Stopy ve

Kdo má potřebu vás špehovat? Zrádce skrytý ve vašem počítači. Windows vědí, co děláte...

M. Hermannsdorfer

V tomto článku najdete

Hesla, uživatelské účty, fotky z poslední oslavy... Jediným problémem většiny uživatelů je to, jak to všechno do počítače „nacpat“. Co se s daty děje dál, to už zajímá málokoho. Vzhledem k tomu, že slovo „soukromí“ je v rámci platformy Windows téměř neznámé, nemělo by vás překvapit, co vše je z cizího počítače možné „vydolovat“.

Operační systém loguje vše a otevřeně sděluje hackerům, Microsoftu a zvědavým kolegům, co na počítači děláte. Tuto „upovídanost systému“ lze však samozřejmě podstatně omezit – a my vám ukážeme jak. Nečekejte však rozsáhlé návody na konfiguraci firewallu nebo antivirových skenerů. V tomto případě půjde spíše o jemné manipulace se systémem.

ČTENÍ UŽIVATELSKÝCH DAT

Co o vás prozrazují XP

Dříve než systém zabezpečíme, je dobré vědět, jaká data mohou útočníci odcizit a jak. Ve většině případů je pochopitelně největší zájem o data související s financemi…

ŠPION: Upravená webová stránka dokáže zkopírovat text ze schránky a zobrazit jej.

Schránka odhaluje tajemství

Nástroj: JavaScript

Také patříte mezi ty uživatele, kteří pomocí CTRL+C a CTRL+V kopírují svá hesla do on-line formulářů? To je ale nebezpečná chyba! Speciálně upravené stránky mohou přečíst obsah vaší schránky – tedy pokud používáte Internet Explorer. Zde je malý příklad, jak to v praxi funguje: napište pár znaků ve Wordu nebo v Poznámkovém bloku a poté je zkopírujte pomocí [CTRL]+[C] do schránky. Nyní spusťte Internet Explorer a navštivte stránku **www.novnet.org/pub/ie-clipboard-test/ie-clipboard-test.html** – a uvidíte (překvapivě) obsah své schránky. Nejnovější (sedmá) verze Internet Exploreru se vás naštěstí zeptá, zda programu povolíte přístup ke schránce. Ve starších verzích uvidíte přímo obsah schránky.

Použitý trik: Webová stránka je upravena pomocí JavaScriptu, který dokáže zkopírovat text ze schránky a zobrazit jej. Doporučenou ochranou je používání jiného browseru. Například Firefoxu nebo Opery…

Browser odhaluje váš internetový profil

Nástroj: X-Ways trace

Marketingové firmy nebo různí čmuchalové by rádi věděli, které stránky navštěvujete, jak dlouho na nich zůstáváte a jaké soubory stahujete. Speciální nástroj X-Ways trace, který lze najít na stránce **www.x-ways.net**, může prozradit celou řadu výše zmiňovaných informací. Jeho pomocí není těžké odhalit vaše „internetové zvyky“. Vyzkoušejte si to sami – nainstalujte „trace“ na USB disk a odtamtud

Windows

Najdete na Chip DVD

Programy k tomuto článku najdete na Chip DVD v rubrice Testy a praxe.

Spamihilator
www.spamihilator.com

Firewall
www.personalfirewall.comodo.com

ProcX
www.ghostsecurity.com/procx

Stream Explorer
http://rekenwonder.com/streamexplorer.htm

Vispa
www.download.com/Vispa/3000-2094_4-10701495.html

xpy
http://nsis.whyeye.org/xpy

disk defrag
www.auslogics.com/disk-defrag

Ccleaner
www.ccleaner.com

X-Ways Trace:
www.winhex.com/trace

spusťte soubor „trace.exe“. V závislosti na používaném prohlížeči program otevře buď soubor index.dat (pro Internet Explorer), „history.dat“ (pro Firefox), nebo dcache4.url (pro Operu). Tyto soubory obvykle najdete ve složce „Documents and Settings\User Name\Application Data\Browser Name“. Nyní uvidíte, které webové stránky jste navštívili, jak dlouho jste je prohlíželi, jak často tyto stránky navštěvujete a jaká data jste si z internetu stáhli. A to není zdaleka vše. Pokud v programu zvolíte příkaz *File | Open data carrier* a označíte příslušnou partition Windows, můžete si prohlédnout seznam uživatelských účtů. Tento nástroj vám tak může snadno prozradit, kde vaše děti surfují a co si z navštěvovaných webů stahují…

Dávkový soubor čte systémové soubory

Nástroj: Chip Trojan.bat

Soubor o velikosti 4 KB, jehož vytvoření zabere i průměrnému programátorovi méně než deset minut, dokáže odhalit kompletní seznam systémových (i skrytých) souborů a kompletní konfiguraci vašeho počítače. Na tomto dávkovém souboru vám jako na příkladu ukážeme, jak snadné je získat z počítače důležitá data.

