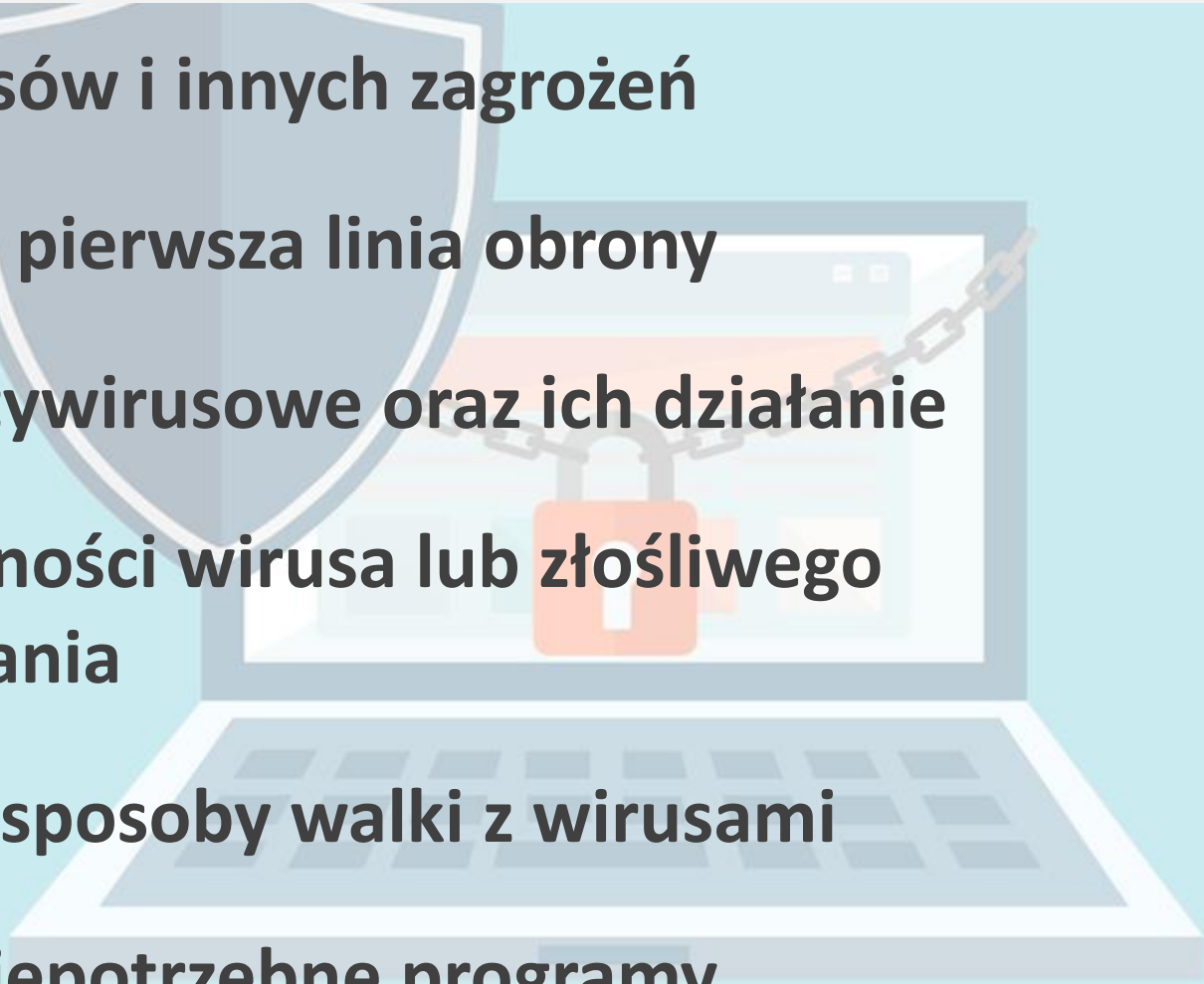
KONRAD POSTAWA

Czy złapałem wirusa?

