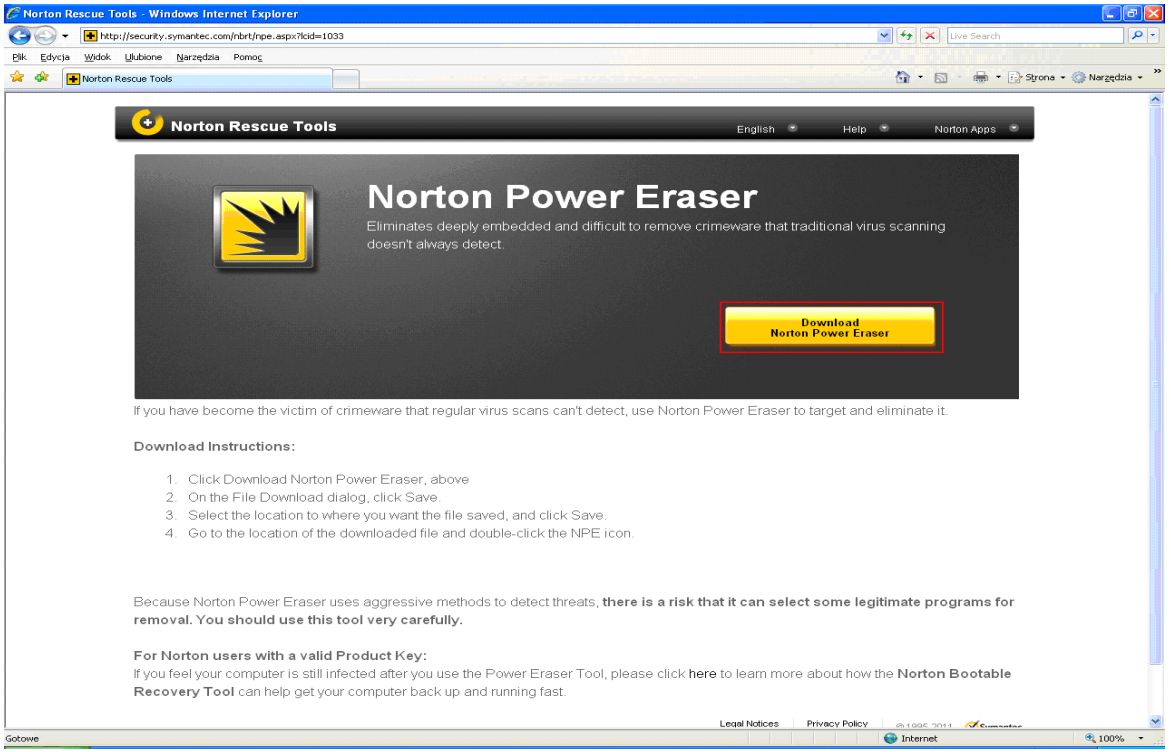
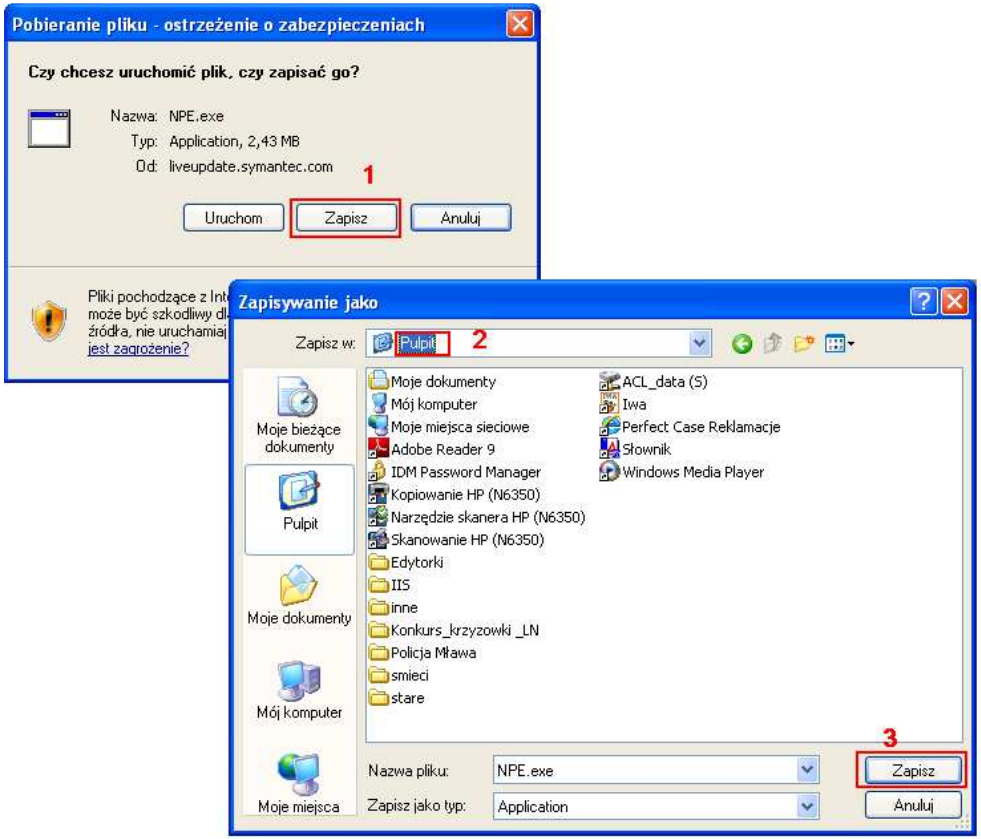
Usuwanie Trojana SpyEye

Skąd pobrać program?

W poniższym przykładzie został wykorzystany program NPE (Norton Power Eraser) firmy Symantec
Program można pobrać ze stron:
- http://security.symantec.com/nbrt/npe.aspx?lcid=1033
- http://us.norton.com/support/DIY/index.jsp



Po naciśnięciu przycisku ***Download Norton Power Eraser*** otwiera się okno pobierania pliku.