Stáhněte si soubor Chip Trojan.bat z našeho webu na plochu a spusťte ho. Malý „špionský“ nástroj vytvoří přímo na disku C soubor s názvem „output.txt“, obsahující zjištěná data.

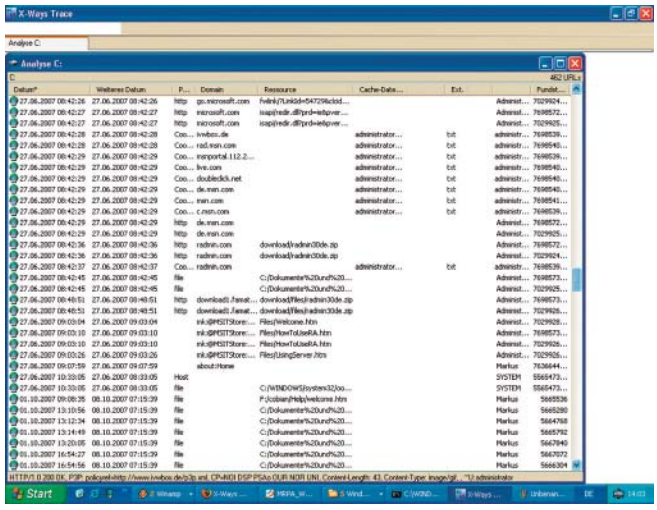
Z technického hlediska na tom není nic složitého – obyčejný příkaz „dir“ s několika parametry zjistí skryté systémové soubory, seřadí je podle abecedy, přiřadí ke každému jeho vlastníka a ukáže, kdy byl soubor naposledy změněn. Síťová konfigurace je zjištěna pomocí příkazu „ipconfig /all“.

Uživatele zrazují i registry

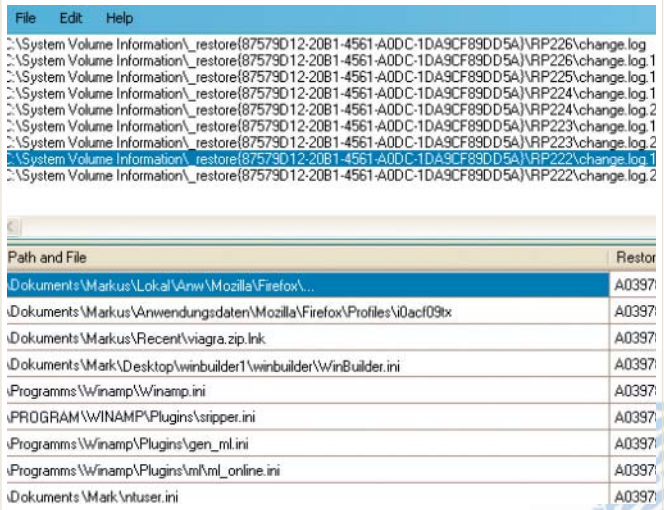
Nástroj: AD Registry Viewer

Windows registrují, který uživatel Windows používá, kdy se přihlásil a jak často mění heslo. A také další zajímavou informaci: jak dlouho ještě bude heslo platné.

