INSTRUKCJA UŻYTKOWNIKA

Wydanie: 1.0 ©2001

SPIS TREŚCI

WSTĘP

Doctor Web dla Windows 95-2000 należy do nowej, 32-bitowej generacji antywirusowych skanerów Doctor Web (lub DrWeb). Nowa linia produktów (DrWeb32) zawiera również wersje dla systemów Novell NetWare, OS/2 oraz DOS/386.
Program jest przeznaczony dla 32-bitowych systemów Windows (na przykład Windows 9x/Me/NT/2000) i nazywany jest Dr.Web dla Win'9x/NT/2000 lub w skrócie DrWeb32W.
Wersja ta oferuje dwa mechanizmy obsługi: przy użyciu interfejsu graficznego (DrWeb32W) oraz przy użyciu linii poleceń (DrWebWCL). Oba warianty obsługują te same opcje linii komend. DrWeb32W (wersja graficzna), może być również kontrolowana i konfigurowana poprzez panele dialogowe, co jest zazwyczaj znacznie wygodniejsze. Jednak z drugiej strony, DrWebWCL (wersja korzystająca z linii poleceń) wymaga znacznie mniejszej ilości zasobów systemowych.

Oba programy korzystają z tego samego pliku konfiguracyjnego i z tych samych ustawień. Możesz alternatywnie używać tych dwóch wariantów, w zależności od tego, który z nich jest bardziej odpowiedni w danej chwili.

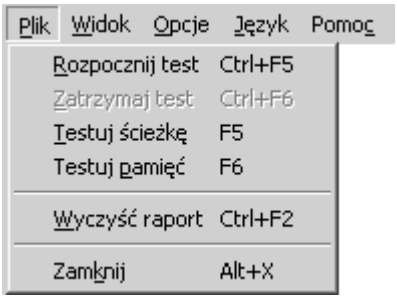
Pakiet Doctor Web dla Windows 95-2000 zawiera program SpIDer Guard dla Windows 9x/Me (lub w skrócie, SpIDer.). Narzędzie to, jest rezydentnym programem antywirusowym. Programy takie nazywane są wartownikami lub monitorami.

Ponadto, w pakiecie znajduje się również program Doctor Web Scheduler. Jest on prostym w obsłudze, intuicyjnym terminarzem, pozwalającym na zautomatyzowanie pracy programu DrWeb. Scheduler pozwala zarówno na automatyczne uruchamianie testu, w wyznaczonym przez użytkownika terminie, jak i na samoczynną aktualizację programu DrWeb poprzez Internet.

ROZDZIAŁ 1 – MENU PROGRAMU DOCTOR WEB

Menu programu DrWeb pozwala na kontrolowanie testu, przejście do innych elementów programu, zmianę ustawień, wybór języka oraz na uruchomienie systemu pomocy. Menu programu DrWeb można otworzyć w każdym oknie, z wyjątkiem okna *Ustawienia*.

1.1. Menu Plik

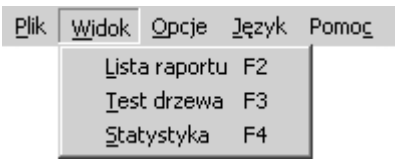


- **Rozpocznij test** – uruchamia test wybranych napędów. Test można również uruchomić za pomocą odpowiedniego przycisku lub wciskając klawisze CTRL+F5;
- **Zatrzymaj test** – przerywa test wybranych napędów. Test można również zatrzymać za pomocą odpowiedniego przycisku lub wciskając klawisze CTRL+F6;
- **Testuj ścieżkę** – po wybraniu tej opcji pojawia się okno, w którym możesz podać ścieżkę i maskę testu. Opcję tą można również wywołać wciskając klawisz F5;

Testuj pamięć – uruchamia test wszystkich procesów aktywnych w pamięci komputera. Pamięć można również przetestować wciskając klawisz F6;

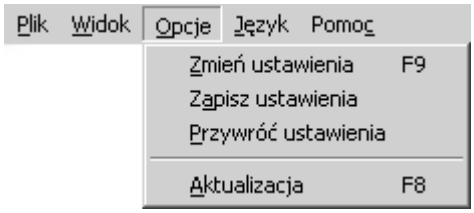
- **Wyczyść raport** – powoduje wyczyszczenie listy raportu. Funkcję tą można również wywołać za pomocą odpowiedniego przycisku lub wciskając klawisze CTRL+F2;
- **Zamknij** – zamyka program DrWeb. Program można również zamknąć przy pomocy odpowiedniego przycisku lub wciskając klawisze ALT+X.

1.2. Menu Widok



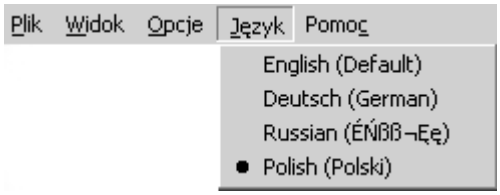
- **Lista raportu** – uaktywnia okno przedstawiające listę raportu. Listę raportu można wywołać również za pomocą odpowiedniego przycisku lub wciskając klawisz F2;
- **Test drzewa** – otwiera okno główne programu DrWeb. Alternatywnie, można użyć odpowiedniego przycisku lub wcisnąć klawisz F3;
- **Statystyka** – otwiera okno przedstawiające statystykę bieżącego testu. Okno to można wywołać podczas trwania testu. Statystykę można uaktywnić również za pomocą odpowiedniego przycisku lub wciskając klawisz F4.

1.3. Menu Opcje



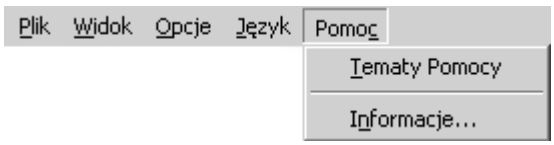
- **Zmień ustawienia** – otwiera arkusz właściwości programu DrWeb. Okno to można również wywołać przy pomocy odpowiedniego przycisku lub wciskając klawisz F9;
- **Zapisz ustawienia** – zapisuje ustawienia, aby mogły być wykorzystane podczas następnej sesji;
- **Przywróć ustawienia** – przywraca ustawienia standardowe;
- **Aktualizacja** – uruchamia mechanizm aktualizujący program DrWeb oraz jego bazy antywirusowe poprzez Internet. Proces ten jest w pełni zautomatyzowany i nie wymaga od użytkownika żadnej ingerencji. Aktualizację można również wywołać przy użyciu odpowiedniego przycisku lub wciskając klawisz F8.

1.4. Menu Język



To Menu pozwala wybrać język, w którym DrWeb ma pracować. Wybrany język obejmuje również system pomocy.

1.5. Menu Pomoc



- **Tematy Pomocy** – otwiera system pomocy programu DrWeb;
- **Informacje** – otwiera okno, w którym znajdują się informacje o wersji programu, ilości rozpoznawanych wirusów oraz o programistach.

ROZDZIAŁ 2 – PRZYCISKI STERUJĄCE PROGRAMEM DOCTOR WEB

Wszystkie przyciski, z wyjątkiem przycisków *Rozpocznij/Zatrzymaj test* oraz *Odśwież*, są aktywne w każdym oknie programu, wyłączając okno *Ustawienia*.

Lista raportu – otwiera okno przedstawiające raport z testu. Listę raportu można również wywołać z menu *Widok* lub wciskając klawisz F2.

Test drzewa – otwiera okno główne programu DrWeb. Okno to można również wywołać z menu *Widok* lub wciskając klawisz F3.

Statystyka – otwiera okno przedstawiające statystykę bieżącego testu. Statystykę można otwierać w dowolnym momencie, także podczas trwania testu. Okno to można również uaktywnić z menu *Widok* lub wciskając klawisz F4.

Czyszczenie listy raportu – służy do czyszczenia listy raportu. Funkcję tą można również wywołać z menu *Plik* lub wciskając klawisze CTRL+F2

Aktualizacja – uruchamia mechanizm aktualizujący program DrWeb oraz jego bazy antywirusowe poprzez Internet. Proces ten jest w pełni zautomatyzowany i nie wymaga od użytkownika żadnej ingerencji. Aktualizację można również wywołać w menu *Opcje* lub wciskając klawisz F8.

Ustawienia – otwiera arkusz właściwości programu DrWeb. Okno to można również wywołać w menu *Opcje* lub wciskając klawisz F9

Zamknij - zamyka program DrWeb. Program można również zamknąć w menu *Plik* lub wciskając klawisze ALT+X.

Przycisk *Rozpocznij/Zatrzymaj test* może przybierać następujące formy:

Nie wybrano żadnego obiektu do testu. Nie można rozpocząć testu. Naciśnięcie przycisku nie wywoła żadnej reakcji.

Wybrano obiekt lub obiekty do testu. Naciśnięcie przycisku spowoduje rozpoczęcie testu. Test można również rozpocząć w menu *Plik* lub wciskając klawisze CTRL+F5.

Test w toku. Naciśnięcie przycisku spowoduje zatrzymanie testu. Test można również zatrzymać z menu *Plik* lub wciskając klawisze CTRL+F6.