Radzimy jak rozpoznać zagrożenie i co z tym zrobić.

INTERMEDIA
warsztaty komputerowe

Plan warsztatów



- Rodzaje wirusów i innych zagrożeń
- Firewall, czyli pierwsza linia obrony
- Programy antywirusowe oraz ich działanie
- Objawy obecności wirusa lub złośliwego oprogramowania
- Podstawowe sposoby walki z wirusami
- Szkodliwe i niepotrzebne programy
- Internet bez reklam i więcej prywatności

Rodzaje wirusów komputerowych

Wirusy komputerowe

W skrócie wirus to program, który sam się kopiuje!

Klasyczny wirus to „mały” program, który przyczepia się do jakiegoś pliku i dzięki temu ma możliwość dostania się do komputera oraz może się replikować (kopiować).

Robak, to samoreplikujący się program, bardzo przypominający wirusa, ale nie potrzebujący „nosiciela”.

Wabbit, to wirus, który nie przenosi się przez sieć, a jego głównym zadaniem jest powielanie się bez końca. Do czasu, aż zapełni pamięć komputera.

Wirusy komputerowe

Ciąg dalszy…

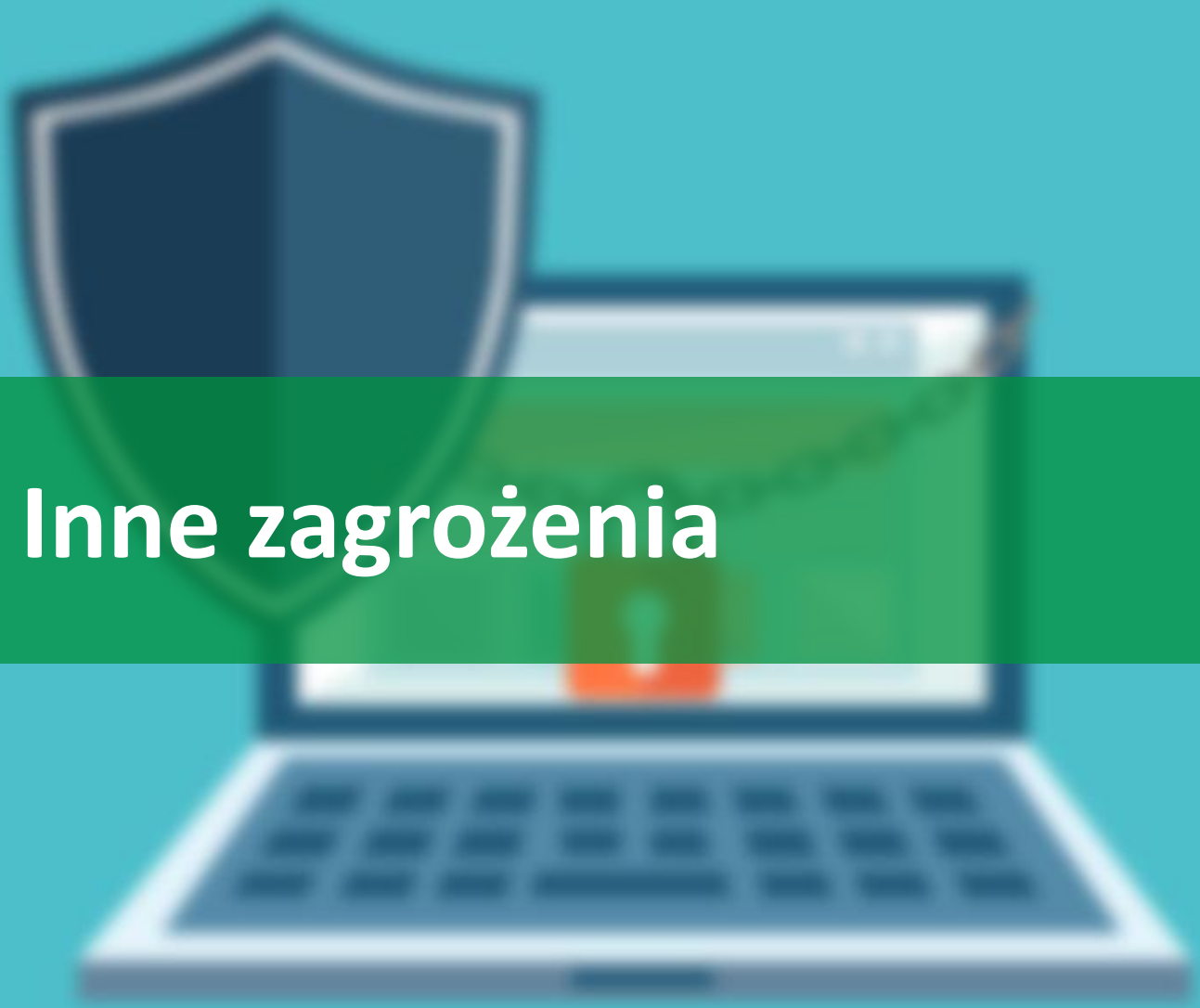
Koń trojański lub **trojan**, to oprogramowanie, które podszywa się pod inne i dzięki temu stara się dostać do komputera.