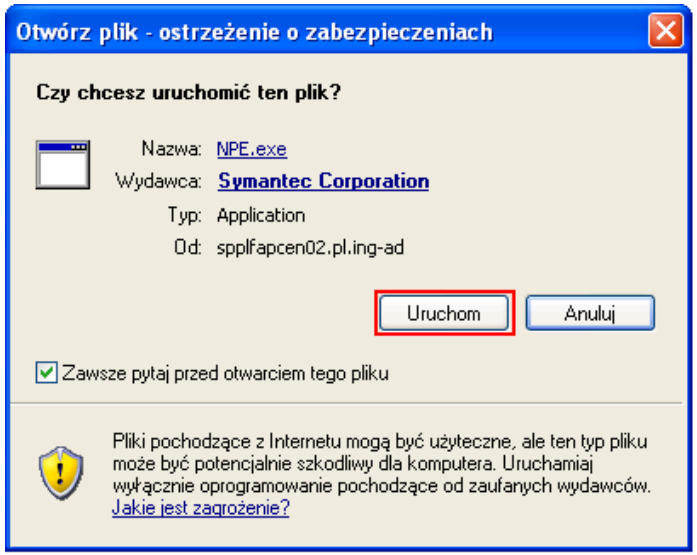
W celu pobrania pliku należy wykonać następujące czynności:

1. Pobrać plik **NPE.exe** poprzez przycisk ***Zapisz***
2. Wybrać miejsce, gdzie zostanie zapisany plik **NPE.exe** (np Pulpit)
3. Ponownie wybrać przycisk ***Zapisz***

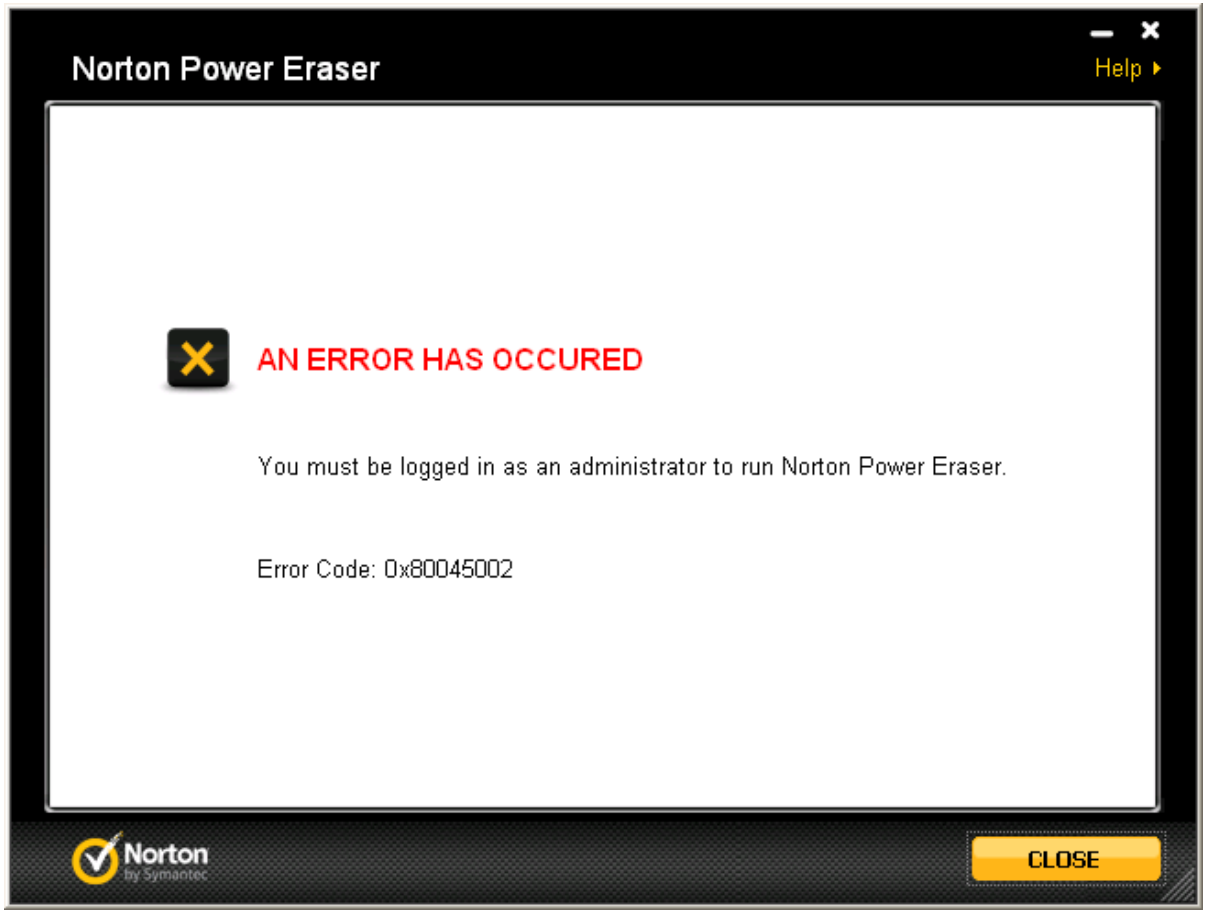
Po prawidłowym wykonaniu wszystkich opisanych powyżej czynności na pulpicie pojawi się nowa ikona pliku **NPE.exe**

Jak zainstalować NPE i usunąć Trojana?

