ZABEZPEČTE SI počítač

Nemůžete investovat do drahých bezpečnostních balíků a zároveň nechcete nechat počítač bez ochrany? Vyzkoušejte jednoduché a bezplatné bezpečnostní nástroje.

PETR KRATOCHVÍL

Redaktor Chipu Petr Kratochvíl se testováním bezpečnostních aplikací, virů a malwaru zabývá už více než 15 let.

Většina uživatelů už si uvědomuje, že malware, viry a hackerské útoky nejsou jen výmysly hollywoodských scenáristů nebo autorů sci-fi románů, ale běžná denní skutečnost. Metod, jak se bránit, je celá řada, naprostá většina z nich ale vyžaduje nemalé investice. Ideálním řešením je například koupě komplexního bezpečnostního balíku (jejich test najdete v Chipu 2/2013), který vás ochrání před velkým množstvím potenciálních hrozeb. Při této volbě ale počítejte s cenou přibližně tisíc korun za rok, což nemusí být pro každého zrovna zanedbatelná částka. Pokud ale nejste tak nároční a nepatříte mezi počítačové začátečníky, můžete si počítač ohlídat sami a zdarma. Je to sice cesta plná kompromisů, pokud ale chcete na bezpečnosti šetřit, nic jiného vám nezbývá.

Jde to i zadarmo, ale...

Základem by vždy měl být (bezplatný) antivir či bezpečnostní balík a jako doplněk specializovaný software, který vám nyní představíme. Při této volbě je ale nutné počítat s celou řadou kompromisů.

1/ Naprostá většina bezplatných programů nenabízí ochranu v reálném čase – většinou jde jen o detekční nebo dezinfekční nástroje. Oblíbeným trikem je také to, že bezplatný nástroj malware pouze najde, ale nedokáže jej odstranit. V tomto případě musíte pro eliminaci nalezených škůdců použít software jiné firmy.

2/ Většina bezplatného softwaru pochází až na výjimky z dílen menších firem, nebo dokonce jednotlivých programátorů. S tím souvisí i často omezená frekvence aktualizací a riziko ukončení vývoje programu. Pokud se tedy pro takový program rozhodnete, doporučujeme vám pravidelně sledovat stránky autorů, abyste se vyhnuli nepříjemným překvapením.

3/ I autoři bezplatného softwaru potřebují peníze, a proto se vás obvykle snaží přesvědčit k nákupu lepší (placené) verze

NA CHIP DVD

Tyto nástroje najdete na Chip DVD pod indexem AntiMalware

Secunia PSI – kontrola aktualizací zranitelného softwaru

Process Explorer – průzkumník a správce procesů ve Windows

Hijack This – osvědčený nástroj na analýzu a zabezpečení systému

Browser Guard – pomocník pro ochranu prohlížeče před hrozbami

Ultimate Process Manager – profesionální nástroj na boj proti malwaru

System Explorer – nástroj na správu běžících procesů a aplikací

Spybot Search and Destroy – známý bojovník proti spywaru a adwaru

Spyware Guard – štít bránící počítač před spywarem a jinými hrozbami

EMCO Malware Bouncer – pomocník na rychlou kontrolu PC na malware

Spyware Terminator 2012 – účinný nástroj na odstranění spywaru ze systému

softwaru. U některých programů jde o decentní upozornění nebo je nutné jednou za čas odkliknout potvrzení, že opravdu nemáte o placený software zájem. Existuje ale nezanedbatelné procento produktů, u kterých jdou autoři přes mrtvoly. V těchto programech jste k nákupu tlačeni s decentností autorů předváděcích akcí pro důchodce (ano, těch s tlačenkou a zájezdem zdarma) a to, že používáte bezplatnou verzi, je vám neustále připomínáno.

Zjištění problémů

Prvním krokem při podezření na zavirování počítače by měla být kontrola systému. Pro tento účel je vhodné nejprve použít on-line antivir (jejich test najdete například v Chipu 5/2012) a teprve poté nasadit jeden z dále popisovaných programů.

SPYWARE TERMINATOR 2012

Praktický nástroj na nalezení spywaru v systému a také blokování hrozeb z internetu. Výhodou softwaru je jeho široký záběr: kromě klasického malwaru program detekuje také spyware, adware, viry typu hijack a další nebezpečné hrozby. Tento program lze označit jako ideální doplněk bezplatného antiviru – například od AVG či Avastu. Spyware Terminatoru totiž chybí realtime antivirová ochrana (respektive tu nabízí až placená verze) nebo pokročilejší bezpečnostní nástroje.