Adware, to program wyświetlający wszechobecne reklamy i zarabiający na tym (tych reklam nie możemy zamknąć).

Stealware, to program, który okrada użytkownika z zasobów komputera lub z danych.

Rootkit, to szczególnie ciężki przeciwnik, bo wirus ten maskuje swoje działanie i jest niemal niewykrywalny.

Inne zagrożenia



Nie tylko wirusy nam szkodzą…

…jest coś jeszcze.

Backdoor, czyli „tylna furtka” to luka w oprogramowaniu, która została tam umieszczona specjalnie, by mieć dostęp do systemu.

Exploit, sprytnie wykorzystuje błędy w oprogramowaniu, by przejąć kontrolę nad systemem.

Ransomware, czyli podmienione strony np. banków czy mediów społecznościowych. Sami oddajemy tam swoje dane.

Keylogger, to mechanizm podkradania danych prosto z klawiatury.

Firewall

Firewall, czyli zapora ogniowa

To pierwsza linia obrony!

Firewall pozwala na zdecydowanie jakie programy czy funkcje mogą wykorzystywać połączenie internetowe. Zapora ogniowa domyślnie blokuje wszystkie programy, a to my sami decydujemy, który z nich jest zaufany, a który nie.

Gdzie jest Firewall?

Ogólnie to wszędzie ;)

Pierwszy zapora ogniowa działa po stronie naszego dostawcy Internetu np. Orange, Vectra, TVK, Netia itp.

Druga zapora ogniowa działa na naszym routerze (o ile ją włączyliśmy) i ma za zadanie filtrować ruch zarówno z Internetu, jaki i pomiędzy naszymi urządzeniami.

Trzecia zapora ogniowa znajduje się w naszym systemie operacyjnym. Czasem zamiast tej wbudowanej może działać firewall z antywirusa.

Programy antywirusowe

Programy antywirusowe

Jest ich dość dużo, ale kilka jest wartych uwagi.

