Kaspersky Internet Security 2012
Poradnik recenzenta

KASPERSKY lab

Poradnik ten wyjaśnia, jak należy korzystać z oprogramowania Kaspersky Internet Security 2012 (KIS 2012) – zintegrowanego produktu zapewniającego ochronę systemu Microsoft Windows XP, Vista oraz Windows 7 przed szkodliwym oprogramowaniem, trojanami, atakami hakerskimi, spamem, oprogramowaniem spyware, phishingiem, wyciekami poufnych danych oraz niepożądaną treścią.

1 Wprowadzenie

Kaspersky Internet Security 2012 zapewnia doskonałą ochronę przed wirusami, trojanami, spamem, hakerami i innymi zagrożeniami. **Opiera się na nowym hybrydowym podejściu** do bezpieczeństwa cyfrowego, które łączy innowacyjne technologie oparte na chmurze z zaawansowaną ochroną antywirusową, aby zapewnić szybszą, skuteczniejszą reakcję na dzisiejsze złożone i nieustannie ewoluujące zagrożenia. Niezależnie od tego, czy korzystasz z bankowości online, portali społecznościowych czy dokonujesz zakupów przez Internet, możesz mieć pewność, że dane umożliwiające dostęp do twojego konta są bezpieczne, nie trafisz na szkodliwe strony internetowe i będziesz otrzymywał tylko bezpieczne wiadomości od znajomych i współpracowników. Dzięki zaawansowanej funkcji kontroli rodzicielskiej twoje dzieci mogą w sposób bezpieczny i odpowiedzialny korzystać z Internetu.

2 Kluczowe zalety

2.1 Ochrona proaktywna przed nieznanymi zagrożeniami

Dzisiaj nowe szkodliwe programy pojawiają się w niewiarygodnie szybkim tempie – każdego dnia przybywa około 35 000 nowych szkodników, przez co tradycyjna analiza sygnatur przestaje być skutecznym narzędziem zwalczania takich zagrożeń. Z tego powodu główną metodę zapewniania bezpieczeństwa stanowi ochrona proaktywna, której działanie polega na analizowaniu zachowania aplikacji i blokowaniu tych, które wydają się podejrzane.

KIS 2012 zawiera znacznie udoskonaloną technologię **Kontrola systemu,** która monitoruje i rejestruje aktywność wszystkich aplikacji w systemie, analizuje ich zachowanie i blokuje niepożądane akcje. **Kontrola systemu** umożliwia również cofnięcie działań dowolnego szkodliwego oprogramowania.

Więcej na temat nieznanych zagrożeń można przeczytać w następującym artykule:

Zagrożenia 2020: co przyniesie kolejna dekada?

http://www.kaspersky.pl/about.html?s=news_warnings&cat=4&newsid=1494

2.2 W kierunku ochrony opartej na “chmurze”

Krajobraz rozwiązań bezpieczeństwa zmienia się w coraz szybszym tempie. Obecnie każdego dnia pojawiają się dziesiątki tysięcy nowych cyberzagrożeń, co oznacza, że skuteczne rozwiązanie bezpieczeństwa musi sprostać nowym wymaganiom. W celu zapewnienia szybkiej reakcji na nowe zagrożenia KIS 2012, podobnie jak poprzednia wersja, zawiera **Kaspersky Security Network**, system baz danych online zlokalizowanych na serwerach Kaspersky Lab, które zawierają informacje o zaufanych, niebezpiecznych i podejrzanych aplikacjach. Bazy danych są bardzo szybko uaktualniane – po ustaleniu poziomu zagrożenia odpowiednia informacja pojawia się w bazie sygnatur w ciągu zaledwie kilku minut. Za każdym razem, gdy użytkownik uruchamia na komputerze plik, KIS odwołuje się do „chmury” w celu uzyskania aktualnych informacji o danej aplikacji i jej uprawnieniach systemowych.

KIS 2012 zapewnia rozszerzoną ochronę opartą na “chmurze”. Nowa funkcja **File Advisor** pozwala jednym kliknięciem sprawdzić reputację potencjalnie niebezpiecznych plików. Moduł **URL Advisor** ostrzega przed odsyłaczami do podejrzanych lub niebezpiecznych stron internetowych, pobierając “z chmury” najnowsze informacje o zasobach online.

2.3 Bezpieczeństwo online

Internet stanowi obecnie główne źródło szkodliwego oprogramowania znajdującego się na komputerach PC. Co więcej, stał się istotną częścią współczesnego życia i jest wykorzystywany między innymi do komunikacji, nauki, dokonywania zakupów itd. Dlatego tak istotna jest ochrona komputerów użytkowników przed najnowszymi zagrożeniami internetowymi.

KIS 2012 zapewnia całkowitą ochronę komputera podczas różnego rodzaju aktywności online: surfowania po Internecie, korzystania z poczty e-mail, komunikatorów internetowych (ICQ, MSN itd.), portali społecznościowych czy dokonywania zakupów online. Zwiększoną ochronę online zapewnia udoskonalony moduł **URL Advisor,** który pozwala użytkownikowi na odwiedzanie tylko zaufanych stron o dobrej reputacji, z kolei **Ochrona przed phishingiem** zabezpiecza dane przed hakerami, a **Bezpieczne uruchamianie stron internetowych** w połączeniu z modułem **Bankowość elektroniczna** zapewniają dodatkową warstwę ochrony podczas dokonywania płatności online oraz wprowadzania poufnych informacji.

Więcej na temat bezpieczeństwa internetowego można przeczytać w następującym artykule:

Oszustwa internetowe oraz jak się przed nimi bronić: poradnik dla opornych

http://www.viruslist.pl/analysis.html?newsid=642

1.1 Ochrona tożsamości cyfrowej podczas bankowości i zakupów online

Wraz z rozpowszechnianiem się aplikacji internetowych, takich jak rozwiązania wykorzystywane do bankowości online oraz handlu elektronicznego coraz większego znaczenia nabiera ochrona wszelkiego rodzaju danych osobistych. KIS 2012 zapewnia pełną ochronę takich informacji poprzez

blokowanie odsyłaczy do **zasobów wykorzystywanych w ramach ataków phishingowych,** oferowanie **wirtualnej klawiatury** w celu bezpiecznego wprowadzania haseł i zezwalanie na dostęp do danych użytkownika **tylko zaufanym aplikacjom**. Ponadto, specjalne systemy bezpieczeństwa **bankowości elektronicznej** zapewniają zwiększony poziom ochrony podczas dokonywania transakcji za pośrednictwem Internetu. Po wpisaniu adresu URL strony banku przeglądarka będzie działać w trybie bezpiecznego uruchamiania (sandbox) i będzie zupełnie odizolowana od głównego systemu.

Więcej na temat zagrożeń bankowych można przeczytać w następującym artykule:

Crimeware: rozpoczyna się nowa runda starcia...

http://www.viruslist.pl/analysis.html?newsid=602

1.2 Bezpieczne uruchamianie podejrzanych aplikacji i stron internetowych

Bezpieczne uruchamianie pozwala otwierać aplikacje i strony internetowe w środowisku wirtualnym. **Bezpieczne uruchamianie aplikacji** umożliwia włączanie podejrzanych programów w odizolowaniu od głównego systemu. Jest to przydatne, gdy trzeba przetestować aplikację wątpliwego pochodzenia, która potencjalnie mogłaby wyrządzić szkody w komputerze użytkownika. Moduł ten może załadować wyizolowaną wersję systemu, w której można uruchamiać podejrzane aplikacje.

Bezpieczne uruchamianie stron internetowych umożliwia włączenie przeglądarki w wirtualnym środowisku odizolowanym od głównego systemu. Nawet jeżeli oprogramowanie spyware przeniknęło do właściwego systemu, przeglądarka będzie chroniona przed potencjalnymi szkodami. Funkcja ta jest bardzo przydatna podczas pracy z poufnymi danymi, na przykład podczas korzystania z bankowości online.

1.3 Ochrona poczty e-mail i komunikatorów internetowych

KIS 2012 zapewnia ochronę poczty e-mail i komunikatorów internetowych (ICQ, MSN itd.). Moduł **Ochrona poczty** skanuje wiadomości przychodzące i wychodzące na komputerze użytkownika i blokuje szkodliwe treści, dzięki czemu może komunikować się, nie przejmując się zagrożeniami i podejrzanymi odsyłaczami.

