Krádeže dat pomocí spyware

Stealing data via spyware

Jan Adámek

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan ADÁMEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Krádež dat pomocí spyware**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Objasněte pojem spyware a vysvětlete jeho nebezpečnost vzhledem ke krádeži dat.**
3. **Popište druhy spyware a uveďte příklady jednotlivých druhů.**
4. **Navrhněte základní opatření proti infiltraci spyware do počítače.**
5. **Porovnejte několik antispywarových programů, popište jejich aplikaci, porovnejte jejich výhody a nevýhody.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 200 s. ISBN 80-251-0106-1.**
2. **DOSEDĚL, Tomáš. 21 základních pravidel počítačové bezpečnosti. Brno: Computer Press, 2005. 56 s. ISBN 80-251-0574-1.**
3. **KOCMAN, Rostislav, LOHNISKÝ, Jakub. Jak se bránit virům, spamu a spyware. Brno: Computer Press, 2005. 152 s. ISBN 80-251-0793-0.**
4. **THOMAS, M. Thomas. Zabezpečení počítačových sítí. Brno: Computer Press, 2005. 344 s. ISBN 80-251-0417-6.**
5. **MITNICK, Kevin, SIMON, William. Umění klamu. Gliwice: Helion, 2003. 348 s. ISBN 83-7361-210-6.**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Práce mapuje oblast ochrany dat před zcizením prostřednictvím spyware. Specifikuje samotný pojem spyware, jeho chování a rozpoznání jeho přítomnosti v počítači. Dále sumarizuje jednotlivá opatření proti průniku spyware. V praktické části na příkladu tří konkrétních produktů a jejich vzájemného porovnání vysvětluje způsob použití od instalace, aktualizace, skenování, po odstranění spyware z počítače.

Klíčová slova: spyware, ochrana dat, antispywarové programy, adware, zranitelnost

ABSTRACT

Work presents data protection against theft via spyware. Specifies the concept of spyware, its behavior and recognize its presence in the computer. Further summarizes the various actions against spyware intrusion. In a practical example of the three specific products and their mutual comparison explains how to use the installation, update, scan, after removing spyware from your computer.

Keywords: spyware, data protection, anti-spyware programs, adware, vulnerability

Děkuji především panu profesorovi Ing. Miroslavu Matýskovi, Ph.D. za vedení při psaní práce.

Dále všem mým příbuzným, kteří nejprve klikají a poté naříkají, což mě přivedlo k výběru a zpracování tématu.

Nakonec vývojářům antispyware za kvalitní, každodenní, volně šiřitelnou ochranu.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

V dnešní době, kdy se použití počítače stává samozřejmostí a používání Internetu se stalo každodenní součástí našeho života, jak pracovního tak osobního, vzrůstá míra rizikovosti. S tímto soužitím se objevují čím dál větší hrozby.

Jsou má soukromá či firemní data v počítači opravdu v bezpečí? Je bezpečné provádět finanční transakce přes internet? Obavy rostou a čím víc do této problematiky člověk vidí, tím více získává dojem, že jediná bezpečná data jsou ta, která jsou na počítači, který není připojen do celosvětové sítě jménem Internet a i tato data mohou být do jisté míry ohrožena. Taková obava, může narůst do rozměrů paranoy.

Můžeme zajistit, aby byl náš počítač úplně v bezpečí? Kdo by se v dnešní moderní době obešel bez internetu? Bez ohledu na bezpečnost je to jeden z nejširších a nejrozsáhlejších zdrojů informací. Pokud člověk ví jak hledat je internet jako knihovna a najdete tam úplně vše. Jedinou nevýhodou bývá to, že ve chvíli kdy vejdete, stáváte se potenciálním cílem mnoha škůdců. Ohrožují vás viry, hackeři, spyware, podvodníci a mohou na vás číhat i jiná nebezpečí. Z toho důvodu se snažíme své osobní počítače všemožně chránit před čímkoliv nebo spíše kýmkoliv, kdo by mohl naše drahocenná data ohrozit, nebo je zneužít.

I pro pracovníky komerční bezpečnosti je otázka zabezpečení jejich dat velmi důležitá. Jak by asi vypadalo, kdyby někdo prestižní bezpečnostní firmě odcizil databázi jejích kontaktů, případně by zneužil z počítače získaná hesla do kritických systémů? Velké škody by rovněž mohly nastat zcizením technické dokumentace, případně únikem dat týkající se převozů peněz. A to už vůbec nemluvíme o tom, kdyby byly odcizeny spisy s osobními daty kupříkladu z detektivní agentury. Jakýkoliv únik takových informací jednak bere agentuře těžce nabytou prestiž, daleko závažnější ovšem je, že může ohrozit pracovníky, případně objekty, které daná agentura spravuje.

Proto je otázka bezpečnosti dat každodenním problémem, kterým je třeba neustále řešit. Práce se zabývá jen jedním aspektem tohoto nebezpečí a to programy, kterým se říká spyware. Na začátku je stručně charakterizuje, poté popisuje volně dostupné programy na ochranu proti nim a nakonec některé tyto spywarové programy popisuje.

I. TEORETICKÁ ČÁST

1 SPYWARE V POČÍTAČI

V této kapitole se práce zabývá pojmem spyware, statistikami četnosti jeho výskytu v počítačích, příznaky jeho výskytu v systému, jeho vlivem na samotný operační systém a možnými následky pro uživatele. Veškerou problematiku se snaží dostatečně vysvětlit a popsat tak, aby jí každý dobře porozuměl.

V práci je zařazen i některý škodlivý software, který podle některých odborníků informatiků není přímo spyware. Rozhodl jsem se tak z důvodu, že se přikláním k názoru, který chápe spyware komplexněji, spíše z pohledu antispywarových programů. Tento názor označuje, že cokoliv antispywarový software vyhledá, dá se považovat za spyware. Na této definici je postavena celá má práce.

1.1 Vysvětlení pojmu spyware

Pro vysvětlení pojmu spyware, ho porovnejme s definicí viru, která je známější. K pochopení hlavního rozdílu mezi virem a spywarem uveďme základní charakteristiku viru. Počítačové viry mají určitou podobnost s viry biologickými a to je kód, který se podobně jako u virů biologických dokáže kopírovat a šířit. Tyto viry zneužívají prostředků počítače bez vědomí uživatele a proti jeho vůli, většinou k poškození dat uživatele, či k úplnému hardwarovému zničení počítače. Kromě toho se stejně jako vir snaží svou přítomnost v počítači skrýt a během této doby odeslat za pomoci internetu co největší počet ukradených dat. Na rozdíl od virů se spyware masově nemnoží.

Ta nejjednodušší definice říká, že jde o program, který bez vědomí uživatele odcizuje „statická“ data jako je přehled navštívených stránek či soupis programů, které má uživatel ve svém počítači nainstalované, či jiná pro uživatele citlivá data. Tato data poté odesílá jinému uživateli. Kvůli těmto důvodům, je jejich přítomnost v systému nepříjemná a nežádoucí.

Idea při vytvoření spyware, byla jako vždy mírumilovná a zdánlivě prospěšná. Spyware měl pouze zjišťovat různé informace z důvodu různých průzkumů a zjištěné informace měli být využity pro cílenou reklamu. Z toho je ovšem patrné, že zneužití takového programu se přímo nabízí, bylo jen otázkou času, kdy budou tyto prostředky použity ke zcizení citlivých dat, jako jsou například čísla kreditních karet, hesla k různým službám, případně zcizení celých dokumentů. Většina uživatelů je rozhořčena už jen samotnou existencí spyware tím spíše jejich legálností. [1]

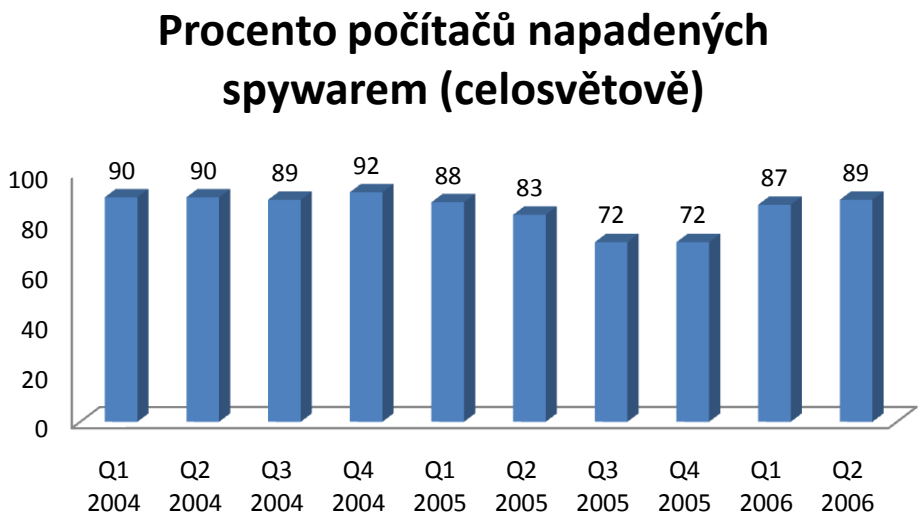
1.2 Statistiky Spyware

Navzdory publicitě o růstu nebezpečné infekce spywarem, počet nakažených počítačů roste. Podle dat skanu firmy Webroot spyware je vidět, že takřka 89% počítačů je infikováno spywarem.

Programátoři spyware neustále modifikují své programy, jejich způsoby instalace tak, aby tyto programy byly hůře detekovatelné. Používají ke svým útokům rootkity (způsob, kterým se snaží zamaskovat svou přítomnost v PC) a kernel driver level (v úrovni operačního systému) technologii, kterou používají k schování před antispywarovými aplikacemi.

1.2.1 Růst 2004 -2006

Průzkumy za rok 2004 - 2006 dokazují, že spywarové ohrožení se kolísavě pohybuje od 70% do 90%.



Obr. 1. Graf celosvětového napadení počítačů spywarem[1]

To ze spywaru dělá velkou hrozbu, když si uvědomíme, že ze 100 počítačů je 70 až 90 napadeno škodlivým software a tím mohou být jejich soukromá data ohrožena, dá se předpokládat, že tyto údaje od posledního průzkumu z roku 2006 spíše rostou.

[1] Graf byl převzat z: http://www.webroot.com/resources/stateofspyware/excerpt.html

Z tohoto grafu dále vyplývá, že mnoho volných programů na odstranění antispyware nedosahuje potřebného stupně zabezpečení. Ne vždy poskytují dostatečnou detekci škodlivého software a tím nejsou schopny spyware vůbec kvalitně odstranit.

Zvýšená infekce spywarem také dokazuje, že i když uživatelé používají k ochraně svého počítače antispywarový program, není tento dostatečně sofistikovaný, případně ho zapomínají aktualizovat, či vůbec řádně kontrolovat obsah svého počítače.

Firma Webroot v letech 2004 – 2006 skenovala náhodně vybraných 1000 počítačů se zaměřením na přítomnost spywaru, tabulky níže ukazují průměr nakažení na jeden počítač (Tab. 1). Zajímavým údajem níže uvedených statistik je, které státy na tom byly podle výzkumu firmy Webroot celosvětově nejhůře. Většina těchto států jsou buď exotické destinace, nebo země třetího světa. Z toho vyplývají dva možné důvody, proč je tam tak vysoký podíl spywaru.

Za prvé nedostatečné zkušenosti a malá informovanost obyvatelstva o této hrozbě. Za druhé podcenění hrozby, nebo navýšení díky turistickému ruchu, kdy turisté zapomínají s exotickou destinací na jakoukoliv bezpečnost. Což je ovšem spíše nepravděpodobné, ale možné.

Tab. 1. Celosvětové hodnoty spyware[2]

Celosvětové hodnoty Spyware Největší počet spywaru na 1 počítač z 1 000 skenovaných podle země		
Q2 2006 pozice	**Země**	**Množství**
1	Puerto Rico	42,6
2	Algerie	38,4
3	Bahrain	35,7
4	Dominikánská republika	35,1
5	Trinidad a Tobago	33,8

Dále zde máme stejnou statistiku, tentokrát jen pro Evropu (Tab. 2), ve které nejhůře dopadlo Spojené Království. Ze statistik je vidět, že země EU jsou na tom více méně stejně a to něco kolem 30 spyware na počítač. Tento údaj je docela překvapivý, když si uvědomíme, co se za ním skrývá. Každý má na svém počítači něco kolem třiceti nechtěných programů, které v lepším případě minimálně brzdí systém.

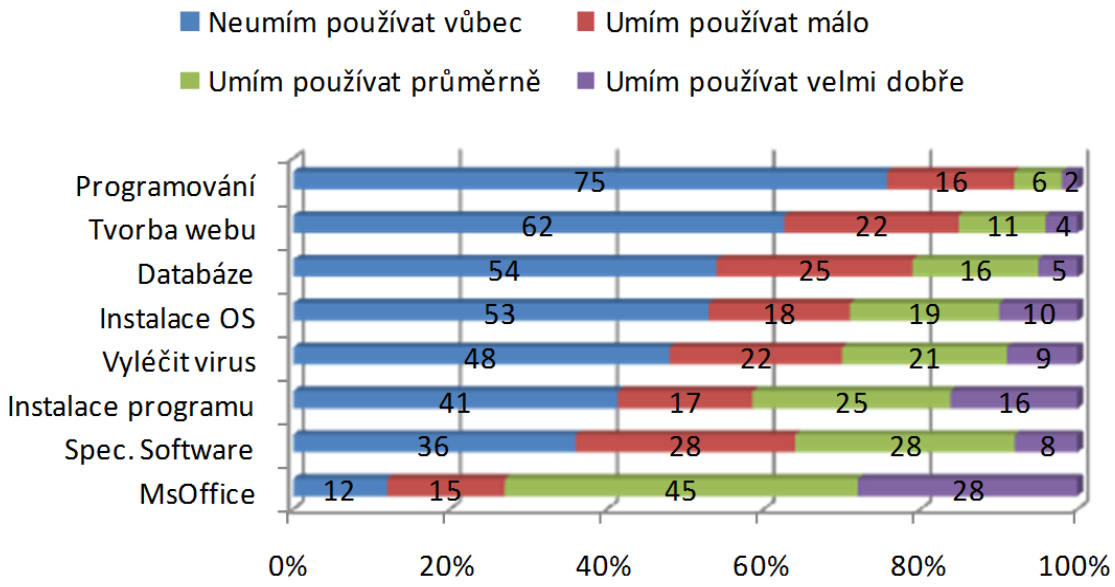
[2] Tabulka byla převzata z: http://www.webroot.com/resources/stateofspyware/excerpt.html

Tab. 2. Evropské hodnoty spyware[3]

Evropské hodnoty Spyware Největší počet spywaru na 1 počítač z 1 000 skenovaných podle země v Evropě		
Q2 2006 pozice	**Země**	**Množství**
1	Spojené Království	30,5
2	Irsko	30,3
3	Litva	29,3
4	Lotyšsko	26,5
5	Norsko	26,1

1.2.2 Stav v České republice

Z vlastních zkušeností s počítačem a problematikou spyware mohu potvrdit, že infiltrace spywaru do počítače není nic obtížného.



Obr. 2. Graf dovedností s počítačem[4]

Na počítači s nainstalovaným firewallem, antivirovým programem a antispywarovým programem s pravidelnou aktualizací, po měsíčním užívání počítače, antispywarový program detekuje přibližně 40 spywarů.

---

[3] Tabulka byla převzata z: http://www.webroot.com/resources/stateofspyware/excerpt.html

[4] Graf byl převzat z: SOUKUP, Petr, et al. *Češky a Češi v kyberprostoru* [online]. Praha : MV ČR, 2008. 194 s. Výzkumná zpráva. UNIVERZITA KARLOVA V PRAZE, FAKULTA SOCIÁLNÍCH VĚD, Institut sociologických studií. Dostupné z WWW: <www.mvcr.cz/soubor/cyber-vyzkum-fsv-zprava-pdf.aspx>.

Podle výzkumu Fakulty sociálních věd Univerzity Karlovy z roku 2008 (Obr. 2), může být vzhledem ke stavu počítačových dovedností samotný výskyt škodlivého software v počítači problém.

Zde je vidět, že pro 48% české populace je těžké, takřka nemožné se vypořádat s virem, což se týká i odstranění spyware z počítače. To je další důvod, proč není radno tuto hrozbu podceňovat a proč je potřebné řádně o ní veřejnost informovat a proškolit ve způsobech odstranění škodlivého softwaru z počítače.

1.3 Příznaky výskytu spyware v počítači

Příznaky výskytu škodlivých programů v počítači mohou být různé, od celkového zpomalení vašeho počítače k vyskakování takzvaných pop-up oken, které samotné prohlížení internetu značně znepříjemňují. Některé tyto příznaky byly podrobněji rozebrány níže.

1.3.1 Neustálá změna domovské stránky

Jedná se o změnu nastavení domovské stránky na stránku nebo webový server, který nechcete používat jako domovskou stránku, přesto se tak děje. Většinou se nastavení dá opravit, avšak po restartu systému je zase zpátky nastavena nechtěná domovská stránka. Tento spyware je vlastně neškodný. Jedinou jeho nevýhodou je, že uživatele ustavičně obtěžuje. Na druhou stranu na sebe upozorní a vy jako uživatel máte možnost se ho co nejdříve zbavit.

1.3.2 Celkové zpomalení počítače

Jeden z projevů spyware v počítači je také celkové zpomalení systému, protože spyware je přeci jen program, který běží na pozadí vašeho systému. To znamená, že využívá jistý podíl systémových prostředků jako každý jiný software, ovšem bez uživatelova vědomí. Proto kolísání výkonu systému může být jedním z příznaků přítomnosti škodlivého softwaru na vašem počítači.

1.3.3 Vyskakování takzvaných pop-up oken při prohlížení internetu

Dalším projevem bývá vyskakování pop-up oken, které stejně jako změna domovské stránky není nikterak nebezpečné, jako spíš otravné. Jde vlastně o náhodné vyskakování oken při prohlížení internetové sítě. A je to jen další důkaz přítomnosti spyware.

1.3.4 Přesměrování telefonní linky

Na přesměrování telefonní linky většinou přijde uživatel ve chvíli, kdy obdrží velmi drahý účet za telefon. Přesměrovávací spyware se používal v době, kdy se na internet připojovalo pomocí modemu. Funkcí Spyware bylo, že při připojení pomocí modemu bylo číslo vašeho připojení přesměrováno na čísla se zvláštní tarifikací a každá minuta surfování uživatele například stála 60 Kč.

1.3.5 Nestabilita operačního systému

Programy typu spyware nejsou většinou kompatibilní jak s různými operačními systémy, tak s různým hardwarem v počítači, a to z důvodu, že to není potřeba. Jedná se přeci jen o škodlivý software a z toho důvodu jej není nutno odlaďovat, jako jiné námi používané softwary. Tato nekompatibilita může způsobit pád systému, jeho špatnou funkci či časté „zamrzání“ počítače.

1.3.6 Záhadně se objevující ikony nebo jiná záhadná činnost počítače

Ve chvíli, kdy začínáte mít pocit, že váš počítač žije vlastním životem, objevují se záhadné ikony, podivné dokumenty a podobně, je pravděpodobné, že váš počítač je již napaden některým takovým škodlivým softwarem.

2 DRUHY SPYWARE

Spyware je široký pojem, který zahrnuje velké množství škodlivého softwaru, jehož společná definice je infiltrace a utajený provoz bez upozornění uživatele počítače. To platí na většinu toho „horšího“ spyware. Ten „lehčí“ vás bude jen neustále otravovat a znepříjemňovat vám život a tím na sebe upozorňovat, což by mělo být pro uživatele dostatečně alarmující, že jeho počítač není dobře zabezpečen vůči takovým hrozbám.

Škodlivý software dělíme podle způsobu jeho činnosti. [3]

2.1 Adware

Většinou je součástí software, který je volně šiřitelný. Ten může být doplněn reklamami, či důsledkem jeho nainstalování je „vyskakování“ oken, o která většinou uživatel ovšem nestojí. Také může jít o vyhledávací toolbar, který se vám nahraje do používaného prohlížeče.

Při instalaci takového volně šiřitelného, neplaceného softwaru musí uživatel před samotnou instalací souhlasit s takzvanou „EULA“ – End User License Agreement – licenčním ujednáním, které většina uživatelů ani nečte a jehož potvrzením většinou souhlasí se samotnou instalací aplikace adware do počítače.

Jiná možnost nechtěné instalace adware je při výběru jednotlivých komponentů softwaru, kdy je přidána i možnost nainstalování takovéhoto nedobrého softwaru, která je většinou primárně zaškrtnuta. Vydavatel softwaru spoléhá na ukvapenost a nepozornost uživatele, který komponenty neprozkoumá a pouze odsouhlasí „pokračuj“ v instalaci.

