Odstranění malwaru z počítače

On-line záchrana

Většina informací, které jste až doposud v Chipu nalezli, se věnovala prevenci: jak se ochránit proti virům, spywaru nebo podobným škůdcům. Je nejvyšší čas si ukázat, co dělat, když tyto rady selžou...

Text: Petr Kratochvíl, *petr.kratochvil@vogelburda.cz*

V počítačových časopisech a na internetu lze narazit na desítky stránek opakujících s mechanickou přesností stále stejné tipy na téma „Jak se nenechat nakazit“. O tom, co dělat, když se vám v počítači zahnízdí škůdce, se dozvíte jen málokde. Většina rad je navíc typu „Proskenujte disk antivirovým programem“, což je rada hodná génia. Pokud navíc vezmete na vědomí testy na předchozích stránkách, jde také často o radu špatnou. My vám ukážeme jinou cestu...

Jak poznat infekci

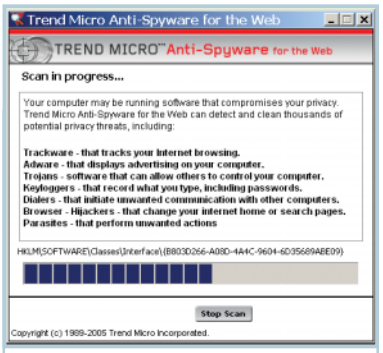
Prvním krokem k úspěšné a rychlé očistě je rozpoznání infekce. Na rozdíl od růžové minulosti, kdy se viry hrdě uživatelům hlásily nebo rovnou mazaly určité typy souborů, je v současnosti rozpoznání „nakažení“ mnohem obtížnější. Většina tipů v tomto případě řadí mezi symptomy „zpomalení počítače“, což není úplná pravda.

Pokud nemáte počítač z minulého století nebo pokud počet virů a malwaru nedosahuje rekordní hranice, není ve většině případů očividné žádné zpomalení. Mnohem zřetelnější bývá zpomalení internetového připojení (zvlášť u pomalejších druhů) a větší objem přenesených dat. Ovšem ani to nemusí být pravidlem – trojský kůň slídící po osobních údajích přenáší řádově maximálně kilobajty.

Ještě očividnější bývají změny na disku – nové složky a soubory by neměly uniknout pohledům i méně zkušenějších uživatelů. Proto nelze než doporučit pečlivě sledovat obsah složky Program Files a System a také →

ANTISPYWARE INTERNETOVÉ SKENERY

	Doporučujeme		Jen pro případ nouze		
Firma	Trend Micro	BitDefender	Kaspersky	Panda	Symantec
Adresa	*www.trendmicro.com/spyware-scan/*	*www.bitdefender.cz*	*www.kaspersky.com/virusscanner*	*www.pandasoftware.com/activescan/*	*www.symantec.com/home_homeoffice/index.jsp*
Objem stahovaných dat	-	nezjištěno	7,5 MB	8 MB	nezjištěno
Doba skenování (min:s)	5:28	14:41	6:55	8:26	6:12
Instalace	Pouze nainstalování ActiveX prvku. Rychlá a snadná instalace i pro naprostého začátečníka.	Nejjednušší a nejrychlejší spuštění.	Jasná a přehledná. Indikátor ukazující stav stahování i instalace.	Poněkud zdlouhavější, ale srozumitelná. Zvládne ji i začátečník.	Složitá, nepřehledná. Chybí nápověda nebo vysvětlení, jak postupovat dále.
Možnosti	Pouze antispywarový sken.	Na sousední stránce nabídka antirootkit produktů.	Na vedlejší stránce encyklopedie a nápověda.	-	K dispozici i nic neříkající „security scan“, detekující „nedefinovaná“ on-line rizika.
Nalezeno spywaru	22	18	26	26	3
Odstraněno spywaru	20	12	-	-	-
Poznámka	Na sousední stránce se nabízí i antivirový test...	Široké možnosti nastavení ve spojení s přehledným ovládáním z něj dělají jasný tip nejen pro začátečníky.	Překvapivě široké možnosti nastavení, nabízející prohledání archivů nebo pošty.	Nejdůkladnější a nejdelší sken v testu. Odstranění pouze po zakoupení plné verze.	Ovládání chaotické stejně jako instalace. Už jen proklikat se ke skeneru je životní úkol. Kromě virů hledá i spyware.
Hodnocení	Momentálně asi nejlepší volba pro mírně až středně „infikovaný“počítač. Výborná rychlost a přehlednost. Při druhém skenu odstranil i dva zbývající spywary.	Nejdelší sken disku. I zde však zůstalo několik škůdců, se kterými si neporadil...	Delší, ale pečlivý sken disku nalezl i to, co část konkurence přehlédla. Před pokusem o odstranění nalezeného malwaru okno programu „zatuhlo“ a už se ho nepodařilo aktivovat. Chybí možnost odstranění škůdců.	Finální hodnocení by bylo více než nadšené, bohužel stejně jako u Symantecu chybí možnost odstranění nalezených „problémů“. Navíc zde nenajdete ani odkaz na jednorázový nástroj pro odstranění...	Pokud chcete disk zároveň zkontrolovat na výskyt virů, lze skener v případě nouze použít. Bohužel neumí nalezený spyware zlikvidovat. Pouze nabídne odkaz na podporu, kde po chvilce hledání naleznete potřebné informace a především jednorázový nástroj na odstranění problému.