Więcej na temat zagrożeń związanych z portalami społecznościowymi można przeczytać w następującym artykule:

Zagrożenia związane z portalami społecznościowymi

http://www.viruslist.pl/analysis.html?newsid=598

1.4 Ochrona przed spamem przy użyciu informacji z chmury

Moduł **Anti-Spam** może znacząco zmniejszyć liczbę niepożądanych wiadomości e-mail. Jest zintegrowany z programem pocztowym zainstalowanym na komputerze użytkownika i skanuje wszystkie wiadomości przychodzące w celu wykrycia spamu. Filtry analizują nagłówki oraz treść wiadomości, jak również załączoną grafikę. Elementy charakterystyczne dla wiadomości spamowych są przechowywane w nieustannie uaktualnianych bazach antyspamowych firmy Kaspersky Lab. Nowy silnik antyspamowy zawarty w KIS 2012 wykorzystuje najnowsze technologie “chmury” oraz analizę heurystyczną, które znacząco zwiększają skuteczność rozpoznawania spamu. Co więcej, dzięki dostępowi do bazy próbek wiadomości spamowych “w chmurze” moduł **Anti-Spam** nie wymaga uczenia.

1.5 Zaawansowana kontrola rodzicielska

Celem **Kontroli rodzicielskiej** jest ochrona dzieci i nastolatków przed zagrożeniami istniejącymi na komputerach i w Internecie. KIS 2012 zawiera szeroki wachlarz funkcji przeznaczonych do zapewnienia takiej ochrony. Program umożliwia kontrolowanie dostępu użytkownika do komputera i Internetu oraz uruchamianych aplikacji, nakładanie ograniczeń na pobieranie plików z Internetu oraz kontrolę dostępu do portali społecznościowych i komunikatorów internetowych. Ponadto, funkcja ta może być wykorzystywana do przeglądania raportów statystycznych dotyczących działań kontrolowanych użytkowników.

Więcej na temat kontroli rodzicielskiej można przeczytać w następującym artykule:

World Wide Web: uczy czy szkodzi?

http://www.kaspersky.pl/about.html?s=news_warnings&cat=4&newsid=1441

1.6 Analiza luk w zabezpieczeniach

Aby zapewnić pełną ochronę przed słabymi punktami w komputerze użytkownika, które mogą zostać wykorzystywane przez hakerów, trzeba regularnie instalować aktualizacje dla systemu i aplikacji. KIS 2012 zawiera moduł **Skanowanie luk**, który pozwala wykryć luki w zabezpieczeniach systemu i aplikacji użytkownika. Jeżeli podczas skanowanie zostaną zidentyfikowane luki, system wyświetla użytkownikowi szczegółowe informacje dotyczące każdej dziury i sposób rozwiązania problemu.

1.7 Prostota i łatwość użytkowania

Kaspersky Lab dąży do tworzenia rozbudowanych produktów, które są jednocześnie łatwe w użyciu niezależnie od poziomu zaawansowania użytkownika. Dzięki wykorzystaniu najnowszych i najbardziej innowacyjnych technik produkty firmy Kaspersky Lab minimalizują potrzebę interakcji użytkownika z aplikacją.

Nowoczesny interfejs pozwala szybko uzyskać wgląd w stan ochrony komputera i sprawia, że zarządzanie bezpieczeństwem komputera jest łatwe dla każdego. Aplikacja zawiera również **gadżet pulpitu** dla systemu Windows Vista oraz Windows 7, który umożliwia uruchomienie najbardziej wymagających zadań niezależnie od okna głównego KIS 2012.

1.8 Dysk ratunkowy

Dysk ratunkowy zawiera zestaw funkcji służących do wykrywania i usuwania infekcji na komputerze w sytuacji, gdy nie można normalnie uruchomić systemu operacyjnego i oprogramowania antywirusowego. W tym celu można użyć płyty instalacyjnej produktu (w przypadku zakupienia go w wersji pudełkowej), co jest bardzo wygodne w przypadku gdy użytkownik nie ma dostępu do drugiego komputera, aby pobrać obraz dysku ratunkowego z Internetu.

2 Instalacja i aktywacja

2.1 Wymagania systemowe

KIS 2012 został zoptymalizowany, tak aby wymagał minimalnych zasobów systemowych. Wymagania te obejmują:

- System operacyjny: Microsoft Windows XP, Windows Vista lub Windows 7 (32 lub 64-bitowy).
- Procesor: 800 MHz CPU dla Windows XP lub 1 GHz CPU dla Windows Vista lub Windows 7.
- RAM: 512 MB dla Windows XP lub 1 GB (wersja 32-bitowa) / 2 GB (wersja 64-bitowa) dla Windows Vista lub Windows 7
- Miejsce na dysku: 480 MB wolnego miejsca na dysku twardym w celu instalacji produktu.

KIS 2011 wymaga również napędu CD/DVD (jeżeli aplikacja została zakupiona na płycie), połączenia z Internetem, przeglądarki Internet Explorer 6 lub nowszej (w celu aktywacji produktu i aktualizacji baz danych).

Uwaga: niektóre funkcje produktu są dostępne tylko w 32-bitowych systemach operacyjnych.

Pełną listę wymagań systemowych można znaleźć można znaleźć na stronie www.kaspersky.pl.

2.2 Instalacja

W celu rozpoczęcia instalacji Kaspersky Internet Security 2012 na komputerze należy uruchomić plik instalacyjny znajdujący się na płycie (autorun.exe). Przed instalacją program sprawdza serwery aktualizacji firmy Kaspersky Lab w celu ustalenia, czy istnieje nowsza wersja Kaspersky Internet Security. Jeżeli jest dostępna nowsza wersja produktu, użytkownik ma możliwość pobrania jej i zainstalowania na swoim komputerze.

Kaspersky Internet Security jest instalowany przy pomocy interaktywnego kreatora. Na początku procesu użytkownik może wybrać najodpowiedniejszy dla siebie typ instalacji. Po wyborze opcji **Standardowa instalacja** (pole wyboru **Zmień ustawienia instalacji** nie jest zaznaczone) aplikacja przeprowadzi kompletną instalację na komputerze przy użyciu ustawień ochrony zalecanych przez Kaspersky Lab.

Jeżeli użytkownik chce zmienić ustawienia instalacji, powinien zaznaczyć pole **Zmień ustawienia instalacji.** W przypadku gdy aplikacja jest wykorzystywana do ochrony więcej niż jednego komputera, instalacja przebiega identycznie na wszystkich z nich.

Instalacja w zainfekowanym systemie operacyjnym

W pewnych okolicznościach komputer może być zainfekowany w stopniu uniemożliwiającym zainstalowanie rozwiązania antywirusowego (np. gdy został zainfekowany niektórymi rodzajami rootkitów). W takich wypadkach produkt oferuje możliwość pobrania specjalnego narzędzia, które skanuje komputer i automatycznie neutralizuje zagrożenia.

Kaspersky Security Network

Podczas procesu instalacji program proponuje użytkownikowi udział w sieci **Kaspersky Security Network** (KSN). KSN automatycznie gromadzi i przesyła do Kaspersky Lab informacje dotyczące prób zainfekowania komputera oraz wykrytych na nim podejrzanych plików (anonimowo i tylko za zgodą użytkownika). Dane te są wysyłane do Kaspersky Lab w celu analizy oraz dodawane do

internetowej bazy szkodliwego oprogramowania. KNS zapewnia najwyższy poziom i prędkość wykrywania zagrożeń.

2.3 Aktywacja i konfiguracja

Po tym jak **Kreator ustawień** zakończy pracę, **Kreator aktywacji** poprosi użytkownika o aktywowanie programu. Podczas aktywacji należy wprowadzić kod aktywacyjny produktu. Użytkownicy posiadający kod aktywacyjny dla KIS 2011, który nie utracił ważności, mogą użyć go do aktywowania KIS 2012. Do aktywowania aplikacji wymagane jest połączenie z Internetem. Po instalacji i aktywacji nie ma potrzeby ponownego uruchamiania komputera.

