



# **DeRA Tyzacja komputerów**

Jak schwytać i ubić trojany, gdy  
antywirusy zawodzą ...

**Leszek IGNATOWICZ**

Warszawa maj 2013

[www.SysClinic.pl](http://www.SysClinic.pl)

DeRATyzacja kOMPUTERA

Samowystarczalni umysłowo  
są jedynie geniusze i głupcy

Stanisław Jerzy Lec

Leszek IGNATOWICZ

## DeRATyzacja komputerów

Jak schwytać i ubić trojany, gdy  
antywirusy zawodzą...

Wydanie I, maj 2013

ISBN 978-83-62255-42-9

Autor: Leszek IGNATOWICZ

Korekta: Agnieszka Kwiatkowska

Projekt okładki: Leszek IGNATOWICZ

Zdjęcie na okładce: Ola Kwiatkowska

Copyright© 2013 by Leszek IGNATOWICZ

---

# Spis Treści

<b><u>SPIS TREŚCI.....</u></b>	<b><u>3</u></b>
<b><u>WSTĘP.....</u></b>	<b><u>5</u></b>
<b><u>JAK KORZYSTAĆ Z E-BOOKA?.....</u></b>	<b><u>9</u></b>
<b><u>I. EMSISOFT EMERGENCY KIT 3.0 – WYGODNY KOMBAJN.....</u></b>	<b><u>10</u></b>
Ogólny opis Emsisoft Emergency Kit (EEK).....	10
Przygotowanie EEK do użycia.....	11
Skaner Emergency Kit.....	13
<i>Szybkie skanowanie.....</i>	<i>17</i>
<i>Inteligentne skanowanie.....</i>	<i>17</i>
<i>Dokładne skanowanie.....</i>	<i>18</i>
<i>Własne skanowanie.....</i>	<i>19</i>
<i>Kwarantanna - bezpieczne usuwanie szkodników.....</i>	<i>20</i>
Skaner bez GUI (interfejsu graficznego).....	21
HiJackFree.....	22
BlitzBlank.....	23
<b><u>II. NORTON POWER ERASER – OBOSIECZNY MIECZ.....</u></b>	<b><u>24</u></b>
Ogólny opis Norton Power Eraser (NPE).....	24
Przygotowanie NPE do użycia.....	25
Skanowanie w poszukiwaniu zagrożeń.....	27
Ustawienia.....	33
<b><u>III. REGRUN REANIMATOR – SZYBKI PARTYZANT.....</u></b>	<b><u>34</u></b>
Ogólny opis RegRun Reanimatora (RRR).....	34
Przygotowanie RRR do użycia.....	35
Funkcjonalności RegRun Reanimatora.....	36
<i>Perform action on the current computer.....</i>	<i>37</i>

---

<a href="#"><u>Check for updates.....</u></a>	<a href="#"><u>37</u></a>
<a href="#"><u>Backup System Files.....</u></a>	<a href="#"><u>38</u></a>
<a href="#"><u>Next.....</u></a>	<a href="#"><u>39</u></a>
<a href="#"><u>Fix problems.....</u></a>	<a href="#"><u>39</u></a>
<a href="#"><u>Zakładka Clean after Viruses.....</u></a>	<a href="#"><u>41</u></a>
<a href="#"><u>Zakładka Protect.....</u></a>	<a href="#"><u>43</u></a>
<a href="#"><u>Zakładka Open RNR File.....</u></a>	<a href="#"><u>45</u></a>
<a href="#"><u>Zakładka Uninstall Partizan.....</u></a>	<a href="#"><u>45</u></a>
<a href="#"><u>Zakładka Restore.....</u></a>	<a href="#"><u>45</u></a>
<a href="#"><u>Zakładka Contact.....</u></a>	<a href="#"><u>48</u></a>
<a href="#"><u>Fix Browser Redirect.....</u></a>	<a href="#"><u>48</u></a>
<a href="#"><u>Scan Windows Startup.....</u></a>	<a href="#"><u>55</u></a>
<a href="#"><u>On-line Multi-Antivirus Scan.....</u></a>	<a href="#"><u>71</u></a>
<a href="#"><u>Check File (Sprawdź plik).....</u></a>	<a href="#"><u>77</u></a>
<a href="#"><u>RegRun Reanimator dla zaawansowanych.....</u></a>	<a href="#"><u>78</u></a>
<b><a href="#"><u>IV. SYSTEM EXPLORER – SOLIDNY OCHRONIARZ.....</u></a></b>	<b><a href="#"><u>82</u></a></b>
<a href="#"><u>Ogólny opis System Explorera (SE).....</u></a>	<a href="#"><u>82</u></a>
<a href="#"><u>Przygotowanie SE do użycia.....</u></a>	<a href="#"><u>83</u></a>
<a href="#"><u>Funkcjonalności System Explorera.....</u></a>	<a href="#"><u>85</u></a>
<a href="#"><u>Zakładka Procesy.....</u></a>	<a href="#"><u>86</u></a>
<a href="#"><u>Zakładka Moduły.....</u></a>	<a href="#"><u>93</u></a>
<a href="#"><u>Zakładka Security Info.....</u></a>	<a href="#"><u>94</u></a>
<b><a href="#"><u>V. STREAM ARMOR – WNIKLIWY DETEKTYW.....</u></a></b>	<b><a href="#"><u>95</u></a></b>
<a href="#"><u>Ogólny opis Stream Armor'a (SA).....</u></a>	<a href="#"><u>95</u></a>
<a href="#"><u>Przygotowanie SA do użycia.....</u></a>	<a href="#"><u>96</u></a>
<a href="#"><u>Analiza wyników SA.....</u></a>	<a href="#"><u>97</u></a>
<b><a href="#"><u>DODATEK I – SYSINTEGRUS.....</u></a></b>	<b><a href="#"><u>100</u></a></b>
<a href="#"><u>Komputer bez antywirusa! Sysintegrus – bastion ochrony komputerów przed złośliwym oprogramowaniem.....</u></a>	<a href="#"><u>100</u></a>
<b><a href="#"><u>DODATEK II – WITRYNA I BLOG WWW.SYSCLINIC.PL.....</u></a></b>	<b><a href="#"><u>108</u></a></b>

