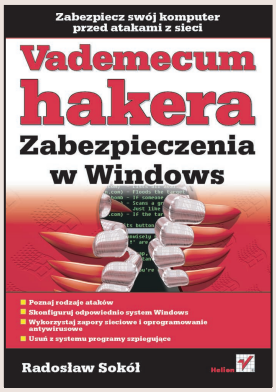
Vademecum hakera. Zabezpieczenia w Windows

Autor: Radosław Sokół
ISBN: 83-7361-636-5
Format: B5, stron: 304



Czasy, w których do zabezpieczenia komputera i zgromadzonych w nim danych wystarczył kluczyk i plomba, bezpowrotnie minęły. Rozwój sieci, poza ogromnym ułatwieniem komunikacji, stworzył wiele nowych zagrożeń — regularnie spotykamy się z coraz bardziej wymyślnymi wirusami komputerowymi, atakami na sieci i portale korporacyjne, a coraz częściej również na komputery prywatne. Lekceważenie tych zagrożeń może spowodować poważne kłopoty, nie tylko z komputerem, ale także i z prawem. Jak więc zabezpieczyć przed atakami z sieci komputer pracujący pod kontrolą systemu z rodziny Windows?

Odpowiednie „opancerzenie" Windows nie jest zadaniem łatwym, ale też nie jest niemożliwe. Książka „Vademecum hakera. Zabezpieczenia w Windows" opisuje wszystkie elementy tego procesu — od odpowiedniego skonfigurowania systemu operacyjnego, poprzez zainstalowanie oprogramowania antywirusowego i monitorującego połączenia sieciowe, aż do odpowiedniego przeszkolenia użytkowników komputera.

- Rodzaje ataków i wirusów
- Podstawowe informacje o protokole TCP/IP
- Konfiguracja BIOS-u
- Konfiguracja systemu Windows XP — aktualizacje, konta użytkowników, zapora sieciowa i udostępnianie zasobów
- Konfiguracja systemu Windows 98 SE
- Szkolenie użytkowników komputera
- Instalowanie i wykorzystywanie programów antywirusowych, zapór sieciowych oraz programów monitorujących połączenia sieciowe

Pamiętaj, że każdy komputer można w pewnym stopniu zabezpieczyć. Nawet najbardziej podstawowe zabezpieczenia mogą uchronić Cię przed wieloma nieprzyjemnymi sytuacjami.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Wprowadzenie **7**

Część I Ataki i zabezpieczenia **13**

Rozdział 1. Podstawy **15**

Ataki 15
Ataki DoS 15
Włamania 17
Wirusy 18
System operacyjny 18
Funkcjonalność sieciowa 18
Wielodostęp 20
Wieloprogramowość i wielozadaniowość 21
Konta użytkowników 22
Sieci TCP/IP 23
Model ISO/OSI 26
Działanie zapory sieciowej 27
Podsłuchiwanie transmisji sieciowej 28
Sieci bezprzewodowe 30
Wirusy, konie trojańskie i moduły szpiegujące 31
Czym jest wirus komputerowy? 32
Jak komputer ulega infekcji? 36
Jaki może być skutek infekcji? 37
Jak zabezpieczyć komputer przed infekcją? 38
Czy program antywirusowy jest pewnym zabezpieczeniem? 40
Jakie są wady korzystania z programów antywirusowych? 41
Przepełnianie buforów 41

Rozdział 2. Konfiguracja programu BIOS **43**

Wejście do programu konfiguracyjnego płyty głównej 44
Włączanie ochrony antywirusowej 44
Modyfikacja sekwencji startowej komputera 45
Zabezpieczanie dostępu do ustawień BIOS-u hasłem 46

Rozdział 3. Konfiguracja Windows XP 49
Instalacja pakietów ServicePack 49
Aktualizacja poprzez Windows Update 53
Automatyczna aktualizacja systemu 53
Ręczna aktualizacja systemu 54
Zakładanie kont użytkowników 56
Windows XP Professional 57
Windows XP Home 62
Odłączanie usług od interfejsów sieciowych 66
Zapora sieciowa systemu Windows XP 68
Uaktywnianie zapory sieciowej 69
Udostępnianie wybranych usług 71
Tworzenie własnej reguły zapory sieciowej 72
Kontrolowanie zasad ruchu ICMP 73
Polisy systemowe 75
Usługi systemowe 76
Udostępnianie zasobów i kontrola uprawnień 78
Zmiana uprawnień do plików i folderów na partycjach NTFS 79
Udostępnianie plików i folderów 80
Wyłączanie zdalnego dostępu do pulpitu 83

Rozdział 4. Konfiguracja Windows 98 SE 85
Aktualizacja systemu 86
Zakładanie kont użytkowników 88
Dołączanie komputera do domeny 91
Odłączanie usług od interfejsów sieciowych 93
Udostępnianie zasobów 95
Wyświetlanie listy udostępnionych zasobów 97

Rozdział 5. Szkolenie użytkowników 99
Korzystanie z kont użytkowników o ograniczonych uprawnieniach 99
Szybkie przełączanie użytkowników 102
Tworzenie haseł 106
Instalacja oprogramowania 108
Uruchamianie załączników pocztowych 109
Korzystanie z aplikacji Peer to Peer 110
Monitorowanie działających procesów 111
Przeglądanie dziennika zdarzeń 115

Część II Oprogramowanie dodatkowe 119

Rozdział 6. Agnitum Outpost Firewall 121
Instalacja 121
Aktualizacja pakietu 123
Konfiguracja programu 125
Zakładka Główne 125
Zakładka System 127
Zakładka Tryb pracy 135
Zakładka Wtyczki 136
Tworzenie reguł filtrowania ruchu 150
Półautomatyczne tworzenie reguł filtrowania ruchu 151
Ręczne tworzenie reguł filtrowania ruchu 157
Modyfikowanie reguły filtrowania ruchu 159
Usuwanie informacji o programie 161

Podgląd aktywnych połączeń TCP ... 161
Podgląd aktywnych połączeń i gniazd nasłuchujących TCP ... 161
Zrywanie wybranych połączeń ... 163
Przeglądanie dziennika aktywności zapory sieciowej ... 164
Wybór wyświetlanych kolumn dziennika ... 164
Wybór zakresu czasu wyświetlanych zdarzeń ... 166
Czyszczenie dziennika aktywności ... 166

Rozdział 7. SpyBot Search & Destroy ... 167
Instalacja programu ... 168
Aktualizacja bazy informacji o modułach szpiegujących ... 173
Uruchamianie programu ... 176
Konfiguracja programu ... 177
Skanowanie systemu w poszukiwaniu modułów szpiegujących ... 180
Wyłączanie programów uruchamianych w czasie ładowania systemu operacyjnego ... 183

Rozdział 8. Internetowy skaner MkS_Vir ... 185
Uruchamianie skanera ... 185
Aktualizowanie bazy danych skanera ... 187
Skanowanie plików i folderów ... 189
Zainfekowane pliki ... 191

Rozdział 9. Norton AntiVirus 2004 ... 193
Instalacja pakietu ... 193
Wstępna konfiguracja i aktualizacja pakietu ... 197
Zmiana konfiguracji pakietu ... 203
Zakładka Auto-Protect ... 205
Zakładka Auto-Protect: Bloodhound ... 206
Zakładka Auto-Protect: Advanced ... 207
Zakładka Auto-Protect: Exclusions ... 208
Zakładka Script Blocking ... 210
Zakładka Manual Scan ... 211
Zakładka Manual Scan: Bloodhound ... 212
Zakładka Manual Scan: Exclusions ... 213
Zakładka Email ... 215
Zakładka Email: Advanced ... 216
Zakładka Instant Messenger ... 217
Zakładka LiveUpdate ... 218
Zakładka Threat Categories ... 220
Zakładka Threat Categories: Advanced ... 221
Zakładka Threat Categories: Exclusions ... 222
Zakładka Miscellaneous ... 223
Aktualizowanie bazy danych o wirusach ... 224
Automatyczna aktualizacja bazy informacji o wirusach ... 226
Włączanie i wyłączanie aktywnego skanera antywirusowego ... 227
Skanowanie systemu w poszukiwaniu wirusa ... 227
Działanie aktywnego skanera antywirusowego ... 230
Antywirusowy filtr poczty elektronicznej ... 231
Wyświetlanie zawartości magazynu kwarantanny ... 233
Encyklopedia wirusów ... 235

