secure.com/blacklight** jako soubor BLBETA.EXE o velikosti 613 KB.

řit čas procesoru a službu vypnout, dokud ji nebudeme potřebovat.

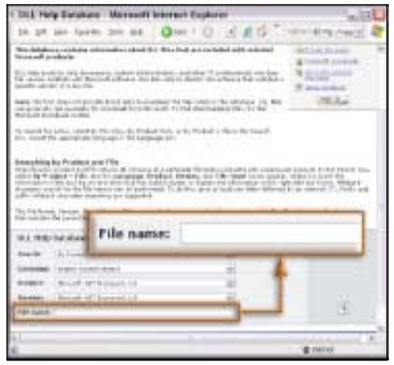
Druhým souborem bez popisu je WLTRYSVC.EXE. Jeho odhalení je však prostřednictvím záložky *Services* ještě jednodušší. Vzhledem k tomu, že jméno procesu (*WLTRYSVC service*) není o tolik jasnější než samotný název souboru, je přímo pod ním odsazený ještě jeden soubor, což znamená, že WLTRYSVC volal ještě jednu aplikaci s názvem BCMWLTRY.EXE. Tento soubor je identifikován jako **Broadcom Wireless Network Tray Applet**, o němž si vzpomínáme, že jsme jej instalovali, aby nám ukazoval sílu signálu bezdrátové sítě Wi-Fi. Vzhledem k tomu, že připojení pomocí Wi-Fi používáme často, rozhodneme se tento proces nechat nadále spuštěný.

Podobně jako v předcházejících dvou případech se i vy pokuste identifikovat všechny spuštěné služby a aplikace běžící na pozadí. Složitější část práce přijde až v okamžiku, kdy nebudete žádným z prostředků schopni proces či aplikaci identifikovat a ani se vám nebude zdát, že by daná aplikace či proces mohly být nějak užitečné. Pak je načase použít pro vyhledání odpovědi internet.

Hledání a identifikace procesů na internetu

Jestliže máte podezření, že by nějaká DLL knihovna mohla představovat škodlivý software, prvním místem, na které vám doporučujeme se obrátit, je **DLL Help Databáze Microsoftu** na internetové adrese **support.microsoft.com/dllhelp**, která vám umožní vyhledat informaci o DLL knihovně podle jejího jména. Pokud existuje podezření, že nějaký soubor může být napojen na spyware, je možné se informovat na **Computer Associates Spyware Information Center** na adrese **www3.ca.com/securityadvisor/pest**. Jiným vynikajícím zdrojem informací je **Pest Encyclopedia** od **PestPatrol Center for Pest Research** na internetové stránce **research.pestpatrol.com**, která poskytuje informace o více než 27 000 druzích malwaru.

Pokud není možné jednoznačně říci, zda je nějaký soubor legitimní, lze získat cenné informace na internetových stránkách **www.answers-thatwork.com**, kde po klepnutí na tlačítko *Task List* můžete získat informace jak o legitimním softwaru, tak o spywaru či virech. Další pomocnou rukou, kterou nám internet podává, mohou být utility **WinPatrol** či **WinTasks 5 Professional** od firmy **Uniblue**. WinPatrol ve verzi 9.5 naleznete NA NAŠEM CD, popř. na internetové adrese **www.winpatrol.com/download.html** jako soubor WPSETUP.EXE o velikosti 1,04 MB, zkušební verzi programu WinTasks 5 Professional si můžete stáhnout z internetu na adrese **www.liutilities.com/products/trial**. Oba programy jsou velmi účinným pomocníkem při rozhodování a určování toho, zda daný program či DLL knihovna představuje legitimní software nebo malware.