TrendMicro: Ideální volba pro většinu běžných surfařů.

kontrolovat, co a jak se kam instaluje. Už jen proto, abyste se vyhnuli scénám typu „Hele, Tondo, mám tady složku WINSYSTEM, nevíš, co to je?“.

Není také od věci mít pod kontrolou spuštěné procesy. Pokud navíc používáte vylepšený „správce procesů“ (například Process Explorer), můžete jedním kliknutím podezřelé procesy „prolustrovat“ na internetu.

Samozřejmě že na malware využívající rootkity je podobný postup krátký, zde však zase pomohou jednorázové utility proti rootkitům. Používejte vždy aktuální verze, které zaručují nejširší záběr a nejlepší vyhledávání.

A je tam

Co tedy dělat, když důkladná prohlídka (nebo náhodný pohled) odhalí podezřelé soubory, složky či procesy? Nejprve doporučuji zvážit, zda jsou na disku důležitá a citlivá data, která je nutné bezpodmínečně zachránit, a poté je možné postupovat dále. Ve chvíli, kdy se na počítači začne dít něco podezřelého (blikající disk, vysoký datový tok na internet, zpomalující se počítač), doporučuji počítač odpojit od internetu, popřípadě vypnout a na další záchranné práce se připravit.

Pokud se zdá, že je vše v pořádku, počítač lze použít ke zjišťování informací o dalším postupu. Nejjednodušší metodou, která ve většině případů přináší nejlepší výsledky, je zadání vhodného dotazu do vyhledávače. Jméno podezřelého souboru, procesu nebo složky ve spojení se slovem vir či spyware vás vždy dovede k cíli. Nevýhodou tohoto postupu je to, že obvykle vyžaduje znalost angličtiny a zkušenějšího surfaře. Českých zdrojů o spywaru totiž zatím příliš mnoho není a méně zkušený surfař se v záplavě vyhledaných odkazů ztratí.

Cesta k záchraně

V žádném případě se nedejte zlákat blikajícími okny varujícími před „spywarem na vašem počítači“, které vám nabízejí nástroj na jeho odstranění. Z 99 procent jde jen o metodu, jak do vašeho počítače dostat dalšího škůdce. Problémy však mohou dělat i rádoby seriózní nástroje. Pokud tedy umíte alespoň trochu anglicky, nelze než doporučit stránky *www.spywarewarrior.com/rogue_anti-spyware.htm,* kde najdete mimo jiné i seznam programů, které si na antispyware jen hrají. Českou pomoc lze očekávat na českých fórech, ovšem jen málo z nich splní to, co od nich uživatelé očekávají. Za jednu z mála výjimek lze označit fóra serverů Spyware.cz (*www.viry.cz/forum/*) a Trojanhelp

