Obiekty skanowania

Ta zakładka umożliwia określenie, które obiekty mają być skanowane i warunki wyszukiwania anomalii.

Górna część zakładki zawiera okno *Napędy dysków*. Pozwala ono na wybór napędów, które mają być skanowane. Po wejściu do okna, kursor można przesuwać przy pomocy klawiszy ze strzałkami. By włączyć lub wyłączyć zaznaczenie napędu, użyj klawisza spacji lub dwa razy kliknij lewym przyciskiem myszki. Okno jest podzielone na trzy kolumny:

- *Dysk* – wyświetla ikonę i nazwę dysku
- *Typ* – określa typ dysku
- *Podłączony do* - wyświetla nazwę dysku sieciowego

Na prawo od okna *Napędy dysków* istnieje możliwość dokonania wyboru jednej z opcji.

- *Lokalne* – pozwala na dokonywanie wyboru tylko wśród dysków zainstalowanych lokalnie
- *Sieciowe* – pozwala na dokonywanie wyboru tylko wśród dysków dostępnych poprzez sieć

Poniżej znajdują się dwa przyciski:

- *Wszystkie* – powoduje zaznaczenie wszystkich napędów
- *Wyłącz zaznaczenia* – wyłącza wszystkie zaznaczenia napędów

W oknie *Foldery* , umieszczonym w dolnej części zakładki, wyświetlana jest lista indywidualnie wybranych folderów, które mają być sprawdzane pod względem obecności wirusów. Zawartość listy może być zmieniana przy pomocy dwóch przycisków:

- *Dodaj* – otwiera okno dialogowe służące do dodawania nowych folderów
- *Usuń* – usuwa zaznaczone foldery z listy

Dziennik zdarzeń

Głównym składnikiem zakładki jest okno *Dziennika skanowania,* które prezentuje wyniki wykonanego skanowania. Po zakończeniu skanowania zostaje utworzony zbiór (o domyślnej nazwie: Nod32.log), który zawiera istotne informacje na temat stanu skanowania i jego zaawansowania.

Wybranie opcji *Przeglądaj dziennik zdarzeń* (lewy dolny róg zakładki) powoduje, że wszystkie nowe wpisy do dziennika są wyświetlane w dolnej części okna a wcześniejsze wpisy przesuwane automatycznie do góry. W przypadku wyłączenia opcji, automatyczne przewijanie dziennika nie będzie miało miejsca. Niezależnie od wybranej opcji, całość wpisów można przeglądać wykorzystując strzałki przewijania na prawej ramce okna.

Poszczególne rodzaje wpisów do dziennika są wykonywane różnymi kolorami. Informacje o nie zainfekowanych plikach są wykonywane w kolorze czarnym, obiekty zainfekowane są oznaczane kolorem czerwonym, informacje o błędach w dostępie do danych obiektów kolorem niebieskim a komunikaty o zbiorach usuniętych, oczyszczonych z wirusów oraz takich, których nazwa została zmieniona w kolorze brązowym.

W dolnym prawym rogu zakładki wyświetlany jest numer używanej wersji programu.

Czynności

Ta zakładka określa jakie czynności mają być wykonywane po wykryciu wirusa

Zakładka zawiera dwie niezależne sekcje: *Zbiory* oraz *Sektory Boot i MBR*

Lewa część sekcji *Zbiory* zawiera przełącznik *Po wykryciu wirusa*, który posiada następujące pozycje:

Lewa część sekcji *Zbiory* zawiera przełącznik *Po wykryciu wirusa,* który posiada następujące pozycje:

- *usuń wirusa* – powoduje automatyczne usunięcie wirusa z zainfekowanego zbioru
- *zaproponuj rozwiązanie* – wyświetla panel zawierający propozycje sugerowanych czynności w danej sytuacji
- *pozostaw bez zmian* – pozostawia zbiór bez dokonywania żadnych zmian
- *zmień nazwę* – zmienia nazwy wszystkich zainfekowanych zbiorów
- *usuń zbiór* – usuwa wszystkie zainfekowane zbiory

Przełącznik *Wirusy niemożliwe do usunięcia,* umieszczony po prawej stronie posiada te same pozycje co przełącznik *Po wykryciu wirusa*, oprócz jednej *usuń wirusa*. Opcje oferowane przez przełącznik są dostępne tylko wtedy kiedy NOD nie jest w stanie naprawić zainfekowanego zbioru. Przełącznik jest dostępny tylko w przypadku wybrania opcji automatycznego usuwania wirusów.

