

IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK

DODAJ DO KOSZYKA

CENNIK I INFORMACJE

ZAMÓW INFORMACJE
O NOWOŚCIACH

ZAMÓW CENNIK

CZYTELNIA

FRAGMENTY KSIĄŻEK ONLINE

Internet. Jak surfować bezpiecznie

Autorzy: Maria Sokół, Radosław Sokół

ISBN: 83-7361-393-5

Format: B5, stron: 288



Internet jest jednym z największych fenomenów naszych czasów. Dostarcza nam informacji, pozwala poznać nowych ludzi, zapewnia rozrywkę i dostęp do wiedzy. Ma niestety również ciemną stronę – zagrożenia w postaci wirusów, programów szpiegujących, spamu i dostępu osób niepowołanych do naszych danych. Wszystkie te ataki są wynikiem błędów leżących zarówno po stronie systemów operacyjnych i protokołów sieciowych, jak i, niestety bardzo często, po stronie użytkowników komputerów. Szacuje się, że ponad połowa udanych ataków z sieci wynika z zaniedbań użytkowników komputerów. Tymczasem elementarne zabezpieczenie komputera nie wymaga wiedzy na poziomie informatycznego guru – wystarczy zainstalować i skonfigurować odpowiednie oprogramowanie.

Książka „Internet. Jak surfować bezpiecznie” to poradnik dla tych, którzy chcą korzystać z dobrodziejstw internetu bez obaw. Opisuje metody zabezpieczenia komputera przed największymi niebezpieczeństwami związanymi z korzystaniem z sieci – wirusami, programami szpiegującymi, atakami hakerów oraz przechwytywaniem informacji przesyłanych pocztą elektroniczną i wpisywanych w formularzach na stronach WWW. Przedstawia sposoby konfiguracji oprogramowania chroniącego komputer, usuwania wirusów i niepożądanych plików. Książka zawiera również informacje dotyczące bezpiecznego korzystania z zasobów sieci.

- Rodzaje zagrożeń
- Zapora sieciowa systemu Windows i inne aplikacje realizujące funkcje firewalla
- Rodzaje wirusów
- Usuwanie dialerów za pomocą edycji rejestru systemowego
- Instalacja i konfiguracja programu Norton AntiVirus 2005
- Wyszukiwanie i usuwanie programów szpiegujących
- Zabezpieczanie przeglądarki Internet Explorer
- Alternatywne rozwiązanie – Mozilla Firefox
- Bezpieczne korzystanie z poczty elektronicznej i ochrona przed spamem

Jeśli chcesz, aby Twój komputer i dane były bezpieczne, przeczytaj tę książkę i wykorzystaj zawarte w niej informacje.

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



Spis treści

Wstęp	7
Rozdział 1. Co grozi komputerom w internecie?.....	9
Kto reaguje na zagrożenia?	10
Włamania	12
Przepełnianie buforów	13
Oszuści internetowi	14
Rodzaje zagrożeń związanych z funkcjonowaniem sieci i podłączeniem do internetu ...	15
Kim jest cracker?	15
Kim jest haker?	16
Co to jest sniffing?	16
Co to jest spoofing?.....	17
Czy hijacking jest groźny?	17
Co to jest blokada usług?	17
Czy wirus komputerowy ma coś wspólnego ze zwykłym wirusem?.....	19
Jak działają moduły szpiegujące?.....	21
Dialery	22
Czy istnieją aplikacje agresywne?.....	23
Czy cookies są niebezpieczne?.....	23
Dlaczego należy ograniczać innym dostęp do własnego komputera?	25
Co może program monitorujący?	25
Co to jest spam?	25
Błędy w aplikacjach	27
Czy przestępstwa komputerowe są karalne?	27
Jak się bronić?	28
Jak zabezpieczyć komputer przed infekcją?.....	28
Czy program antywirusowy jest pewnym zabezpieczeniem?	30
Jak chronić hasło?	31
Bezpieczeństwo kart kredytowych	32
Podpis elektroniczny	33
Jak zadbać o bezpieczeństwo dzieci w internecie?	34
Najważniejsze informacje	36
Rozdział 2. „Mury obronne” komputera	39
Jak i czym „załatać” system Windows?	40
Po co aktualizować system Windows?	48
W jaki sposób pobierane są aktualizacje?	48
Jak skonfigurować automatyczną aktualizację systemu?	48