Smutným faktem je bohužel to, že vývojáři programu nevěnují tolik času, kolik by si zasloužil. To je vidět nejen na ergonomii jeho ovládání, která rozhodně nepatří k nejlepším, ale i na jeho webech. Česká verze webu má novinky ze září 2011, diskusní fórum zeje prázdnotou a za moc nestojí ani oficiální web programu s nabídkou placené verze. I přes zmiňované výhrady lze Spyware Terminator označit jako použitelnou bezplatnou ochranu.

EMCO MALWARE BOUNCER/DESTROYER

Decentní alternativou ke Spyware Terminatoru je EMCO Malware Bouncer, který se specializuje na detekci malwaru na základě signatur. I díky tomu dokáže zkontrolovat celý počítač za několik desítek sekund. Už v základní instalaci software obsahuje téměř 5 000 signatur nejznámějších a nejrozšířenějších hrozeb. Za zmínku například stojí specializovaný engine pro detekci a odstranění oblíbených adwarů a toolbarů Hotbar, Alexa nebo Gator. Jako bonus si můžete z webu výrobce (**www.emcosoftware.com/malware-destroyer**) stáhnout vylepšenou verzi, která je ještě o něco rychlejší a nabízí dvojnásobný počet signatur malwaru.

SPYBOT SEARCH AND DESTROY

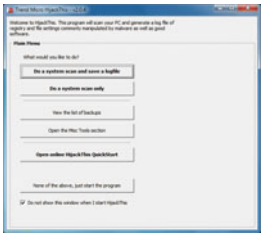
Jeden z nejstarších a nejznámějších nástrojů na boj s malwarem funguje podobně jako kolega od EMCO Software – hledá škůdce převážně na základě virových definic. Na rozdíl od něj si ale poradí i s rootkity a dokáže i imunizovat systém. Jako jeden z mála bezplatných bezpečnostních nástrojů nabízí i možnost editace programů spouštěných při startu a také zálohování a opravu registru Windows. U Spybotu nemusí uživatelé bezplatné verze příliš pošilhávat po placené variantě. Ta toho totiž, kromě skenování profilů iPhonu, lepší ochrany prostředí Windows a nabídky automatizací funkcí, moc nenabídne. Ve srovnání s konkurencí je navíc lákání na placenou verzi spíše decentní. Z naší trojice bychom tedy doporučili spíše tento nástroj.

Nejen pro přímý boj

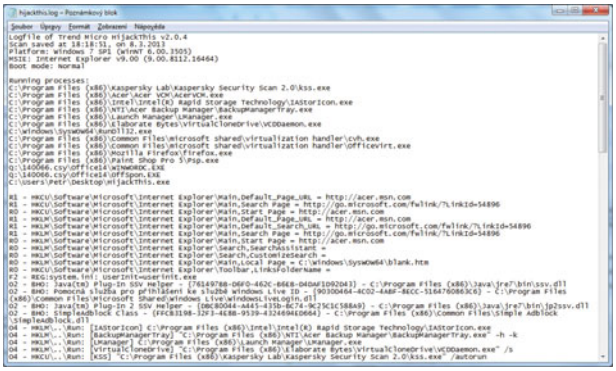
Ve chvíli, kdy už víte, že je na vašem počítači škůdce, začíná poměrně komplikovaný boj. Asi nikoho nepřekvapí, že většina bezplatných nástrojů si se sofistikovaným malwarem neporadí. Pro jeho eliminaci je tak nutné nasadit mnohem silnější kalibr. Ideálním řešením je využít specializované nástroje na odstranění konkrétní hrozby. Například pokud je na vašem počítači detekován trojský kůň Zbot, zadejte do Googlu „zbot removal“, a ihned se objeví řešení. V tomto případě lze narazit na nástroje na odstranění této hrozby na webech AVG a Symantecu. Zde je ale nutné být na pozoru a odstraňovače stahovat pouze z webů velkých a důvěryhodných antivirových firem. Ke starým a dobrým trikům podvodníků patří i vytvoření nástroje na „odstranění malwaru“, který místo eliminace hrozby přidá do systému dalšího škůdce. Univerzálnějším nástrojem na eliminaci hrozeb je například program AVPTool (najdete ho na **www.kaspersky.com/free-virus-removal-tool**), který si poradí s širokým spektrem hrozeb. Stažený soubor stačí jen nainstalo-

NECHTE SI ZDARMA ZKONTROLOVAT POČÍTAČ!

