Główne okno

To jest główne kontrolne i informacyjne okno AMON-a – rezydentnego programu monitorującego wirusy. AMON zajmuje się stałym, automatycznym wykrywaniem zagrożeń wirusowych niezależnie od ich źródła (dyskietka, internet, etc.).

Pulsujące logo NOD w lewym górnym rogu ekranu oznacza, że program pracuje w trybie domyślnym. W tym trybie wszystkie obiekty (dyskietki, boot sektory, zbiory) są automatycznie sprawdzane na obecność wirusów.

Aby wyłączyć skanowanie kliknij na pulsujące logo. Logo przestanie migać a program zawiesi skanowanie. Aby powrócić do stanu poprzedniego i ponownie uruchomić skaner wirusów kliknij dwukrotnie na logo (logo ponownie zacznie pulsować).

Tryb, w którym skaner jest wyłączony został przygotowany dla specyficznych celów i stosunkowo rzadkich sytuacji. Dlatego aktywny tryb skanowania jest automatycznie przywracany przy każdym uruchomieniu systemu.

Prawa strona Głównego okna zawiera zestaw czterech przycisków uruchamiających następujące funkcje:
- *Ukryj* – zamyka główne okno pozostawiając uruchomiony program
- *Setup* – wyświetla okno konfiguracji
- *Odinstaluj* – kończy pracę programu
- *Pomoc* – otwiera okno pomocy

W lewym dolnym rogu wyświetlone są ważne informacje na temat:
- Liczby testowanych zbiorów
- Liczby zainfekowanych zbiorów
- Liczby zbiorów, z których usunięto wirusy
- Nazwy ostatniego sprawdzanego zbioru
- Wersji programu

Obiekty

Zakładka Obiekty pozwala na określenie, które obiekty mają być skanowane (typy zbiorów, nośniki, boot sektory, etc.) oraz jakie warunki muszą być spełnione by do tego doszło.

Zakładka składa się z dwóch sekcji: *Zbiory* oraz *Skanuj boot sektory podczas*

Sekcja Zbiory zawiera trzy grupy opcji i jeden przycisk. Pierwsza z nich zawiera następujące pozycje:
- *Zbiory wykonywalne* – skanowanie wykonywalnych zbiorów typu (COM, EXE, DLL, VXD, BAT, ...)
- *Dokumenty* – skanowanie dokumentów i arkuszy roboczych, które mogą zawierać makra

W grupie *Skanuj* można określić by skanowanie zbiorów miało miejsce gdy następuje ich:
- *Otwarcie*
- *Zmiana nazwy*
- *Uruchomienie*
- *Tworzenie*

Grupa *Nośniki* pozwala na dokładne określenie jakie napędy dyskowe mają być skanowane:
- *Dyskietki*
- *Lokalne* – wszystkie stałe i wymienne dyski lokalne za wyjątkiem dyskietek
- *Sieciowe* – dyski dostępne za pośrednictwem sieci

Przycisk *Rozszerzenia* otwiera edytor rozszerzeń zbiorów, które chcemy skanować.

Sekcja *Skanuj boot sektory gdy* określa kiedy ma następować skanowanie boot sektorów dyskietek. Do wyboru są możliwe dwie opcje:
- *dostęp* – sprawdzenie będzie wykonywane w momencie włożenia nowej dyskietki do napędu
- *zamknięcie systemu* – sprawdzenie będzie wykonywane w momencie zamykania systemu

Metody skanowania

To okno pozwala na wybranie metody skanowania i szczegółowości analizy heurystycznej – jednego z najsilniejszych narzędzi udostępnianych przez NOD32.

Grupa Metody, umieszczona w górnej części okna, zawiera dwie opcje: Sygnatury i Czułość analizy heurystycznej.

- *Sygnatury* – pozwala na identyfikację poszczególnych wirusów na podstawie ich "sygnatur", to znaczy specyficznych elementów ich kodu
- *Czułość analizy heurystycznej* – uruchamia analizę heurystyczną kodu zbiorów (bazującą na zachowaniu wirusów)

Poniżej grupy Metody, umieszczony jest przełącznik, którym można określać szczegółowość i czułość z jaką analiza heurystyczna ma być wykonywana. Ogólnie rzecz ujmując, im bardziej szczegółowa jest analiza tym dłużej trwa skanowanie zbiorów ale jednocześnie zapewniony jest wyższy poziom bezpieczeństwa. Użytkownik może wybrać spośród następujących opcji:

- *Podstawowa* – minimalizuje liczbę fałszywych alarmów
- *Standardowa* – optymalna w większości przypadków
- *Wysoka* – zapewnia maksymalną czułość analizy

Czynności

Ta zakładka pozwala określić parametry programu i czynności jakie mają być wykonywane w momencie wykrycia wirusa. Zawiera ona 9 opcji podzielonych na trzy grupy.

