



Instrukcja obsługi programu

ArcaVir 2010

© Copyright 2004-2010 by **ArcaBit Sp. z o.o.**

Zarówno program, jak i instrukcja korzystają z pełnej ochrony określonej przepisami prawa autorskiego. Wszystkie aktualne informacje dotyczące oprogramowania oraz kontaktu z firmą ArcaBit Sp. z o.o. są dostępne na stronach internetowych pod adresem: <http://www.arcabit.pl>.

Ponieważ program podlega ciągłym zmianom, możliwe są rozbieżności, pomiędzy aktualnie wykorzystywaną przez Państwa wersją programu oraz wersją tego dokumentu. Najbardziej aktualna wersja dokumentacji dostępna jest na naszych stronach w Internecie.

Spis treści

1. Wstęp	5
2. Wymagania ArcaVira 2010.....	6
2.1. Wymagania systemowe.....	6
3. Instalacja ArcaVir 2010	6
3.1. Instalacja pakietu ArcaVir.....	6
3.2. Odinstalowanie pakietu ArcaVir	7
4. Obsługa ArcaVir 2010	8
4.1. Ochrona antywirusowa.....	9
4.1.1. Monitor antywirusowy	10
4.1.2. Skaner poczty.....	10
4.2. Bezpieczeństwo w sieci	11
4.2.1. Zapora sieciowa – firewall	11
4.2.2. Antyspam.....	12
4.2.3. Skaner http	12
4.2.4. Kontrola rodzicielska.....	13
4.2.5. Monitor rejestru	13
4.3. Aktualizacja.....	13
4.4. Skanownie	15
4.5. Szybkie skanowanie	17
4.6. Ustawienia	17
4.6.1. Skanowanie - Ustawienia	18
4.6.1.1. Skaner	18
4.6.1.2. Szybkie skanowanie.....	21
4.6.2. Ochrona antywirusowa.....	21
4.6.2.1. Monitor	21
4.6.2.2. Poczta.....	23
4.6.3. Bezpieczeństwo w sieci	28
4.6.3.1. Zapora sieciowa	28
4.6.3.2. Antyspam.....	31
4.6.3.3. Skaner HTTP.....	35
4.6.3.4. Monitor rejestru	35
4.6.3.5. Kontrola rodzicielska	37
4.6.4. Obsługa pakietu	38
4.6.4.1. Kwarantanna	38
4.6.4.2. Zadania	38
4.6.4.3. Powiadamianie.....	39
4.6.5. Narzędzia	39
4.6.5.1. Kopie zapasowe	39
4.6.6. Aktualizacja.....	40
4.6.6.1. Ustawienia aktualizacji.....	41
4.6.6.2. Serwer.....	41

4.7. Raporty.....	42
4.7.1. Raporty pakietu	42
4.7.2. Raporty zapory sieciowej.....	42
4.8. Kwarantanna	42
4.9. Pomoc	43
5. Zasobnik systemowy (ikona ArcaVir 2010)	43
5.1. Otwórz ArcaVir 2010.....	44
5.2. Skanowanie.....	44
5.3. Aktualizacja	44
5.4. Obsługa pakietu	45
5.4.1. Antyspam – naucz mnie	45
5.4.2. Kwarantanna	47
5.4.3. Naprawa instalacji	48
5.4.4. Rejestracja	48
5.4.5. Tryb gry - włącz	48
5.5. Narzędzia	49
5.5.1. Aktualizacja ArcaVir USB	49
5.5.2. Kopie zapasowe	49
5.5.3. Łatanie systemu	50
5.5.4. Audyt systemu	50
5.5.5. Menadżer procesów	51
5.5.6. ArcaCoolka	52

1. Wstęp

Macie Państwo przed sobą instrukcję do najnowszej wersji programu antywirusowego ArcaVir 2010, kolejnego produktu firmy ArcaBit Sp. z o.o.. Począwszy od roku 2004 nasza firma dokłada wszelkich starań, aby stworzyć ochronę antywirusową, która sprosta Państwa oczekiwaniom. Cały nasz zespół nieustannie tworzy i udoskonala program antywirusowy abyście Państwo bezpiecznie i bez obaw mogli korzystać z Waszych komputerów.

Program, który właśnie oddajemy Państwu do użytku został zaprojektowany z myślą o maksymalnej prostocie obsługi tak, aby każdy Użytkownik bez kłopotu mógł z niego korzystać. Jednocześnie, ArcaVir 2010 posiada duże możliwości konfiguracyjne i diagnostyczne, przydatne bardziej zaawansowanym użytkownikom. Niniejsza instrukcja ma na celu pomoc i ułatwić korzystanie z programu ArcaVir 2010.

Dziękujemy za zaufanie, jakim Państwo nas obdarzyliście kupując program ArcaVir 2010. Liczymy, że nowy program poprzez zapewnienie doskonałej ochrony oraz swą prostotę obsługi sprosta wymaganiom wszystkich Użytkowników. Będziemy wdzięczni za każde konstruktywne uwagi.

W razie jakichkolwiek pytań lub problemów, które nie rozwiązuje poniższa instrukcja prosimy o kontakt z **Działem Pomocy Technicznej tel. (22) 532-69-20 w godz. 8:00-20:00, pomoc@arcabit.pl.**

2. Wymagania ArcaVira 2010

2.1. Wymagania systemowe

ArcaVir 2010 działa na następujących systemach operacyjnych:

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows XP Professional x64 Edition SP1
- Windows Vista SP1 (x86 i x64, wszystkie edycje)
- Windows 7
- Windows Server 2003 SP2,
- Windows Home Server
- Windows Server 2008

Nabywca pakietu ArcaVir 2010 może korzystać w ramach tej samej licencji na starszych systemach Windows z pakietu instalacyjnego ArcaVir98ME2000.exe.

3. Instalacja ArcaVir 2010

3.1. Instalacja pakietu ArcaVir

Program można zainstalować **z płyty CD** otrzymanej przy zakupie programu ArcaVir w wersji BOX, lub **z pliku instalacyjnego**, który należy pobrać ze strony internetowej <http://arcabit.pl/pobierz>.

Po uruchomieniu programu instalacyjnego zostanie wyświetlone okno pozwalające wybrać wersję językową pakietu. Potwierdzenie

wyboru rozpocznie proces instalacji programu. Kolejnym korkiem jest podanie numeru licencji otrzymanego w momencie zakupu programu ArcaVir. Znajduje się on wewnątrz pudełka z płytą CD (w przypadku wersji pudełkowej, natomiast w wersji elektronicznej jest on wysyłany e-mailem).

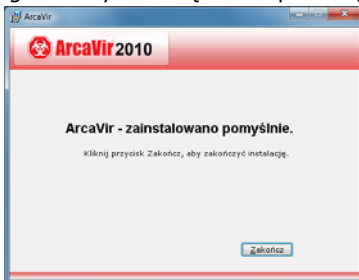


Rozpoczęcie procesu instalacji programu zasygnalizowane zostanie pojawieniem się ekranu powitalnego. Nawigacja między oknami programu instalacyjnego odbywa się za pomocą przycisków **Dalej** i **Wstecz**.

Aby przejść do instalacji programu należy zaakceptować postanowienia umowy licencyjnej.

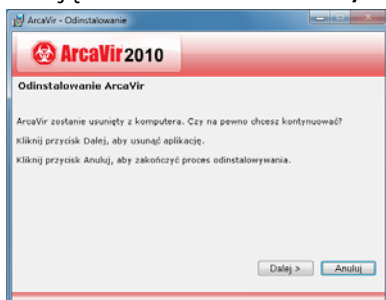
Kolejne okno pozwala wybrać rodzaj instalacji standardowy lub zaawansowany. Zalecamy jednak wybór instalacji standardowej, który spowoduje zainstalowanie programu w wersji, która nie zawiera elementów umożliwiających zarządzanie programem w sieci korporacyjnej. Instalacja zaawansowana pozwala między innymi wybrać katalog, w którym zainstalowany zostanie program.

Poprawne zainstalowanie programu zasygnalizowane zostanie ekranem z informacją o stanie zakończzonego procesu.



3.2. Odinstalowanie pakietu ArcaVir

Klikając na menu **START/Programy/ArcaVir/Odinstaluj**



ArcaVir możemy usunąć z systemu instalację pakietu **ArcaVir**. Deinstalacja jest również możliwa przez **Panel sterowania / Dodaj lub usuń programy**, gdzie na liście zainstalowanych programów należy odszukać **ArcaVir**. Odinstalowanie programu możliwe jest także poprzez uruchomienie pliku instalatora. W tym

przypadku należy potwierdzić chęć usunięcia programu. Po potwierdzeniu, program **ArcaVir 2010** zostanie usunięty z systemu. Na koniec deinstalacji wymagany jest restart komputera.

4. Obsługa ArcaVir 2010

Program **ArcaVir 2010** został wyposażony w nowy interfejs użytkownika. Dzięki temu obsługa programu stała się prostsza i bardziej intuicyjna. Dostęp do wszystkich elementów tworzących system ochronny komputera uzyskujemy za pomocą:

- głównego okna programu (wywołanie przez dwukrotne kliknięcie ikony programu w zasobniku systemowym, lub z paska zadań, należy wybrać: Start → Wszystkie programy → ArcaBit → ArcaVir → ArcaVir Skaner).
- menu kontekstowego (wywołanie po naciśnięciu prawym klawiszem myszy na ikonę programu w zasobniku systemowym). Więcej informacji na temat opcji dostępnych z zasobnika systemowego w dziale 5. *Zasobnik systemowy (ikona ArcaVir 2010)*.



Główne okno programu pozwala na szybki dostęp do najważniejszych modułów ochronnych. Można je aktywować, dezaktywować i konfigurować wedle własnych preferencji. Zaleca się jednak, aby jeżeli nie ma takiej potrzeby opcji tych nie zmieniać, ponieważ domyślnie zostały one skonfigurowane tak, aby zapewniały optymalny poziom bezpieczeństwa komputera.

Okno programu ArcaVir 2010 składa się z następujących elementów:

- Ochrona antywirusowa
- Bezpieczeństwo w sieci
- Aktualizacja
- Skanowanie
- Szybkie skanowanie
- Ustawienia
- Raporty
- Kwarantanna
- Pomoc

Dokładny opis tych modułów znajduje się w następnym dziale pt.:

4.1. Ochrona antywirusowa.

Dostępna jest również opcja przełączania głównego okna na:

- Widok podstawowy (ogólne informacje o modułach)
- Widok zaawansowany (pokazuje szczegółowe informacje na temat aktywności dostępnych modułów).

Elementem informującym o poziomie bezpieczeństwa komputera w programie ArcaVir 2010 jest znak graficzny komputera w kuli i jego podpis.

4.1. Ochrona antywirusowa

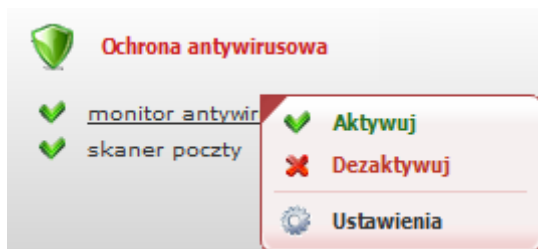
Pakiet **ArcaVir** zapewnia wszechstronne bezpieczeństwo komputera. Program pracuje w oparciu o nowoczesny silnik antywirusowy, który wyposażony jest w bazę danych o wszelkich wariantach szkodliwych obiektów (wirusach, koniach trojańskich, robakach internetowych, programach typu spyware, adware, riskware, obiektach typu rootkit itp.). Zawiera wszystkie elementy niezbędne do pełnej ochrony antywirusowej nawet największych systemów.