Kaspersky Lab zaleca wykonanie pełnego skanowania dysku twardego oraz wszystkich podłączonych do komputera zewnętrznych pamięci masowych natychmiast po instalacji. Czas trwania pierwszego skanowania zależy od prędkości procesora oraz liczby plików na komputerze.

3 Przegląd interfejsu

3.1 Okno główne – Udoskonalono!

Podstawowe informacje

Interfejs KIS 2012 został znacznie udoskonalony i teraz jest jeszcze łatwiejszy w użytkowaniu. W centralnym miejscu wyświetlane są informacje dotyczące liczby wykrytych zagrożeń, stanu antywirusowych baz danych (np. „aktualne”) oraz data wygaśnięcia licencji. Kolor monitora oraz gadżetu pulpitu odzwierciedla stan ochrony komputera.

Ochrona przy użyciu chmury

Klikając **Ochronę w chmurze**, użytkownik uzyska szczegółowe informacje o technologiach „chmury” wykorzystywanych w programie KIS 2012 i będzie mógł ocenić skuteczność ich działania.

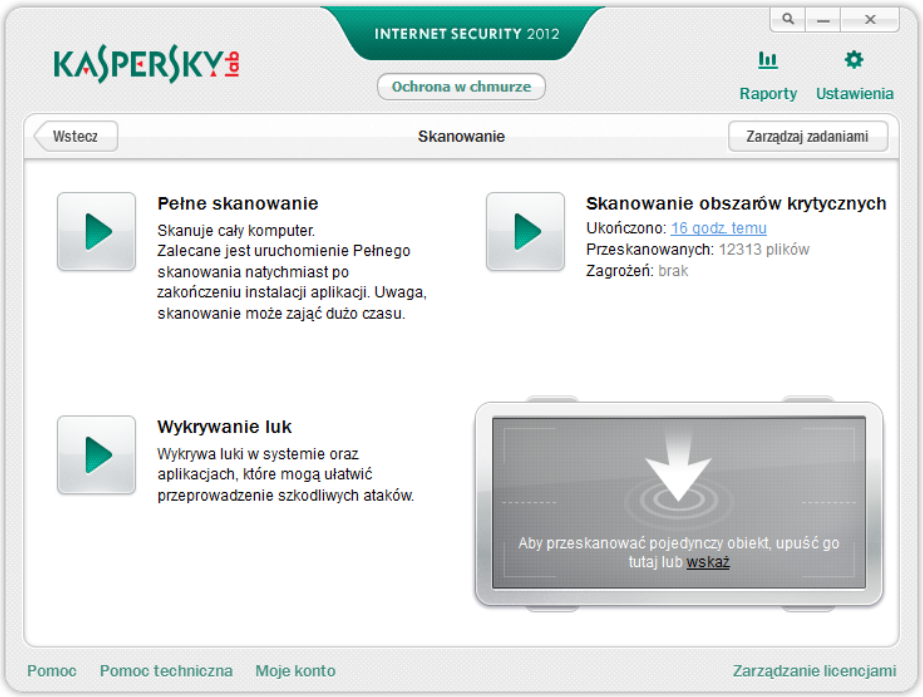
Składniki programu

W dolnej części okna głównego przedstawione są główne składniki produktu. Po kliknięciu ikony z symbolem strzałki otwiera się pełna lista składników:

3.2 Skanowanie

Skanowanie komputera w celu wykrycia wirusów i luk w zabezpieczeniach to jeden z najważniejszych elementów bezpieczeństwa. Skanowanie należy przeprowadzać regularne, aby zapobiec rozprzestrzenianiu szkodliwego oprogramowania, które nie zostało wykryte przez składniki ochrony z powodu ustawienia niskiego poziomu zabezpieczeń lub innego.

W celu przeskanowania komputera w poszukiwaniu szkodliwego oprogramowania zalecamy wykonanie **Pełnego skanowania** lub **Skanowania obszarów krytycznych**. **Skanowanie obszarów krytycznych** obejmuje obiekty załadowywane wraz z systemem operacyjnym, pamięć systemową, sektory rozruchowe dysku twardego oraz inne obiekty dodane przez użytkownika.



Na zakładce tej można również przeprowadzić skanowanie określonych folderów i plików.

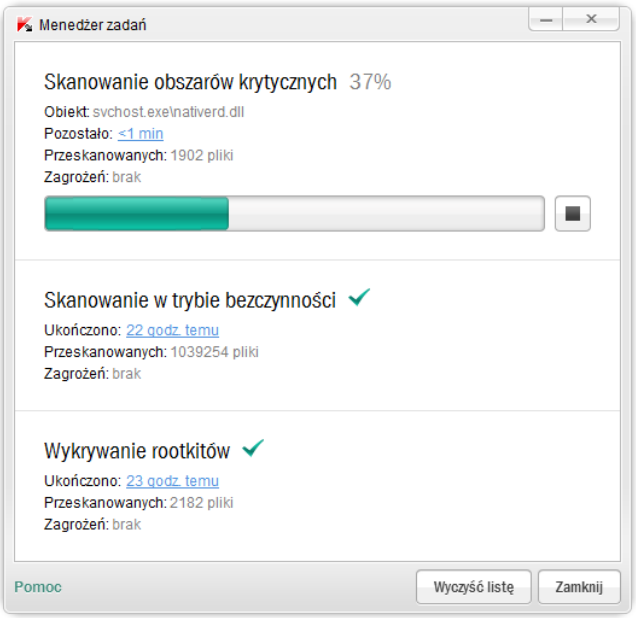
Wykrywanie luk

Luki w zabezpieczeniach systemu operacyjnego mogą być spowodowane błędami w oprogramowaniu, słabymi hasłami, szkodliwymi atakami itd. Aby je wykryć, należy zbadać system, poszukać anomalii lub błędów w ustawieniach systemu operacyjnego, skontrolować usługi podatne na ataki itd.

Wykrywanie luk obejmuje wszystkie aplikacje zainstalowane na komputerze użytkownika. Każda z nich jest sprawdzana w oparciu o największe na świecie bazy znanych luk w zabezpieczeniach, stworzone i utrzymywane przez firmę Secunia, duńską organizację specjalizującą się dostarczaniu informacji o krytycznych lukach w oprogramowaniu dla różnych systemów operacyjnych.

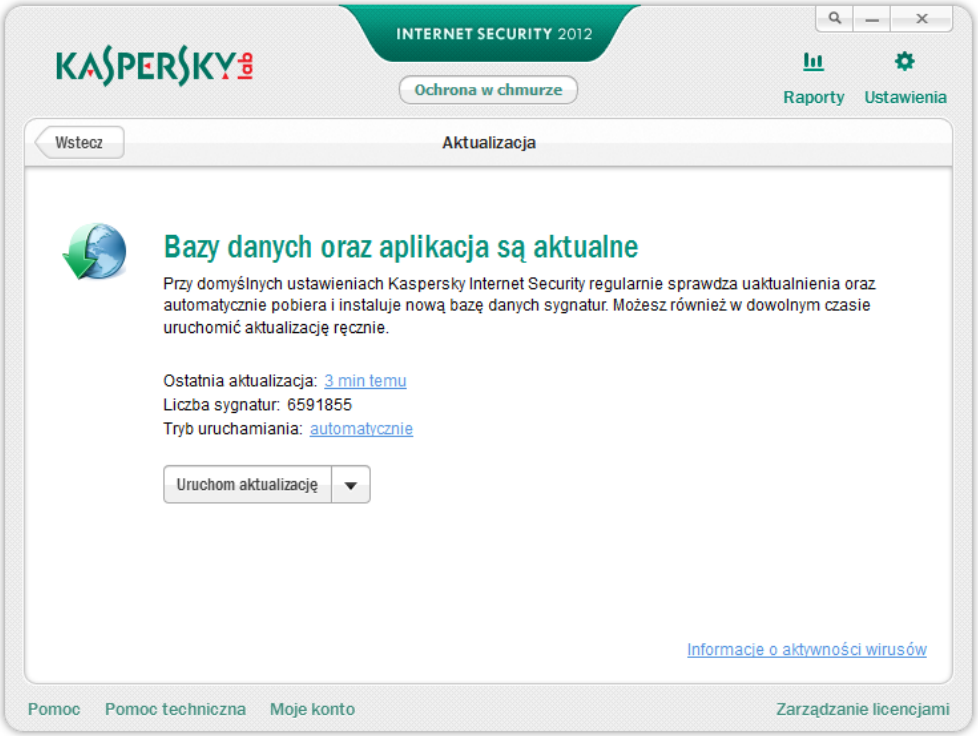
Zarządzaj zadaniami – Nowość!