Rozdział 10. Narzędzia Registry Monitor i File Monitor 237
O Autorach 238
Instalacja 238
Registry Monitor 240
Uruchamianie programu 240
Wstrzymywanie i wznawianie monitorowania dostępu 241
Ograniczanie zbioru danych 241
Podświetlanie określonych wpisów 243
Wybór formatu zapisu czasu 244
Zmiana czcionki 244
File Monitor 244
Wstrzymywanie i wznawianie monitorowania dostępu 245
Ograniczanie zbioru danych 246
Podświetlanie określonych wpisów 248
Wybór formatu zapisu czasu 248
Zmiana czcionki 249

Rozdział 11. Portscan i NMapWin 251
Portscan 251
NMapWin 253
Instalacja programu NMapWin 253
Instalacja sterownika WinPCap 255
Używanie programu NMapWin 256

Dodatki 263

Dodatek A Słowniczek terminów i pojęć 265

Dodatek B Przedrostki i jednostki miary stosowane w informatyce 279

Dodatek C Numery portów TCP i UDP 283

Dodatek D Podpowiedzi 287

Skorowidz 293

Rozdział 7.
SpyBot Search & Destroy

Moduły szpiegujące instalowane — często skrycie — przez strony WWW lub niby całkowicie darmowe programy mogą naprawdę uprzykrzyć życie. Nie dość, że spowalniają komputer i naruszają Twoją prywatność, bo zbierają dane o Twoich zwyczajach związanych z użytkowaniem komputera, ale jeszcze same mogą stać się „tylnym wejściem", jeśli ktoś wykorzysta błędy w ich kodzie do poważniejszego włamania.

Niektóre programy tego typu zawierają moduły wyświetlające w najmniej oczekiwanych momentach okna reklamowe (wyobraź sobie, że Twoja córka lub młodsza siostra podczas zabawy z programem edukacyjnym nagle ujrzy na ekranie okno reklamujące stronę z ostrą pornografią), inne zbierają tylko informacje i wysyłają je do centrali firmy, która stworzyła dany program, jeszcze inne zaś wykonują na Twoim komputerze różne obliczenia, zwiększając zużycie prądu, spowalniając komputer i podnosząc ryzyko awarii sprzętu na skutek zbyt słabego chłodzenia.

Nie trzeba wcale odwiedzać pornograficznych stron WWW lub archiwów nielegalnego oprogramowania, by zainfekować komputer modułem tego typu. Nawet niektóre programy użytkowe — nęcące użytkownika darmową pełną wersją — są darmowe tylko dlatego, że wraz z programem instalowany jest jakiegoś typu moduł szpiegujący. Nigdy nie wiadomo, gdzie w Internecie natkniesz się na szpiega.

Program *SpyBot Search & Destroy* (jego autorem jest Patrick M. Kolla) powstał, by umożliwić użytkownikom walkę z zarazą programów szpiegujących — tak zwanych programów *spyware*. Sam program jest całkowicie darmowy — autor prosi tylko o przysyłanie informacji o nowych, niedawno powstałych modułach szpiegujących oraz — w miarę możliwości — dotowanie prac nad programem niewielkimi datkami. Dzięki temu programowi odszukiwanie i usuwanie modułów szpiegujących sprowadza się do kliknięcia kilku przycisków wyświetlanych w jego oknie; SpyBot sam utworzy listę znanych mu modułów, pozwoli wybrać dowolne z nich do usunięcia i w bezpieczny sposób je zablokować.

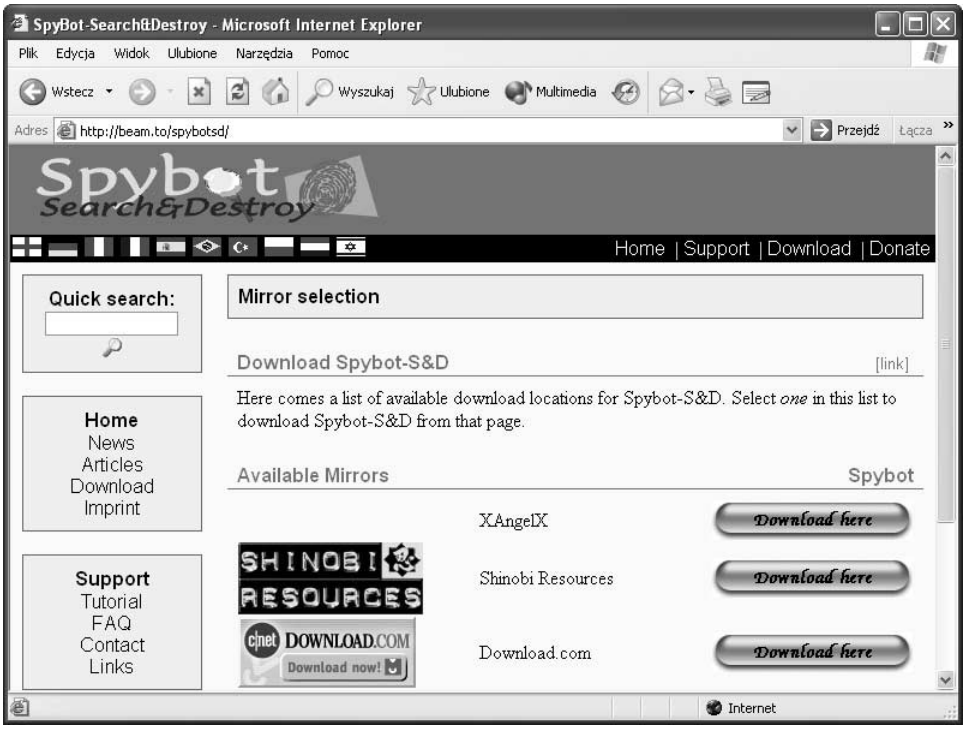
Pamiętaj, że programu używasz wyłącznie na własną odpowiedzialność. Jeśli jeden z używanych przez Ciebie programów wymaga modułu szpiegującego, by się uruchomić, a program SpyBot usunie go, uniemożliwiając start aplikacji, nie wiń autora, tylko ponownie zainstaluj uszkodzony program (lub lepiej poszukaj zamiennika pozbawionego takich „dodatków").

Instalacja programu

Wersję instalacyjną programu SpyBot Search & Destroy — jak zresztą również pakiety aktualizujące bazę informacji o modułach szpiegujących — znajdziesz w Internecie na stronie domowej programu. Aby się na niej znaleźć, wystarczy otworzyć okno przeglądarki internetowej i wpisać w pasku adresu *http://beam.to/spybotsd/*. Kliknięcie pola *Download*, znajdującego się w lewym panelu strony, przeniesie Cię na stronę podrzędną zawierającą listę elementów programu możliwych do pobrania z Sieci (rysunek 7.1).

Rysunek 7.1. *Strona domowa programu SpyBot Search & Destroy*

Odszukaj teraz na stronie pole zatytułowane *SpyBot – Search & Destroy 1.2*, po którego prawej stronie znajduje się duży przycisk *Download here*. Kliknij ten przycisk, a przeniesiesz się na stronę podrzędną serwisu umożliwiającą wybór najszybszego według Ciebie serwera (rysunek 7.2).