W przypadku wybrania opcji *Wyświetl panel ostrzegawczy* odpowiednie okno będzie pojawiało się przy każdym wykryciu wirusa, przedstawiając jednocześnie listę możliwych do wykonania czynności. Jeżeli opcja nie zostanie wybrana, program będzie automatycznie blokować dostęp do zainfekowanych zbiorów.

Wybór kolejnej opcji *W pierwszej kolejności spróbuj usunąć wirusa automatycznie* powoduje, że program będzie się starał usunąć wirusa z każdego zainfekowanego zbioru bez interwencji użytkownika. Jeżeli czynność się nie powiedzie, będzie wyświetlany panel ostrzegawczy i/lub nastąpi zablokowanie dostępu do zbioru, w zależności od tego jaka opcja została wybrana w punkcie pierwszym.

Pozostałe zestawy opcji kontrolują treść jaka znajdzie się w wyświetlanym panelu ostrzegawczym. Jeżeli jego wyświetlanie zostało zablokowane – opcje te będą niedostępne.

Pierwszy zestaw – *Wirusy zbiorów* określa sposób postępowania w przypadku zainfekowania zbioru i dopuszcza następujące możliwości:

- *Usuń wirusa* – usuwa wirusa z zainfekowanego zbioru
- *Zmień nazwę* – zmienia nazwę zainfekowanego zbioru
- *Usuń zbiór* – usuwa zainfekowany zbiór
- *Izoluj* – umieszcza zainfekowany zbiór na liście plików tymczasowo wyłączonych ze skanowania

Drugi zestaw – *Boot wirusy* jest używany w przypadku infekcji boot sektorów i wyświetla następujące opcje:

- *Usuń wirusa* – usuwa wirusa z rekordu startowego
- *Zastąp* – zastępuje zainfekowany kod rekordu startowego odpowiednim kodem standardowym
- *Izoluj* – tymczasowo wyłącza boot sektor tej dyskietki ze skanowania

Wyłączenia

Ta zakładka umożliwia tworzenie listy zbiorów, folderów i boot sektorów, które mają być wyłączone ze skanowania. Znajduje się w niej okno prezentujące wyłączone ze skanowania pozycje oraz cztery przyciski.

Okno jest podzielone na cztery kolumny o zmiennej szerokości. Te kolumny to:

- *Nazwa* - określa ścieżkę do obiektu
- *Typ* – określa typ obiektu
- *Podfoldery* – jeżeli wybrany obiekt jest folderem, to ta kolumna określa czy podfoldery mają być również wyłączone ze skanowania
- *Tymczasowo* – jeżeli w kolumnie wyświetlone jest “Tak”, wyłączenie ze skanowania jest tymczasowe – tylko do momentu ponownego uruchomienia programu. Po ponownym uruchomieniu pozycja ta zostanie usunięta z listy.

Jeżeli jest to konieczne, szerokość każdej z kolumn może zostać zmieniona. Należy najechać kursorem na linię dzielącą dwie sąsiadujące kolumny (wyświetli się specjalny wskaźnik myszy), wcisnąć lewy klawisz myszy i przesuwać wskaźnik w prawo lub w lewo, zmieniając w ten sposób szerokość kolumn.

Cztery przyciski w dolnej części okna mają następujące funkcje:

- *Dodaj* – dodaje nowe pozycje do listy
- *Zmień* – zmienia pozycje na liście
- *Usuń* - usuwa pozycję z listy
- *Domyślne* – zastępuje pozycje aktualnie znajdujące się na liście domyślnymi pozycjami

Sieć

Ta zakładka ustawia parametry programu związane z pracą w sieci oraz parametry jego Centralnej Aktualizacji. Składa się z dwóch sekcji:

W górnej części sekcji *Komunikatów sieciowych* można zaznaczyć pozycję *Wyślij wiadomość o przeniknięciu wirusów do sieci.* Po jej zaznaczeniu, jeżeli AMON wykryje w sieci wirusa, odpowiednia informacja zostanie wysłana do wybranych użytkowników. Ich aktualna lista jest wyświetlana w oknie znajdującym się poniżej.

By uzupełnić listę o nowych adresatów, wciśnij przycisk *Dodaj*. Nazwa stacji lub grupy komputerów pojawi się w oknie dialogowym, wyświetlanym po wciśnięciu przycisku. Jeżeli zamiast nazwy wprowadzona zostanie gwiazdka, to komunikaty będą wysyłane do wszystkich członków grupy, do której należy użytkownik.