KIS 2012 zawiera całkowicie nową funkcję: teraz można przeglądać zadania wykonywane przez aplikację oraz ich status. Pozwala to zoptymalizować wykorzystanie zasobów komputera.



3.3 Aktualizacja – Udoskonalono!

Aktualizacja baz danych i modułów Kaspersky Internet Security chroni komputer przed najnowszymi zagrożeniami. Każdego dnia pojawiają się nowe wirusy, trojany i inne rodzaje szkodliwego oprogramowania. Informacje dotyczące zagrożeń i sposobów ich neutralizacji są zawarte w bazach danych Kaspersky Internet Security. Regularna aktualizacja aplikacji pozwala zabezpieczyć komputer przed nowymi zagrożeniami. KIS 2012 jest uaktualniany automatycznie, jednak w razie konieczności można również pobrać uaktualnienia poprzez zakładkę **Aktualizacja.**



Istnieje również możliwość zmiany ustawień baz aktualizacji. W tym celu należy wejść w ustawienia aplikacji, klikając zakładkę **Ustawienia** w oknie głównym, i wybrać zakładkę **Aktualizacja.**

Funkcja aktualizacji w KIS 2012 zawiera kilka istotnych usprawnień:

1. KIS 2012 pobiera uaktualnienia tylko dla aktywnych składników aplikacji, co pomaga zminimalizować liczbę uaktualnień oraz czas potrzebny do ich pobrania.
2. Dzięki udoskonalonej wewnętrznej optymalizacji programów KAV/KIS 2012 pobieranie uaktualnień jest jeszcze szybsze i efektywniejsze.
3. Ponadto, w automatycznym trybie aktualizacji KAV/KIS 2012 wykonuje zadania aktualizacji po upłynięciu 15 minut od momentu włączenia komputera z trybu czuwania, tak aby nie spowolnić procesu przywracania systemu operacyjnego.

3.4 Kontrola rodzicielska

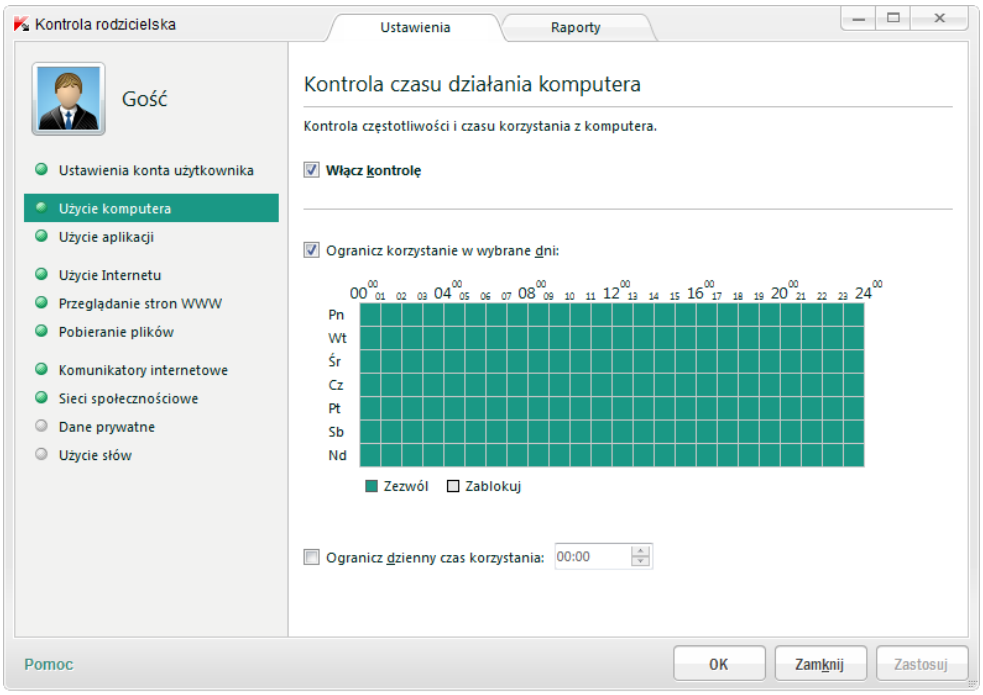
Celem **Kontroli rodzicielskiej** jest ochrona dzieci i nastolatków przed zagrożeniami na komputerze i w Internecie. Funkcja ta pozwala zastosować różne rodzaje ograniczeń:

1. Ograniczyć czas działania komputera.
2. Zablokować lub zezwolić na dostęp do określonych aplikacji na komputerze.
3. Zablokować lub zezwolić na dostęp do określonych stron internetowych.
4. Kontrolować korzystanie przez dziecko z poczty elektronicznej, komunikatorów internetowych (ICQ, MSN) oraz portali społecznościowych (Facebook itd.). Pełna lista obsługiwanych komunikatorów internetowych i portali społecznościowych znajduje się poniżej.
5. Kontrolować pobierane pliki.
6. Kontrolować przesyłanie informacji osobistych.

Moduł Kontrola rodzicielska obsługuje następujące komunikatory internetowe: ICQ, QIP. MSN, Yahoo Messenger, Google Talk, mIRC, Mail.RU Агент, Psi, Miranda, AIM. Digsby, Pidgin, Qnext, SIM, Trilian, Xchat, Instantbird, RnQ, Jabber.
Obsługiwane są także następujące portale społecznościowe: MySpace, Twitter, Facebook.

Kontroluj czas działania komputera

Przy pomocy Kontroli rodzicielskiej można ograniczyć czas korzystania z komputera. Opiekun może określić, kiedy dziecko może mieć dostęp do komputera (dni tygodnia oraz godziny w ciągu dnia), jak również ograniczyć dzienny czas działania komputera.

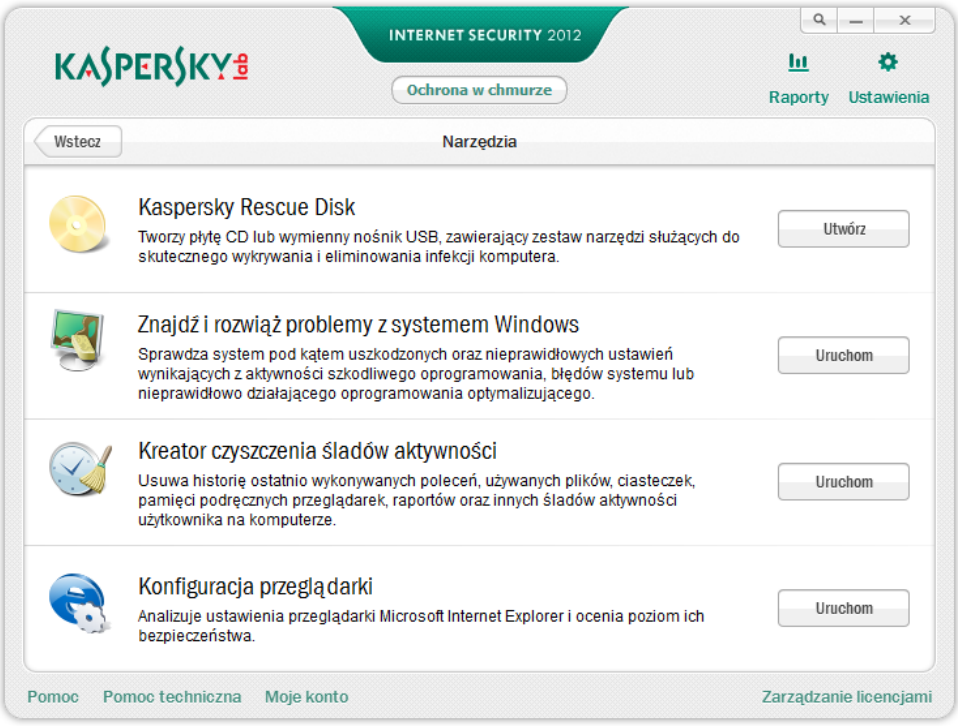


Kontrola korzystania z portali społecznościowych

Kontrola korzystania z portali społecznościowych umożliwia nadzór nad kontaktami zdobywanymi przez dziecko w obrębie portali społecznościowych. Ponadto, pozwala zablokować niepożądane kontakty oraz kontrolować treść wysyłanych i otrzymywanych wiadomości. Użytkownik może również stworzyć listy dozwolonych i zablokowanych kontaktów, określić kluczowe słowa i frazy, które będą wyszukiwane w wiadomościach, oraz informacje osobiste, które nie mogą być wysyłane.