Kiedy korzystać z ręcznego trybu aktualizacji systemu?	51
Gdzie szukać zapory połączenia sieciowego w Windows XP i jak ją włączyć?	58
Czy mogę zezwalać Zaporze systemu Windows na odblokowanie niektórych połączeń?	59
Czy zapora ochroni mój komputer w obcej sieci?	60
Czy blokować pakiety polecenia ping?	62
Jak rejestrować próby połączeń?	64
Jak rozdzielić połączenie sieciowe na dwa komputery?	67
Jak dostosować przeglądarkę do współużytkowanego połączenia internetowego?	68
Czy istnieją inne zapory sieciowe?	69
Agnitum Outpost Firewall	70
Najważniejsze informacje	89
Rozdział 3. Strzeż się wirusów	91
Wirusy	91
Jakie są typy wirusów?	92
Czy wirusy to wymysł ostatnich lat?	94
Na co zwracać uwagę, aby nie zainstalować konia trojańskiego?	96
Jak reagować na fałszywki?	97
Co to są robaki komputerowe?	97
Gdzie mogę znaleźć zwięzłą informację o najnowszych wirusach i robakach?	98
Jak zapobiegać infekcji wirusowej?	99
Jak komputer ulega infekcji?	101
Jakie są objawy infekcji wirusowej komputera?	102
Jaki może być skutek infekcji?	103
Czy wirus może zarazić program na zabezpieczonej przed zapisem dyskiecie?	103
Co zrobić, gdy komputer „złapał” wirusa?	104
Jak działa program antywirusowy?	104
Jak walczyć z dialerami?	105
Jak instalują się dialery?	105
Jakie są pierwsze objawy obecności dialera?	105
Jak wysledzić i usunąć dialera?	106
Jak zapobiegać dialerom?	112
Czy istnieje oprogramowanie chroniące przed dialerami?	114
Czy mks_vir potrafi usuwać dialery?	120
Czy muszę płacić rachunek za połączenia realizowane przez dialera?	121
Najważniejsze informacje	121
Rozdział 4. Krótki przegląd programów antywirusowych	125
Internetowy skaner mks_vir	125
Jak uruchomić skaner mks_vir?	126
Jak zaktualizować bazę danych skanera mks_vir?	127
Jak szukać wirusów za pomocą programu mks_vir?	129
Jak postępować z wirusami znalezionymi za pomocą programu mks_vir?	132
Norton AntiVirus 2005	133
Jak zainstalować program antywirusowy Norton AntiVirus 2005	134
Jak przygotować pakiet Norton AntiVirus do pracy?	138
Jakie są funkcje pakietu Norton AntiVirus?	144
Kiedy i jak aktualizować pakiet Norton AntiVirus?	169
Jak wyłączyć i włączyć aktywny skaner antywirusowy?	170
Jak przeskanować system w poszukiwaniu wirusa?	171
Jak działa aktywny skaner antywirusowy?	174
Czy Norton AntiVirus kontroluje pocztę?	175
Do czego może się przydać magazyn kwarantanny?	176
Gdzie można znaleźć pełną informację o wykrytych wirusach?	178
Najważniejsze informacje	179

Rozdział 5. Jak pozbyć się szpiegów?	181
SpyBot Search & Destroy	181
Jak zainstalować program SpyBot Search & Destroy?	182
Jak przygotować program do pracy?	187
Jak zaktualizować program SpyBot Search & Destroy?	187
Jak sterować działaniem programu SpyBot Search & Destroy?	192
Jak szukać modułów szpiegujących?	195
Jak wyłączyć niebezpieczny program, który uruchamia się wraz z systemem operacyjnym?	197
Ad-Aware	199
Jak instalować Ad-Aware?	199
Jak aktualizować plik Ad-Aware?	204
Jak skanować komputer za pomocą programu Ad-Aware?	208
Najważniejsze informacje	214
Rozdział 6. Bezpieczne przeglądanie stron WWW	215
Jakie przeglądarki?	215
Co to jest przeglądarka?	215
Przeglądarki — najczęściej zadawane pytania (FAQ)	216
Jak naprawić przeglądarkę Internet Explorer?	219
Firefox — rozwiązanie dla ostrożnych	221
Jak instalować przeglądarkę Firefox?	222
Jak obsługiwać przeglądarkę Firefox?	226
Jak zdefiniować nową stronę główną?	229
Co nowego w przeglądarce Firefox?	230
Jak tworzyć zakładki?	238
Firefox i pliki cookie	240
Jak w przeglądarce Firefox blokować dodatkowe, „wyskakujące” okienka?	244
Jak w przeglądarce Firefox kontrolować wykonywanie skryptów JavaScript?	245
Jak w przeglądarce Firefox zablokować banery reklamowe?	246
Najważniejsze informacje	248
Rozdział 7. Bezpieczna poczta e-mail	249
Jak walczyć ze spamem?	249
Jakie są metody zapobiegania spamowi?	249
Jak bronić się przed wirusami rozpowszechnianymi w poczcie e-mail?	251
Thunderbird 1.0	252
Jak zainstalować program pocztowy Thunderbird 1.0?	253
Jak w programie Thunderbird skonfigurować filtr antyspamowy?	256
Jak w programie Thunderbird obsługiwać obrazki?	262
Najważniejsze informacje	264
Dodatek A Słowniczek terminów i pojęć	265
Skorowidz	279