ROZDZIAŁ 3 – OKNO TEST DRZEWA

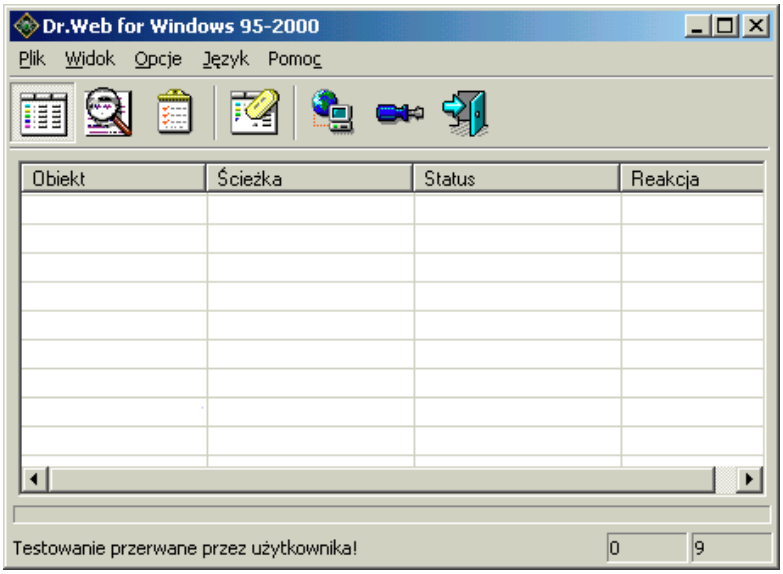
W oknie tym możesz wybrać napęd, napędy lub konkretną ścieżkę przeznaczoną do testu, ustawić podstawowe parametry testu oraz rozpocząć i zakończyć test. Możesz także przejść do innych okien programu, korzystając z menu lub odpowiednich przycisków. Okno *Test Drzewa* można otworzyć za pomocą odpowiedniego przycisku, korzystając z menu *Widok* lub wciskając klawisz F3.

Rys. 1. Okno główne programu DrWeb dla Windows 95-2000

- **Pokaż pliki** – jeśli ten przycisk jest wciśnięty, wyświetlane są zarówno katalogi jak i pliki testowanego drzewa. W przeciwnym wypadku wyświetlane są tylko katalogi. Zaznacz tą opcję jeśli chcesz wybierać do testowania pojedyncze pliki. Gdy chcesz testować cały dysk lub folder, możesz nie zaznaczać tej opcji, co uczyni drzewo znacznie bardziej czytelnym;
- **Odśwież** - ten przycisk odświeża testowane drzewo. Może to być konieczne, jeśli na przykład odłączysz dysk sieciowy lub utworzysz nowy folder podczas sesji z programem Doctor Web.
- **Zapamiętaj** - Ten przycisk zapisuje dany zestaw folderów (dysków), które są często testowane. Podczas następnej sesji możesz przywrócić zapisane ustawienia (wciskając przycisk **Odtwórz**), zamiast ponownie zaznaczać te same obiekty.
- **Odtwórz** - Ten przycisk przywraca zapisany uprzednio zestaw obiektów przeznaczonych do testu.
- **Czyść** - Naciśnij ten przycisk zamiast pojedynczo usuwać obiekty przeznaczone do testu.

ROZDZIAŁ 4 – OKNO LISTA RAPORTU

W oknie tym możesz przejrzeć rezultaty ostatniego testu. Lista raportu składa się z czterech kolumn pozwalających zlokalizować podejrzany obiekt oraz zaobserwować reakcję programu DrWeb na wystąpienie potencjalnie niebezpiecznego pliku. Listę raportu można otworzyć za pomocą odpowiedniego przycisku, korzystając z menu *Widok* lub wciskając klawisz F2.

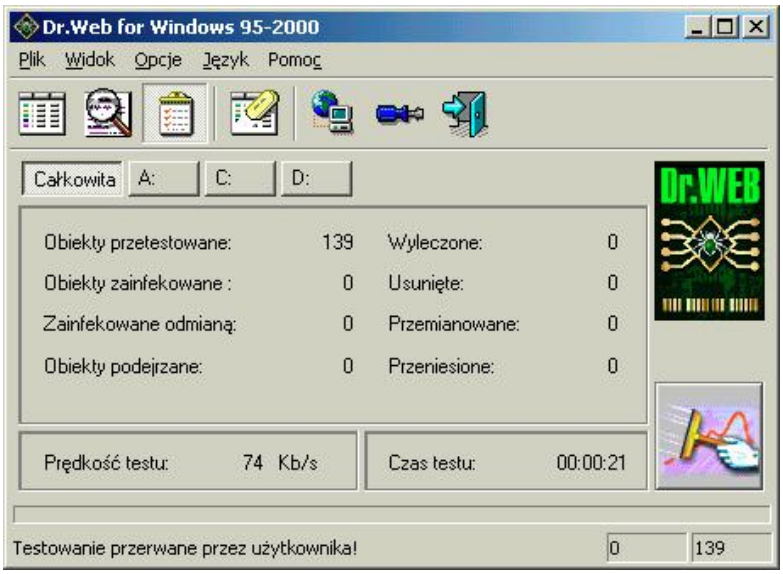


Rys. 2. Okno *Lista Raportu.*

- **Obiekt** – ta kolumna zawiera pliki, które wywołały podejrzenie programu DrWeb. Mogą to być pliki zainfekowane wirusem komputerowym;
- **Ścieżka** – ta kolumna zawiera pełne ścieżki dostępu do podejrzanych plików;
- **Status** - ta kolumna wskazuje powód wystąpienia podejrzenia. Może się tutaj pojawić nazwa wirusa, który zainfekował plik;
- **Reakcja** - ta kolumna opisuje reakcję, jaką Doctor Web odpowiedział dla konkretnego pliku (leczenie, usunięcie, zmiana nazwy, itd.). Reakcje te możesz wybierać w oknie *Ustawienia.*

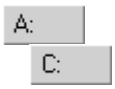
ROZDZIAŁ 5 – OKNO STATYSTYKA

To okno wyświetla statystykę bieżącej sesji. Można je otworzyć w dowolnym momencie, także podczas trwania testu. Statystykę można uaktywnić za pomocą odpowiedniego przycisku, korzystając z menu *Widok* lub wciskając klawisz F4.

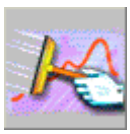


Rys. 3. Okno *Statystyka.*

Ten przycisk pokazuje statystykę dla wszystkich testowanych dysków.



Te przyciski pokazują statystykę dla konkretnego dysku.



Ten przycisk czyści statystykę. Można go używać także podczas trwania testu.

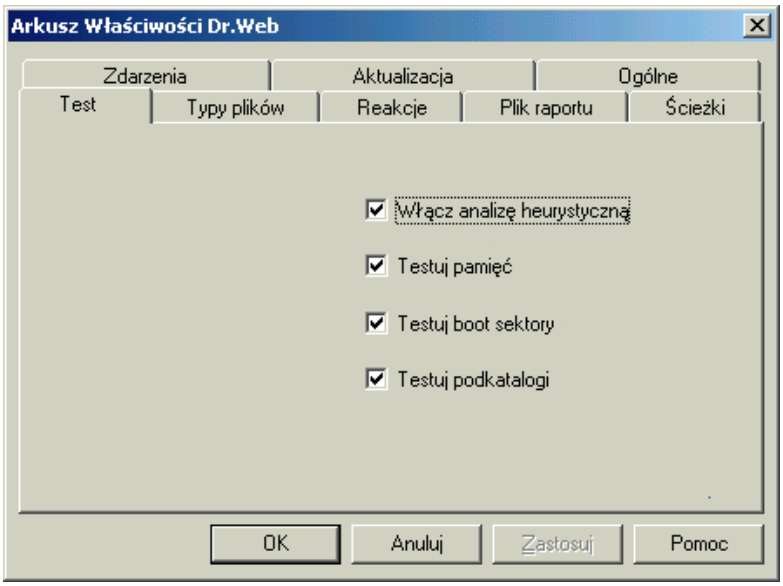
- **Obiekty przetestowane** - ilość przetestowanych obiektów;
- **Obiekty zainfekowane** - ilość obiektów zainfekowanych głównymi wariantami znanych wirusów;
- **Zainfekowane odmianą** – ilość obiektów zainfekowanych modyfikacjami wirusów;
- **Obiekty podejrzane** - ilość obiektów zgłoszonych przez analizator heurystyczny;
- **Wyleczone** - ilość wyleczonych obiektów;
- **Usunięte** – ilość usuniętych obiektów;
- **Przemianowane** – ilość obiektów, których nazwy zostały zmienione;
- **Przeniesione** – ilość przeniesionych obiektów;
- **Prędkość testu** – prędkość w kB/s, z jaką odbywa się w danej chwili test;
- **Czas testu** – czas, który upłynął od rozpoczęcia testu lub od ostatniego wyczyszczenia statystyki.

