Nedejte špiónům šanci

Pohybují se skrytě. Registrují aktivity na vašem osobním počítači. Manipulují s vaším systémem. Špióni se uhnízdili ve vašem počítači a sledují vás. Proto je třeba se jim bránit.

Daniel Behrens

Slídivý software se na vašem počítači uchytí rychleji, než si dokážete představit. Může přitom jít například o spyware, který se instaluje spolu s nějakým drobným programem. Může se rovněž jednat o trojské koně, které se šíří vinou nedostatečného zabezpečení Windows nebo Internet Exploreru. Je ovšem také docela dobře možné, že vám na služebním osobním počítači nainstaloval kontrolní program váš zaměstnavatel, aniž vás o tom uvědomil.

Špióni se sice pokoušejí ukrýt, jak jen to jde, přesto však existují příznaky, které je prozradí. Například když se vám v nepravidelných intervalech otevírají reklamní pop-up okna, přestože nejste zrovna připojeni k internetu. Nebo váš systém neustále přenáší data na internet, aniž k tomu vy sám dáváte jakýkoli podnět. Je také možné, že úvodní stránka vašeho prohlížeče je pozměněná a vám se tuto změnu vůbec nedaří odstranit.

Nejpozději v okamžiku, kdy váš počítač začne vykazovat podobné chování, měli byste ho důkladně vyčistit. Zde se dozvíte, jak na to a jaké nástroje vám při tom mohou pomoci.

Spyware

Spyware je dosti rozšířený, ale naštěstí není úplně na každém počítači. Každému počítači však napadení hrozí. Spyware není tak nebezpečný jako červi a trojské koně. Zpravidla nijak nepoškodí osobní počítač, ani se samostatně nedokáže podstatněji rozšířit. Zato však sleduje vaše uživatelské návyky. Některé druhy spywaru hlásí svému autorovi, kdy používáte osobní počítač, které internetové stránky si prohlížíte a na jaké reklamy klikáte.

Obzvlášť nehorázné typy spywaru otevírají v nepravidelných intervalech reklamní okna - přestože vůbec nesurfujete po internetu, ale třeba jen píšete nějaký text.

Šíření spywaru prostřednictvím oblíbeného freewaru

Spyware se ve většině případů šíří přes hostitelský program. Bezplatná verze aplikace Kazaa je toho názorným příkladem.

Obsahuje Kazaa Spyware?

Výrobce aplikace Kazaa popírá, že by jeho produkt obsahoval spyware. Tvrdí, že v tomto případě nejde o spyware, jelikož uživatel je na tyto komponenty upozorněn při instalaci. Tento názor ovšem nesdílíme.

Při instalaci jste sice víceméně jasně upozorněni na to, že Kazaa je financována reklamou od firem Cydoor a GAIN Network. Kromě toho se dozvíte, že se nainstalují "Altnet Peer Points Manager Package" a panel nástrojů "My Search". Jaká data tyto pochybné komponenty sbírají a vyhodnocují se ovšem uživatel dozví pouze tehdy, přečte-li si několikastránkové licenční podmínky, které jsou částečně v angličtině. Často až teprve na tomto místě objeví zvláštní prohlášení o ochraně dat na internetu.

Celkem vzato je bezplatná verze apliakce Kazaa velmi neprůhledná, alespoň co se týče připojeného spywaru. Někteří uživatelé proto používají neoficiální **Kazaa Lite K+ 2.6.1** - bezplatnou variantu, kterou vynalézaví programátoři zbavili špionážních komponent. Kazaa je zvláště křiklavým příkladem toho, jak se spolu s oblíbeným programem může mezi lidmi masově šířit spyware. Naštěstí jsme v současnosti nezaznamenali žádný další případ takového rozsahu a dosahu.

Prominentní spyware

Následující velmi známé programy obsahují spyware a šíří se přes webové servery: Gagot eWallet pro vyplňování formulářů, Date Manager, což je kalendář a plánovací diář pro Systray, konečně i Precision Time, nástroj, který seřizuje hodiny osobního počítače podle serveru s atomovými hodinami na internetu. Vlastní funkce těchto programů jsou užitečné. Všechny ovšem obsahují spyware.

Spywarová infekce: buďte opatrní při surfování

Spyware se může skrývat nejen v instalacích softwaru. I při surfování na webu se vystavujete riziku, že se na vás nalepí špionážní komponenty - ne snad na velkých a důvěryhodných webových serverech, nýbrž v postranních uličkách webu, do nichž se dostanete např. v důsledku zmanipulovaných výsledků nabídnutých vyhledávacím strojem.

Šiřitelé spywaru proto popisují své webové stránky hojně používanými vyhledávacími výrazy a pojmy, aby se dostali do indexů vyhledávacích strojů. Při návštěvě takové stránky uvidíte odkaz s názvem "Bezpečnostní varování (Security warning)", který vás upozorní na instalaci nějaké komponenty. V takovém případě byste neměli ze zbrklosti nebo z pouhého zvyku kliknout na "Ano", popřípadě na "Spustit instalaci".