W skład ochrony antywirusowej wchodzi monitor antywirusowy oraz skaner poczty. Aby włączyć/wyłączyć ochronę antywirusową należy dwukrotnie kliknąć na nią. Szczegółowe informacje na temat ochrony antywirusowej będą wyświetlone jedynie po przełączeniu na *Widok zaawansowany*.

4.1.1. Monitor antywirusowy

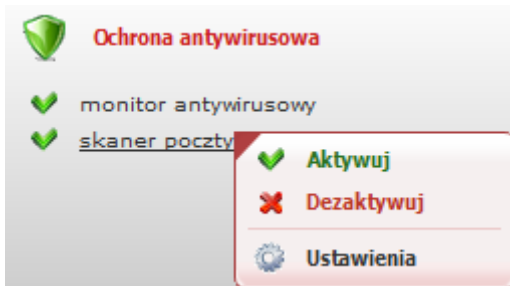
To rezydentny moduł, który w czasie rzeczywistym kontroluje wszystkie zapisywane, otwierane, kopiowane czy też pobierane z Internetu pliki. Mechanizm ten nie dopuszcza do zainfekowania systemu przez przypadkowe czy świadome uruchomienie czy też otwarcie zainfekowanego pliku. Każdy taki plik jest momentalnie blokowany i w zależności od konfiguracji lub decyzji użytkownika - kasowany, leczony albo przenoszony do kwarantanny.

Aby włączyć lub wyłączyć monitor antywirusowy należy kliknąć na niego prawym klawiszem myszki a gdy się pojawi okno jak na obrazku proszę wybrać żadaną akcję. Konfiguracja monitora zostanie omówiona w rozdziale 4.6.2. *Ustawienia → Ochrona antywirusowa.*



4.1.2. Skaner poczty

Skanuje pocztę przychodzącą i wychodzącą pod względem zawirusowania, współpracuje z każdym programem pocztowym. Poczta elektroniczna jest nadal jednym z głównych źródeł infekcji. Każdego dnia docierają do naszych skrzynek niezliczone ilości zainfekowanych listów. Naszą odpowiedzią na to wyzwanie jest skaner poczty. Nie wymaga on żadnej dodatkowej konfiguracji kont pocztowych i od razu po instalacji chroni wszystkie skrzynki niezależnie od tego, jakim programem pocztowym posługuje się użytkownik. Skanuje zarówno pocztę przychodzącą jak i wychodzącą. Potrafi obsługiwać archiwa i pliki osadzone. W nowej wersji skaner został wzbogacony o obsługę SSL przy skanowaniu poczty, niewymagającą zmian portów i nie powodującą ostrzeżeń ze strony programów pocztowych.



Aby włączyć lub wyłączyć ochronę poczty należy kliknąć na skaner poczty prawym klawiszem myszki a gdy się pojawi okno jak na obrazku proszę wybrać żadaną akcję. Konfiguracja skanera poczty zostanie omówiona w rozdziale 4.6.2.2. *Ustawienia* → *Ochrona antywirusowa* → *Poczta*.

4.2. Bezpieczeństwo w sieci

W skład pakietu bezpieczeństwa w sieci wchodzi następujące moduły:

- Zapora sieciowa – firewall
- Antyspam
- Skaner http
- Kontrola rodzicielska
- Monitor rejestru

Szczegółowe informacje na temat bezpieczeństwa w sieci będą wyświetlone jedynie po przełączeniu się na *Widok zaawansowany*.

4.2.1. Zapora sieciowa – firewall

Zapora sieciowa chroni system przed atakami z sieci. W dzisiejszych czasach rzadko który komputer jest odizolowany od sieci, dlatego istotną rolę w bezpieczeństwie w sieci pełni zapora sieciowa. Zapora pracuje w oparciu o nowoczesną technologię kontroli aplikacji, co pozwala na bardzo precyzyjne określenie jaki ruch sieciowy i dla jakiej aplikacji jest dozwolony, a jaki nie.

Zaporę sieciową aktywujemy/dezaktywujemy klikając prawym przyciskiem myszki wybierając *Aktywuj* lub *Dezaktywuj*. Można również w ten sposób przejść do jej ustawień. Ustawienia zostaną omówione omówiona w rozdziale 4.6.3. *Ustawienia* → *Bezpieczeństwo w sieci*.

4.2.2. Antyspam

Spam, czyli niechciana korespondencja zaśmiecająca nasze skrzynki to jedna z bolączek niemal wszystkich użytkowników komputerów, którzy przy każdym odbiorze poczty muszą ręcznie wybierać wartościowe listy z natłoku spamu. Antyspam potrafi oznakować niechcianą pocztę a tym samym umożliwia jej wygodne filtrowanie w programie pocztowym. Wykorzystuje do tego celu zaawansowane techniki statystyczne, białe i czarne listy, RBL-e itp. Oprócz filtrowania niechcianej poczty antyspam wykrywa MassMailing - listy generowane masowo.

Antyspam aktywujemy/dezaktywujemy klikając prawym przyciskiem myszki wybierając *Aktywuj* lub *Dezaktywuj*. Możemy również w ten sposób przejść do jego ustawień. Ustawienia zostaną omówione w rozdziale 4.6.3.3. *Ustawienia* → *Bezpieczeństwo w sieci* → *Antyspam*.

4.2.3. Skaner http

Zabezpiecza system przed obiektami wykorzystującymi do rozprzestrzeniania się protokołów HTTP. Przeglądanie witryn internetowych stało się niebezpiecznym zajęciem, odkąd powstało złośliwe oprogramowanie, które instaluje się na dysku podczas surfowania w sieci. Zwykły obrazek może zawierać ukrytą treść zawierającą szkodliwy kod. W nowej wersji została dodana możliwość konfiguracji skanera http, ustalenie reguł skanowania oraz stworzenie białej listy stron.

Aktywację/dezaktywację skanera http wywołujemy przez prawy klawisz myszki wybierając *Aktywuj* lub *Dezaktywuj*. Możemy również w ten sposób przejść do jego ustawień. Ustawienia zostaną omówione w rozdziale 4.6.3.4. *Ustawienia* → *Bezpieczeństwo w sieci* → *Skaner http*.

4.2.4. Kontrola rodzicielska

Moduł kontroli rodzicielskiej pozwala na wygodne określenie, z jakich stron można korzystać, a jakie należy blokować. Administrator sieci szkolnej czy firmowej jak również rodzic może ustalić, jakie strony w obrębie danej struktury mogą być udostępnione użytkownikom.

Aktywację/dezaktywację kontroli rodzicielskiej wywołujemy przez prawy klawisz myszki wybierając *Aktywuj* lub *Dezaktywuj*. Możemy również w ten sposób przejść do jej ustawień. Ustawienia zostaną omówione w rozdziale 4.6.3.1. *Ustawienia* → *Bezpieczeństwo w sieci* → *Kontrola rodzicielska*.

4.2.5. Monitor rejestru

Służy do kontrolowania zmian w rejestrze systemu. Rejestr systemowy to kluczowa baza danych w systemie Windows. Od jego zawartości i kondycji zależy stabilność systemu i jakość naszej pracy. Monitor rejestru stale kontroluje, czy uruchamiane i wykorzystywane przez użytkownika aplikacje nie próbują umieścić w rejestrze szkodliwych wpisów (np. w kluczu Run, który odpowiada za uruchamianie aplikacji przy starcie systemu). Każda potencjalnie szkodliwa zmiana powoduje alarm, a program daje użytkownikowi możliwość cofnięcia lub uznania zmiany.

Aby włączyć lub wyłączyć monitor rejestru należy kliknąć na nim prawym klawiszem myszki a gdy się pojawi okno proszę wybrać żadaną akcję. Ustawienia skanera poczty zostaną omówione w rozdziale 4.6.3.5. *Ustawienia* → *Bezpieczeństwo w sieci* → *Monitor rejestru*.

4.3. Aktualizacja

Aktualizacja to w przypadku oprogramowania antywirusowego jeden z podstawowych czynników decydujących o jego skuteczności. Moduł aktualizacji gwarantuje, że zainstalowany w systemie pakiet ArcaVir zawsze będzie posiadał aktualne bazy wirusów, aktualne mechanizmy skanujące, aktualne bazy heurystyki itp. Aktualizacja programu może pracować w dwóch trybach. Pierwszy z nich to tryb aktualizacji alertowej, uruchamianej przez sygnał z serwerów aktualizacyjnych firmy ArcaBit. Drugi to tryb zadaniowy, bazujący na zawartej w pakiecie

funkcji harmonogram zadań. Dla większych sieci moduł aktualizacji oferuje mechanizm repozytorium, dzięki któremu pliki aktualizacyjne pobierane są tylko przez jeden komputer w sieci i udostępniane (w wybranym przez administratora protokole, w tym także HTTP) pozostałym maszynom w sieci.

Klikając na *Aktualizację* lewym klawiszem myszy mamy podgląd następujących danych:

- data aktualizacji
- data bazy wirusów
- pozostała liczba dni abonamentu
- numer licencji

The screenshot shows a software interface with the following elements:

- Data aktualizacji :** 2009-10-02 17:40:48
- Data bazy wirusów :** 2009.10.02 08:26:04
- Aktualizuj teraz** (button)
- Pozostała liczba dni abonamentu :** 8
- Kup licencję** (button)
- Numer licencji :** 8N6C-L69I-NIS5-PTCF-7RGU-YPJW-SJSB-....
- Wpisz nowy numer** (button)

Data aktualizacji pokazuje datę i godzinę ostatniego sprawdzania przez program czy są dostępne nowe sygnatury baz wirusowych.

Data bazy wirusów podaje datę zainstalowanych baz wirusów.

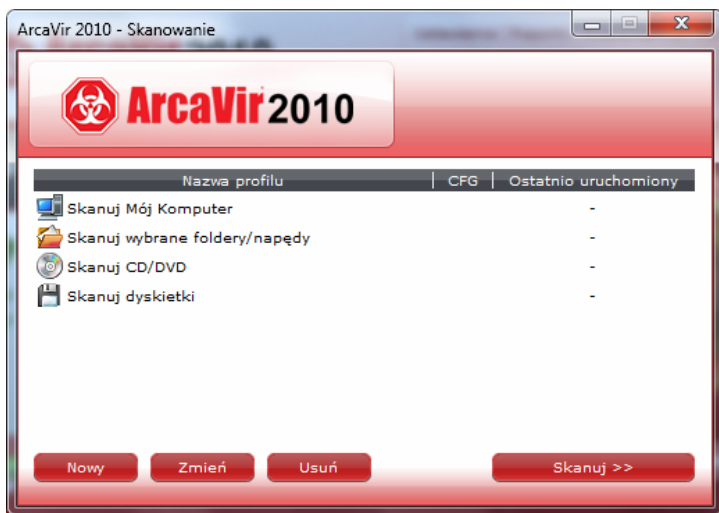
Pozostała liczba dni abonamentu pokazuje ile dni jeszcze program będzie mógł się aktualizować. Liczba ta zależy od wykupionej licencji. Licencji ArcaVir są roczne (366 dni) i dwu letnie (712 dni). Oferowane są również licencje specjalne o różnej liczbie dni abonamentu.

Ważne! Data w komputerze powinna być zawsze aktualna, inaczej program będzie błędnie podawał liczbę dni do końca aktualizacji.