3.5 Narzędzia

Zakładka Narzędzia zawiera zestaw pomocniczych funkcji, które zapewniają dodatkową ochronę komputera.



Kaspersky Rescue Disk

Niektóre szkodliwe programy uszkadzają pliki niezbędne do rozruchu systemu operacyjnego. W takiej sytuacji można użyć **Dysku ratunkowego.** Jest to dysk rozruchowy zawierający zestaw narzędzi służących do wykrywania i usuwania infekcji na komputerze w sytuacjach, gdy nie można w sposób standardowy załadować systemu operacyjnego oraz oprogramowania antywirusowego. Kolejną innowacją w KIS 2012 jest możliwość przechowywania **Dysku ratunkowego** na nośniku USB (a nie tylko na płycie CD/DVD).

KIS 2012 oferuje możliwość użycia jako dysku ratunkowego dysku instalacyjnego produktu (jeżeli KAV/KIS 2012 został zakupiony w wersji pudełkowej). W tym celu należy umieścić dysk instalacyjny produktu w napędzie CD/DVD i w BIOS-ie wybrać opcję rozruchu z płyty CD/DVD. To oznacza, że nie trzeba już wcześniej tworzyć dysku ratunkowego lub wykorzystywać do tego innego komputera.

Rozwiązywanie problemów z systemem Microsoft Windows

Przy pomocy tego kreatora można przywrócić system operacyjny Windows po awarii lub uszkodzeniu na skutek szkodliwego ataku. Jako eksperci w branży, w celu zwiększenia bezpieczeństwa zalecamy wyłączenie funkcji automatycznego uruchamiania z pamięci flash. Jeżeli funkcja ta jest włączona, do infekcji może dojść już podczas włączania komputera, gdy w jego porcie znajduje się zarażony pendrive.

Ustawienia przeglądarki

Kreator ustawień przeglądarki dokładnie analizuje ustawienia Internet Explorera i proponuje sposoby ulepszenia ich w oparciu o zalecenia firmy Kaspersky Lab. Ustawienia mogą zostać zmienione za zgodą użytkownika w celu zwiększenia bezpieczeństwa i ochrony poufnych informacji podczas korzystania z Internet Explorera. Zmiany mogą obejmować na przykład blokowanie komponentów ActiveX lub usuwanie plików zawierających poufne informacje z pamięci podręcznej.

Czyszczenie śladów aktywności

Użytkownicy zawsze pozostawiają ślady swojej aktywności, takie jak dane wprowadzane na forach internetowych, informacje o odwiedzonych stronach oraz nazwy plików i folderów zapisanych na komputerze.

Aby zachować poufność, zalecamy usuwanie takich informacji. Jest to istotne, na przykład w przypadku, gdy komputer jest wykorzystywany przez więcej niż jedną osobę. Tego rodzaju informacje mogą również zostać skradzione za pośrednictwem Sieci. Dzięki tej specjalnej funkcji wbudowanej w KIS 2012 do wyczyszczenia śladów aktywności wystarczy kilka kliknięć.

3.6 Klawiatura wirtualna

Klawiatura wirtualna uniemożliwia rejestrowanie znaków wprowadzanych z klawiatury przez oprogramowanie spyware oraz przesyłanie do cyberprzestępców danych dotyczących bankowości i innych poufnych informacji. Klawiatura wirtualna może być używana tak samo jak klawiatura standardowa do wpisywania dowolnego tekstu poprzez wciskanie odpowiednich klawiszy. Wbudowana technologia zapewnia niezawodną ochronę przed najnowszą generacją aplikacji, które potrafią wykonywać graficzne zrzuty zawartości ekranu, oraz przed wyciekiem danych za pośrednictwem przeglądarek internetowych.

3.7 Kwarantanna

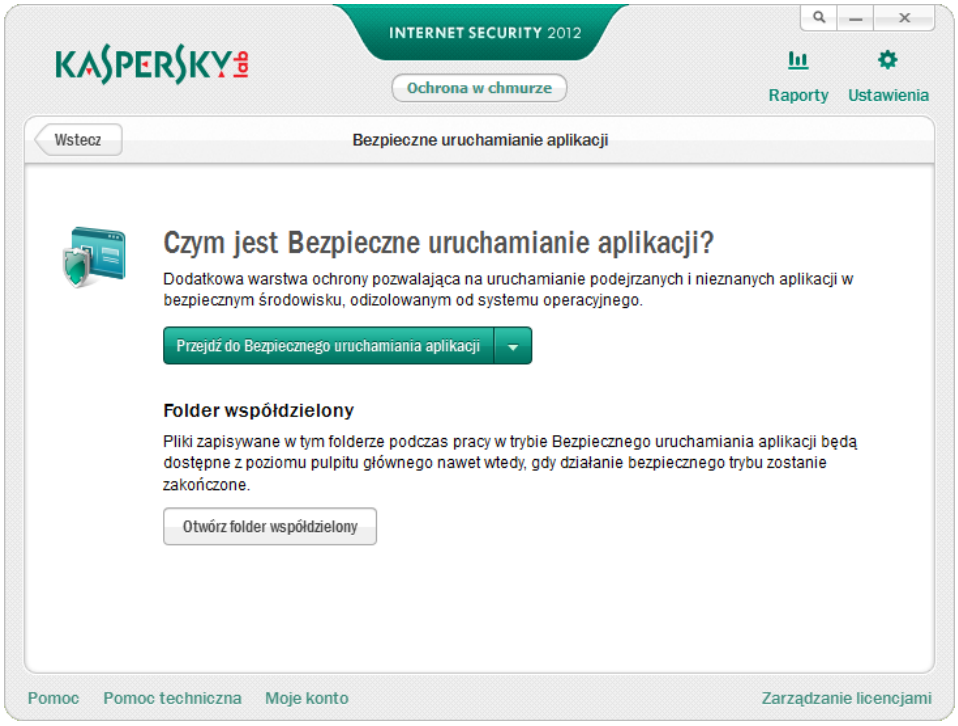
Kwarantanna to specjalny obszar przechowywania plików, które zostały prawdopodobnie zainfekowane wirusami, oraz takich, które nie mogą zostać wyleczone w momencie ich wykrycia. Pliki te są przechowywane w specjalnym formacie i nie stanowią zagrożenia dla systemu. Pliki umieszczone w kwarantannie są skanowane za każdym razem po uaktualnieniu antywirusowych baz danych.

3.8 Aktywność aplikacji

Aby przejrzeć listę aplikacji oraz procesów uruchomionych na komputerze PC, należy otworzyć okno główne aplikacji i wybrać znajdującą się w dolnej części sekcję **Aktywność aktywacji**.

3.9 Bezpieczne uruchamianie aplikacji

Bezpieczne uruchamianie zapewnia wirtualne środowisko, odizolowane od głównego systemu operacyjnego, pozwalające na bezpiecznie ładowanie podejrzanych aplikacji i korzystać z zasobów online, w przypadku których istotne jest ma bezpieczne wprowadzanie poufnych informacji, np. podczas dokonywania transakcji bankowych online.



Aby **Bezpieczne uruchamianie** było jeszcze wygodniejsze w użyciu, KIS 2012 oferuje opcję uruchomienia wirtualnego pulpitu. Ten bezpieczny pulpit otwiera się w trybie pełnego ekranu i stanowi kopię głównego pulpitu wraz z wszystkimi obiektami systemu plików. Przy użyciu wirtualnego pulpitu można uruchomić dowolną aplikację na komputerze w obszarze **Bezpiecznego uruchamiania**. Domyślnie wszystkie zmiany dokonane podczas bezpiecznego uruchamiania aplikacji są zapisywane i będą dostępne podczas kolejnego uruchomienia.