Ażeby usunąć wybraną pozycję z listy, przesuń na nią kursor, zaznacz klikając lewym przyciskiem myszy i wciśnij na klawiaturze klawisz DEL lub kliknij na przycisk *Usuń.*

Treść komunikatu jest wprowadzana w oknie dialogowym *Format wiadomości.* Wymagana zawartość komunikatu powinna być wprowadzona w tym polu a miejsce, w którym ma się pojawić nazwa wykrytego wirusa zaznaczone przez parametr <virus>.

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.

Zabezpieczenia

Zakładka Zabezpieczenia jest używana do konfiguracji opcji zabezpieczeń programu. Składa się z dwóch sekcji.

W sekcji *Zabezpieczenia*, można ustawić zabezpieczenie hasłem wybranych pozycji. W górnej części okna można wybrać następujące opcje:

- *Wyłącz możliwość odinstalowania i wyłączenia programu Amon* – uniemożliwia standardowe odinstalowanie lub wyłączenie rezydentnego skanera.
- *Nie wyświetlaj ikony programu Amon na pasku zadań* – po zaznaczeniu, uruchomienie programu Amon nie będzie sygnalizowane na pasku zadań.

Ostrzeżenie: Ponowne wyświetlenie ikony na pasku zadań nastąpi po uruchomieniu programu Amon z parametrem /SHOWICON i ponownym uruchomieniu systemu.

Lista wymienionych poniżej opcji zapewnia kontrolę przed dostępem do wybranych zakładek:

- *Obiekty*
- *Metody*
- *Czynności*
- *Wyłączenia*
- *Sieć*
- *Zabezpieczenia*

Zaznaczenie dowolnej z powyższych opcji powoduje automatyczne zabezpieczenie hasłem dostępu do zakładki *Zabezpieczenia*.

W dolnej części sekcji znajdują się dwa przyciski:

- *Hasło* – służy do wprowadzenia hasła zabezpieczającego chronione fragmenty programu.
- *Wybierz wszystkie* – automatycznie zaznacza wszystkie opcje

Druga sekcja zawiera możliwość *zaznaczenia Automatyczna aktywacja Amon-a w momencie uruchamiania systemu.* Jeżeli jest ona wybrana to rezydentny skaner wirusów jest uruchamiany automatycznie przy każdym uruchomieniu systemu operacyjnego.

Wciśnij przycisk Domyślna konfiguracja Amon-a, by przywrócić parametry sugerowane przez producenta.

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

Dodawanie pozycji do listy wyłączeń

Okno dialogowe w górnej części panelu pozwala określić ścieżkę do dodawanego obiektu. Pod spodem znajdują się cztery przełączniki:

Przełącznik *Dodaj do listy* ma następujące pozycje:
- *trwale wyłączony* – na stałe wyklucza obiekt ze skanowania
- *tymczasowo wyłączony* – wyklucza obiekt ze skanowania do momentu zakończenia pracy programu Amon.

Przełącznik *Pozycje wyłączone ze skanowania zawiera trzy opcje*:
- *folder* – wyklucza cały folder
- *zbiór* – wyklucza tylko pojedyńczy zbiór
- *boot sektor* – wyłącza ze skanowania obszary systemowe dysku

Przełącznik *Wyłącz ze skanowania podfoldery* daje dwie możliwości:
- *nie* – podfoldery wyłączonego obiektu będą skanowane
- *tak* – podfoldery będą również wyłączone ze skanowania

Przełącznik boot sektor dyskietki pozwala wybrać, który z napędów nie będzie skanowany:
- *A:* – wyłączy ze skanowania boot sektor dyskietki umieszczonej w napędzie A:
- *B:* – wyłączy ze skanowania boot sektor dyskietki umieszczonej w napędzie B:

Dolna część zawiera cztery przełączniki o następujących funkcjach:
- *OK* – aktualne ustawienia są potwierdzone a obiekt dodany do listy
- *Anuluj* – operacja jest anulowana a obiekt nie będzie do listy dodany
- *Przeglądaj* – uruchamia standardowy dialog z systemem umożliwiający wybór foldera spośród znajdujących się na dysku (dyskach)
- *Zbiór* – uruchamia standardowy proces wybierania zbioru spośród znajdujących się na dysku (dyskach)

Dokonywanie modyfikacji na liście obiektów wyłączonych ze skanowania

Okno dialogowe w górnej części panelu pozwala określić ścieżkę do modyfikowanego obiektu. Pod spodem znajdują się cztery przełączniki:

Przełącznik *Dodaj do listy* ma następujące pozycje:
- *trwale wyłączony* – na stałe wyklucza obiekt ze skanowania
- *tymczasowo wyłączony* – wyklucza obiekt ze skanowania do momentu zakończenia pracy programu Amon.