---

# Wstęp

Programy antywirusowe nie wykrywają najgroźniejszego złośliwego oprogramowania. Dzieje się tak dlatego, że na komputerze ofiary instalują się potajemnie, unikatowe w formie binarnej, kontrolowane przez cyberprzestępców programy. Ich obecność w komputerze jest maskowana przez zastosowanie wyrafinowanych technik ukrywania w systemie, określanych mianem rootkit'a. Określane są jako Trojany zdalnego dostępu, z ang. remote access Trojans RATs<sup>1</sup>, stąd w tytule DeRATyzacja, a więc wytępienie „szczurów” z komputera;) Służą do wykradania z komputerów poufnych informacji, wykorzystywanych w przestępczych celach, najczęściej w celu osiągnięcia finansowych korzyści.

Dlaczego tak się dzieje, pomimo bieżącego aktualizowania zainstalowanego na komputerze oprogramowania antywirusowego? Problem wynika z samej zasady działania takiego oprogramowania. Wykrywanie zagrożeń polega na poszukiwaniu w skanowanych plikach pewnych charakterystycznych dla określonego szkodnika ciągów binarnych, określanych mianem sygnatur<sup>2</sup>. Takie sygnatury muszą być uprzednio zdefiniowane przez producentów programów antywirusowych i dostarczone użytkownikom. Cyberprzestępcy stosują zaawansowane techniki modyfikacji kodu w celu uniknięcia wykrycia przez antywirusy: powstają zmienione pliki binarne, które jednak realizują te same, szkodliwe dla ofiary funkcje. W takim przypadku oprogramowanie antywirusowe nie wykryje szkodnika w momencie jego instalowania w systemie. Potem sytuacja staje się jeszcze gorsza, bo uaktywniony szkodnik może obezwładnić antywirusa i ściągnąć dodatkowy malware.

<sup>1</sup> <http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan> (w jęz. angielskim)

<sup>2</sup> <http://locos.pl/publikacje/6433-w-jaki-sposob-antywirusy-rozpoznaj-zoliwe-programy>

Z powyższego wynika konkluzja, że obrona przed malware'm oparta na klasycznym oprogramowaniu antywirusowym jest niewystarczająca. Skuteczność antywirusów w zakresie ochrony aktywnej w starciu z nowymi bądź unikatowymi binarnie szkodnikami jest bliska zeru. Zainteresowanych tym tematem odsyłam do bloga <http://www.sysclinic.pl/blog/?id=zbt4yh86>.

Wyływa stąd dalszy, niepokojący wniosek: komputery chronione przez antywirusy, nawet najbardziej znanych producentów, aktualizowane na bieżąco, mogą być zainfekowane malware'm<sup>3</sup>. Komputer zainfekowany Trojanem zdalnego dostępu (ang. RAT) już nie jest nasz. Cyberprzestępcy skrycie i zdalnie, poprzez Internet, mają do niego pełny dostęp. Mogą nas okraść lub wpędzić w kłopoty, używając naszych – „nie naszych” komputerów. Godna pożałowania może być sytuacja właściciela komputera, na którym cyberprzestępcy przechowują i udostępniają dziecięcą pornografię. Organa ścigania mogą zidentyfikować taki komputer, natomiast wykrycie w nim trojana będzie o wiele trudniejsze.