ROZDZIAŁ 6 – OKNO USTAWIENIA

W ośmiu zakładkach będących składnikami tego okna, możesz w pełni konfigurować wszystkie funkcje programu Doctor Web. Okno to, jako jedyne nie posiada menu oraz przycisków sterujących. Do *Ustawień* możesz się dostać przy pomocy odpowiedniego przycisku, korzystając z menu *Opcje* lub wciskając klawisz F9.

6.1. Zakładka Test

Korzystając z opcji udostępnianych przez tą zakładkę, możesz wybierać dyski testowane domyślnie oraz zmieniać domyślne opcje testu.

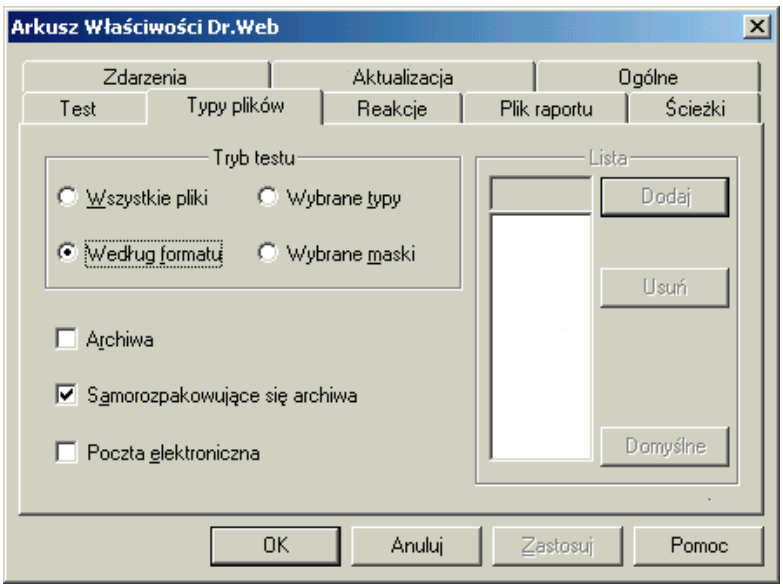


Rys. 4. Okno *Ustawienia*, zakładka *Test.*

- **Włącz analizę heurystyczną** - jeśli ta opcja jest zaznaczona, Doctor Web wykorzystuje swój analizator heurystyczny, który umożliwia wykrywanie nieznanych wirusów i podejrzanych plików. Zalecamy uaktywnienie tej opcji, mimo iż powoduje ona spowolnienie procesu testowania.
- **Testuj pamięć** - jeśli ta opcja jest zaznaczona, Doctor Web po uruchomieniu automatycznie testuje pamięć. Test pamięci można również wywołać ręcznie, wybierając opcję *Testuj Pamięć* z menu *Plik* lub wciskając klawisz F6;
- **Testuj boot sektory** - jeśli ta opcja jest zaznaczona, Doctor Web testuje boot sektory wybranych do testu dysków;
- **Testuj podkatalogi** - jeśli ta opcja jest zaznaczona, Doctor Web rekursywnie testuje wszystkie podkatalogi;

6.2. Zakładka Typy Plików

W tej zakładce możesz zdefiniować jakie pliki Doctor Web ma brać pod uwagę podczas testu.



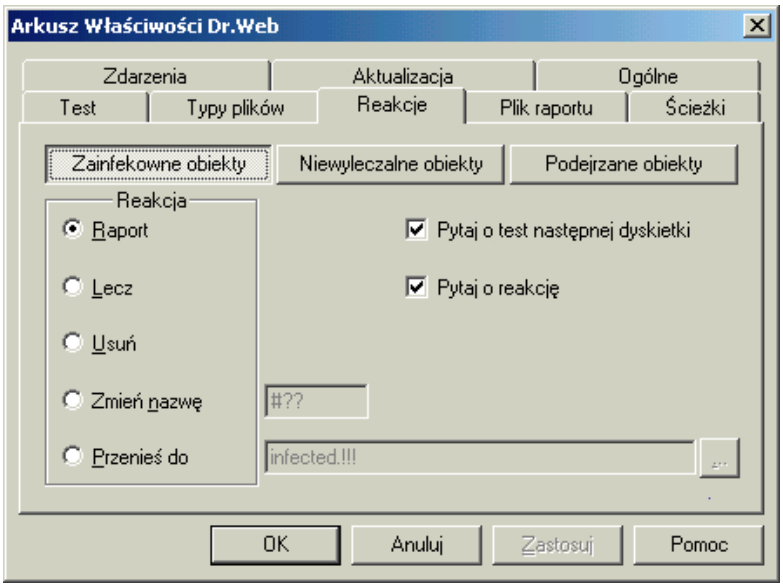
Rys. 5. Okno *Ustawienia*, zakładka *Typy plików*.

- **Tryb testu** - ta grupa przycisków umożliwia wybór trybu testowania, czyli metody, której Doctor Web używa podczas decydowania o typach plików poddawanych testowi:
  - **Wszystkie pliki** - jeśli ta opcja jest zaznaczona, Doctor Web testuje wszystkie pliki w Twoim systemie. Może to być bardzo czasochłonne;
  - **Według formatu** - jeśli ta opcja jest zaznaczona, Doctor Web rozpoznaje typ pliku ze względu na jego wewnętrzny format, niezależnie od rozszerzenia. Masz zatem pewność, że na przykład, plik uruchamialny zostanie przetestowany, mimo iż nie posiada rozszerzenia odpowiedniego dla takiego pliku;
  - **Wybrane typy** - jeśli ta opcja jest zaznaczona, Doctor Web testuje tylko pliki, których rozszerzenia zawierają się w liście z prawej strony. Możesz tą listę edytować (np. dodawać i usuwać rozszerzenia);
  - **Wybrane maski** - jeśli ta opcja jest zaznaczona, Doctor Web sprawdza tylko pliki, których rozszerzenia są zgodne ze zdefiniowanymi przez użytkownika maskami, wyświetlonymi z prawej strony. Opcja ta może zasadniczo skrócić czas testu, jeśli na przykład chcesz testować tylko pliki programu Microsoft Word (np.: pliki DOC i DOT pasujące do maski DO?);
- **Lista** – tutaj możesz określić typy lub maski. Aby dodać nowy typ pliku lub nową maskę, użyj przycisku *Dodaj*, natomiast aby usunąć z listy istniejący wpis, użyj przycisku *Usuń*. Przycisk *Domyślne* przywraca standardowy zestaw masek.
- **Archiwa** - jeśli ta opcja jest zaznaczona, Doctor Web testuje spakowane pliki (np. plik DOC zawarty w archiwum ZIP). Opcja ta wymaga dodatkowego czasu i miejsca na dysku, ponieważ archiwa są rozpakowywane do tymczasowych plików. Doctor Web nie leczy zainfekowanych plików zawartych w archiwach;
- **Samo rozpakowujące się archiwa** - jeśli ta opcja jest zaznaczona, Doctor Web testuje uruchamialne pliki spakowane (tworzone przez programy takie jak LZEXE). Jeśli taki plik został zainfekowany przed spakowaniem, wirus nie zostanie rozpoznany. Opcja ta daje pewność, że dane przechowywane w samo rozpakowujących archiwach są bezpieczne;
- **Poczta elektroniczna** - jeśli ta opcja jest zaznaczona, Doctor Web testuje pliki zakodowane UUENCODE oraz MIME. Aby określić rodzaj kodowania, Doctor Web musi przeczytać cały plik, co znacznie spowalnia proces testowania. Używaj tej opcji tylko jeśli musisz testować wiadomości e-mail.

Maski działają w następujący sposób:
- znak "*****" oznacza każdy (nawet pusty) ciąg znaków;
- znak "**?**" oznacza jakikolwiek pojedynczy znak;
- każdy inny znak oznacza ten konkretny znak.

6.3. Zakładka Reakcje

W tej zakładce możesz zdefiniować jak DrWeb32W ma reagować na zainfekowane i podejrzane obiekty.



Rys. 6. Okno *Ustawienia*, zakładka *Reakcje.*

Zainfekowne obiekty — Ten przycisk określa reakcję, jaką Doctor Web ma odpowiedzieć na wystąpienie zainfekowanych obiektów. Możesz wybierać spośród następujących możliwości: twórz raport, lecz, usuń, zmień nazwę (zmień rozszerzenie na podane) oraz przenieś do określonego foldera.

Niewyleczalne obiekty — Ten przycisk określa reakcję, jaką Doctor Web ma odpowiedzieć na wystąpienie zainfekowanych obiektów, które nie mogą być wyleczone. Dla tych obiektów dostępne są następujące reakcje: twórz raport, usuń, zmień nazwę (zmień rozszerzenie na podane) oraz przenieś do określonego foldera. Opcja “lecz” jest nieaktywna.

Podejrzane obiekty — Ten przycisk określa reakcję, jaką Doctor Web ma odpowiedzieć na wystąpienie podejrzanych obiektów, które prawdopodobnie są zainfekowane. Dla tych obiektów dostępne są następujące reakcje: twórz raport, usuń, zmień nazwę (zmień rozszerzenie na podane) oraz przenieś do określonego foldera. Opcja “lecz” jest nieaktywna.