Numer licencji pokazuje tylko początek pierwotnie wpisanego numeru. Jest to dodatkowe zabezpieczenie uniemożliwiające nieuprawnionym użytkownikom jego skopiowanie.

4.4. Skanowanie

Skanner pozwala na wygodną i wszechstronną kontrolę wszelkich zasobów komputera pod kątem infekcji.



Elastyczna konfiguracja daje możliwość tworzenia tzw. profili skanowania, dzięki którym użytkownik może w dowolnym momencie, za pomocą jednego kliknięcia, uruchomić skanowanie wybranych zasobów.

Aby utworzyć swój własny profil skanowania należy kliknąć na przycisk **Nowy**. W oknie *Dodanie/edycja profilu skanowania* należy podać jego nazwę, dodać napędy i foldery, jakie mają być skanowane w ramach profilu. Taka konfiguracja profilu spowoduje, że klikając na niego od razu program przeskanuje to co chcemy.



W ramach skonfigurowanego profilu możemy również do niego przypisać odrębną konfigurację skanera antywirusowego, np. aby po wykryciu wirusa przenosił go do kwarantanny, skanował z większą heurystyką itp. Konfiguracja ta będzie miała jedynie zastosowanie w przypadku uruchomienia skanowania z tego profilu.

W oknie skanowania oprócz dodawania nowych możemy również edytować i kasować wybrane profile. Po wybraniu dowolnego profilu skanowanie rozpoczyna kliknięcie przycisku *Skanuj*>>.

Skanner potrafi skanować większość typów archiwów (zarówno tych popularnych jak i mniej znanych) - ZIP, RAR, ARJ, CAB, ACE, BZIP, TAR, DBX i wiele innych. Posiada również zaawansowany moduł obsługujący tzw. pliki osadzone oraz zaszyfrowane pliki wykonywalne (np. UPX, FSG, PEPACK, PECOYPT itp.) oraz np. dokumenty uniodowane. Dzięki temu jest w stanie wykryć szkodliwy kod nawet w plikach, z którymi nie radzą sobie inne, standardowe skanery antywirusowe.

4.5. Szybkie skanowanie

Służy do błyskawicznej kontroli systemu pod kątem infekcji bez konieczności skanowania wszystkich zasobów komputera. Większość zagrożeń i infekcji można wykryć bez skanowania całego systemu - wystarczy skontrolować jego istotne elementy takie jak rejestr czy też uruchomione procesy. Taką rolę w pakiecie ArcaVir pełni ArcaCheck. Uruchamiany przy starcie systemu za każdym razem sprawdza, czy gdzieś w systemie nie ma czegoś podejrzanego, co mogłoby zagrozić bezpieczeństwu naszych danych.

Szybkie skanowanie wykorzystuje w procesie skanowania moduł **ArcaRD**, który służy do wyszukiwania w systemie obiektów ukrytych typu RootKit. Gdy zostaną odkryte w systemie podejrzanymi zmiany, to moduł zaszyfrowuje to wyświetlając okno z informacją o zagrożeniu. Wybór akcji **Wylecz** spowoduje przywrócenie stanu sprzed modyfikacji wprowadzonej przez wykryte obiekty. Istnieje możliwość wysłania raportu do firmy ArcaBit. Podstawowe parametry konfiguracji modułu **ArcaCheck** możemy ustalić wybierając gałąź ArcaCheck na ekranie opcji konfiguracyjnych programu. Program może zostać wywołany automatycznie w trakcie uruchamiania komputera.

4.6. Ustawienia

W ArcaVir 2010 ustawienia wszystkich modułów, z jakich składa się program zostały umieszczone w jednym oknie. Pozwala ono w szybki sposób konfigurować i zarządzać programem antywirusowym. Można również zabezpieczyć zmianę ustawień pakietu hasłem zaznaczając opcję „*Chroń hasłem zmianę ustawień programu*”. Wówczas osoby bez uprawnień nie będą mogły zmieniać konfiguracji programu.



4.6.1. Skanowanie - Ustawienia

4.6.1.1. Skaner

W tym oknie znajdują się ogólne opcje mające wpływ na pracę skanera:

- Logo programu przy starcie skanera
- Zamykaj program po skanowaniu kontekstowym (uruchomionym za pomocą prawego przycisku myszy) - włączenie tej opcji spowoduje, że program będzie automatycznie wyłączany po sprawdzeniu obiektu.
- Wyślij podejrzone pliki do firmy ArcaBit.
- Wyłączaj mechanizm System Restore na czas skanowania (zapobiega przywracaniu przez system operacyjny zainfekowanych plików wykrytych przez skaner).
- Usuwać pliki tymczasowe przeglądarki przed skanowaniem.

+ Opcja „Skaner → Obszar skanowania”

Tutaj określa się typ skanowanych plików oraz poziom heurystyki. Włączenie tej opcji spowoduje, że program będzie szczegółowo analizował skanowane obiekty pod kątem zachowań charakterystycznych dla wirusów i koni trojańskich. W szczególnych przypadkach włączenie tej opcji może powodować występowanie fałszywych alarmów. Podejrzany plik można

prześć do analizy bezpośrednio z programu, bądź samodzielnie na adres: wirus@arcabit.pl.

+ Opcja „Skaner → Obszar skanowania → Nosiciele”



Opcja ta daje możliwość modyfikacji bazy typów plików, które traktowane są przez program jako nosiciele. Bazę można rozbudować dodając własne typy plików. Można także usunąć z niej wcześniej zdefiniowane typy. Istnieje także możliwość przywrócenia domyślnej konfiguracji.

+ Opcja „Skaner → Obszar skanowania → Wykluczenia”



W oknie wykluczenia określa się, które obiekty mają być wyłączone z procesu skanowania. Wykluczone mogą być foldery, pliki albo maski plików (służą do tego odpowiednie przyciski z prawej strony okna dialogowego). Dodatkowo znajduje się tutaj opcja **Umieszczaj w raporcie informacje o**

wykluczonych plikach i folderach. Jej włączenie spowoduje, że skaner będzie umieszczał w raporcie dodatkowe informacje o pomijaniu wybranych obiektów przy skanowaniu.



+ Opcja „Skaner → Akcje”

Określa się tutaj, jakie akcje mają być podejmowane w momencie znalezienia zainfekowanego obiektu. Akcje automatyczne funkcjonują na zasadzie: „Wykonaj akcję pierwszą, a jak się nie uda, to wykonaj akcję drugą. Jeśli żadna akcja się nie powiedzie, to zapytaj użytkownika”.

+ Opcja „Skaner → Archiwa”

Tutaj definiuje się opcje kontrolujące skanowanie archiwów. Opcje skanowania archiwów to:

- Włączone skanowanie archiwów (po wyłączeniu tej opcji archiwa nie będą rozpakowywane przez program).
- Głębokość skanowania archiwów (archiwa mogą zawierać w sobie kolejne archiwa – rozpakowywanie zagnieżdżonych archiwów trwa długo, więc dla wolniejszych maszyn można określić limit głębokości skanowania).
- Maksymalny rozmiar skanowanego archiwum (opcja ta pozwala określić maksymalną wielkość dla plików archiwum, które mają być uwzględniane przez program w procesie skanowania).
- Skanowanie skompensowanych plików wykonywalnych (np. UPX).



+ Opcja „Skaner → Raporty”

Skaner tworzy obszerne raporty z procesu skanowania. Opcje tworzenia raportów to:

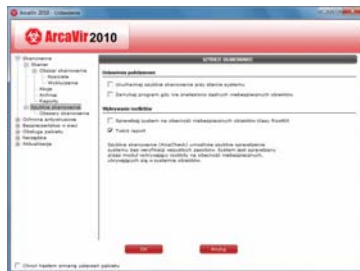
- Twórz raporty ze skanowania (wyłączenie tej opcji spowoduje, że program nie będzie generował raportów).
- Pokaż raport po zakończeniu skanowania.
- Usuń raporty starsze niż (po dłuższym korzystaniu z programu liczba raportów może okazać się bardzo duża)

– opcja ta pozwoli na kasowanie starych, niepotrzebnych raportów).

4.6.1.2. Szybkie skanowanie

W oknie tym mamy możliwość:

- Uruchamiaj szybkie skanowanie przy starcie systemu,
- Zamykaj program, gdy nie znaleziono żadnych niebezpiecznych obiektów,
- Sprawdzaj system na obecność niebezpiecznych obiektów klasy RootKit,
- Twórz raport.



⊕ Opcja „Szybkie skanowanie → Obszar skanowania”

Dla szybkiego skanowania jest możliwe określenie obszaru skanowania:

- skanowanie rejestru
- skanowanie pamięci procesów
- wyszukiwanie ukrytych procesów
- skanowanie sektorów (MBR/DBR)

4.6.2. Ochrona antywirusowa

Za bieżącą ochroną zasobów systemu operacyjnego komputera odpowiedzialne są dwa elementy systemu ochrony antywirusowej. Są to: monitor antywirusowy oraz skaner poczty. Ich konfigurację podajemy poniżej.

4.6.2.1. Monitor

W oknie tym mamy możliwość zdefiniowania parametrów startowych monitora, takich jak:

- aktywacja monitora przy starcie systemu,
- tworzenie raportu,
- priorytet pracy monitora – monitor szybciej obsługuje kolejkę plików (opcja polecana jedynie w przypadku wydajnych komputerów).

⊕ Opcja „Monitor → Reguły skanowania”

Reguły skanowania pozwalają określić, jakie obiekty mają podlegać kontroli:

- Skanowane pliki – tutaj można zdecydować, czy skanowane mają być wszystkie pliki, czy tylko nosiciele (tzn. pliki, których rozszerzenia wskazują na to, że mogą być one potencjalnymi nosicielami wirusów). W ramach tej opcji można również kontrolować listę nosicieli i ewentualnie wykluczać z procesu skanowania wybrane katalogi albo pliki (opcje **Nosiciele** i **Wykluczenia**).
- Skanowanie sektorów – tutaj określa się, czy mają być skanowane sektory startowe wykorzystywanych dyskiekt.
- Sposób traktowania programów typu Dialer, Spyware i Adware.

⊕ Opcja „Monitor → Akcje”

W ramach kolejnej opcji można określić, jakie akcje mają być podejmowane przez monitor w momencie wykrycia zainfekowanego obiektu. Akcje działają na zasadzie „wykonaj akcję pierwszą, a jeśli się nie uda wykonaj akcję drugą” (np. usuń wirusa, a jeśli się nie uda zmień nazwę). Jeśli nie chcesz, aby program wyświetlał informację o poprawnym wykonaniu zadanej operacji, wyłącz opcję *Wyświetl informację o poprawnym wyleczeniu/zmianie nazwy/usunięciu pliku*.

⊕ Opcja „Monitor → Heurystyka”

Następna grupa opcji pozwala określić, czy w trakcie skanowania obiektów mają być wykorzystywane zaawansowane metody heurystyczne.

Wykorzystanie metod heurystycznych, zwłaszcza na wyższych poziomach (**Wysoki** i **Bardzo wysoki**) może powodować fałszywe alarmy (informacja o znalezieniu podejrzenia infekcji w czystym pliku). W takim przypadku zalecamy kontakt z firmą **ArcaBit Sp. z o.o.** w celu wyjaśnienia, czy informacja o infekcji jest zasadna.