Rozdział 5.

Jak pozbyć się szpiegów?

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, zbierając 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 modulem 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.

W sieci znajdziesz dwa bezpłatne narzędzia, które pozwolą Ci rozprawić się ze szpiegami na Twoim komputerze. To programy SpyBot Search & Destroy i Ad-Aware — warto je oba zainstalować, ponieważ mają uzupełniające się nawzajem bazy rozpoznawanego oprogramowania szpiegowskiego.

SpyBot Search & Destroy

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.

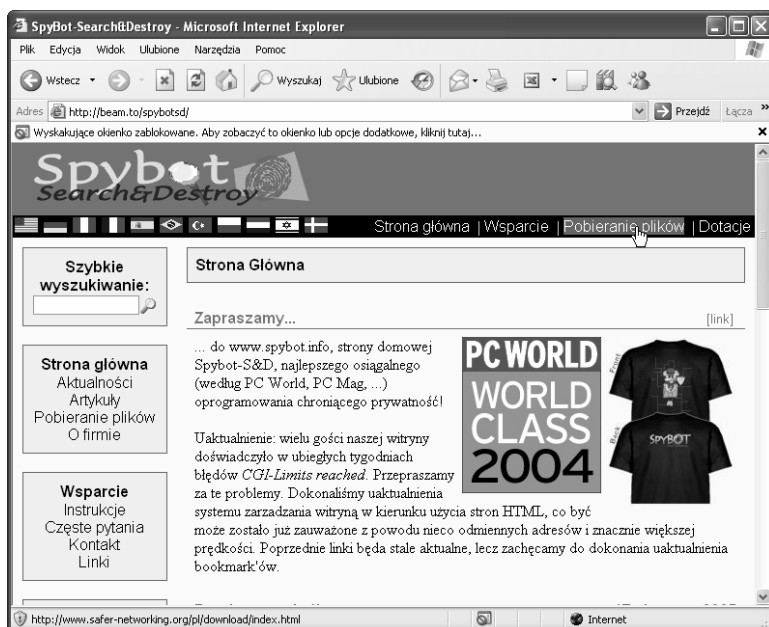
Pamiętaj, że program instalujesz i korzystasz z niego wyłącznie na własną odpowiedzialność. Jeśli któryś z Twoich programów wymaga do poprawnego działania modułu szpiegującego, a program SpyBot usunie go, uniemożliwiając uruchomienie tej aplikacji, nie wini autora, tylko ponownie zainstaluj uszkodzony program (lub lepiej poszukaj zamiennika pozbawionego takich „dodatków”).

Jak zainstalować program SpyBot Search & Destroy?

Aby zainstalować program:

1. Otwórz okno przeglądarki i przejdź do strony domowej programu:
<http://beam.to/spybotsd/>.
2. Znajdziesz tu wersję instalacyjną programu SpyBot Search & Destroy, jak zresztą również pakiety aktualizujące bazę informacji o modułach szpiegujących.
3. Kliknięcie pola *Pobieranie plików*, znajdującego się w lewym panelu strony, przeniesie Cię na stronę podrzędną zawierającą listę elementów programu możliwych do pobrania z sieci (rysunek 5.1).