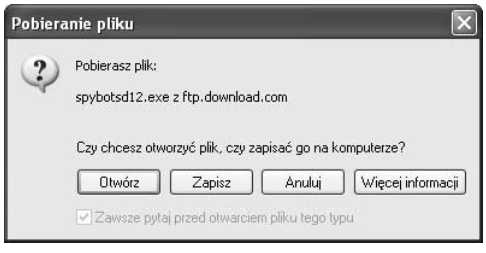
Rysunek 7.2. *Wybór serwera, który umożliwi najszybsze pobranie wersji instalacyjnej programu*

Niestety, za każdym razem lista wyświetlanych serwerów jest inna. Bez problemu powinieneś sobie poradzić z pobraniem pliku instalacyjnego pakietu SpyBot Search & Destroy i zapisaniem go na dysku twardym komputera; jeśli jednak potrzebujesz dokładnej instrukcji, odśwież kilkakrotnie stronę, aż na ekranie (na liście *Available Mirrors*) wyświetlona zostanie pozycja zatytułowana *Download.com*, a następnie kliknij przycisk *Download here* umieszczony po jej prawej stronie.

Po przejściu na stronę serwisu *Download.com* musisz jeszcze raz potwierdzić chęć pobrania programu. W tym celu kliknij odnośnik *Download Now* i poczekaj, aż rozpocznie się pobieranie pliku (rysunek 7.3).

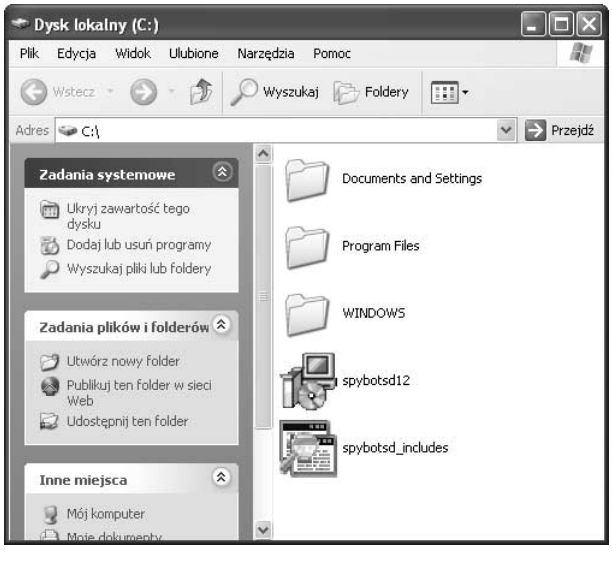
Rysunek 7.3. *Kliknięcie przycisku Download Now rozpocznie proces pobierania wersji instalacyjnej programu SpyBot Search & Destroy*

O poprawnym rozpoczęciu pobierania pliku z sieci poinformuje pojawienie się okna dialogowego *Pobieranie pliku* (rysunek 7.4). Kliknij w nim przycisk *Zapisz*, a następnie w oknie *Zapisywanie jako* wskaż folder, w którym umieszczony ma zostać plik instalacyjnej wersji programu. Zapisanie pobieranego programu na dysku twardym pozwoli wykorzystać wielokrotnie raz pobrany program — niezależnie od tego, czy zdecydujesz się ponownie instalować system operacyjny czy szukać modułów szpiegujących na innym komputerze połączonym z Twoim za pomocą sieci lokalnej.



Rysunek 7.4. *Kliknij przycisk Zapisz*

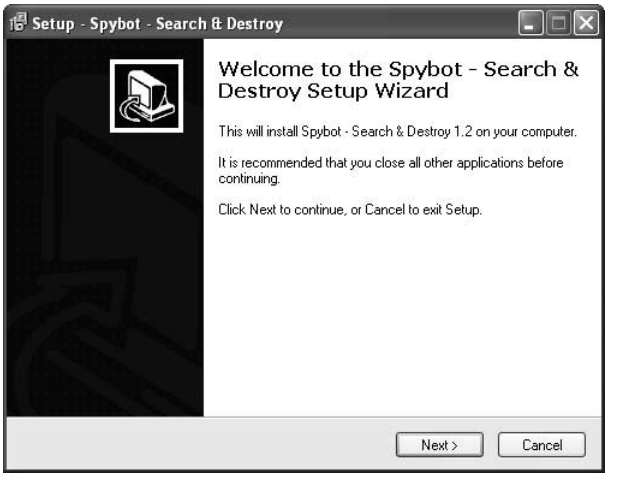
Poczekaj teraz, aż cały plik instalacyjny programu zostanie pobrany z sieci (o stopniu zaawansowania procesu pobierania pliku przeglądarka WWW będzie na bieżąco informować za pomocą okna dialogowego *Skopiowano*), a następnie przenieś się do folderu, w którym zapisałeś plik, i kliknij dwukrotnie jego ikonę, nazwaną najprawdopodobniej *spybotsd12* (rysunek 7.5). Uruchomisz w ten sposób program instalacyjny pakietu SpyBot Search & Destroy.



Rysunek 7.5. *Dwukrotnie kliknięcie ikony spybotsd12 rozpocznie instalację programu*

Nazwa *spybotsd12* dotyczy wersji 1.2 pakietu SpyBot Search & Destroy dostępnej w czasie pisania tej książki. Plik zawierający nowszą wersję instalacyjną — gdy tylko nowsza wersja programu zostanie opublikowana — może nosić inną nazwę.

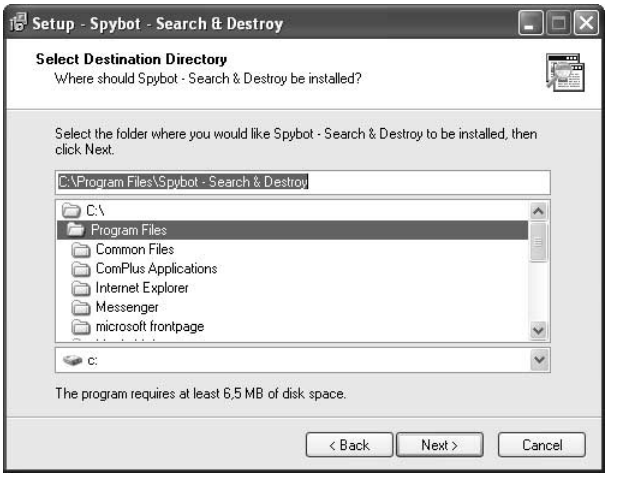
Pierwszą, powitalną planszę programu instalacyjnego możesz spokojnie pominąć, klikając przycisk *Next* (rysunek 7.6). W oknie pojawi się tekst umowy licencyjnej programu — przejrzyj go i, jeśli nie masz nic przeciwko jego postanowieniom, umieść znacznik w polu *I accept the agreement* i kliknij przycisk *Next*.



Rysunek 7.6. *Plansza powitalna programu instalacyjnego pakietu SpyBot Search & Destroy*

Jeszcze raz podkreślam: programu SpyBot Search & Destroy używasz na własną odpowiedzialność i jeśli nie będzie on działał poprawnie lub uniemożliwi Ci korzystanie z potrzebnych Ci programów, nie możesz nikogo za to winić.

Kolejna plansza programu instalacyjnego oferuje wybór folderu dysku twardego, w którym zainstalowany zostanie program (rysunek 7.7). Jeśli nie masz nic przeciwko domyślnej propozycji (*C:\Program Files\Spybot – Search & Destroy*), kliknij przycisk *Next*; jeśli jednak bardziej odpowiada Ci instalacja na innej partycji dysku twardego lub w innym folderze, dokonaj odpowiednich zmian w polach okna dialogowego i dopiero wtedy kliknij *Next*.

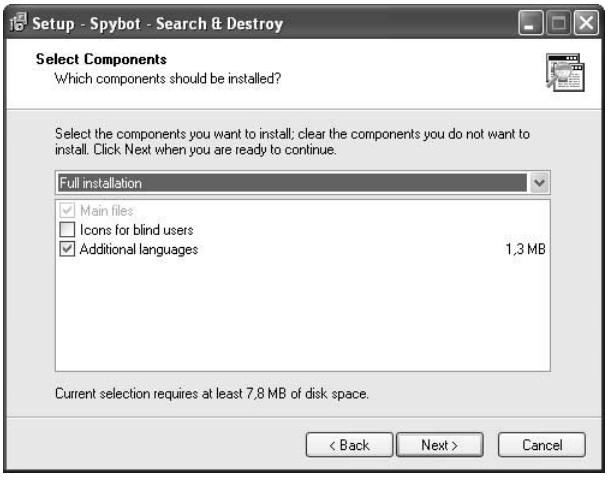


Rysunek 7.7. *Wybór folderu instalacyjnego programu*

Zapamiętaj nazwę folderu instalacyjnego programu SpyBot Search & Destroy — może być potrzebna w czasie aktualizowania bazy informacji o modułach szpiegujących.

