Bojovník proti spywaru

NAJDETE NA NAŠEM CD

KVALITNÍ A TÉMĚŘ ZADARMO

VOJTĚCH BEDNÁŘ

Obáváte se, že se ve vašem počítači nacházejí nevítaní špióni? Spyware je téměř všudypřítomným rizikem. Naštěstí proti němu existuje celá škála obranných prostředků. Spybot Search & Destroy je jedním z těch nejlepších, a co více, je zadarmo.

Spyware je souhrnné označení používané pro několik různých věcí, všechny ovšem souvisejí s internetem a určitým druhem aplikací nebo obsahu. Asi největšího rozšíření dosáhly cookies, tedy webové „sušenky“ serverů, sledující činnost uživatele. Na základě záznamu, na co všechno se uživatel díval, mu lze adresovat reklamu.

O něco složitějšími jsou moduly, které aktivně sledují uživatele počítače. Nejde už jen o to zjistit, jaké servery osoba sedící za počítačem navštěvuje, ale také jaké programy používá, které dokumenty otevírá a co vlastně dělá. Výsledkem takovéhoto sledování jsou informace, které daný modul odesílá svým majitelům. Posledním, a zdaleka nejnebezpečnějším druhem nechtěných softwarových hostů jsou programy zvané dialery. Ty slouží ke zprostředkovávání většinou pornografického obsahu tak, že přesměrují vytáčené připojení k internetu na placené linky v zahraničí.

Nechtěný software některého z předchozích typů se do PC může dostat mnoha různými způsoby. Instalace z webových stránek je pouze jednou z variant. Spyware obsahují standardně i instalační balíky různých bezplatných aplikací, typicky klientů P2P sítí, různých manažerů stahování, dokonce i multimediálních přehrávačů.

Existují samozřejmě aplikace, které se snaží nezvané aplikační moduly různého typu v prostředí Windows jednak vyhledávat, a jednak eliminovat. Mezi nejznámější patří program Ad Aware německého Lavasoftu. Kromě něj ale existuje jiný, velmi kvalitní nástroj jménem Spybot Search & Destroy, kterému se budeme věnovat dnes.

Instalace programu pro Windows (funguje na všech operačních systémech typu Win32) má velikost přibližně 2,5 Mb a lze ji stáhnout z adresy autora *http://security.kolla.de*. Po jejím spuštění je nutné vybrat několik standardních možností včetně komunikačního jazyka (nechybí čeština), potvrdit licenční ujednání a program je připraven k použití.

Spybot Search & Destroy (S&D) je tvořen jedním hlavním oknem. Mezi jeho jednotlivými funkcemi se pohybujeme pomocí ikon v liště na levé straně rozdělené do několika kategorií. Celé to vzhledem nápadně připomíná známou aplikaci Microsoft Outlook, a vlastně vše co je od ní odvozeno. Aplikace podporuje skinování, takže její vzhled můžeme do jisté míry ovlivnit. Tou jistou mírou rozumíme změnu barev a několika obrázků, představujících základ motivu. Několik motivů je součástí standardní instalace, další lze doplnit aktualizací, o té ale až za chvíli.

JAK TO FUNGUJE?

S&D není ve skutečnosti vyhledávací aplikací klasického typu, ale jen jejím funkčním rámcem. V něm pracují moduly, které se specializují na vyhledávání různých druhů spywaru, malwaru, dialerů, sledovacích cookies a mnoha dalších zajímavých PC parazitů. S&D, respektive jeho vyhledávací složky, nepředstavují žádnou antivirovou ochranu, i když některé prvky, jež jsou schopny najít a odstranit, vyhledávají i moderní antivirové aplikace.

Samotná činnost hlavní funkce programu, podle které vznikl i jeho název, je rozdělena do dvou fází. V první dojde ke spuštění prohledávacích modulů. Ty zjistí, zda se v počítači nenachází to, na co jsou nastaveny, a výsledek svého pátrání zobrazí uživateli. Ve druhé fázi je možné označit „problémy“, které si uživatel přeje opravit. Pak dojde k samotné nápravě.