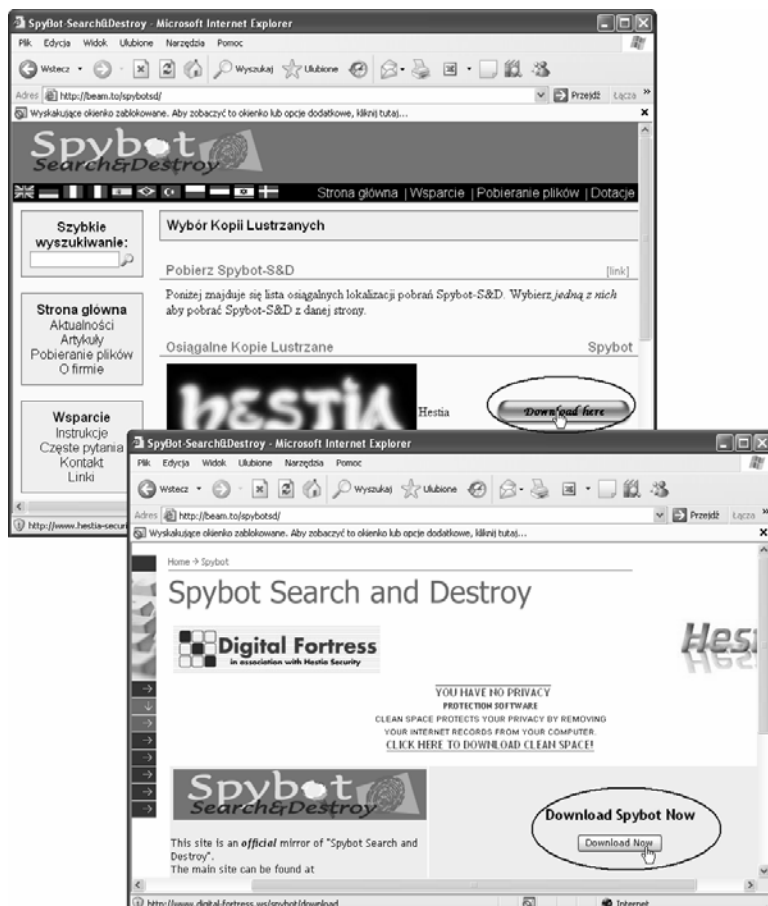
Rysunek 5.1.
Strona domowa programu SpyBot Search & Destroy



4. Odszukaj teraz na stronie pole zatytułowane *SpyBot — Search & Destroy 1.3*, 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. Niestety za każdym razem lista wyświetlanych serwerów jest inna i czasami konieczne jest odwiedzenie kilku stron, aby dotrzeć do programu. Gdy wreszcie klikniesz przycisk *Download Now*, rozpocznie się pobieranie pliku (rysunek 5.2).

Rysunek 5.2.

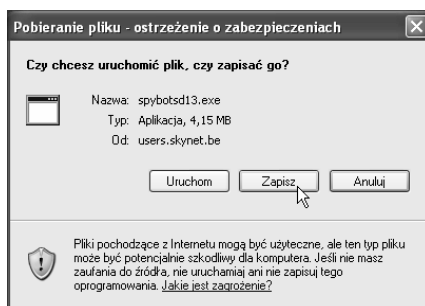
*Wybór serwera, który umożliwi najszybsze pobranie wersji instalacyjnej programu. Kliknij *Download Now*, aby pobrać plik*



5. Bez problemu jednak powinieneś sobie poradzić z pobraniem pliku instalacyjnego pakietu SpyBot Search & Destroy i zapisaniem go na dysku twardym komputera. O poprawnym rozpoczęciu pobierania pliku z sieci poinformuje pojawienie się okna dialogowego *Pobieranie pliku*. Kliknij w nim przycisk *Zapisz* (Rysunek 5.3), a następnie w oknie *Zapisywanie jako* wskaż folder, w którym umieszczony zostać plik instalacyjnej wersji programu.

Rysunek 5.3.