Co więc robić? Nawet jeżeli masz aktualnego antywirusa, warto sprawdzać swój komputer, czy nie zagnieździł się w nim malware. W Internecie są dostępne bezpłatne, nadające się do tego celu programy. Trzeba jednak poświęcić dużo czasu, żeby odnaleźć i wyłowić te najlepsze. Albo szybko i wygodnie skorzystać z tego e-booka. Proponowane w nim sposoby wykrywania (schwywania) i usuwania (ubicia) szkodników są zróżnicowane, od prostych typu „kliknij i wykryj” po bardziej złożone. Opierają się na wykorzystaniu bezpłatnego oprogramowania, dostępnego w Internecie jako freeware<sup>4</sup>, bądź bezpłatnych wersji produktów komercyjnych. Do ich użycia wystarczą podstawowe, praktyczne umiejętności, jakie posiada każdy aktywny internauta.

<sup>3</sup> <http://websecurity.pl/wirusy-trojany-robaki-co-to-jest-malware/>

<sup>4</sup> <http://pl.wikipedia.org/wiki/Freeware>

A może ja tylko straszę, może nie jest tak źle?

Proponuję więc szybkie zbadanie, jakie szkodniki ukrywają się w twoim komputerze. Zajmie to kilkanaście minut. Jesteś przekonany, że twój komputer jest na pewno „czysty”? Może tak – ja w to wątpię...

W eksperymencie posłużymy się komercyjnym programem Enigma SpyHunter w bezpłatnej wersji testowej (tylko wykrywa szkodniki, usuwanie - w pełnej wersji).

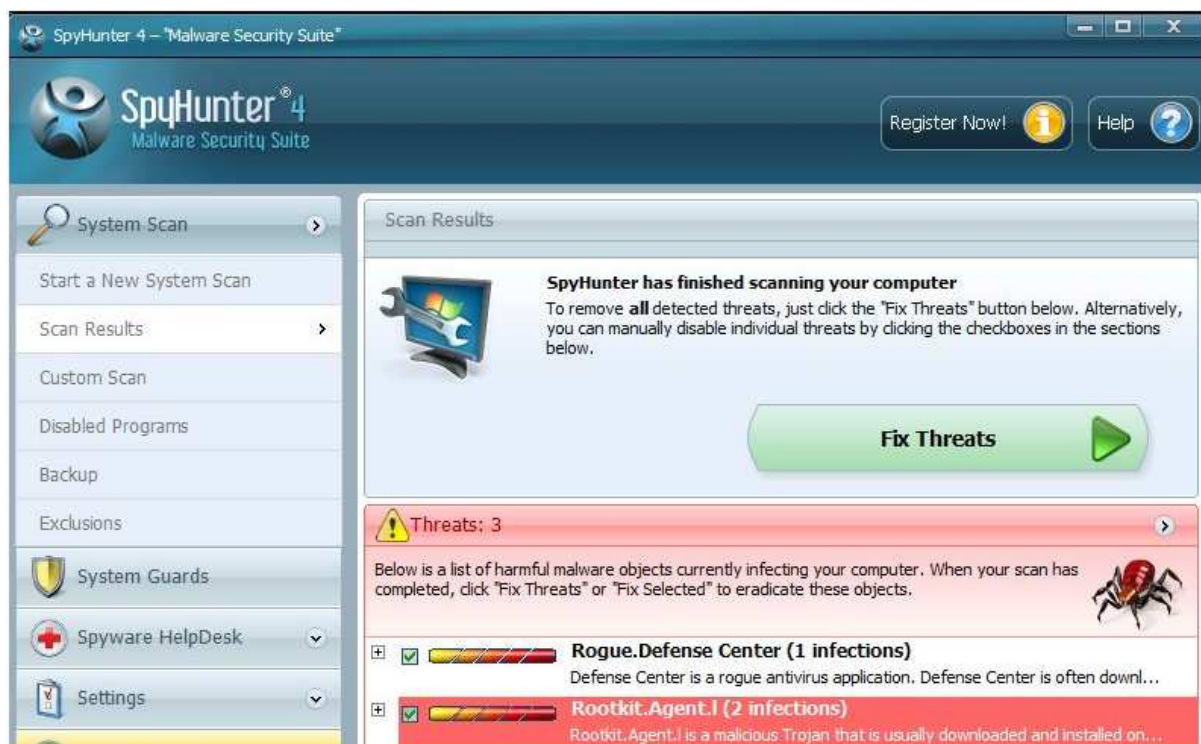
Ściągnij program ze strony producenta Enigma Software Group USA: [http://www.enigmasoftware.com/download\\_scanner/enigmasoftware.com/SpyHunter-Installer.exe](http://www.enigmasoftware.com/download_scanner/enigmasoftware.com/SpyHunter-Installer.exe), zapisz na pulpicie i zainstaluj z domyślnymi ustawieniami (to tylko kilka kliknięć myszką, Next, Next ... i Finish)



W systemach Vista/7/8 trzeba zezwolić na uruchomienie [SpyHunter-Installer.exe](#) z uprawnieniami administratora - [SpyHunter Downloader](#) (podpisany cyfrowo) zainstaluje właściwy program w aktualnej wersji.