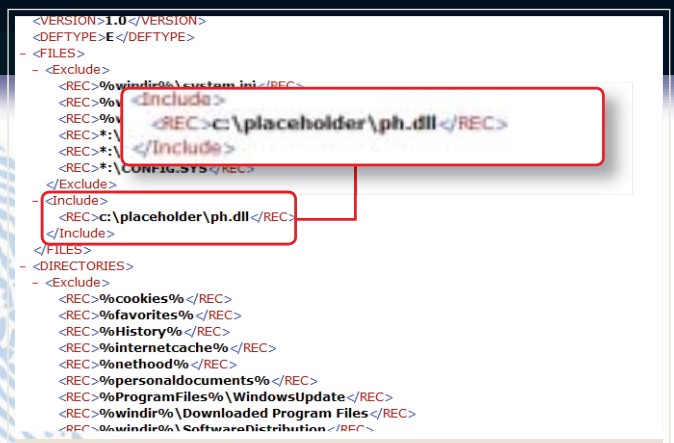
Všechny tyto informace Windows ukládají v SAM (Security Account Manager), což je část registru. Nicméně nikdo kromě administrátora by k informacím ze SAM neměl mít přístup. Spuštění regeditu a zadání HKEY_LOCAL_MACHINE\SAM je zbytečné. Navzdory tomu je přístup k těmto informacím překvapivě snadný. S programem Registry Viewer (**www.accessdata.com**) stačí otevřít soubor „windows\system32\config\sam.bak“ a přejít na položku „SAM\Domains\Account\Users“. Zde můžete vidět existující uživatelská konta jako hexadecimální klíče. Na našem testovacím počítači znamenalo kliknutí na „000001F4“ přístup k údajům konta administrátora. V sekci pod stromovou strukturou můžete vidět, kdy byl uživatel naposledy přihlášen (Last Logon Time). Za údajem „Last Password →



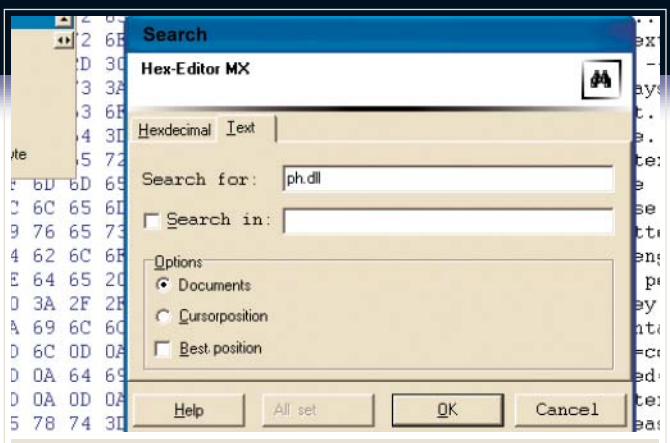
STOPY: Ze záznamů lze snadno zjistit kdo a kdy stáhl vybraný soubor z internetu.



ZRÁDCE: Restore Point Analyzer nabídne seznam nainstalovaných, smazaných nebo přejmenovaných programů.



PŘEKVAPIVÝ NÁLEZ: V seznamu souborů filelist.xml jsme nalezli podivný soubor patřící Eudoře, který je pomocí bodu obnovení pravidelně „oživován".



DOMÁCÍ HLEDÁNÍ: Pomocí HexEditoru MX jsme hledali skryté stopy vedoucí k tajemnému souboru ph.dll, který by měl patřit Eudoře...

→ Change Time" jsme našli překvapivou hodnotu – „Never" (nikdy). Bohužel v demoverzi tohoto šikovného nástroje nelze zjištěné údaje ukládat, takže existuje jediné řešení – screenshot obrazovky.

Obnova systému ukládá viry

Nástroj: Restore Point Analyzer, MX

Obnova systému je pro datové čmuchaly opravdovým pokladem. Tady lze zjistit, jaký program byl smazán či nainstalován, případně kdy. Nástroj Restore Point Analyzer vám pomůže s prohledáním tohoto datového pokladu. Prvním kontaktním bodem je soubor C:\Windows\System32\Restore\filelist.xml. Po otevření tohoto souboru (v internetovém prohlížeči) zjistíte, které složky jsou do obnovy systému zahrnuty („Include") nebo které jsou z ní vyloučeny („Exclude"). K tomuto souboru má přístup každá aplikace, což znamená, že šikovný vir se může obnovovat při každém spuštění počítače. Na našem testovacím počítači jsme díky tomuto seznamu našli neznámý soubor – C:\placeholder\ ph.dll. Na disku C jsme žádnou složku jménem placeholder nenašli (ani po povolení zobrazení skrytých a systémových souborů). Ve spolupráci s webem Program-Checker (**www.programchecker.com**) jsme zjistili, že tento soubor by měl patřit e-mailovému klientovi jménem Eudora, který byl kdysi na PC nainstalován. Na první pohled je tedy vše v pořádku – až na jednu „drobnost": Eudora obvykle vytváří tento soubor ve složce qualcomm\eudora, nikoliv ve složce jménem „placeholder".