Rozpoczyna się proces pobierania wersji instalacyjnej programu SpyBot Search & Destroy

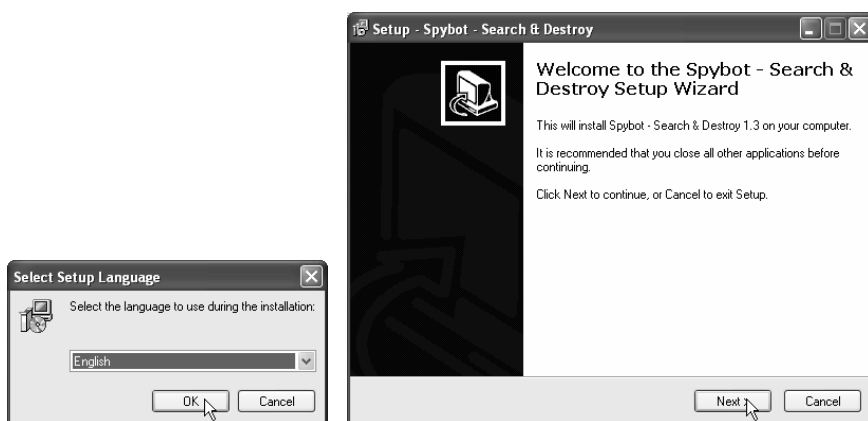


6. Poczekaj teraz, aż cały plik instalacyjny programu zostanie pobrany z sieci (o stopniu zaawansowania procesu pobierania pliku przeglądarka WWW będzie na bieżąco informować za pomocą okna dialogowego *Skopiowano*), a następnie przenieś się do folderu, w którym zapisałeś plik, i kliknij dwukrotnie jego ikonę, nazwaną najprawdopodobniej *spybotsd13* (rysunek 5.4). Uruchomisz w ten sposób program instalacyjny pakietu SpyBot Search & Destroy.



Rysunek 5.4. Dwukrotnie kliknięcie ikony *spybotsd13* rozpocznie instalację programu; numer na końcu nazwy pliku oznacza numer wersji programu

7. Najpierw pojawi się okno wyboru języka stosowanego w czasie instalacji — niestety nie ma tu języka polskiego, pozostaje więc angielski (język polski jest natomiast dostępny w opcjach konfiguracyjnych programu). Pierwszą, powitalną planszę programu instalacyjnego możesz pominąć, klikając przycisk *Next* (rysunek 5.5).

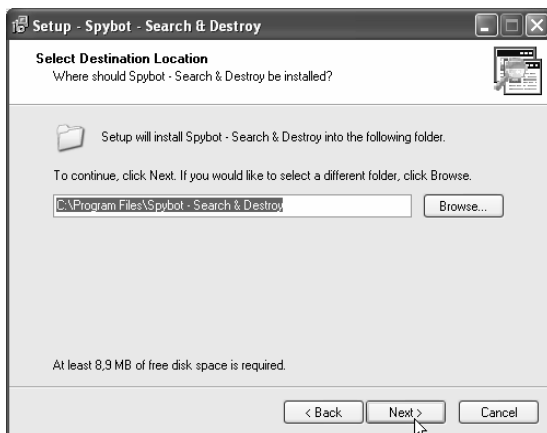


Rysunek 5.5. Wybór języka i plansza powitalna programu instalacyjnego pakietu SpyBot Search & Destroy

8. W oknie pojawi się tekst umowy licencyjnej programu — przejrzyj go i, jeśli nie masz nic przeciwko jej postanowieniom, umieść znacznik w polu *I accept the agreement* i kliknij przycisk *Next*.

9. Kolejna plansza programu instalacyjnego oferuje wybór folderu dysku twardego, w którym zainstalowany zostanie program (rysunek 5.6). 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*.

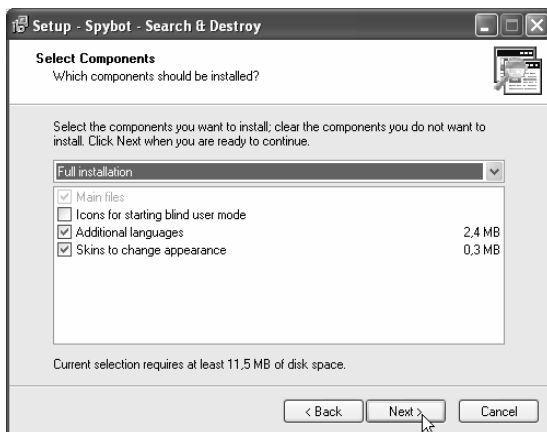
Rysunek 5.6.
*Wybór folderu
instalacyjnego
programu*