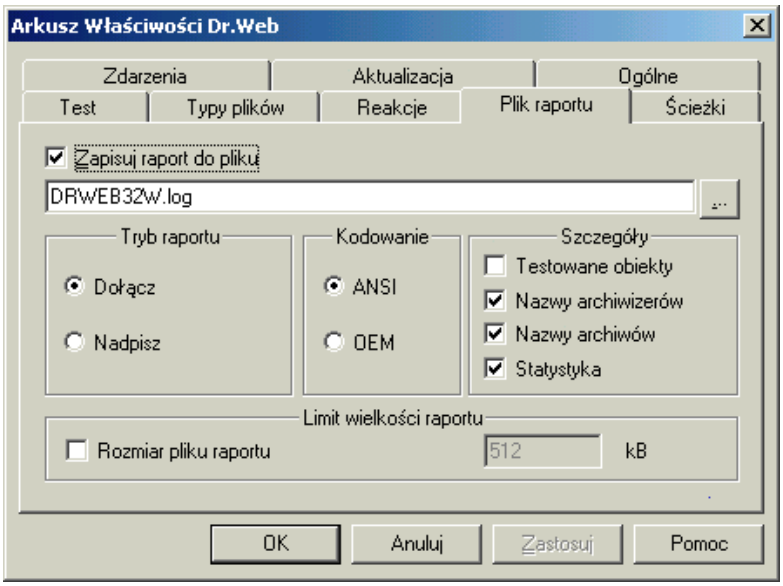
- **Reakcja** - ta grupa opcji określa reakcję, którą Doctor Web odpowie na wystąpienie obiektów wybranych jednym z trzech powyższych przycisków. Reakcje te muszą być zdefiniowane oddzielnie dla wszystkich trzech kategorii obiektów: zainfekowanych, niewyleczalnych i podejrzanych:

- **Raport** - Jeśli ta opcja jest zaznaczona, Doctor Web tylko tworzy raport zawierający informacje o obiektach, które wywołały alarm;
- **Lecz** - jeśli ta opcja jest zaznaczona, Doctor Web leczy zainfekowane obiekty;
- **Usuń** - jeśli ta opcja jest zaznaczona, Doctor Web usuwa wszystkie obiekty, które wywołały alarm (np. obiekty podejrzane lub zainfekowane). Używaj tej funkcji z rozwagą, w szczególności jeśli opcja *Informuj o reakcji* nie jest zaznaczona;
- **Zmień nazwę** - jeśli ta opcja jest zaznaczona, Doctor Web zmienia nazwy wszystkich obiektów, które wywołały alarm (np. obiektów podejrzanych lub zainfekowanych). Obiekty te otrzymują rozszerzenie określone w okienku po prawej stronie;
- **Przenieś do** - jeśli ta opcja jest zaznaczona, Doctor Web przenosi do foldera wyszczególnionego w okienku po prawej stronie, wszystkie obiekty, które wywołały alarm (np. obiekty podejrzane lub zainfekowane). Opcja ta może być użyteczna, jeśli obiekty mają być w przyszłości zbadane;

- **Pytaj o test następnej dyskietki** - jeśli ta opcja jest zaznaczona, po zakończeniu testu dyskietki lub płyty CD, Doctor Web pyta o test kolejnej dyskietki lub płyty CD;
- **Informuj o reakcji** - jeśli ta opcja jest zaznaczona, Doctor Web prosi o potwierdzenie każdej reakcji.

6.4. Zakładka Plik Raportu

W tym oknie możesz zdefiniować opcje raportu.



Rys. 7. Okno *Ustawienia*, zakładka *Plik raportu.*

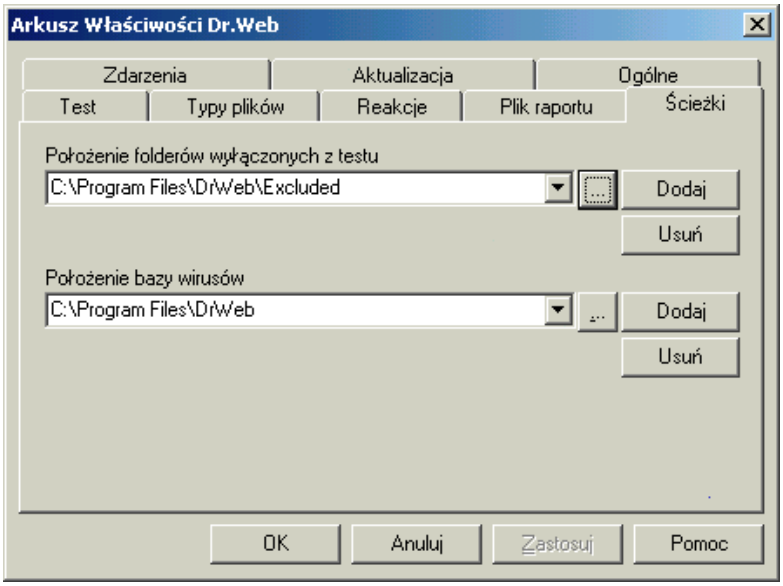
- **Zapisuj raport do pliku** - jeśli ta opcja jest zaznaczona, Doctor Web tworzy plik raportu, zawierający informacje o plikach zainfekowanych, wyleczonych, itd. W poniższym okienku możesz podać nazwę pliku raportu;
- **Tryb raportu** – możesz wybrać spośród dwóch opcji – **Dołącz** (Doctor Web dopisuje raport do istniejącego pliku, jeśli plik nie istnieje – jest tworzony) oraz **Nadpisz** (Doctor Web nadpisuje istniejący plik raportu rezultatami ostatniego testu);
- **Kodowanie** - tutaj możesz wybrać rodzaj kodowania znaków w raporcie. Masz do dyspozycji dwa rodzaje kodowania: **ANSI** (strona kodowa systemu Windows) oraz **OEM** (strona kodowa systemu DOS);
- **Szczegóły** - tutaj możesz szczegółowo określić, jakie informacje będą zapisywane w pliku raportu:

- **Testowane obiekty** - jeśli ta opcja jest zaznaczona, do raportu zapisywane są informacje o wszystkich testowanych obiektach. Może to sprawić, że plik raportu będzie bardzo duży;
- **Nazwy archiwizerów** - jeśli ta opcja jest zaznaczona, do raportu zapisywane są nazwy programów tworzących samo rozpakowujące się archiwa (LZEXE, PKLITE itp.), które były używane podczas kompresowania plików uruchamialnych;
- **Nazwy archiwów -** jeśli ta opcja jest zaznaczona, do raportu zapisywane są nazwy narzędzi (PKZIP, ARJ, itp.), które były używane podczas tworzenia archiwów;
- **Statystyka** - jeśli ta opcja jest zaznaczona, do raportu zapisywana jest statystyka testu (ilość sprawdzonych obiektów, zainfekowanych obiektów, itd.). W momencie zakończenia sesji, Doctor Web zapisze jej statystykę do pliku raportu;

- **Limit wielkości raportu** - tutaj możesz określić maksymalny rozmiar pliku raportu. Opcja ta może być użyteczna jeśli na Twoim dysku jest mała ilość wolnego miejsca:
  - **Rozmiar pliku raportu** - jeśli ta opcja jest zaznaczona, Doctor Web ogranicza rozmiar pliku raportu do wartości wpisanej po prawej stronie.

6.5. Zakładka Ścieżki

W tej zakładce możesz określić lokację baz antywirusowych programu Doctor Web oraz lokację folderów wyłączonych z testu.

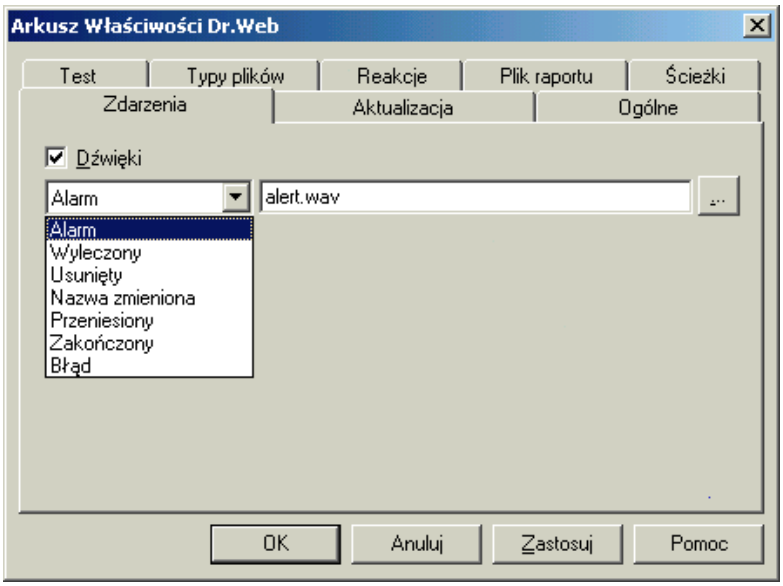


Rys. 8. Okno *Ustawienia*, zakładka *Ścieżki.*

- **Położenie folderów wyłączonych z testu** – w tym okienku możesz określić foldery, które nie będą sprawdzane. Aby dodać do listy kolejny folder, użyj przycisku *Dodaj*, natomiast aby usunąć z listy istniejący folder, użyj przycisku *Usuń*;
- **Położenie bazy wirusów** – tutaj możesz określić lokację baz antywirusowych (głównych oraz dodatkowych) programu Doctor Web.