Po ściągnięciu [SpyHunter installer'a](#) uruchomi się instalator – wybierz język angielski (polskiego nie ma), zaakceptuj warunki licencji i klikając **Next** zainstaluj program (odpowiedz **No** na propozycję włączenia ochrony przeglądarki). Program się uruchomi, automatycznie zaktualizuje i przystąpi do skanowania. Wyniki widać na bieżąco. Pełne skanowanie trwa dość długo. Możesz je w każdej chwili przerwać przyciskiem **Stop Scan** – jak już przekonasz się, że trochę tego malware'u jest w twoim kompie, chyba, że to fałszywe wykrycia;)

A oto przykładowe wyniki:



Po zakończeniu badania odinstaluj program (Start → Wszystkie Programy → SpyHunter → **Uninstall SpyHunter**).



Program SpyHunter nie będzie omawiany w e-booku.




## Jak korzystać z e-booka?

E-book ma być w zamyśle autora praktycznym poradnikiem z zakresu zwalczania złośliwego oprogramowania w komputerach PC z systemami Windows. Nie ma nic wspólnego z systematycznym wykładem, jest raczej „skrzynką z narzędziami”. Nie musi być czytany w kolejności rozdziałów, chociaż zostały one ułożone na zasadzie wzrastającej złożoności omawianych w nich programów. Warto jednak zacząć od przeczytania Wstępu, który w przystępnej formie prezentuje krajobraz współczesnego złośliwego oprogramowania oraz dostępnych narzędzi do jego zwalczania.

Zalecany sposób czytania e-booka, czy też raczej korzystania z zawartych w nim narzędzi, to jego otworenie w czytniku plików PDF – najbardziej znany jest bezpłatny Adobe Reader<sup>5</sup>. E-book zawiera szczegółowy spis treści, który domyślnie otwiera się jako stale dostępne boczne zakładki oraz bardzo dużo linków zarówno wewnętrznych, jak również do programów i materiałów informacyjnych w Internecie.

Linki w tekście są podkreślone – ustawiony na nich kursor zmienia się w symbol ręki z palcem wskazującym (linki wewnętrzne) lub w symbol ręki z palcem wskazującym oraz literą W (linki internetowe).

Zwracam uwagę, że Adobe Reader ma wygodne skróty klawiszowe. Szczególnie pomocny jest szybki powrót do poprzedniego widoku (na przykład po kliknięciu linku wewnętrznego) - naciśnij i przytrzymaj klawisz <Alt>, a następnie  (Lewa strzałka).

Spis treści (główny i boczne zakładki), linki wewnętrzne i linki internetowe działają tylko w pełnej wersji e-booka.

Zaczynamy deRATyzację twojego komputera. Powodzenia!

<sup>5</sup> <http://www.dobreprogramy.pl/Adobe-Reader-XI,Program,Windows,11539.html>

# I. Emsisoft Emergency Kit 3.0 – wygodny kombajn

## Ogólny opis Emsisoft Emergency Kit (EEK)

Producent tego oprogramowania, austriacka firma Emsisoft, tak opisuje swój produkt: „Emsisoft Emergency Kit to kolekcja specjalnie dobranych programów nie wymagających instalacji, przeznaczonych do skanowania i usuwania złośliwego oprogramowania z poważnie zainfekowanych komputerów”<sup>6</sup>. Jak wynika z opisu, kombajn zawiera **Skaner** antywirusowy - w niezależnych testach plasujący się w ścisłej czołówce najlepszych<sup>7</sup>. Istotne jest to, że może być on użyty niezależnie od już zainstalowanego na komputerze oprogramowania antywirusowego jako tzw. second opinion<sup>8</sup>. Jego użycie jest bardzo proste. Pozostałe składniki pakietu, **Skaner bez GUI**, **HiJackFree** oraz **BlitzBlank** są przeznaczone dla zaawansowanych użytkowników (w tym e-booku będą opisane tylko informacyjnie).



**Emsisoft Emergency Kit** może być używany bezpłatnie tylko do użytku prywatnego.

<sup>6</sup> <http://www.emsisoft.eu/pl/software/EEK/>

<sup>7</sup> <http://www.anti-malware-reviews.com/category/tests/> (w jęz. angielskim)

<sup>8</sup> <http://netsecurity.about.com/od/antivirusandmalware/a/Second-Opinion-Malware-Scanners.htm> (w jęz. angielskim)