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

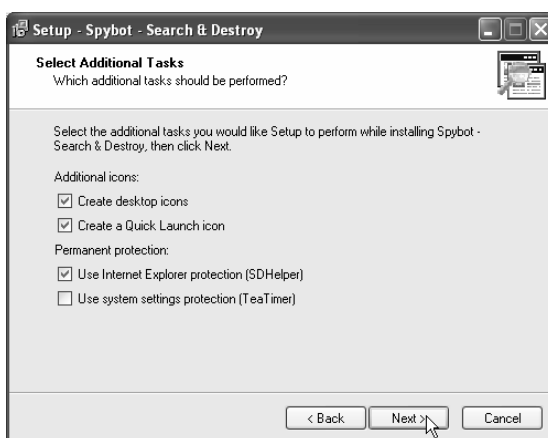
10. Program instalacyjny zaoferuje teraz wybór instalowanych modułów pakietu (rysunek 5.7). Jediną dodatkową opcją, jaką możesz zainstalować, jest zestaw ikon dla osób słabo widzących (pozycja *Icons for blind users*), a moduły, z których możesz zrezygnować, to pakiet językowy (pozycja *Additional languages*), który jednak warto pozostawić zaznaczony — w przeciwnym przypadku program będzie mógł się z Tobą porozumiewać wyłącznie po angielsku — oraz nowe „skórki” (pozycja *Skins to change appearance*). Jak zwykle kliknij przycisk *Next*, aby kontynuować instalację.

Rysunek 5.7.
*Lista instalowanych
modułów programu*



11. Kliknij przycisk *Next* w następnym oknie, które umożliwia wybór nazwy folderu menu *Start*, w którym umieszczone zostaną ikony uruchamiające program.
12. Dojdiesz w ten sposób do wyboru dodatkowych miejsc, w których również mogą zostać umieszczone ikony uruchamiające program. Możesz także włączyć stałą ochronę przeglądarki Internet Explorer (pole *Use Internet Explorer Protection (SDHelper)*) oraz ochronę ustawień systemu (pole *Use system settings protection (Tea Time)*) — rysunek 5.8. 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 5.8.
*Dodatkowe opcje
instalacji programu*

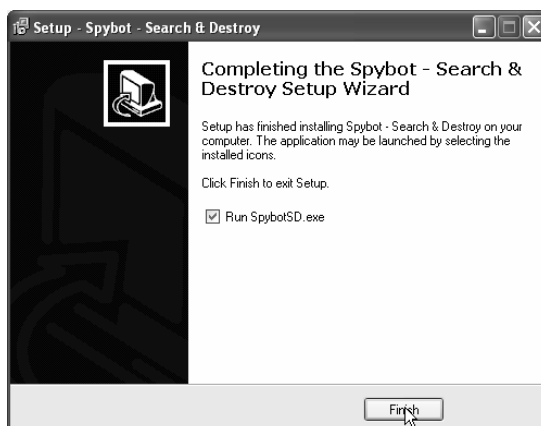


Opcje dotyczące ikon tworzonych na pulpicie oraz pasku szybkiego uruchamiania możesz bez problemów zmienić również po instalacji programu.

13. 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 5.9).
14. 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.

Rysunek 5.9.

Instalacja programu
zakończyła się
sukcesem!



Jak przygotować program do pracy?

Po zainstalowaniu programu SpyBot Search & Destroy wyświetli okno kreatora, który poprowadzi Cię przez resztę procesu instalacji. Kolejne kroki nie są bezwzględnie konieczne.

Aby dokończyć instalację programu i przygotować go do pracy:

1. W oknie SpyBot S&D Wizard kliknij przycisk *Next*. Możesz także utworzyć kopię *Rejestru*, klikając *Create registry backup*. W kolejnych oknach także klikaj przycisk *Next*, a w ostatnim kliknij przycisk *Start using the program* (rysunek 5.10).
2. Na ekranie pojawi się okno programu SpyBot Search & Destroy (rysunek 5.11).

Jak skonfigurować polski interfejs programu SpyBot Search & Destroy?

SpyBot Search & Destroy może komunikować się z Tobą w języku polskim.