6.6. Zakładka Zdarzenia

W tym oknie możesz uaktywnić efekty dźwiękowe programu DrWeb32W (Twój komputer musi być wyposażony w kartę dźwiękową).

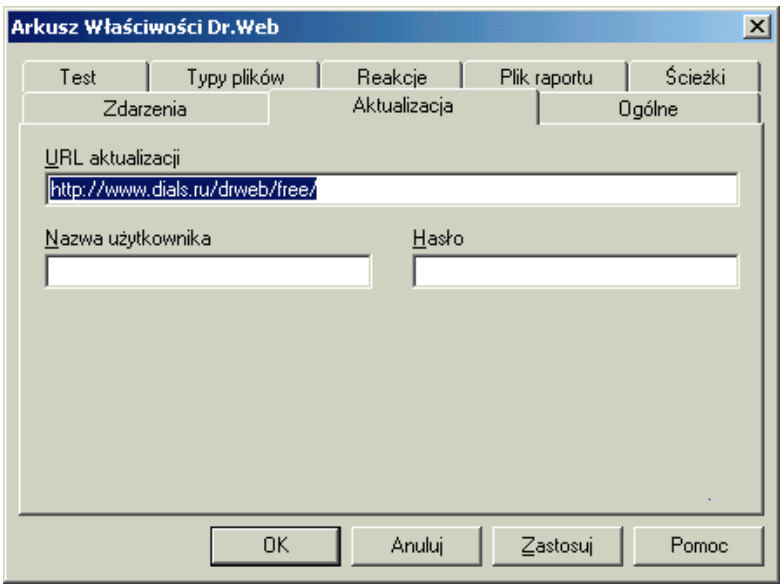


Rys. 9. Okno *Ustawienia*, zakładka *Zdarzenia.*

- **Dźwięki** - jeśli ta opcja jest zaznaczona, Doctor Web odtwarza dźwięki podczas leczenia, usuwania, zmieniania nazwy, przenoszenia, wystąpienia błędu oraz w momencie zakończenia testu.

6.7. Zakładka Aktualizacja

W tym oknie możesz określić opcje automatycznej aktualizacji programu Doctor Web poprzez Internet.

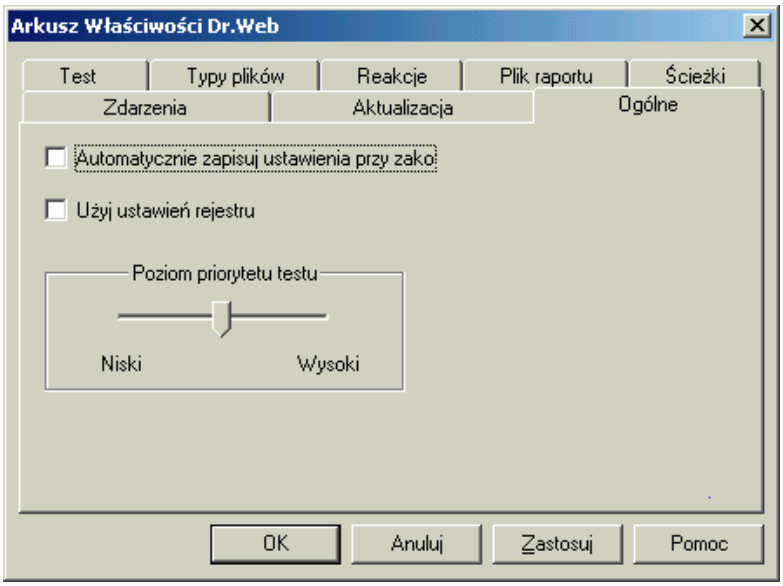


Rys. 10. Okno *Ustawienia*, zakładka *Aktualizacja.*

- **URL aktualizacji** – tutaj wybierasz serwer, z którego mają być pobierane uaktualnienia. Domyślnie jest to *http://www.dials.ru/drweb/free/ obecnie dostępna jest już aktualizacja z polskiego serwera polecamy zmianę na http://www.drweb.com.pl/download/free co przyspieszy aktualizację baz.*
- **Nazwa użytkownika** – tutaj podajesz swój identyfikator (obecnie nie używana)
- **Hasło** – tutaj podajesz swoje hasło dostępowe do serwera. (obecnie nie używane)

6.8. Zakładka Ogólne

W tym oknie możesz ustawić opcje ogólne programu Doctor Web.



Rys. 11. Okno *Ustawienia*, zakładka *Ogólne.*

- **Automatycznie zapisuj ustawienia przy zakończeniu** - jeśli ta opcja jest zaznaczona, wszystkie ustawienia są automatycznie zapisywane w momencie zamykania sesji;
- **Użyj ustawień rejestru** - jeśli ta opcja jest zaznaczona, DrWeb zapisuje (w rejestrze systemowym) bieżące pozycje i rozmiary swoich okien;
- **Poziom priorytetu testu** - suwak służący do ustawiania poziomu priorytetu testu. Wyższy priorytet pozwala działać szybciej programowi Doctor Web lecz spowalnia inne aplikacje i vice versa.

ROZDZIAŁ 7 – SPIDER GUARD

SpIDer jest rezydentnym programem antywirusowym (narzędzia tego typu są nazywane “strażnikami”, “wartownikami” lub ”monitorami”), załączonym do pakietu Doctor Web-32. SpIDer zastał zaprojektowany w celu wykrywania wirusów infekujących pliki, podczas ich otwierania/zamykania oraz w celu przechwytywania akcji wykonywanych przez wirusy.

SpIDer sprawdza wszystkie próby dostępu do plików oraz obszarów systemowych i "w locie" szuka w nich wirusów. Po wykryciu szkodnika, SpIDer usuwa lub blokuje zainfekowany plik i umożliwia dostęp do niego, dopiero po wyleczeniu. SpIDer może również działać w specjalnym trybie, w którym potrafi wykrywać i blokować aktywności podobne do działania wirusów, nawet jeszcze nie znanych. Aktywnością taką może być przykładowo próba infekowania lub usuwania plików.

SpIDer korzysta z tej samej bazy wirusów i z tego samego jądra, których używa Dr.Web dla Windows 95/98/NT/2000. SpIDer jest zawarty w pakiecie Dr.Web dla Win32 i jest instalowany przez ten sam program.

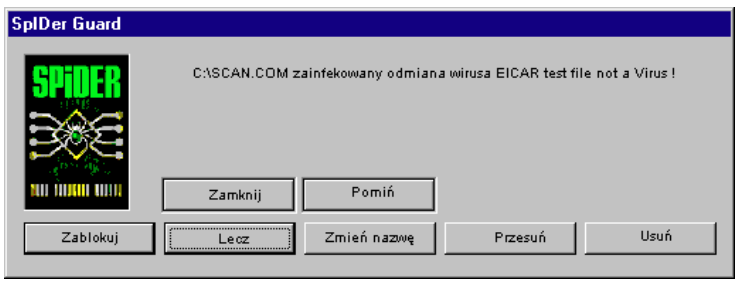
Podczas uruchamiania, SpIDer sprawdza pamięć komputera, a następnie w obszarze zasobnika systemowego pojawia się jego ikona. Kliknięcie na niej prawym klawiszem myszy, spowoduje pojawienie się menu programu, natomiast podwójne kliknięcie lewym klawiszem myszy, otworzy okno, w którym możesz konfigurować wszystkie opcje programu.

Jeśli podczas zamykania systemu Windows, w napędzie A: będzie znajdować się dyskietka, SpIDer sprawdzi ją zapobiegając infekcji, która mogłaby mieć miejsce podczas ponownego uruchomienia systemu.

SpIDer został zaprojektowany dla 32-bitowych systemów Windows. Może pracować w systemach Windows 95, OSR2, 98, Me, NT oraz 2000. Szczegółowe informacje na temat programu SpIDer dla Windows NT/2000, znajdują się w pliku SPIDERNT.TXT, załączonym do pakietu. PROSZĘ RZECZYTAĆ ZAWARTOŚĆ TEGO PLIKU PRZED PRZYSTĄPIENIEM DO KORZYSTANIA Z PROGRAMU!

Możesz skonfigurować program SpIDer tak, aby odpowiadał Twoim wymaganiom. Konfiguracja programu SpIDer jest identyczna jak w przypadku programu Doctor Web.