Zbytečné zkoušet

Webroot *www.webroot.com*	Grisoft *www.ewido.net/en/onlinescan*	Spyware Guide *www.spywareguide.com/onlinescan.php*
10,2 MB	-	-
5:14	6:22	-
Mírně komplikovanější, zvládne ji však i začátečník.	Rychlé a srozumitelné spuštění.	-
Rozsáhlé. Spíše než o on-line scan jde o demoverzi programu.	Na sousední stránce široká nabídka utilit pro boj se spywarem a spamem.	-
7	8	-
-	6	-
Pro rozšíření funkce o odstranění je nutné produkt zaregistrovat.	Příliš malé okno s výsledky přehlednost příliš nezvyšuje.	Nepodařilo se nainstalovat. ActiveX prvek byl spywarem zablokován.
Lze doporučit jen pro občasnou kontrolu, bez možnosti odstranění spywaru téměř ztrácí smysl.	Některé škůdce se nepodařilo odstranit, program to však poctivě přiznal a doporučil nainstalovat „stolní verzi“.	Ostuda kvalitního antispywarového serveru.

JAK JSME TESTOVALI

Na testovacím počítači jsme nejprve nainstalovali Windows XP v „plné polní“. Byl nainstalován Service Pack 2 a poté provedena kompletní aktualizace. Poté jsme využili program Acronis True Image 9 a do „Secure Zone“ vytvořili zálohu disku. Po zapnutí firewallu jsme „navštívili“ sekvenci vybraných stránek a nechali se nakazit vším, co jsme na těchto stránkách nalezli. Poté jsme spustili on-line test a vyzkoušeli jsme, co dovede. Hodnotili jsme rychlost skenování, množství zachycených škůdců a schopnosti při jejich odstraňování. Po dokončení každého testu jsme znovu nabootovali a systém obnovili ze „Secure Zone“.

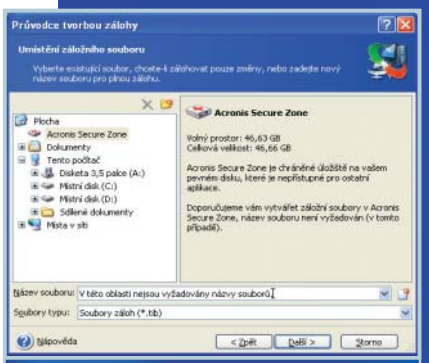
Na závěr jen upozorňujeme, že schopnosti jednotlivých „on-line skenerů“ se mohou lišit v závislosti na celé řadě faktorů. Stačí jen pomalejší reakce na nového škůdce nebo infekce jinými typy malwaru a námi vytipované weby mohou zklamat. Náš test by vám měl především naznačit, jaké jsou možnosti jednotlivých on-line skenerů a kterým se zdaleka vyhnout...

POCIT BEZPEČÍ A JISTOTY, NEJEN KDYŽ MÁTE SVÉ DNY...

ACRONIS TRUE IMAGE

Chcete se smát všem zákeřným útokům na váš disk, ohrnovat nos nad viry mazajícími multimediální soubory nebo spywarem poškozujícím instalace „security programů“? Zazálohujte si bezpečně obsah svého pevného disku. Není to nic obtížného – stačí jen použít program Acronis True Image.

Po nainstalování programu nejprve vytvořte „Secure Zone“. Klikněte v levém okně na položku Správa Acronis Secure Zone a pomocí průvodce snadno vytvořte bezpečnou zónu na vybraném disku. Pak už jen stačí vytvořit zálohu a uložit ji v této zóně. Postupujte takto: V nabídce *Operace / Zálohovat* spusťte „Průvodce tvorbou zálohy“. V dalším okně vyberte položku „celý obsah disku nebo diskového oddílu“ a poté pro umístění záložního souboru zvolte vytvořenou Acronis Secure Zone. Pokud v následujícím okně zvolíte „Nastavit možnosti ručně“, lze ještě nakonec nastavit několik drobností, jako je priorita zálohování nebo úroveň komprese. Nakonec spustíte zálohování a podle zvolených parametrů a velikosti zálohované oblasti čekáte několik minut až hodin.



Secure Zone: **Záloha v této oblasti je před spywarem v bezpečí.**

Pokud dojde k jakémukoliv většímu softwarovému problému, stačí restartovat a po stisknutí klávesy F11 znovu nabootovat a obnovit systém ze zálohy v Secure zone.