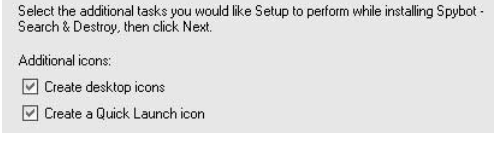
Program instalacyjny zaoferuje teraz wybór instalowanych modułów pakietu (rysunek 7.8). Jedyną dodatkową opcją, jaką możesz zainstalować, jest zestaw ikon dla osób słabo widzących (pozycja *Icons for blind users*), a jedynym modułem, z którego możesz zrezygnować, jest pakiet językowy (pozycja *Additional languages*), który jednak polecam pozostawić zaznaczony — w przeciwnym przypadku program będzie mógł się z Tobą porozumiewać wyłącznie po angielsku. Jak zwykle kliknij przycisk *Next*, aby kontynuować instalację.

Rysunek 7.8. *Lista instalowanych modułów programu*



Planszę wyboru nazwy folderu menu *Start*, w którym umieszczone zostaną ikony uruchamiające program, możesz bez problemów pominąć, klikając przycisk *Next*. Dojdziesz w ten sposób do wyboru dodatkowych miejsc, w których również mogą zostać umieszczone ikony uruchamiające program (rysunek 7.9). Znacznik umieszczony w polu *Create desktop icons* spowoduje utworzenie w czasie instalacji ikony umieszczonej na pulpicie systemu Windows, zaś znacznik w polu *Create a Quick Launch icon* spowoduje utworzenie ikony na pasku szybkiego uruchamiania.

Rysunek 7.9. *Dodatkowe opcje instalacji programu*



Opcje dotyczące ikon tworzonych na pulpicie oraz pasku szybkiego uruchamiania możesz bez problemów zmienić również po instalacji programu.

Klikając teraz *Next*, przejdziesz do ostatnich etapów instalacji programu: najpierw na ekranie wyświetlone zostanie podsumowanie wszystkich danych zebranych przez program instalacyjny, a gdy je zatwierdzisz — klikając przycisk *Install* — rozpocznie się

kopiowanie plików programu na dysk twardy Twojego komputera. W zależności od szybkości komputera potrwa to od kilkunastu sekund do kilku minut, a gdy instalacja zakończy się sukcesem, powiadomi Cię o tym ostatnia plansza instalatora (rysunek 7.10).

Rysunek 7.10. *Instalacja programu zakończyła się sukcesem!*

Kliknij przycisk *Finish*, by zamknąć okno programu instalacyjnego pakietu SpyBot Search & Destroy i powrócić do pulpitu systemu Windows. Program jest już gotowy do użycia, zanim jednak uruchomisz go, warto poświęcić jeszcze chwilę na zaktualizowanie bazy informacji o modułach szpiegujących, by już pierwsze skanowanie systemu było maksymalnie skuteczne.

Aktualizacja bazy informacji o modułach szpiegujących

Nowe moduły szpiegujące pojawiają się w Internecie co parę dni. Aby SpyBot Search & Destroy miał możliwość podjęcia z nimi równej walki, musisz dbać o regularne instalowanie aktualnej bazy danych zawierającej informacje o wszystkich poszukiwanych „zarazkach".

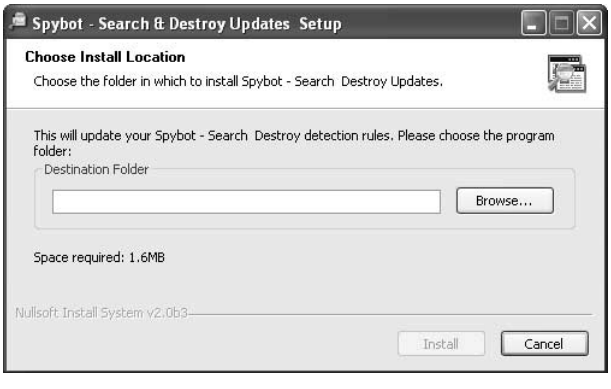
Aktualizacja bazy danych programu SpyBot Search & Destroy może przebiegać na dwa sposoby. W przypadku aktualizacji pojedynczej instalacji programu możesz skorzystać z wbudowanego modułu aktualizującego, wbudowanego w program. Metoda ta wymaga jednak za każdym razem aktywności połączenia internetowego, dlatego w przypadku aktualizowania większej liczby komputerów może bardziej Ci odpowiadać metoda polegająca na pobraniu z Internetu niewielkiego programu instalacyjnego, który aktualizuje zainstalowaną kopię programu niezależnie od tego, ile razy — i czy w ogóle — była ona aktualizowana od czasu instalacji. Mówiąc krótko, najnowsza wersja pakietu aktualizującego zawiera wszystkie poprawki wnoszone przez poprzednie aktualizacje — po świeżej instalacji programu SpyBot Search & Destroy musisz zatem pobrać z Sieci i zainstalować tylko najnowszy pakiet aktualizujący.

Pakiet aktualizujący, który zawiera również wszystkie poprzednie aktualizacje, nazywany jest w informatyce *kumulatywnym*. Przykładami kumulatywnego pakietu aktualizującego mogą być również pakiety ServicePack aktualizujące system Windows — aby zainstalować najnowszą wersję aktualizacji, nie trzeba instalować poprzednich wydań.

Aby pobrać pakiet aktualizujący, raz jeszcze udaj się na stronę domową programu SpyBot Search & Destroy, kliknij odnośnik *Download*, a następnie odszukaj pole zatytułowane *Detection updates*. Kliknięcie umieszczonego po jego prawej stronie przycisku *Download here* natychmiast rozpocznie proces pobierania na dysk twardy Twojego komputera pakietu aktualizującego.

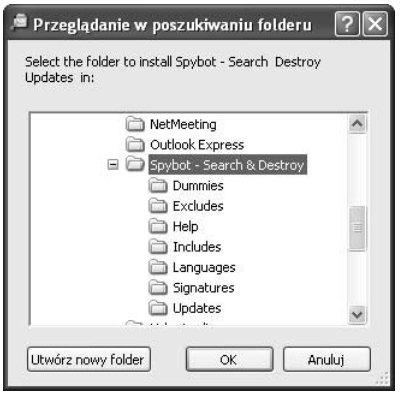
Gdy pobieranie pliku zakończy się sukcesem, odszukaj w folderze, w którym zapisywałeś plik aktualizujący, ikonę tego pliku; powinna nazywać się ona *spybotsd_includes*. Dwukrotne kliknięcie tej ikony otworzy okno programu instalującego zaktualizowaną bazę danych (rysunek 7.11).

Rysunek 7.11. *Pierwsza plansza programu aktualizującego bazę danych*

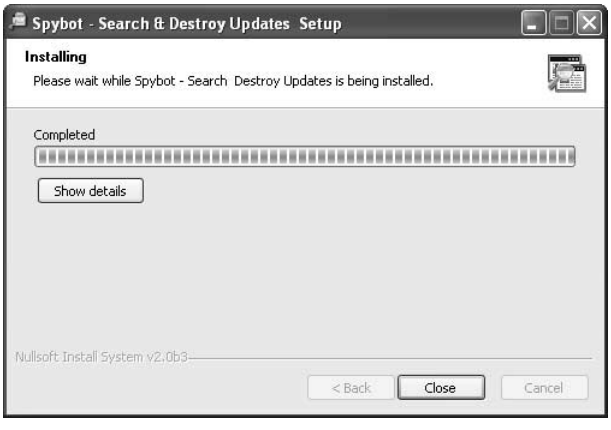


Aby program instalacyjny wiedział, gdzie zapisać zaktualizowaną bazę danych, musisz wskazać mu ulokowanie programu SpyBot Search & Destroy. W tym celu kliknij przycisk *Browse* — wywołując okno dialogowe *Przeglądanie w poszukiwaniu folderu* — i podświetl na liście dysków twardych i folderów ikonę folderu instalacyjnego programu (rysunek 7.12). Kliknięcie przycisku *OK* zatwierdzi wybór i zamknie okno dialogowe *Przeglądanie w poszukiwaniu folderu*.