7.1. Alarm -infekcja



- **Zablokuj (*domyślna)*** uniemożliwia otworzenie zainfekowanego obiektu do momentu jego wyleczenia. **Uwaga wybór tej reakcji podczas odbierania poczty może doprowadzić do zablokowania programu obsługującego pocztą elektroniczną. Zaleca się wybranie opcji pomiń i odebranie poczty a następnie wyleczenie zainfekowanych obiektów lub usunięcie wiadomości zawierających nie wyleczalne robaki.**
- **Zamknij** Wybór tej reakcji powoduje bezpieczne zamkniecie systemu operacyjnego windows.
- **Lecz** Reakcja lecz umożliwia wyleczenie zainfekowanego pliku. W przypadku załączników pocztowych wyleczona zostaje kopia załącznika zapisywana na dysku. Oryginalny załącznik pozostaje zainfekowany w pliku pocztowym.
- **Usuń** skutkuje usunięciem zainfekowanego pliku. SpIDer usuwa obiekt, który wywołał alarm. *Używaj tej opcji z rozwagą !*. Reakcja ta nie wywołuje żadnego skutku w przypadku załączników pocztowych, które musza być usunięte wraz z całą wiadomością.
- **Zmień nazwę** SpIDer zmieni nazwę obiektu, który wywołał alarm. Obiekt otrzymuje rozszerzenie określone w ustawieniach skanera DrWeb. W przypadku załączników pocztowych na dysk zostanie zapisany załącznik z odpowiednio zmienioną nazwa.
- **Przenieś do** Zainfekowany obiekt zostanie przeniesiony do foldera wyszczególnionego w ustawieniach skanera DrWeb. Opcja ta może być użyteczna, jeśli obiekty maja być w przyszłości zbadane

Program SpIDer Guard jako rezydentny monitor antywirusowy, wykrywa wirusy w momencie otwierania lub uruchamiania zainfekowanego pliku. Informuje o próbie zakażenia dysku lokalnego, co ma miejsce w przypadku np. odbierania poczty lub kopiowania plików z dysków sieciowych. W zależności od konfiguracji reakcja może być dla użytkownika niezauważalna (wylecz, usuń , zmień nazwę, zablokuj, przesuń do zainfekowanych) lub każda infekcja może być raportowana sygnałem dźwiękowym wraz z zapytaniem o reakcje. Obecnie najpospolitszym źródłem zakażeń jest poczta elektroniczna. Jednak szkodnik wy-

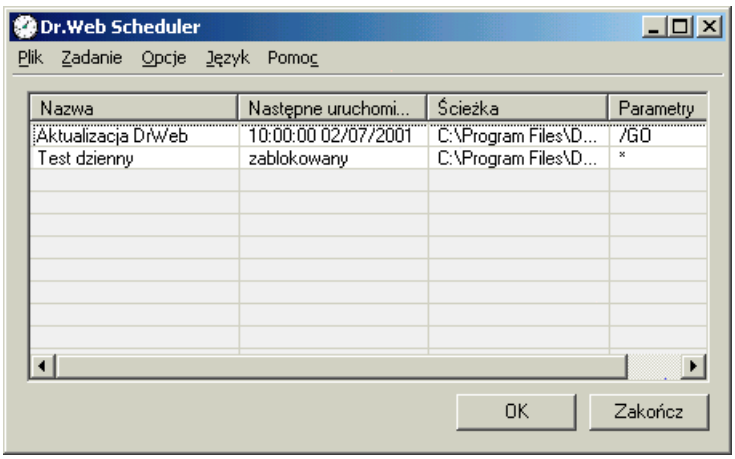
kryty przez SpIDer Guard w odbieranej wiadomości nie ma żadnych szans na dokonanie jakichkolwiek spustoszeń na twoim komputerze. Wszelkie próby otworzenia zainfekowanego załącznika zostaną skutecznie zablokowane a zarażone obiekty (jeżeli jest to możliwe) otwierane lub zapisywane na dysk wyleczone. Należy pamiętać, że załącznik pozostający zaszyty w pliku pocztowym pozostaje niezmieniony i usuwany jest tylko z całą wiadomością.

ROZDZIAŁ 8 – DOCTOR WEB SCHEDULER

8.1. Informacje ogólne

Doctor Web Scheduler jest prostym w obsłudze, intuicyjnym terminarzem, pozwalającym na zautomatyzowanie pracy programu DrWeb. Scheduler pozwala zarówno na automatyczne uruchamianie testu, w wyznaczonym przez użytkownika terminie, jak i na samoczynną aktualizację programu DrWeb poprzez Internet.

Gdy Scheduler jest aktywny (uruchomiony), jego ikona pojawia się w obszarze zasobnika systemowego. Dwukrotne kliknięcie na tej ikonie otwiera okno zawierające menu programu oraz listę zadań.

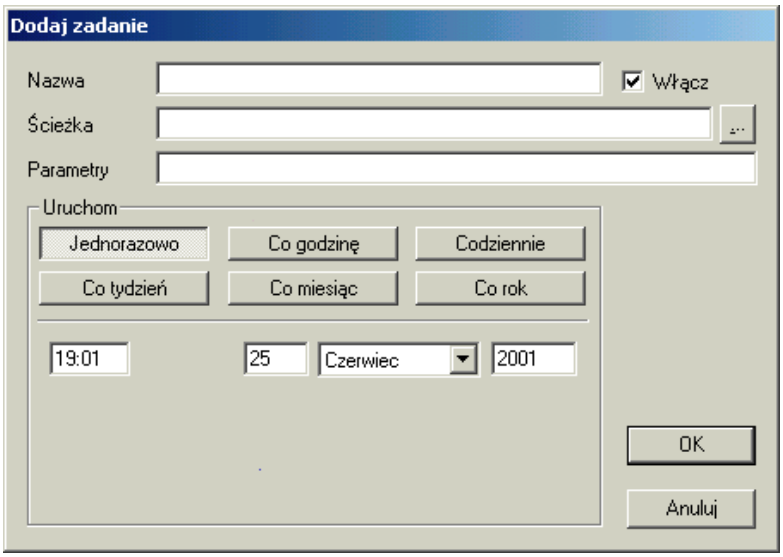


Rys. 12. Okno główne programu *Doctor Web Scheduler.*

- **Nazwa** – nazwa zadania;
- **Następne uruchomienie** – godzina i data następnego uruchomienia zadania. Jeśli zadanie jest nieaktywne, pojawia się tutaj komunikat *zablokowany*;
- **Ścieżka** – ścieżka dostępu do aplikacji która ma być uruchomiona przez zadanie. Jeśli chcesz utworzyć zadanie, które będzie automatycznie uruchamiać program Doctor Web, ścieżka może wyglądać następująco: *C:\Program Files\DrWeb\Drweb32w.exe*. Jeśli natomiast celem zadania ma być aktualizacja programu DrWeb poprzez Internet, ścieżka może mieć postać: *C:\Program Files\DrWeb\Drwebupw.exe*.
- **Parametry** – dodatkowe opcje do uruchomienia programu DrWeb (zobacz *Rozdział 9 – Opcje Linii Poleceń)*.

8.2. Tworzenie zadania

Aby utworzyć nowe zadanie, wybierz opcję *Dodaj zadanie* z menu *Zadanie* programu DrWeb Scheduler. Pojawi się okno *Dodaj zadanie*:



Rys. 13. Okno *Dodaj zadanie* programu *Doctor Web Scheduler.*

- **Nazwa** – tutaj podajesz nazwę zadania;
- **Ścieżka** – w tym okienku musisz podać pełną ścieżkę dostępu do programu, który ma być uruchomiony przez zadanie. Jeśli chcesz utworzyć zadanie, które będzie automatycznie uruchamiać program Doctor Web, ścieżka może wyglądać następująco: *C:\Program Files\DrWeb\Drweb32w.exe*. Jeśli natomiast celem zadania ma być aktualizacja programu DrWeb poprzez Internet, ścieżka może mieć postać: *C:\Program Files\DrWeb\Drwebupw.exe*.
- **Parametry** – dodatkowe parametru uruchomieniowe dla programu Doctor Web (zobacz *Rozdział 9 – Opcje Linii Poleceń*);
- **Uruchom** – za pomocą przycisków i okienek zawartych w tym bloku, możesz ustawić czas i datę uruchomienia zadania oraz odstęp czasowy w kolejnych uruchomieniach zadania;
- **Włącz** – jeśli ta opcja jest zaznaczona, zadanie jest aktywne. Jeśli zadanie nie jest aktywne, w oknie głównym programu Scheduler, w kolumnie *Następne uruchomienie* widnieje komunikat *zablokowany.*

ROZDZIAŁ 9 – OPCJE LINII POLECEŃ

Aby uruchomić program Doctor Web, użyj następującej składni:

program [dysk:][ścieżka] [opcje]

gdzie:

Program nazwa modułu uruchamialnego (DrWeb32W lub DrWebWCL)

Dysk: dysk twardy, stacja dyskietek, dysk sieciowy, CD-ROM lub ***** (lista dysków logicznych – patrz: ustawienia "Dyski testowane domyślnie ")

Ścieżka lokacja plików, które mają być poddane testowi; może zawierać ścieżkę do katalogu na lokalnym/sieciowym dysku i opcjonalnie, nazwę pliku (lub maskę pliku).