Sekcja sektorów *Boot* lub *MBR*, zlokalizowana w dole zakładki zawiera podobne przełączniki jak sekcje opisane powyżej. Jednakże opcje zmień nazwę i usuń zbiór, są tutaj zastąpione przez jedną opcję:

- *zastąp* – zastępuje zainfekowane wirusem rekordy boot sektora czystym standardowym kodem

Sieć

Ta zakładka służy do ustawiania parametrów związanych z siecią komputerową i parametrów Centralnej aktualizacji programu.
Składa się ona z trzech opisanych poniżej sekcji:

W górnej części sekcji *Komunikatów sieciowych* znajduje się możliwa do wybrania opcja *Wyślij komunikat o przedostaniu się wirusów do sieci.* Jeżeli opcja zostanie wybrana, to po wykryciu wirusa, NOD32 wyśle komunikat do określonej wcześniej grupy użytkowników. Lista użytkowników, którzy będą otrzymywać komunikaty jest wyświetlona w oknie poniżej.

Aby dodać do listy nowych adresatów komunikatu kliknij na przycisk *Dodaj*. Nazwa stacji lub grupy komputerów może zostać wprowadzona w oknie dialogowym. Jeżeli zamiast nazwy użyjemy gwiazdki, komunikat zostanie wysłany do wszystkich członków grupy do której należy stacja.

Aby usunąć pozycję z listy, najedź na nią myszką, kliknij by ją zaznaczyć i wciśnij klawisz (DEL) na klawiaturze lub przycisk *Usuń* na ekranie. Wciśnięcie przycisku *Test* powoduje natychmiastowe sprawdzenie czy opcja wysyłania komunikatu działa poprawnie.

Treść komunikatu można wprowadzić w oknie dialogowym *Format wiadomości*. Miejsce, w którym ma się pojawić nazwa wykrytego wirusa należy oznaczyć parametrem <virus> tak jak zostało to zrobione w oryginalnej przykładowej wiadomości.

Ostrzeżenie: W przypadku kiedy używany jest system operacyjny Windows®95 (98), na stacjach które mają otrzymywać komunikaty o przenikaniu wirusów, musi być uruchomiony program Winpopup (standardowy składnik systemu Windows). W przypadku wykrycia przez NOD32 dużej ilości wirusów przenikających do sieci, przesyłany jest tylko komunikat dotyczący pierwszego z nich. Zabezpiecza to przed ewentualnym przeciążeniem systemu spowodowanym zbyt dużą ilością przesłanych w krótkim czasie komunikatów.

Informacje wprowadzone w tej zakładce można zabezpieczyć hasłem. W tym celu wybierz opcję *Zabezpiecz zakładkę hasłem,* wciśnij przycisk *Hasło* i wprowadź jego treść.

Setup

Zakładka jest wykorzystywana do ustawiania podstawowych parametrów użytkowych programu. Zawiera jeden przycisk i sześć sekcji dających możliwość dokonania wyboru wielu opcji.

Sekcja *Obiekty do sprawdzania* zawiera opcje:
- *Zbiory* – włącza skanowanie wykonywalnych zbiorów i zbiorów zawierających makra
- *Boot sektory* – włącza skanowanie boot sektorów dysków logicznych
- *Sektory MBR* – włącza skanowanie głównego boot sektora dysku

Sekcja *Czułość analizy heurystycznej* zawiera przełącznik z opcjami:
- *Podstawowa* – minimalizuje liczbę fałszywych alarmów
- *Standardowa* – optymalna w większości przypadków
- *Wysoka* – zapewnia maksymalną czułość analizy

Sekcja *Metody skanowania* zawiera cztery opcje:
- *Sygnatury* – uruchamia wykrywanie specyficznych elementów kodu wirusa (sygnatur)
- *Analiza heurystyczna* – uruchamia analizę heurystyczną kodu plików
- *Pliki spakowane* – sprawdza czy zbiory utworzone przez programy pakujące nie zawierają wirusów (np. PKLite, LZExe, Diet, etc.)
- *Archiwum* – poszukuje wirusów w skompresowanych archiwach (np. ZIP, ARJ, etc.)

Sekcja *Dziennik skanowania* zawiera kilka elementów. W górnej części można wybrać jedną z opcji:
- *Włączony* – powoduje zapisywanie treści dziennika zdarzeń na dysku
- *Przewijaj dziennik zdarzeń* – powoduje automatyczne przewijanie treści dziennika

Poniżej znajduje się przełącznik służący do wybierania sposobu dokonywania nowych wpisów w dzienniku zdarzeń:
- *Dołącz* – nowy wpis do dziennika zostanie dołączony do poprzednich (jeżeli istnieją)
- *Przepisz* – nowy wpis do dziennika zawsze zastępuje dotychczasowe

Dwa pola dają możliwość określenia następujących parametrów:
- *Maksymalny rozmiar* –określa maksymalny rozmiar dziennika w kB
- *Nazwa* – można tutaj określić nową nazwę zbioru dziennika, jeżeli nazwa domyślna “Nod32.log” musi zostać zmieniona

Sekcja *System* zawiera dwie opcje:
- *Wyświetl wszystkie zbiory* – pełna lista skanowanych zbiorów pojawi się w dzienniku zdarzeń, nawet jeżeli nie były one zainfekowane
- *Sygnał dźwiękowy* – w przypadku wykrycia wirusa zostanie wygenerowany sygnał dźwiękowy

Sekcja konfiguracji zawiera trzy przyciski:
- *Zapisz* – zapisuje aktualną konfigurację
- *Wczytaj* – wczytuje zapisaną konfigurację
- *Domyślna* – przywraca konfigurację domyślną

W prawej dolnej części zakładki znajduje się przycisk *Rozszerzenia*. Umożliwia on edycję rozszerzeń zbiorów, które mają być skanowane.