⊕ Opcja „Monitor → Archiwa”

Monitor antywirusowy, podobnie jak pozostałe elementy pakietu **ArcaVir**, potrafi kontrolować archiwa. W ramach opcji **Archiwa** można określić, w jakich sytuacjach pliki spakowane mają być przez program skanowane (**Skanuj każde nowe archiwum /**

Skanuj tylko archiwa kopiowane i pobierane np. z Internetu).

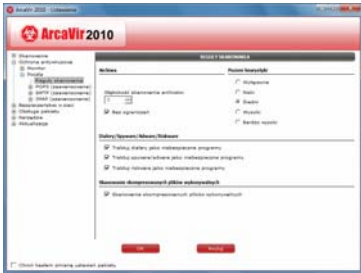
Ważne! Skanowanie każdego nowego archiwum, ze względu na znaczne wymagania pamięciowe, zwłaszcza w przypadku dużych archiwów, może znacznie spowolnić działanie systemu. Dlatego nie zalecamy włączania tej opcji w normalnej pracy. Wystarczy włączenie opcji **Skanuj tylko archiwa kopiowane i pobierane.**

4.6.2.2. Poczta



Możemy określić główne parametry pracy skanera poczty, takie jak:

- Aktywacja skanera poczty przy starcie systemu
- Skanowanie poczty przychodzącej (POP3, IMAP)
- Skanowanie poczty wychodzącej (SMTP)
- Skanowanie połączeń szyfrowanych (SSL)
- Sygnalizowanie połączenia ikoną w zasobniku systemowym.



⊕ Opcja „Poczta → Reguły skanowania

Opcja ta pozwala określić głębokość skanowania archiwów zagnieżdżonych, poziom analizy heurystycznej stosowanej przez skaner poczty, sposób traktowania programów typu dialer i spyware/adware a także zdecydować, czy skanowaniu podlegać mają skompresowa-

ne pliki wykonalne dołączone do przesyłki.

⊕ Opcja „Poczta → POP3 (zaawansowane)“



Do sprawdzenia listu konieczne jest jego odebranie w całości, a przed jego sprawdzeniem nie można go przesłać do programu pocztowego. W sytuacji, gdy skanowanie trwałoby długo, program pocztowy mógłby stwierdzić, że serwer pocztowy zbyt długo nie odpowiada i uznać połączenie za zerwane.

Dlatego skaner poczty w trakcie skanowania wysyła, co pewien czas dane do programu pocztowego (formalnie jest to nic nieznacząca linia nagłówka). W opcji „anti-timeout” dla klienta można ustawić, co ile sekund taka linia ma być wysyłana do programu pocztowego. Z kolei w trakcie skanowania i przesyłania przez skaner poczty długiej wiadomości do programu pocztowego, serwer pocztowy mógłby również potraktować brak kolejnych poleceń jak zerwanie połączenia. Dlatego skaner poczty w tym czasie wysyła do serwera polecenia „nic nie rób” (NOOP), które podtrzymują połączenie. Opcja „anti-timeout” dla serwera określa, co jaki czas ma być wysyłane takie polecenie.

Wykluczenia ze skanowania

Wykluczenia ze skanowania pozwalają na precyzyjniejsze ustalenie, które połączenia mają być skanowane. Standardowo skanowane są wszystkie połączenia wychodzące, tzn. te, których adres docelowy nie jest adresem lokalnym (127.0.0.0/8). Jest to

istotne w przypadku używania innych programów pośredniczących w odbiorze poczty, a działających jako lokalne serwery POP3 (np. Hamster, SpamPal i in.). Bez tego wykluczenia poczta byłaby skanowana dwukrotnie: raz podczas pobierania jej przez program pośredniczący i ponownie, gdy od programu pośredniczącego odbierałby pocztę program pocztowy. Dodatkowo możliwe jest wykluczenie ze skanowania połączeń do serwerów w sieci lokalnej (zakresy adresów: 10.0.0.0/8, 192.168.0.0/16 i 172.16.0.0/12), np. gdy na tych serwerach jest aktywne oprogramowanie antywirusowe.

+ Opcja „Poczta → POP3 (zaawansowane) → Akcje”

W trzech okienkach określa się sekwencję akcji, które są podejmowane w przypadku wykrycia wirusa. Gdy nie powiedzie się pierwsza z nich, podejmowana jest próba wykonania kolejnej. Jeżeli nie zadziała to program wykona kolejną ustawioną. Ma to istotne znaczenie, gdy pierwszą akcją jest *wylecz* a skanowany plik jest np. trojanem, wówczas słuszne jest tylko skasowanie pliku.



+ Opcja „Poczta → POP3 (zaawansowane) → Filtrowanie”



Skaner poczty umożliwia filtrowanie załączników. Jeśli nazwa załącznika jest zgodna ze zdefiniowanym wzorcem, to w stosunku do załącznika podjęta zostanie wybrana akcja. Możliwe akcje to: „Zmień nazwę”, „Skasuj plik” i „Nic nie rób”. Zmiana nazwy załącznika utrudnia otwarcie załącznika bezpośrednio

z programu pocztowego, „Skasuj plik” usuwa załącznik, a „Nic nie rób” wyłącza działanie filtra.

+ Opcja „Poczta → POP3 (zaawansowane) → Znakowanie wiadomości”



Wynik skanowania listu może być dodany do jego tematu (**Dodaj wynik skanowania do pola "Temat"**) lub do specjalnego pola X-Scan nagłówka listu (**Dodaj wynik skanowania do pola "X-Scan"**). Wynik skanowania jest dodawany na początku tematu w postaci „wyniki skanowania ArcaVir:[wynik]” tylko do listów, w których

wykryto niebezpieczną zawartość. Pozwala to na łatwe sortowanie wiadomości w programie pocztowym, w zależności od wyniku skanowania.

Włączenie opcji **“Opakuj listy z wirusami...”** powoduje, że każdy list, który zawierał zainfekowany załącznik, zostanie przetworzony tak, że do programu pocztowego trafi list z informacją o wykrytych zagrożeniach i podjętych w związku z tym akcjach oraz załącznikiem o nazwie "oryginalny list". Załącznik taki zawiera sprawdzony list (razem z załącznikami, które zostały wyleczone i/lub zmieniono im nazwy). List trafiający do programu pocztowego będzie miał identyczne nagłówki (pola: **Temat:**, **Od:**, **Do:** itp.), dzięki czemu ewentualne reguły sortowania listów w programie pocztowym zadziałają prawidłowo. Analogicznie potraktowane zostaną również listy, w których wystąpiły problemy ze sprawdzeniem załączników, np. w przypadku przesłania archiwum zabezpieczonego hasłem.

+ Opcja „Poczta → POP3 (zaawansowane) → Przesyłki wieloczęściowe”

Skaner poczty przed połączeniem przesyłki wieloczęściowej, musi odebrać wszystkie jej części i tymczasowo przechować na dysku. Możliwe jest wybranie rozszerzenia, z jakim będą przechowywane części odebranej wiadomości. Dostępne rozszerzenia to: .eml, .msg i .mbox.

+ Opcja „Poczta → SMTP (zaawansowane)”

Zaznaczenie opcji **Dodaj stopkę do wychodzących wiadomości** spowoduje dodanie do listu informacji o sprawdzeniu listu skanerem poczty. Opcja ta nie będzie aktywna,

jeśli nie będzie zaznaczona opcja **Wyślij list po całkowitym przeskanowaniu**.

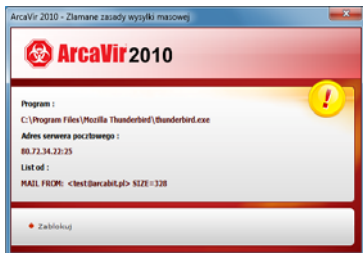


⊕ Opcja „Poczta → SMTP (zaawansowane) → Wysyłka masowa”

Moduł ten służy do wykrywania MassMailingu - listów generowanych masowo przez wirusy. Aktywowanie tego modułu skutecznie zablokuje możliwość wysyłania takich e-maili z komputera.

Użytkownik ma do dyspozycji kilka gotowych profili:

- Wysyłam mało listów (2 listy w ciągu 1 minuty, 5 listów w ciągu 5 minut, 7 listów w ciągu 15 minut)
- Wysyłam dużo listów (4 listy w ciągu 1 minuty, 10 listów w ciągu 5 minut, 20 listów w ciągu 15 minut)
- Wysyłam dużo listów na raz (30 listów w ciągu 1 minuty, 35 listów w ciągu 5 minut, 40 listów w ciągu 15 minut)
- Ustawienia użytkownika (możliwość podania własnych ustawień).
-



W przypadku wykrycia przez program złamania tych reguł zostanie wyświetlony monit jak na oknie poniżej o wykryciu próby masowej wysyłki listów. Użytkownik ma wówczas możliwość **Przepuść** oraz **Rozłącz**. Opcja przepuść umożliwi wysłanie wiadomości, natomiast opcja rozłącz

przerwie wysyłania wiadomości.

Ważne! Dla wygody użytkowników proponujemy wybranie opcji „**Wysyłam dużo listów na raz**”. Wówczas moduł nie przeszkadza w pracy i wysłaniu wiadomości e-mail. Jeżeli jest zaznaczona opcja „Wysyłam mało listów” to często może się pojawiać monit o wykryciu próby masowej wysyłki listów.

⊕ Opcja „Poczta → IMAP (zaawansowane)

W przypadku protokołu IMAP skanowanie odbywa się identycznie jak dla protokołu POP3. Dlatego opcje tego modułu są takie same jak dla Opcja „Poczta → POP3 (zaawansowane)”.

4.6.3. Bezpieczeństwo w sieci

4.6.3.1. Zapora sieciowa



Główny ekran konfiguracyjny programu pozwala ustalić podstawowe ustawienia zapory w systemie operacyjnym. Użytkownik może zdecydować, czy zapora ma być aktywowana przy starcie. Może także określić, czy zapora ma informować o ewentualnej próbie dostępu do sieci przez aplikacje, czy też

ma działać tylko w oparciu o już zdefiniowane reguły („Tryb cichy”).

Kolejną opcją zapory jest "Przepuszczaj połączenia w sieci lokalnej". Włączenie tego trybu powoduje, że zapora nie będzie blokowała, ani też nie będzie informowała o żadnych połączeniach w ramach własnej sieci lokalnej. Sieci lokalne zgodnie z ogólnie przyjętymi regułami, to zakresy:

IP: 192.169.0.0 mask: 255.255.0.0
IP: 172.16.0.0 mask: 255.240.0.0
IP: 10.0.0.0 mask: 255.0.0.0

czyli:

IP: od 10.0.0.0 do 10.255.255.255
IP: od 172.16.0.0 do 172.31.255.255
IP: od 192.168.0.0 do 192.168.255.255

Program posiada predefiniowane reguły dla wielu popularnych aplikacji pogrupowanych w kilku kategoriach, w „Tablicy reguł

zapory sieciowej". Reguły te można dowolnie modyfikować w zależności od preferencji i potrzeb użytkownika. Można także dodawać własne kategorie i w nich umieszczać używane przez siebie aplikacje wymagające dostępu do sieci.