DALŠÍ DŮLEŽITÉ ZDROJE

ANGLICKÉ WEBY

www.spywareguide.com – Databáze spywaru, on-line skener, antispywarové utility a další informace o spywaru.

http://us.mcafee.com/virusInfo/default.asp?id=vrt – Jednorázové utility na odstranění virů.

www.tomcoyote.org/hjt/#Top – Podrobnější informace nejen o šikovném programu na vytváření logů...

www.spywarewarrior.com – Startovní stránka každého bojovníka proti spywaru. Pravděpodobně nejrozsáhlejší seznam zdrojů týkajících se spywaru a boje proti němu.

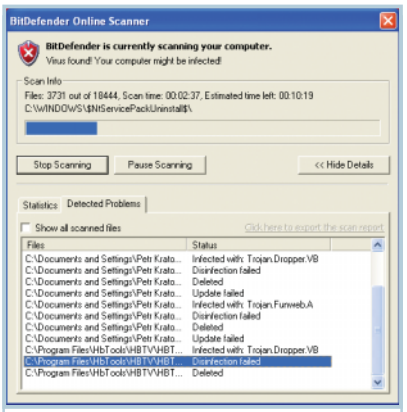
ČESKÉ WEBY

http://trojanhelp.wz.cz/ – Informace o spywaru, tipy a postupy pro odstranění, fórum.

www.spyware.cz – Jedna z nejstarších a nejobsáhlejších českých stránek o spywaru.

➔ (*http://trojanhelp.wz.cz/forum/phpBB2/index.php*). Jen málokdy se stane, že na těchto zmiňovaných webech nenajdete pomoc, a na rozdíl od „lidových fór a diskuzí“ (Živě, Technet) zde nedostanete ani špatnou radu. Před položením dotazu doporučuji nejdříve prohledat databázi, zda někdo podobný dotaz nepoložil už dříve, a poté si přečíst pravidla pro zadávání dotazů. Dotazy typu „Pořád se mi to restartuje, prosím, pomozte“ jsou totiž jen ztrátou času...

Zkušenější uživatelé mohou také využít nástroj HijackThis, který dokáže všechny důležité informace uložit do logu. Na jeho základě vám pak mohou zkušenější uživatelé poskytnout rady na profesionální úrovni. Stačí jen stáhnout si program na *http://tomcoyote.org/hjt/hjt199//hijackthis.zip,* archiv rozbalit a spustit stejnojmenný exe soubor. Po spuštění klikněte na tlačítko *Do a system scan and save a logfile*. Výsledkem je soubor hijackthis.log, který nahrajte do vybraného fóra a vyčkejte na vyjádření odborníků. *Na http://trojanhelp.wz.cz/hijacklog.htm* navíc najdete automatickou analýzu logu, takže si můžete okamžitě udělat obrázek, jak to s vaším počítačem vypadá. Po obdržení podrobnějších rad stačí jen v programu označit vytipované problémy zatržítkem a kliknout na *Fix checked*.



BitDefender: **Snadné použití a slušné výsledky.**

Panda: **Vzhled pro 21. století, ovšem chybí odstranění nalezených problémů.**

On-line pomoc

Poslední variantou pomoci při nákaze je využití on-line skenerů, které lze nalézt na celé řadě stránek. Pochopitelně nelze očekávat, že vás tyto „freewarové nástroje“ zbaví všech problémů, ale jako základní čisticí metodu je lze jen doporučit. Jejich výhody jsou očividné: dostanete k dispozici nejnovější verzi programu a aktuálních signatur, přičemž skenovací utilita není infekcí poškozena nebo upravena. Pro korektnost je nutné přiznat i některé nevýhody – nutnost připojení k internetu a instalace ActiveX komponent.

On-line skenery hledající na vašem počítači přítomnost spywaru najdete na celé řadě webů – nejčastěji to bývají stránky výrobců bezpečnostních programů a v poslední době je najdete i na některých bezpečnostních portálech. Rozhodně nedoporučujeme používat neznámé a nevyzkoušené weby, které vám slibují „on-line kontrolu a odstranění spywaru“. Instalace ActiveX komponenty se v podstatě rovná volné pozvánce do systému, takže používání podezřelých skenerů lze přirovnat k počítačové sebevraždě. Pokud si nejste jisti, zda vámi zvolený skener je hodný vaší důvěry, zkuste si pomocí vyhledávače najít jeho reference na bezpečnostních portálech. ■ ■ ■