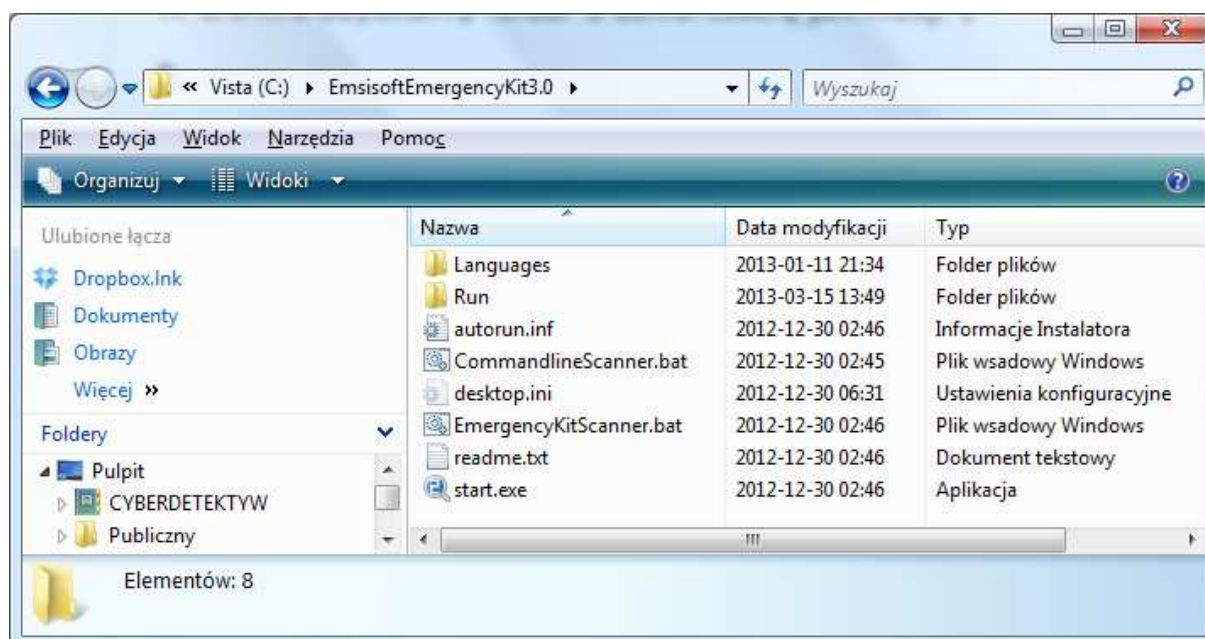
## Przygotowanie EEK do użycia

Program należy ściągnąć ze strony producenta, firmy Emsisoft:

<http://download4.emsisoft.com/EmsisoftEmergencyKit.zip>

Emsisoft Emergency Kit (EEK) nie wymaga instalacji. Ściągnięte archiwum [EmsisoftEmergencyKit.zip](#) (wersja 3.0.0.3, około 260 MB) należy rozpakować w dogodnym miejscu na twardym dysku. Warto najpierw utworzyć folder [Emsisoft Emergency Kit](#) (np. na dysku C:), skopiować do niego ściągnięte archiwum, a następnie rozpakować<sup>9</sup>.

W efekcie uzyskamy folder z zawartością, jak niżej:



Emsisoft Emergency Kit ma wielojęzyczny interfejs. Po dwukliku na pliku [start.exe](#) (lub [start](#)) uruchomi się i automatycznie rozpozna język systemu Windows. Będzie to język polski, chyba że ktoś używa Windows w innej wersji językowej. Ukaże się [Okno interfejsu EEK](#) umożliwiającego wybór właściwego narzędzia wchodzącego w skład kombajnu.

<sup>9</sup> <http://www.sonect.pl/sonectit/content/jak-otworzyc-plik-jak-rozpakowac-plik-zip>



Wszystkie narzędzia kombajnu Emsisoft zostaną omówione w dalszej części e-booka, szczegółowo skaner z interfejsem graficznym, a pozostałe składniki – informacyjnie (są przeznaczone dla zaawansowanych użytkowników systemów Windows).

Najczęściej używamy **Skanera Emergency Kit'a** z interfejsem graficznym. Dla większości użytkowników jest to właściwy wybór.



**Emsisoft Emergency Kit** jest w pełni zgodny z już zainstalowanym na komputerze oprogramowaniem antywirusowym.

## Skaner Emergency Kit

Skaner służy do sprawdzenia komputera - wykrycia złośliwego oprogramowania. Wykorzystuje podwójny silnik skanujący, dlatego zapewnia wysoką wykrywalność szkodników. Własny silnik<sup>10</sup> Emsisoft'a jest wspomagany przez dobry silnik BitDefender'a. Istotne jest to, że oba silniki są odpowiednio zintegrowane, aby uniknąć zbędnego podwójnego wykrywania oraz zmniejszyć obciążenie komputera.