Dost často se stává, že po odstranění takto nainstalovaných adware může přestat fungovat software, s kterým byl adware nainstalován. Proto jsou někteří uživatelé ochotni adware trpět za možnost používat software zdarma. Někteří tvůrci adware jsou dokonce schopni vytvořit takovou aplikaci, kterou je obtížné odinstalovat, či dokonce sama aplikace je schopná provést protiútok a zmařit tak uživatelův pokus o nalezení, či odinstalování. Některé jsou dokonce schopny následné obnovy po smazání. [7]

2.1.1 Základní doporučená ochrana proti Adware

Doporučenou ochranou proti Adware je neinstalovat podezřelý software. Nezávisle na tom, jak je EULA nudná, uživatel by se měl přinutit ji přečíst celou před nainstalováním jakéhokoliv softwaru. Pokud máte jakékoliv pochyby či otázky ohledně licenčního

ujednání, kontaktujte společnost a požádejte je o ujasnění. Pokud vám nebude společnost schopna vysvětlit licenční ujednání, v žádném případě neinstalujte software do počítače.

V současné době existují stránky: http://www.spywareguide.com/analyze/index.php, které jsou schopny po vložení licence ji zanalyzovat a vyhodnotit, zda je součástí licenčního ujednání instalace škodlivého nebo nežádoucího obsahu. Bohužel fungují pouze pro anglický jazyk.

Jinou možností ochrany proti adware je mít nainstalovaný a aktualizovaný software na vyhledávání adware v počítači. Programy proti spyware se budu zabývat v další části práce.

2.1.2 Příklady Adware

2.1.2.1 ICQ

Jedním z pěkných příkladů chtěného adware, je ICQ. Tento program na instant messaging zná snad úplně každý. Jde o program na textovou, hlasovou a obrazovou komunikaci po internetu. Program je zadarmo- což je na jednu stranu pěkné, na druhou stranu je plný otravných reklam, které se načítají v samotném okně konverzace. Kde na uživatele pořád podprahově působí reklamy. Vzhledem k tomu, že reklamy jsou již nedílnou součástí programu, neexistuje způsob, jak se jich zbavit.

Jednou z možností jak se těmto reklamám bránit je používat jiné aplikace, přes které se na samotné ICQ připojíte. Ovšem jejich používáním porušujete licenční podmínky použití ICQ. Takovými programy jsou například: Miranda, QIP, Koppete..

2.1.2.2 Toolbary

Jsou zásuvné moduly neboli pluginy, které se přidají do prohlížeče. Většinou je obtížné je odinstalovat. Jde vlastně o přídavné lišty, které se implementují do Internet Exploreru, nebo jiného prohlížeče. Tyto obsahují kromě pomocných tlačítek, či rychlého vyhledávání na svých domovských stránkách i různé reklamy. Více o pluginech v kapitole Browser Helper Objects.

Příkladem těchto toolbarů jsou: Advanced search bar, Mirar, Oemji, Xang, atd.

2.2 Browser helper object

Byl představen v roce 1997 s vydáním 4. verze Internet Exploreru. Jde o dll modul, který byl navržen pro Microsoft jako plugin do Internet Exploreru. Jde o rozhraní pro programování aplikací (API), které dává programátorovi mnoho možností, které mohou být použity pro zdokonalení prohlížeče, nebo naopak zneužity proti uživateli.

API vlastně odhalilo cesty, jak BHO může přistupovat do objektového modelu dokumentu a tím umožnit přístup, modifikaci obsahu či struktury nebo stylu dokumentu a jeho částí.

Ty dobré BHO zjednodušují samotnou práci s prohlížečem. Ať už si nahrajete pluginy, které vám umožní otevřít ve webovém prohlížeči pdf soubory, aplikace napsané v Javě, či stránky vytvořené pomocí flashe.

Vzhledem k tomu, že má BHO neomezený přístup do modelu událostí Internet Exploreru, jde jej jednoduše zneužít. Například spywarové BHO může čekat na zabezpečené připojení k bankovní instituci a v tu chvíli zaznamenávat úhozy na klávesnici a ty dále odesílat. Zneužité také mohou být vzory, které zadáváte do vyhledávačů či toolbarů. Tyto mohou být rovněž zaznamenávány a odesílány třetí osobě.

Některé tyto objekty jsou v Internet Exploreru ihned viditelné- nové vyhledávácí lišty, nebo dokonce mění samotný vzhled vyhledávače. Ovšem ty ostatní běží bez viditelné změny interface programu. To vytváří velice přijatelné prostředí, pro tvůrce škodlivého kódu, které skrývá akce jím vytvořených aplikací. BHO zřídkakdy potřebuje vůbec povolení k jakýmkoliv dalším akcím po samotné instalaci. [7]

2.2.1 Příklady BHO

2.2.1.1 CISTrojan

CISTrojan použil BHO k instalaci skriptů, které provedly jistý počet příkazů, jako například přidání a mazání hodnot některých záznamů v registrech a dále stažení několika spustitelných souborů. Všechny tyto akce byly pro uživatele naprosto neviditelné a ten ani neměl ponětí o tom, že je jeho počítač napaden a že jsou jeho data ve vysokém nebezpečí. [8]

2.2.1.2 DyFuCA

Tento spyware nenapadl data jako taková, ale nahradil stránku, kterou vám zobrazí prohlížeč chybu při nedostupnosti stránky v Internet Exploreru za svou reklamní stránku. [8]

2.3 Hijacker Browser

Hijacker, neboli únosce prohlížeče je typ spyware, který buď přepisuje uživatelem nastavenou domovskou stránku, chybovou stránku, vyhledávací stránku v používaném prohlížeči za svou vlastní. V některých případech udělá škodlivý kód i přepis v registrech a tím docílí automatické přepisování domovské stránky vždy po startu počítače. V tomto případě vám nepomůže manuální přepsání domovské stránky v nastavení prohlížeče.

Tento spyware může v některých případech dokonce zakázat přístup na některé stránky. Například na stránky s antispywarovými programy. Dokonce se může stát, že budou umět zablokovat antivirus a antispywarový software.

Nejvíce únosců stránek zneužívá možnost Internet Exploreru spouštět ActiveX skripty přímo z webových stránek. Tyto programy zažádají o dovolení nainstalovat se přes pop-up okno, které vyskočí při otevření nějaké webové stránky. Pokud jim třeba i jen náhodou dáte svolení k instalaci, Internet Explorer spustí program na vašem počítači a změní vaše nastavení. Může jít jen o takřka nevinnou otázku: „Chcete tuto stránku nastavit jako domovskou?“.

Jiné zneužívají bezpečnostní díry v prohlížečích k tomu, aby se nainstalovaly bez jakéhokoliv zásahu uživatele. Ten instalaci nemůže nijak ovlivnit.

Únoscovou hlavní činností je upozornění na nějakou určitou stránku a donutit uživatele ji pořád navštěvovat. Samotné otevření takto nastavené stránky je pro uživatele nepříjemné, na druhé straně zvyšuje majiteli stránky, na kterou je donucen dojít, její hodnotu. Více navštěvované stránky, pokud mají placenou reklamu, si tímto zvyšují výdělek. V praxi to většinou znamená- více přístupů, více peněz.

Existuje mnoho variant. Některé se dokonce tváří jako užitečné programy, které se regulérně nainstalují i s možností odinstalace. [3]

2.3.1 Příklady Hijacker Browser

2.3.1.1 Morwill Search

Morwill Search je únosce prohlížeče, který nejdříve přepíše domovské stránky na svou webovou stránku a začne sbírat informace o počítači, který byl tímto spywarem napaden. [8]

2.3.1.2 CoolWebSearch

CoolWebSearch byl jedním z prvních únosců. Přepíše současnou domovskou stránku na podvodný vyhledávací engine, jehož výsledky jsou odkazy sponzorovaných stránek. Většina antivirových a antispamových programů ho nebyla schopna pořádně odstranit. Až Merijn Bellekom vyvinul speciální nástroj zvaný CWShredder který se specializuje na odstranění únosce a jeho dále vzniklé mutace. [8]

2.4 Spyware Dialer

Tento spyware patří mezi zákeřné programy. Program se nainstaluje na počítač a pokouší se vytáčet telefonní linky v jiných zemích. Výsledkem jeho působením jsou velmi drahé účty za telefon, které po nějaké době oběť dialeru obdrží. Je velmi těžké jej předem odhalit a dokázat, že takový dialer je zodpovědný za drahé účty. Také je obtížné rozeznat skutečný dialer od toho spywarového. Z toho důvodu je velmi těžké vůbec kontrolovat, či napravit infekci tímto škodlivým softwarem.

Některé dialery jsou použity legálně a uživatel je obeznámen a souhlasí s vyšší cenou výměnou za jistý online obsah (např. pornografické stránky). Ovšem většina z nich se opět snaží tajně dostat do počítače za použití různých triků. Většinou používají již dříve zmíněné chyby v prohlížečích, systému, či uživatelovu nepozornost a ukvapenost, ze kterých následně těží.

Uživatel by měl vědět, jestli dialer používá a pokud ne, ihned ho za pomoci antispywarového programu odstranit, dříve než bude platit vysoké účty za telefonní linku.

Tyto dialery bývají zneužity prodejci pornografie. To zahrnovalo stáhnutí a instalaci samotného programu nic netušícím uživatelem, donuceným k automatickému vytočení placených, velice drahých porno stránek a to i ve chvílích kdy si lechtivé stránky neprohlížel. (Na rozdíl od legálního použití dialeru při záměrném prohlížení těchto stránek, jak bylo zmíněno výše).

V současné době se tento problém týká uživatelů, kteří ještě používají modemové vytáčené připojení k internetu.

U nás v České Republice byl problém s takzvanými barevnými tarifovými linkami, kde byly uživateli po přesměrování na tyto linky účtovány vyšší tarify. Jedinou výhodou bylo, že ČESKÝ TELECOM omezil dobu volání na takto placené linky a to na deset minut. Provozovatelé takových stránek měli zveřejnit podrobné informace o tom, že uživatel bude platit vyšší tarif, což ovšem nebylo vždy dodrženo. Dalším problémem byla neznalost lidí ať už s rozšiřující dostupností internetu tak v neznalosti anglického jazyka, což často vedlo k instalaci nechtěného programu a drahým účtům za telefon. [7]

2.4.1 Příklady Spyware Dialeru

2.4.1.1 TIBS dialer

Ten přesměroval připojení telefonním modemem přes placené pornografické stránky a tak uživatel, i když byl připojen pouze na internet, platil zvýšený tarif za připojení. [8]

2.5 Keystroke Logger

Taky někdy nazývaný keylogger, je program, nebo zařízení, které je použito k sledování. Mapuje uživatelovy údery do klávesnice a to v reálném čase. Jako typický spyware zaznamenává program uživatelova data a posílá je tvůrci škodlivého softwaru. Tyto záznamy jsou použity ke sbírání uživatelových přístupových jmen a hesel, informací o jeho kreditních kartách, číslech bankovních účtů a jiných citlivých údajů.

Tyto programy už existují dlouhou řadu let, avšak s nárůstem použití ve spyware se opět zvyšuje nebezpečí a obavy, týkající se bezpečnosti. S přihlédnutím k tomu, jak je jednoduché je být sledován, by se měli mít všichni uživatelé internetu na pozoru před infekci tímto škodlivým software.

V současné době webové stránky, které od uživatele vyžadují zadávání citlivých údajů, používají graficky zobrazenou klávesnici, kde uživatel pomocí myši zadá své heslo. [3]

2.5.1 Typy keystroke loggerů

2.5.1.1 Hardwarové loggery

Hardwarové doggery jsou malá zařízení, která se většinou dávají mezi klávesnici a počítač. Jejich malá velikost jím zaručuje takřka neodhalitelnost po dlouhou dobu. Nevýhodou je,

že infiltrátor musí mít fyzický přístup k počítači, který chce napadnout. Tato zařízení mají schopnost zachytit nějaký počet úhozů klávesnice včetně emailových přístupových jmen a hesel, čísel k bankovním účtům. Zachycují jakýkoliv výstup, který jde z klávesnice do počítače. Takže vše co jste zadávali přes klávesnici, je v nebezpečí.

2.5.1.2 Hooking mechanisms

Tento typ zaznamenávání je pomocí softwarové aplikace používající „SetWindowsHookEx“, funkci v operačním systému Windows, která opět monitoruje úhozy do klávesnice. Takovýto program většinou bývá připojen k emailu jako spustitelný EXE soubor, který funkci zachycování iniciuje společně s knihovnou DLL, která má na starost funkce přístupu.

2.5.1.3 Kernel / drive loggery

Tento typ úhozového loggeru je na úrovni kernelu v operačním systému a dostává informace přímo ze vstupního zařízení, kterým bývá obyčejně klávesnice. Tento program nahrazuje základní aplikaci pro interpretování uživatelových úhozů a může být naprogramován tak, že je takřka nedetekovatelný. Vzhledem k tomu, že je spuštěn při systémovém bootování počítače ještě před tím, než je jakákoliv jiná uživatelova aplikace vůbec spuštěna.

3 ZÁKLADNÍ OPATŘENÍ PROTI SPYWARE

Tato kapitola vysvětluje pojem komplexnost systému a dále základní opatření proti spyware, projdeme si jednotlivé bezpečnostní rady a doporučení na efektivní boj proti této hrozbě. Jsou zde uvedeny i jednotlivé programy, které se dají použít, buď jako efektivní štít, nebo k odstranění již nainstalovaného spyware. [2], [3], [4]

3.1 Školení

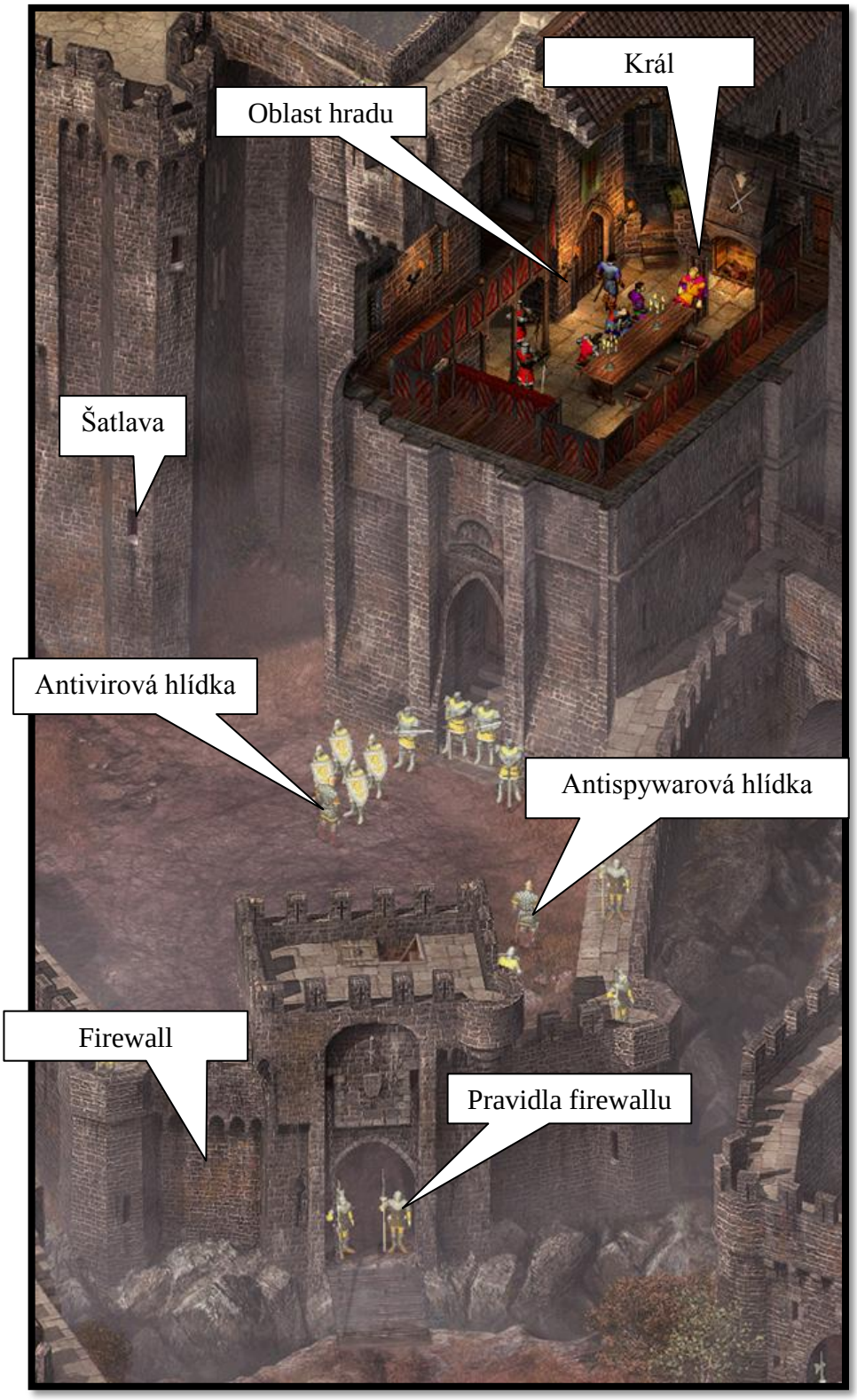
Neznalost neomlouvá. Tuto větu slýcháme už od základní školy a platí stále. To že spyware je hrozba je jasné každému, kdo o tom něco málo ví. Lidé, kteří neztratili data či nebyli napadeni touto hrozbou, mají stále tendenci ji podceňovat či úplně zavrhovat, a v tom je základní problém. Proto by každá firma měla své zaměstnance, kteří pracují s informačními technologiemi alespoň informovat o této hrozbě a vysvětlit jim jak s ní bojovat.

Pravdou bývá, že ta nejjednodušší opatření bývají ta nejlepší. I kdyby jen pár týdnů po přednášce pro zaměstnance všichni dodrželi těchto pár jednoduchých rad, je opět o něco zvýšena bezpečnost.

3.2 Komplexnost systému

Obrana proti spyware se dá jednoduše připodobnit k obraně hradu (Obr. 3.). Zde si vysvětlíme, jaký je rozdíl před zabezpečeným a nezabezpečeným počítačem.

Zabezpečený počítač může vypadat jako tento hrad, jehož obrana má několik úrovní.



Obr. 3. PC jako pevnost[5]

[5] Obrázek převzat z počítačové hry Robin Hood – Legenda Sherwoodu

První je úroveň hradby, tu představuje firewall. Brána v hradbě se stráží představuje pravidla pro jednotlivé výstupní a vstupní packety. Zjednodušeně řečeno, kdo dovnitř může a kdo ne.

Další úrovní je nádvoří se šatlavou, kde máme dvě hlídky. První hlídá schovaný spyware, jsou to antispywarové aplikace. Druhá hlídka ozbrojenců, tj. antivirový program, hledá příznaky rebelie či podivné chování. Šatlava, jinak karanténa antispyware a antivirů. Sem se zavírají škodlivé aplikace.

Poslední úrovní je samotný hrad. Zde jsou rádci, správci a nakonec ten nejdůležitější- král. Rádci jsou programy, které se vždy ptají, jestli tu či onu činnost opravdu chcete udělat a jestli opravdu rozkaz přichází od vás. Správci jsou uživatelé, kteří mají omezená práva k jistým částem pokladnice, toho nejdůležitějšího ve vašem počítači- k datům. Nakonec nejdůležitější postava samotný Král- který má veškerá potřebná práva ke všemu v hradě a přilehlému okolí.

Obr. 4. Kočka a myš[6]

Poslední důležitá činnost, která se vztahuje k celému panství, jsou opravy. Ve světě informatiky nazývány upgrade, patche a bezpečnostní záplaty. Protože jak jistě víte, každý hrad stárne, jednou je moderní jáma s medvědem a podruhé vodní příkop. Záleží na tom, jaká je před vámi hrozba a jak se tato hrozba vyvíjí.

[6] Obrázek převzat z http://abnormal-photography.blogspot.com/2007/09/photograph-cat-and-mouse.html

Pro dokonalou představu jak to vypadá, když máte nezabezpečený počítač, se podívejme na tento obrázek a položme si otázku: „Jste obezřetní k ochraně dat jako kočka na obrázku?“ (Obr. 4).