PŁATNE

ESET NOD32 Antivirus 11

Kaspersky Antivirus 2018

Norton Antivirus 22

DARMOWE

Avira Free Antivirus 15

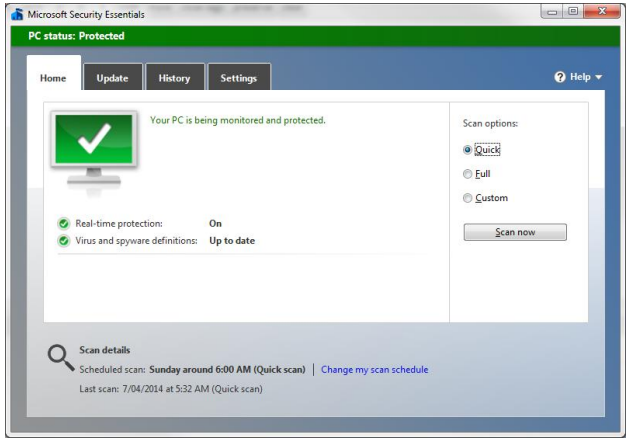
AVG AntiVirsu Free 2017

Avast Free Antivirus 17

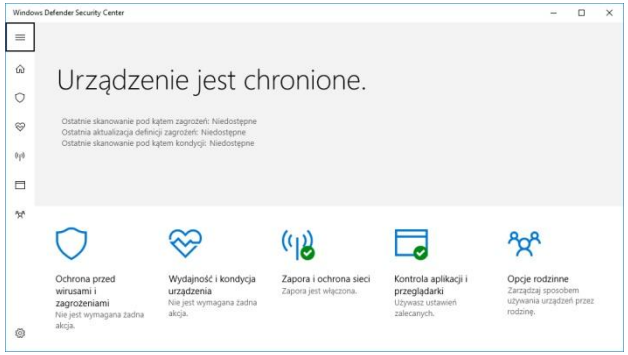
Windows Defender

Centrum bezpieczeństwa Microsoft

Windows Defender to podstawowy program antywirusowy zainstalowany na każdym komputerze z systemem Windows od Vista to 10.



Windows Defender Security Center to centrum bezpieczeństwa z Windows 8 / 8.1 / 10



Jak to działa?

Antywirus = strażnik

- **Antywirus posiada bazę zagrożeń** (bazę sygnatur wirusów), czyli informacje o tym, co może komputerowi zaszkodzić.
- **Monitorowanie zachowań** – sprawdzanie co robią programy i pilnowanie by były „grzeczne”.
- **Monitorowanie poczty** – sprawdzanie czy maile, a szczególnie załączniki nie zawierają wirusów

Co jeszcze?

Antywirus = strażnik

- **Heurystyka**, czyli rozpoznawanie zagrożeń na podstawie wzorców. Działa niezależnie od sygnatur wirusów.
- **Skanowanie zaplanowane**, to okresowe, cykliczne sprawdzanie komputera w poszukiwaniu zagrożeń.
- **Tworzenie kopii** – antywirus może tworzyć kopię ważnych plików systemowych, by móc je naprawić podczas awarii.
- **Kwarantanna** – możliwość izolacji „zakażonych” plików.