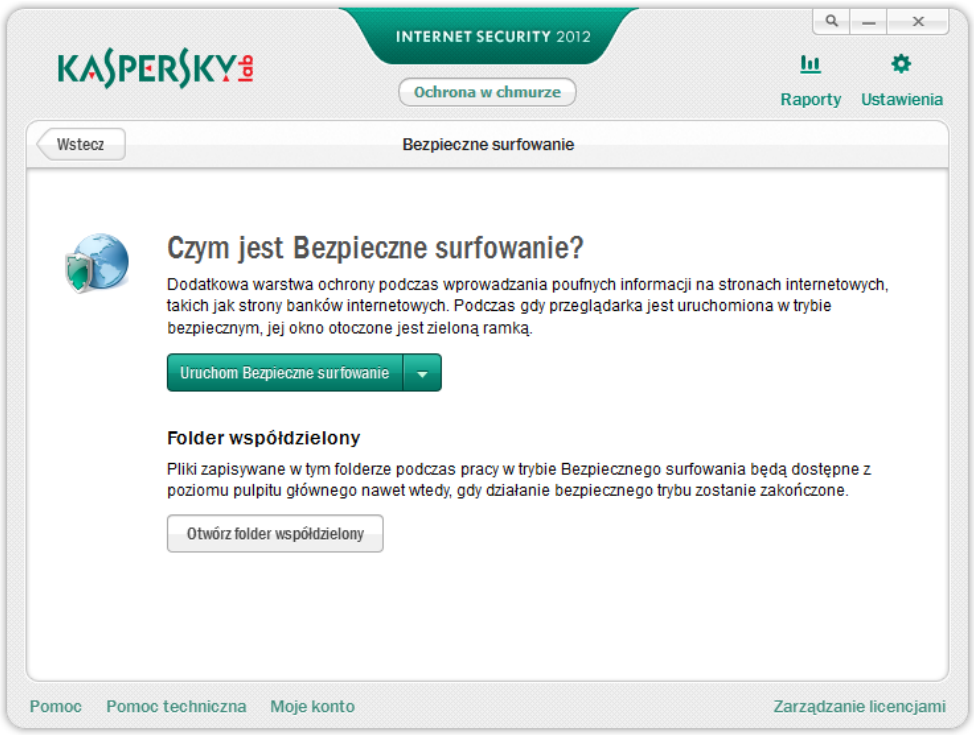
Folder współdzielony służy do wymiany plików pomiędzy obszarem **Bezpiecznego uruchamiania** a głównym systemem. Wszystkie pliki zapisane w folderze współdzielonym w obszarze **Bezpiecznego uruchamiania** są również dostępne z głównego pulpitu. **Folder współdzielony** można również otworzyć z okna głównego KIS 2012 lub z foldera **Mój komputer.**

Aby zamknąć wirtualny pulpit, można użyć skrótu Alt+Shift+Ctrl+K.

3.10 Bezpieczne surfowanie

Bezpieczne surfowanie służy do uzyskiwania dostępu do stron internetowych, na których użytkownik wprowadza poufne dane, np. dotyczące bankowości online.

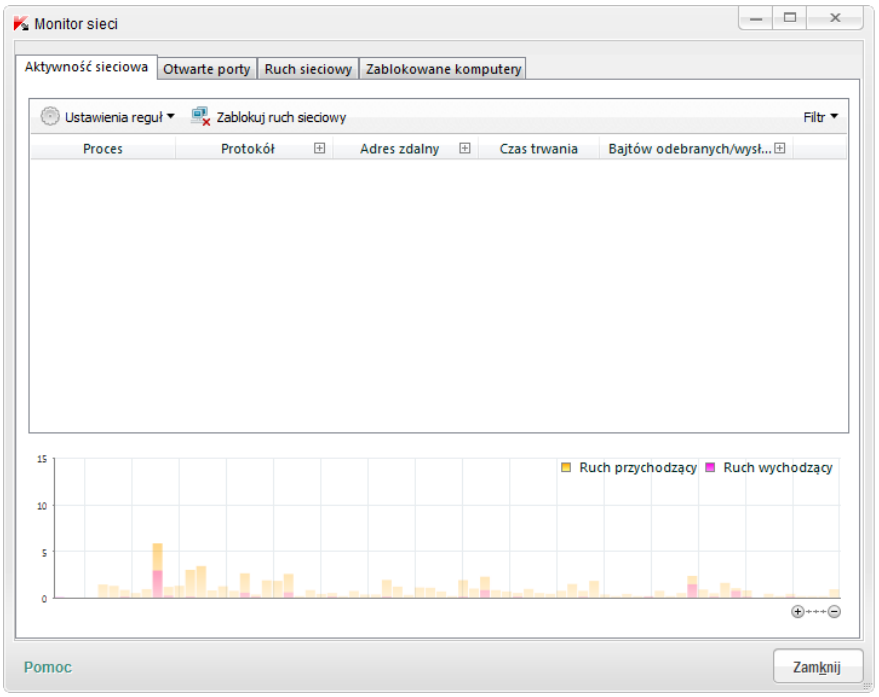
Bezpieczne surfowanie zapewnia ochronę przed szkodliwymi aplikacjami, przy czym chroniony jest nie sam system, ale poufne dane wprowadzane online (np. podczas transakcji bankowych), na wypadek gdyby system był zainfekowany.



Funkcja ta może być wykorzystywana wraz z modułem **Bankowość elektroniczna**. Jeżeli zostanie on włączony, program zaleci wykorzystanie **Bezpiecznego surfowania**, na których są przeprowadzane transakcje bankowe.

3.11 Monitor sieci

Monitor sieci to narzędzie służące do przeglądania informacji o aktywności sieciowej w czasie rzeczywistym. Aby przejrzeć takie informacje, należy otworzyć okno główne aplikacji i wybrać zakładkę **Monitor sieci** znajdującą się w dolnej części okna.



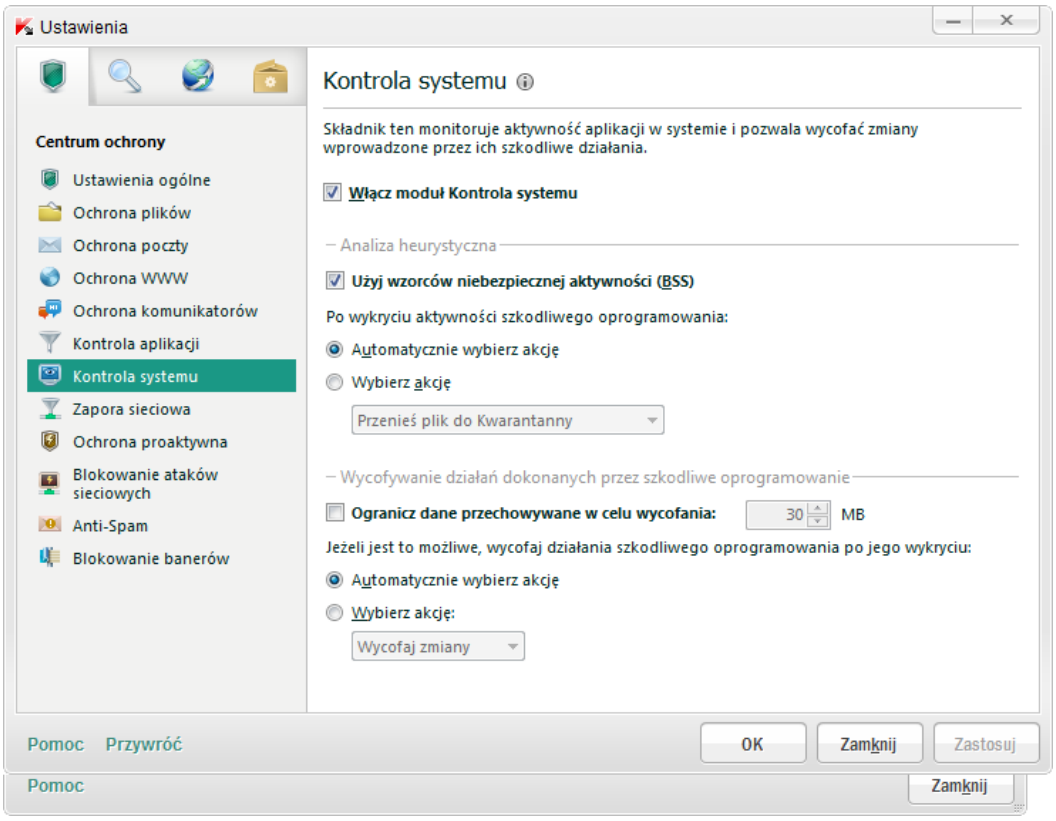
3.12 Kontrola systemu, moduły File Advisor i URL Advisor

Kontrola systemu - Udoskonalono!