Dodawanie aplikacji można realizować w dwojaki sposób:

1. Klikamy prawym klawiszem myszy w kategorię, gdzie chcemy umieścić reguły dla aplikacji i wybieramy "Dodaj nową aplikację/folder", po czym wyszukujemy na dyskach interesujący nas program. Aby umożliwić aplikacji dostęp do sieci klikamy w nią prawym klawiszem myszy i wybieramy "Dodaj regułę dla aplikacji", po czym definiujemy ją. W okienku można określić dla jakich zakresów adresów IP ma działać dana reguła (jeśli ma to być dowolny adres IP należy ustawić w polach adresu i maski "0.0.0.0"), dla jakich portów (najlepiej definiować pojedyncze porty, czyli w obu polach zakresu portów podajemy ten sam numer, chyba że dana aplikacja dynamicznie przydziela sobie używane porty - wtedy podajemy zakres), czy połączenia w danej regule mają być przepuszczane czy blokowane, oraz czy dana reguła ma działać dla połączeń wychodzących, czy przychodzących. Dla każdej aplikacji można zdefiniować wiele różnych reguł. W przypadku próby dostępu do sieci i braku zdefiniowanej dla takiego dostępu reguły, użytkownik zostanie powiadomiony komunikatem ArcaVir'a (wyświetlanie komunikatów nie działa przy aktywnym "trybie cichym").

2. W drugim przypadku po prostu czekamy, aż dany program zażąda dostępu do sieci, o czym użytkownik zostanie poinformowany komunikatem z ArcaVir'a (wyświetlanie komunikatów nie działa przy aktywnym "trybie cichym"). W okienku z komunikatem wybieramy, czy dane połączenie ma być przepuszczone, czy zablokowane. Po zaznaczeniu opcji "Utwórz regułę na podstawie decyzji" i wciśnięciu "Przepuść" (lub "Blokuj"), dla danej aplikacji zostanie utworzona reguła przepuszczająca (lub blokująca) ruch sieciowy, którą później można zmodyfikować w ustawieniach zapory. W przypadku wybrania "Przepuść zawsze" (lub "Blokuj zawsze") zostanie utworzona dla danej aplikacji reguła na stałe przepuszczająca (lub na stałe blokująca) ruch sieciowy dla danej aplikacji.

a) Dla połączeń wychodzących, przy zaznaczonej opcji "Utwórz regułę na podstawie decyzji" i wciśnięciu "Przepuść" (lub "Blokuj")

zostaje utworzona reguła przepuszczająca (lub blokująca) ruch sieciowy danej aplikacji dla dowolnego zewnętrznego adresu IP, ale dla pojedynczego portu.

b) Dla połączeń przychodzących, przy zaznaczonej opcji "Utwórz regułę na podstawie decyzji" i wciśnięciu "Przepuść" (lub "Blokuj") zostaje utworzona reguła przepuszczająca (lub blokująca) ruch sieciowy danej aplikacji dla pojedynczego zewnętrznego adresu IP i dla pojedynczego portu.

c) Dla połączeń wychodzących, po wciśnięciu "Przepuść zawsze" (lub "Blokuj zawsze") zostaje utworzona reguła przepuszczająca (lub blokująca) ruch sieciowy danej aplikacji dla dowolnego zewnętrznego adresu IP i dla całego zakresu portów ("1-65535").

d) Dla połączeń przychodzących, po wciśnięciu "Przepuść zawsze" (lub "Blokuj zawsze") zostaje utworzona reguła przepuszczająca (lub blokująca) ruch sieciowy danej aplikacji dla pojedynczego zewnętrznego adresu IP i dla całego zakresu portów ("1-65535").

Rodzaj połączeń można w prosty sposób rozpoznać: jeśli po lewej stronie okienka z komunikatem ArcaVir'a znajduje się adres/nazwa komputera użytkownika, to połączenie jest wychodzące; gdy nazwa/adres komputera użytkownika znajduje się po prawej stronie okienka z komunikatem ArcaVir'a, to połączenie jest przychodzące.

⊕ Opcja „Zapora sieciowa → Harmonogram”



Zaznaczenie opcji "Blokuj sieć" spowoduje programowe odłączenie komputera od sieci. Harmonogram pozwala określić, kiedy stosowana będzie blokada sieci. Zielony pasek naniesiony na tablicy z harmonogramem tygodniowym, wyznacza okresy, w których dostęp do sieci jest możliwy. W pozostałych okresach program blokuje dostęp do sieci.

4.6.3.2. Antyspam

Moduł antyspamowy oferuje możliwość klasyfikowania przychodzącej do nas poczty jako spam lub ham. Do oznaczania przychodzącej do nas niechcianej poczty wykorzystywane są trzy elementy:

- biała lista,
- czarna lista,
- filtrowanie na podstawie statystyk.

Te trzy elementy mogą być stosowane niezależnie od siebie. Można wykorzystać je pojedynczo lub łącznie, w celu zwiększenia skuteczności klasyfikacji listów.

Pojęcia podstawowe

Przy posługiwaniu się modułem antyspamowym, niezbędna będzie znajomość kilku podstawowych definicji.

SPAM to niechciane, często rozsyłane automatycznie, wiadomości pocztowe, nierzadko o charakterze komercyjnym. W najprostszej definicji spam oznacza wszystkie wiadomości, których nie chcemy otrzymywać.

HAM to wszystkie listy, które chcemy otrzymywać, np. korespondencja prywatna bądź wiadomości z list dyskusyjnych, na które świadomie się zapisaliśmy.

Biała lista służy do określenia adresów e-mail zaufanych nadawców. Listy wysyłane do nas przez nadawców znajdujących się na białej liście nie będą nigdy uznawane, za spam.

Czarna lista służy do określenia adresów e-mail nadawców rozsyłających spam. Listy wysłane przez nadawców znajdujących się na czarnej liście będą zawsze uznawane za spam, niezależnie od ich treści.

RBL (ang. **Realtime Block List** lub **Relay Block List**) to udostępniane w Internecie listy adresów IP, które są znanymi źródłami spamu (adresy IP spamerów lub serwerów SMTP typu open-relay, umożliwiających rozsyłanie spamu). Dostęp do takich baz jest możliwy dzięki wykorzystaniu systemu DNS. Każdy e-mail zawiera informację o swojej trasie – w nagłówku listu znajdują się adresy IP komputerów, za pośrednictwem, których list został przesłany od nadawcy do odbiorcy. Wystąpienie adresu z RBL staje się dodatkową przesłanką do uznania wiadomości jako spam.

⊕ Opcja „AntySpam → Ustawienia użytkownika”

Można tu określić podstawowe ustawienia w konfiguracji modułu antyspamowego.

W zależności od wybranego poziomu bezpieczeństwa, moduł antyspamowy różnie klasyfikuje przychodzące do nas przesyłki.



- Poziom Niski (tylko czarna lista). Listy są uznawane za spam tylko wtedy, gdy nadawca znajduje się na czarnej liście.
- Poziom Standardowy – ustawienie domyślne. Listy są klasyfikowane przy wykorzystaniu białej i czarnej listy oraz filtrowane na podstawie statystyk – domyślnie włączone są statystyki słów.
- Wysoki (tylko biała lista). Listy są uznawane za ham tylko wtedy, gdy nadawca znajduje się na białej liście.
- Ustawienia użytkownika. Poziom ten pozwala na całkowicie dowolne ustawienia poszczególnych elementów modułu antyspamowego. Na tym poziomie moduł klasyfikuje listy w następujący sposób:
 1. Jeśli włączona jest biała lista i znajduje się na niej adres nadawcy, to list jest oceniany jako ham.
 2. Jeśli włączona jest czarna lista i znajduje się na niej adres nadawcy, to list jest oceniany jako spam.
 3. Jeśli włączone jest filtrowanie na podstawie statystyk, to list jest oceniany na podstawie treści przy wykorzystaniu statystyk włączonych w ramce „Filtr”.

Historia

Określa jak długo listy mają być przechowywane na dysku, licząc od momentu ich otrzymania. Służy do przechowywania informacji o odebranych mail-ach na podstawie, których można uczyć moduł antyspamowy.

Elementy modułu

- Włącz białą listę – włącza sprawdzanie występowania adresu nadawcy wiadomości w spisie białej listy.
- Włącz czarną listę – włącza sprawdzanie występowania adresu nadawcy wiadomości w spisie czarnej listy.

- Włącz filtrowanie na podstawie statystyk – włącza klasyfikację przy zastosowaniu metod statystycznych, w oparciu o analizę treści listu. Rodzaje wykorzystywanych statystyk można określić za pomocą ustawień w ramce „Filtr”.

Filtr

- **Włącz statystyki słów** – zaznaczenie opcji powoduje klasyfikowanie wiadomości na podstawie częstotliwości występowania poszczególnych słów z listu w spamie i hamie.
- **Włącz statystyki słów dla sprawdzanych RBL-i** – zaznaczenie opcji powoduje sprawdzanie występowania adresów IP z nagłówka odebranej wiadomości w bazach RBL. Sposób dodawania RBLi do sprawdzania, opisany jest w opcji Opcja „AntySpam > Ustawienia użytkownika > Rbl”.
- **Włącz statystyki dopasowania wyrażeń regularnych** – zaznaczenie opcji spowoduje sprawdzanie, czy w wiadomości występują ciągi znaków pasujące do wyrażeń regularnych zdefiniowanych przez użytkownika. W procesie klasyfikacji listu wykorzystane zostaną statystyki wystąpień tych wyrażeń w spamie i hamie. Sposób definiowania wykorzystywanych wyrażeń regularnych, opisany jest w Opcja „AntySpam > Ustawienia użytkownika > Wyrażenia regularne”.

Znaczniki dodawane do wiadomości

- Znacznik spamu (domyślnie tj. ***SPAM***)
- Znacznik hamu

Pola określają tekst dodawany przez moduł antyspamowy do tematu otrzymanej wiadomości.

⊕ Opcja „AntySpam > Ustawienia użytkownika > Rbl”

Lista zawiera adresy RBLi, w których sprawdzane są adresy IP z nagłówka otrzymanej wiadomości. Do listy należy dodawać adresy RBLi w formie standardowych nazw domenowych. Kilka przykładowych RBLi:

- all.rbl.kropka.net
- bl.spamcop.net
- dnsbl.sorbs.net
- relays.ordb.org
- cbl.abuseat.org
- list.dsbl.org
- sbl-xbl.spamhaus.org
- dnsbl.njabl.org

Adresy i opis RBLi można znaleźć między innymi pod adresem:
<http://www.dnsbl.info/dnsbllist.asp>

⊕ *Opcja „AntySpam → Ustawienia użytkownika → Wyrażenia regularne”*

Lista zawiera wyrażenia regularne, określające wzorce tekstów, które mogą wystąpić w wiadomości. Wyrażenia te dopasowane są do całego tekstu wiadomości, włącznie z polami nagłówka. Podczas uczenia modułu następuje ustalenie, czy dane wyrażenie jest charakterystyczne dla spamu czy hamu.

Opcja „AntySpam → Ustawienia użytkownika → Biała (Czarna) lista”

Elementami zarówno białej, jak i czarnej listy, mogą być jedynie standardowe adresy e-mail, np. User@arcabit.com. W adresach można wykorzystać znak * dla oznaczenia dowolnego ciągu znaków. Pozwala to tworzyć pozycje listy pasujące do wielu adresów e-mail, na przykład wszystkich adresów ze wskazanej domeny. Możemy w ten sposób uniknąć konieczności żmudnego dodawania wielu pojedynczych pozycji do listy.