Pokud by si někdo představoval, že spywarový modul nejlépe zneutralizujeme tím, že jej vymažeme z disku, registrů a paměti počítače, pak se mýlí. Tím by sice došlo k eliminaci nechtěného vetřelce, ale dost možná i aplikace, se kterou byl nainstalován. S&D pozná, kdy je bezpečné nalezeného vetřelce odstranit a také to učiní. V některých případech ale soubory spywarové aplikace nebo modulu nahradí jejich neškodnými imitacemi. Tím se u mnoha programů, které je instalují, zachová korektní činnost, u mnoha ale také ne.

Jinou funkcí S&D je schopnost během kontroly vyhledávat záznamy o používání, nedávných adresách a chování uživatele vůbec, vytvořené konvenčními aplikacemi a operačním systémem a také místa, kde si některé známé aplikace vytvářejí jednoznačné identifikační prvky. Mezi tyto aplikace patří třeba populární Windows Media Player. S&D navíc dokáže vyhledávat a s určitou jistotou i opravovat nesrovnalosti v systémovém registru Windows, tato funkce se podobá analogickým funkcím, obsaženým v Norton Utilities nebo v Ontrack System Suite.

ABY TO FUNGOVALO

Stejně jako vznikají neustále nové viry a proto musí být antivirový systém aktuální, vzniká i nový spyware. S&D má zabudovanou funkci aktualizace z internetu. Tato aktualizace ovšem nespočívá pouze v dodávání nových definic hledaných modulů nebo dat. Program je neustále vyvíjen, autoři přidávají postupně nové jazykové mutace, zdokonalují ty stávající, vylepšují hlavní aplikaci. Pomocí aktualizačního systému lze stahovat všechny části tvořící S&D. Důležité je, že si uživatel může vybrat, co chce stáhnout a nainstalovat, a co nikoliv, podpora například turečtiny v našich podmínkách příliš užitečná asi nebude.

PROBLÉM

S&D dělá v rámci možností kvalitně svou práci. Jeho hlavním úkolem je odstraňovat spyware, malware a podobné „smetí“. Problémem je, že právě toto smetí se někdy do PC dostává spolu s jinými aplikacemi. Integrace spywaru je pro mnoho autorů způsob, jak umožnit bezplatné používání svých programů. Jeho přítomnost je zakotvena v jejich licenčních podmínkách, a odstranění proto znamená porušení těchto podmínek. Některé aplikace navíc funkci vedlejších modulů aktivně kontrolují (proto je S&D nahrazuje imitacemi). Je otázkou, nakolik je neutralizace špionážního modulu vlastně fér. Na tuto skutečnost upozorňují samotní autoři S&D, konečné rozhodnutí je ovšem vždy na uživateli.

CO JEŠTĚ?

S&D dokáže zobrazit obsáhlý seznam „opt out“ adres různých e-mailových bulletinů rozesílajících nevyžádanou poštu. To je užitečné, pokud se chceme zbavit nechtěných e-mailů, ale nevíme jak a kde.

Umí projít seznam instalovaných komponent typu ActiveX, seznam spuštěných procesů (to je užitečné především na Windows 9x). Obsahuje také informační knihovnu spyware modulů.

V ní je možné k většině špiónů najít doplňující informace, ujednání o soukromých údajích a další zajímavosti. Je to opět funkce podobná té, která se považuje za standard ve světě antivirových programů. Velmi obsáhlé jsou rovněž možnosti nastavení samotného programu, jeho prostředí a také seznamu detekčních modulů, jež mají být spouštěny při každém testování. S&D je vybaven možností aktivního feedbacku v případě, že se v aplikaci objeví chyba nebo jiný, abnormální stav. Protože aktuální verze je ale dostatečně stabilní, průměrný uživatel si této funkce příliš neužije.