KAV/KIS zawiera **Kontrolę systemu,** nową technologię, która monitoruje wszystkie działania wykonywane przez programy uruchomione na komputerze oraz porównuje zachowanie każdego programu ze schematami zachowania szkodliwego oprogramowania. Pozwala to skutecznie zidentyfikować nowe podejrzane i niebezpieczne programy.

Kontrola systemu została udoskonalona w KIS 2012:

- informacje dotyczące działań wykonywanych przez podejrzane programy są gromadzone nie tylko w bieżącej sesji, ale również podczas poprzednich. To oznacza, że wszystkie działania wykonane przez program mogą zostać cofnięte, jeżeli zostanie on zidentyfikowany jako szkodliwy.
- Szkodliwe oprogramowanie jest wykrywane na podstawie analizy jeszcze większej liczby zdarzeń.
- Po wykryciu zagrożenia jego szkodliwe działania na komputerze są natychmiast blokowane. Lista szkodliwych działań, które mogą zostać zablokowane, została znacznie rozszerzona.
- **Kontrola systemu** wykorzystuje informacje zebrane przez inne składniki aplikacji (np. Ochronę proaktywną, Ochronę poczty, Ochronę WWW, Ochronę komunikatorów, Zaporę sieciową), co znacznie zwiększa możliwości wykrywania nowych nieznanych zagrożeń.



Cofanie zmian – Udoskonalono!

Ochrona proaktywna może być wykorzystywana do śledzenia zachowania programów uruchomionych na komputerze. Gdy program okaże się szkodliwy, bardzo ważne jest, aby istniała możliwość cofnięcia wszystkich wykonanych przez niego działań. KIS 2012 zawiera taką funkcję. W nowej aplikacji znacznie usprawniono cofanie szkodliwych działań:

- Teraz można cofnąć działania wykonane przez szkodliwe oprogramowanie nie tylko w bieżącej sesji, ale również w poprzednich.
- Lista działań, które można cofnąć, została rozszerzona. Teraz obejmuje tworzenie plików, zmianę nazw i inne modyfikacje plików, zmiany dokonane w rejestrze systemowym oraz inne działania. Moduł ten umożliwia również przerwanie procesów rozpoczętych przez szkodliwe oprogramowanie oraz ograniczenie jego połączeń sieciowych.

W zależności od ustawień produktu cofanie działań wykonanych przez szkodliwe oprogramowanie odbywa się automatycznie lub wymaga zgody użytkownika.

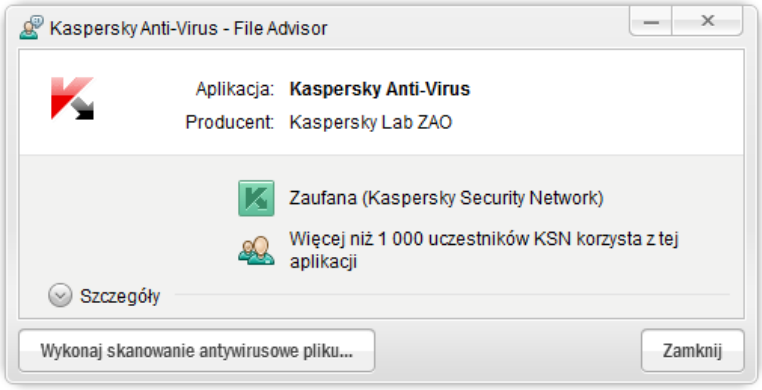
Ponadto, można określić ilość miejsca na dysku twardym (domyślnie jest to 20 MB) przeznaczonego na przechowywanie historii aktywności programów. Przechowywanie tych danych jest niezbędne do cofnięcia działań szkodliwego oprogramowania.

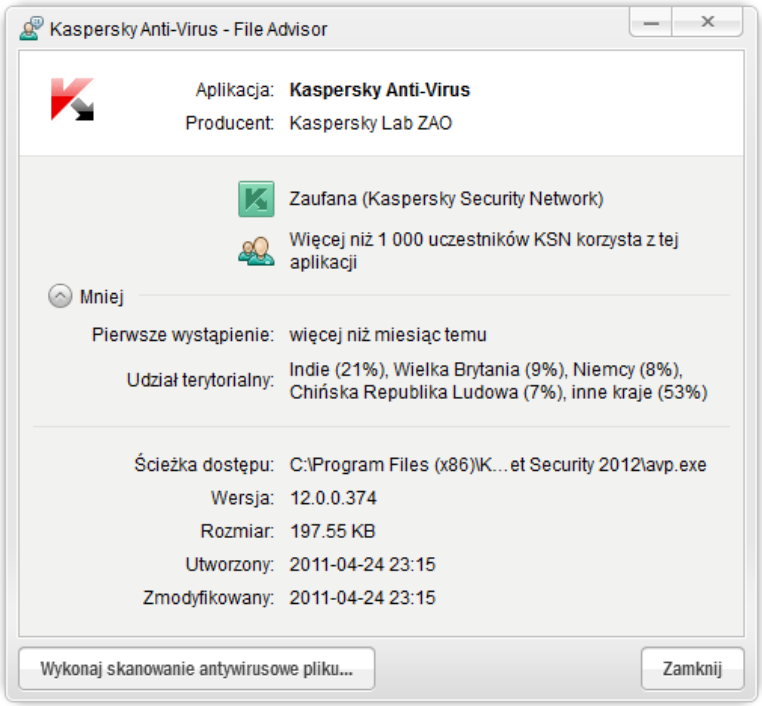
File Advisor - Nowość!

Teraz jednym kliknięciem można sprawdzić reputację dowolnego pliku. W tym celu należy prawym przyciskiem myszki kliknąć żądany plik i z menu kontekstowego wybrać polecenie **Sprawdź reputację w KSN**. Jest to przydatne, np. wtedy gdy użytkownik pobrał plik z Internetu, ale nie jest pewny, czy plik ten jest bezpieczny, i chce szybko sprawdzić jego reputację.

Funkcja ta dostarcza informacje obejmujące nazwę pliku, jego rozmiar, datę utworzenia oraz ostatniej modyfikacji, klasyfikator zagrożenia, podpis cyfrowy, dystrybucję geograficzną oraz poziom zaufania przydzielony przez innych użytkowników. Wszystkie te dane są wyświetlane w Eksploratorze Windows lub w dodatkowej sekcji okna skanowania.

Główna zaleta tej funkcji polega na tym, że do oceny reputacji pliku wykorzystywane są informacje z “chmury” – najbardziej aktualne z dostępnych. Dzięki temu można sprawdzić nawet pliki i programy, które pojawiły się całkiem niedawno.





