Ogólne informacje

SpIDer jest rezydentnym programem antywirusowym (narzędzia tego typu są nazywane “strażnikami” lub “wartownikami”), 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 został zaprojektowany dla 32-bitowych systemów Windows. Ta wersja może pracować w systemach Windows 95, OSR2, 98, NT oraz 2000. Szczegółowe informacje na temat programu SpIDer dla Windows NT, znajdują się w pliku SPIDERNT.TXT, załączonym do pakietu. PROSZĘ PRZECZYTAĆ ZAWARTOŚĆ TEGO PLIKU PRZED PRZYSTĄPIENIEM DO KORZYSTANIA Z PROGRAMU!

Możesz skonfigurować program SpIDer tak, aby odpowiadał Twoim wymaganiom. Aby poznać szczegóły, przeczytaj kolejne rozdziały. Generalnie, konfiguracja programu SpIDer składa się z poniższych kroków:

- SpIDer może wybierać pliki do sprawdzenia, ze względu na ich wewnętrzną strukturę lub ich rozszerzenia. Wybierz jak SpIDer ma wybierać pliki.
- W większości przypadków, SpIDer może z powodzeniem leczyć zainfekowane pliki. Jednak, niektóre wirusy niszczą pliki tak bardzo, że niemożliwe jest ich wyleczenie. Wybierz w jaki sposób SpIDer ma traktować wyleczalne i niewyleczalne pliki.
- SpIDer jest wyposażony w analizator heurystyczny i analizator aktywności wirusów. Narzędzia te umożliwiają wykrywanie nie znanych jeszcze wirusów. Określ jak SpIDer ma reagować gdy wystąpi podejrzane zdarzenie.
- SpIDer zapisuje raport. Określ właściwości raportu.
- Możesz także uaktywnić kilka dodatkowych opcji — na przykład, wyłączyć wybrany folder z testu.

{button Okna Ustawieďž˝,JI(`',`HIDR_MAINFRAME')}.

System Pomocy

Jeśli nie zaznajomiłeś się jeszcze z programem SpIDer, naciśnij {button Ogďż˝lne Informacje,JI(`',`ABOUT')}.

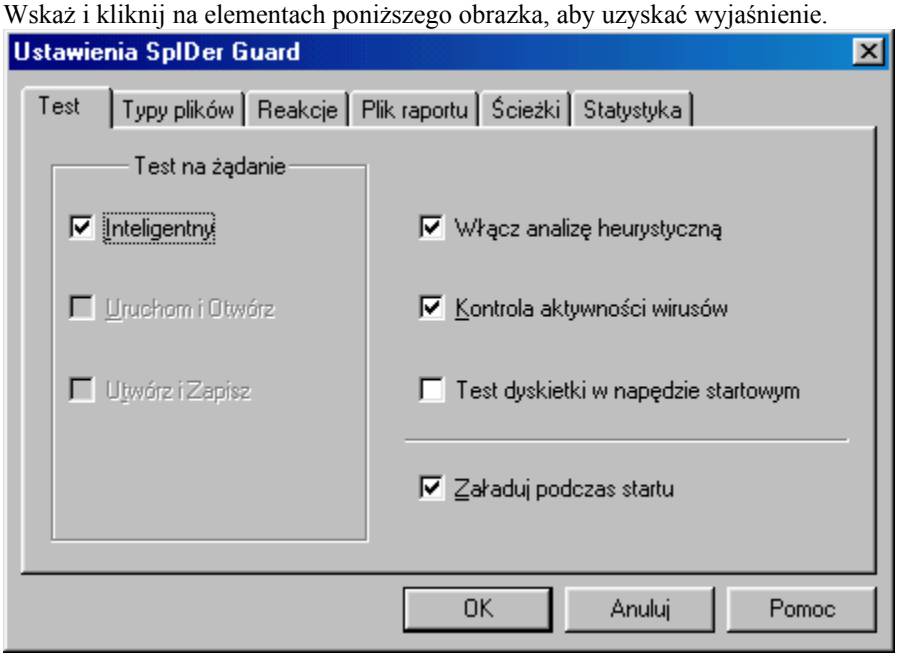
Ta sekcja opisuje okna ustawień, przy użyciu których możesz konfigurować program SpIDer.
Możesz uzyskać szczegółową pomoc na konkretnych oknach:
— podczas oglądania tej strony, klikając na nazwie okna w tekście poniżej;
— podczas oglądania zawartości pomocy, otwierając odpowiednią sekcję;
— podczas pracy z programem SpIDer, klikając na przycisku pomocy (“?”).
Wszystkie opcje konfiguracyjne są pogrupowane w następujących oknach ustawień:
— tryby sprawdzania, ***Okno Tryby Sprawdzania***;
— wybór plików do sprawdzenia, ***Okno Typy Plików***;
— reakcje na wyleczalne, niewyleczalne i podejrzane pliki, ***Reakcje***;
— opcje raportu, ***Raport***;
— foldery, które mają być pomijane podczas sprawdzania oraz lokacja głównych/dodatkowych baz antywirusowych, ***Lokacje***.
Rezultaty działania programu SpIDer są wyświetlane w oknie ***Statystyka***.