Przełącznik *Pozycje wyłączone ze skanowania zawiera trzy opcje*:
- *folder* – wyklucza cały folder
- *zbiór* – wyklucza tylko pojedyńczy zbiór
- *boot sektor* – wyłącza ze skanowania obszary systemowe dysku

Przełącznik *Wyłącz ze skanowania podfoldery* daje dwie możliwości:
- *nie* – podfoldery wyłączonego obiektu będą skanowane
- *tak* – podfoldery będą również wyłączone ze skanowania

Przełącznik boot sektor dyskietki pozwala wybrać, który z napędów nie będzie skanowany:
- *A:* – wyłączy ze skanowania boot sektor dyskietki umieszczonej w napędzie A:
- *B:* – wyłączy ze skanowania boot sektor dyskietki umieszczonej w napędzie B:

Dolna część zawiera cztery przełączniki o następujących funkcjach:
- *OK* – aktualne ustawienia są potwierdzone a obiekt dodany do listy
- *Anuluj* – operacja jest anulowana a obiekt nie będzie do listy dodany
- *Przeglądaj* – uruchamia standardowy dialog z systemem umożliwiający wybór foldera spośród znajdujących się na dysku (dyskach)
- *Zbiór* – uruchamia standardowy proces wybierania zbioru spośród znajdujących się na dysku (dyskach)

Okno alarmu wirusowego

Okno zostaje wyświetlone w momencie wykrycia przez program wirusa. Przed jego wyświetleniem Amon odcina dostęp do zainfekowanego zbioru nie ma więc powodu do obaw, że wirus może się uaktywnić. Wygląd okna zależy od możliwości i ustawień twojej karty graficznej.
W górnej lewej części znajdują się dwa przyciski:

- *Zamknij* – zamyka okno alarmowe (zainfekowane zbiory nadal pozostają niedostępne)
- *Informacje* – wyświetla okno informacyjne z krótkim opisem rekomendowanych do wykonania czynności

Obszar poniżej wyświetla pełną ścieżkę do zainfekowanego pliku i informacje o rodzaju wykrytego wirusa. Dodatkowo znajduje się tam informacja przy wykonywaniu jakiej operacji wirus został wykryty oraz czy Amon może go usunąć.

Można też zaznaczyć opcję *Wyświetl to ostrzegawcze okno.* Ma to zastosowanie w szczególnych sytuacjach. Jeżeli na przykład program, który otwiera setki zainfekowanych zbiorów jest uruchomiony i jego praca nie może zostać przerwana, można tymczasowo wyłączyć pojawianie się okna alarmowego i tym samym przyśpieszyć jego pracę. Dostęp do zainfekowanych zbiorów pozostaje zablokowany. Wyświetlanie okna alarmowego można ponownie przywrócić albo poprzez wybór odpowiedniej opcji w zakładce Czynności albo ponownie uruchamiając program Amon.

W prawej części znajduje się grupa czterech przycisków:

- *Usuń wirusa* – powoduje usunięcie wirusa ze zbioru (jeżeli Amon nie może usunąć wirusa to przycisk nie jest aktywny)
- *Zmień nazwę* – zmienia nazwę zainfekowanego zbioru by uniknąć dalszego rozprzestrzeniania
- *Usuń* – usuwa zainfekowany zbiór
- *Wyłącz ze skanowania* – w przypadku fałszywego alarmu istnieje możliwość wyłączenia pliku ze skanowania

W przypadku infekcji boot sektora przycisk *Zmień nazwę* nie jest wyświetlany. Zamiast niego pojawi się przycisk *Zastąp*. Po kliknięciu na przycisk Amon zastąpi zainfekowane rekordy boot sektora, sektora, czystym, standardowym kodem.

Okno informacyjne

Wyświetla dodatkowe informacje na temat czynności, jakie można wykonać po wykryciu obecności wirusa.

W dolnej części znajdują się dwa przyciski:

- *Anuluj* – zamyka okno informacyjne
- *Eksportuj zbiór* – generuje zbiór zawierający zainfekowany obiekt w celu wysłania go do analizy w firmie ESET LLC company.

Informacje o Amon-ie

NOD - AMON

Edytor rozszerzeń

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

Aktualna lista rozszerzeń jest wyświetlona w porządku alfabetycznym 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* otwierający okno, w którym można wpisać nowe rozszerzenie (maksymalna długość to 10 znaków). 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.*

Spis treści