Je tedy ten správný čas k prozkoumání obnovy systému. Všechny body obnovy jsou v systému uloženy ve složce „System Volume Information", kterou však mohou otevřít pouze sama Windows. Ke změně přístupových práv spusťte příkazový řádek a zadejte:

```
cacls „c:\system volume information"
/E /G uživatelskéjméno:F
```

kde C:\ je váš systémový disk a uživatelské jméno je to, pod kterým budete data zkoumat. Nyní spusťte Restore Point Analyzer (**www.mandiant.com/mrpa.htm**) a otevřete příslušnou složku pomocí příkazu *File* | *Open Folder*. Poté se zobrazí všechny nově instalované nebo změněné soubory, které byly přidány do seznamu pro bod obnovy systému. Zde najdeme i námi hledaný záznam s (potenciálními) daty Eudory – v našem případě je to položka A0397917.ini. Opouštíme Restore Point Analyzer a prohledáváme zmiňovaný ini soubor ve složce System Volume Information. Nyní budeme potřebovat Hex-Editor MX (**www. nextsoft.de).** V ini souboru nacházíme záznam k položce „ph.dll". Byl záznam změněn? Dochází k jeho „úpravě" automaticky? Pak bychom měli co do činění s malwarem…

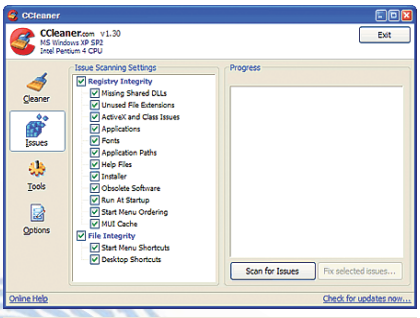
Pomocí utility MX však nacházíme příkaz ke smazání pro Eudoru a složku „placeholder". Nyní je vše jasné – Eudora tuto složku vytvořila při instalaci a přidala záznam do souboru filelist.xml, kde uvedla, že tato složka (a soubor v ní) je zahrnuta do obnovy systému. Při odinstalování Eudora zapomněla tento záznam odstranit…

Nyní je tedy jeho odstranění na nás. Nejprve je nutné odstranit z xml souboru ochranu proti zápisu. Klikneme na něj pravým tlačítkem, zvolíme *Vlastnosti* a zrušíme zatržítko u položky „Jen pro čtení". Poté otevřeme soubor v jednoduchém textovém editoru (např. Poznámkovém bloku) a smažeme záznam C:\placeholder\ ph.dll z oblasti mezi tagy "<Include>" a "</Include>. Poté znovu aktivujeme ochranu proti zápisu a příkazem

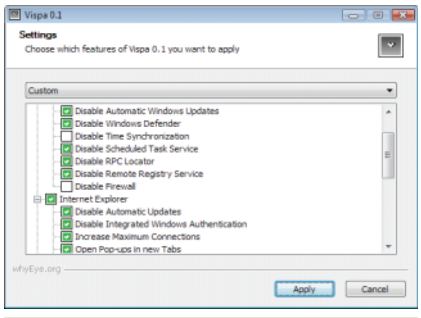
```
cacls „C:\System Volume Information"
/E /R uživatelskéjméno
```

obnovíme správná přístupová práva.

Zdá se vám tento „příběh" zábavný? Tak si představte, že šikovný čmuchal může



ŽÁDNÉ OTISKY PRSTŮ: S tímto programem po sobě odstraníte všechny důležité „logy".



DEAKTIVACE ZRÁDCŮ: Uživatelé Windows Vista mohou použít nástroj Vispa.

z vašeho počítače získat podobné informace – třeba o všech programech, které jste v poslední době instalovali a používali…

ŠPIONSKÁ OCHRANA

Zakrývání stop

Poté, co jsme vám ukázali, jak hluboko se čmuchalové mohou dostat, je čas si ukázat, jak se proti těmto praktikám chránit. Vybrali jsme ty nejlepší nástroje, které společně s našimi návody váš počítač skryjí před „zraky“ čmuchalů.

Mazání logů

Nástroj: CCleaner

Windows XP zaznamenávají téměř vše. Hackeři tak mohou zjistit celou řadu informací, nebo naopak přidat vlastní, obsahující malware. Řešení je snadné – pryč s nimi!