Pomocí programu Hijack This si můžete nechat rychle a snadno prověřit svůj počítač.

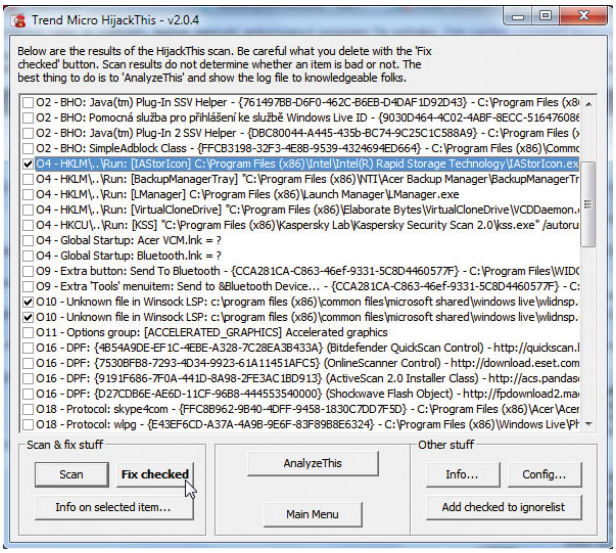


Po spuštění programu klikněte na »Do a system scan and save a logfile«.



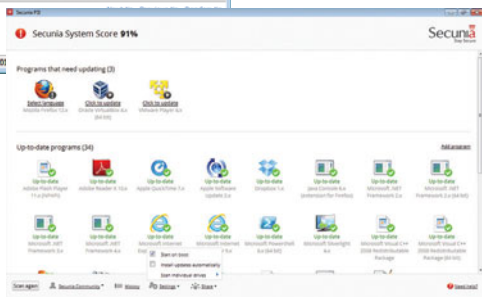
Výsledkem skenu je textový soubor s analýzou systému.

Přejděte na adresu **www.hijackthis.de/cz**, text zkopírujte do příslušného okna a klikněte na »Analyzuj«. V okně prohlížeče se zobrazí rozbor vašich výsledků.



V programu nakonec označte problematické položky a klikněte na »Fix checked«.

Spybot: Jako jeden z mála komplexních bezpečnostních nástrojů si poradí i s rootkity.



Secunia PSI: Základním kamenem zabezpečení počítače by měly být aktuální verze programů.

vat a kliknout na tlačítko »Scan« – zbytek zvládne program sám. Pokud ale žádný specializovaný nástroj na odstranění nalezených hrozeb nenajdete, je nutné využít další softwarové pomocníky.

HIJACK THIS

Tento specializovaný nástroj je určen k analýze systému a vytvoření logu – záznamu o stavu vašeho systému. Sám o sobě tedy program boj s malwarem nezvládne, ale pomůže vám zjistit, jak na něj. Software provede analýzu systému a vytvoří přehledný popis klíčových lokací a konfiguračních nastavení, která jsou uložena do záznamu označovaného jako log. Ten je možné například vložit na web autorů (**www.hijackthis.de/cz**), kde vám česky prozradí, co která položka znamená.

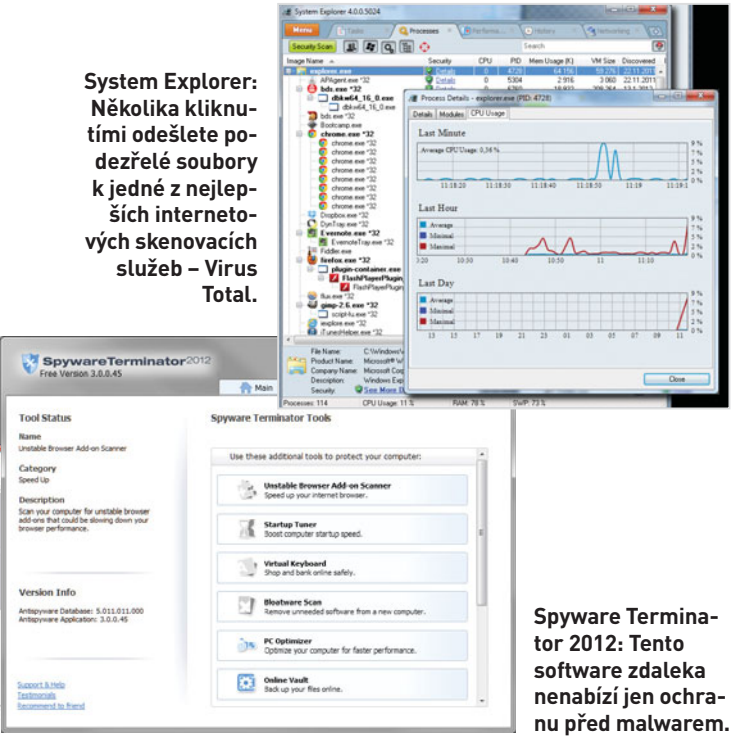
Mnohem lepší je ale nahrát zjištěné informace na některé ze specializovaných fór, například na portálu Viry.cz, kde vám zkušenější uživatelé poradí, zda máte skutečně problém a jak ho odstranit.