SpIDer został stworzony przez: ***ID Antivirus Lab***.
Oficjalny dystrybutor: ***DialogueScience, Inc.***

Okno Tryby Sprawdzania

W tym oknie możesz określić ogólne opcje programu.

Wskaż i kliknij na elementach poniższego obrazka, aby uzyskać wyjaśnienie.



{button Lista okien,JI(`',`HIDR_MAINFRAME')}.

Ten przycisk **zapisuje** wszystkie zmiany i zamyka to okno. Jednak, nowe ustawienia będą aktywne dopiero po ponownym uruchomieniu komputera.

Ten przycisk **ignoruje** wszystkie zmiany i zamyka to okno.

Ten przycisk wywołuje pomoc kontekstową.

Ten panel określa tryb pracy programu SpIDer.

Jeśli uaktywniony jest **Optymalny** Tryb Sprawdzania, SpIDer wykonuje test tylko w określonych przypadkach. Ta wersja sprawdza:
— pliki na lokalnych dyskach twardych, tylko podczas ich odczytywania/zapisywania (uruchamiane programy nie są sprawdzane, ponieważ uruchomienie otwiera je w trybie tylko do odczytu);
— pliki na dyskach sieciowych, zawsze gdy są otwierane (zarówno w trybie tylko do odczytu, jak również do odczytu i zapisu);
— pliki na dyskietkach wymiennych, zawsze gdy są otwierane (zarówno w trybie tylko do odczytu, jak również do odczytu i zapisu).

Jeżli ten tryb jest uaktywniony, SpIDer sprawdza **wszystkie uruchamiane programy i pliki otwierane w trybie tylko do odczytu**. Zwróć uwagę, że uruchomienie zestawu “ADinf32+DrWeb32”, spowoduje niepotrzebne, dwukrotne sprawdzanie tych samych plików.

Jeżli ten tryb jest uaktywniony, SpIDer sprawdza **nowe pliki podczas ich tworzenia** oraz **istniejące pliki podczas ich otwierania w trybie do odczytu i zapisu**. Uruchamiane programy nie są sprawdzane.

Ta opcja aktywuje **analizator heurystyczny**, który wykrywa nie znane jeszcze wirusy.

Ta opcja aktywuje **analizator aktywności wirusów**, który zabezpiecza pliki przed zainfekowaniem przez znane i nie znane jeszcze wirusy (nawet jeżeli nie zostały wykryte przez analizator heurystyczny). W tym trybie, możesz wyłączyć operację zapisywania do pliku (pamiętaj jednak, że niektóre wirusy rezydentne mogą uszkodzić wynikowy plik).