Rysunek 7.12. *Aby zainstalować uaktualnienie bazy danych, musisz wskazać folder instalacyjny programu SpyBot Search & Destroy*

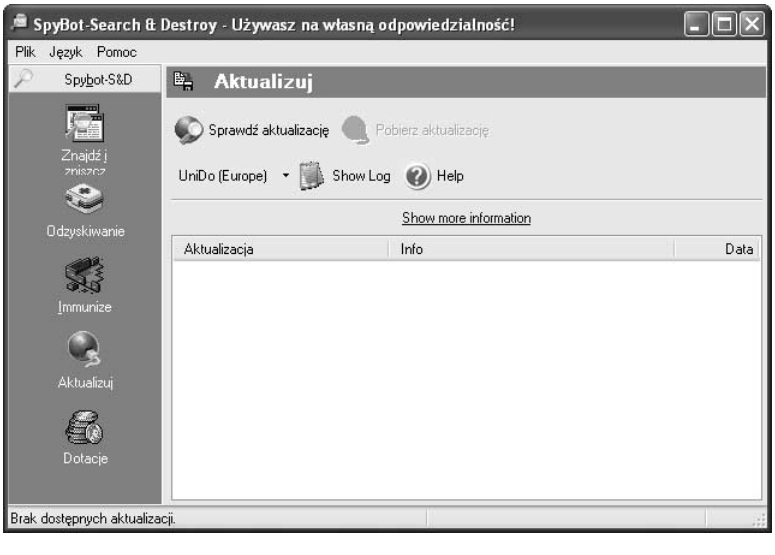


Klikając teraz przycisk *Install*, rozpoczniesz aktualizację bazy danych. Aktualizacja powinna potrwać tylko kilka lub kilkanaście sekund — gdy napis *Completed* poinformuje o jej pomyślnym zakończeniu, kliknij przycisk *Close* i uruchom zaktualizowaną wersję programu SpyBot Search & Destroy (rysunek 7.13).



Rysunek 7.13. *Aktualizacja bazy danych zakończyła się sukcesem!*

Jeśli wolisz przeprowadzić aktualizację pojedynczej instalacji programu, kliknij ikonę *Aktualizuj* wyświetlaną w lewym panelu okna, a następnie przycisk *Sprawdź aktualizację*, aby pobrać listę dostępnych aktualizacji (rysunek 7.14). Jeśli na ekranie pojawi się okno dialogowe z komunikatem *Brak dostępnych aktualizacji*, znaczy to, że dysponujesz możliwie najbardziej aktualną wersją programu; w przeciwnym razie na liście wyświetlanej wewnątrz okna programu znajdziesz wpisy odpowiadające zaktualizowanym modułom. Teraz wystarczy byś umieścił znaczniki w wierszach listy odpowiadających tym modułom, które chcesz zaktualizować, a następnie kliknął przycisk *Pobierz aktualizację* — program sam dokona aktualizacji i ponownie uruchomi się, aktywując nowe wersje modułów.



Rysunek 7.14. *Aktualizacja programu SpyBot Search & Destroy za pomocą wbudowanego modułu aktualizującego*

Uruchamianie programu

Aby uruchomić program SpyBot Search & Destroy, kliknij przycisk *Start* (otwierając w ten sposób panel *Start*), rozwiń menu *Wszystkie programy*, w menu podrzędnym rozwiń pozycję *Spybot – Search & Destroy*, a następnie kliknij jedną z dwóch pozycji menu:

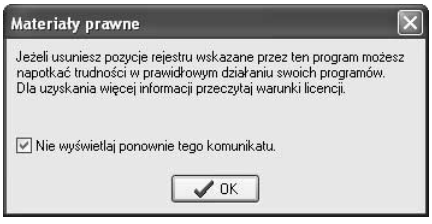
- *Spybot-S&D (easy mode)* — by uruchomić wersję programu udostępniającą tylko podstawowe, wystarczające w codziennym użyciu opcje i polecenia.
- *Spybot-S&D (advanced mode)* — by uruchomić pełną wersję programu udostępniającą wszystkie opcje i polecenia.

W czasie codziennej pracy możesz spokojnie korzystać z uproszczonej wersji programu — jest ona tak samo skuteczna jak wersja pełna. Uruchomienie wersji pełnej może być jednak potrzebne na przykład wtedy, gdy masz ochotę na dokonanie zmian w konfiguracji programu.

W czasie pierwszego uruchomienia program SpyBot Search & Destroy poprosi o wskazanie języka, w którym wyświetlane będą wszystkie komunikaty (rysunek 7.15). Kliknięcie pozycji *Polski* pozwoli delektować się polskimi komunikatami — przynajmniej w większości pól programu, gdyż, niestety, nie wszystkie jego elementy zostały przetłumaczone.

Rysunek 7.15. *Wybór języka, w którym porozumiewać się będzie program*

Zanim ujrzysz na ekranie główne okno programu, jeszcze raz przeczytasz, że programu SpyBot Search & Destroy używasz wyłącznie na własną odpowiedzialność i jeśli w efekcie „czyszczenia" systemu operacyjnego i usuwania zainstalowanych w nim modułów szpiegujących jakiś z używanych programów przestanie działać, jest to Twój problem i autor nie ponosi za to żadnej odpowiedzialności (rysunek 7.16). Aby komunikat ten nie pojawiał się ponownie, gdy będziesz uruchamiał program SpyBot Search & Destroy, umieść znacznik w polu *Nie wyświetlaj ponownie tego komunikatu* i dopiero wtedy kliknij przycisk *OK*.



Rysunek 7.16. *Program SpyBot Search & Destroy jeszcze raz przypomina, że używasz go na własną odpowiedzialność*

W ten sposób zakończyłeś proces instalowania i wstępnego konfigurowania programu, po chwili oczekiwania na ekranie pojawi się główne okno programu *SpyBot Search & Destroy* (rysunek 7.17).

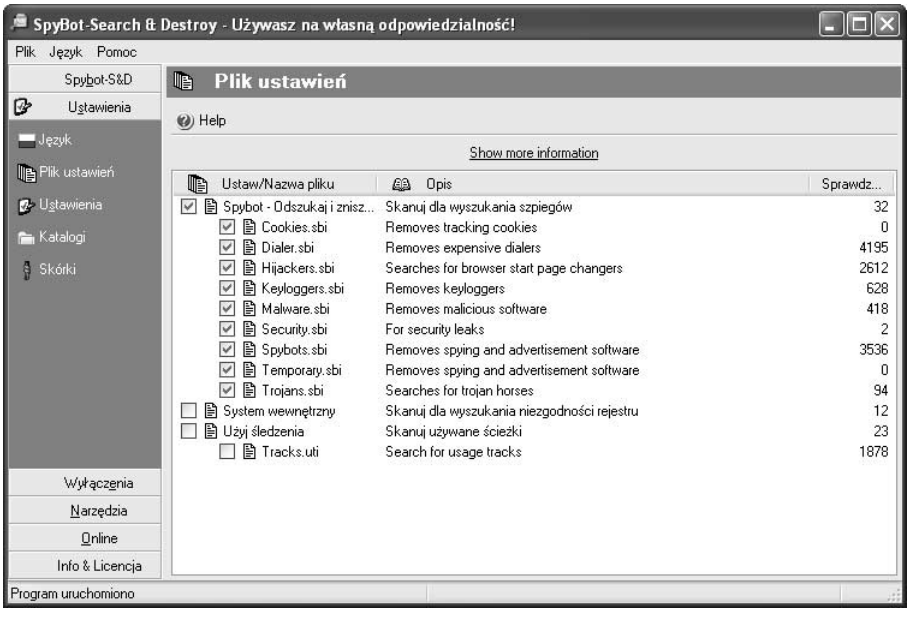
Rysunek 7.17. *Oto — nareszcie — główne okno programu SpyBot Search & Destroy*

Konfiguracja programu

SpyBot Search & Destroy to nie tylko skuteczne narzędzie usuwające moduły szpiegujące oraz wszystkie elementy systemu, które — choćby potencjalnie — naruszają Twoją prywatność. Jeden z modułów programu umożliwia również wyszukiwanie w rejestrze Windows wielu niespójności, które mogą być przyczyną wolniejszej i mniej stabilnej pracy systemu.