Przykłady:

- *@arcabit.pl - pasuje do wszystkich adresów z domeny „arcabit.pl”, np. user1@arcabit.pl, user2@arcabit.pl, xyz@arcabit.pl
- *@arcabit.* - pasuje do wszystkich adresów e-mail, których pierwszy człon domeny to „arcabit”, np. user@arcabit.com.pl, user@arcabit.com, user@arcabit.pl
- *.pl - pasuje do wszystkich adresów z końcówką domeny „.pl”
- User@* - pasuje do wszystkich adresów z nazwą konta „user” w dowolnej domenie

⊕ *Opcja „AntySpam → Ustawienia użytkownika → Opcje zaawansowane”*

Maksymalna liczba słów wykorzystywana do analizy – jest to największa liczba słów, jaka zostanie pobrana z przychodzącego listu do stwierdzenia, czy jest to spam, czy ham. Jeśli ilość słów w wiadomości jest mniejsza od tej wielkości, wykorzystywane są wszystkie słowa.

Maksymalna liczba słów w statystykach – maksymalna wielkość słownika wykorzystywanego przy analizie przychodzących wiadomości. Wielkość tego parametru wpływa na

skuteczność, prędkość skanowania wiadomości i uczenia modułu. Zmniejszenie tej wielkości przyspieszy skanowanie i uczenie, może jednak powodować obniżenie skuteczności modułu.

Maksymalna wielkość skanowanej wiadomości (kB) – określa maksymalną wielkość skanowanej wiadomości w kilobajtach. Przesyłki przekraczające tę wielkość nie będą skanowane i oceniane przez moduł antyspamowy.

Maksymalna liczba niesklasyfikowanych wiadomości – określa dopuszczalną ilość wiadomości, które mogą być niesklasyfikowane przez użytkownika, zanim zostanie wygenerowane ostrzeżenie o konieczności nauczenia modułu antyspamowego. Po przekroczeniu tej wielkości potrzeba nauczenia modułu jest sygnalizowana za pomocą migającej ikony ArcaVir w zasobniku systemowym.

Ważne! Wpisanie wartości „0” w pole **Maksymalna liczba niesklasyfikowanych wiadomości** wyłącza ostrzeżenia o konieczności nauczenia modułu antyspamowego.

Uczenie modułu – więcej w dziale 5.4.1. Antyspam – naucz mnie

4.6.3.3. Skaner HTTP

Konfiguracja Skanera HTTP dzieli się na:

- Reguły skanowania – pozwalają określić maksymalny rozmiar skanowanego pliku, głębokość skanowanego archiwum, poziom heurystyki, wykrywanie Dialerów/Spyware/Adware/Riskware oraz skanowanie plików UPX
- Biała lista – lista stron internetowych nie skanowanych przez skaner http
- Filtrowanie treści – usuwanie aktywnych treści (aplety, skrypty Javy, kontrolki Activex), usuwanie banerów,
- Czarna lista banerów – zdefiniowanie adresy serwerów z niechcianymi banerami.

4.6.3.4. Monitor rejestru

W oknie monitora rejestru znajdują się Ustawienia podstawowe oraz Lista monitorowanych kluczy.

Ustawienia podstawowe zawierają opcje: Aktywacji monitora rejestru przy starcie systemu oraz Twórz raport.



Lista monitorowanych kluczy wyświetla informacje, jakie klucze są aktualnie monitorowane. Można je samemu modyfikować i ustawiać wedle własnych upodobań. Czasami zachodzi potrzeba wykluczenia z procesu monitorowania określonych wartości z wybranych kluczy.

Należy wtedy wybrać gałąź **Wykluczenia** w drzewie **Monitor Rejestru**. Wykluczenia powodują, że wartości zawarte w kolumnie **Etykieta**, występujące w odpowiadających im kluczach w kolumnie **Klucz** nie będą brane pod uwagę w trakcie monitorowania i wszelkie zmiany będą w ich przypadku pomijane. Jeśli Monitor Rejestru jest aktywny, to każda zmiana w zaznaczonych kluczach, nieuwzględniona w wykluczeniach, spowoduje wyświetlenie okna dialogowego z informacją o wprowadzonej zmianie. W każdym momencie można zmienić zawartość listy monitorowanych kluczy na domyślną, naciskając w głównym oknie przycisk **Domyślne**.

W zależności od rodzaju wprowadzonej modyfikacji, mamy możliwość podjęcia kilku decyzji:

- **Usuń klucz** – kasuje utworzony klucz.
- **Przywróć poprzednią wartość** – pozwala wycofać wprowadzoną zmianę.
- **Usuń wpis** – kasuje wartość.
- **Nic nie rób** – pomija zmianę.

W oknie tym można również wygodnie dodać do wykluczeń wprowadzoną modyfikację. Wystarczy zaznaczyć opcję **Dodaj do wykluczeń**. Jeśli zaznaczymy opcję **Twórz raport**, to wszystkie zdarzenia wykryte przez Monitor Rejestru odnotowane zostaną w systemie raportowania. Raport zawiera informacje o czasie wystąpienia zdarzenia, jego opis i akcję podjętą przez użytkownika.

4.6.3.5. Kontrola rodzicielska



Użytkownik ma do dyspozycji kilka prostych, a zarazem skutecznych mechanizmów kontrolnych.

Pierwszy z nich to tzw. biała oraz czarna lista adresów.

Biała lista zawiera adresy (adresy mogą być definiowane również jako fragmenty adresów lub wręcz wyrażenia regularne), do których dostęp

uznajemy za bezpieczny.

Na **czarnej liście** umieszczamy te adresy, które uznajemy za niepożądane (podobnie jak w przypadku białej listy, możemy tutaj podać także fragmenty adresów, pojedyncze wyrazy lub wyrażenia regularne). Przykład wykorzystania: jeśli chcemy zablokować dostęp do wszystkich stron poza wybranymi, to na czarnej liście umieszczamy wyrażenie identyfikujące wszystkie adresy - ".*" (kropka gwiazdka), a na białej liście umieszczamy adresy dopuszczone.

Drugim mechanizmem filtrującym jest kontrola zawartości stron WWW. Podobnie jak w przypadku adresów, możemy tutaj określić dowolne wyrażenia i ich wpływ na klasyfikację strony jako dopuszczoną albo zakazaną.

Dodatkowo użytkownik może zdefiniować, kiedy sieć ma być dostępna, a kiedy dostęp do sieci ma być zablokowany. **Opcja „Zapora sieciowa → Harmonogram”** więcej na stronie 31.

Ważne! Aby mieć pewność, że narzucone restrykcje będą przez pakiet ArcaVir pilnowane, musimy zabezpieczyć hasłem możliwość zmiany opcji pakietu i aktywności modułów.

4.6.4. Obsługa pakietu

4.6.4.1. Kwarantanna

Po wybraniu opcji kwarantanny zostanie wyświetlone okno dające możliwość zdefiniowania podstawowych parametrów pracy kwarantanny:

- **Maksymalny rozmiar pliku** – graniczny rozmiar pliku, powyżej którego pliki nie będą umieszczane w kwarantannie
- **Folder kwarantanny** – folder, w którym będą umieszczane zainfekowane pliki
- **Pytaj o docelową lokalizację przy odtwarzaniu plików** – jeśli włączysz tę opcję, to przy każdym odtwarzaniu pliku kwarantanna zapyta o docelowy folder
- **Usuwanie plików z kwarantanny.**

4.6.4.2. Zadania

Program umożliwia zdefiniowanie zadań skanowania, aktualizacji i kopii zapasowej, które będą wykonywane automatycznie zgodnie z określonym harmonogramem.

Aby utworzyć nowe zadanie należy kliknąć na przycisk **Dodaj**. W oknie dodaj zadanie wpisujemy nazwę zadania np. *skanowanie raz w miesiącu*. W typie zadania do uruchomienia wybieramy jedną z trzech

opcji **Aktualizacja, Skaner lub kopia zapasowa**. Z parametrów zadania wybieramy *Profil* a następnie *Skanuj Mój Komputer*. Przy wyborze kopii zapasowej musimy utworzyć wcześniej jej profil w **Narzędzia -> Kopie zapasowe**. Na koniec musimy jeszcze ustawić parametry uruchamiania zadania.

Mamy do wyboru:

- Przy starcie systemu
- Według ustawień czasowych
- Tygodniowy



4.6.4.3. Powiadamianie

Program, umożliwiał wysyłanie informacji o wykryciu zagrożenia do odbiorców znajdujących się na przygotowanej wcześniej liście. Powiadomienia można wysyłać przy pomocy poczty elektronicznej, usługi poštaniec oraz systemu komunikatów SMS.

4.6.5. Narzędzia

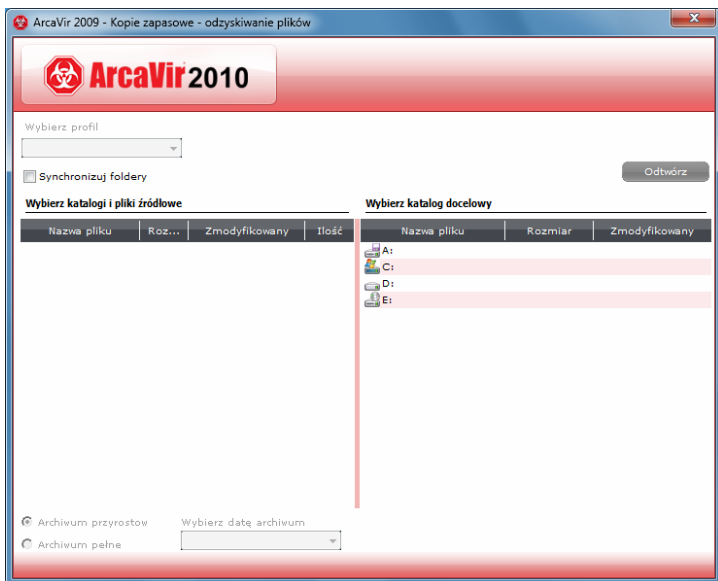
Zawiera dodatkowe narzędzia wspomagające i podnoszące bezpieczeństwo komputera chronionego przez pakiet ArcaVir 2010.

4.6.5.1. Kopie zapasowe

Konfigurujemy profil kopii zapasowej, czyli wybieramy, jakie dane mają być archiwizowane przez program. Aby utworzyć profil kopii zapasowej klikamy na przycisk **Dodaj**. W oknie Profil wpisujemy nazwę profilu. Wskazujemy również folder archiwum, czyli miejsce gdzie kopia będzie zapisywana. Wybieramy rodzaj kopii zapasowej Pełna lub Przyrostowa. Przyrostowa polega na uzupełnieniu wcześniej utworzonej kopii plikami nowym lub zmienionymi, pozostałe nie są zmieniane. Jest ona dużo szybciej wykonywana niż kopia pełna. Możemy również podać maksymalny rozmiar archiwum, jakie ma zostać utworzone z kopią. Jeżeli nie chcemy kontrolować jego wielkości zaznaczamy opcję „Bez ograniczeń”. Jeżeli zaś chodzi o usuwanie starych kopii to można je kasować według następującej zasady: Usun starsze niż (liczba dni) dni.

Kolejnym krokiem jest wskazanie obszarów, z jakich będzie tworzona kopia. Wskazujemy je przyciskiem **Dodaj**. Możemy wskazywać dowolne pliki z różnymi rozszerzeniami np.: *.doc lub wybrane pojedyncze pliki oraz foldery. Po ich wybraniu klikamy na przycisk **OK**. W liście obszarów pojawił się nasz wpis. Po zamknięciu tego okna widzimy również nowy wpis w oknie z listą profili. W razie potrzeby możemy dowolnie je modyfikować przez kliknięcie na przycisk Zmień.

Ważne! Konieczne jest jeszcze ustawienie zadania, które będzie uruchamiało i tworzyło kopie zapasową. Konfiguracja zadania zostało to opisane w dziale **4.6.4.2. Zadania**.