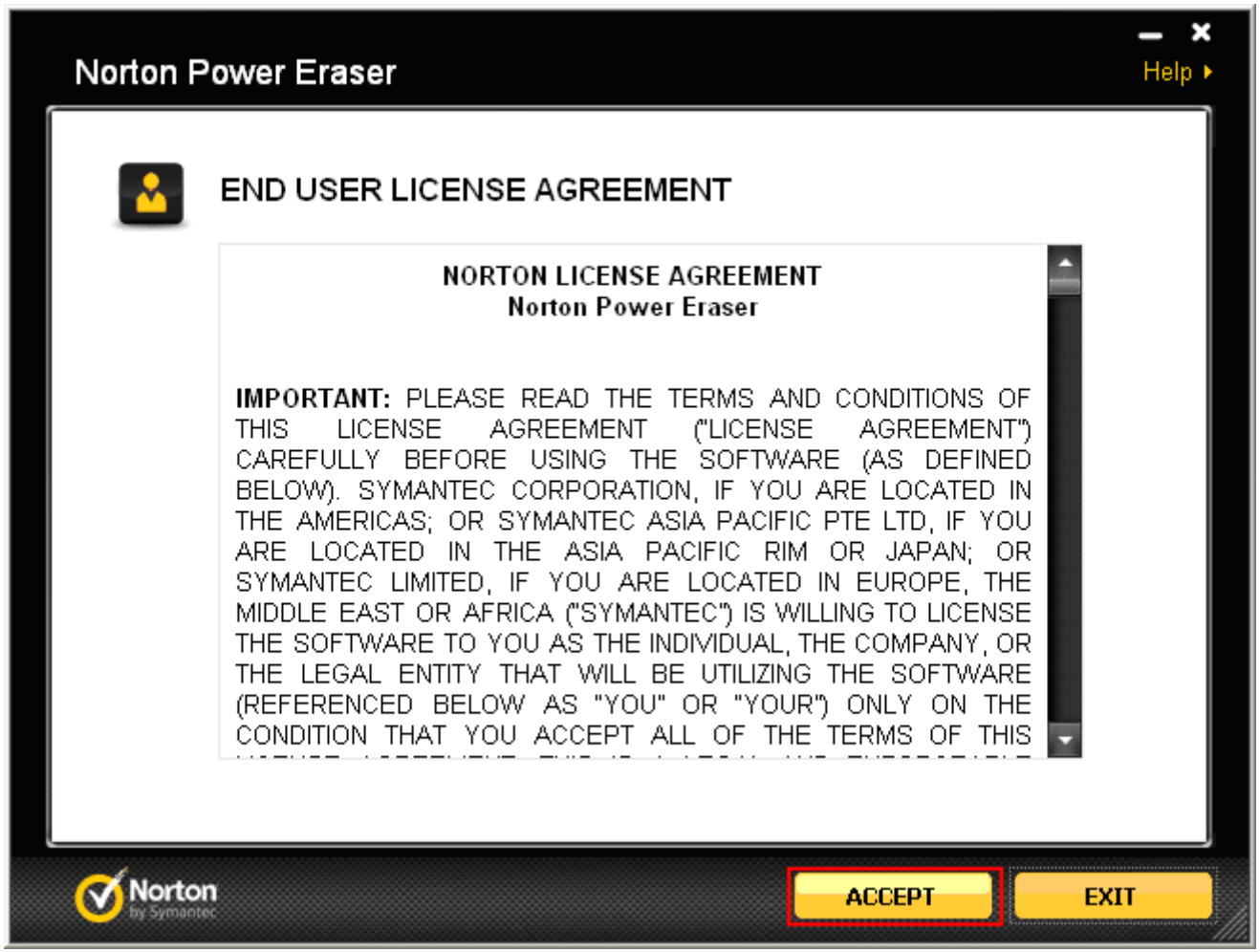
Program nie wymaga tradycyjnej instalacji. Wystarczy dwukrotnie nacisnąć lewy przycisk myszki na ikonie programu **NPE.exe**. Należy wybrać opcję ***Uruchom.***



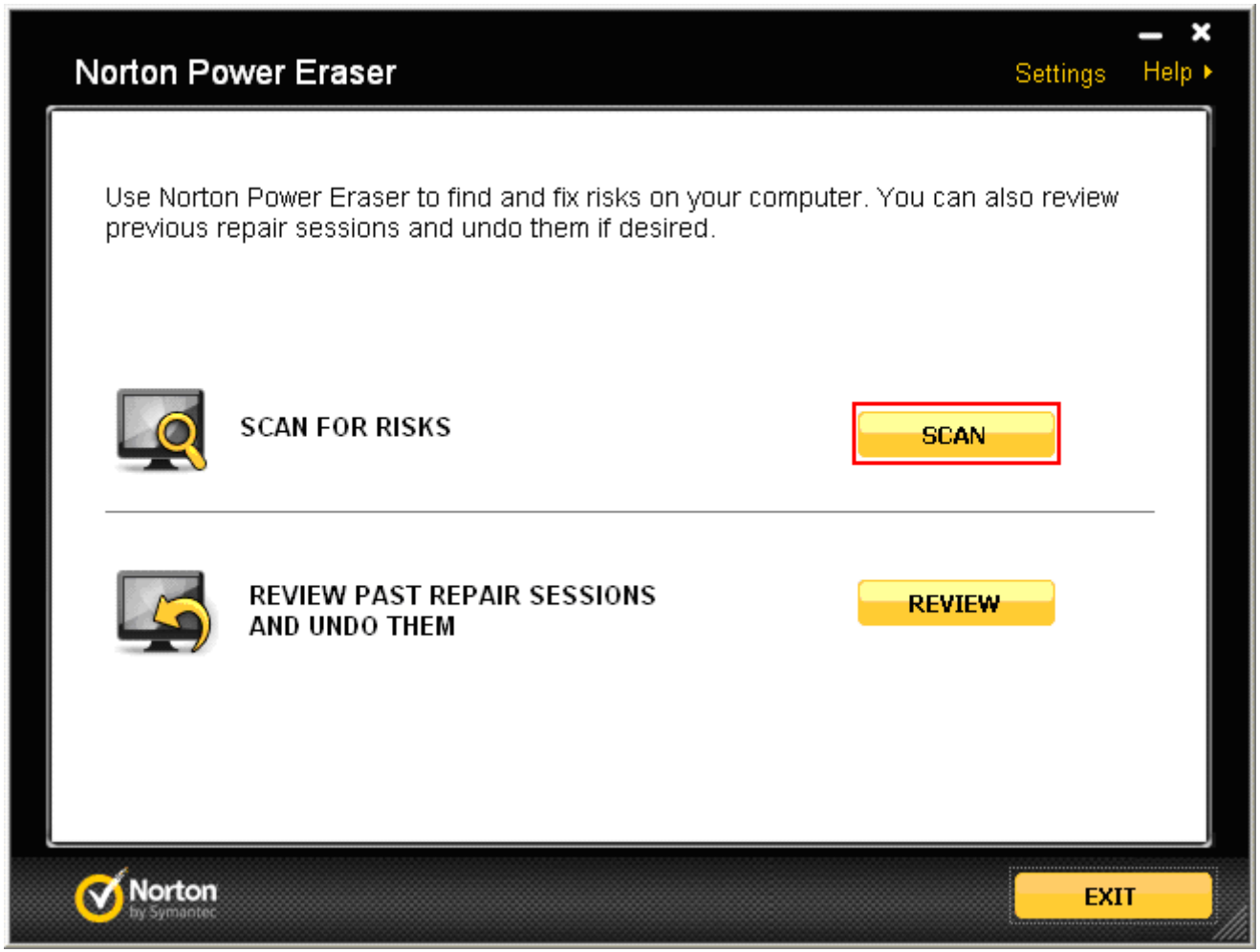
W przypadku braku uprawnień administratora na ekranie pojawi się poniższy komunikat:



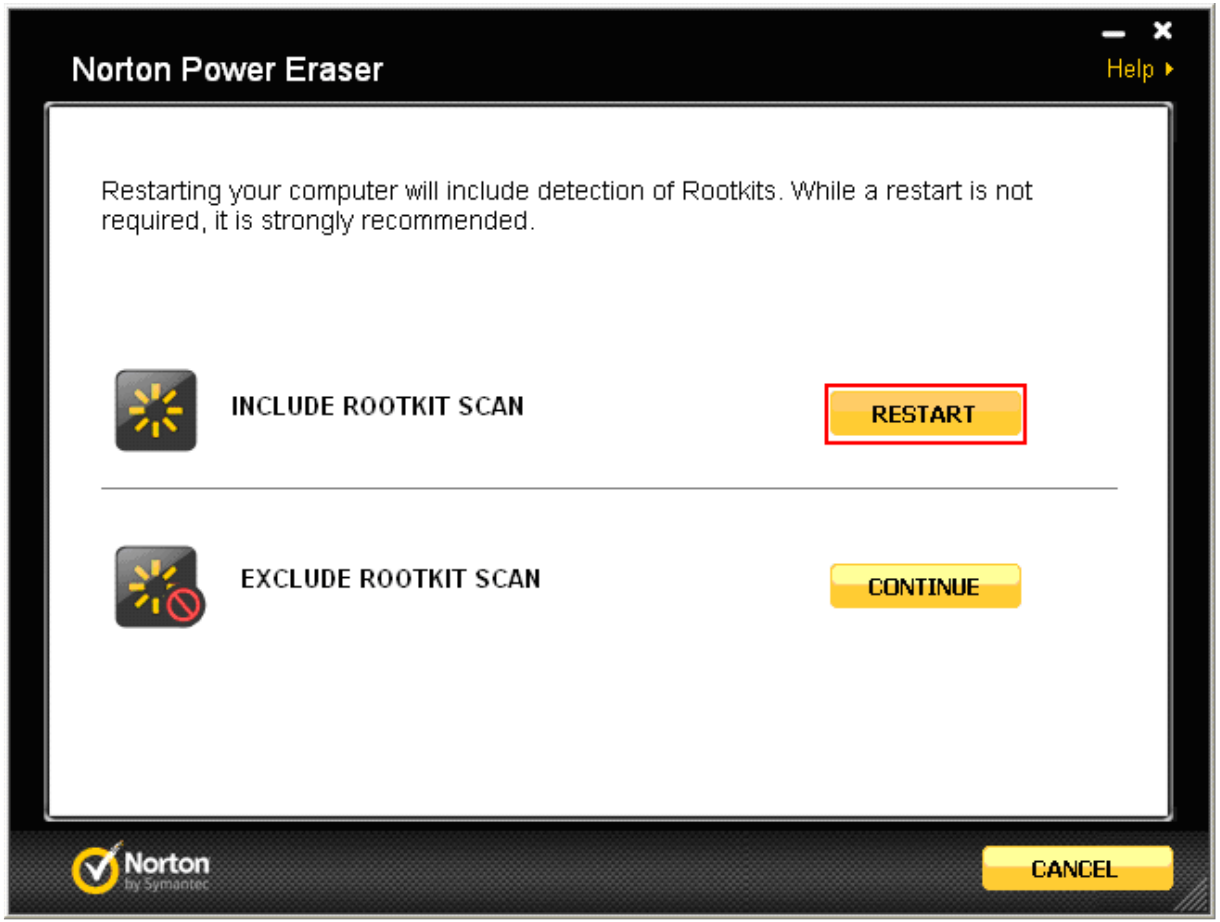
W przypadku posiadania uprawnień administratora należy zaakceptować licencję klawiszem ***ACCEPT***:



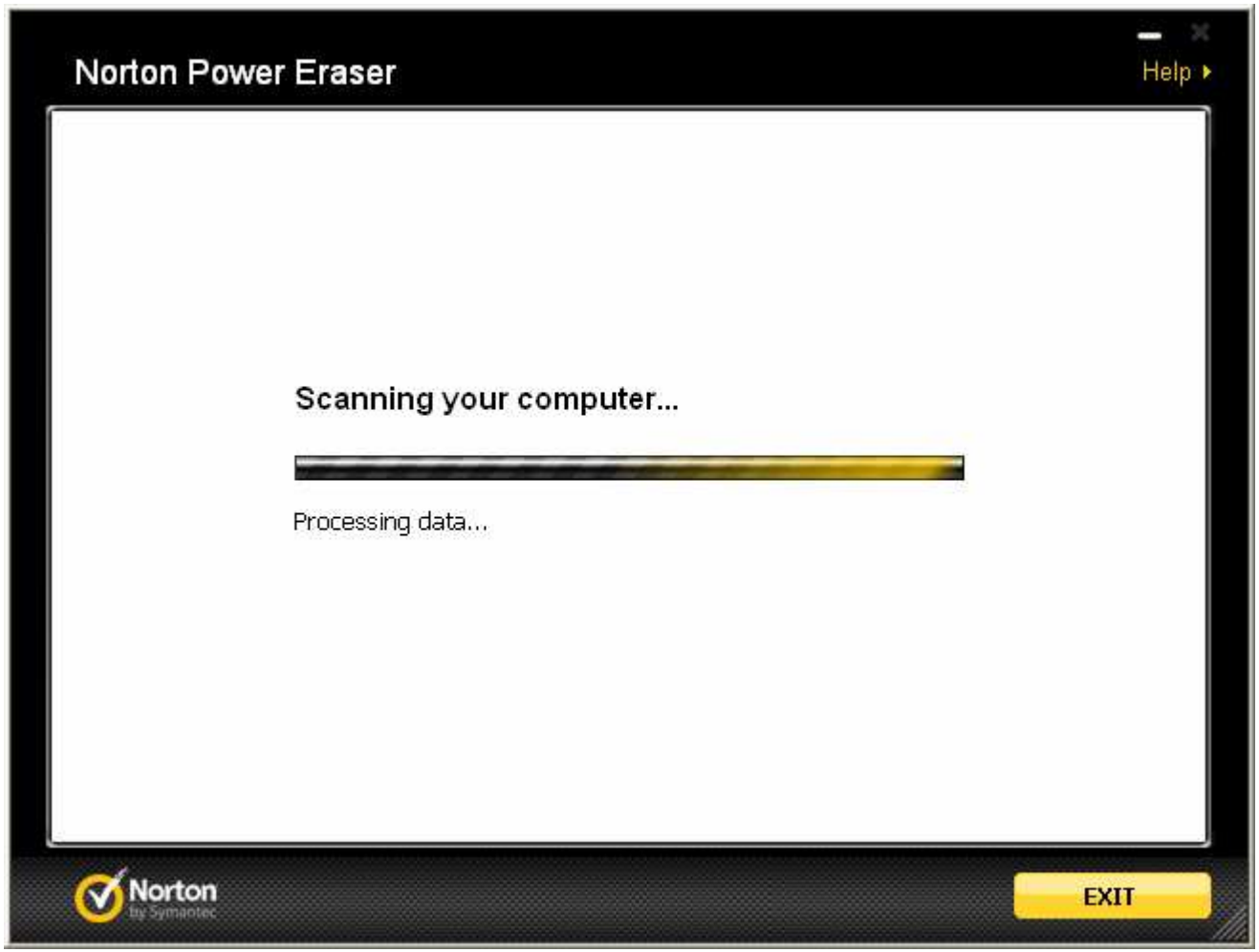
Po zaakceptowaniu licencji należy wybrać przycisk ***SCAN***



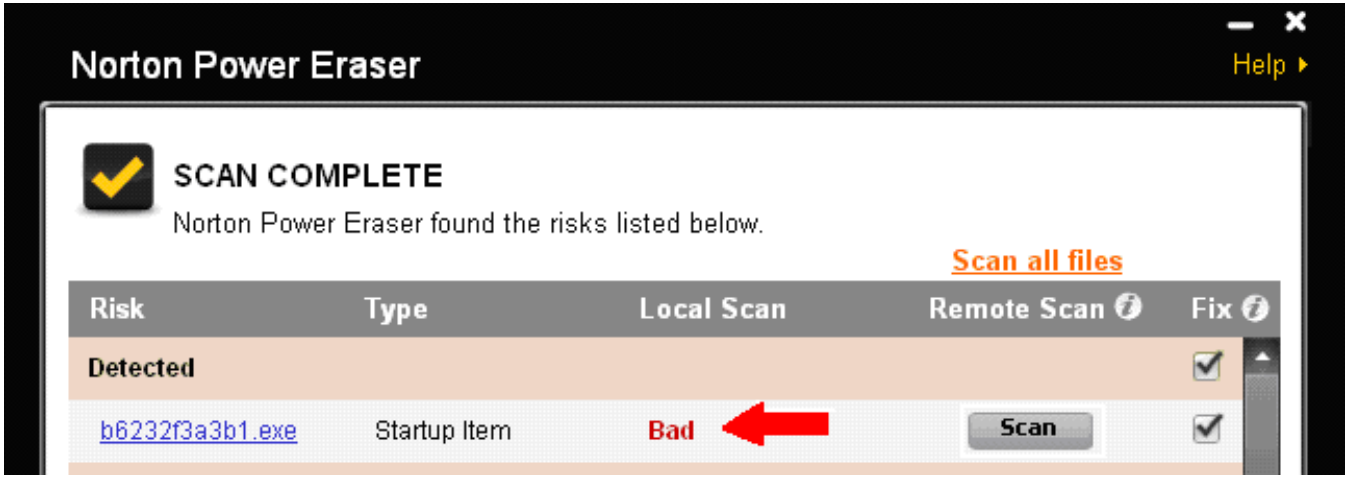
W kolejnym oknie pojawiają się dwie opcje do wyboru: **INCLUDE ROOTKIT SCAN** lub **EXCLUDE ROOTKIT SCAN.**
Należy wybrać **INCLUDE ROOTKIT SCAN** poprzez przycisk ***RESTART.*** Łączy się to z przeładowaniem systemu.
Opcja ta pozwala na dokładniejsze sprawdzenie naszego systemu.



Po przeładowaniu sytemu program **NPE** uruchomi się i zacznie skanowanie komputera.