Aby wybrać aktywne moduły poszukujące nieprawidłowości, uruchom program w trybie zaawansowanym, klikając w menu *Start* pozycję *SpyBot-S&D (advanced mode)*. Gdy na ekranie pojawi się okno programu, w lewym panelu kliknij zakładkę *Ustawienia*, a następnie ikonę — *Plik ustawień* (rysunek 7.18).

Prezentowana w oknie programu lista odpowiada wszystkim dostępnym modułom pakietu SpyBot Search & Destroy. Standardowo włączone są tylko moduły znajdujące się w kategorii *Spybot – Odszukaj i zniszcz listy* — odpowiadają one za wyszukiwanie programów



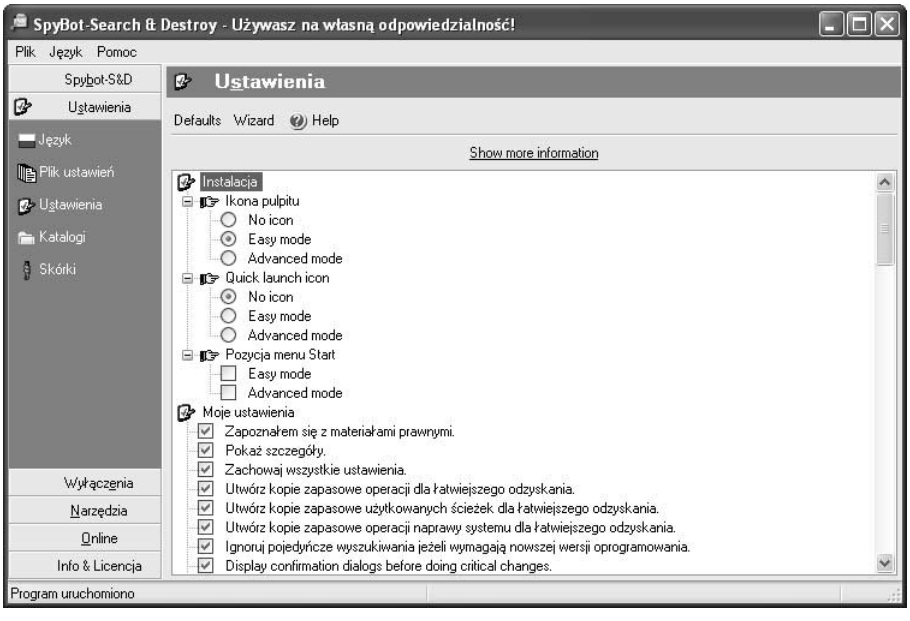
Rysunek 7.18. *Wybór aktywnych zestawów filtrów*

szpiegujących, niektórych dialerów oraz wpisów rejestru systemu Windows, które mogą naruszać Twoją prywatność. Trzy ostatnie elementy listy — *System wewnętrzny*, *Użyj śledzenia* oraz *Tracks.uti* — nie są zaznaczone. Jeśli je włączysz, następne skanowanie systemu pozwoli usunąć z rejestru wszystkie niespójności niepotrzebnie zwiększające obciążenie obliczeniowe komputera oraz zużycie pamięci operacyjnej (pozycja *System wewnętrzny*), a także wszelkie informacje umożliwiające odtworzenie Twoich działań na komputerze, takich jak lista otwieranych plików, odwiedzanych folderów czy przeglądanych stron WWW (pozycje *Użyj śledzenia* oraz *Tracks.uti*).

Pełne skanowanie systemu wraz z wyszukiwaniem w rejestrze systemu Windows potencjalnych niespójności może zająć sporo czasu i wykazać znacznie więcej błędów wymagających dokładnego, indywidualnego rozpatrzenia. Z tego powodu polecam wykonywać pełne skanowanie tylko okazjonalnie, podczas gdy standardowe poszukiwanie modułów szpiegujących — jak najczęściej.

Kolejna plansza — wywoływana kliknięciem ikony *Ustawienia* w lewym panelu okna — służy do dostosowania działania programu SpyBot Search & Destroy do Twoich potrzeb (rysunek 7.19). Oto najprzydatniejsze z dostępnych opcji.

- *Ikona pulpitu* — pozwala wyłączyć wyświetlanie ikony na pulpicie systemu Windows (pozycja *No icon*) lub za jej pomocą umożliwić uruchamianie programu SpyBot Search & Destroy w trybie podstawowym (pozycja *Easy mode*) lub zaawansowanym (pozycja *Advanced mode*).
- *Quick launch icon* — pozwala wyłączyć wyświetlanie ikony w pasku szybkiego uruchamiania systemu Windows (pozycja *No icon*) lub za jej pomocą umożliwić uruchamianie programu SpyBot Search & Destroy w trybie podstawowym (pozycja *Easy mode*) lub zaawansowanym (pozycja *Advanced mode*).



Rysunek 7.19. *Dodatkowe opcje konfiguracyjne programu SpyBot Search & Destroy*

- *Display confirmation dialogs before doing critical changes* — pozwala wyłączyć wyświetlanie okien dialogowych ostrzegających przed możliwymi skutkami niektórych operacji i dających możliwość anulowania danej czynności.
- *Wybierz dźwięk alarmu wykrytego szpiega* — uaktywnia dźwiękową sygnalizację wykrycia nowego modułu szpiegującego oraz umożliwia wybór odtwarzanego w takiej sytuacji pliku dźwiękowego.
- *Priorytety skanowania* — zmienia priorytet działania programu SpyBot Search & Destroy, co pozwala forsować skanowanie systemu kosztem szybkości działania pozostałych programów (pozycje *Wysoki* i *Najwyższy*) lub wręcz przeciwnie — spowolnić skanowanie, umożliwiając jednak w tym czasie wygodną pracę z komputerem (pozycje *Niski* lub *Najniższy*).

Odradzam stosowanie skrajnych priorytetów działania programu, a w szczególności priorytetu *Stan krytyczny*. Podwyższanie priorytetu programu SpyBot Search & Destroy nie zwiększy w jakiś magiczny sposób szybkości jego działania, lecz tylko ograniczy szybkość działania pozostałych uruchomionych w tym czasie programów. Najwyższa pozycja — *Stan krytyczny* — całkowicie zablokuje komputer na czas skanowania.

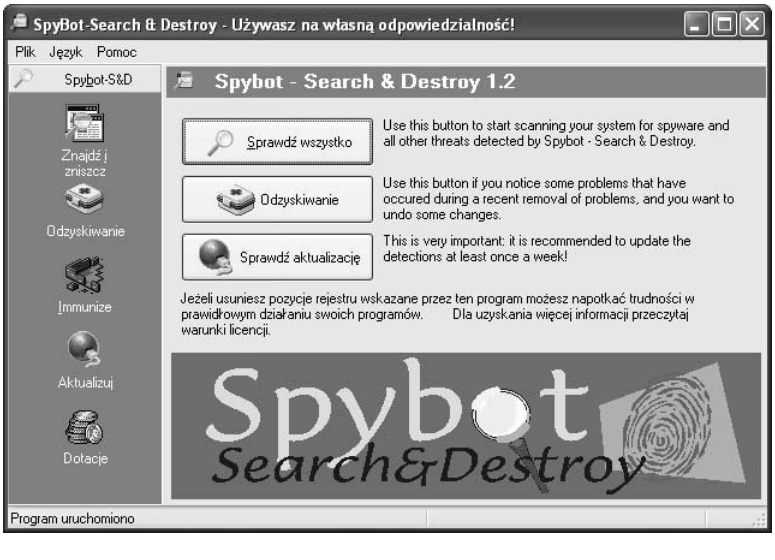
- *Ze startem programu: Pełne skanowanie systemu* — uaktywnia automatyczne rozpoczynanie pełnego skanowania systemu po każdym uruchomieniu programu SpyBot Search & Destroy.
- *Ze startem programu: Napraw wszystkie problemy* — uaktywnia automatyczne rozpoczynanie pełnego skanowania systemu wraz z naprawianiem wykrytych problemów po każdym uruchomieniu programu SpyBot Search & Destroy.