Jako nástroj k čištění doporučujeme CCleaner. Tento nástroj vyčistí registry dokonale a má speciální volby pro mazání „log souborů“, a dokonce i index souboru browseru. Vše důležité najdete pod nabídkou *Cleaner* | *Analyze*. Tímto způsobem lze zkontrolovat, které soubory může nástroj vymazat. Pokud v seznamu objevíte něco, co smazat nechcete, lze takový záznam vyjmout ze seznamu pomocí nabídky *Setting* | *Exclude*. Stejným způsobem doporučujeme vyčištění registrů, protože osobní nastavení mohou být zjištěna i odsud.

Jak vyčistit prázdný harddisk

Nástroj: Space Eraser

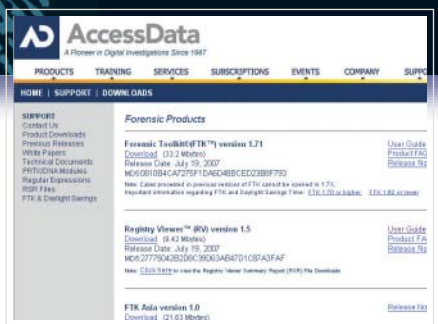
Pojem „vymazáno z disku“ ještě neznamená, že vše je navždy pryč. Pomocí nástroje typu PC Inspector File Recovery totiž dokážou datoví špioni velice rychle obnovit vymazaná data. Space Eraser tento problém dokáže vyřešit. Tento nástroj přepíše smazanou oblast disku náhodnými znaky. Po spuštění nejprve zvolte příslušnou oblast disku a zvyšte počet cyklů alespoň na dva. Pak klikněte na *Start* a čekejte, dokud „eraser“ neskončí svou práci. Pokud je poté na disku k dispozici málo místa, smažte soubor „erazer.dat“ na vyčištěném disku a poté ho odstraňte i z koše.

Skrytí uspořádání souboru

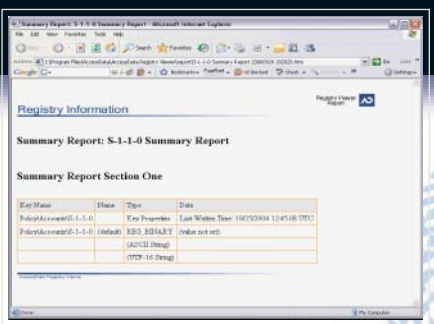
Nástroj: defrag.exe, defragmentace disku

Nyní je váš počítač téměř v bezpečí před běžnými hackerskými útoky. Například tajné služby však používají nástroje, jako je Emfase, který dokáže přímo indikovat sekci na harddisku, na které je určitý soubor umístěn.

Na tento problém je ale snadný lék: při defragmentaci disku Windows změní polohu souborů na disku – přesunou sektory tak, aby byly blízko sebe. Zní to neuvěřitelně, ➜



PRAKTICKÝ NÁSTROJ: **Ze stránky www.accessdata.com si stahněte program Registry Viewer.**



REGISTRY VIEWER: **Prozradí důležité informace o zkoumaném účtu. Například údaj, kdy byl uživatel naposledy přihlášen.**

→ ale Windows vytváří log soubor se záznamem „starého uspořádání“ disku. Výsledek je tedy následující: pokud se budou profesionálové pokoušet obnovit data na nově defragmentovaném disku, mají smůlu. Žádným postupem totiž není možné docílit původní „konfigurace“ sektorů na disku. Tipem pro tento případ je tedy použití defragmentace Windows (defrag exe), popřípadě alternativního nástroje pro defragmentaci disku (např. programu Disk Defrag).

ZABEZPEČENÍ POČÍTAČE

Košík pro Windows

Nyní už tedy není na vašem počítači nic, co by mohli špioni zjistit, přesto je Windows stále vítají s otevřenou náručí. Nyní vám ukážeme, jak můžete zablokovat „zvědavce“ z internetu a také jak zabránit „zbytečnému vybublávání“ informací přímo z Windows.