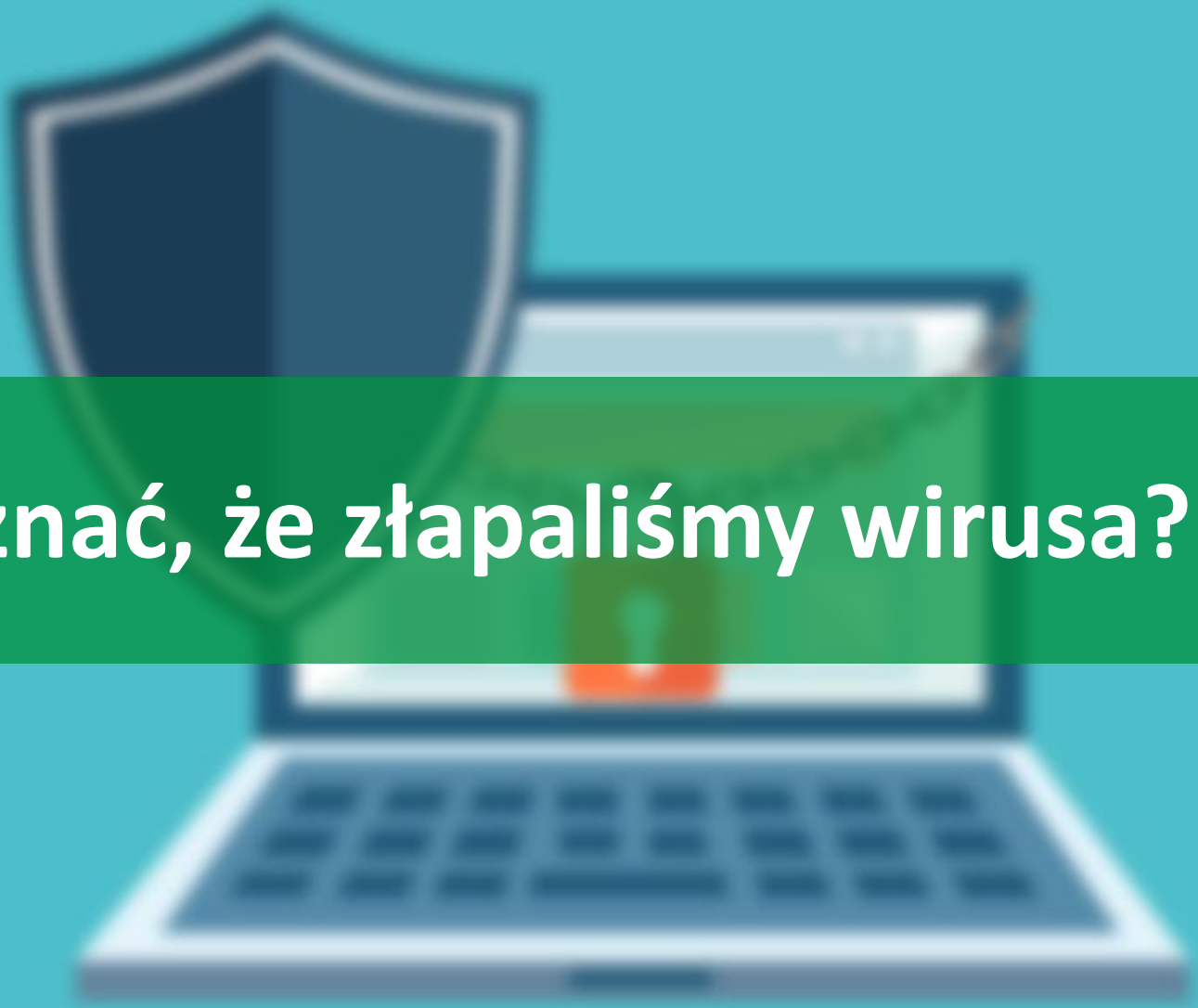
O czym musimy pamiętać?

Bo o czymś musimy ;)

- **Antywirus musi być włączony – zawsze!**
- **Antywirus musi być aktualizowany regularnie!**
- **Jeśli antywirus wyświetli komunikat to czytajmy go uważnie!**

Możemy plik „Wyleczyć”, „Usunąć” lub możemy nic nie robić. Wszystko zależy od sytuacji.

Jak rozpoznać, że złapaliśmy wirusa?



Objawów infekcji jest wiele

Tylko jakie to objawy?

Najczęściej jeśli złapiemy wirusa to zadziała on tak, że to zauważymy. Objawy mogą być bardzo różne, ale gwarantuje, że komputer będzie zachowywał się dziwnie, inaczej niż zwykle.

W takiej sytuacji powinniśmy się rozejrzeć i sprawdzić co się zmieniło, bo często to widać.

1. Komputer działa wolniej

Uwaga! Spowolnienie musi być gwałtowne!

Komputer spowalnia podczas pracy i jest to normalne, jeśli używamy komputera rok, dwa, trzy to naturalnie go zaśmiecamy i musi zwolnić o 10-20%.

Jeśli złapiemy wirusa, to komputer potrafi zwolnić o 90% z dnia na dzień. Wtedy wiemy, że coś jest nie tak.

Zwykle jakiś proces „podkrada” moc obliczeniową komputera.