Kontakt

ESET, LLC
4025 Camino del Rio South
Suite 300
San Diego, CA 92108
Phone: (619) 542-7872
Fax: (619) 542-7701
E-mail: eset@nod32.com
www.nod32.com

dystrybutor w Polsce:
DAGMA sp. z o.o.
Ul. Pszczyńska 15
40-478 Katowice
Poland
Tel: +48-32-202 11 22
Fax: +48-32-202 55 55
E-mail: nod32@dagma.pl
www.dagma.pl

Panel dodawania folderów

W górnej części panelu znajduje się pole, w którym można wprowadzać ścieżki do nowych folderów, które mają zostać dodane do listy folderów przeznaczonych do skanowania

Panel zawiera trzy przyciski:

- *OK* – dodaje folder do listy
- *Anuluj* – zamyka panel bez dokonania żadnych zmian
- *Przeglądaj* – uruchamia standardowy dialog z systemem umożliwiający wybór foldera spośród znajdujących się na dysku (dyskach)

Informacje o programie

NOD32

Edytor rozszerzeń

Edytor rozszerzeń służy jako narzędzie do określania typów rozszerzeń zbiorów, które mają być skanowane na obecność wirusów.

Aktualna lista rozszerzeń jest w porządku alfabetycznym wyświetlona w lewej części okna.

Pięć przycisków w prawej części okna uruchamia następujące funkcje:

- *OK* – kończy edycję listy rozszerzeń i ją zapisuje
- *Anuluj* – kończy edycję listy rozszerzeń bez dokonywania jakichkolwiek zmian
- *Dodaj* – dodaje rozszerzenie do listy wyświetlonej w oknie
- *Usuń* – usuwa z listy rozszerzenia zaznaczone kursorem
- *Domyślna* – kasuje aktualną listę rozszerzeń i zastępuje ją programową listą domyślną

W dolnej części okna znajduje się opcja *Skanuj wszystkie zbiory*. Jeżeli jest zaznaczona, to skanowane są wszystkie pliki niezależnie od ich rozszerzenia. W tym przypadku lista rozszerzeń oraz przyciski Dodaj i Usuń przestaną być dostępne. Wybór tej opcji w standardowych warunkach nie jest zalecany.

By dodać nowe rozszerzenie do listy sprawdzanych zbiorów wciśnij przycisk *Dodaj*. Powoduje to otwarcie okna, w którym można wpisać nowe rozszerzenie (maksymalna długość to 10 znaków). Następnie kliknij na przycisk OK by go dodać do listy.

Zaktualizowana lista rozszerzeń zbiorów, które mają być skanowane zostanie zapisana po wciśnięciu przycisku *Zapisz* w zakładce *Setup.*

Panel wykrytego wirusa

Górna część panelu wyświetla przewijające się okno z informacją o zbiorze, w którym wykryto wirusa. Wyświetlone są również dodatkowe informacje, takie jak: nazwa i charakterystyka wirusa, oraz czy może on być usunięty przy pomocy tego programu.

Sekcja *Zainfekowany zbiór* zawiera cztery przyciski:
- *Pozostaw bez zmian* – pozostawia zbiór bez dokonywania zmian
- *Usuń wirusa* – powoduje usunięcie wirusa ze zbioru
- *Zmień nazwę* – zmienia nazwę zbioru zawierającego wirusa by zapobiec jego przypadkowemu uruchomieniu
- *Usuń* – usuwa zainfekowany zbiór

W przypadku przeniknięcia wirusa do boot sektora, nazwa sekcji zmienia się na: *Zainfekowany boot sektor* i wyświetlają się trzy przyciski:
- *Pozostaw bez zmian* – pozostawia boot sektor bez dokonywania żadnych zmian
- *Usuń wirusa* – uruchamia proces usuwania wirusa
- *Zastąp* – zastępuje zainfekowane rekordy boot sektora standardowym kodem

Sekcja *Czynności w przypadku kolejnych zainfekowanych zbiorów (lub boot sektorów)* zawiera przycisk *Setup*, który powoduje wyświetlenie zakładki *Setup*. Ten przycisk jest wykorzystywany jeżeli chcemy określić czynności jakie mają być wykonywane po wykryciu wszystkich kolejnych wirusów.

Dolna część panelu zawiera jeden przycisk:
- *Zakończ skanowanie* – powoduje on natychmiastowe przerwanie procesu skanowania

Spis treści