Skaner uruchom korzystając z [Okna interfejsu EEK](#). Ładowanie programu trwa dość długo - kilkanaście/ kilkadziesiąt sekund i ukaże się poniższy interfejs:

**Emsisoft EMERGENCY KIT**

Pomoc

**Status Ochrony**

**Skaner Malware**

Ostatnie skanowanie: 13-03-11 21:33 [Skanuj teraz](#)

Wykryte obiekty: 0 [Zresetuj licznik](#)

**Emergency Kit**

Ostatnia aktualizacja: 13-03-11 20:40 [Aktualizuj teraz](#)

Wersja programu: 3.0.0.4 [Ustawienia aktualizatora](#)

Sygnatury malware: 12 241 751

Licencja: bezpłatna

**Podpowiedź: Emsisoft Anti-Malware**

Wypróbuj za darmo 30 dniową wersję testową Emsisoft Anti-Malware ze strażnikiem (i więcej), aby chronić swój komputer przed szkodnikami!

[Pobierz 30 dniową wersję teraz!](#) [Kup online - tylko \\$40!](#)

**Emsisoft online:**

- [Strona domowa](#)
- [Centrum pomocy](#)
- [Forum dyskusyjne](#)
- [Biuletyn informacyjny](#)
- [Wyślij podejrzany plik](#)

**Wiadomości:**

2013-02-25

**Hacked NBC websites infected unsuspecting visitors with malware**

[Wstecz](#) [Starsze newsy](#)

© 2003-2013 Emsisoft

<sup>10</sup> [http://www.wiruspc.pl/glossary/id,16935/silnik\\_antywirusowy\\_.html](http://www.wiruspc.pl/glossary/id,16935/silnik_antywirusowy_.html)

Domyślnie wyświetla się okno **Okno Statusu Ochrony**. W oknie tym niezwykle ważna jest data ostatniej aktualizacji sygnatur skanera - **wyświetlana w kolorze czerwonym**, sygnalizuje nam, że są już dostępne nowsze sygnatury.

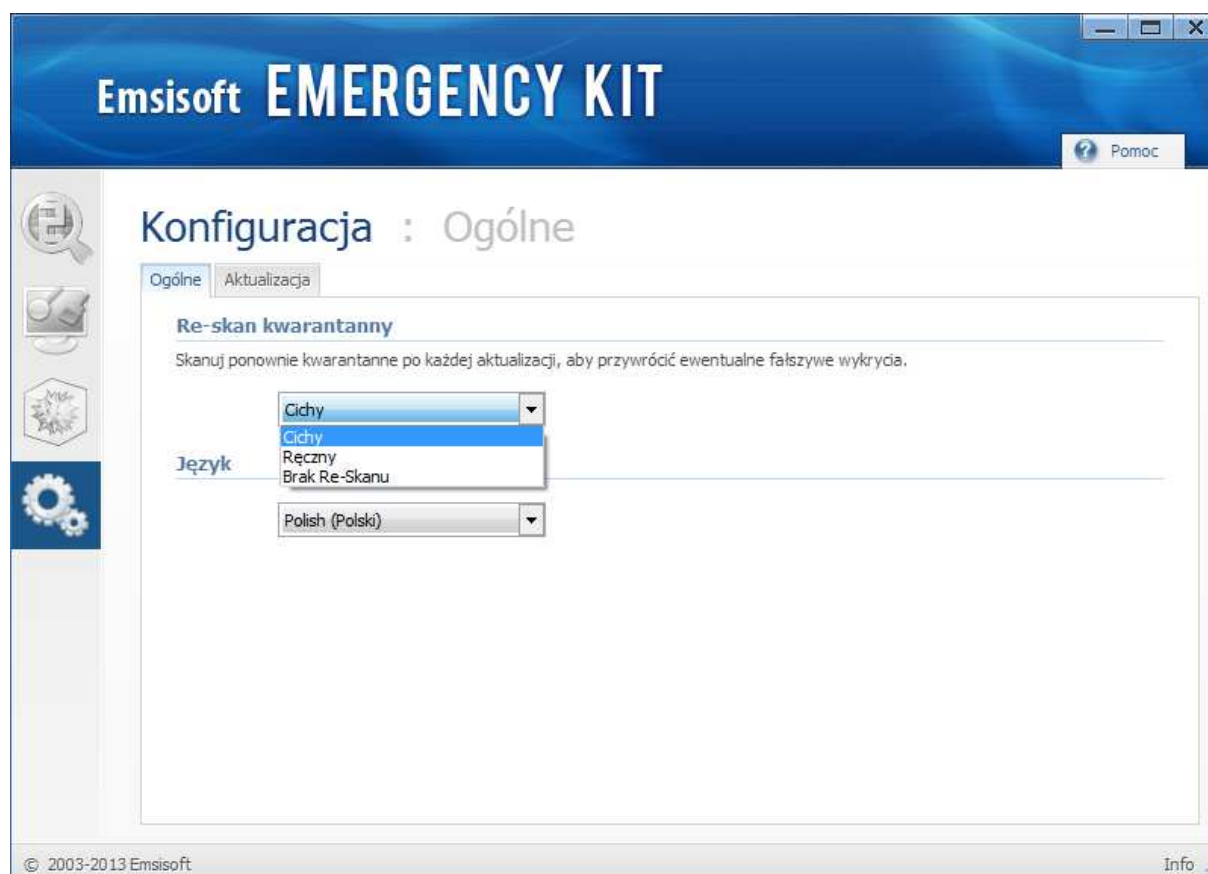
**!** Aktualizacja Skanera Malware decyduje o jego zdolności do wykrywania najnowszych szkodników. **Zawsze aktualizuj skaner, jeżeli data ostatniej aktualizacji jest wyświetlana na czerwono.**

W prawym dolnym rogu znajduje się mało widoczny, lecz ważny przycisk **Info**. Zawarte są tam informacje o oprogramowaniu.