Když se bezpečnostní výstraha objeví na stránce, kterou neznáte, ukončete dialog stisknutím tlačítka "Ne", popřípadě "Neinstalovat". Pokud se výstraha objeví na důvěryhodné stránce, pozorně si ji přečtěte. Mohlo by se totiž jednat o komponentu, která je pro prezentaci stránky nezbytná, například Macromedia Flesh Player.

Nejtroufalejší šiřitelé spywaru využívají na svých webových stránkách mezer v zabezpečení Internet Exploreru (IP), aby vám vnutili špionážní programy bez vašeho vědomí. Snažte se proto provádět vždy poslední, nejčerstvější aktualizace svého prohlížeče nebo používejte jiný prohlížeč, například **Firefox 1.5** (zdarma ke stažení například ze stránek *www.firefox.cz*).

Firefox má mnoho dalších předností: je nejen bezpečnější, ale mnohdy též rychleji načítá stránky. Je vybaven větším počtem funkcí než IE a o další jej lze ještě rozšířit pomocí doplňkových funkcí.

Najít spyware a odstranit ho: takhle se to dělá

K detekci a odstranění již nainstalovaného spywaru je nejlepší použít nějaký specializovaný nástroj. Počítač můžete nechat prohledat pro jistotu několikrát za sebou. Doporučit můžeme například program **Ad-Aware SE Personal 1.06** (pro soukromé použití bezplatný, na našem CD) a **Spybot Search & Destroy 1.4** (zdarma, na našem CD). Poměrně nový program je **Microsoft Antispyware**. Nejde o vlastní produkt Microsoftu, pochází od Giant Company Software. Microsoft koupil tuto společnost v prosinci roku 2004. V době psaní tohoto článku byl Antispyware ještě betaverzí, ve verzi 1.0.701 jej naleznete na našem CD. Zatím se jedná o freeware.

Instalace a obsluha antispywaru je jednoduchá. Při prvním spuštění programu vás průvodce naviguje při konfiguraci. Ptá se vás, zda si budete přát automatické aktualizace (podobně jako je tomu u antivirových programů) a zda budete chtít aktivovat ochranu v reálném čase. V posledním kroku určíte, zda má nástroj po druhé hodině v noci spouštět vyhledávání spywaru, pokud váš osobní počítač bude zapnutý. Tuto možnost lze odmítnout, pokud jste si nastavili ochranu v reálném čase.

Po instalaci spustíte skenovací proceduru tlačítkem "Run Quick Scan Now". Standardně Antispyware prohledává pouze místa, na nichž se nejčastěji zachytává. Chcete-li prohledat celý pevný disk, klikněte na "Spyware Scan Options" a zvolte "Run a Full System Scan." Prohledávání pak ovšem zabere podstatně delší dobu.

Po skenování získáte přehledný seznam výsledků. Na něm se ukáže mimo jiné název každého typu nalezeného spywaru a jemu odpovídající bezpečnostní riziko. Když u nějaké položky kliknete na "+", spatříte všechny příslušné soubory a záznamy v registru. U každého nálezu navrhne Antispyware příslušnou akci, kterou můžete potvrdit nebo pozměnit, například "Remove" (Odstranit) nebo "Ignore"(Ignorovat). Tlačítkem "Continue" spustíte čisticí proceduru. Uživatelé Windows XP by měli nejprve aktivovat volbu "Create Restore Point", aby se v případě selhání systému vytvořil ve Windows záloha pro obnovení.

Strážci v Antispywaru: Ochrana v reálném čase poskytovaná systémem Microsoft Antispyware chrání vyčištěný počítač před novým spywarem. Pokud jej během instalace aktivujete, poběží na pozadí permanentně. Poté jej máte možnost zapínat či vypínat přes "Real-time Protection", přičemž musíte aktivovat, popřípadě deaktivovat všechny tři položky "Agents".

Nástroje upozorňují na podezřelé procesy

Vyčistili jste svůj osobní počítač pomocí několika antispywarových programů, přesto se však nemůžete zbavit dojmu, že ještě něco přehlédly? Systém nadále vykazuje chování, signalizující přítomnost spywaru?

V takovém případě je třeba, abyste sami přiložili ruku k dílu a podívali se, které procesy běží na vašem PC - samozřejmě za předpokladu, že máte administrátorská práva. Nejprve si opatřete nástroj, který ukazuje i skryté procesy, například **Process Viewer 3.7** (zdarma, na našem CD).

Na tomhle programu je dobré zejména to, že ukazuje i oblast, kde se právě běžící procesy odehrávají. Podle jmen adresářů můžete zhruba odhadnout, který z nich by mohl odpovídat nežádoucímu programu.

Spyware se může ovšem v adresáři Windows usadit pod takovým jménem, že ho sotva rozeznáte od jmen důležitých systémových souborů. Pak se musíte řídit detektivním instinktem. Otevřete příslušný adresář, klikněte na podezřelý soubor pravým tlačítkem myši a vyberte položku "Vlastnosti/Verze". Pod "Popisem" by mělo ;být uvedeno jméno, které má jistou vypovídací hodnotu pod "Copyrightem" by měl být uveden původce. Na tom, nakolik je původce ochoten poskytovat o sobě další informace, záleží také to, zda o něm najdete další informace i v polích "Komentáře" nebo "Zvláštní popis".