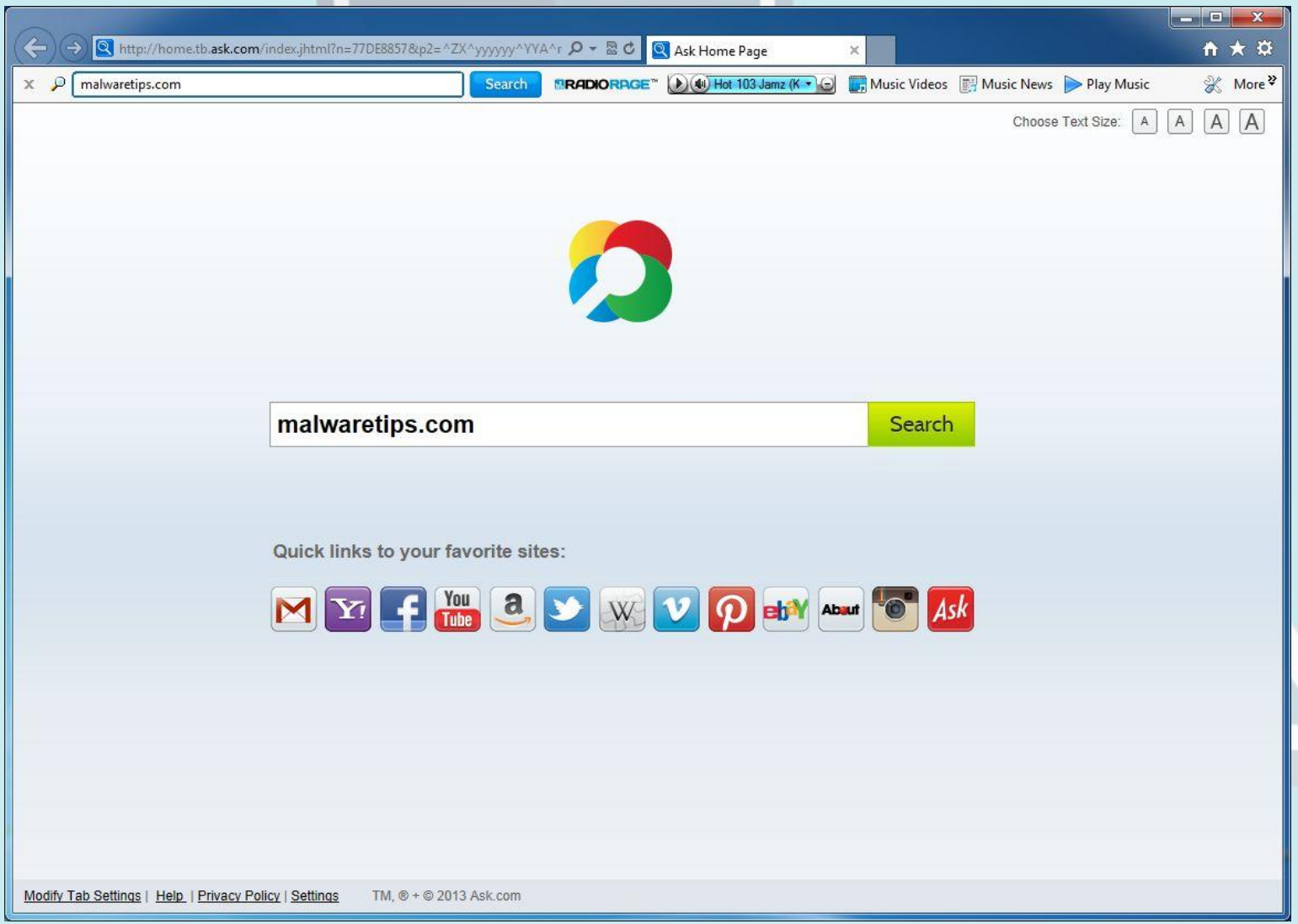
2. Problem z przeglądarką

Czasem przeglądarka zaczyna być „dziwna”.