Przycisk **Pomoc** w prawym górnym rogu otwiera plik tekstowy [readme.txt](#) z informacjami w języku angielskim.

Zanim przejdziemy od omówienia opcji *Skanowania i Kwarantanny*, omówimy *Ustawienia*. Kliknij **Ustawienia**, aby otworzyć okno, jak niżej:



Opcja *Re-skan kwarantanny* pozwala wybrać tryb przywracania plików lub wpisów rejestru, fałszywie zakwalifikowanych przy wcześniejszym skanowaniu jako złośliwe i usuniętych do kwarantanny. Domyślne ustawienie **Cichy** oznacza automatyczne przywrócenie bez udziału użytkownika.

Opcja *Język (Language)* pozwala zmienić język interfejsu. Może to być przydatne, gdy EEK nie rozpozna automatycznie języka polskiego.

Kolejna zakładka [Okna Konfiguracja](#) - *Aktualizacja* zawiera opcje *Prywatność* oraz *Ustawienia aktualizacji* (dostępne również jako *Ustawienia aktualizatora* w [Oknie Statusu Ochrony](#)). Domyślnie włączoną opcję *Dołącz do sieci Anti-Malware Network* można odznaczyć – żadne informacje z komputera nie będą przekazywane do Emsisoft. Opcja *Instaluj dodatkowe języki* jest domyślnie włączona i tak powinno być, jeśli używamy polskiego interfejsu. Domyślnie wyłączonej opcji *Instaluj aktualizacje beta* nie warto włączać. Kliknięcie *Ustawień połączenia* umożliwia ustawienie parametrów serwera proxy, lecz najczęściej jest to niepotrzebne.

Zmienione ustawienia zostaną zapamiętane przez program.

Warto podkreślić, że **domyślne ustawienia będą właściwe w większości przypadków i nie ma potrzeby ich zmieniania**. Domyślnie włączona opcja *Dołącz do sieci Anti-Malware Network* nie jest zagrożeniem prywatności. Można się o tym przekonać czytając Politykę prywatności (Privacy Policy) Emsisoft.

Przycisk **Skanowanie** wyświetla [Okno Skanuj PC](#), umożliwiające wybór rodzaju i rozpoczęcie skanowania (omówione na następnej stronie).

Dostępne są cztery rodzaje skanowania: *Szybkie*, *Inteligentne*, *Dokładne* oraz *Własne*.

Proponowana domyślnie opcja *Dokładne* zapewnia gruntowne sprawdzenie, ale będzie ono bardzo długo trwało. Zalecam skanowanie raz na kilka dni lub chociaż raz na tydzień, przy czym wystarczy wybrać opcję *Szybkie* lub *Inteligentne*.

W czasie skanowania można normalnie pracować – jeżeli uruchomione skanowanie zbyt mocno spowalnia komputer, warto użyć [Ustawień wydajności](#) i obniżyć *Priorytet skanowania*. Do wyboru mamy ustawienia od *Poniżej normalnego* do *W czasie bezczynności* (komputera).





## Szybkie skanowanie

Umożliwia szybkie wykrycie aktywnego w komputerze malware'u. Skanowane są wszystkie uruchomione programy, procesy w pamięci operacyjnej oraz ślady spyware. Jego zaletą jest szybkość, lecz nie wykryje wszystkich szkodników, ukrywających się w twoim komputerze.

## Inteligentne skanowanie

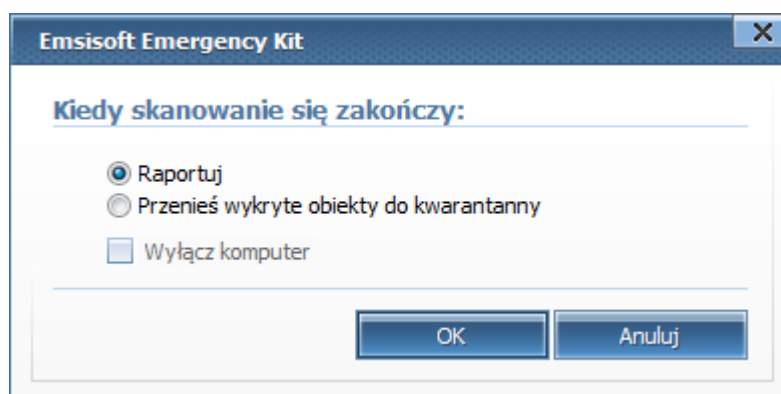
*Inteligentne skanowanie* sprawdza te same obiekty, co skanowanie *Szybkie*, i dodatkowo foldery *C:\Windows\* i *C:\Program Files\* w których najczęściej ukrywa się malware. Oprócz tego skanowane są niewidoczne w Eksploratorze Windows tzw. Alternatywne Strumienie Danych (więcej w [Rozdziale V Stream Armor – wnikliwy detektyw](#)).