Pokud se ani s těmito informacemi nedá mnoho pořídit, může vám pomoci, vyhledáte-li si v Googlu jméno souboru. To platí i v případě, že v souboru není k dispozici žádná informace, jež by vás mohla nasměrovat někam dál, registrační karta tedy neukazuje "verzi". S nástrojem **pcwProcview** (na našem CD) probíhá hledání

opravdu pohodlně. Zobrazuje seznam všech probíhajících procesů a nabízí možnost "Hledat v Googlu". Protože pcwProcview pracuje pod Windows 95/98 a NT 4, musíte si ze stránek *www.pcwelt.de/6e5* nainstalovat **Microsoft WMI** (Windows Management Instrumentation).

Únos

Po delším surfování internetem si povšimnete, že se změnila domácí stránka vašeho prohlížeče. Při každém spuštění se místo vámi nastavené úvodní stránky objeví podivný vyhledávací stroj.

Únos prohlížeče: právě to se vám přihodilo

Zřejmě jste se stali obětí únosu prohlížeče. Nekalé živly na internetu využívají nedostatků v zabezpečení prohlížeče - zpravidla Internet Exploreru - k tomu, aby vám podstrčili nějaký prográmek. Ten pak běží trvale na pozadí a snaží se, aby se změnilo nastavení domácí stránky prohlížeče a aby nová startovací stránka už zůstala zachovaná - i když se snažíte tuto chybu v konfiguraci prohlížeče odstranit.

Jak se únosců prohlížeče zbavit

Zbavit se nechtěných hostů na vašem osobním počítači je občas docela těžké. Částečně se totiž zabydlí hluboko v systému. V tom nejjednodušším případě antispywarové programy rozpoznají software, který je zodpovědný za únos, a odstraní ho.

Beplatný nástroj **CW-Shredder 2.12** (na našem CD) vymaže únosce, kteří přesměrovali domácí stránku na Coolwebsearch a jeho varianty.

Vydělávání peněz únosem

Většinou se domácí stránka nastaví na vyhledávací stroje typu *www.coolwebsearch.com*. Díky většímu počtu lidí, kteří zavítají na takové stránky, mohou pak jejich provozovatelé požadovat vyšší cenu od zadavatelů reklamy. Coolwebsearch a jim podobní ovšem únosce sami nerozšiřují. Namísto toho dávají prémie "partnerům," kteří přitáhnou nové zákazníky. Oficiálně se sice provozovatelé tváří, že nespolupracují s žádnými partnery, kteří používají takové triky jako unášení prohlížeče. Ale na druhé straně vše nasvědčuje tomu, že proti nim nijak důsledně nepostupují, jinak by tento nešvar nebyl tak rozšířen.

Slídilové na internetu

K tomu, aby se pídil po důvěrných informacích a vašich heslech, se špión nutně nemusí vloupat do vašeho počítače. Může mu stačit jen přítomnost ve stejné síti, v níž se nachází i váš počítač. Pomocí speciálního slídicího nástroje (tzv. "snifferu") pak může zachytit všechny složky, které odesíláte a přijímáte. To může být nebezpečné zejména ve firemním prostředí, neboť tam bývají k jedné sítí připojeny stovky, někdy i tisíce spolupracovníků. Důvěrné e-maily, hesla a adresy požadovaných webových stránek představují jen několik příkladů, co všechno může zvědavý slídil tajně sledovat. Jestliže podnik či soukromý uživatel používá třeba špatně zabezpečený nebo dokonce úplně nezabezpečený bezdrátový přístup, mohou operace s daty odposlouchávat slídilové přímo z ulice - aniž jim hrozí, že by na ně někdo přišel.

Slídilové vás mohou napadnout i freewarovými nástroji

K tomu, aby vás začal sledovat, potřebuje špión nějaký "packet-sniffer", například **Ethereal 0.10.14** (zdarma na našem CD).

Jeho pomocí lze zachytit datové pakety a vyhodnotit je. Ethereal potřebuje k provozu program, který zachytává pakety - v našem případě například **Winpcap 3.1 beta 4**. Používejte prosím tyto nástroje pouze k testování zabezpečení vašeho vlastního systému.

Ethereal nefunguje, pokud jsou osobní počítače v síti propojeny přes switche (přepínače) a ne přes rozbočovače (huby). Tím, že budeme používat pouze přepínače, se nám do jisté míry podaří systém ochránit . Existují ovšem i dokonalejší nástroje než Ethereal. Manipulují směrovací tabulky počítače takovým způsobem, že směrují všechny datové pakety na osobní počítač špióna. Takovému útoku se říká "Man in the Middle Attack". Je přitom na pováženou, že příslušnými nástroji lze takto odposlouchávat i spojení zabezpečená přes protokol "https". Obrana proti tomu je náročná, například pomocí statických propojovacích tabulek.

Poznejte spyware sami - Process Viewer přitom pomůže. U každého procesu uvádí rovněž cestu (path) k místu, kde se nachází příslušný soubor.