Linia poleceń może zawierać kilka parametrów **[dysk:][ścieżka]** oddzielonych spacjami. W takim przypadku program będzie sekwencyjnie testował wyszczególnione obiekty. Gdy testowanie jest zakończone, DrWebWCL zamyka się. DrWeb32W (jeśli jest uruchomiony bez **/QU**) otwiera swoje okno główne, gdzie użytkownik może wybrać nowe obiekty do testu, obejrzeć rezultaty testu, personalizować ustawienia, uaktualnić lub zamknąć program. Jeśli DrWeb32W zostanie uruchomiony bez parametru **[dysk:][ścieżka]**, automatycznie otwierane jest jego okno główne

Opcje Linii Poleceń (należy oddzielać spacjami)

/@[+]<plik> ADinf może budować listę plików, które mają być sprawdzone przez skaner. Doctor Web może testować pliki znajdujące się na liście, co znacznie zmniejsza ogólny czas testu. W tym celu użyj opcji **/@** i określ plik znajdujący się na liście. Po zakończeniu testowania, Doctor Web usunie ten plik. Aby zachować plik, użyj parametru **"+"**. Jeśli Doctor Web zostanie uruchomiony z poziomu programu ADinf32, ten ostatni automatycznie utworzy linię poleceń, zawierającą wszystkie niezbędne opcje (patrz: plik pomocy dotyczący konfigurowania ADinf32)

/AL. test wszystkich plików na podanym dysku

/AR[N] test plików zawartych w archiwach. Ta wersja obsługuje tylko testowanie (bez leczenia) archiwów wykonanych przy użyciu **ARJ, PKZIP** oraz **RAR**. Parametr **N** powoduje, że nazwa archiwizera nie jest zapisywana w raporcie

/CU[RDM][P] leczenie zainfekowanych plików i obszarów systemowych, usuwanie plików niewyleczalnych. Użyj opcjonalnych parametrów aby określić jak zainfekowane pliki mają być traktowane: **R** – zmiana nazwy (domyślnie pierwszy znak rozszerzenia zamieniany jest na "#"), **D** – usunięcie, **M** – przeniesienie (domyślnie do folderu INFECTED.!!!); **P** – akcja z potwierdzeniem

/SP[RDM][P] określa jak traktować podejrzane pliki: **R** – zmiana nazwy, **D** – usunięcie, **M** – przeniesienie; **P** – akcja z potwierdzeniem

/IC[RDM][P] określa jak traktować niewyleczalne pliki: **R** – zmiana nazwy, **D** – usunięcie, **M** – przeniesienie; **P** – akcja z potwierdzeniem

/DA uruchomienie programu Doctor Web tylko raz dziennie. Dla tej opcji musi istnieć plik konfiguracyjny (plik INI)

/EX test plików posiadających "standardowe" rozszerzenia, np. pliki uruchamialne i dokumenty pakietu MS Office (**COM, EXE, SYS, BAT, CMD, DRV, BIN, DLL, OV?, BOO, PRG, VXD, 386, SCR, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VBS, JS*, INF, A??, ZIP, R??, PP?, HLP, OBJ, LIB, MD?, INI, MBR, IMG, CSC, CPL, MBP**)

/FM sprawdzanie plików ze względu na ich wewnętrzny format, niezależnie od rozszerzenia.

/GO Doctor Web działa nie wyświetlając żadnych komunikatów (niewystarczająca ilość wolnego miejsca na dysku do zapisania plików tymczasowych, błędna opcja linii poleceń, Doctor Web jest zainfekowany nieznanym wirusem, itd.). Opcja ta może być użyteczna w przypadku automatycznego sprawdzania, na przykład przychodzącej poczty elektronicznej.

/HA włączenie analizatora heurystycznego, który potrafi wykrywać nieznane wirusy

/INI:<plik> użycie alternatywnego pliku konfiguracyjnego (pliku INI)

/NI ignorowanie ustawień zapisanych w pliku konfiguracyjnym DRWEB32.INI

/LNG[:<plik>] użycie alternatywnego pliku językowego (plik DWL) lub domyślnego języka (angielski)

/NS uruchomienie programu Doctor Web bez możliwości przerwania jego pracy przy użyciu klawisza <Esc> (ta opcja nie jest obecnie obsługiwana przez DrWeb32W)

/OK. wyświetlanie nazwy każdego testowanego obiektu i wyświetlanie “OK” jeśli obiekt nie jest zainfekowany

/RP[+]<plik> zapisywanie raportu do pliku określonego przez parametr **<plik>**. Domyślnie jest to plik DRWEB32W.LOG lub DRWEBWCL.LOG. Parametr "**+**" dodaje raport do już istniejącego pliku

/NR wyłączenie raportu

/SD rekursywne testowanie podkatalogów

/SO włączenie efektów dźwiękowych

/SS zapisywanie ustawień przy wyjściu

/TB sprawdzanie boot sektorów oraz MBR-ów

/TM szukanie wirusów w pamięci

/UP[N] sprawdzanie samo rozpakowujących się archiwów, wykonanych przy użyciu A

SPACK, COMPACK, DIET, EXEPACK, LZEXE, OPTLINK, PEPACK, PGMPAK, PKLITE, WWPACK, WWPACK32, UCEXE, UPX; plików skonwertowanych przez BJFNT, COM2EXE, CONVERT, CRYPTCOM, CRYPTEXE, PECRYPT, PESHIELD, PROTECT, TINYPROG; oraz plików zabezpieczontch przez CPAV, F-XLOCK, PGPROT, VACCINE. Aby ukryć nazwę archiwizera, użyj parametru **N**.

/WA czekaj po skończonym teście jeśli wirus lub podejrzany obiekt został znaleziony (tylko DrWebWCL)

/? wyświetlenie skróconej pomocy (dla DrWebWCL) lub uruchomienie systemu pomocy (dla DrWeb32W)

Jeśli nie istnieją lub nie są używane pliki INI, domyślnie stosowane są następujące opcje:

/AR /FM /HA /PR /SD /TB /TM /UP.

Niektóre opcje mogą być zakończone znakiem **"-"**. Jest to forma negacji, która wyłącza odpowiednią funkcję lub tryb. Negacja może być użyteczna, jeśli tryb jest włączony domyślnie lub poprzez ustawienia w pliku INI. Negacja może być zastosowana do poniższych opcji linii poleceń:

/AR /CU /FN /HA /IC /OK /PF /PR /SD /SO /SP /TB /TM /UP /WA.

Zauważ, że zaprzeczenie **/CU**, **/IC** oraz **/SP** wyłącza wszystkie akcje uaktywniane przez te opcje. Oznacza to, że informacje o zainfekowanych i podejrzanych plikach będą się pojawiać tylko w pliku raportu.

/AL, **/EX** oraz **/FM** nie mogą być używane w formie negacji. Jednak każda z tych opcji wyłącza dwie pozostałe.

ROZDZIAŁ 10 – KODY ZWRACANE PRZEZ PROGRAM

Kod	Znaczenie kodu
0	- nie znaleziono wirusów
1	- wykryto znanego wirusa
2	- wykryto modyfikację znanego wirusa
4	- wykryto podejrzany obiekt
8	- wykryto znanego wirusa w archiwum
16	- wykryto modyfikację znanego wirusa w archiwum
32	- wykryto podejrzany plik w archiwum
64	- przynajmniej jeden wirus został pomyślnie usunięty
128	- przynajmniej jeden zainfekowany lub podejrzany plik został usunięty/przemianowany/przeniesiony

Rzeczywista wartość zwrócona przez program jest równa sumie kodów, którą można łatwo rozpisać na konkretne kody.

Przykładowo, kod 9 = 1 + 8 oznacza, że wykryte zostały znane wirusy, włącznie z wirusami w archiwach. Leczenie i inne reakcje nie wystąpiły.
Podczas dalszej części testu nie wystąpiły żadne podejrzane zdarzenia.

ROZDZIAŁ 11 - DOWIEDZ SIĘ WIĘCEJ

Antywirusowy program
Program zaprojektowany do walki z wirusami komputerowymi. Oprogramowanie antywirusowe może występować w wielu formach, np.: skaner, inspektor, wartownik, szczepionka, itd.

Wartownik
Sprzęt i oprogramowanie zaprojektowane w celu ochrony danych i obszarów systemowych, przed nieautoryzowaną modyfikacją. Przeważnie jest to karta, instalowana na płycie głównej komputera. Jako przykład takiego rodzaju wartownika można podać system Sheriff..

Nie rezydentna szczepionka
Program modyfikujący plik lub boot sektor, w celu zapobiegania lub wykrywania infekcji wirusów. Szczepienia można stosować przeciwko konkretnym wirusom (np. poprzez zmianę pliku tak, aby wirus myślał, że jest on już zainfekowany) oraz przeciwko wszystkim wirusom. W takim przypadku, szczepionka musi posiadać zdolność wykrywania i informowania o modyfikacji szczepionego obiektu. Niektóre szczepionki mogą leczyć zainfekowane obiekty.