3.3 Co instalujeme?

Důležité je vědět, co si v kterou chvíli instaluji do svého počítače. Každý uživatel, by si měl před jakoukoliv instalací položit několik následujících otázek: Je tento program pro mě opravdu důležitý? Jaké má ohlasy ostatních uživatelů? Není s ním opravdu přidaný nějaký spyware, či adware? Mohu důvěřovat vývojářům programu? Pokud jde o známou vývojářskou skupinu je méně pravděpodobné, že se s instalací jejich software bude instalovat i nějaká škodlivá aplikace a pokud ano, bude takováto aplikace spíše jako volitelný doplněk. Ve chvíli kdy je software opravdu dobrý, by bylo zřejmě nemožné, že by byl zadarmo. Pak je nutné ba spíše nezbytné donutit se přečíst instalační licenci. Pokud je v ní uvedeno, že program posílá data třetí osobě, je dobré vyhnout se instalaci a chránit svá data. Nejdůležitější je používat zdravý rozum a uvědomit si, že nic není zadarmo a pokud ano, je to podezřelé. [3]

3.4 Čtěte, s čím souhlasíte

Je mnoho lidí, kteří nejdříve klikají a pak až přemýšlejí. Pro ně je to úspora času, která má za následek značné zpomalení počítače a to již v několika dnech po instalaci operačního systému. Pravda je taková, že tento přístup si můžeme dovolit ve chvíli, kdy pro nás data na našem počítači nejsou důležitá a je nám jedno kdo k nim má přístup. To si ovšem nemůže dovolit žádná agentura, která pracuje s osobními údaji, nebo schraňuje citlivá data.

Uživatelé počítače většinu času nemyslí, při instalaci softwaru je to samé: ano, ano, dále, ano, ano, atd. V záplavě těchto otázek je možné, že znuděný uživatel odsouhlasí i něco co by za jiných okolností určitě zamítl. O to koneckonců autorům spyware jde. Je to taková hra, lépe je nepospíchat a pracovat pečlivě, než odsouhlasit třetí straně úplný přístup na disk s povolením zápisu. [2]

3.5 Prohlížeče a zabezpečení

Skutečností je, že tvůrci spyware se nejvíce snaží napadnout prohlížeče, které jsou nejvíce používané. Tedy pokud nejde o cílený útok na nějakou firmu a jde jen o náhodné vybírání počítačů na internetu. Je to logické. Proč napadat nebo zneužívat něco, co vlastně vůbec

nikdo nepoužívá. Vzhledem k tomu, že z větší části spyware využívá uživatelovu nepozornost, jsou lepší kvantitativní útoky, kde se alespoň jeden uživatel může chytit.

Některý spyware tedy používá k napadení počítače a k samotné instalaci bezpečnostní díry, nebo „výhody“ (doinstalované moduly) běžně užívaných prohlížečů. Proto je dobré používat alternativní prohlížeč.

Je minimálně nutné nastavit si vyšší zabezpečení u Internetu Exploreru, pokud ho chceme nadále používat jako hlavní prohlížeč. Doporučené zvýšení jeho úrovně zabezpečení zóny internet je minimálně na středně vysoké, či vyšší. Případně můžeme používat jiný, bezpečnější prohlížeč.

K porovnání prohlížečů slouží hodnocení různých firem či jednotlivců. Tyto si můžeme projít a na základě zjištěných informací se rozhodnout pro prohlížeč, který nám bude vyhovovat. Z pohledu bezpečnosti prohlížečů jsou zajímavé každoroční statistiky od firmy Symantec. [6]

3.5.1 Doba zranitelnosti

Doba ohrožení, někdy také zranitelnosti, je časový rozdíl, mezi dobou, kdy je zneužita chyba prohlížeče a dobou, kdy je tato chyba odstraněna. Jinými slovy je to doba, která uplyne od zveřejnění škodlivého kódu zneužívajícího některou zranitelnost a dobou, kdy je veřejně dostupná záplata na postižený program, vytvořená vývojáři daného prohlížeče. V tomto čase není počítač nebo systém, na kterém aplikace s bezpečnostní dírou běží, dostatečně chráněn před venkovními útoky.

Míra zranitelnosti je odvozena z průměrné hodnoty času, který je zapotřebí k vydání záplaty oproti průměrné době zveřejnění škodlivého kódu. Tato hodnota zahrnuje nejdelší možný čas záplatování, což je nejvyšší možná doba k vydání záplaty pro všechny zranitelnosti v záznamovém listě (data sheet). Změřením času potřebného k vydání záplaty na zranitelnost je možné získat náhled na obecnou reakci vývojářské firmy a na bezpečnostní hrozby vůči jejím aplikacím. Některé nalezené zranitelnosti byly zazáplatované ihned po zveřejnění hrozby, což odráží účelnost bezpečnostního auditu prováděného výrobcem softwaru prohlížeče, nebo externí firmou. Pokud je audit prováděn externí firmou měl by na takto zjištěné hrozby dopředu upozornit výrobce a tím mu i poskytnout dostatečný čas na vytvoření adekvátní záplaty daného programu, před

zveřejněním výsledků testů. Některé tyto hrozby jsou uveřejněny a popsány ve zprávě až ve chvíli, kdy vyjde nová verze programu, která je v danou chvíli opravuje.

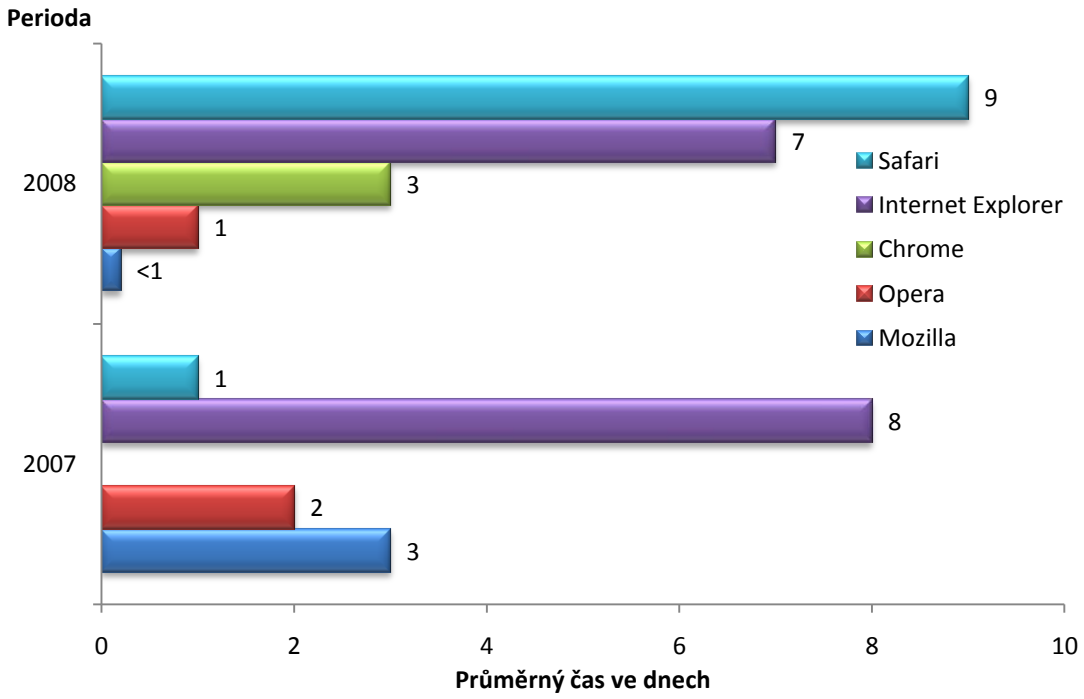
Někdy se může stát, že firma provádějící bezpečnostní audit softwaru neupozorní na chyby vydavatele, ale pouze je zveřejní, nebo upozorní vydavatele a ten dané chyby podcení a nereaguje na ně. Následky tohoto jednání mohou být často tragické, protože ve chvíli, kdy je uveřejněna taková chyba a každý o ní ví, není těžké ji zneužít proti uživateli.

Doba zranitelnosti bere všechny tyto možnosti v potaz k získání průměrného času, po který jsou koncoví uživatelé a společnosti vystaveni riziku škodlivého kódu. Díky době zranitelnosti administrátoři a uživatelé mohou snížit možnost napadení systému třetí osobou na minimum, vybráním adekvátního softwaru s nejkratší dobou zranitelnosti a tím maximálně chránit svá data.

3.5.1.1 Porovnání doby zranitelnosti u jednotlivých prohlížečů:

- Apple Safari
- Google Chrome
- Microsoft Internet Explorer
- Mozilla browsers
- Opera

V roce 2008 byla průměrná doba zranitelnosti pro Apple Safari devět dní, což bylo zjištěno na základě 31 balíků záplat zranitelností. Na rozdíl od roku 2007, kdy doba zranitelnosti byla pouhý jeden den. Navýšení o osm dní bylo způsobeno velkým počtem nezávisle zjištěných zranitelností. Nejdelší doba, za kterou firma Apple zazáplatovala zranitelnost prohlížeče Safari, byla 156 dní, což negativně ovlivňuje průměrný čas, který je podstatně delší než nejdelší doba v roce 2007, kdy vydání záplaty trvalo osm dní.



Obr. 5. Doba zranitelnosti[7]

Internet Explorer měl v roce 2008 průměrnou dobu zranitelnosti 7 dní, což bylo zjištěno na základě 31 balíků záplat. Nejdelší potřebný čas k vydání záplaty v roce 2008 byl 147 dní. V roce 2007 byla průměrná doba zranitelnosti 8 dní, na základě 28 zranitelností a nejdelší doba vydání záplaty 90 dní.

Poprvé byl testován a uveden ve zprávě Symantecu i Google Chrome. Přestože byl vydán poměrně nedávno, a to v září 2008, byl do zprávy zahrnut hlavně vzhledem k jeho výkonnosti oproti jiným prohlížečům. V roce 2008 Symnatec zdokumentoval průměrnou dobu zranitelnosti pro tento prohlížeč tři dny, na základě 6 balíků záplat zranitelností. Nejdelší doba vydání záplaty byla 11 dní.

Doba zranitelnosti pro Operu v roce 2008 byl jeden den a to na základě 33 balíků záplat zranitelností. V roce 2008 byla nejdelší doba v odpovědi na zjištěnou hrozbu vydáním záplaty 29 dní. V roce 2007 byla tato hodnota 2 dny, na základě 14 balíků záplat zranitelností a nejdelší doba od vydání záplaty 23 dní.

---

[7] Graf byl převzat z: FOSSI, Marc, et al. Security Threat Report [online]. [s.l.] : Symantec, 2008 [cit. 2010-03-30]. Vulnerability Trends, Dostupné z WWW: <http://www.symantec.com/connect/sites/default/files/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf>.

Prohlížeč Mozilla měl dobu zranitelnosti v roce 2008 menší než jeden den, zjištěno na základě 83 balíků záplat zranitelností a nejdelší dobu v odpovědi na hrozbu vydáním záplaty 30 dní. V roce 2007, měla Mozilla dobu zranitelnosti tři dny, na základě 103 balíků záplat zranitelností a nejdelší dobu v odpovědi na hrozbu vydáním záplaty bylo 109 dní.

Z tohoto průzkumu je vidět, že velké firmy, jako je Microsoft a Apple, vzhledem k jejich širokému působení nemají tolik času zabývat se minoritními projekty, jako je webový prohlížeč. Je jasné, že pokud máte chybu v systému, je daleko důležitější zabývat se jí, než nějakou malou ve webovém prohlížeči. Z toho důvodu jsou jejich prohlížeče Internet Explorer a Safari mezi posledními na rozdíl od jejich konkurentů, kteří se povětšinou zabývají pouze vývojem prohlížeče.

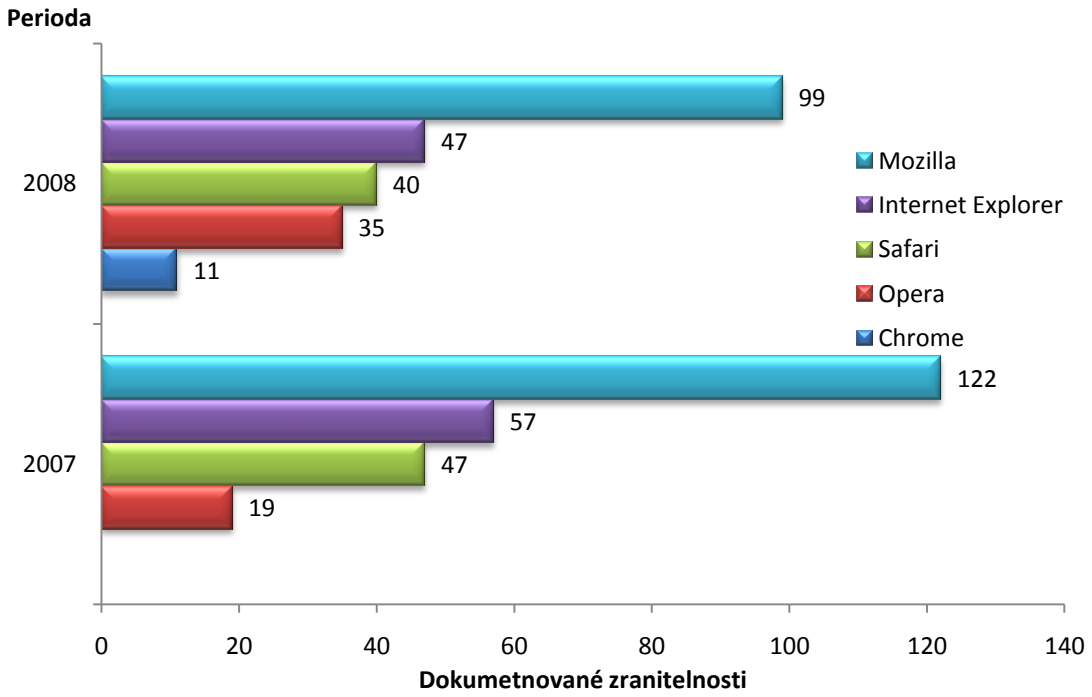
3.5.2 Zranitelnosti webových prohlížečů

Vzhledem k jejich vztahu k internetovým podvodům hrají zranitelnosti webových prohlížečů důležitou roli při napadení škodlivým kódem. Obavy o bezpečnost jsou na místě z důvodu vystavení prohlížečů velkému počtu lidí, kteří mohou být potenciálními programátory škodlivých kódů. Prohlížeče dále mohou usnadnit útoky spyware ze strany uživatele a to kvůli používání plug-inů a jiných aplikací což vede k ulehčení manipulace s potenciálně škodlivým obsahem podávaným z webových stránek skrze dokumenty a média.

3.5.2.1 Počet zranitelností pro jednotlivé prohlížeče:

- Apple Safari
- Google Chrome
- Microsoft Internet Explorer
- Mozilla browsers
- Opera

V průběhu roku 2008 postihlo prohlížeč Mozilla 99 zranitelností. Čtyřicet z těchto zranitelností bylo střední závažnosti. To je méně než 122 zranitelností, které byly zdokumentovány v roce 2007, z nichž bylo 91 považováno za nízkou hrozbu a 31 za střední hrozbu.



Obr. 6. Počet zranitelností[8]

Internet Explorer byl vystaven 47 novým zranitelnostem v roce 2008. Z toho 16 hrozeb s nízkou závažností a 31 se střední závažností. To je méně než 57 zdokumentovaných zranitelností v roce 2007, ze kterých bylo 28 považováno za nízkou hrozbu, dalších 28, kterým byla přidělena střední hrozba a jedna s vysokou hrozbou.

Safari bylo v roce 2008 postiženo 40 novými zranitelnostmi, z toho 16 bylo ohodnoceno nízkou hrozbou a 24 střední hrozbou. Toto je méně než 47 hrozeb v roce 2007, kdy 27 bylo označeno za nízkou hrozbu, 19 za střední hrozbu a jedna vysoká hrozba.

V roce 2008 Symnatec zdokumentoval 35 nových zranitelností u prohlížeče Opera, ze kterých bylo 12 s nízkou hrozbou a 23 se střední hrozbou. To je více zranitelností, než v roce 2007 kdy bylo objeveno 19 zranitelností, ze kterých 8 bylo s nízkou hrozbou a 11 hrozbou střední.

[8] Graf byl převzat z: FOSSI, Marc, et al. Security Threat Report [online]. [s.l.] : Symantec, 2008 [cit. 2010-03-30]. Web browser vulnerabilites, s. 110. Dostupné z WWW: <http://www.symantec.com/connect/sites/default/files/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf>.

Google Chrome byl postižen 11 zranitelnostmi, ze kterých bylo sedm ohodnoceno jako nízká hrozba a čtyři jako hrozba střední. Chrome byl vydán v září 2008 a proto zde není porovnání s rokem 2007.

Kromě prohlížeče Opera je vidět, že bylo nalezeno méně zranitelností než v roce 2007. To ukazuje, že se vývojáři prohlížečů snaží o větší bezpečnost a ze soutěže mezi nimi vycházejí dobré výsledky, které přispívají k větší bezpečnosti dat.

3.6 Podezřelé přílohy či skripty v emailu

Zásadou je neotevírat a už vůbec nespouštět podezřelé přílohy v emailu. Není důležité, zda se jedná o obrázek, či něco jiného. Všechny tyto přílohy mohou obsahovat škodlivý kód, který může samotný spyware do našeho počítače stáhnout a nainstalovat.

Dalším doporučeným opatřením je přijatý email zobrazovat jako text a vypnout zobrazování jakéhokoliv aktivního obsahu. Důvod je jednoduchý a to že v kódu, který samozřejmě nevidíme, může být vepsaný skript, který opět může otevřít vrátka spywaru a vpustit ho bez našeho vědomí do počítače. Ovšem zakázání aktivního obsahu má i své zápory. Znemožňuje použití aktivního obsahu, kterým by jinak email mohl disponovat. Proto v současné době většina emailových klientů skripty v emailu na bázi html automaticky blokují, dokud uživatel nezvolí jinak.

3.7 Aktualizace

Klíčovou a mnohdy hlavní uživatelovou zbraní v boji proti spyware jsou aktualizace. Ať už operačního systému, antispyware, antiviru, firewallu, používaných aplikací, atd. Samotný spyware totiž využívá, jak jsme si už z větší části popsali, díry v samotných programech a v systému jako takovém. Z toho důvodu je pro nás nadmíru důležité, co nejvíce takovýchto děr do systému „ucpat“ záplatou.

Používat aktualizované webové prohlížeče, mít nainstalované veškeré záplaty windows a to co nejdříve. Protože antispyware, byť sebelepší, který nemá aktualizované spywarové definice, je nám takřka k ničemu.

Uživatel si musí uvědomit, že hrozba spywaru je každodenní. Není to záležitost jednou do roka, ale každých několika minut. Není se čemu divit, vždyť dnešním nejcennějším zbožím jsou samotná data. [4]

3.8 Nainstalujte si Firewall

Firewally jsou programy, které můžeme přirovnat ke zdi s bránou do vašeho počítače. Řídí veškerý provoz, který jde jak z vašeho počítače, tak do něj. V čem je tento software dobrý? Pokud si s nějakým freewarem, či jiným softwarem nainstalujete do vašeho počítače spyware, tak ve chvíli, kdy se tento škodlivý software pokusí komunikovat přes internet, laicky řečeno se pokusí projít přes vaši střeženou firewallovou bránu, bude zadržen „stráží“, která se vás jako správce počítače zeptá, jestli tento program může vycestovat s vašimi daty ven, či ne. Pak závisí už jen na vás, jestli to dané aplikaci povolíte, či nikoliv.

Tímto firewall jako takový přímo nezastaví nainstalování spyware do vašeho počítače, ale zabrání úniku dat. Informace od firewallu, že se nějaká podezřelá aplikace snaží komunikovat ven, by vás měla upozornit, že je asi něco v nepořádku a můžete podniknout další kroky proti škodlivému software.

3.9 Antispyware programy

Programy, které se zabývají vyhledáváním škodlivého software v počítači a jeho následným odstraněním. V dnešní době je jich velké množství. Některé bývají zdarma, jiné placené. Existují osvědčené programy a existují takové, které se tak jenom tváří. Na stránkách skupiny spywarewarrior je seznam velkého množství podvržených programů. [3]

3.9.1 Programy, které se považují za antispyware

Instalace a jejich provozování na počítači, je často velmi riskantní a to proto, že se spoléháme na něco, co buď ani nefunguje dostatečně, nebo funguje jen částečně. V současné době je na seznamu podezřelých antispywarů přes 300 programů. V seznamu jsou programy, které buď neposkytují dostatečnou ochranu, nebo nutí uživatele k jejich zakoupení. Tyto programy manipulují psychikou uživatele varovnými pop-upy se sdělením o možném fiktivním zamoření počítače spyware a vybídkou k zakoupení podvodného software. Tento nátlak je značné neetický a mnohdy uživatele donutí ke koupi nekvalitního software. Některé tyto „antispyware“ dokonce samotný spyware do počítače instalují, nebo instalují jiné nežádoucí programy, jako jsou trojské koně. To vše může vést k pádu systému a ztrátě dat. [9]

3.9.1.1 Kritéria umístnění programu jako podezřelého:

- Instaluje adware, spyware nebo malware.