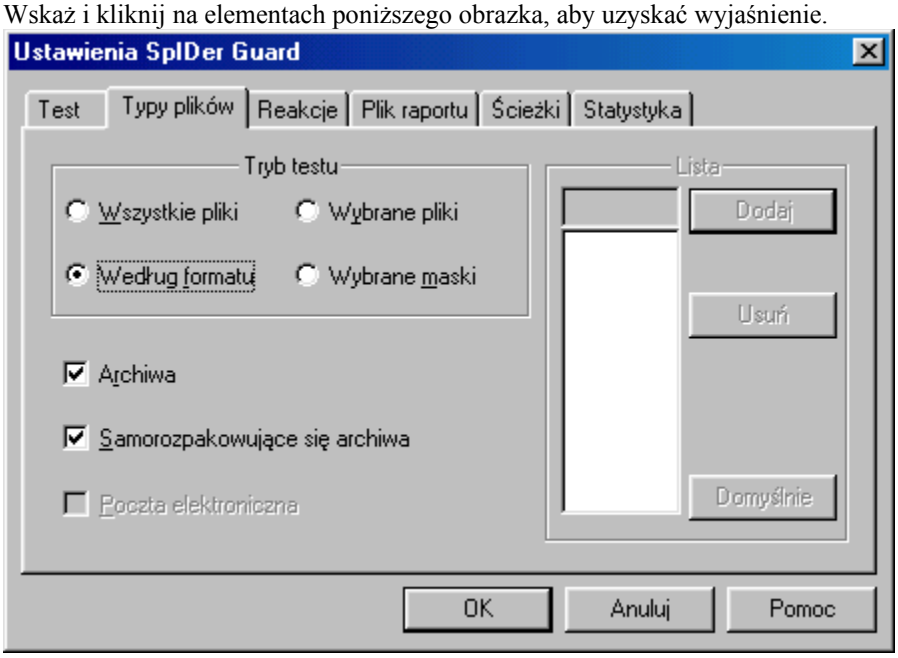
Jeśli ta opcja jest zaznaczona, SpIDer testuje dyskietkę (jeśli znajduje się w stacji dyskietek) podczas każdego zamykania systemu. Opcja ta może zapobiec rozprzestrzenieniu się wirusa z dyskietki.

Ta opcja powoduje uruchomienie programu SpIDer podczas następnego startu systemu. W przeciwnym wypadku, SpIDer nie zostanie uaktywniony po zresetowaniu komputera.

Okno Typy Plików

W tym oknie możesz określić jak SpIDer ma wybierać pliki do sprawdzenia.

Wskaż i kliknij na elementach poniższego obrazka, aby uzyskać wyjaśnienie.



{button Lista okien,JI(`',`HIDR_MAINFRAME')}.

Ten panel określa kategorię plików do sprawdzenia.

Jeśli ta opcja jest zaznaczona, SpIDer **zawsze** sprawdza plik, niezależnie od jego rozszerzenia i wewnętrznego formatu.

Jeśli ta opcja jest zaznaczona, SpIDer sprawdza pliki ze względu na ich **wewnętrzny format** (niezależnie od rozszerzenia).

Jeśli ta opcja jest zaznaczona, SpIDer sprawdza plik jeśli jego **rozszerzenie** znajduje się na sąsiadującej liście. Możesz edytować tą listę (np. dodawać lub usuwać rozszerzenia.)

Jeśli ta opcja jest zaznaczona, SpIDer sprawdza plik jeśli jego **nazwa i rozszerzenie** pasują do zdefiniowanych przez użytkownika masek, znajdujących się na sąsiadującej liście. Opcja ta może znacznie skrócić całkowity czas sprawdzania (na przykład, jeśli chcesz sprawdzić tylko pliki programu Microsoft Word (pliki DOC i DOT), które pasują do maski DO?.)

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

Jeśli ta opcja jest zaznaczona, SpIDer sprawdza także zawartość archiwów. Ta wersja działa z archiwami ZIP, ARJ, oraz RAR.