Deaktivace zrádců z XP a Visty

Nástroj: xpy, Vispa

Zabraňte tajné „rádiové komunikaci“ ve Windows XP pomocí nástroje xpy. Uživatelé Windows Vista mohou použít nástroj Vispa, který je přímo optimalizován pro nejnovější verzi operačního systému Microsoftu. Po instalaci a spuštění přímo uvidíte seznam jednotlivých „nediskrétností“. Tentokrát vám ale nedoporučujeme zvolit volbu „All Settings“, protože byste přišli i o celou řadu praktických funkcí. Zdaleka ne každý uživatel chce také deaktivovat implicitní vzhled Windows (Luna). Proto zde deaktivujte pouze ty volby, které vám doopravdy vadí.

Zabraňte tajným „data streamům“

Nástroj: Stream Explorer

„Stealth“ malware je obzvlášť nebezpečný. V souborovém systému NTFS totiž používá skryté „data streamy“, které mu zaručují téměř dokonalé maskování. S nástrojem jménem Stream Explorer můžete snadno prohledat svůj disk a tato skrytá data odhalit. Na neškodném příkladu vám ukážeme, jak „data stream“ detekovat. Naše oběť se jmenuje AutoRuns, byla vyvinuta firmou Sysinternals a dokáže zobrazit programy, které se automaticky spouštějí při startu Windows. Po spuštění programu Stream Explorer označíme složku jako „Auto runs861“.

Nyní jsou v sousedních oknech zobrazeny čtyři soubory, z nichž každý obsahuje alespoň dva ADS streamy. Hlavním NTFS streamem je <default>; ten by v žádném případě neměl být vymazán. Také bychom měli zachovat další stream <no name>, který byl označen klíčem pro pozdější dobu. Licenční agreement Eula.txt má třetí datový stream, který může teoreticky obsahovat malware. Klikněte na něj a zobrazí se vám binární kód a (v některých případech) také integrovaný ASCII text.

Nicméně v našem příkladě tento binární kód neposkytuje žádné „racionální“ informace. Mnohé programy zálohují informace ve skrytých ADS strea-

Jak pracují profesionální vyšetřovatelé

Nástroje zmiňované v článku bude většina čtenářů používat v boji s malwarem, proto asi většinu uživatelů překvapí, že tyto (a podobné) nástroje jsou v praxi používány i v boji se zločinem. Například speciální protiteroristické jednotky na západ od našich hranic používají nástroj EnCase (**www.guidancesoftware.com**) k odhalení plánů organizace al-Káida.

Ovšem zatímco tento nástroj mohou používat pouze vyšetřovatelé, námi zmiňovaný The Forensic Toolkit (jeho součástí je Registry Viewer) může použít kdokoliv. A byť je na webu výrobce (**www.acessdata.com**) zdarma pouze demo, na jeho efektivitě to nepoznáte.

Metody vyšetřovatelů

K pochopení toho, jak se EnCase nebo FTK využívají, musíte znát předepsané postupy vyšetřování. Trestní vyšetřování má následující kroky.

HLEDÁNÍ VINY: **Forensic Toolkit analyzuje celý počítač pomáhá při odhalování zločinů...**

■ **Soudní záloha:** Nejprve je vytvořena identická kopie zkoumaného disku, včetně vadných sektorů. Teprve tato kopie je zkoumána speciálními nástroji.

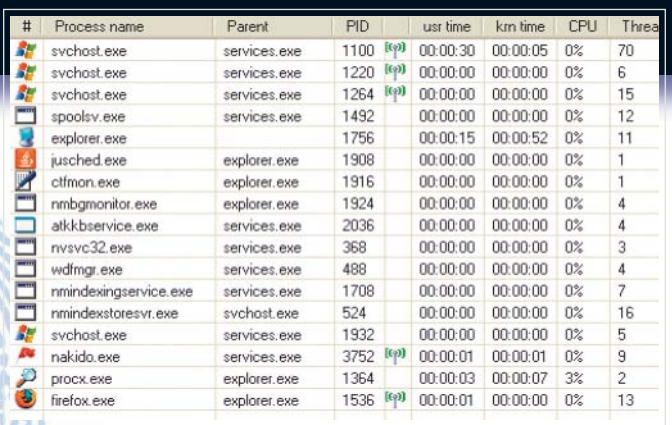
■ **Identifikace:** Zaznamenán je „počáteční stav“. Jaké soubory jsou na disku? Má na něm obžalovaný skryté, šifrované nebo smazané soubory? Po všech těchto shrnutích vyšetřovatelé rozhodnou, která data mohou být použita jako důkaz. Pro vytřídění nedůležitých informací policie definuje základní otázky a pravidla – na jejich základě se poté data třídí. Například při vyhledávání informací vedoucích k bombovým atentátům se vyhledávají linky vedoucí k podezřelým webům s informacemi o výbušninách nebo se hledají rozsáhlejší maily předávané dalším uživatelům...