- Unáší uživatelův prohlížeč, či samotnou plochu.
- Je nainstalován adwarem, spywarem, nebo malwarem.
- Je doporučován, či nabízen skrze adware, nebo spyware.
- Je nainstalován neviditelně bez uživatelova plného vědomí.
- Uživatel je k instalaci dotlačen agresivní, klamnou, nebo zavádějící reklamou.
- Je nabízen a prezentován firmou, která vyrábí spyware / malware, nebo je s nimi v úzkém spojení.
- Používá falešné, klamné, zavádějící výsledky skenování, které uživatele nutí, podvádějí, či mystifikují za účelem zakoupení produktu.

3.9.1.2 Dále se hodnotí i tato kritéria:

- Sofistikovanost a spolehlivost skenování (zahrnuje design programu a provedení detekčního schématu).
- Přesnost a spolehlivost skenování (zahrnuje špatné vyhledání).
- Přirozenost a přehlednost konečné zprávy.
- Informace o firmě a programu přístupná online.
- Ohlasy uživatelů, jejich zkušenostech s programem.
- Současné stavy definicí.

3.9.2 Doporučené antispywarové programy

Uvádím některé léty a praxí ověřené antispywarové programy, které lze na internetu nalézt. Každý uživatel internetu, který nechce svá data jednoduše poskytovat třetí osobě, by měl mít alespoň jeden z nich nainstalován ve svém počítači, pravidelně ho aktualizovat a skenovat s ním svá data. Zde si uvedeme jen jejich popis, podrobně se jimi budu zabývat v praktické části této práce.

- **Spybot Search & Destroy –** jeden z nejznámějších softwarů na odstranění spyware. Je jednoduchý a účinný. Jeho výhoda je v české lokalizace a tak ho mohou používat i uživatelé neznalí anglického jazyka. Neklade hlavní důraz na design, což může být jeho výhodou při používání na slabších počítačích.

- **Spyware terminator –** odstraňuje veškeré škodlivé programy, které mají cokoliv společného se spyware. Z rozšířených funkcí umožňuje automatickou aktualizaci antispywarové databáze, nastavení automatického skenování počítače v uživatelem stanoveném čase. Taktéž obsahuje nástroj security guard, který funguje jako ochranný štít při prohlížení internetu.
- **Ad-aware** – Další vysoce kvalitní antispywarový program, bohužel pouze v anglickém jazyce. Je sice pravdou, že by v dnešní době neměl být problém s takovým software pracovat, pravdou ale zůstává, že většina Čechů raději používá programy v češtině. Další nevýhodou jsou jeho omezené funkce volné verze.
- **AVG Anti-spyware –** chrání před viry a spyware. Jeho výhodou je, že i základní verze zdarma obsahuje E-mail scanner, který chrání před nebezpečnými přílohami a odkazy. Obsahuje aktivní štít, který zabezpečuje bezpečné prohlížení internetu a LinkScanner® AVG Active Search-Shield, který zobrazuje bezpečnostní hodnocení webových stránek u vyhledávačů Google, MSN a Yahoo. Dále jsou zajištěny pravidelné aktualizace přes internet.
- **Windows Defender –** další bezplatný program, který chrání počítač před automaticky otevíranými okny, hrozbami zabezpečení před spyware. Jeho ochranný štít funguje v reálném čase a při detekci spyware ihned nabídne možné zákroky proti nalezené hrozbě.

II. PRAKTICKÁ ČÁST

4 SPYBOT SEARCH & DESTROY

Spybot search & destroy, dále jen Spybot-SD, je program, který je proti spyware jedním z nejlepších a proto je zde uváděn na prvním místě. Program zaručuje jak vyhledávání škodlivého obsahu ve vašem počítači, tak pasivní protekci. Ta chrání proti samotnému vniknutí spyware do počítače. Překlad do českého jazyka je takřka celá, kromě nápovědy. [11]

4.1 Instalace programu

Tato část se zabývá postupem instalace od samotného stažení instalačního balíčku z internetových stránek po instalaci krok za krokem. Kapitola je vhodně doprovázena obrázky z instalace pro lepší pochopení.

4.1.1 Stažení programu

Vzhledem k všeobecné oblíbenosti je možné program najít téměř na všech českých serverech, které poskytují programy. Kupříkladu tyto servery:

- Stahuj - http://www.stahuj.centrum.cz.
- Slunečnice - http://www.slunecnice.cz.
- Studna - http://www.studna.cz, atd.

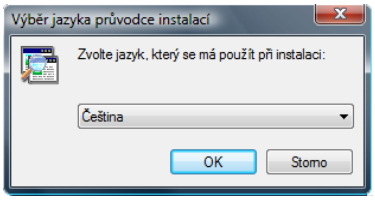
Kvůli nejnovější verzi je ovšem nejlepší navštívit samotné domovské stránky programu - http://www.safer-networking.org. Je zde možné přepnout i na počeštěnou verzi stránek, která je pro uživatele neznalého anglického jazyka dobrá na orientaci.

4.1.2 Průběh instalace

Po stažení instalačního klienta a jeho spuštění se doporučuje postupovat krok za krokem dle tohoto návodu:

4.1.2.1 Výběr jazyka instalace

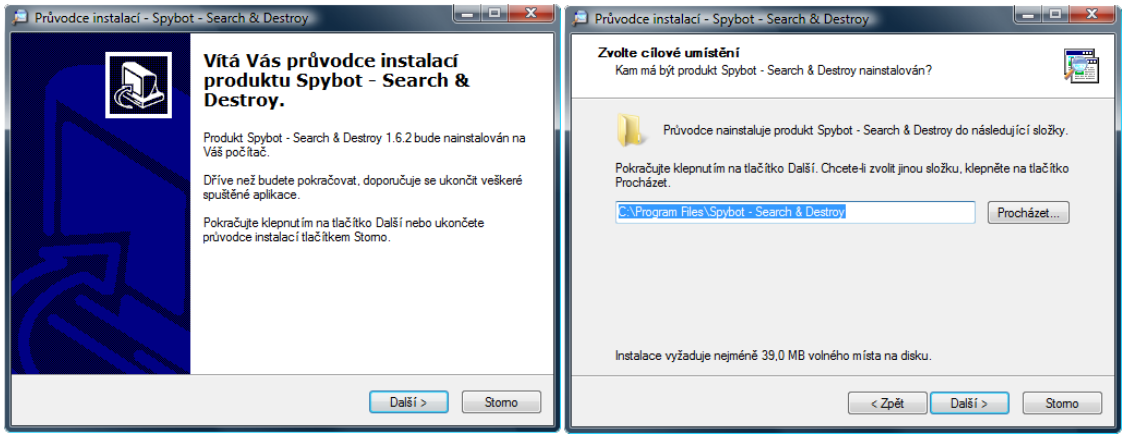
První okno, které vyskočí po začátku instalace (Obr. 7), je okno s výběrem jazyka instalace. Jinak také v jakém jazyku bude celá instalace probíhat. Je zde na výběr ze 44 světových jazyků.



Obr. 7. Výběr jazyka

4.1.2.2 Průvodce instalací

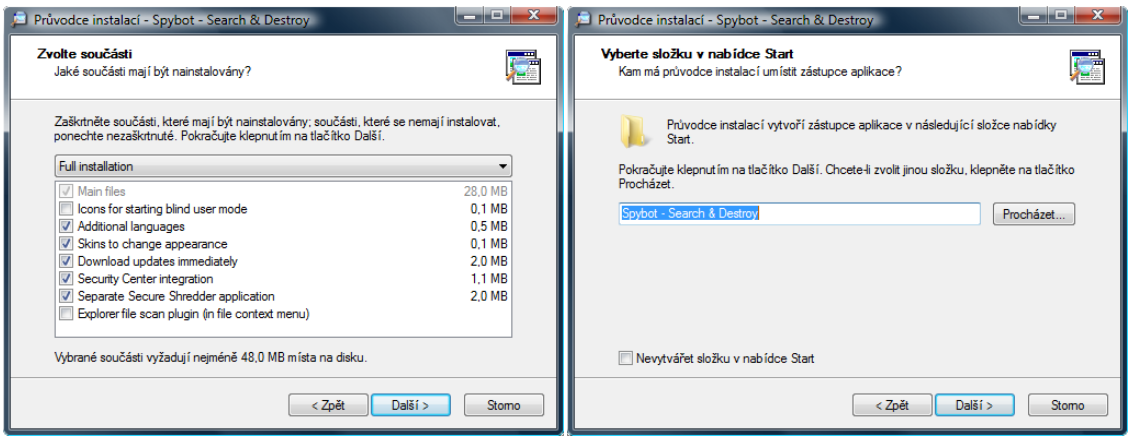
Uvítací okno (Obr. 8) – pokračuje se stiskem tlačítka *další*



Obr. 8. Průvodce instalací a volba cíle instalace

Výběr kam bude program nainstalován (Obr. 8) - zde se volí cesta, nebo se nechá program nainstalovat standardně do složky Program Files.

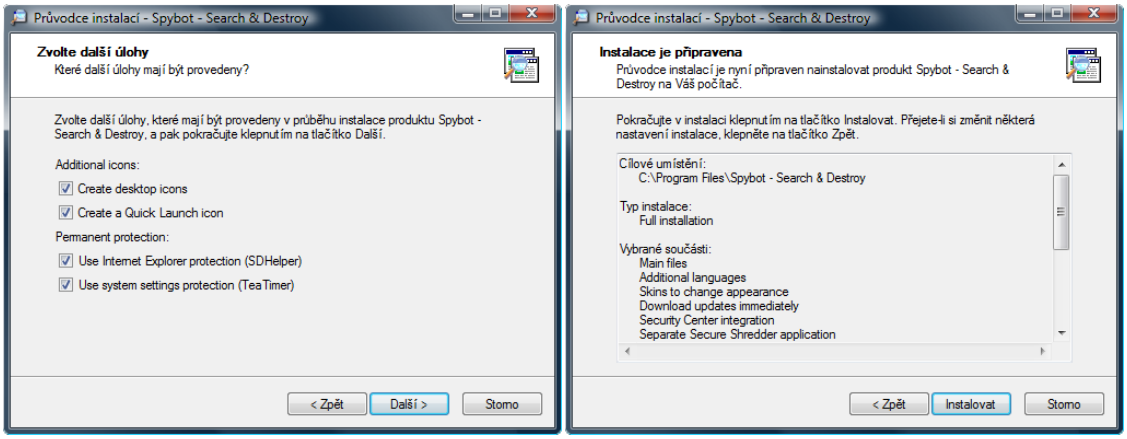
Volitelné části programu (Obr. 9) - zde se mohou přidat či odebrat volitelné části programu (soubory programu, ikony pro skrytý start, přídavné balíčky jazyků, změny vzhledu, ihned stáhnout aktualizace, integrování centra bezpečnosti, aplikace secure shredder (aplikace na bezpečné odstranění některého spyware)).



Obr. 9. Zvolení součástí a vytvoření zástupce v liště start

Pod čím se program nachází v liště start (Obr. 9) - zde je možné zvolit, zda program má být v liště start či nikoliv.

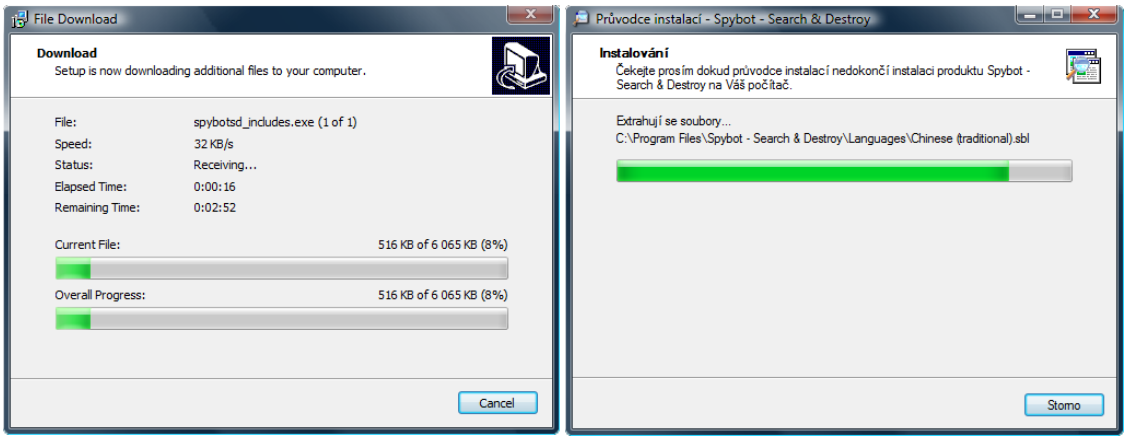
Další úlohy (Obr. 10) – uživatel volí co chce, aby aplikace po instalaci vytvořila nebo prováděla (vytvoření ikon na ploše, vytvořit ikonu rychlého spuštění, stálá ochrana Internet Exploreru, ochrana systémových nastavení).



Obr. 10. Další úlohy a souhrn instalace

Souhrn aplikace (Obr. 10) – přehledně shrnuto vše, co bylo zvoleno v průběhu instalace. Souhrn je dobrý pro kontrolu rozhodnutí.

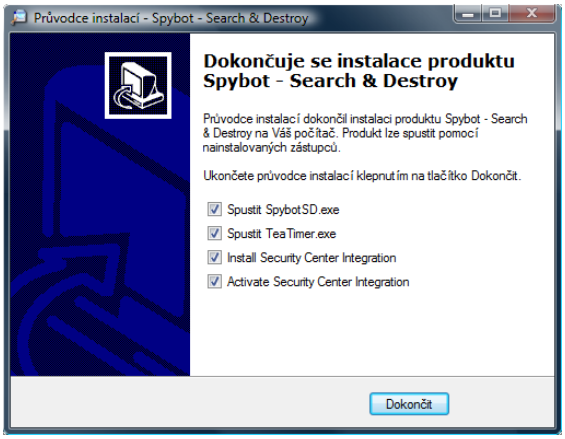
Stažení komponent pro instalaci (Obr. 11) - instalace bohužel funguje tak, že si potřebné soubory stahuje z internetu a proto je nutné, aby byl počítač přípojen k internetu.



Obr. 11. Průběh stahování a průběh instalace

Samotná instalace (Obr. 11) - nyní je zobrazena samotná instalace programu.

Konec instalace (Obr. 12) - úplný konec s nabídkou, které komponenty chce uživatel ihned spustit.



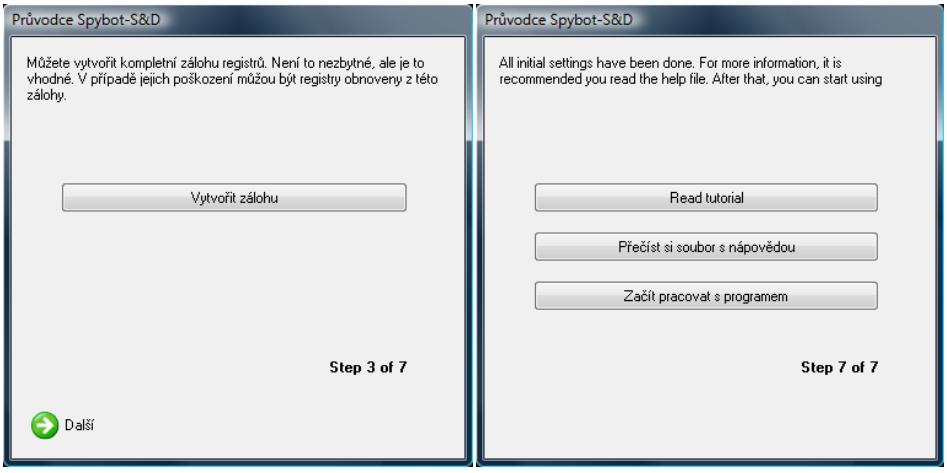
Obr. 12. Konečná nabídka

4.2 Použití programu

Podkapitola popisuje jak program Spybot-SD nejlépe používat a tím chránit svá data. Vysvětluje, jak se program chová při svém prvním spuštění. Dále jak aktualizovat, skenovat a používat pasivní protekci.

4.2.1 První spuštění

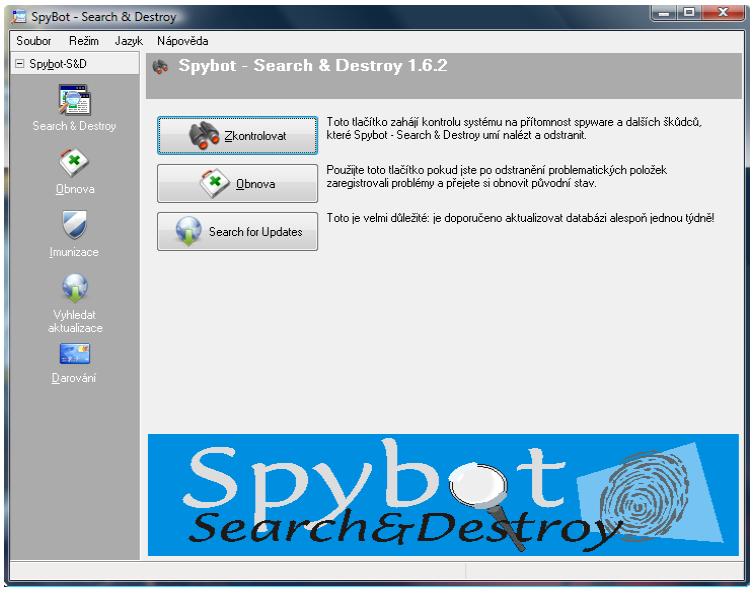
Po prvním spuštění se program zeptá, jestli má provést zálohu registrů. Tato záloha není nutná, ale je doporučená. Pokud je Spybotem-SD odstraněna nějaká důležitá hodnota registrů, je možné provést obnovu registrů, viz níže. Pokračuje se tlačítkem *další*.



Obr. 13. Nabídky při prvním spuštění

Další okno může českého uživatele zaskočit, protože je přeložené jen částečně. Tlačítka ze shora - *čti tutoriál* (česky návod jak používat program), *přečíst soubor s nápovědou* (nápověda je pouze v anglickém jazyce), *začít pracovat s programem* (Obr. 13). Pokračuje

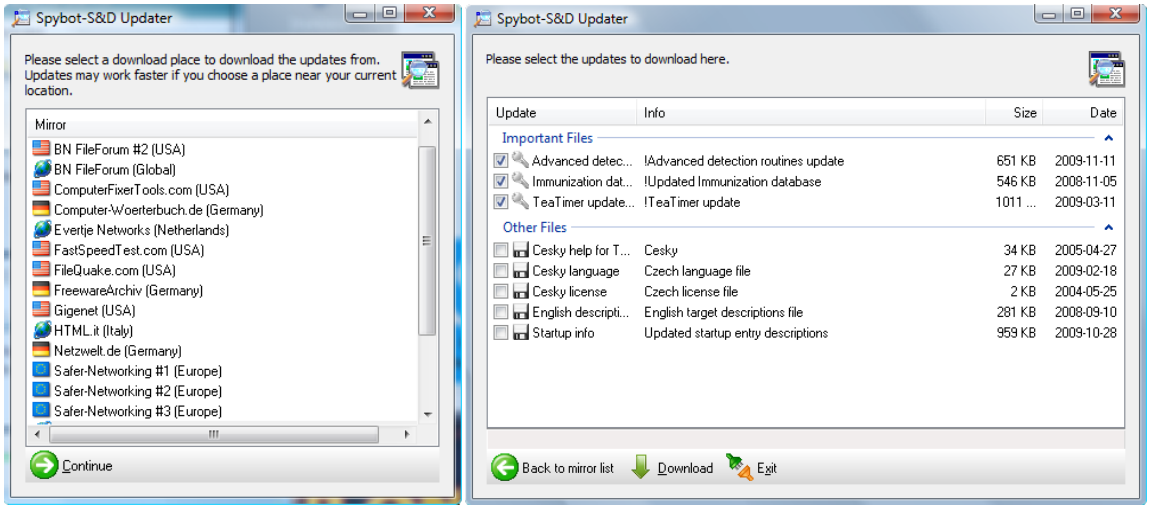
se stiskem posledního tlačítka. Nyní je před uživatelem hlavní obrazovka aplikace (Obr. 14).



Obr. 14. Hlavní nabídka

4.2.2 Aktualizace

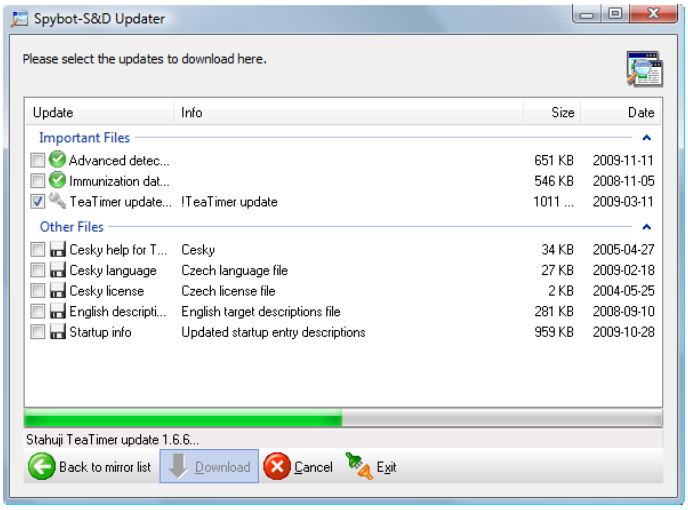
První doporučený úkon po instalaci je aktualizovat samotný program. Hlavním důvodem jsou spywarové definice (databáze, podle kterých se vyhledává spyware). Ihned na úvodní obrazovce je tlačítko *Search for Updates*, kliknutím na něj program začne hledat aktualizace.