Rezydentna szczepionka
Program rezydujący w pamięci, imitujący infekcję systemu i w ten sposób zapobiegający rzeczywistym atakom wirusów. W przeciwieństwie do nie rezydentnych szczepionek, ich rezydentne odpowiedniki oddziałują na system operacyjny, nie zaś na indywidualnie obiekty.

Boot-wirus
Wirus wykorzystujący boot sektory dysków do rozmnażania się. Dyskietki posiadają tylko jeden *boot sektor*, podczas gdy dyski twarde – dwa. Pierwszy to *boot sektor* logicznej partycji, natomiast drugi - *master boot record* (MBR) fizycznego dysku.

Wirus towarzyszący (satelita)
Wirus korzystający z następującej techniki infekowania. Dla pliku uruchamialnego (np. EXE), wirus tworzy plik "bliźniaczy" (np. plik COM), który jest uruchamiany zamiast oryginalnego.

Wirus komputerowy
Nie istnieje precyzyjna definicja wirusa komuterowego. Ogólnie, można powiedzieć, że jest to program posiadający zdolność reprodukowania swoich kopii (często z modyfikacjami), które również mogą się rozmnażać. Termin "wirus komputerowy" został po raz pierwszy użyty w roku 1984 przez F.Cohen'a.

Wirus sieciowy
Jest to wirus rozprzestrzeniający się w sieciach komputerowych. Niektóre wirusy podróżują w sieciach lokalnych (np. Novell NetWare), inne rozsyłają się poprzez Internet. Wszystkie znane wirusy sieciowe wykorzystują błędy w sieciowym oprogramowaniu. Dlatego, mimo usunięcia wirusów z sieci, nie mamy gwarancji, że oprogramowanie jest wolne od błędów, które mogą zostać wykorzystane przez nowe bakcyle.

Wirus plikowy-boot (łączony)
Wirus posiadający właściwości wirusa plikowego i boot-wirusa.

Wirus zaszyfrowany
Wirus korzystający ze specjalnego algorytmu szyfrującego jego kod, co uniemożliwia deasemblację i analizę. Wirusy takie zawsze posiadają sekcję deszyfrującą, która nie jest zaszyfrowana lub jest zaszyfrowana tylko częściowo. W tym ostatnim przypadku, kod deszyfratora jest rozkodowywany w momencie uaktywnienia się wirusa. Istniejące wirusy korzystają z różnych kluczy szyfrujących. Wirusy takie mogą tworzyć potomków zaszyfrowanych różnymi metodami. Wirusy zaszyfrowane posiadające różne klucze szyfrujące, to już w połowie wirusy polimorficzne.

Robak
Wirus, który nie korzysta z innych plików w celu rozprzestrzeniania się. Robaki rozmnażają się samodzielnie, jednak mogą wykorzystywać błędy w innych programach (było tak w przypadku wirusa Morris).

Konstruktor wirusów
Specjalne środowisko programistyczne, umożliwiające tworzenie wirusów komputerowych. Zazwyczaj, programista może określić parametry wirusa, takie jak jego typ i częstotliwość atakowania. Istnieją konstruktory praktycznie dla każdego typu wirusów, włącznie z polimorficznymi i makrowirusami.

Makrowirus
Wirus napisany w języku używanym przez popularne edytory tekstu i arkusze kalkulacyjne. Szczególnie "popularne" i rozpowszechnione są makrowirusy atakujące dokumenty programu Microsoft Word. Istnieją również wirusy, których celem są: Microsoft Excel, Microsoft Access, Microsoft PowerPoint, a nawet System Pomocy Windows. Wirusy te pisane są w językach Word Basic oraz Visual Basic.

Makro
Program napisany w specjalnym języku (takim jak Word Basic lub Visual Basic), wykorzystywany przez niektóre zaawansowane edytory tekstu i arkusze kalkulacyjne.

Wirus ukrywający się (stealth)
Niektóre wirusy używają specjalnych sztuczek aby ukrywać swoją obecność i w ten sposób unikać wykrycia. Zakłócają one informacje o zainfekowanych obiektach, przejmując kontrolę nad dostępem do tych obiektów. Wirusy ukrywające się to ciężki orzech do zgryzienia dla programów antywirusowych. Jednak nie dla ADinf, który wykrywa je bez problemu.

Wirus polimorficzny
Polimorfizm to zdolność wirusów do tworzenia potomków całkowicie różniących się od oryginałów. Istnieje kilka poziomów polimorfizmu wirusów.

Trojan (koń trojański)
Program, który z pozoru wykonuje żądane i pożyteczne funkcje, jednak posiada również szkodliwe procedury.

Skaner antywirusowy
Program, który potrafi wykrywać i eliminować wirusy komputerowe. Najczęściej, skanery korzystają ze specjalnej bazy danych, która zawiera informacje znanych wirusach. Ponadto, nowoczesne skanery wyposażone są w analizator heurystyczny, umożliwiający wykrywanie nie znanych jeszcze wirusów. Przykładem skanera antywirusowego jest Doctor Web.

Inspektor antywirusowy
Program utrzymujący integralność danych, zapisanych na dyskach twardych. Inspektor kontroluje integralność plików, boot sektorów oraz obszarów systemowych i zgłasza każdą ich zmianę. Jeśli zostaną zmienione, niektóre z tych obiektów (na przykład boot sektory) mogą być odtworzone przez samego inspektora, bez pomocy innych programów antywirusowych. Ponadto, inspektor może być zastosowany wraz ze specjalnym modułem leczącym, posiadającym zdolność naprawiania plików o określonych typach. Podczas sprawdzania integralności danych, inspektor korzysta ze specjalnych tabel, zawierających tzw. sumy kontrolne, obliczane przez specjalne algorytmy. Przykładem inspektora jest ADinf. Program ten spełnia wszystkie wymagania stawiane nowoczesnym inspektorom. Potrafi czytać bezpośrednio z sektorów dysku, dzięki czemu żadne sztuczki ukrywające, stosowane przez wirusy, nie stanowią dla niego problemu. Ponadto, ADinf może kontrolować integralność plików przy użyciu różnych sum kontrolnych, włącznie z bazującym na CRC, wiarygodnym algorytmem LAN64. ADinf może być używany wraz z własnym modułem leczącym.

Wartownik antywirusowy
Program rezydujący w pamięci, monitorujący operacje wykonywane przez inne programy. Wartownik kontroluje operacje, które często są wykonywane przez wirusy komputerowe i informuje użytkownika o wystąpieniu takich operacji (na przykład modyfikacji boot sektora).

Program goat
Mały program testowy, celowo zainfekowany w celu przechwycenia kodu wirusa.

Sygnatura
Sekwencja bajtów, charakterystyczna (teoretycznie unikalna) dla konkretnego programu. Skanery antywirusowe używają sygnatur podczas wykrywania wirusów.

Suma kontrolna

Numeryczna wartość, obliczona dla pliku przez specjalny algorytm. Gdy plik się zmienia, zmienia się również jego suma kontrolna. Programy antywirusowe typu inspektor, używają sum kontrolnych podczas sprawdzania integralności danych.

Poziomy polimorfizmu

Różne wirusy polimorficzne mogą być wykrywane i usuwane przez algorytmy o różnym stopniu skomplikowania. Na przykład, prosty wirus polimorficzny może być wykryty poprzez sprawdzenie maski, podczas gdy bardziej skomplikowane wirusy są wykrywane przy użyciu całkiem innych algorytmów. Istnieje pięć poziomów polimorfizmu.

Odmiana (wariant) wirusa

Modyfikacja oryginalnego wirusa. Odmiany pojawiają się w zależności od dostępności źródłowego kodu wirusa.

Analizator heurystyczny

Narzędzie programistyczne, zaprojektowane w celu wykrywania fragmentów kodu, charakterystycznych dla wirusów komputerowych. Analizator heurystyczny jest stosowany do wykrywania nieznanych jeszcze wirusów. Wydajność analizatora heurystycznego zależy od dwóch parametrów: procentowej ilości wykrytych wirusów i procentowej ilości fałszywych alarmów. Analizator heurystyczny, w który wyposażony jest Doctor Web, jest jednym z najlepszych na świecie tego typu narzędzi.

Emulator CPU

Narzędzie programistyczne, emulujące instrukcje CPU (procesora). Emulacja CPU jest wykorzystywana przez skanery antywirusowe, podczas wykrywania wirusów polimorficznych.

ROZDZIAŁ 12 – TWÓRCY PROGRAMU DOCTOR WEB

11.1. Zespół programistów

Igor Daniloff, Vsevolod Lutovinov, Dmitry Belousov, Andrew Basharimov, Serge Popov

11.2. Oficjalny przedstawiciel w Polsce

DrWeb Polska

Adres: ul. Owocowa 4; 61-306 Poznań

Telefon: +48 61 8727008, +48 61 8727065

Telefon komórkowy: +48 602 479854

WWW: http://www.drweb.com.pl

Biuro: biuro@drweb.com.pl

Wsparcie techniczne: support@drweb.com.pl