Jeśli ta opcja jest zaznaczona, SpIDer sprawdza archiwa samo rozpakowujące się. W rzeczywistości, SpIDer rozpakowuje je i sprawdza poszczególne pliki. Metoda ta wykrywa wirusy w plikach, które zostały zainfekowane przed spakowaniem..

Jeśli ta opcja jest zaznaczona, SpIDer sprawdza **pliki wiadomości e-mail**, zakodowane w UUENCODE oraz MIME.

Te przyciski dodają i usuwają elementy z listy.

To okienko edycyjne może zawierać **rozszerzenie** lub **maskę** plików, które mają być sprawdzane.

Ten przycisk **dodaje** rozszerzenie lub maskę, której nazwa figuruje w okienku edycyjnym.

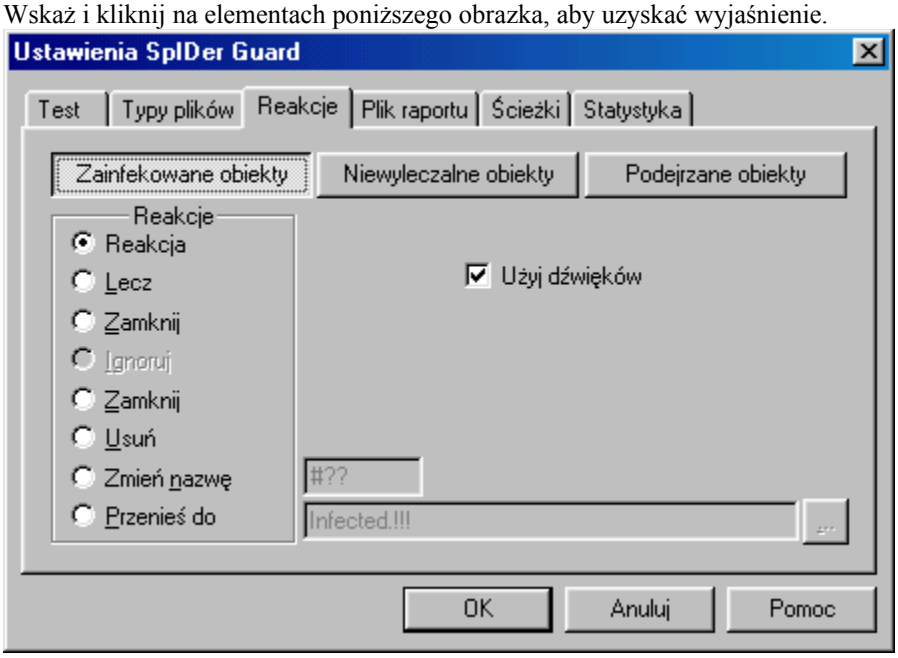
Ten przycisk **usuwa** rozszerzenie lub maskę, której nazwa figuruje w okienku edycyjnym.

Ten przycisk **przywraca** domyślną zawartość listy.

Okno Reakcje

W tym oknie możesz określić jak SpIDer ma reagować na to zainfekowane lub podejrzane obiekty.

Wskaż i kliknij na elementach poniższego obrazka, aby uzyskać wyjaśnienie.



{button Lista okien,JI(`',`HIDR_MAINFRAME')}.

Ten przycisk pozwala wybrać reakcję na **zainfekowane** obiekty, które **mogą być wyleczone**.

Ten przycisk pozwala wybrać reakcję na **zainfekowane** obiekty, które **nie mogą być wyleczone**.

Ten przycisk pozwala wybrać reakcję na **podejrzane** obiekty wykryte przez analizator heurystyczny.

Ta grupa opcji określa reakcję na obiekty wybrane powyżej. Dla niektórych obiektów pewne opcje mogą być nieaktywne..

Jeśli ta opcja jest zaznaczona, SpIDer **tylko sygnalizuje** wykrycie podejrzanego obiektu.