Obr. 15. Výběr serverů a výběr aktualizací

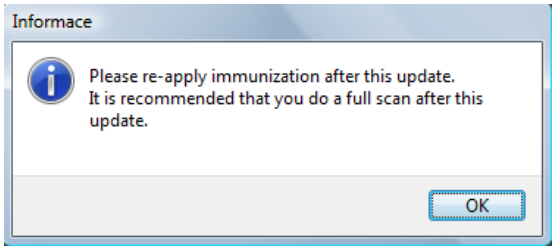
Vzápětí se objeví okno s výběrem serverů různých zemí (Obr. 15), ze kterých je možné aktualizace stáhnout. Pravidlem většinou bývá, že čím je země blíže, tím je přenos aktualizací rychlejší. Je možné vybrat Německo, případně některou jinou evropskou zemi.

Poté co je vybrán server se pokračuje tlačítkem *continue*. Vyskočí další okno s přehledem dostupných aktualizací (Obr. 15). Ty důležité bývají zpravidla zaškrtnuté. Pokud se tak z nějakého důvodu nestane, je možné postup opakovat s jiným serverem. Po stisknutí tlačítka *download* se začnou stahovat vybrané aktualizace. Po stisknutí tlačítka *exit* ve spodní části se toto okno zavře.



Obr. 16. Průběh instalace

Je možné, že po nainstalování aktualizací vyskočí tato hláška (Obr. 16) - neznamená nic jiného, než že se aktualizovala pravidla pro pasivní protekci. Proto je doporučené nechat pasivní protekci znovu projít systém. Více viz níže pasivní protekce.

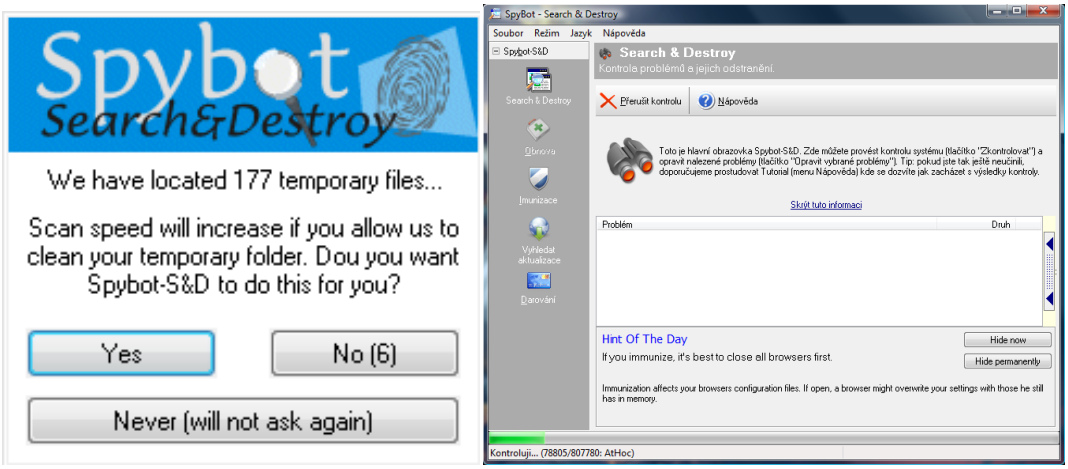


Obr. 17. Informační okno

4.2.3 Skenování obsahu počítače

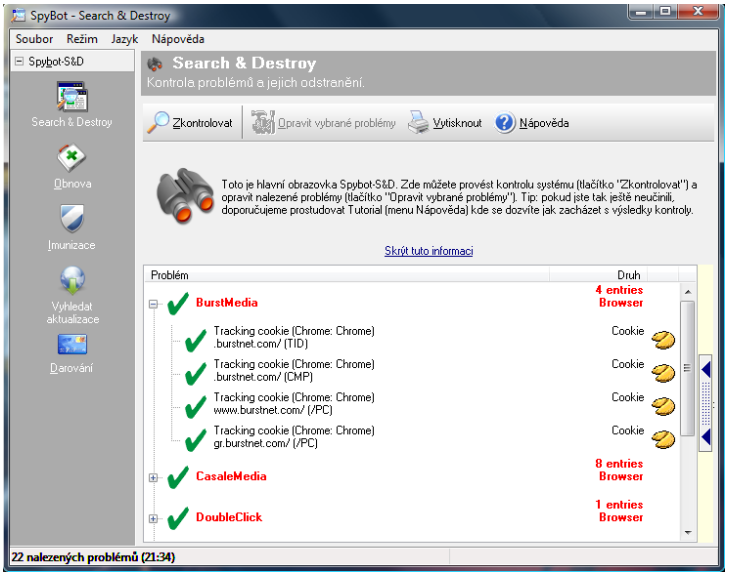
Skenování počítače je zahájeno po kliknutí na tlačítko *zkontrolovat* na úvodní obrazovce. Program nejdříve zjistí, jestli jsou odstraněny dočasné soubory v počítači. Pokud ne,

vyskočí hláška (Obr. 18) a program nabídne jejich smazání z počítače. Dále se spustí samotné skenování. Jeho průběh je možné sledovat ve spodní části okna (Obr. 18).



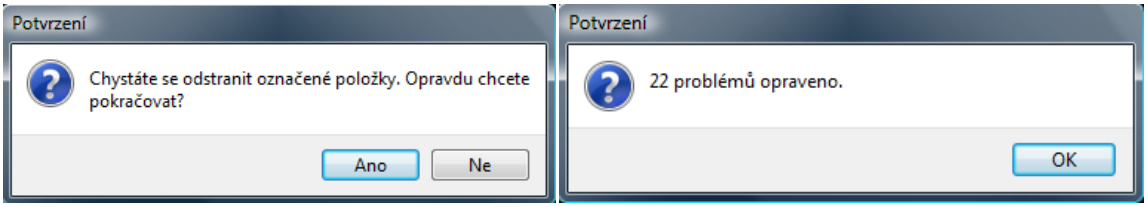
Obr. 18. Výzva k odstranění dočasných souborů a průběh skenování

Po ukončení skenování program vypíše seznam nalezených škodlivých programů. Každý jednotlivý záznam je možné rozbalit a dozvědět se o jednotlivých špiónech více (Obr. 19). Je možné zde zjistit typ a umístění (na obrázku je vidět příklad cookie, který byl detekován v prohlížeči Google Chrom). Kliknutím na tlačítko *opravit vybrané problémy* v horní liště je možné odstranit nežádoucí software.



Obr. 19. Výsledek testu

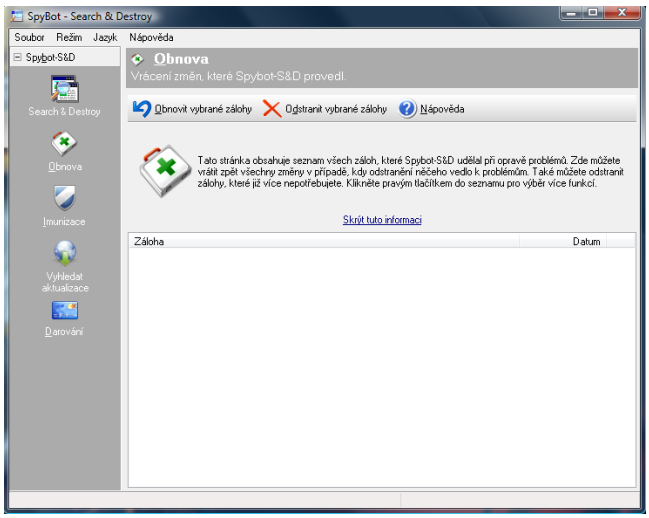
Po vyskočení okna (Obr. 20) uživatel potvrdí, že opravdu chce nežádoucí spyware smazat. Pokud bylo vše úspěšné, vyskočí potvrzující okno, problémy byly opraveny (Obr. 20). Tímto je spyware z počítače odstraněn.



Obr. 20. Potvrzení odstranění položek a výsledek zvolené akce

4.2.4 Obnova smazaných souborů

Tato část programu se používá, pokud po odstranění škodlivého softwaru je zaregistrováno zhoršení systému či nefunkčnost některých programů (Obr. 21). Obnoví předchozí stav před smazáním položek. Stačí jen zaškrtnout, které ze záloh je třeba obnovit a kliknout na tlačítko *obnovit vybrané zálohy* v horním panelu.



Obr. 21. Okno obnovy

4.2.5 Pasivní protekce

Neboli imunizace slouží k zabezpečení různých softwarových děr do počítače tím, že je program zabezpečí vytvořením metod, které blokují škodlivé cookies, instalaci malware a otevírání nežádoucích webových stránek. Znemožní tedy jejich zneužití proti uživateli. Vzhledem k nedokonalosti jednotlivých prohlížečů a operačního systému je tato vlastnost programu značně žádoucí. V současné době chrání přes 120 000 zneužitelných míst.

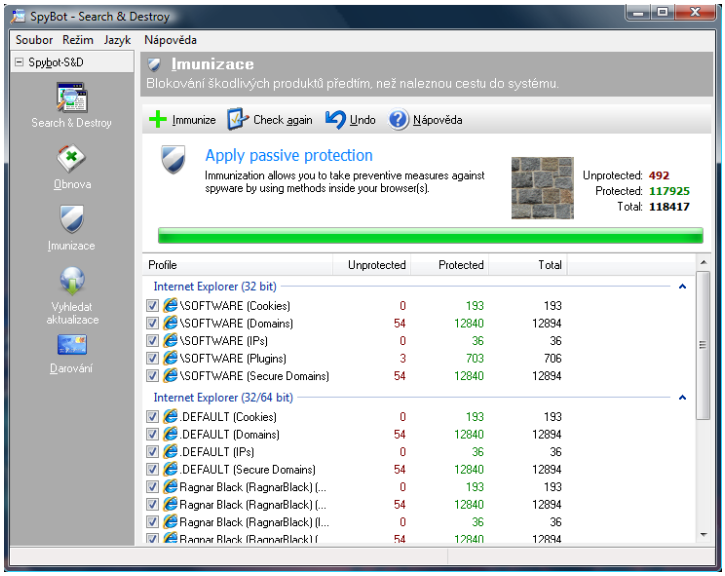
Před začátkem imunizace je zpravidla důležitá aktualizace samotného programu, viz výše. Tím jsou aktualizované knihovny metod proti škůdcům.

Spuštěná imunizace se dá najít ve správci úloh systému a zabírá z paměti 60 800 kB, což je poměrně mnoho, ale ochrana dat je přednější.

4.2.5.1 Zapnutí imunizace

Při kliknutí na nabídku imunizace na postranním panelu programu se ihned zapne skenování současného stavu, kde se zobrazí kolik metod proti spyware máte již vytvořeno a kolik ne (Obr. 22). Po kliknutí na tlačítko *imunizovat* je spuštěn samotný proces imunizace, kdy se vytvářejí nové metody proti nalezeným „dírám“.

Aplikování imunizace může trvat i několik desítek minut, v závislosti na výkonu PC. Po ukončení imunizace by ve sloupci unprotected (nechráněno) měla být nula.



Obr. 22. Okno imunizace

4.3 Odinstalace

Pokud chce uživatel program odinstalovat, stačí ho najít buď v nabídce start pod složkou Spybot - Search & Destroy. Kliknutím na ikonku *uninstal* je program odinstalován. Případně je možné ho najít ve Windows Vista pod programy a funkce, kde je rovněž možné program odinstalovat. Při odinstalování může proces odinstalace chtít vypnout běžící program. Pravým tlačítkem se klikne na ikonu programu na liště start a vybere se Ukončit Spybot – S&D Rezident. Nyní by měl jít program bez problémů odinstalovat.

5 SPYWARE TERMINATOR

Spyware Terminator je další z vysoce kvalitních software na obranu proti spyware. Překvapí svým příjemným vzhledem v české verzi. Menu může být pro laického uživatele na první pohled komplikované. [12]

5.1 Instalace programu

5.1.1 Stažení programu

Spyware Terminator se dá nalézt na všech českých serverech, které poskytují programy.

- Stahuj - http://www.stahuj.centrum.cz.
- Slunečnice - http://www.slunecnice.cz.
- Studna - http://www.studna.cz, atd.

Program se rovněž dá najít na domovské stránce - http://www.spywareterminator.com/cs/Default.aspx. Z hlediska přehlednosti je zde uveden odkaz na českou mutaci.

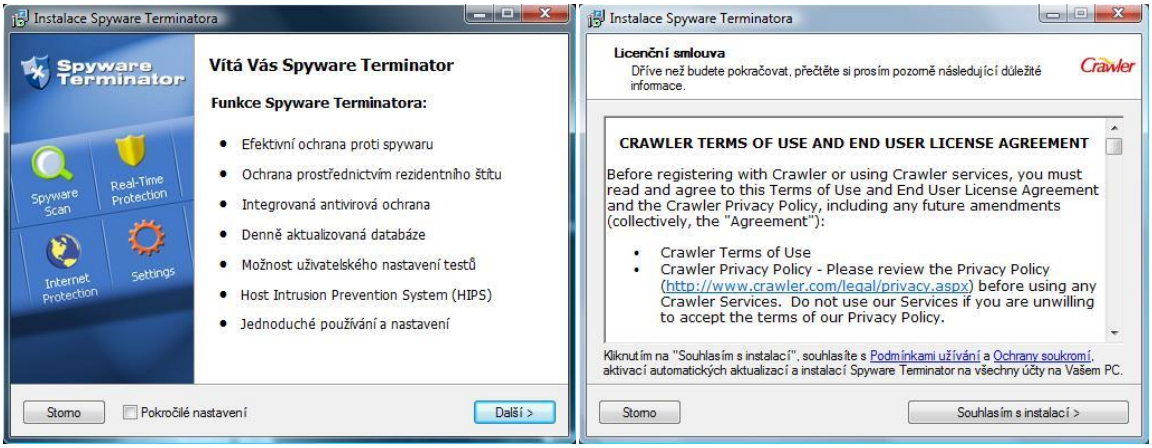
5.1.2 Průběh instalace

Po stažení instalačního klienta a jeho spuštění je možné postupovat krok za krokem dle tohoto návodu:

5.1.2.1 Průvodce instalací

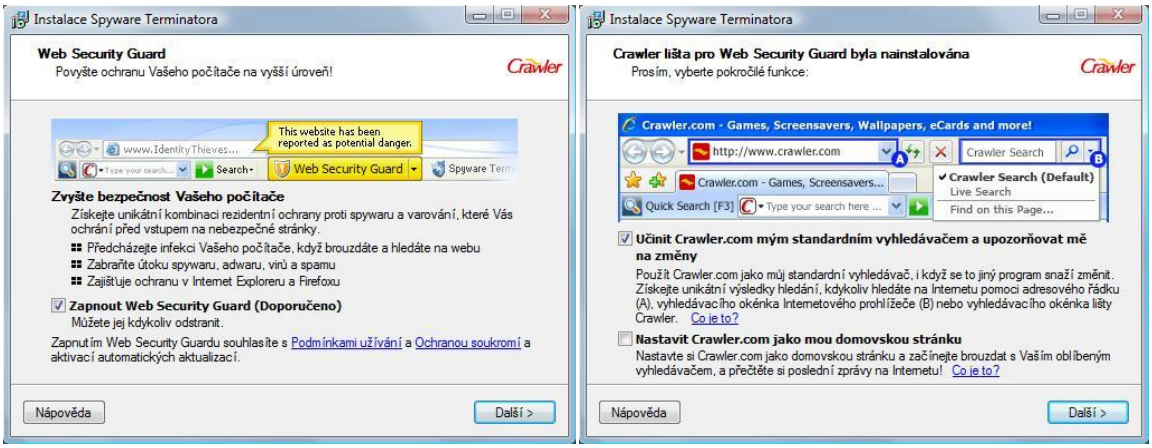
Při stažení české verze programu, bude instalace vypadat následovně. Ihned v prvním okně je dobré zaškrtnout volbu *pokročilého nastavení*, která dále umožní rozhodnout se, které další programy mohou být nainstalovány (Obr. 23).

V dalším okně je Licenční smlouva, kterou je doporučeno prostudovat před samotnou instalací. Nevýhodou je, že ujednání není v českém jazyce, ale v angličtině (Obr. 23).



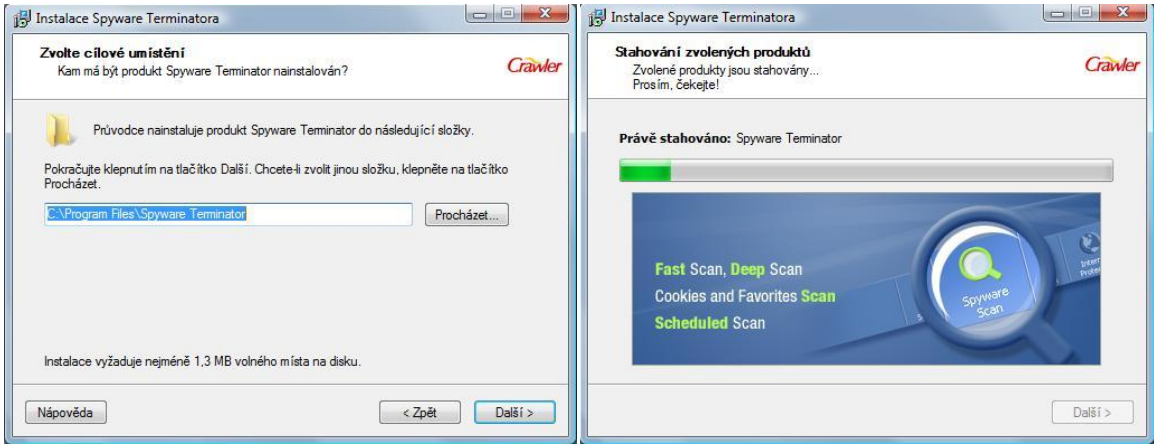
Obr. 23. Uvítací okno a licenční smlouva

Další dvě okna obsahují možnost nainstalovat doplňkový program, nebo povolit některá nastavení. Programy jsou toolbar do aplikace Internet Explorer, který zajišťuje ochranu před vstupem na nebezpečné stránky, který by mohly samotný spyware obsahovat. Tento toolbar je pouze pro Internet Explorer a Firefox, takže je jen na uživateli, jestli mu tato nabízená možnost vyhovuje (Obr. 24). Dále je možné nastavit stránky www.crawler.com jako výchozí vyhledávač v Internet Exploreru a jako domácí stránky prohlížeče (Obr. 24).



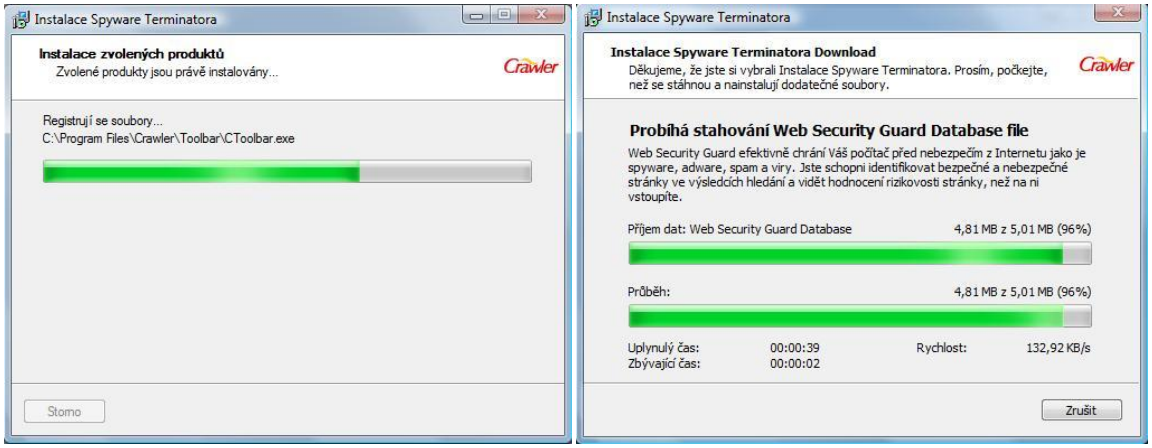
Obr. 24. Instalace Doplňkových aplikací Web Security Guard a Crawler

Další okno umožňuje vybrat, kam bude program instalován. Instalace zabere pouhých 1,3 MB místa na disku.