- *Ze startem programu: Ponowne sprawdzenie po usunięciu problemów* — uaktywnia opcję dwukrotnego automatycznego skanowania systemu, co pozwala wykryć odnowienie się infekcji na skutek zabezpieczeń wbudowanych w moduły szpiegujące.
- *Ze startem systemu: Automatycznie uruchamiaj program podczas startu systemu* — automatycznie uruchamia program SpyBot Search & Destroy w trakcie ładowania systemu operacyjnego, dzięki czemu możesz profilaktycznie przeskanować system zaraz po jego uruchomieniu.
- *Ze startem systemu: Uruchom program tylko raz przy następnym starcie systemu* — uaktywnia jednokrotne automatyczne uruchomienie programu SpyBot Search & Destroy w trakcie ładowania systemu operacyjnego, dzięki czemu program ma szansę usunąć moduły szpiegujące wyposażone w zabezpieczenia powodujące odnawianie się infekcji.

Jeśli program SpyBot Search & Destroy wykryje moduł szpiegujący wyposażony w takie zabezpieczenie, sam zaproponuje automatyczne uruchomienie programu podczas następnego ładowania systemu operacyjnego. W takim przypadku wydaj mu na to zgodę, po czym zamknij system operacyjny i ponownie uruchom komputer, by jak najszybciej pozbyć się infekcji.

Skanowanie systemu w poszukiwaniu modułów szpiegujących

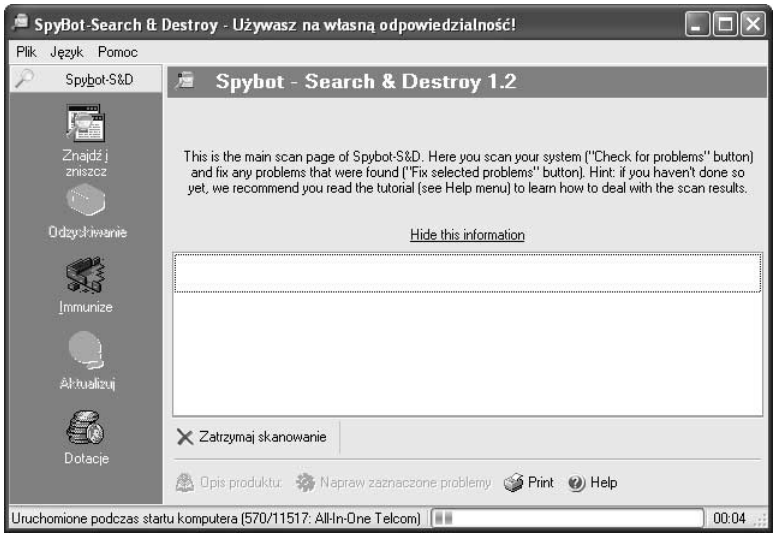
Nie ma chyba nic prostszego, niż rozpoczęcie skanowania systemu w poszukiwaniu modułów szpiegujących: uruchom program SpyBot Search & Destroy, poczekaj, aż na ekranie pojawi się jego plansza powitalna i kliknij przycisk *Sprawdź wszystko* (rysunek 7.20).



Rysunek 7.20. *Główne okno programu SpyBot Search & Destroy*

Skanowanie systemu przeprowadzaj po każdej instalacji nowego oprogramowania oraz każdym dłuższym przeglądaniu stron WWW. Tylko w ten sposób zminimalizujesz ryzyko zainstalowania się w systemie jakiegoś modułu szpiegującego.

Zawartość okna programu SpyBot Search & Destroy zmieni się, pokazując teraz listę zapełnianą powoli opisami znalezionych niebezpieczeństw (rysunek 7.21). Kliknięcie odnośnika *Hide this information* pozwoli Ci ukryć opis zawartości listy i przeznaczyć na nią prawie całą powierzchnię prawego panelu okna.

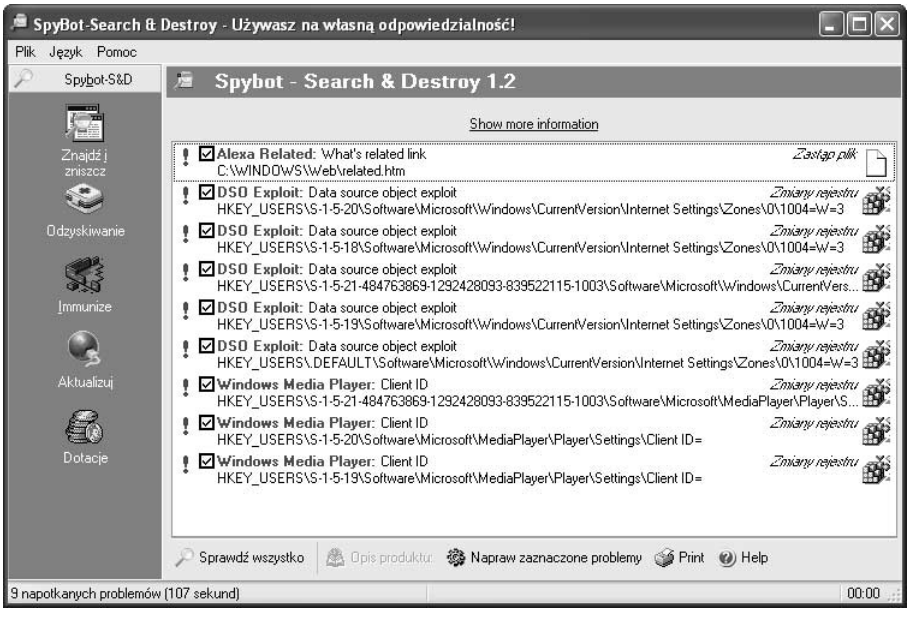


Rysunek 7.21. *Przeglądanie systemu w poszukiwaniu zainstalowanych modułów szpiegujących w toku*

Prawie każdy z paneli programu SpyBot Search & Destroy zawiera krótki opis swojej zawartości, który możesz ukryć — odzyskując używaną przez niego powierzchnię okna programu — klikając odnośnik *Hide this information*.

Na pasku statusu programu wyświetlany jest pasek postępu informujący o stopniu zaawansowania procesu przeszukiwania komputera. W zależności od wydajności komputera, wersji bazy danych programu SpyBot Search & Destroy oraz rozmiaru rejestru systemu Windows, operacja skanowania może trwać od kilku do kilkudziesięciu minut. Jeszcze w czasie jej trwania będziesz mógł ocenić stopień skażenia systemu modułami szpiegującymi; lista aktualizowana jest dynamicznie, a więc każdy odszukany element od razu się na niej pojawia.

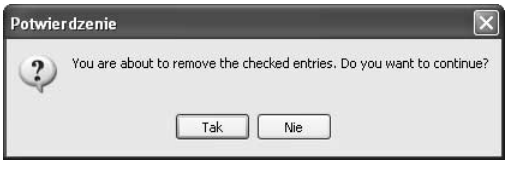
Gdy skanowanie się zakończy, na ekranie znajdować będzie się kompletna już lista niebezpiecznych programów oraz wpisów rejestru (rysunek 7.22). Twoim zadaniem jest teraz umieszczenie znaczników w wierszach odpowiadających elementom, które chcesz usunąć z systemu; przy tych najgroźniejszych — wyróżnionych czerwonymi wykrzyknikami — znaczniki zostaną umieszczone automatycznie, ręcznie będziesz musiał je postawić tylko przy pozycjach odpowiadających programom o wątpliwym przeznaczeniu.