Jeśli ta opcja jest zaznaczona, SpIDer **leczy** podejrzany obiekt.

Jeśli ta opcja jest zaznaczona, SpIDer **wyłącza** interakcję aplikacji z podejrzanym obiektem.

Jeśli ta opcja jest zaznaczona, SpIDer **ignoruje** podejrzany obiekt.

Jeśli ta opcja jest zaznaczona, SpIDer **zawiesza system** po wykryciu podejrzanego obiektu.

Jeśli ta opcja jest zaznaczona, SpIDer **usuwa** podejrzany obiekt.

Jeśli ta opcja jest zaznaczona, SpIDer **zmienia nazwę** podejrzanego obiektu na określoną w sąsiadującym okienku.

Jeśli ta opcja jest zaznaczona, SpIDer **przenosi** podejrzany obiekt do folderu określonego w sąsiadującym okienku.

To okienko edycyjne zawiera maskę, która jest wykorzystywana do zmiany nazwy podejrzanych plików. Użyj symbolu "**?**" aby zachować na danej pozycji znak z oryginalnego rozszerzenia. Mimo iż możesz wprowadzić praktycznie każdą kombinację znaków, unikaj jednak używania standardowych rozszerzeń (DOC, PAS, BAS, itp.)

Do tego **foldera** SpIDer **przenosi** zainfekowane lub podejrzane obiekty. Jeśli nie podasz pełnej ścieżki, folder ten zostanie utworzony w katalogu, w którym zainstalowany jest SpIDer. Możesz użyć tej opcji jeśli chcesz w przyszłości badać podejrzane obiekty lub wysłać je do DialogueScience

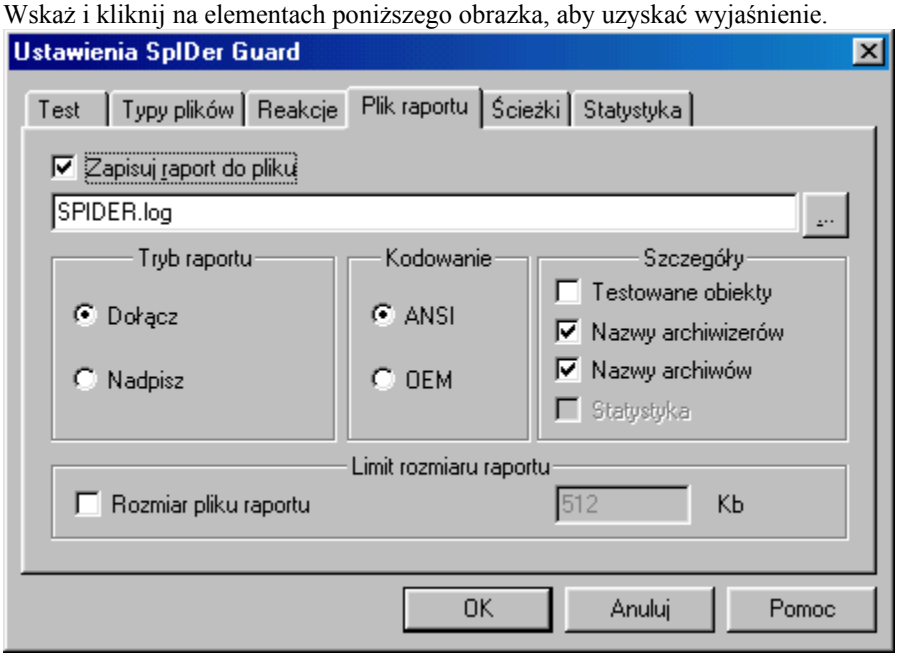
Ten przycisk wyświetla okno “Wybierz folder”.

Jeśli ta opcja jest zaznaczona, SpIDer generuje efekt dźwiękowy w przypadku znalezienia podejrzanego obiektu lub wystąpienia aktywności wirusa.

Okno Raport

W tym oknie możesz określić opcje raportu.