Jeżeli program wykrył jakiekolwiek złośliwe oprogramowanie w oknie pojawi się informacja **Bad**



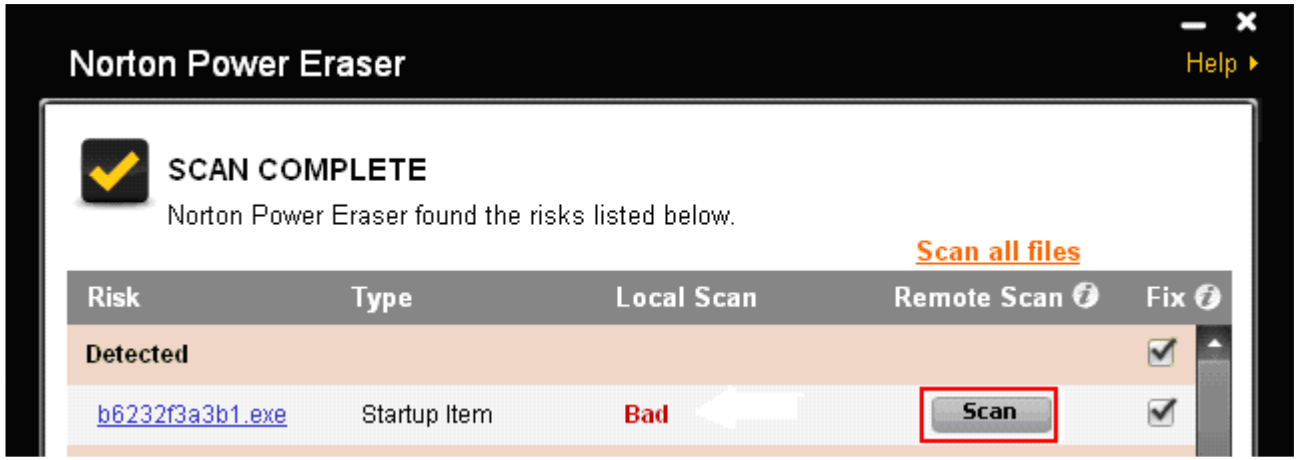
SpyEye w starej wersji tworzył ukryty katalog bezpośrednio w katalogu głównym, gdzie nazwa katalogu była taka sama jak nazwa pliku z Trojanem. Na przykład:

- ✓ **C:\mssm.exe\mssm.exe**
- ✓ **C:\cleansweep.exe\cleansweep.exe**
- ✓ **C:\ moonxxxxxx.exe \moonxxxxxx.exe**

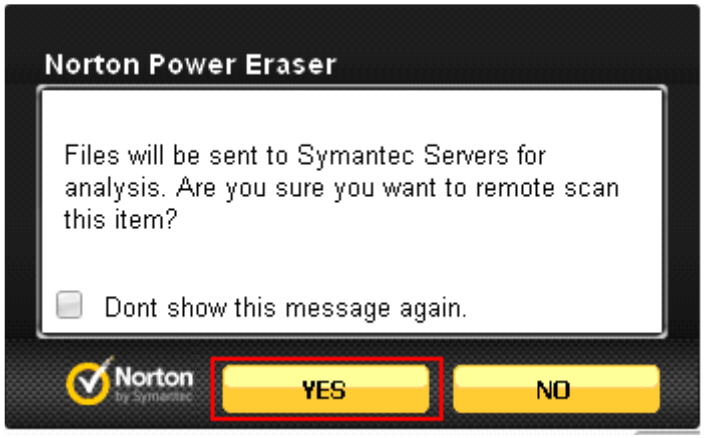
W obecnej wersji Trojan tworzy plik o losowej nazwie. W powyższym przykładzie jest to plik **b6232f33b1.exe**.

Plik ten znajduje się w katalogu ukrytym bezpośrednio w katalogu głównym. Można sprawdzić gdzie znajduje się znaleziony plik **b6232f33b1.exe** klikając myszka na pliku i wybierając ***Thread Details***
Widzimy ze plik znajduje się w **c:\recycle.bin**

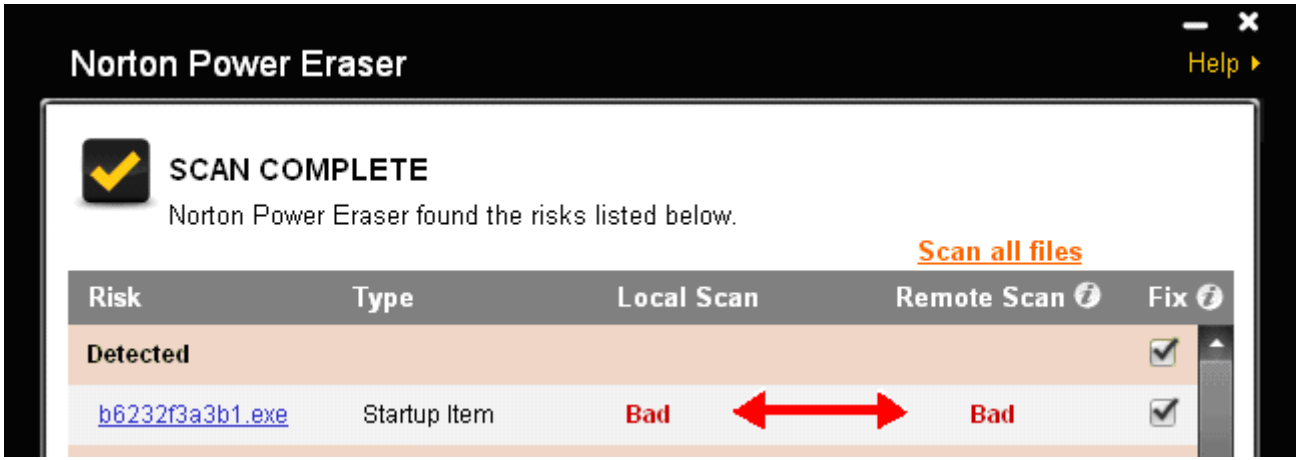
Mimo, że program oznaczył go, jako **Bad** dla pewności można przeskanować plik zdalnie.
W tym celu należy wybrać przycisk ***Scan*** znajdujący się obok nazwy pliku:



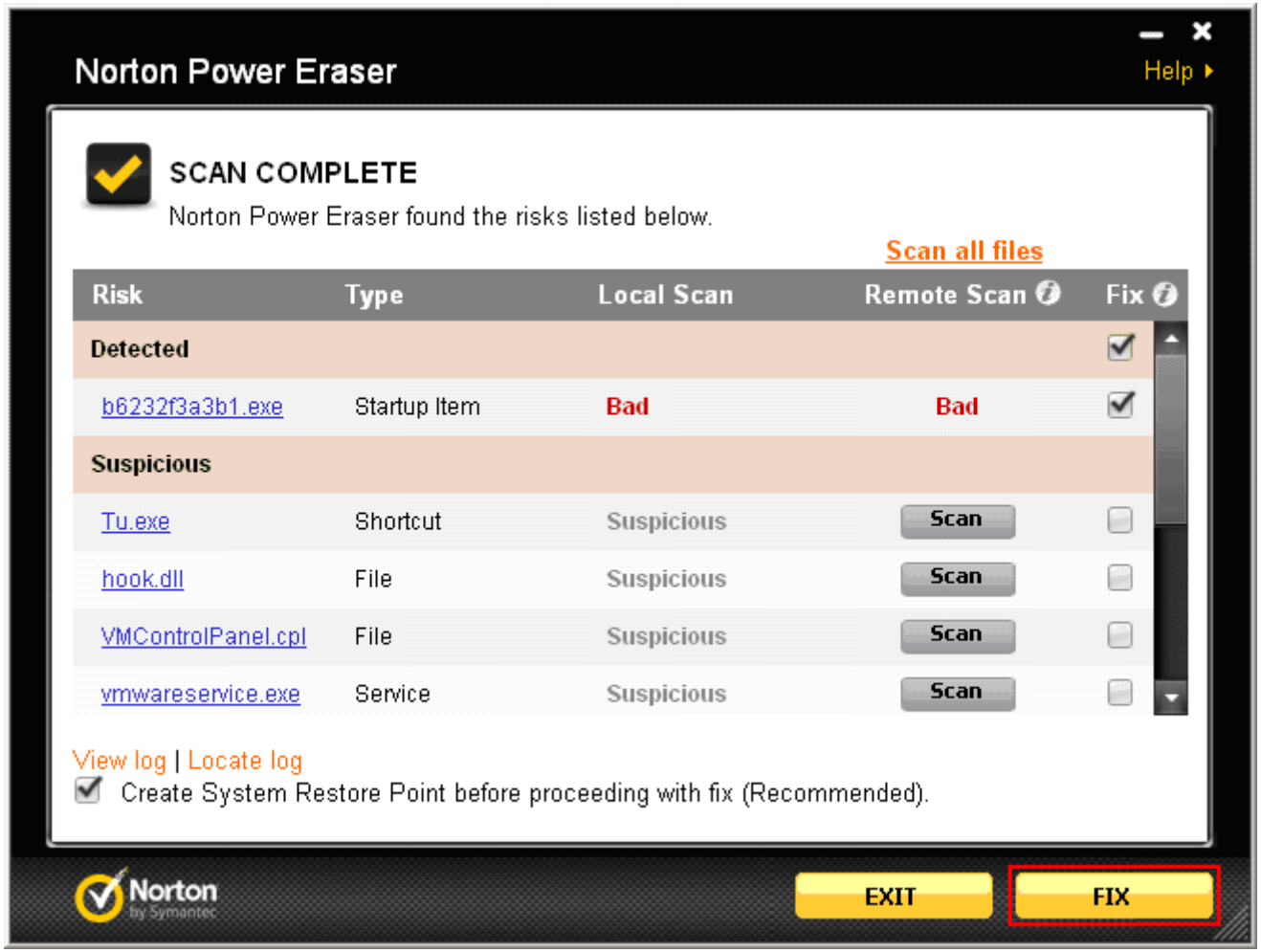
Należy następnie zgodzić się na przesłanie pliku na serwer firmy Symantec wybierając przycisk ***YES***



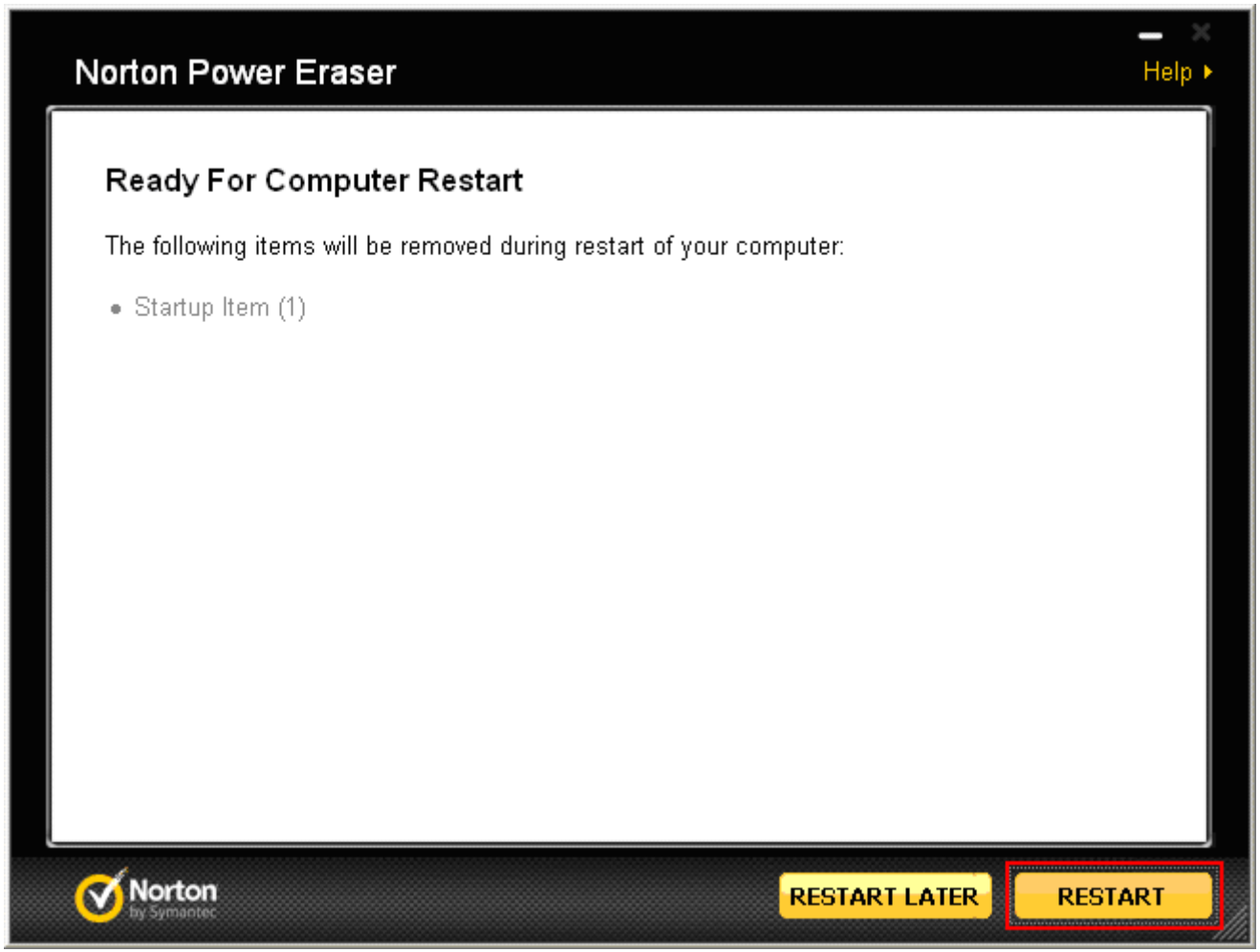
Poniżej otrzymane potwierdzenie, że plik jest złośliwym oprogramowaniem **Bad** przy **Remote Scan**:



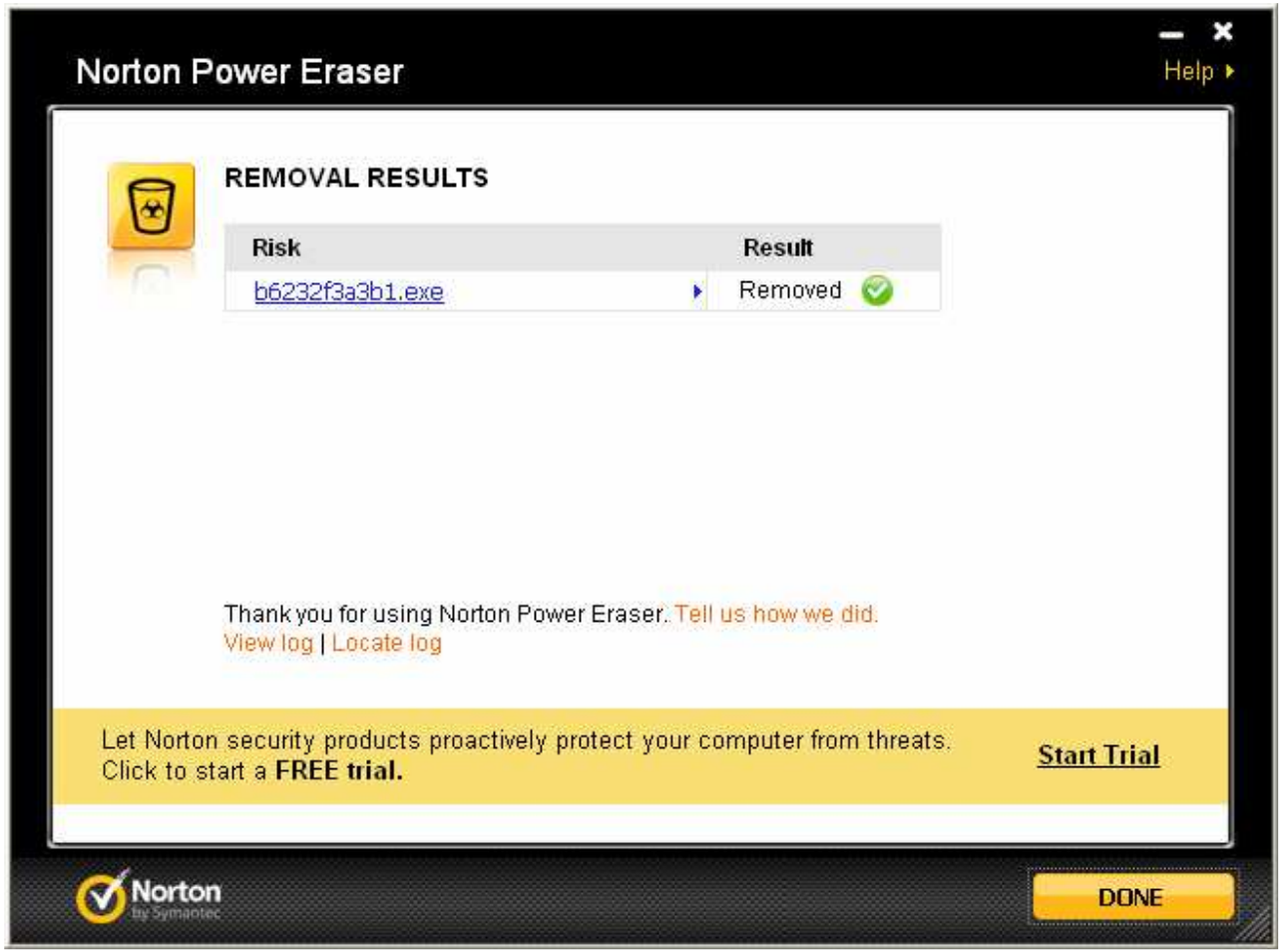
Można teraz przystąpić do usunięcia Trojana z komputera poprzez wybraniu przycisku ***FIX.***
Wszystkie zaznaczone pliki zostaną usunięte.



Po usunięciu Trojana należy wybrać ponowny restart systemu przyciskiem ***RESTART.***



Po przeładowaniu sytemu program NPE informuje o usuniętym pliku. Teraz należy nacisnąć przycisk ***DONE,*** który spowoduje zamknięcie aplikacji Norton Power Eraser.



Prezentowane powyżej informacje oparte są na faktach opisanych w ogólno-dostępnych publikacjach i służą jedynie poszerzaniu wiedzy ich czytelników o zagrożeniach występujących w Internecie.