SYSTEM EXPLORER

Dalším nástrojem, který by vám měl umožnit snadnější eliminaci hrozeb, je System Explorer. Ten totiž nabízí nejen všechny důležité informace o systému, spuštěných aplikacích a procesech, ale také s nimi dokáže pracovat. Díky němu můžete o běžícím malwaru získat skutečně detailní informace: jaké využívá procesy, služby, ovladače, případně kam je na internetu připojen a zda má v systému další otevřené soubory. Obrovskou výhodou nástroje je snadná kontrola podezřelých souborů – několika kliknutími je odešlete k jedné z nejlepších internetových skenovacích služeb – Virus Total.

ULTIMATE PROCESS MANAGER

Na závěr našeho představování nástrojů na boj s malwarem jsme si nechali to nejlepší, co současná bezplatná antivirová scéna nabízí. Dříve než se ale pustíme do hodnocení programu, musíme vás upozornit, že tento software není příliš vhodný pro méně zkušené uživatele. Jeho rozsáhlé možnosti totiž mohou v rukou začátečníka systém zničit lépe a rychleji, než by to provedl nejzákeřnější malware. Ačkoliv se totiž Ultimate



System Explorer: Několika kliknutími odešlete podezřelé soubory k jedné z nejlepších internetových skenovacích služeb – Virus Total.

Spyware Terminator 2012: Tento software zdaleka nenabízí jen ochranu před malwarem.

process manager tváří jako jednoduchý správce úloh, jeho schopnosti přesahují i celou řadu placených antivirových nástrojů. Za zmínku například stojí možnost blokovat funkce jednotlivých programů – například lze zakázat spouštění dalších procesů nebo zápis do registrů. Unikátní je také možnost provádět hromadné akce s více procesy najednou – to se hodí především tam, kde malware využívá dva navzájem se hlídající procesy. Zkušenější uživatelé mohou tento nástroj využít i k ochraně domácího počítače před vlastními dětmi, protože nabízí například možnost zákazu úpravy plochy Windows, přístupu do registrů nebo ke správci procesů. Pro boj proti rootkitům je zase možné využít možnost eliminace souborů po restartu počítače.

Ultimate process manager zkrátka patří k tomu nejlepšímu, co lze pro boj s viry využít, je ale určen především do rukou zkušenějších uživatelů. Méně zkušení ho mohou využít alespoň k vytvoření komplexního logu (textový soubor), který poté může posloužit při konzultaci problémů s experty.

Pro klidné spaní

V případě, že se vám podařilo zbavit se všech nežádoucích problémů, lze doporučit ještě jeden krok. Aby se problémy neopakovaly, měl by být počítač zbaven slabých míst. Ideálním řešením je již zmiňovaný antivirový nástroj s ochranou v reálném čase – například plná verze AVG Internet Security z Chip DVD. Pokud ale z nějakého důvodu není možné tuto ochranu využít, měli byste alespoň ucpat díry ve vlastním systému. Za samozřejmost považujeme aktualizaci systému, podceňované jsou ale především aktualizace nainstalovaných programů. A protože manuální práce by v tomto případě byla zdlouhavá a náročná, doporučujeme využít program Secunia Personal Software Inspector (PSI). Ten váš počítač automaticky zkontroluje a umožní vám několika kliknutími aktualizovat všechny problematické programy.