Wskaż i kliknij na elementach poniższego obrazka, aby uzyskać wyjaśnienie.



{button Lista okien,JI(`',`HIDR_MAINFRAME')}.

Ta opcja uaktywnia raport (plik zawierający informacje o wszystkich zainfekowanych, wyleczonych, itp. plikach). Nazwa pliku raportu może być określona w sąsiadującym okienku edycyjnym.

Tutaj możesz określić nazwę pliku raportu.

Ten przycisk wyświetla okno “Wybierz folder”.

Ta grupa opcji określa czy istniejący raport jest nadpisywany, czy też dopisywane są do niego nowe informacje.

Jeśli ta opcja jest zaznaczona, nowe informacje są **dopisywane** do istniejącego raportu (jeśli raport nie istnieje – jest tworzony.)

Jeśli ta opcja jest zaznaczona, istniejący raport jest **nadpisywany**.

Ta grupa opcji określa rodzaj kodowania pliku raportu.

Wybiera kodowanie ANSI dla pliku raportu (strona kodowa Windows).

Wybiera kodowanie OEM dla pliku raportu (strona kodowa DOS).

Tutaj możesz określić szczegółowe informacje, które będą zapisywane w pliku raportu.

Jeśli ta opcja jest zaznaczona, do raportu zapisywane są informacje o **wszystkich** sprawdzanych obiektach. Może to sprawić, że plik raportu będzie bardzo duży.

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.

Jeśli ta opcja jest zaznaczona, do raportu zapisywane są **nazwy narzędzi** (PKZIP, ARJ itp.), które były używane podczas tworzenia archiwów.

Jeśli ta opcja jest zaznaczona, SpIDer zamieszcza w raporcie **statystykę sesji**.

Ta grupa opcji ogranicza rozmiar pliku raportu i określa w jaki sposób raport ma wykorzystywać przyporządkowane mu miejsce na dysku.

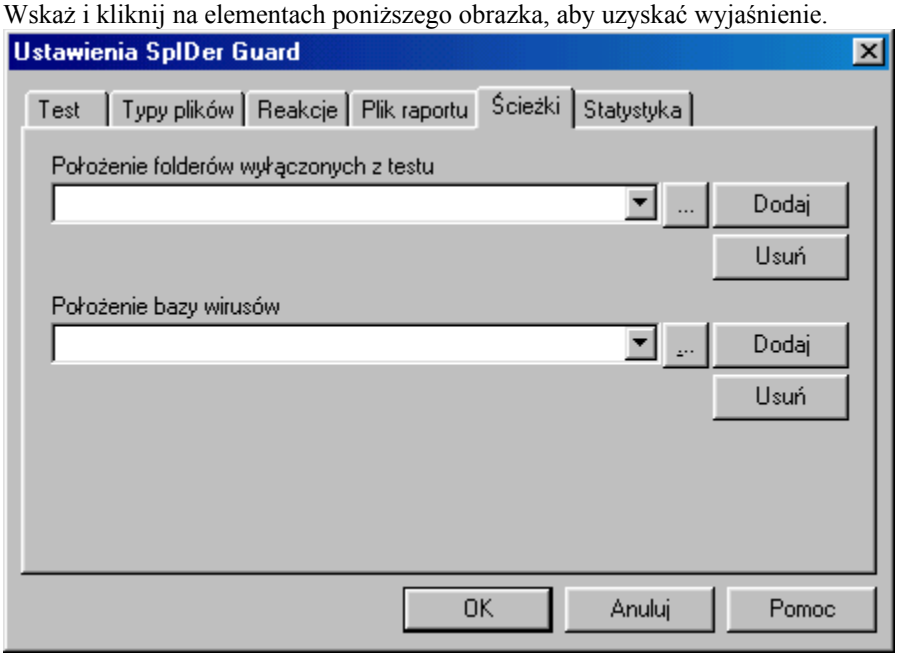
Jeśli ta opcja jest zaznaczona i rozmiar raportu przekroczy limit podany w sąsiadującym okienku, plik raportu jest czyszczony.