4.6.6. Aktualizacja

Konfiguracja Aktualizacji zawiera następujące opcje:

- Aktywuj moduł aktualizacji
- Włącz aktualizację alertową
- Dopuszczaj restarty w czasie aktualizacji oprogramowania. Jeśli użytkownik nie zezwoli na restart maszyny, a restart będzie wymagany do poprawnego zakończenia aktualizacji, to przywrócony zostanie stan sprzed aktualizacji
- Informuj o zakończeniu abonamentu
- Pokaż pasek postępu aktualizacji.

Ważne! Jeśli w trakcie pobierania pliku przerwany zostanie proces aktualizacji, to kolejna próba pobrania pliku wznowiona zostanie od tego miejsca, w którym proces został przerwany.

4.6.6.1. Ustawienia aktualizacji

Możemy tu określić, czy ma być aktualizowany tylko program, tylko repozytorium czy jednocześnie program i repozytorium. Możemy także wskazać foldery pobierania dla aplikacji i repozytorium, oraz udostępnić utworzone repozytorium komputerom w sieci wykorzystując w tym celu protokół http.

Repozytorium

Opcja ta jest szczególnie przydatna w dużych sieciach, gdy jedna stacja aktualizuje repozytorium z Internetu, a wszystkie pozostałe aktualizują się z repozytorium utworzonego na tej stacji. W efekcie odciążamy łącza „ze światem”. Aby utworzyć repozytorium, należy wskazać folder, do którego mają być pobierane pliki aktualizacyjne i udostępnić wskazany zasób w sieci lokalnej. Proces aktualizacji stacji z repozytorium może wykorzystać mechanizm udostępniania plików i folderów oferowany przez Windows, lub też jeden z protokołów HTTP bądź FTP. Mając na uwadze względy bezpieczeństwa oraz wygodę użytkownika, sugerujemy wykorzystanie protokołu HTTP do udostępniania zawartości repozytorium. Program **ArcaVir 2010** zawiera moduł serwera HTTP, którego zadaniem jest udostępnianie repozytorium w sieci. Aby go uruchomić wystarczy zaznaczyć opcję **Udostępnij repozytorium** w opcji **Udostępnij repozytorium po HTTP** i wskazać port, na którym ma działać usługa (domyślnie jest to port 80). Teraz na stacjach, które mają pobierać aktualizację z repozytorium, w opcji „Aktualizacja > Server” wystarczy wybrać protokół HTTP, a w polu adres wpisać adres stacji udostępniającej repozytorium w postaci: `http://adres_IP_stacji`.

Ważne! Jeżeli komputer udostępniający repozytorium chroniony jest przez program zapory sieciowej (firewall), to należy w konfiguracji zapory odblokować możliwość świadczenia serwisu przez serwer http wykorzystywany do udostępniania repozytorium. Konfiguracja zapory sieciowej w ArcaVir zostanie automatycznie prawidłowo zmodyfikowana.

4.6.6.2. Serwer

Opcja ta pozwala wybrać protokół i serwer dla procesu aktualizacji, a także określić parametry autoryzacji, jeśli jest ona wymagana. Można także podać parametry serwera proxy.

4.7. Raporty

Dostęp do listy zdarzeń w systemie ochrony antywirusowej uzyskujemy po wybraniu opcji **Raporty** w głównym oknie programu.

4.7.1. Raporty pakietu

Zawierają informacje o wszystkich zdarzeniach i incydentach, jakie miały miejsce w systemie. Pochodzą one ze skanera, monitora antywirusowego, modułu aktualizacji, zadań, ochrony rodzicielskiej, serwera Exchange, szybkiego skanowania, monitora rejestru, skanera poczty, zarządzania i skanera http.

Ważne! Listę zdarzeń można sortować według każdej z kolumn klikając na jej nagłówek. Dwukrotne kliknięcie na zdarzenie spowoduje wyświetlenie okna zawierającego szczegółowe informacje na temat wybranego zdarzenia.

4.7.2. Raporty zapory sieciowej

Przejrzysty widok raportów pozwala użytkownikowi oglądać historię połączeń sieciowych. Można dzięki temu wykryć potencjalne zagrożenia dla systemu (aktywność podejrzanych programów, próby włamań do systemu, próby ataków wirusów). Okno raportu zawiera bogaty zestaw filtrów ułatwiających analizę zgromadzonych informacji. Pozwalają one na wygodne wyszukiwanie podejrzanych połączeń i nadmiernej aktywności sieciowej aplikacji. W przypadku nieznanymi lub potencjalnie podejrzanych połączeń widocznych w raporcie, można uzyskać o nich dodatkowe informacje.

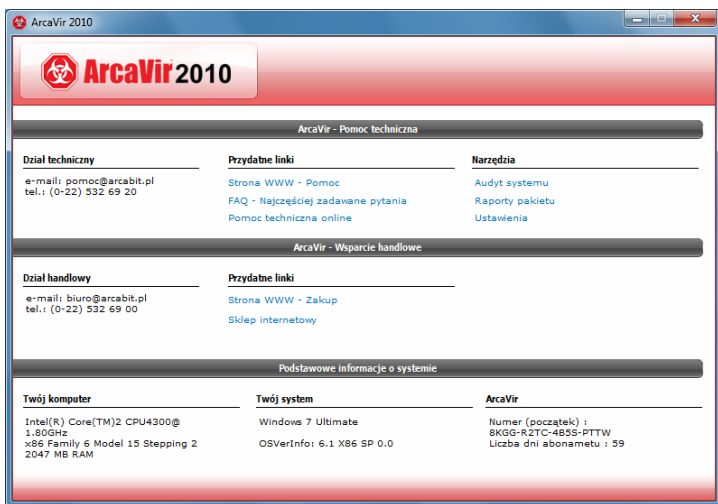
4.8. Kwarantanna

Moduł kwarantanny pozwala na bezpieczne przechowywanie na dysku podejrzanych plików. Pliki w kwarantannie są zaszyfrowane, dzięki czemu w żaden sposób nie stanowią zagrożenia zarówno dla systemu jak i dla zawartych w nim danych. Kwarantanna pozwala na wygodne zarządzanie przechowywanymi w niej plikami. Pliki można w dowolnym momencie przeskanować wykorzystując aktualną wersję bazy, odtworzyć albo przesłać do wsparcia technicznego firmy ArcaBit.

4.9. Pomoc




W oknie tym podane są informacje na temat:

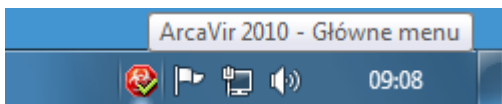
- pomocy technicznej do programu - tel. (022) 532-69-20 email: pomoc@arcabit.pl Pomoc telefoniczna udzielana jest zarejestrowanym użytkownikom oprogramowania firmy ArcaBit. Pomoc telefoniczna świadczona jest od poniedziałku do piątku w godzinach 8:00 - 20:00.
- możliwościach zakupu programu, tel. (022) 532-69-10, fax. (022) 532-69-01, biuro@arcabit.pl
- podstawowych informacji o systemie.



ArcaVir - Pomoc techniczna		
Dział techniczny e-mail: pomoc@arcabit.pl tel.: (0-22) 532 69 20	Przydatne linki Strona WWW - Pomoc FAQ - Najczęściej zadawane pytania Pomoc techniczna online	Narzędzia Audyt systemu Raporty pakietu Ustawienia
ArcaVir - Wsparcie handlowe		
Dział handlowy e-mail: biuro@arcabit.pl tel.: (0-22) 532 69 00	Przydatne linki Strona WWW - Zakup Sklep internetowy	Podstawowe informacje o systemie
Twój komputer Intel(R) Core(TM)2 CPU4300@ 1.80GHz x86 Family 6 Model 15 Stepping 2 2047 MB RAM	Twój system Windows 7 Ultimate OSVerInfo: 6.1 X86 SP 0.0	ArcaVir Numer [początek] : 8KGG-R2TC-485S-PTTW Liczba dni abonamentu : 59

5. Zasobnik systemowy (ikona ArcaVir 2010)

Służy do szybkiej komunikacji użytkownika z programem ArcaVir 2010. Kolor czerwony  oznacza, że program ArcaVir 2010 jest włączony i chroni komputer. Natomiast żółty wykrzyknik  na ikonie ArcaVir 2010 oznacza, że ochrona antywirusowa jest wyłączona. Migająca niebieska strzałka  oznacza aktualizację programu.



Kliknięcie na nią lewym klawiszem myszki powoduje uruchomienie głównego okna programu ArcaVir 2010. Kliknięcie prawym klawiszem myszki na ikonę programu rozwija menu kontekstowe z opcjami jak na rysunku poniżej:



5.1. Otwórz ArcaVir 2010

Otwiera główne okno programu ArcaVir 2010. Okno to zostało opisane w rozdziale **4. Obsługa ArcaVir 2010**.

5.2. Skanowanie

Pozwala szybko wywołać skanowanie:

- **pełne** (skanuje mój komputer, wybrane foldery, CD/DVD oraz dyskietki)
- **szybkie** (skanuje uruchomione procesy).

5.3. Aktualizacja

Uruchamia aktualizację oprogramowania ArcaVir 2010. Program łączy się z serwerami firmy ArcaBit w celu sprawdzenia od „ręki” dostępnych aktualizacji baz wirusów jak również oprogramowania.

5.4. Obsługa pakietu

Na obsługę pakietu składa się:

- Antyspam – naucz mnie
- Kwarantanna
- Naprawa instalacji
- Rejestracja

5.4.1. Antyspam – naucz mnie

Moduł antyspamowy bezpośrednio po zainstalowaniu nie będzie poprawnie rozpoznawał całego spamu. Wynika to ze sposobu działania – moduł “uczy się” na przykładach. Takie rozwiązanie ma na celu dopasowanie zachowania modułu do tego, co każda osoba indywidualnie uznaje za spam. Moduł przechowuje otrzymane wiadomości, dając użytkownikowi możliwość wskazania, które przesyłki mają być uznawane za spam. Dopiero po wskazaniu kilku przykładowych listów, klasyfikacja spamu zacznie działać poprawnie.

Narzędzie do uczenia modułu antyspamowego można uruchomić z poziomu ArcaVir Menu w zasobniku systemowym. Należy wybrać: **Obsługa pakietu → AntySpam – naucz mnie.**

Na ekranie zostanie wyświetlone okno dialogowe Lista **Historia** zawiera informacje o wiadomościach odebranych w czasie, gdy moduł antyspamowy był aktywny. Jeśli moduł był wyłączony lub nie zostały odebrane żadne wiadomości, to lista będzie pusta. Domyślnie w liście widoczne są kolumny: Temat, Nadawca, Ocena filtru, Poprawna ocena i Prawdopodobieństwo.

Kolumna **Ocena filtru** pokazuje jak dany list ocenił moduł antyspamowy.

Kolumna **Ocena użytkownika** pokazuje ocenę użytkownika. Domyślna wartość w tej kolumnie dla każdego nowo odebranego listu to **NIESKLASYFIKOWANY**.

Nienauczony moduł antyspamowy będzie klasyfikował większość przesyłek jako ham. Uczenie modułu polega na wskazywaniu przykładów spamu i hamu w otrzymanych listach. Jeżeli w historii znajdują się jakieś listy, których nie chcemy otrzymywać, należy zaznaczyć je i nacisnąć przycisk **Oceń jako SPAM**. Wszystkie pozostałe przesyłki, np. Listy od znajomych, należy zaznaczyć i nacisnąć przycisk **Oceń jako HAM**. Po pewnym czasie moduł powinien poprawnie znajdować SPAM.