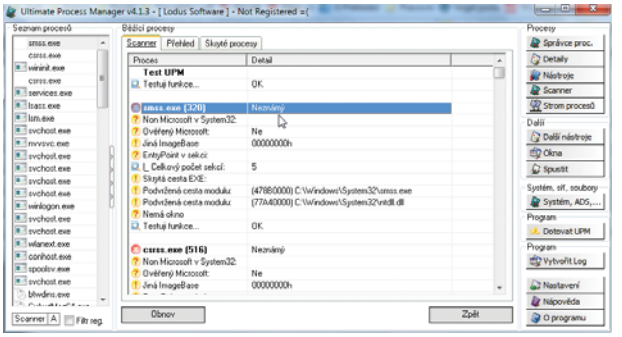
Obrovské množství hrozeb však ohrožuje uživatele především při surfování po internetu, proto je vhodné používat nějaký nástroj na ochranu prohlížeče. My doporučujeme Browser Guard od firmy TrendMicro, který pracuje na pozadí a hrozby odhaluje v reálném čase.

PETR.KRATOCHVIL@CHIP.CZ

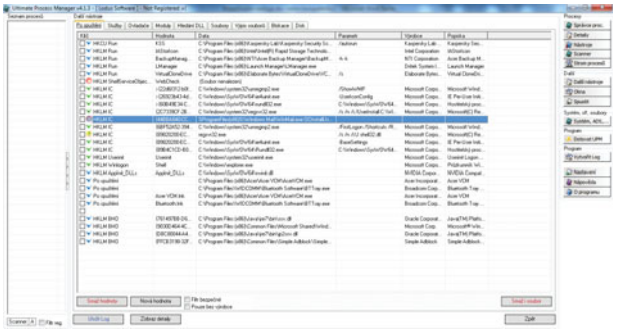
ULTIMATE PROCESS MANAGER: PŘEDEVŠÍM PRO ZKUŠENĚJŠÍ

Pravděpodobně nejlepším bezplatným programem pro boj proti malwaru a běžným hrozbám je český program Ultimate Process Manager. Na jedné straně musíme autorovi zatleskat za vynikající a schopný program, na straně druhé ale stojí fakt, že vývoj se zastavil na konci roku 2009, takže s nejnovějšími operačními systémy si program zcela nerozumí (například s Windows 7 64b). Ocenit lze však skutečnost, že na webu autora (**www.lodusweb.net**) najdete i praktické návody na práci s programem.

Dříve než se pustíte do jeho vyzkoušení, musíme znovu upozornit, že schopnosti programu jsou natolik rozsáhlé, že nezkušený uživatel si s jeho pomocí může z Windows udělat během několika sekund kůlničku na dříví. Nedoporučujeme tudíž s programem experimentovat, pokud přesně nevíte, co děláte! Vzhledem k rozsahu funkcí programu vám ani zdaleka neukážeme vše, co program umí (to by zabralo celé číslo časopisu), ale spíše jen naznačíme jeho nejzajímavější možnosti. Nezapomeňte také, že program je nutné spouštět s právy administrátora.



Po spuštění programu by mělo být prvním krokem spuštění skenu – stačí jen kliknout na tlačítko »Scanner«. Po rychlém prověření systému se v okně programu objeví shrnutí zjištěných informací, ve kterých se vyzná i laik. Vzhledem k chybějící aktualizaci programu bohužel UPM nezná nové verze systémových procesů, a proto je označuje jako neznámé.



Pokud si chcete ověřit, zda váš systém skutečně neovládl malware, klikněte na »Další nástroje« a zde zaměřte svou pozornost na kartu »Po spuštění«. Níže vidíte vzor výstupu z webu autora programu, na kterém je nalezen malware.

Klíč	Hodnota	Data	Parametr
HKCU Run	CTFMON.EXE	C:\WINDOWS\system32\ctfmon.exe	
HKCU Run	taskdir	C:\WINDOWS\system32\taskdir.exe	
HKCU Run	3469a83f.exe	C:\Documents and Settings\Raya\Local Settings\Data a...	
HKLM Run	VMware Tools	C:\Program Files\VMware\VMware Tools\VMwareTray.exe	
HKLM Run	VMware User P...	C:\Program Files\VMware\VMware Tools\VMwareUser.exe	
HKLM Run	winsync	C:\WINDOWS\system32\paqkcq.exe	reg_run
HKLM Run	3469a83f.exe	C:\WINDOWS\system32\3469a83f.exe	
HKLM Sh...	PostBootRemin...	C:\WINDOWS\system32\SHELL32.dll	
HKLM Sh...	CDBurn	C:\WINDOWS\system32\SHELL32.dll	
HKLM Sh...	WebCheck	C:\WINDOWS\system32\webcheck.dll	
HKLM Sh...	SysTray	C:\WINDOWS\system32\stobject.dll	
HKU Run	CTFMON.EXE	C:\WINDOWS\system32\CTFMON.EXE	