To okienko edycyjne zawiera **maksymalny rozmiar raportu**. Pole to jest aktywne tylko, gdy zaznaczona jest sąsiadująca opcja.

Okno Lokacje

W tym oknie możesz wybrać foldery, które nie będą sprawdzane i/lub alternatywną lokację baz antywirusowych.

Wskaż i kliknij na elementach poniższego obrazka, aby uzyskać wyjaśnienie.



{button Lista okien,JI(`',`HIDR_MAINFRAME')}.

Ta grupa opcji wybiera dyski i/lub foldery, które nie będą sprawdzane. Zalecamy UNIKANIE wybierania takich folderów.

To okienko edycyjne zawiera **lokację folderu, który nie będzie sprawdzany**.

Ten przycisk wyświetla okno “Wybierz folder”.

Ten przycisk **dodaje** folder do sąsiadującej listy.

Ten przycisk **usuwa** folder z sąsiadującej listy.

Ta grupa opcji określa **lokację baz antywirusowych**. Standardowo, jest to folder, w którym SpIDer jest zainstalowany (prawdopodobnie znajduje się tam również Doctor Web). Jednak, ponieważ dodatkowe bazy są uaktualniane co tydzień, możesz je umieścić na dysku sieciowym, dzięki czemu będą do nich mieli dostęp inni użytkownicy (na przykład pozbawieni dostępu do Internetu).

To okienko edycyjne określa folder, w którym przechowywane są główne i dodatkowe bazy antywirusowe programu Doctor Web.

Ten przycisk wybiera maskę z sąsiadującej listy.

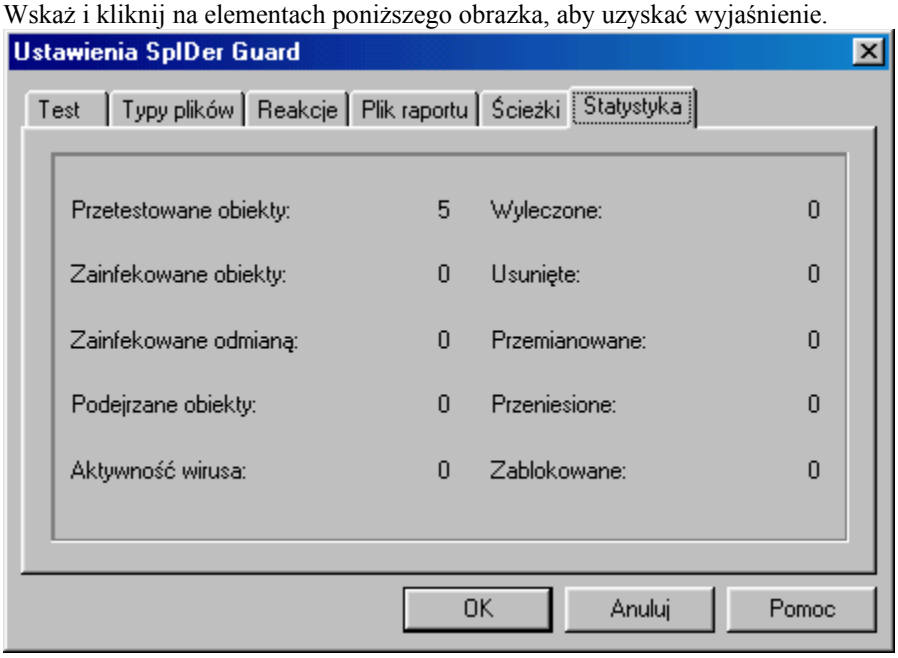
Ten przycisk **dodaje** do listy folder z sąsiadującego okienka edycyjnego.

Ten przycisk **usuwa** z listy folder z sąsiadującego okienka edycyjnego.