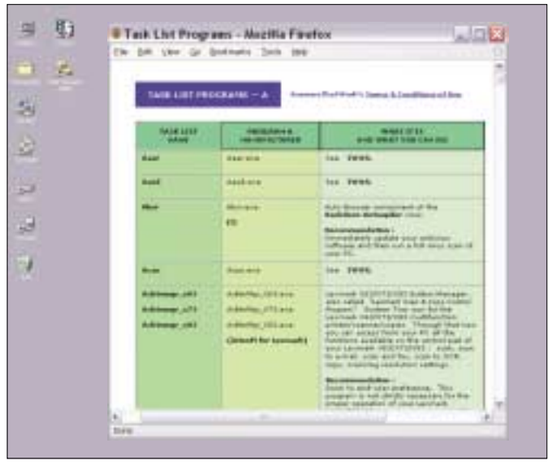


▲ **Faktické informace o knihovně DLL získáte zadáním jejího názvu do DLL Help databáze firmy Microsoft.**

Oba programy mají k dispozici velmi rozsáhlou on-line databázi obsahující informace o tisícovkách DLL knihoven či aplikací, s nimiž se můžete setkat, WinTasks navíc dokáží umístit některé procesy na „černou listinu" (*blacklist*), takže je už nelze spustit znovu.

Dalším pomocníkem, který vám umožní vyhodnotit na počítači se vyskytující spustitelný soubor, ovladač či DLL knihovnu (ať je spuštěn, nebo ne) je **Security Task Manager** od firmy **Neuber Software**. Utilitu naleznete NA NAŠEM CD, popř. na internetu na adrese **www.neuber.com/taskmanager** jako soubor TASKMANAGER16.EXE o velikosti 1,44 MB. Program existuje i v české jazykové mutaci.

Poznámka: Vždy, když hledáte na internetu informace o nějakém neznámém souboru, nedoporučujeme důvěřovat prvním několika výsledkům, které naleznete. Dokonce i když stovky internetových stránek pojednávají o tom, že se u nějakého souboru jedná pravděpodobně o malware, pak jedna stránka firmy Microsoft objasňující legitimní užití tohoto souboru systémem Windows může tyto informace o souboru zcela zvrátit. Jinými slovy, čím více informací o neznámém souboru získáte dříve, než použijete internet, tím menší bude pravděpodobnost, že odstraníte legitimní program či DLL knihovnu. 5 0456/OK ❑



▶ **Na internetových stránkách www.answers-thatwork.com naleznete řadu užitečných informací, které vám pomohou odlišit legitimní aplikace od malwaru.**

Nová utilita pro odhalení rootkitů a skrytých programů používaných hackery

Uživatelům počítačů se dostává do rukou další z utilit, kterou mohou použít pro vyhledávání velmi odolného malwaru nainstalovaného v jejich systému. Mluvíme o skrytých virech, trojských koních či spywaru, který se stále snaží proniknout do našich počítačů. Touto utilitou je **RootkitRevealer**, jenž umožňuje uživatelům skenování počítače za účelem vyhledání tohoto zrádného softwaru.

Typ škodlivých programů, který je v oblasti zabývající se zabezpečením počítačových systémů známý jako rootkit, lze vysvětlit jako používání malwaru – virů nebo trojských koní, které se dokáží samy v systému schovat. Rootkity rovněž hackerům pomáhají získat daleko větší kontrolu nad systémem, do něhož pronikly.

Rootkity jsou daleko častější ve světě Linuxu a UNIXových systémů. Jejich název vychází z toho, že pomáhají hackerovi získat přístup do systému jako *root* (nejvyšší práva na úrovni administrátora systému). V nedávné době se objevily i rootkity pro systémy Windows. Existuje tendence spojovat rootkity s nejnebezpečnějšími druhy malwaru jako jsou např. keyloggery, které zjišťují přístupová hesla uživatelů ke službám, jež využívají (elektronická pošta, internetové služby apod.).

Silné a slabé stránky

Rootkity jsou ve své podstatě pouze prostředkem k dosažení cíle, jímž je pro hackera ovládnutí cizího počítače. Např. tím, že skryje aplikaci typu trojského koně, zabrání tomu, aby byl detekován obvyklými antiviry. RootkitRevealer dokáže detekovat přítomnost několika obvyklejších rootkitů na počítačích se systémy Windows NT, 2000 či XP. Bohužel nefunguje ve Windows 95, 98 nebo ME.

RootkitRevealer má však i svoje omezení. Abyste jej mohli opravdu účinně využívat, potřebujete porozumět tomu, jak interpretovat výsledky jeho skenování.