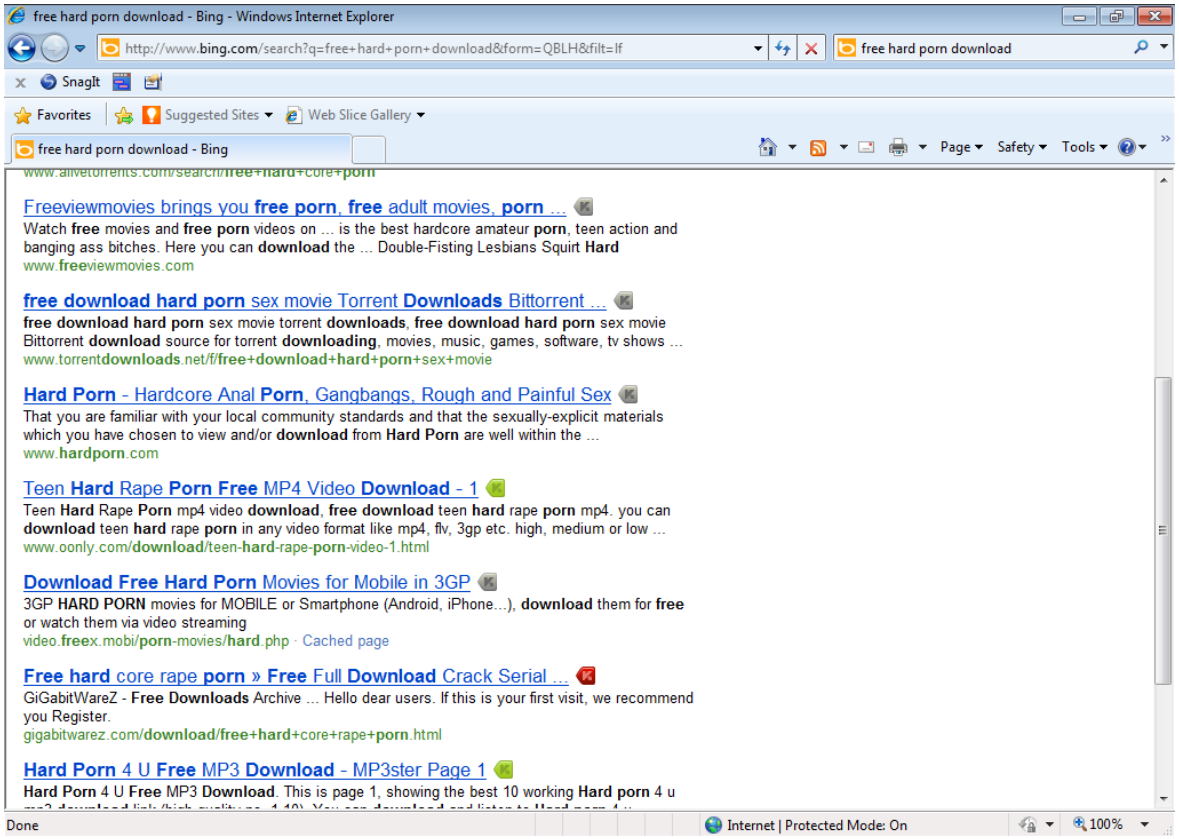
URL Advisor - Udoskonalono!

KIS 2012 zawiera moduł **URL Advisor,** który ostrzega przed odsyłaczami do podejrzanych lub niebezpiecznych stron internetowych. Moduł ten występuje w postaci paska narzędzi dla przeglądarki. Za pomocą specjalnego znacznika koloru oznaczane są odsyłacze do zainfekowanych lub sfałszowanych zasobów (phishing).

Odsyłacze mogą być skanowane na dwa sposoby:

1. Skanowane są wszystkie odsyłacze na każdej stronie.
2. Skanowane są tylko wyniki wyświetlane przez wyszukiwarki oraz wyszukiwania na stronie.

URL Advisor ostrzega przed potencjalnym niebezpieczeństwem, jakie może stanowić strona internetowa, jeszcze zanim użytkownik kliknie odsyłacz.

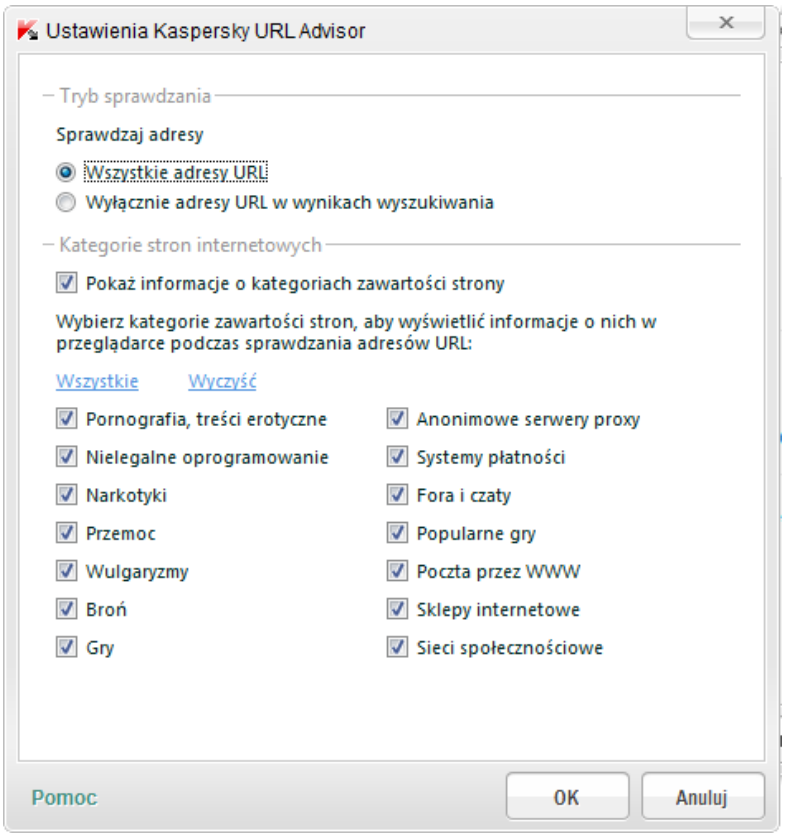


W procesie określania poziomu zagrożenia wykorzystywane są informacje nie tylko z bazy szkodliwych i phishingowych adresów URL, ale również z baz danych znajdujących się na serwerach firmy Kaspersky Lab, które dostarczają oceny reputacji dla adresów IP (na przykład czy zawierają szkodliwy kod lub odsyłacze do podejrzanych stron, ilu mają odwiedzających itp.).

Główne udoskonalenia wprowadzone do KAV/KIS 2012 obejmują:

1. Dodatkowe informacje o zasobach online umożliwiające podjęcie właściwej decyzji odnośnie odwiedzenia określonej strony internetowej.
2. Informacje zgromadzone w “chmurze” o zasobach online zapewniające dokładniejszą definicję szkodliwych oraz sfałszowanych (phishingowych) stron internetowych.
3. Rozszerzoną listę obsługiwanych przeglądarek.

Co więcej, moduł **URL Advisor** pozwala określić niechciane kategorie stron internetowych (takie jak “pornografia”, “okrucieństwo i przemoc” itd.).



3.13 Gadżet pulpitu - Udoskonalono!

KIS 2012 zawiera całkowicie nową funkcję: gadżet pulpitu dla systemu Windows Vista oraz Windows 7. Gadżet jest elementem interfejsu na pulpicie Windows, który zapewnia szybki dostęp do głównych funkcji produktu. Teraz nie trzeba już otwierać głównego okna aplikacji, aby wykonać pilne zadania – wystarczy kliknąć gadżet.

Po instalacji Kaspersky Internet Security w systemie Microsoft Windows 7 gadżet pojawia się na pulpicie automatycznie. W systemie Windows Vista gadżet należy dodać ręcznie do panelu bocznego (zobacz dokumentację dot. systemu operacyjnego).

Gadżet pulpitu w KAV/KIS 2012 został znacznie udoskonalony. Teraz wyświetla stan skanowanych obiektów. Na przykład, jeżeli odbywa się skanowanie określonych plików lub obszarów komputera, w gadżecie pojawia się wskaźnik stanu wykonania zadania. Co więcej, została rozszerzona lista

funkcji, które mogą zostać uruchomione bezpośrednio z poziomu gadżetu. Zmienił się także jego wygląd.

4 Licencjonowanie i pomoc techniczna

4.1 Informacje dotyczące licencji

Informacje o okresie ważności licencji są wyświetlane w centralnym miejscu okna głównego KIS 2012. Aby uzyskać bardziej szczegółowe informacje, należy kliknąć **Zarządzanie licencjami** na dole okna.

Wygodnym sposobem przedłużenia licencji jest kliknięcie bezpośredniego odsyłacza do sklepu internetowego Kaspersky Lab. Produkt aktywowany jest przy użyciu kodu aktywacyjnego (wymagane jest połączenie z Internetem).

4.2 Pomoc techniczna

Jeżeli pojawią się problemy techniczne lub pytania dotyczące produktu, można kontaktować się z działem pomocy technicznej dostępnym bezpłatnie na terenie Polski poprzez telefon i pocztę e-mail. Można także skorzystać z zasobów online w języku polskim zawierających odpowiedzi na często zadawane pytania dotyczące instalacji i użytkowania produktu.