Ważne! Pojedynczy list można zaznaczyć klikając na niego lewym przyciskiem myszy. Kilka listów występujących po sobie wybieramy zaznaczając pojedynczy list (początkowy), a następnie trzymając wciśnięty klawisz SHIFT zaznaczamy list końcowy. Aby wybrać kilka listów niekoniecznie sąsiadujących ze sobą, należy zaznaczyć je trzymając wciśnięty klawisz CTRL.

Opis przycisków:

Odśwież – odczytuje na nowo historię odebranych wiadomości,

Oceń jako SPAM – zmiana oceny wybranych wiadomości na SPAM,

Oceń jako HAM – zmiana oceny wybranych wiadomości na HAM,

Usuń z historii – usuwa z dysku plik z wybranymi wiadomościami,

Dodaj do białej listy – dodaje e-mail do białej listy i jest zawsze znakowany jako HAM,

Dodaj do czarnej listy – dodaje e-mail do czarnej listy i jest zawsze znakowany jako SPAM,

Pokaż SPAM – w historii pokazywane są wiadomości, które zostały ocenione jako spam przez moduł lub użytkownika,

Pokaż HAM – w historii pokazywane są wiadomości, które zostały ocenione jako ham przez moduł lub użytkownika,

Pokaż wszystko – pokazuje wszystkie listy,

Importuj Statystyki/Eksportuj statystyki – umożliwia zapisanie aktualnych ustawień i ich późniejsze zaimportowanie np. po reinstalacji programu ArcaVir 2010,

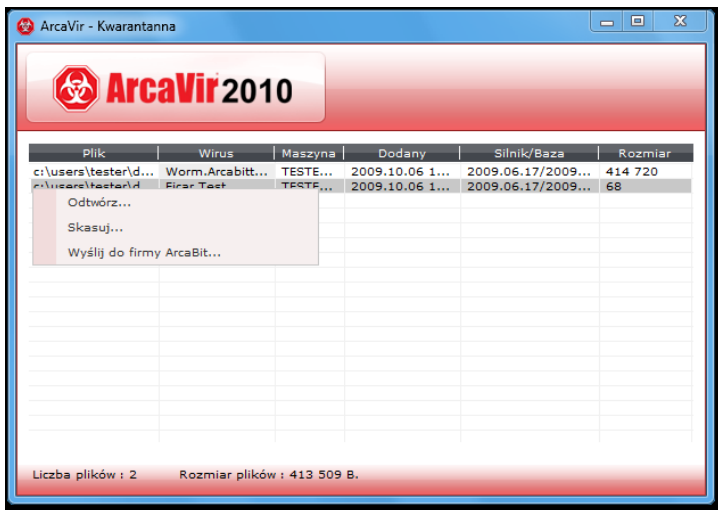
Wybierz kolumny – wyświetla okno dialogowe pozwalające wybrać widoczne w liście kolumny.

Część z opisanych powyżej operacji może być wykonana z poziomu menu kontekstowego, które uruchomi się po kliknięciu prawym klawiszem myszy w obszarze listy. Jest ono dostępne wtedy, gdy na liście zaznaczona jest przynajmniej jedna pozycja. W menu kontekstowym znajduje się kilka dodatkowych opcji:

- **Dodaj nadawcę do CZARNEJ LISTY** – dopisanie adresów z zaznaczonych listów do czarnej listy,
- **Dodaj nadawcę do BIAŁEJ LISTY** – dopisanie adresów z zaznaczonych listów do białej listy,
- **Podgląd** – otwiera okno z podglądem listu. Zawartość listu nie jest interpretowana. Okno zawiera cały tekst wiadomości wraz z nagłówkiem. Podgląd można również

wywołać poprzez podwójne kliknięcie lewym przyciskiem myszy na zaznaczonej pozycji listy.

5.4.2. Kwarantanna



Dostęp do kwarantanny uzyskujemy z menu **Obsługa Pakietu** → **Kwarantanna** po naciśnięciu ikony programu prawym klawiszem myszy w zasobniku systemowym. Po wybraniu opcji **Kwarantanna** pojawi się okno umożliwiające zarządzanie plikami, które zostały umieszczone w kwarantannie. Kwarantanna dostarcza następujących informacji o plikach, które zawiera:

- oryginalna nazwa pliku,
- nazwa wirusa/trojana/robaka, którym plik jest zainfekowany,
- nazwa komputera, na którym plik został znaleziony,
- data i czas dodania pliku do kwarantanny,
- wersja silnika antywirusowego i bazy wirusów, którymi plik został zidentyfikowany jako zainfekowany,
- rozmiar pliku.

Po zaznaczeniu plików w kwarantannie można wykonać na nich wybrane operacje, klikając prawym przyciskiem myszy:

- **Odtwórz** – wskazane pliki zostaną skasowane z kwarantanny i umieszczone w folderach, w których pierwotnie się znajdowały (pliki nie zostaną wyleczone).
- **Skasuj** – wskazane pliki zostaną usunięte z kwarantanny i z dysku. Nie będzie możliwości odzyskania ich zawartości.
- **Wyślij do firmy ArcaBit** – wysła zainfekowany plik do firmy ArcaBit w celu przeprowadzenia analizy zagrożenia.

W formacie przygotowującej wysłanie pliku do analizy należy podać swój adres e-mail, temat oraz wpisać komentarz. Zaznaczone pliki zostaną automatycznie dołączone do wysyłanej wiadomości. Listę załączników można zmodyfikować, wykorzystując w tym celu przyciski **Dodaj** i **Usuń**.

5.4.3. Naprawa instalacji

Naprawa instalacji jest narzędziem, z którego należy skorzystać w sytuacji, gdy pojawią się problemy w użytkowaniu programu. Na przykład wtedy, gdy pomimo podejmowanych prób uruchomienia któregoś ze składników, składnik ten nie chce się uruchomić lub wyświetla komunikaty o błędach.

5.4.4. Rejestracja

Służy ona do rejestracji online produktów firmy ArcaBit. Po zakupie programu i otrzymaniu numeru licencji należy zarejestrować swoją licencję wypełniając na naszej stronie formularz rejestracji.

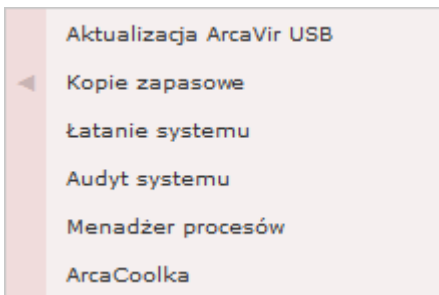
Rejestracja umożliwi Państwu korzystanie z telefonicznej Pomocy Technicznej, która świadczona jest w dni robocze w godzinach 8:00 - 20:00.

5.4.5. Tryb gry - włącz

Gdy „tryb gry” jest włączony, nie są wyświetlane okienka alertowe i nie jest uruchamiana alertowa aktualizacja. W przypadku każdego modułu jest podejmowana domyślna akcja (czyli zazwyczaj "blokuje").

5.5. Narzędzia

W ArcaVir 2010 dostępne są dodatkowe narzędzia rozszerzające funkcjonalność programu antywirusowe takie jak:



5.5.1. Aktualizacja ArcaVir USB

Opcja "Aktualizacja ArcaVir USB" służy do aktualizacji baz wirusów na oryginalnych napędach pendrive firmy ArcaBit.

5.5.2. Kopie zapasowe



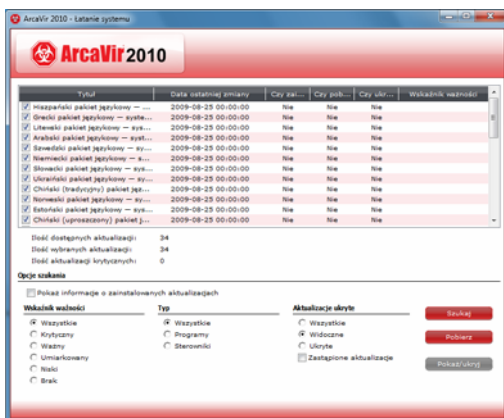
Kopie zapasowe to wygodne i wszechstronne narzędzie pozwalające na tworzenie kopii zapasowych ważnych danych.

Program posiada intuicyjną konfigurację, dzięki której użytkownik może bez problemów zdefiniować, jakie zasoby mają być archiwizowane.

Zgodnie z założonym harmonogramem program automatycznie wykonuje kopie zapasowe. Gdy zajdzie taka konieczność, pliki można szybko odzyskać.

5.5.3. Łatanie systemu

To moduł do zarządzanie łataniami i aktualizacjami systemów Windows. Moduł „Łatanie systemu” uzupełnia mechanizm Windows Update dając użytkownikom wygodny dostęp zarówno do aktualizacji krytycznych jak i opcjonalnych. Program pozwala na elastyczne pobieranie wybranych aktualizacji i instalację ich w dogodnym dla użytkownika momencie.



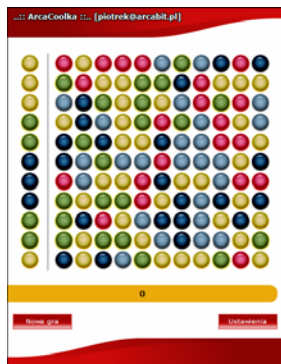
5.5.4. Audyty systemu

Jest to raport dotyczący bieżącego stanu systemu operacyjnego komputera. Audyt o systemie zawiera informacje na temat ważnych kluczy rejestru systemowego oraz istotnych dla prawidłowej pracy systemu plików. Na podstawie przygotowanego raportu, specjaliści firmy ArcaBit będą mogli ustalić, czy w systemie zostały zainstalowane i są aktywne szkodliwe obiekty. Aby utworzyć raport, należy nacisnąć przycisk **Start**. Przygotowany raport można wysłać do firmy ArcaBit. Należy podać swój adres e-mail oraz opisać problem, który był powodem przygotowania raportu. Uporządkowana tematycznie forma prezentacji ułatwia użytkownikowi dołączenie do raportu podejrzanych plików, a także samodzielne usunięcie ich z systemu. Narzędzie **Audyty systemu** wyposażone zostało w mechanizm umożliwiający przywrócenie stanu sprzed zmian, tzn. jeśli wykonamy operację usunięcia wskazanych plików czy też

Każda pozycja listy zawiera nazwę procesu, jego numer identyfikujący w systemie (PID), opis oraz nazwę producenta. W dolnej części okna wyświetlane są szczegółowe informacje na temat zaznaczonego procesu.

Operacje zakończenia działania procesu lub zmiany jego priorytetu w systemie dostępne są po wybraniu odpowiedniej opcji z menu kontekstowego.

5.5.6. ArcaCoolka



ArcaCoolka to prosta gra logiczna, w której gracz zdobywa punkty eliminując z planszy jak największe grupy kolorowych Coolek. Plansza posiada własną grawitację, więc każda modyfikacja układu powoduje reorganizację planszy. Wyczyszczenie pierwszej kolumny powoduje napływ nowych Coolek z poczekalni znajdującej się z lewej strony planszy. Wszystkie rekordy są rejestrowane przez nasz firmowy serwer - dlatego zachęcamy do wprowadzenia w **ArcaCoolce** prawidłowego adresu email, co pozwoli nam na

informowanie zwycięzców o nagrodach - tak tak, wraz z wprowadzeniem nowego modułu ogłaszamy permanentny konkurs na najlepszy wynik w miesiącu!

Notatki