Okno Statystyka

To okno wyświetla statystykę bieżącej sesji.

Wskaż i kliknij na elementach poniższego obrazka, aby uzyskać wyjaśnienie.



{button Lista okien,JI(`',`HIDR_MAINFRAME')}.

Całkowita ilość przetestowanych obiektów (plików i boot sektorów).

Całkowita ilość obiektów zainfekowanych znanymi, “standardowymi” wirusami.

Całkowita ilość obiektów zainfekowanych modyfikacjami “standardowych” wirusów

Całkowita liczba podejrzanych obiektów (zgłoszonych przez analizator heurystyczny). Mogą to być obiekty zainfekowane nieznanym wirusem lub obiekty zawierające “podejrzany” kod. Zalecamy sprawdzenie tych obiektów przy użyciu na przykład ADinf32.

Całkowita liczba podejrzanych obiektów (zgłoszonych przez analizator aktywności wirusów). Jeśli wartość ta jest niezerowa, oznacza to, że system jest zainfekowany nieznanym wirusem lub jedna z aplikacji wykonuje “podejrzane” operacje. Zalecamy sprawdzenie tych obiektów przy użyciu na przykład ADinf32.

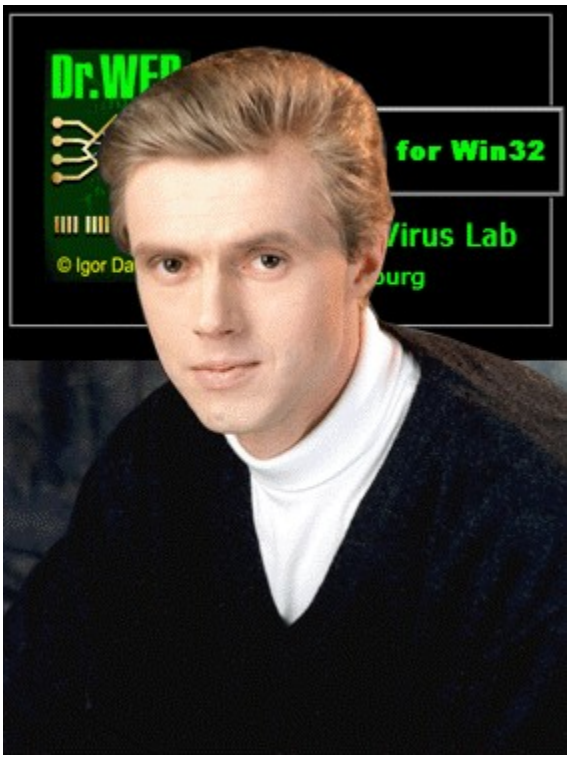
Całkowita liczba wyleczonych obiektów (reakcje na zainfekowane i podejrzane obiekty możesz określić w Oknie Reakcje).

Całkowita liczba usuniętych obiektów (reakcje na zainfekowane i podejrzane obiekty możesz określić w Oknie Reakcje).

Całkowita liczba obiektów, których nazwy zostały zmienione (reakcje na zainfekowane i podejrzane obiekty możesz określić w Oknie Reakcje).

Całkowita liczba przeniesionych obiektów (reakcje na zainfekowane i podejrzane obiekty możesz określić w Oknie Reakcje).

Całkowita liczba zablokowanych obiektów (reakcje na zainfekowane i podejrzane obiekty możesz określić w Oknie Reakcje).



(c) 1992-2001 Igor Daniloff

Zespół programistów:

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

Jak się z nami skontaktować

Adres: ul.Vavilova 40, Moskwa 117786, Rosja.

E-mail: Antivir@Dials.ru – komentarze, sprzedaż, wsparcie techniczne, wiadomości o nowych wirusach

Serwer WWW: http://www.Dials.ru

Oficjalny przedstawiciel w Polsce:

DrWeb Polska s.c.

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

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 plikowy
Wirus dołączający się do plików w celu rozprzestrzeniania się.

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.