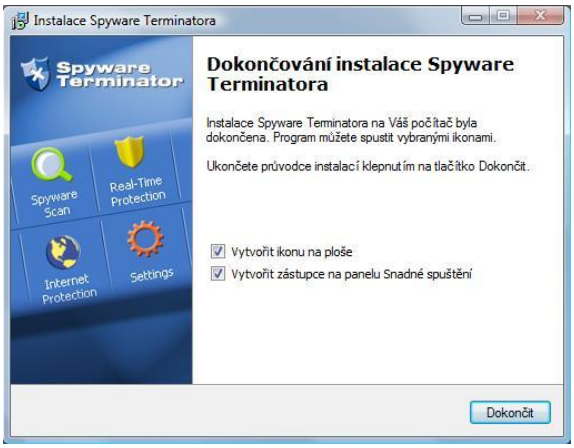


Obr. 25. Volba cíle instalace a stažení zvolených produktů

Následující okna zobrazují průběh stahování jednotlivých částí programu, které byly vybrány (Obr. 25). Pokračuje samotná instalace (Obr. 26) a aktualizace (Obr. 26) programu.



Obr. 26. Instalace programu a instalace aktualizací



Obr. 27. Dokončení instalace

O dokončení instalace vás informuje další okno. Je možné vybrat, zda se má vytvořit ikona na ploše, či zda má být vytvořen zástupce na panelu snadného spuštění. Obě tyto nabídky jsou primárně zaškrtnuty.

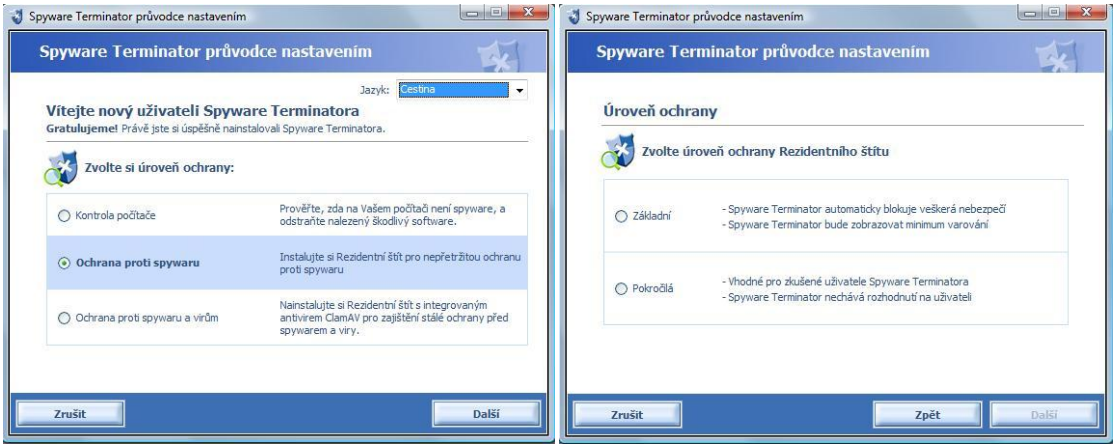
5.2 Použití programu

5.2.1 První spuštění

Po inicializaci programu (Obr. 28) se spustí řada nabídek pro nejlepší přizpůsobení aplikace uživateli.

Obr. 28. Inicializace programu

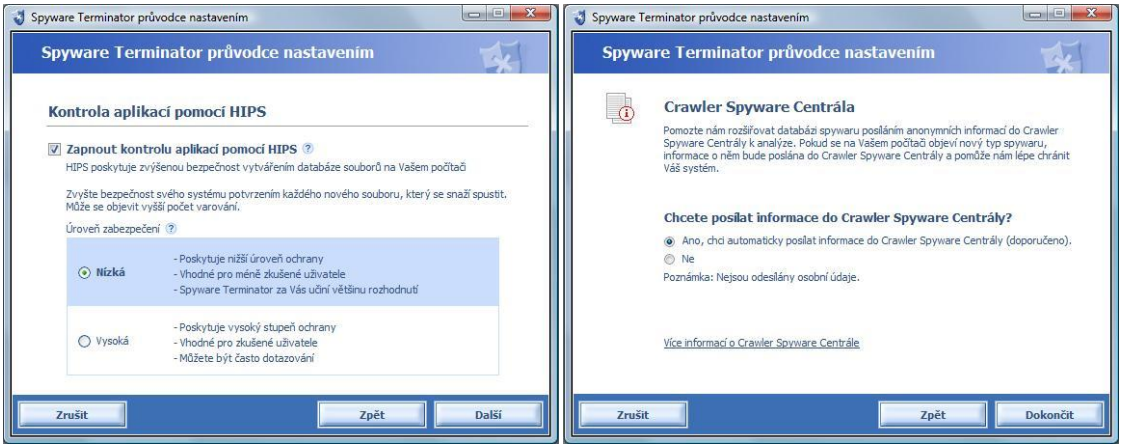
První okno nám nabízí výběr jazyka aplikace (Obr. 24) a způsobu jakým má být aplikace používána. V našem případě byla vybrána ochrana proti spyware. V druhém okně (Obr. 24) je možné nastavit úroveň ochrany rezidentního štítu (lze dále změnit). Co je rezidentní štít bude probráno níže.



Obr. 29. Výběr jazyka a nastavení úrovně ochrany

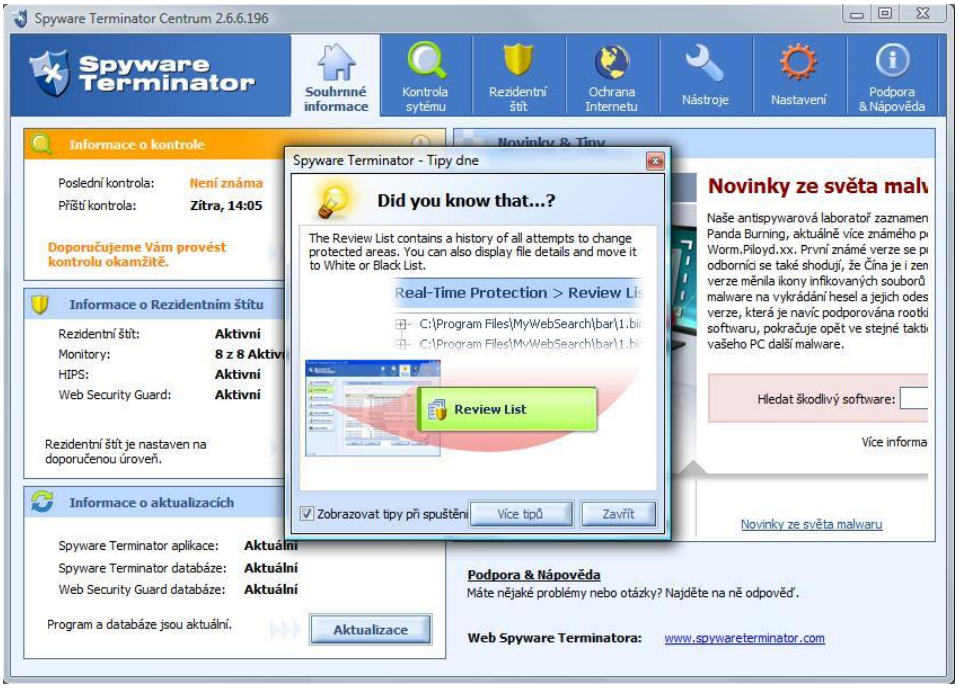
Další dvě okna s nastavením nabídnou možnost kontroly aplikací pomocí HIPS (Obr. 30). HIPS, (jinak Host Intrusion Prevention System), je zabezpečení v reálném čase, které sleduje chování spouštěných aplikací a rozhoduje o tom, zda je daná aplikace pro systém nebezpečná či ne. Pokud je tato funkce povolena, program vytvoří na pevném disku

databázi spustitelných souborů na lokálním disku. Pokud se některá aplikace bude chovat podezřele, například se bude snažit zapsat do nějaké cizí knihovny, program ihned zobrazí varování. V dalším okně je prosba o pomoc firmě Crawler Spyware Central (Obr. 30). Pokud je zaškrtnuta, je každý nový spyware, který se objeví na počítači, zaslán této firmě.



Obr. 30. Zapnutí kontroly aplikací pomocí HIPS a odesílání informací

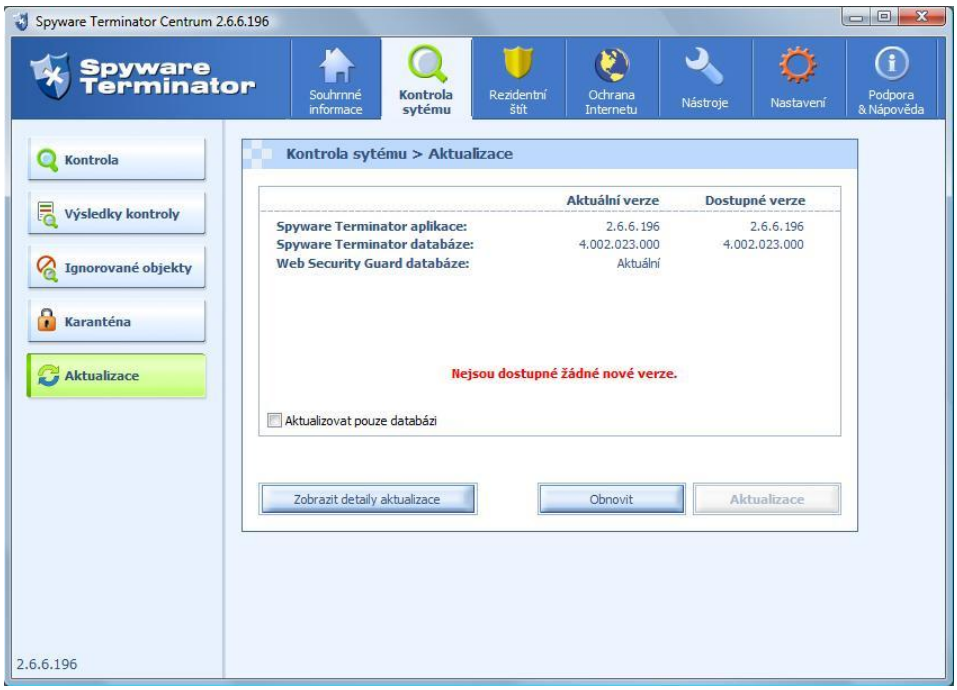
Dále následuje už jen samotné spuštění programu, kde bohužel *tipy dne* počeštěny nejsou (Obr. 31).



Obr. 31. Tipy dne

5.2.2 Aktualizace

Možnost aktualizace je přístupná již z úvodního menu, kde vlevo dole po kliknutí na tlačítko *aktualizace* program přejde do této nabídky (Obr. 32). Další možností je kliknout na záložku *Kontrola systému* a na levém postranním menu vybrat položku *aktualizace*. Ovšem vzhledem k tomu, že je možné v nastavení vybrat automatické aktualizace, není nutná manuální kontrola. Nastavení a jeho možnosti jsou podrobně popsány níže.

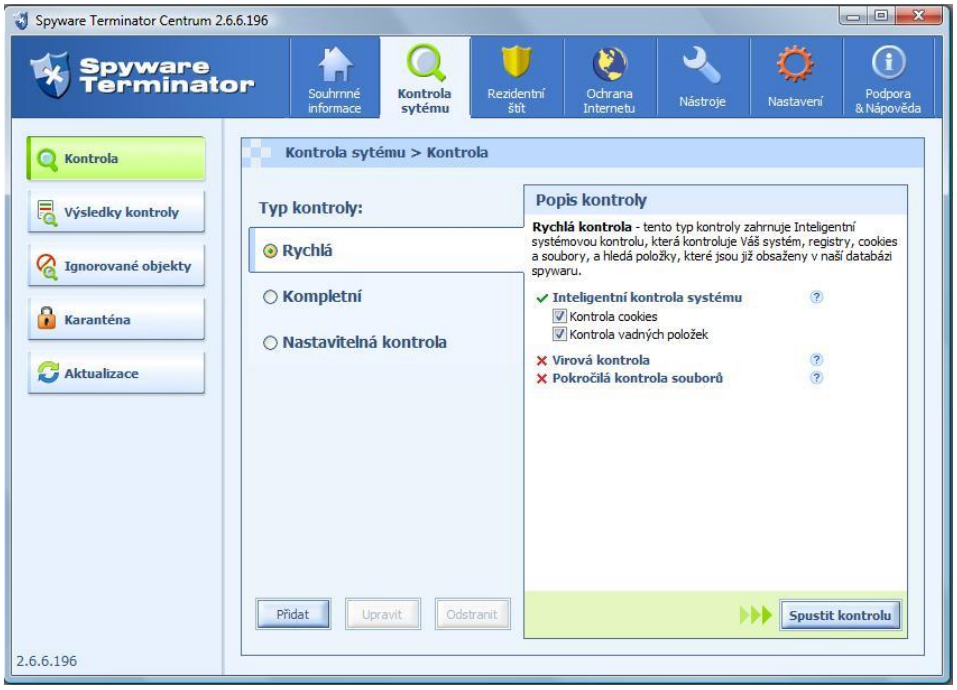


Obr. 32. Aktualizace

5.2.3 Skenování obsahu počítače

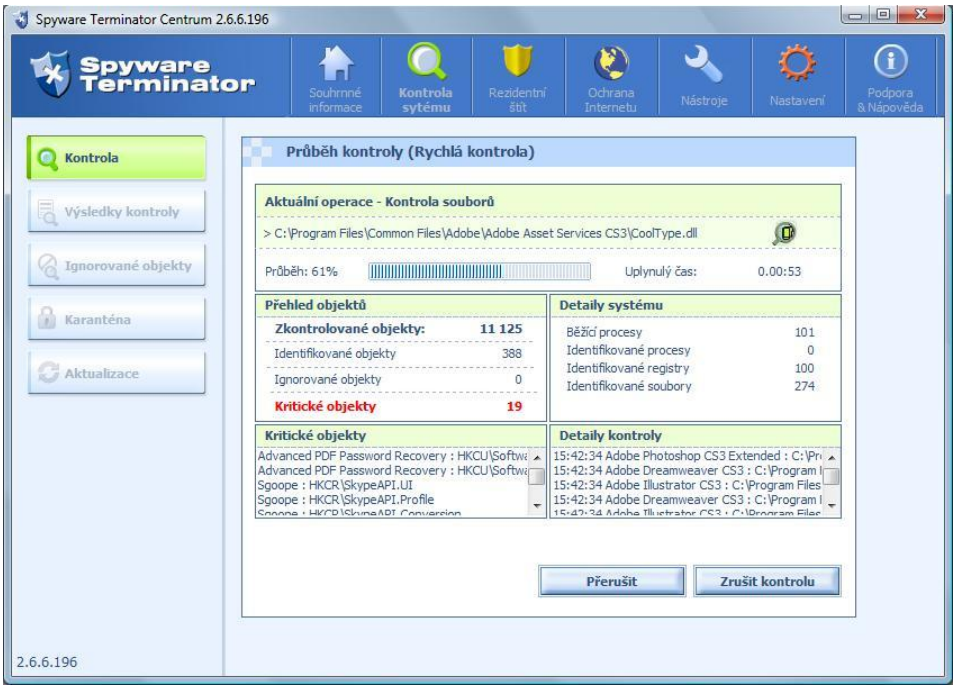
Spyware terminator nabízí tři druhy skenování počítače:

- **Rychlé** (kontroluje registry, cookies a soubory, hledá položky, které jsou v databázi spyware).
- **Kompletní** (kontroluje registry, cookies a soubory, hledá položky, které jsou v databázi spyware + vybrané soubory a disky).
- **Nastavitelná kontrola** (zde se dá navíc vybrat filtr typů souborů, které se mají proskenovat).



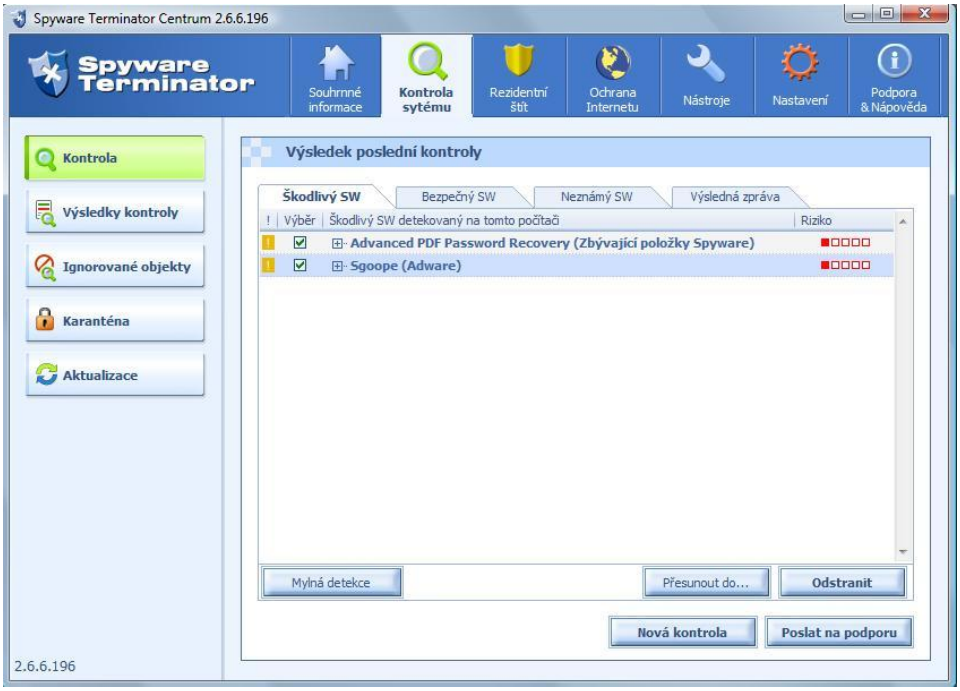
Obr. 33. Kontrola systému

Vybraná kontrola se spouští tlačítkem *spustit kontrolu* vpravo dole (Obr. 33). Průběh kontroly vypadá následovně (Obr. 34).



Obr. 34. Průběh kontroly

Výsledek zobrazuje škodlivý software, který je doporučen odstranit, bezpečný software, který firma zná a neznámý software, který běží na PC a většinou je neškodný. U každého škodlivého software je stupeň nebezpečnosti (červené čtverečky 1 - 5) - (Obr. 35).



Obr. 35. Výsledek kontroly

Další nabídky v záložce Kontrola systému:

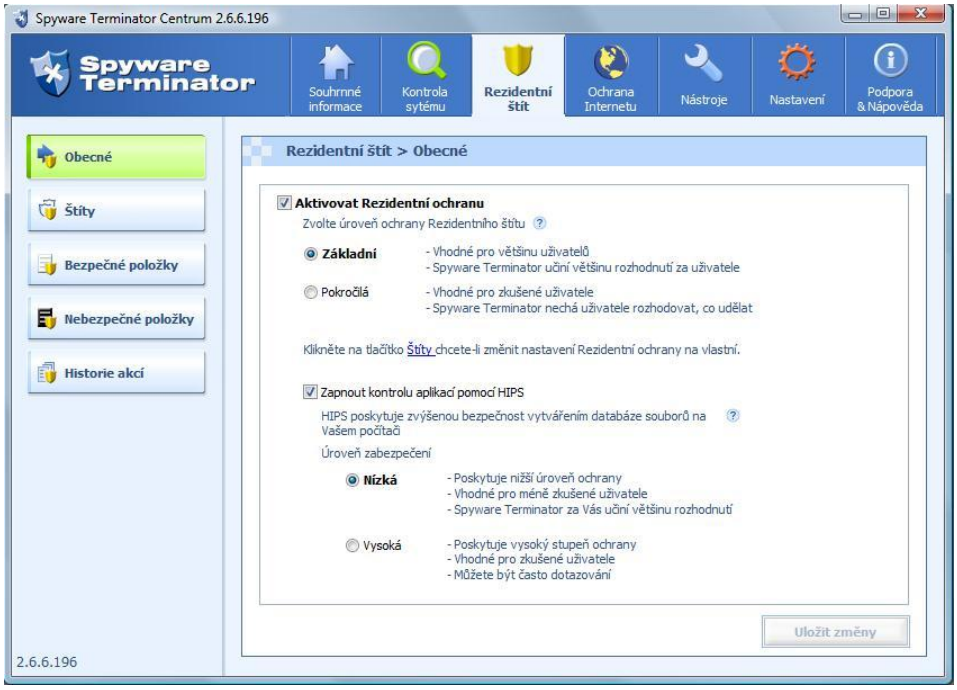
- **Výsledky kontroly** (zde jsou záznamy dřívějších skenování).
- **Ignorované objekty** (objekty které jsme se rozhodli ignorovat, program je již nepovažuje za škodlivé).
- **Karanténa** (objekty, které nešly smazat, jsou přesunuty do karantény).
- **Aktualizace** (viz výše).