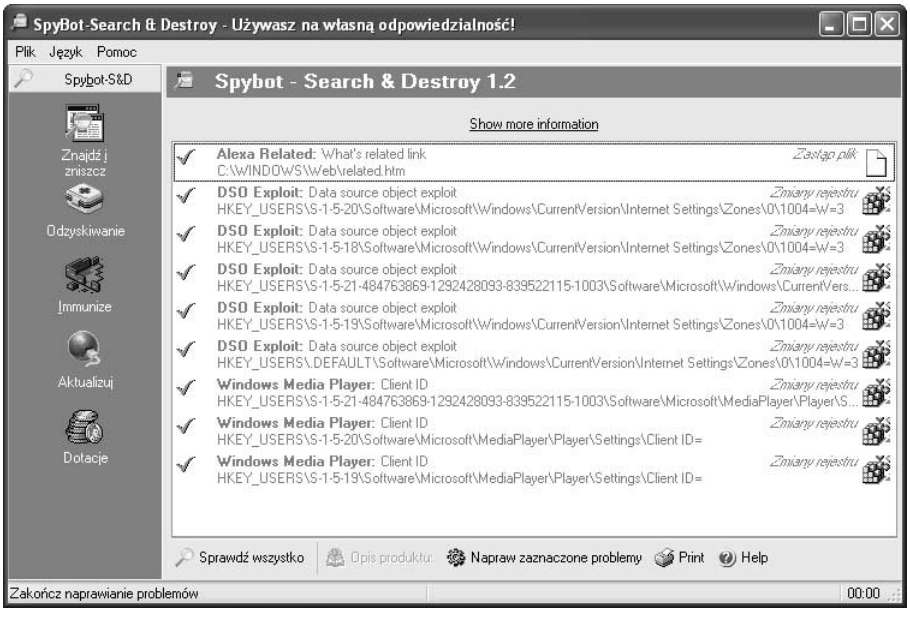
Rysunek 7.22. *Te wszystkie niebezpieczeństwa obecne są w dopiero co zainstalowanej kopii systemu Windows XP!*

Zaznaczyłeś już wszystkie pozycje, które chcesz usunąć? Kliknij zatem przycisk *Napraw zaznaczone problemy* i potwierdź chęć przeprowadzenia naprawy, klikając przycisk *Tak* w oknie dialogowym *Potwierdzenie* (rysunek 7.23). Po chwili oczekiwania — w tym czasie program SpyBot Search & Destroy będzie w możliwie najbezpieczniejszy sposób dezaktywował zaznaczone moduły — wszystkie pomyślnie unieszkodliwione pozycje listy zostaną wyróżnione zielonymi znacznikami (rysunek 7.24). Gratulacje!

Rysunek 7.23. *Program SpyBot Search & Destroy wymaga potwierdzenia operacji usuwania zaznaczonych elementów listy*



Lista zagrożeń znajdująca się na powyższych rysunkach wcale nie jest efektem instalowania niezliczonej liczby programów niewiadomego pochodzenia lub wielogodzinnego przeglądania pornograficznych stron WWW. Te wszystkie elementy instalowane są wraz z samym systemem Windows XP! Choć nie są to ściśle moduły szpiegujące, umożliwiają one stronom WWW uzyskanie dostępu do Twoich danych lub uzyskanie informacji na Twój temat.



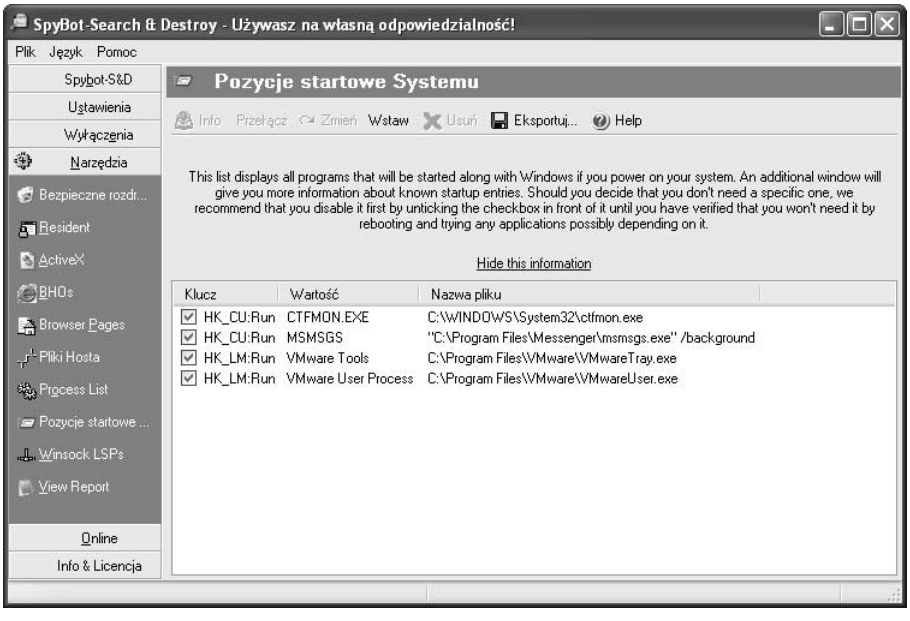
Rysunek 7.24. *Wszystkie zagrożenia zostały wyeliminowane*

Wyłączanie programów uruchamianych w czasie ładowania systemu operacyjnego

Z wieloma prostymi modułami szpiegującymi i dialerami — nawet jeśli nie są one jeszcze wykrywane przez program SpyBot Search & Destroy — możesz sobie poradzić samodzielnie. System operacyjny prowadzi listę programów, które uruchamiane są za każdym razem w czasie ładowania systemu do pamięci operacyjnej; do listy tej dopisują się bardzo często właśnie nowe moduły szpiegujące lub dialery. Wystarczy, byś regularnie sprawdzał tę listę, a natychmiast wykryjesz ewentualną infekcję — a może nawet będziesz w stanie jej zapobiec.

Listę automatycznie uruchamianych programów możesz wyświetlić choćby za pomocą jednego z modułów pakietu SpyBot Search & Destroy. Uruchom program w trybie zaawansowanym (klikając w menu *Start* pozycję *Spybot-S&D (advanced mode)*), w lewym panelu okna kliknij zakładkę *Narzędzia*, a następnie kliknij ikonę *Pozycje startowe Systemu* — na ekranie wyświetlona zostanie lista programów przeznaczonych do automatycznego startu (rysunek 7.25).

Aby wyłączyć teraz jeden z programów i uniemożliwić mu automatyczne uruchomienie się podczas następnego ładowania systemu, usuń znacznik z podejrzanego wiersza i uruchom ponownie system. Jeśli komputer nadal pracuje całkowicie normalnie i nie



Rysunek 7.25. *Lista programów uruchamianych automatycznie podczas ładowania systemu operacyjnego*

utraciłeś żadnej potrzebnej funkcji, najprawdopodobniej wyłączyłeś właściwy program; w przeciwnym przypadku jeszcze raz wyświetl listę automatycznie uruchamianych programów i przywróć znacznik w miejscu, z którego go usunąłeś.

Jak rozpoznać programy, które należy usunąć? Nie ma prostej odpowiedzi na takie pytanie. Doświadczeni użytkownicy systemu Windows wiedzą, które z programów potrzebne są do prawidłowej pracy systemu, i potrafią rozpoznać automatycznie uruchamiające się programy należące do zainstalowanych w komputerze „niegroźnych" pakietów oprogramowania. Jeśli nie jesteś jeszcze na takim etapie zaawansowania, pozostaje Ci jedynie uczyć się na błędach. Pomóc może regularne weryfikowanie listy automatycznie uruchamiających się programów; gdy zobaczysz jakąś nową pozycję i masz wątpliwości, czy należy ona do instalowanych przez Ciebie ostatnio aplikacji, będzie ona dobrym kandydatem do wyłączenia.