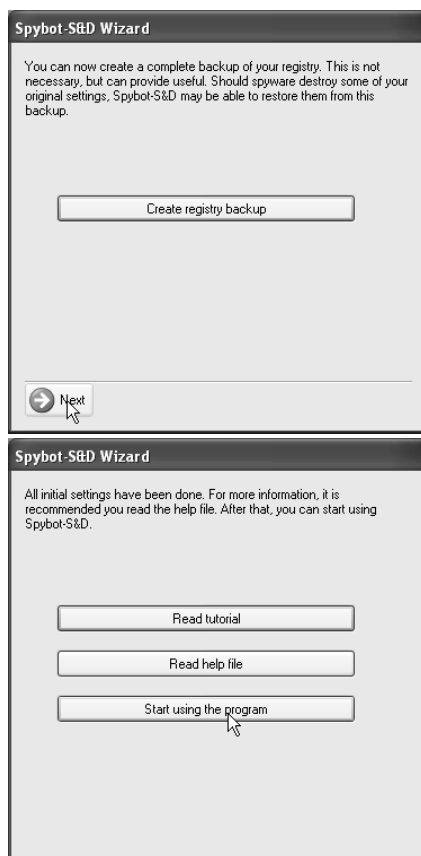
- ♦ Kliknij menu *Language* i wybierz w nim język *Polski*. Teraz polecenia i opisy funkcji są wyświetlane w języku polskim (rysunek 5.12).

Jak zaktualizować program SpyBot Search & Destroy?

Nowe moduły szpiegujące pojawiają się w internecie co parę dni. Aby program SpyBot Search & Destroy miał możliwość podjęcia z nimi równej walki, powinieneś dbać o regularne instalowanie aktualnej bazy danych zawierającej informacje o wszystkich poszukiwanych „zarazkach”. Skorzystaj z modułu aktualizującego, wbudowanego w program. Procedura aktualizacji wymaga nawiązania połączenia z internetem.

Rysunek 5.10.

*Klikaj przycisk
Next, aby dotrzeć
do ostatniego
z okien kreatora
— tu kliknij Start
using the program*

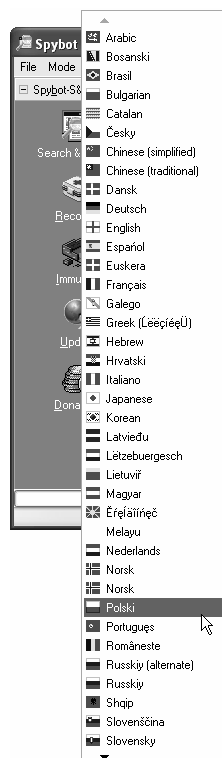
**Rysunek 5.11.**

*Główne okno
programu Spybot
— Search & Destroy*



Rysunek 5.12.

Wybierz język polski z menu Language, aby program miał polski interfejs

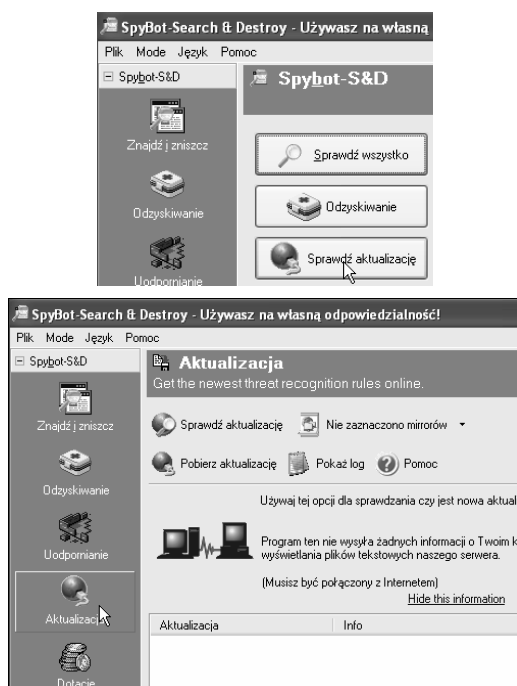


Aby przeprowadzić aktualizację bazy modułów szpiegujących programu SpyBot Search & Destroy:

1. Kliknij w głównym oknie programu przycisk *Sprawdź aktualizację* lub kliknij w panelu z lewej strony przycisk *Aktualizacja*, a następnie kliknij odnośnik *Sprawdź aktualizację* w panelu po prawej (rysunek 5.13).

Rysunek 5.13.