■ **Ochrana:** Všechny nalezené indicie jsou poté uloženy a zazálohovány.

■ **Analýza:** Na základě důkazů vyšetřování se odhaluje průběh událostí (je důležitý i časový údaj u indicií) a zjišťuje se posloupnost akcí obžalovaných.

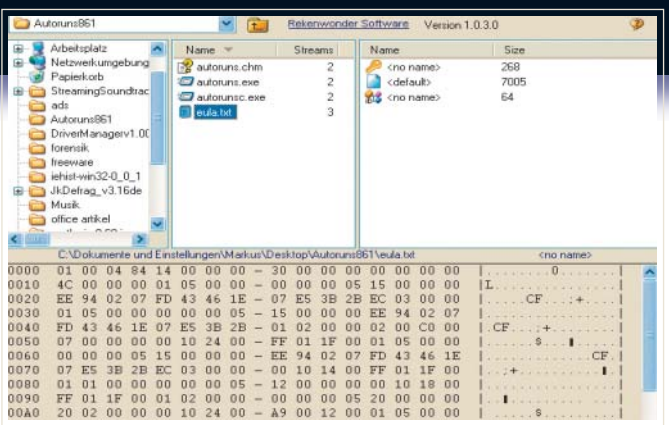
■ **Proces:** Důkazy jsou „zpracovány“ do papírové podoby a uloženy do složek.

■ **Důvod:** Soudce je schopen sledovat vyšetřování, aniž by musel studovat původní počítačové informace. Více informací můžete najít na adrese: **www.forensicswiki.org/wiki**.



#	Process name	Parent	PID	usr time	krn time	CPU	Threa
	svchost.exe	services.exe	1100	00:00:30	00:00:05	0%	70
	svchost.exe	services.exe	1220	00:00:00	00:00:00	0%	6
	svchost.exe	services.exe	1264	00:00:00	00:00:00	0%	15
	spoolsv.exe	services.exe	1492	00:00:00	00:00:00	0%	12
	explorer.exe		1756	00:00:15	00:00:52	0%	11
	jusched.exe	explorer.exe	1908	00:00:00	00:00:00	0%	1
	ctfmon.exe	explorer.exe	1916	00:00:00	00:00:00	0%	1
	nmbgmonitor.exe	explorer.exe	1924	00:00:00	00:00:00	0%	4
	atkkbservice.exe	services.exe	2036	00:00:00	00:00:00	0%	4
	nvsvc32.exe	services.exe	368	00:00:00	00:00:00	0%	3
	wdfmgr.exe	services.exe	488	00:00:00	00:00:00	0%	4
	nmindexingservice.exe	services.exe	1708	00:00:00	00:00:00	0%	7
	nmindexstoresvr.exe	svchost.exe	524	00:00:00	00:00:00	0%	16
	svchost.exe	services.exe	1932	00:00:00	00:00:00	0%	5
	nakido.exe	services.exe	3752	00:00:01	00:00:01	0%	9
	procx.exe	explorer.exe	1364	00:00:03	00:00:07	3%	2
	firefox.exe	explorer.exe	1536	00:00:01	00:00:00	0%	13

VINEN: S pomocí nástroje ProcX lze odhalit aplikace bezdůvodně komunikující „s internetem".



BEZPEČNĚJI: Program Stream Explorer dokáže skryté NTFS streamy odhalit, což může pomoci při hledání malwaru.

mech, např. odkaz na autora. Klikněte tedy nyní pravým tlačítkem na „Eula.txt" a zvolte „Properties". Ani zde není žádná informace, která by měla být zachována. Pro větší bezpečí tedy raději tento stream vymažte, a to následujícím způsobem: spusťte příkazovou řádku a přesuňte se k adresáři s programem AutoRuns. Tam postupně použijte následující příkazy:

```
ren eula.txt temp.txt
type tmp.txt >> eula.txt
del temp.txt
```

ADS stream bude vymazán, jakmile je soubor přejmenován, což si ihned ověřte pomocí Stream Exploreru.