## Dokładne skanowanie

*Dokładne skanowanie* trwa bardzo długo, lecz zapewnia wykrycie szkodników ukrytych np. w plikach archiwów. Skanowane są wszystkie twarde dyski zainstalowane w komputerze i te podłączone przez USB.

*Dokładne skanowanie* komputera jest zalecane, gdy po raz pierwszy używamy EEK lub gdy skanowanie *Szybkie* lub *Inteligentne* wykryło szkodniki.

Można uruchomić *Dokładne skanowanie* po zakończeniu pracy, np. na noc, i użyć opcji *Po zakończeniu skanowania*.



Domyślnie zaznaczona jest opcja *Raportuj* i jest to rozsądny wybór, ponieważ pozwala użytkownikowi zdecydować, co zrobić z wykrytymi obiektami. Wymaga to interakcji użytkownika po zakończeniu skanowania. Można też wybrać opcję *Przenieś wykryte obiekty do kwarantanny*<sup>11</sup> (jest możliwość ich przywrócenia, w przypadku fałszywego wykrycia). Zapewnia to zautomatyzowaną obsługę wykrytych obiektów, co jest dobrym wyborem dla większości użytkowników.

Zaznaczenie opcji *Wyłącz komputer* spowoduje automatyczne zamknięcie Windows i wyłączenie komputera po zakończeniu skanowania.

<sup>11</sup> [http://pl.wikipedia.org/wiki/Kwarantanna\\_\(informatyka\)](http://pl.wikipedia.org/wiki/Kwarantanna_(informatyka))

## Własne skanowanie



Jest to opcja dla doświadczonych użytkowników. Umożliwia własny wybór parametrów przed rozpoczęciem skanowania - nie tylko konkretnych dysków, czy folderów, lecz również ustawień skanowania. Zwracam uwagę na możliwość wybrania opcji *Używaj bezpośredniego dostępu do dysku*. Jest to realizowane za pomocą drivera *A2 Direct Disk Access Support Driver*, instalowanego podczas startu **Skanera**. Bezpośredni dostęp do dysku umożliwia skuteczne wykrycie maskowanych za pomocą rootkit'a<sup>12</sup> (lub podobnego mechanizmu) plików. Driver jest odinstalowywany po zamknięciu **Skanera Emergency Kit'a**.

<sup>12</sup>[http://www.sans.org/score/checklists/rootkits\\_investigation\\_procedures.odt](http://www.sans.org/score/checklists/rootkits_investigation_procedures.odt) (bardzo dobre opracowanie SANS Institute na temat rootkit'ów, w języku angielskim, strona 4)

Antywirusy nie wykrywają najgroźniejszego złośliwego oprogramowania. Dzieje się tak dlatego, że na komputerze ofiary instalują się unikatowe w formie binarnej, kontrolowane przez cyberprzestępców programy. Ich obecność w komputerze jest maskowana przez zastosowanie wyrafinowanych technik ukrywania w systemie, określanych mianem rootkita. Są to zaawansowane trojany, służące do wykradania z komputerów wartościowych informacji wykorzystywanych w przestępczych celach, najczęściej w celu osiągnięcia finansowych korzyści.

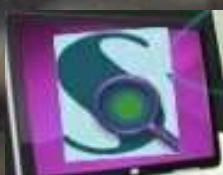
W literaturze są one określane jako Trojany Zdalnego Dostępu, z ang. Remote Access Trojans. W skrócie RAT, stąd w tytule DeRATyzacja komputerów.

E-book jest poradnikiem w zakresie praktycznych metod wykrywania i usuwania złośliwego oprogramowania z komputerów PC. Do ich użycia wystarczą podstawowe, praktyczne umiejętności, które posiada każdy aktywny internauta oraz bezpłatne oprogramowanie.

ISBN 978-83-62255-42-9

**Leszek IGNATOWICZ** Ekspert w zakresie badania cyfrowych śladów w komputerach PC, wykrywania i analizy złośliwego oprogramowania. Członek stowarzyszenia **Instytut Informatyki Śledczej**. Pracuje w zespole reagowania na incydenty komputerowe.

Twórca i lider projektu **SysClinic.pl** popularyzującego skuteczne sposoby zwalczania złośliwego oprogramowania z wykorzystaniem najlepszych, bezpłatnych i łatwo dostępnych w Internecie programów.



[www.SysClinic.pl](http://www.SysClinic.pl)