Program rovněž neumožňuje rootkity odstranit nebo dát do karantény a rovněž vám nedokáže říci, zda soubor, který nalezl, je skutečně rootkitem. Pokud se však objeví nějaký objekt, který by na daném místě být neměl a antivirus jej nedokáže odstranit, pak jedinou cestou, jak se zbavit takové nákazy, je kompletní přeinstalování systému – zformátování disku, smazání všech dat a reinstalace Windows.

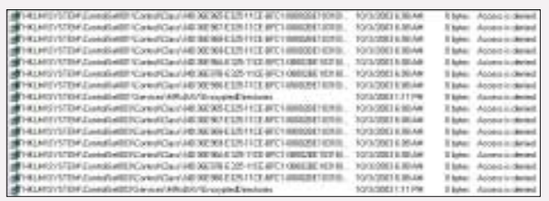
První skenování systému

Jak již bylo uvedeno výše, RootkitRevealer lze najít NA NAŠEM CD, popřípadě na internetových stránkách firmy Sysinternals. Program není nutno instalovat, stačí pouze rozbalit soubor archivu a spustit EXE soubor. Než začnete systém skenovat, máme pro vás několik upozornění.

Jakmile program spustíte, pak do chvíle, než skenování skončí, na počítači nic nedělejte. Doporučujeme rovněž před spuštěním kontroly systému vypnout všechny aplikace, které by se mohly během skenování aktivovat – například spořič obrazovky, antivirus či jakýkoliv jiný program. Pokud během skenování začne nějaká utilita vyvíjet činnost, počítač se sice nezhroutí, nicméně výsledky skenování systému mohou být nepřesné nebo zavádějící.

Vyhodnocení výsledků

Prakticky už po chvíli, kdy spustíte skenování, se začnou v okně aplikace objevovat nějaké výsledky. Jakmile se prohlídka systému dokončí (to poznáte podle tlačítka *Scan*, které se v průběhu skenování změní na *Abort* a po skončení skenování opět na *Scan*), uvidíte ve spodní části okna počet nalezených položek. Celá řada z nich je fakticky neškodných. Například prvních 10 až 20 výsledků bude vypadat jako klíče registru a bude u nich nápis *Access denied*. Tyto údaje jsou normální a objevují se na každém počítači. V žádném případě neukazují na nic podezřelého.



Níže pak uvidíte položky, které vypadají jako názvy složek ve Windows a jejich jména začínají znakem doluru (*$*). Tyto soubory jsou metasoubory souborového systému NTFS a jsou opět standardní součástí tohoto systému souborů. Jejich počet se liší systém od systému. Tento seznam se na vašem počítači vytváří zvlášť pro každý diskový oddíl.

Pokud uvidíte další soubory, u nichž bude popis *Hidden from Windows API*, tak zde je nutno zbystřit. Tyto soubory mohou být umístěny ve složkách pro dočasné soubory, ve složce Windows, popřípadě kdekoliv na pevném disku. Pokud tyto soubory objevíte, spusťte Průzkumníka a zkuste, zda jsou tyto soubory vidět i v tomto programu. Pokud vidět nebudou, mohlo by to indikovat přítomnost skrytých souborů, ale jisté to není.

Pokud během skenování systému kupříkladu spustíte Internet Explorer a budete prohlížet nějakou internetovou stránku, pak RootkitRevealer soubory této stránky označí jako podezřelé, což ale ve skutečnosti pravda není.

Dále jde také o to, že i celá řada legitimních programů používá techniky skrývání souborů – typickým programem je **Kaspersky Antivirus**.

Asi nejproblematičtějšími výsledky jsou programy, jejichž soubory mají jména sestavena z dlouhé řady náhodně zvolených písmen a číslic. Objeví-li se takové soubory ve vašem systému, doporučuje se aktualizovat antivirový systém a provést co možná nejpodrobnější analýzu vašeho systému.

RootkitRevealer je v současné době teprve v rané fázi a může, jako ostatně každý program, obsahovat chyby. Pokud si nejste jisti, zda nějaký soubor náhodou není nějakým způsobem spojen s rootkitem, dříve, než začnete podnikat nějaké radikální kroky, prohledejte nejprve internet, popřípadě Usenet.