5.2.4 Rezidentní štít

Tato aplikace chrání před špatnými rozhodnutími, před nebezpečným software, před jeho tajnou infiltrací a to včasným zastavením a varováním, případně dotazem, zda chce uživatel program opravdu nainstalovat.

Zapnutý rezidentní štít je ve správci úloh systému a zabírá pouze 5 224 kB z paměti, což je pozitivní.

Rezidentní ochrana má dvě úrovně. V základní úrovni rozhoduje program, v pokročilé rozhoduje uživatel (Obr. 36). Pokud se uživatel nechce zabývat každým rozhodnutím, které za něj obvykle dělá program, je doporučena základní úroveň. Pokud naopak uživatel chce pokročilou, rozhodně by si měl přečíst příručku k programu, kterou nalezne na stránkách firmy (pouze v anglickém jazyce).



Obr. 36. Rezidentní štít

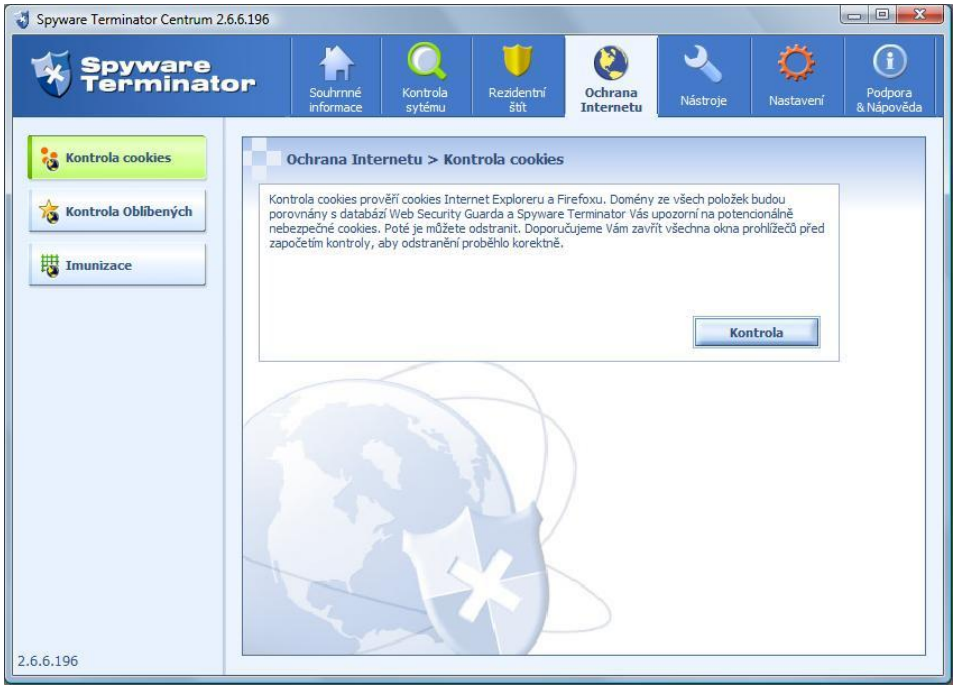
Další nabídky v záložce Rezidentní štít:

- **Štíty** (nastavení jednotlivých zabezpečení Exploreru, systémových knihoven, hostů, atd.).
- **Bezpečné položky** (zde může uživatel přidat aplikace, které štít bude brát jako bezpečné).
- **Nebezpečné položky** (zde může uživatel přidat aplikace, které štít bude brát jako nebezpečné).
- **Historie akcí** (výpis všech akcí, ať už povolení nějaké aplikace, zakázání, atd.).

5.2.5 Ochrana Internetu

Několik užitečných nástrojů k ochraně pohybu na internetu (Obr. 37):

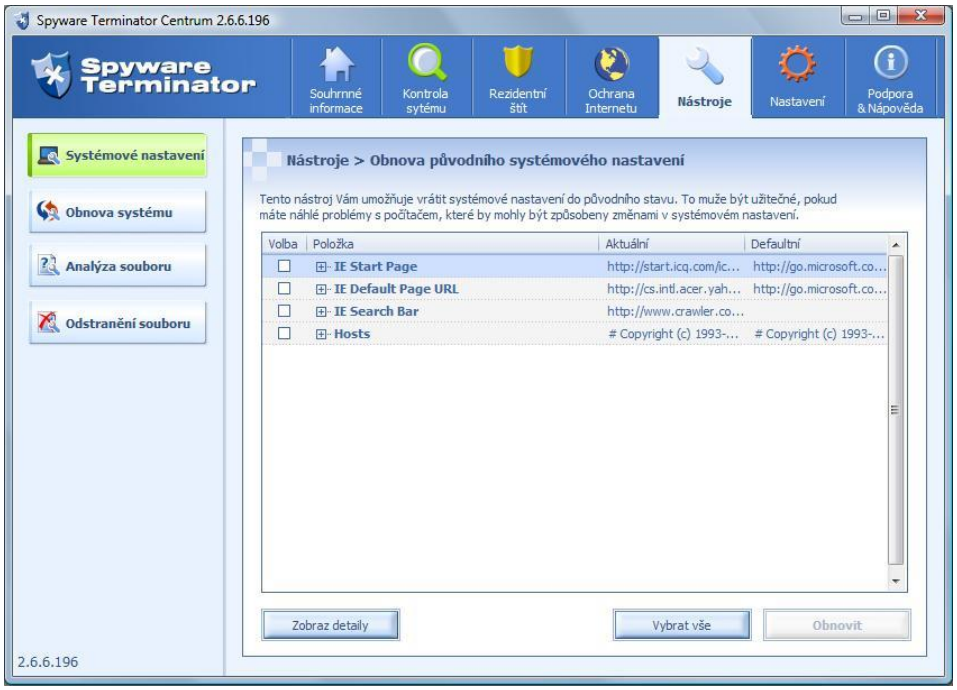
- **Kontrola cookies** (cookies v počítači porovná s databází Web Security Guard a nebezpečné nabídne k odstranění. Ovšem funguje pouze pro Internet Explorer a Firefox).
- **Kontrola oblíbených položek** (záložky v počítači porovná s databází Web Security Guard a nebezpečné nabídne k odstranění. Ovšem opět funguje pouze pro Internet Explorer a Firefox).
- **Imunizace** (slouží k zabezpečení různých softwarových děr - k 23. 2. 2010 na 5681 pravidel).



Obr. 37. Ochrana Internetu

5.2.6 Nástroje

V záložce *nástroje* je možné nalézt nástroje k původnímu systémovému nastavení změn, jako třeba změna domovské stránky (Obr. 24).



Obr. 38. Nástroje

Dále je zde možné nalézt:

- **Obnova systému** - při jakékoliv změně provádí Spyware Terminator zálohu systému, která může být jednoduše obnovena.
- **Analýza souboru** - Spyware Terminator vybraný soubor analyzuje a zjistí, zda je spuštěn, jaké jsou jeho vazby, kdo jej vyvinul a za jakým účelem. Zanalyzovaný soubor je možné poslat do centrály k další analýze.
- **Odstranění souboru** - umožní smazat i zamčený, chráněný soubor.

5.2.7 Nastavení

Nastavení všech komponent programu Spyware Terminator.

- **Nastavení programu:** volba jazyka, základní nastavení, nastavení odesílaní informací skupině vývojářů.
- **Nastavení kontroly:** volba nastavení kontroly, tj. jestli se mají kontrolovat nečitelné soubory (zamčené systémové soubory s příponou DLL a EXE), kontrola „Alternative file streams“ (AFS je funkcí, umožňující vývojářům spyware jejich kód schovat do existující aplikace). Dále jsou zde volby jako vytvořit po každé kontrole bod obnovení, který slouží k obnovení stavu systému před kontrolou.
- **Rezidentní štít:** nastavení automatické detekce instalací a možnost jejich zakázání, nebo automatické povolování aplikací, které jsou přidány v databázi bezpečného softwaru.
- **Nastavení plánovače:** plánovač se dá nastavit na plánované kontroly, dá se zde navolit, který den začít, v kolik hodin, a doplňující nastavení jak má kontrola probíhat.
- **Nastavení aktualizace:** důležité jsou dva typy stahování aktualizací. První přímo ze serveru firmy a druhý na principu peer to peer sítě, kde každý uživatel, který stahuje aktualizace je i zároveň poskytuje ostatním, což je poměrně inovativní a efektivní způsob. Příjemné je i to, že se dá nastavit jakou rychlostí odesílání a přijímání paketů má jít. Primárně je povoleno automatické stahování aktualizací, takže se o tuto činnost uživatel nemusí zajímat.
- **Web Security Guard:** tato záložka nastavení se zabývá přídavným pluginem do Internetu Exploreru, či Firefoxu. Jde o program, který hlídá navštívené stránky a upozorňuje, či dokonce zakáže vstup na stránky, které by mohly být škodlivé pro obsah počítače.

- **Clam Antivirus:** do samotného Spyware Terminatora je možné doinstalovat tento antivirový program, který je zcela zdarma. Jeho vlastnostmi a efektivností jsem se nezabýval.

5.3 Odinstalace

Program lze odinstalovat buď v nabídce start pod složkou Spyware Terminator, kde je možné kliknout na ikonku odinstalovat aplikaci, nebo jej lze najít v ovládacích panelech Windows Vista pod programy a funkce, kde jej lze rovněž odinstalovat.

6 AD-AWARE

Ad-aware patří mezi nejpoužívanější programy na obranu proti spyware. Přehledná menu a dobrý grafický design zpříjemňují samotné užívání. Jediným nedostatkem je chybějící překlad do českého jazyka. Ovšem díky jednoduchosti programu toto neodrazuje ani uživatele, kteří jinak preferují pouze počeštělé programy. [10]

6.1 Instalace programu

6.1.1 Stažení programu

Ad-aware také jako předešlé dva programy lze nalézt na všech českých serverech, které poskytují programy.

- Stahuj - http://www.stahuj.centrum.cz.
- Slunečnice - http://www.slunecnice.cz.
- Studna - http://www.studna.cz, atd.

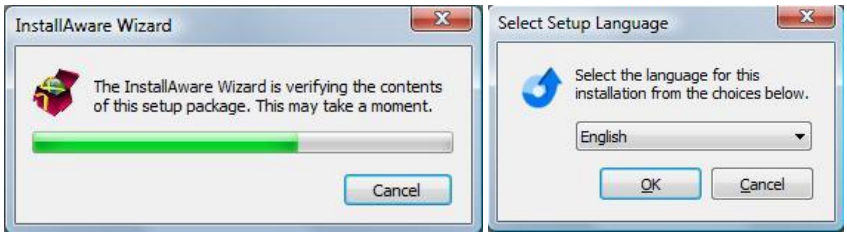
Dále lze program najít na domovské stránce - http://www.lavasoft.com.

6.1.2 Průběh instalace

Po stažení instalačního klienta a jeho spuštění postupujeme krok za krokem dle tohoto návodu:

6.1.2.1 Průvodce instalací

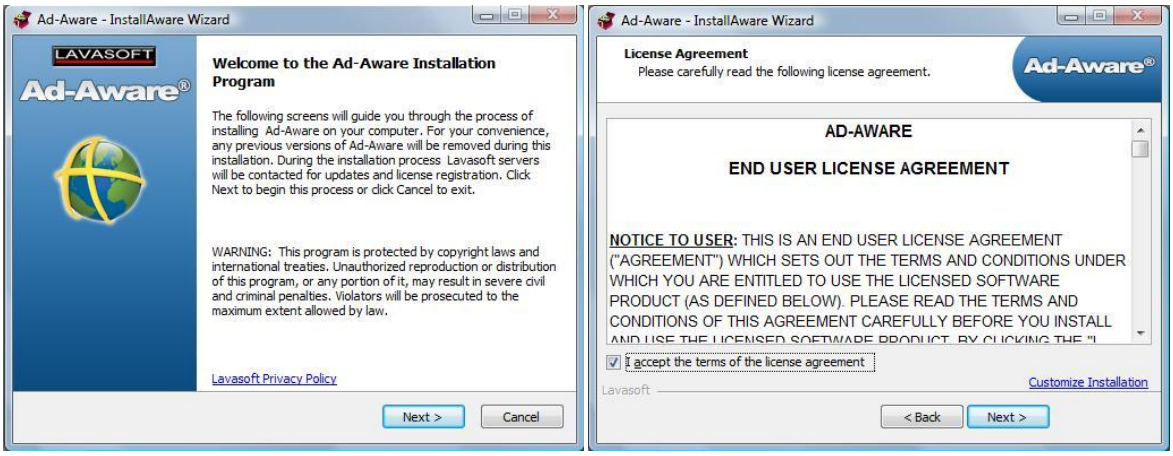
Prvním rozhodnutím v instalaci je výběr jazyka instalace (Obr. 39). Jsou zde na výběr jen nejrozšířenější jazyky, pro názornost zvolena instalace v angličtině.



Obr. 39. Inicializace instalace a výběr jazyka

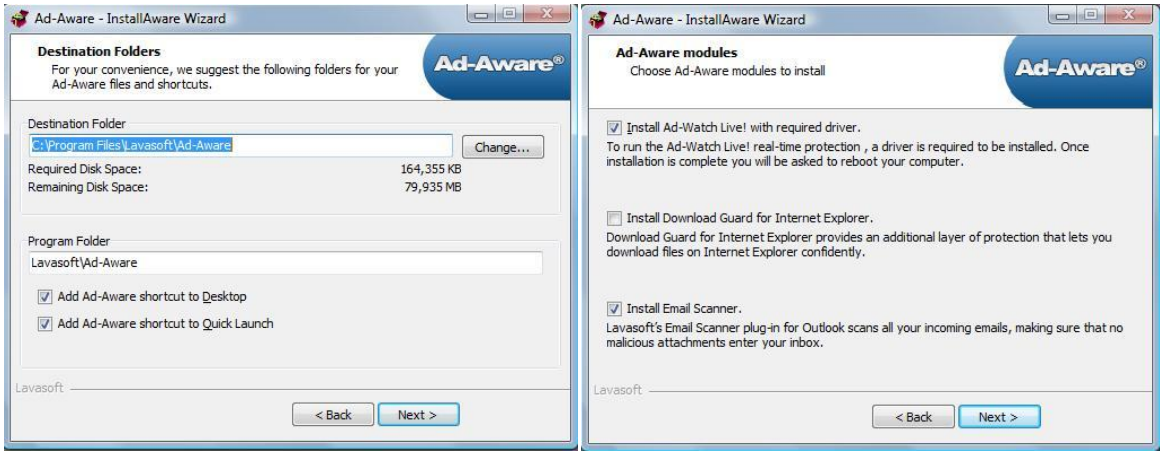
Po vybrání jazyka instalace se otevře uvítací okno, které je možné přečíst a pokračovat v instalaci tlačítkem *next* vpravo dole (Obr. 40). V instalaci je na výběr ze dvou možností: klasické a uživatelské (*customize installation*). Při klasické je program standardně nainstalován dvěma kliknutími, při uživatelské instalaci je na výběr z několika možností

navíc. Taktéž je zde uvedeno licenční ujednání, se kterým musí uživatel pro pokračování souhlasit (Obr. 40).



Obr. 40. Úvodní okno a licenční ujednání

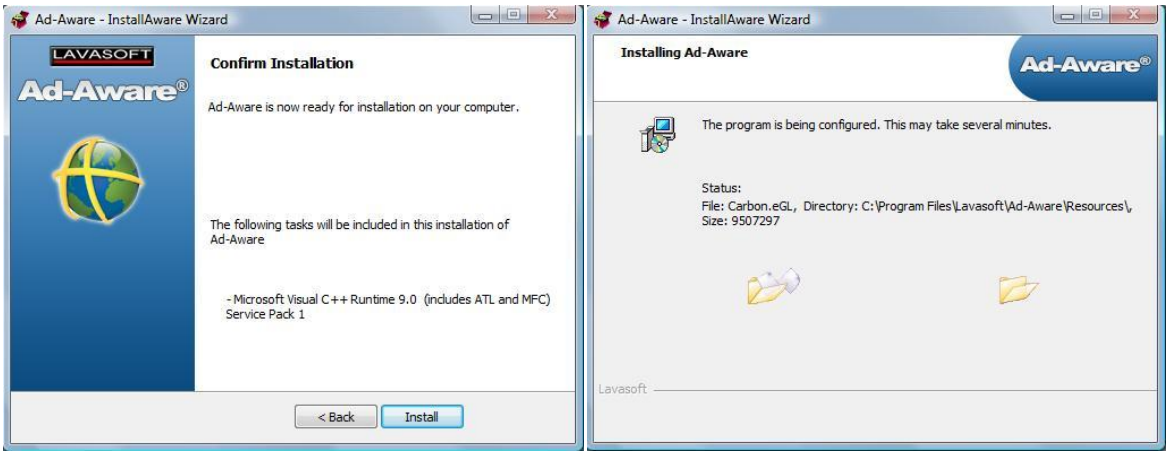
Pro prezentaci je vybrána uživatelská instalace, která po uživateli bude chtít několik rozhodnutí navíc. První z těchto rozhodnutí je kam chce program nainstalovat, kde ho lze nalézt v liště start a zda bude vytvořena ikona na ploše a na liště (Obr. 41). Další okno udává možnost nainstalovat se samotným programem některé funkce navíc (Obr. 41). První z nich je Ad-Watch Live, což je ochrana v reálném čase, která brání před špatnými uživatelskými rozhodnutími.



Obr. 41. Volba cíle instalace a možné funkce navíc

Druhá věc, kterou je možné nainstalovat, je strážce stahovaných souborů do Internetu Exploreru. Poslední volitelná součást je instalace Emailového Scanneru pro Outlook, která hlídá přílohy příchozích emailů. Tato součást je vhodná pro uživatele, který používá Outlook.

Dalším oknem je potvrzení instalace. Po potvrzení se spustí samotná instalace, která nepotřebuje přístup k internetu (Obr. 42).

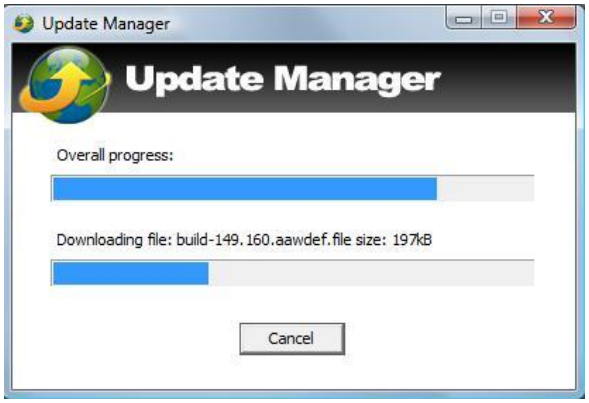


Obr. 42. Potvrzení instalace a průběh instalace

Na závěr instalace má uživatel poslední dvě možnosti a to restartovat počítač a aktivovat Ad-Watch Live! (Obr. 43). Další možností je poskytnout email firmě, která bude uživatele informovat o novinkách a speciálních nabídkách těchto produktů.

Obr. 43. Dokončení instalace

Pokud si uživatel ihned nevybere restart počítače, spustí se ještě po ukončení instalace update manager. Ten zajistí stažení potřebných definic do data nainstalování (Obr. 44). Při této akci už je potřeba připojení k internetu.



Obr. 44. Stahování definic

6.2 Použití programu

Uvítací okno po prvním spuštění informuje o dvou módech použití programu – jednoduchý a pokročilý (Obr. 45). Následující kapitoly se zabývají pokročilým módem.

Obr. 45. Uvítací okno

6.2.1 První spuštění

Program při prvním spuštění nabídne zakoupení licence (Obr. 46). Práce posuzuje rozdíl mezi některými volně šiřitelnými prostředky proti spyware a proto se dále zabývá volnou verzí.

Obr. 46. Nabídka zakoupení licence

6.2.2 Aktualizace

Ihned na první stránce otevřeného programu je stav aktualizací. Pokud se na něj klikne, začne samotný proces stahování aktualizací. Po něm se samotný program restartuje. Pokud je vše nejnověji aktualizováno, objeví se upozornění (Obr. 47).

Obr. 47. Aktualizace

Primárně je program nastaven tak, že aktualizace automaticky stahuje z internetu, kdykoliv jsou dostupné. Toto nastavení se dá změnit v samotném nastavení programu, které bude podrobně popsáno níže.

6.2.3 Skenování obsahu počítače

Na samotné skenování je možné přejít dvěma způsoby: Jednak z hlavní obrazovky po kliknutí na *scan system*, nebo kliknutím na horní záložku *scan*. Obě cesty uživatele zavedou na toto okno (Obr. 48).