Poslední podstatnou funkcí je možnost vrácení změn. Pokud si například neutralizujeme špionážní modul v nějaké aplikaci a ta pak odmítne spuštění, nemáme přístup k jejím datům. Modul lze zpětně rekonstruovat, data zachránit a aplikaci i se špiónem pak odinstalovat. Bohužel, funkce obnovení nefunguje vždy zcela korektně.

NENÍ VŠECHNO ZLATO...

Nic není dokonalé a o volně šiřitelných programech to platí dvojnásob. Asi největší slabinou S&D je jeho start. Aplikace se spouští opravdu pomalu. Přestože hardwarová náročnost není kritická (na P120 funguje bez problémů), S&D zkonzumuje poměrně hodně paměti. Aplikace umožňuje určit prioritu procesu při hledání spywaru, mohu doporučit nastavit spíše nižší.

V některých případech došlo při použití S&D k zajímavé situaci. Program objevil špionážní modul, ale při pokusu o jeho odstranění oznámil, že se nějaká část nebo soubor právě používají. Po restartování počítače a novém testu již tuto část opravil, avšak při opakovaném otestování našel celý, již opravený modul znovu. Těžko říct, zda se jednalo o tak neoblomného špióna nebo chyby v S&D, spíše bych ale řekl, že na vině je to druhé.

Další problémy mívá, nebo alespoň donedávna mívala, aktualizace S&D. Po načtení seznamu aktualizovaných komponent a zahájení jejich stahování došlo k zaseknutí aplikace. To nebylo způsobeno její chybou, ale nepřístupností serveru s aktualizacemi. Momentálně je možné si vybrat z několika serverů obsahujících aktualizace, a k této chybě již nedochází. V každém případě byla velmi nepříjemná a může se teoreticky objevit kdykoliv znovu.

S&D kromě těchto zmíněných obsahuje několik dalších menších chybiček a nedodělků. Vesměs nejsou nijak kritické pro samotný provoz aplikace, jen občas dokáží zkomplikovat život. Protože se ale nejedná o profesionální produkt, je nutné s přítomností takových nepříjemnůstek počítat.

ZAPLAŤ A POUŽIJ

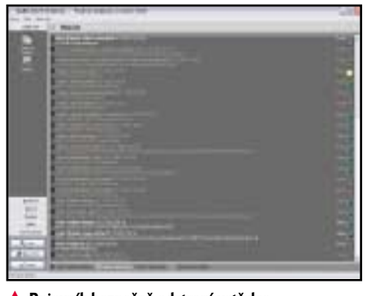
Spybot Search&Destroy je aplikace dostupná zadarmo, nejde o žádný shareware nebo omezenou demoverzi. Jeho autor přesto na svých stránkách vyzývá uživatele, aby přispěl na vývoj malou částkou. Implicitně se požaduje pět amerických dolarů. Bohužel, pro jejich výběr je používán systém PayPal, který v našich podmínkách není zatím příliš použitelný, Spybot Search & Destroy tak zůstává v podstatě zadarmo. A za tu cenu se jedná o velmi užitečnou aplikaci.

Spybot Search & Destroy má své nedostatky a má své přednosti. Pokud je váš počítač trvale připojen k internetu a síť také aktivně používáte, je velmi dobré pouvažovat o jeho nainstalování.

Program neobsahuje rezidentní ochranu, a proto je třeba jej také pravidelně používat a starat se o aktualizaci jeho definic. V případě, kdy k síti připojeni nejste, je pro vás Spybot Search & Destroy zbytečný. Na každý pád se ovšem jedná o zajímavého a užitečného pomocníka. 3 0062/FEL ❑

▲ S&D umí aktualizovat z internetu

▲ S&Destroy vám pomůže v boji proti spywaru



▲ Bojovník bezpečně odstraní vetřelce