Jak zamezit tajné komunikaci

Nástroj: ProcX

Bohužel i některé nainstalované aplikace nebo služby Windows dokazují, že jsou zrádci – ProcX (**www.ghostsecurity.com/procx**) však snadno odhalí pachatele. Tento freewarový nástroj ani nemusí být instalován. Zobrazuje všechny běžící programy a služby ihned, jakmile kliknete na „ProcX.exe". Programy a služby, které mohou přenášet data na internet, jsou označeny zeleným symbolem. Vyhledávání se stává zajímavým především u „prázdných" procesů, jako jsou „alg.exe". To je podle Microsoftu „Gateway service on application level", tedy jakýsi druh dveří, které Windows otevírají, jakmile chce aplikace komunikovat s internetem. Tato služba tedy není nebezpečná. Je ale opravdu nutná?

Abychom to zjistili, ukončili jsme Firefox, v tuto chvíli jediný nástroj, který má spojení s internetem. Pak jsme pravým tlačítkem klikli na „alg.exe" a zvolili jsme příkaz „Terminate", který službu (po potvrzení tohoto příkazu) deaktivuje. Necháme program ProcX běžet, spustíme Firefox a otevřeme webovou stránku. Spojení funguje, ale alg.exe navzdory našemu očekávání není restartováno. Tato služba tedy není na našem testovacím PC vyžadována k vytvoření spojení.

Na seznam všech Windows služeb se dostanete pomocí *Start* | *Run* a příkazem

```
services.msc
```

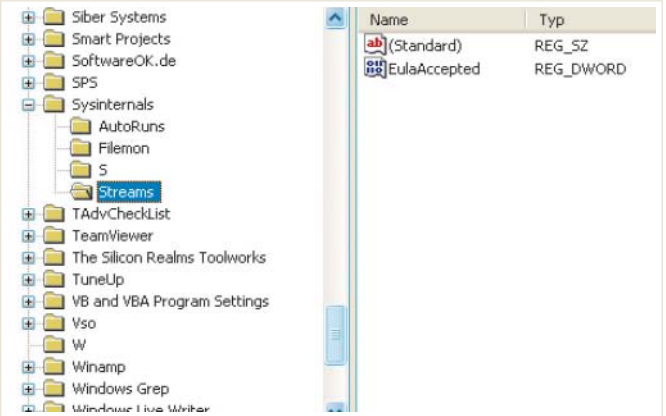
Zde pak vyhledejte „Gateway service on application level" a klikněte na *Deactivate*.

Tímto způsobem zkontrolujte všechny služby a programy označené v ProcX zeleně. Poté jednoduše deaktivujte nechtěné „práskače".

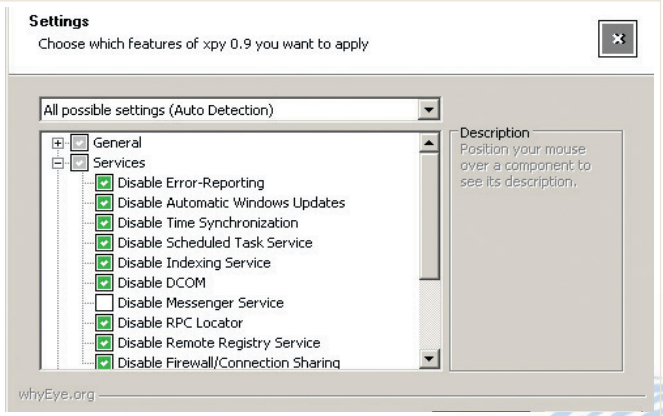
BEZPEČNOST

Jak ochránit Windows jako bankovní trezor

Nakonec, poté, co jste provedli všechna důležitá opatření, zabezpečte svůj systém před hackery a vlezlými čmuchaly pomocí firewallu a virového skeneru. Zjistíte, že nástroj AVG Anti-Virus plus Firewall 7.5 Chip, který pravidelně naleznete zdarma na našem DVD, vám ušetří celou řadu problémů – a to nejen s prozrazením citlivých údajů. *M.Hermannsdorfer*



SKRYTĚ: V registrech program AutoRuns od Sysinternals vytváří hodnotu pro data stream v EULA.



XPY: Zde deaktivujte pouze ty volby pro Windows XP, které vám doopravdy vadí...