Obr. 48. Nabídka skenování počítače

Záložky:

- **Scan -** zde se provádí samotné skenování počítače.
- **Quarantine** - neboli karanténa. Složka v PC kam se přesune spyware, který z nějakého důvodu nelze programem odstranit. Spyware zůstane na pevném disku, ovšem veškerá jeho činnost je zastavena.
- **Ignore list -** seznam ignorovaných programů v systému. Programy, které sem uživatel přidá, jsou při skenování ignorovány, i kdyby obsahoval spyware. Tato funkce se používá v případě, že uživatel používá volně šiřitelný program, jehož funkčnost závisí na přítomnosti spyware v PC. Například program obsahující reklamu viz. Adware.

Metody používané testy:

- **Criticals areas -** skenuje kritická místa počítače.
- **Running applications** - skenuje aplikace, které právě aktivně běží v paměti počítače.
- **Windows registry -** skenuje známý spyware v oblasti registrů.
- **Layered services Providers (LSPs) -** detekuje a zavírá nežádoucí programy, které zjišťují aktivitu uživatele na síti. LSPs musí být spuštěno k jeho zachycení.
- **Alternative data stream (ADS) -** skenuje soubory a zároveň kontroluje ADS proti podezřelým souborům. ADS – jsou skryté soubory, které jsou provázány s těmi viditelnými. Skrytý soubor může být jakéhokoliv typu a může být přidružen k souboru, ke složce, dokonce i ke kořenovému adresáři disku. Hlavní důvod, proč jsou nebezpečné je ten, že jsou pro uživatele skryty a pouze několik málo

antispywarových programů v nich dokáže skenovat. Dále je těžké je odstranit, dají se odstranit s provázaným souborem. Jejich velikost se nedá zjistit Explorerem ani příkazem Dir.

- **Host files** - skenuje soubory hosta. Některé změny zde mohou být provedeny spywarem typu unášeč stránek (viz. 2.3). Pokud uživatel používá některý program k jejich chránění, přidá ho na konci testu do ignorovaných pro nadcházející kontroly. Tím je zabráněno, že úpravy ochranným programem budou brány Ad-Awarem za nepřátelské a neprovede se jejich změna.
- **Most recetly used (MRUs)** - skenuje odkazy na dříve otevřené soubory v počítači.
- **Browsers hijacks** - skenuje prohlížeče, jejich domovskou stránku, vyhledávací stránku a oblíbené k zjištění nebezpečných URL adres. Více viz výše v kapitole Browsers hijackers.
- **Tracking cookies** - vyhledává tracking cookies, které sledují uživatelovo chování na internetu (navštívené stránky, zadávané požadavky do vyhledávače, apod.). Toto chování zaznamenávají a mohou ho odesílat třetí straně. Tuto schopnost tracking cookies využívají firmy, které si zadávají průzkum účinnosti reklamy, ovšem informace takto získané mohou být zneužity k profilování uživatelů a sledování jejich pohybu po internetu.
- **Rootkits** - metody schování programů či procesů před normálním způsobem vyhledávání, používané škodlivými programy k zneviditelnění své přítomnosti v počítači.
- **Archives** - program projde při skenování i soubory v archivech jako jsou rar a zip.
- **Executable files only** - kontrola pouze spustitelných programů typu exe.
- **Behavior-based detection** - tato kontrola pracuje na základě systému pravidel a šablon chování škodlivého software k odstranění ještě neznámého spyware.
- **Anti-Virus engine** - pokud má uživatel Ad-ware extended může ho použít i k hledání a odstraňování virů.

Máme zde na výběr ze tří druhů skenování, každý obsahuje jinou hloubku testu:

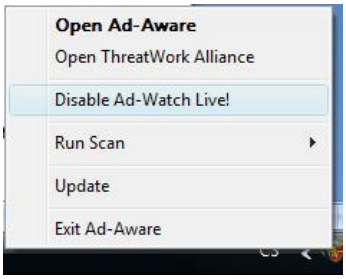
- **Smart Scan** - skenuje pouze spustitelné soubory, prohledává kritická místa, běžící aplikace, registry Windows, LSPs, unášeče stránek, tracking cookies, rootkits, a to i na základě pravidel v behavior-based detection.
- **Full Scan** - skenuje všechny soubory, prohledává kritická místa, běžící aplikace, registry Windows, LSPs, ADS, soubory hosta, MRUs, unášeče stránek, tracking cookies, rootkits, archívy a to i na základě pravidel v behavior-based detection.
- **Profile Scan** - u tohoto skenování je možné přesně nastavit, co chce uživatel skenovat a co ne. Nastavení se provádí po klinutí na tlačítko *settings*.

6.2.4 Ad-Watch live!

Jde o pasivní ochranu počítače, která ve volně šiřitelné verzi pouze chrání před nebezpečnými procesy váš systém. Tyto procesy budou ihned blokovány, pokud uživatel nebude chtít jinak. Všechny blokované procesy se zapisují do pravidel procesů (process rules), kde je možné je znovu případně povolit. Další možnosti ochrany mohou být zpřístupněny až po zakoupení produktu (Obr. 49).

Obr. 49. Nabídka Ad-Watch Live!

Pokud chce uživatel Ad-Watch vypnout stačí na spodní liště kliknout pravým tlačítkem na jeho ikonu a v otevřené nabídce vybrat disable Ad-Watch Live! (Obr. 50).



Obr. 50. Nabídka na liště

6.2.5 Extras

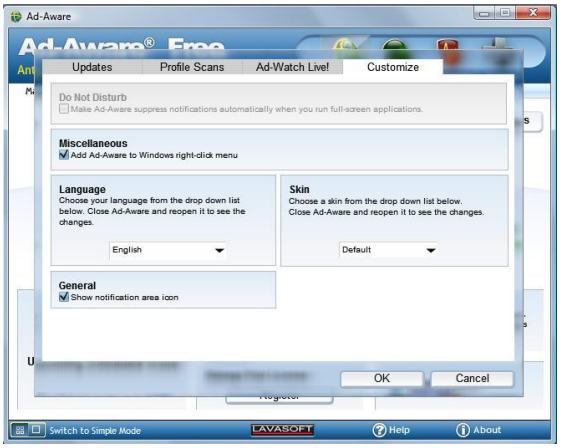
Několik doplňkových programů (Obr. 51):

- **TrackSweep** - maže paměť, historii, cookies, poslední psané URL, záložky v aplikaci Internet Explorer.
- **Toolbox** - zde je možné podezřelý soubor poslat k analýze společnosti Lavasoft. Stačí ho jen přetáhnout na nově otevřené okno.
- **Email scanner** - při používání Outlooku blokuje v příchozích emailech škodlivé přílohy.

Obr. 51. Nabídka extra

6.2.6 Nastavení

Do nastavení je možné se dostat z kterékoliv obrazovky programu po kliknutí na tlačítko *settings* (Obr. 52).



Obr. 52. Nastavení

Jsou zde tyto záložky:

- **Updates -** zde je možné nastavit, zda uživatel chce aktualizace automatické, nebo ne, dále jestli chce automaticky odesílat podezřelé soubory firmě Lavasoft.
- **Profile Scans –** uživatel zde může nastavit způsob skenování, a co vše chce skenovat (jaké adresáře). Tento profil si program pamatuje a může být kdykoliv znovu použit.
- **Ad-Watch Live! –** je možné zapnout či vypnout ochranu procesů pomocí Ad-Watch Live!
- **Customize -** přizpůsobení aplikace volbou jazyka, vzhledu a možnost zobrazení informační ikony na liště.

6.3 Odinstalace

Program lze odinstalovat jako oba předchozí buď v nabídce start pod složkou Lavasoft, kde se klikne na ikonku *odinstalovat aplikaci*, nebo je možné ho najít v ovládacích panelech Windows Vista pod programy a funkce, kde je rovněž možné ho odinstalovat.

7 POROVNÁNÍ VYBRANÉHO ANTISPYWARU

Všechny výše uvedené programy byly na konci ohodnoceny známkami 1-4 v těchto kategoriích:

1. **Grafické rozhraní** – design programu.
2. **Účinnost** – jaká byla účinnost programu po měsíčním používání, kdy počítač byl proskenován každým ze tří programů, bez smazání škodlivého software v počítači. Výsledkem byl počet nalezeného škodlivého software, který byl poté oznámkován.
3. **Přehlednost** – přehlednost rozhraní programu a jeho komunikace s uživatelem.
4. **Aktualizace** – způsob sledování a následná aktualizace.
5. **Systémové zdroje** – kolik běžící program používá ze systémových prostředků.
6. **Doprovodné programy** – možnosti doprovodných programů.
7. **Imunizační štít** – efektivita a množství blokovaných procesů.
8. **Rezidentní ochrana** – co vše je programem chráněno.
9. **Instalace** – hodnocena byla jednoduchost instalace.
10. **Výsledný průměr**

7.1 Grafické rozhraní

Grafické rozhraní Spyware Terminatora je stejně jako u Ad-ware graficky zdařilé. Ze všech tří programů se grafika u Spybot – S&D jeví jako nejméně zdařilá. Z toho vychází i hodnocení (Tab. 3).

Tab. 3. Hodnocení grafického rozhraní, přehlednosti a aktualizačního procesu

	Grafické rozhraní	Přehlednost	Aktualizační proces
Ad-Aware	1	2	2
Spyware Terminator	1	3	1
Spybot - S&D	4	1	3

7.2 Účinnost

Skeny byly provedeny na třech různých počítačích s těmito výsledky účinnosti (Tab. 4). Výsledný průměr je vyjádřen v procentech. Testovaný PC byl postupně proskenován všemi programy bez odstranění nalezeného spyware. Výsledek programu, který našel nejvíce spyware byl považován jako nejúspěšnější, výsledku bylo přiřazeno 100%. Výsledek

skenování ostatními programy byl převeden na procenta v závislosti na tomto nejúspěšnějším výsledku. V procentuální úspěšnosti byl nejlepší program Spybot - S&D.

Tab. 4. Účinnost vyhledání spyware.

	Skenování 1	Skenování 2	Skenování 3	Průměr úspěšnosti
Spybot - S&D	38 (38 cookies) (100%)	4 (4 cookies) (50%)	21 (21 cookies) (100%)	(83%) -1
Ad-Aware	0 (0%)	8 (8 cookies) (100%)	2 (2 cookies) (9,5%)	(36%) - 2
Spyware Terminator	2 (2 spyware) (5%)	0 (0%)	0 (0%)	(2%) - 4

7.3 Přehlednost

V přehlednosti jsou na předních místech jak Spybot - S&D, tak Ad-aware (Tab. 3), které nezatěžují uživatele zbytečnostmi, a všechny nejdůležitější procesy je možné spustit ihned z úvodní obrazovky. Snad jedinou nevýhodou Ad-aware je chybějící překlad do českého jazyka, proto je hodnocen známkou 2. Spyware Terminator by mohl ze začátku uživatele odradit velkým množstvím položek a propagací různého softwaru firmy, proto je hodnocen známkou 3.

7.4 Aktualizace

V práci byl nejlépe hodnocen (Tab. 3) Spyware Terminator a to za jeho zajímavý přístup k aktualizacím (viz.5.2.2). Stejně hodnocen byl i Ad-aware. Uvádí datum posledních nainstalovaných aktualizací, takže si uživatel může ověřit, že firma stále aktualizuje spywarové definice. Spybot - S&D byl hodnocen známkou 3 kvůli nutnosti hlídání nových aktualizací uživatelem, nelze nastavit automatické stahování aktualizací.

7.5 Systémové zdroje

Z programů nejvíce systémových prostředků při otevřeném okně programu využívá Spyware terminator a to 76 072 kB.Druhým je Spybot - S&D s 34 432 kB a nejméně zatěžuje systém Ad-aware s 14 004 kB.

Tab. 5. Využití systémových zdrojů

	Využití paměti	Hodnocení
Ad-Aware	14 004 kB	1
Spybot - S&D	34 432 kB	2
Spyware Terminator	76 072 kB	3

7.6 Doprovodné programy

Ad-aware, umí odstranit paměť, historii, poslední psané URL a cookies z těchto prohlížečů: Internet Explorer, Firefox, Opera, čímž čistí počítač od zbytečných dat.

Spybot - S&D, má doplňující program shredder, který dokáže soubor odstranit tak, že už nikdy nepůjde obnovit, což se uplatní proti některým druhům spyware.

Spyware Terminator, umí odstranit jinak neodstranitelný soubor (zamknutý, chráněný) a také můžete podezřelý soubor poslat na analýzu společnosti.

Tab. 6. Doprovodné programy

	Výhody	Hodnocení
Spyware Terminator	Analýza podezřelého souboru	1
Spybot - S&D	Program Shreeder	2
Ad-Aware	Čištění paměti	3

7.7 Imunizační štít

Nejvíce blokovaných procesů (Tab. 9) přes 120 000 v imunizačním štítu má Spybot - S&D. Následuje Spyware Terminator, který blokuje přes 5 000 procesů. Zajímavé je, že po provedení imunizace Spybotem - S&D zůstane ještě 4 300 neimunizovaných děr, které doplní Spyware Terminator. Ad-Aware bohužel žádný takový štít v základní verzi nemá.

Tab. 7. Imunizační štít

	Blokovaných procesů	Hodnocení
Spybot - S&D	120 000	1
Spyware Terminator	5 000	2

Ad-Aware	Nemá imunizační štít	4

7.8 Rezidentní ochrana

Zatímco Ad-Aware má ve volně šiřitelné verzi jen základní štít ochrany procesů po startu systému, ostatní dva programy jsou vybaveny lépe. Spybot - S&D chrání systémová nastavení a blokuje škodlivé stahování pro Internet Explorer. Nejvíce možnostmi v této kategorii disponuje Spyware Terminator, kdy se jeho rezidentní štít může nastavit tak, aby uživateli maximálně vyhovoval. Štít poté chrání a kontroluje položky po spuštění, ovladače, webové prohlížeče, asociaci přípon souborů, Internet Explorer, systémové INI soubory, a host files (Tab. 8).

Tab. 8. Rezidentní ochrana

	Chrání	**Hodnocení**
Spyware Terminator	Položky po spuštění, ovladače, web. prohlížeče, systémové INI, atd.	1
Spybot - S&D	Systémová nastavení, blokuje škodlivé stahování IE	2
Ad-Aware	Procesy po startu	3

7.9 Instalace

V porovnávání instalací byla v práci nejlépe hodnocena snadná a rychlá instalace s minimem potřebných kliknutí. Z toho důvodu je nejlépe hodnocena instalace Ad-aware která, neinstaluje žádné zbytečné aplikace navíc a vyžaduje minimální pozornost uživatele. Druhá nejlépe hodnocená instalace je u programu Spybot - S&D, která je také přehledná, ovšem už s větší interakcí uživatele. Na podobné úrovni je instalace Spyware terminatora, která doinstaluje některé programy navíc pro ochranu Internet Exploreru a Firefoxu, což může být pro uživatele používajícího alternativní prohlížeč nepotřebné.

Tab. 9. Instalace

	Interakce při instalaci	**Hodnocení**
Ad-Aware	Nejpřehlednější	1
Spyware Terminator	Přehledná	2
Spybot - S&D	Méně přehledná	3

7.10 Výsledný průměr

V této tabulce je zobrazen průměr ze všech dosažených známek vycházející z celé práce a hodnocení, které dokazuje, že zkoumané antispywarové programy jsou na podobné úrovni.

Tab. 10. Výsledný průměr

	Průměrná známka	Výsledné hodnocení
Spybot - S&D	1,7	1
Ad-Aware	2,1	2
Spyware Terminator	2,4	3

ZÁVĚR

Hlavním cílem bakalářské práce bylo upozornit na nebezpečí krádeže dat a varovat před stálou hrozbou spyware. Většina uživatelů si tuto hrozbu uvědomuje, ale s postupem času jí podcení, nebo jí nepřikládá dostatečnou důležitost. Dílčím cílem bylo seznámit s touto problematikou a navrhnout řešení, které je nejvíce přijatelné vzhledem k základní ochraně dat a zároveň specifické ke konkrétním potřebám konkrétního uživatele.

V současné době se uživatelé brání spíše virovému ohrožení, ovšem většina antivirových aplikací na samotný spyware nestačí. Z toho důvodu bylo vyvinuto několik aplikací, které se soustředí pouze na vyhledávání a odstranění spyware. S tím se ovšem objevila i řada falešných programů, které naopak spyware do počítače stahují. Z toho důvodu je v práci věnována pozornost vysvětlení samotného pojmu spyware a jeho rozpoznání, případně rozpoznání jeho projevů v počítači. Vzhledem k vysoké produkci nových a zákeřnějších druhů spyware je nutné být v této problematice obezřetný, proto je v ochraně dat nejdůležitější samotné školení uživatelů, které si tato práce klade za cíl. Z toho důvodu bylo v práci porovnáno několik antispywarových programů, s podrobným návodem k použití.

V úvodu práce byla ochrana dat přirovnána k ochraně hradu před vpádem nepřátel. Kde nejdůležitější postavou byl samotný Král, který má veškerá potřebná práva ke všemu v hradě a přilehlému okolí. Z toho vyplývá, že obrana může být jen tak dobrá, jak dobrý a poučený je král- uživatel.

Výsledkem práce je ucelený přehled o této problematice využitelný jak pro výuku, tak jako základní materiál do každodenní praxe.

CONCLUSION

The main objective of this thesis was to highlight the dangers of data theft and warn against the constant threat of spyware. Most users are aware of this threat, but over time underestimate it, or it does not place such importance. The secondary objective was therefore familiar with this problem and proposes a solution that is most suitable, given the basic data protection, and specific to the particular needs of individual users.

Currently, users rather prevent against viral threats, but most antivirus applications on the spyware itself is not enough. Therefore, several applications have been developed, which focuses only on finding and removing spyware. With that, however, appeared a number of fake programs that in turn download spyware to your computer. For this reason the work given to the explanation of the term spyware and its recognition or recognition of his speeches on the computer. Given the high production of new and insidious types of spyware is necessary to be cautious in this issue, therefore, is the most important data protection by users training, which this work taking like a objective. Therefore, it was the work of comparison of several anti-spyware programs, with detailed instructions.

In introduction was data protection equated to protect the castle against an onslaught of enemies. The most important person in whole castle was the king. He has all necessary rights to everything in the castle and to all adjacent places. It follows that the defense can be just as good as a good and informed the king-user.

The result of this work is a comprehensive overview of the issue is usable as a teaching as a base material into everyday practice.

SEZNAM POUŽITÉ LITERATURY

[1] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. 200 s. ISBN 80-251-0106-1.

[2] DOSEDĚL, Tomáš. *21 základních pravidel počítačové bezpečnosti*. Brno: Computer Press, 2005. 56 s. ISBN 80-251-0574-1.

[3] KOCMAN, Rostislav, LOHNISKÝ, Jakub. *Jak se bránit virům, spamu a spyware.* Brno: Computer Press, 2005. 152 s. ISBN 80-251-0793-0.

[4] THOMAS, M. Thomas. *Zabezpečení počítačových sítí*. Brno: Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

[5] SOUKUP, Petr. *Češky a Češi v kyberprostoru* [online]. Praha : MV ČR, 2008. 194 s. Výzkumná zpráva. UNIVERZITA KARLOVA V PRAZE, FAKULTA SOCIÁLNÍCH VĚD, Institut sociologických studií. Dostupné z WWW: <www.mvcr.cz/soubor/cyber-vyzkum-fsv-zprava-pdf.aspx>.

[6] FOSSI, Marc, et al. *Security Threat Report* [online]. [s.l.] : Symantec, 2008 [cit. 2010-03-30]., s. 110. Dostupné z WWW: <http://www.symantec.com/connect/sites/default/files/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf>.

[7] *Spam Laws* [online]. 2009 [cit. 2009-11-24]. Dostupné z WWW: <http://www.spamlaws.com>.

[8] *Spyware Guide* [online]. 2007 [cit. 2009-12-04]. Dostupné z WWW: <http://www.spywareguide.com>.

[9] *Spyware Warrior* [online]. 2007 [cit. 2010-01-13]. Dostupné z WWW: <http://www.spywarewarrior.com>.

[10] *Lavasoft* [online]. 2010 [cit. 2010-02-20]. Dostupné z WWW: <http://www.lavasoft.com/>.

[11] *Spybot Search & Destroy* [online]. 2010 [cit. 2010-03-08]. Dostupné z WWW: <http://www.lavasoft.com/>.

[12] *Spyware Terminator* [online]. 2010 [cit. 2010-03-13]. Dostupné z WWW: <http://www.spywareterminator.com/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ADS	Alternative data streams
AFS	Alternative file streams
BHO	Browser helper objels
DLL	Přípona knihoven
EXE	Přípona spustitelného souboru
IE	Internet Explorer
LSPs	Layered services Providers
MRUs	Most recetly used
PC	Personal computer (osobní počítač)
S&D	Search & Destroy

SEZNAM OBRÁZKŮ

SEZNAM TABULEK