*Oto dwa sposoby
aktywowania procesu
aktualizacji*

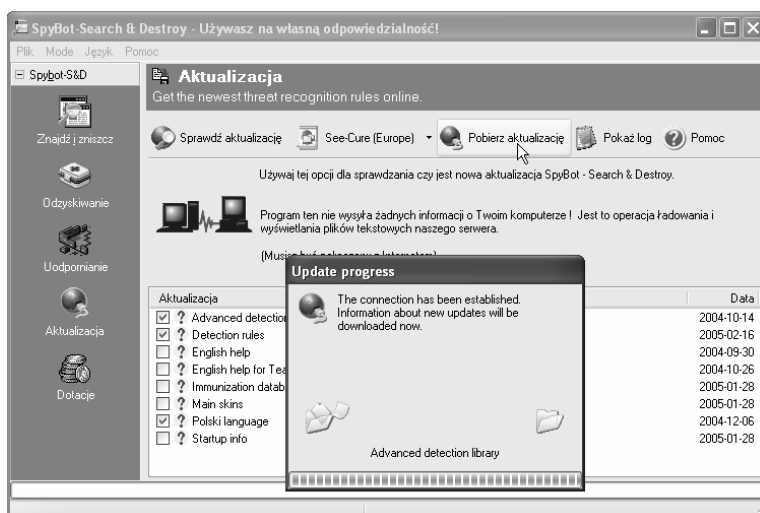


Zawsze możesz powrócić do głównego okna, klikając w panelu z lewej strony okna przycisk Spybot-S&D

2. Program sprawdzi w internecie, czy pojawiły się zaktualizowane moduły, i wyświetli ich listę w oknie programu. Umieść znaczniki w polach wyboru obok pozycji, które chcesz zaktualizować, i kliknij przycisk *Pobierz aktualizacje* (rysunek 5.14).

Rysunek 5.14.

*Po naciśnięciu
przycisku Pobierz
aktualizacje program
przystąpi do
realizacji zadania*





Może się zdarzyć, że domyślny serwer udostępniający aktualizacje programu nie będzie dostępny. Kliknij wówczas przycisk oznaczony jego nazwą, wybierz inny serwer i powtórz aktualizację (rysunek 5.15).

Rysunek 5.15.

Jeśli pliki nie są aktualizowane, a w kolumnie Info okna aktualizacji pojawia się komunikat !!!Bad checksum!, zmień serwer



- Po wykonaniu operacji w oknie *Aktualizacja* zaktualizowany element zostanie oznaczony ikoną ✓ (rysunek 5.16).

Rysunek 5.16.

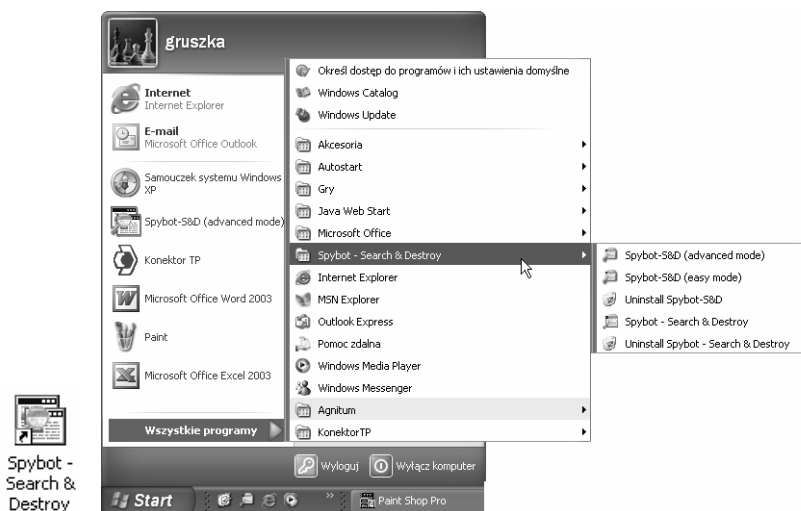
Zaktualizowany element oznaczony jest ikoną ✓

Aktualizacja	Info
☐ ? English help	English help file (178 KB)
☐ ? English help for TeaTimer	English help file for TeaTimer add-on (34 KB)
☒ ✓ Immunization database	Updated Immunization database (57 KB)
☐ ? Main skins	New skin for colorblind people (393 B)
☐ ? Startup info	Updated startup entry descriptions (354 KB)

- Możesz zamknąć okno programu.



Aby uruchomić program SpyBot Search & Destroy, kliknij dwukrotnie ikonę programu na pulpicie lub skorzystaj z menu *Start* (rysunek 5.17).



Rysunek 5.17. Aby uruchomić program SpyBot Search & Destroy, kliknij dwukrotnie ikonę programu na pulpicie lub skorzystaj z menu *Start*