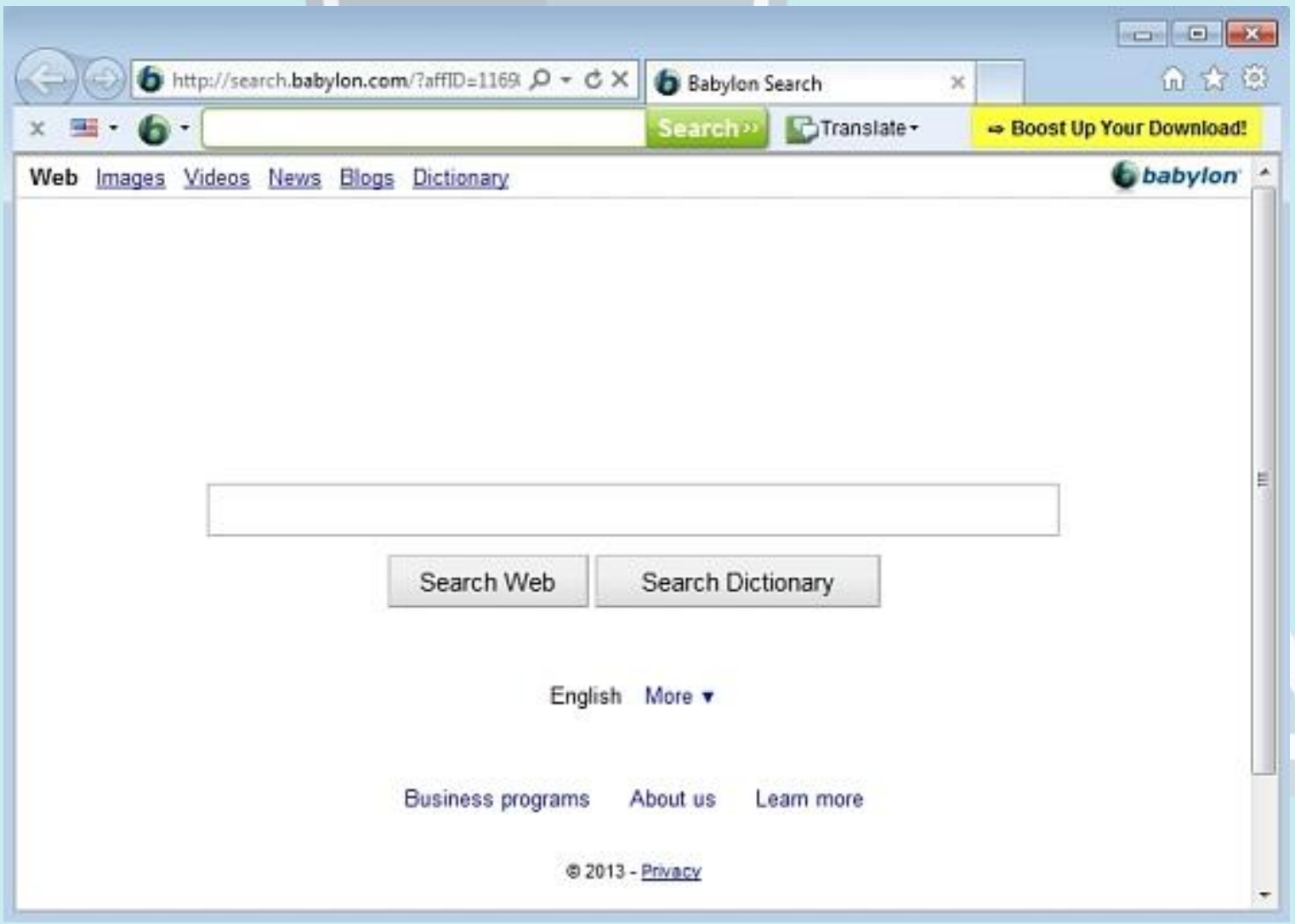
Zmienia się strona startowa oraz pojawia się dodatkowy pasek z wyszukiwarką i ikonami.

Może to świadczyć o infekcji typu adware, czyli zamiast stron internetowych zobaczymy mnóstwo reklam. Najpopularniejsze złośliwe programy to tb.ask, babylon oraz snap-do.

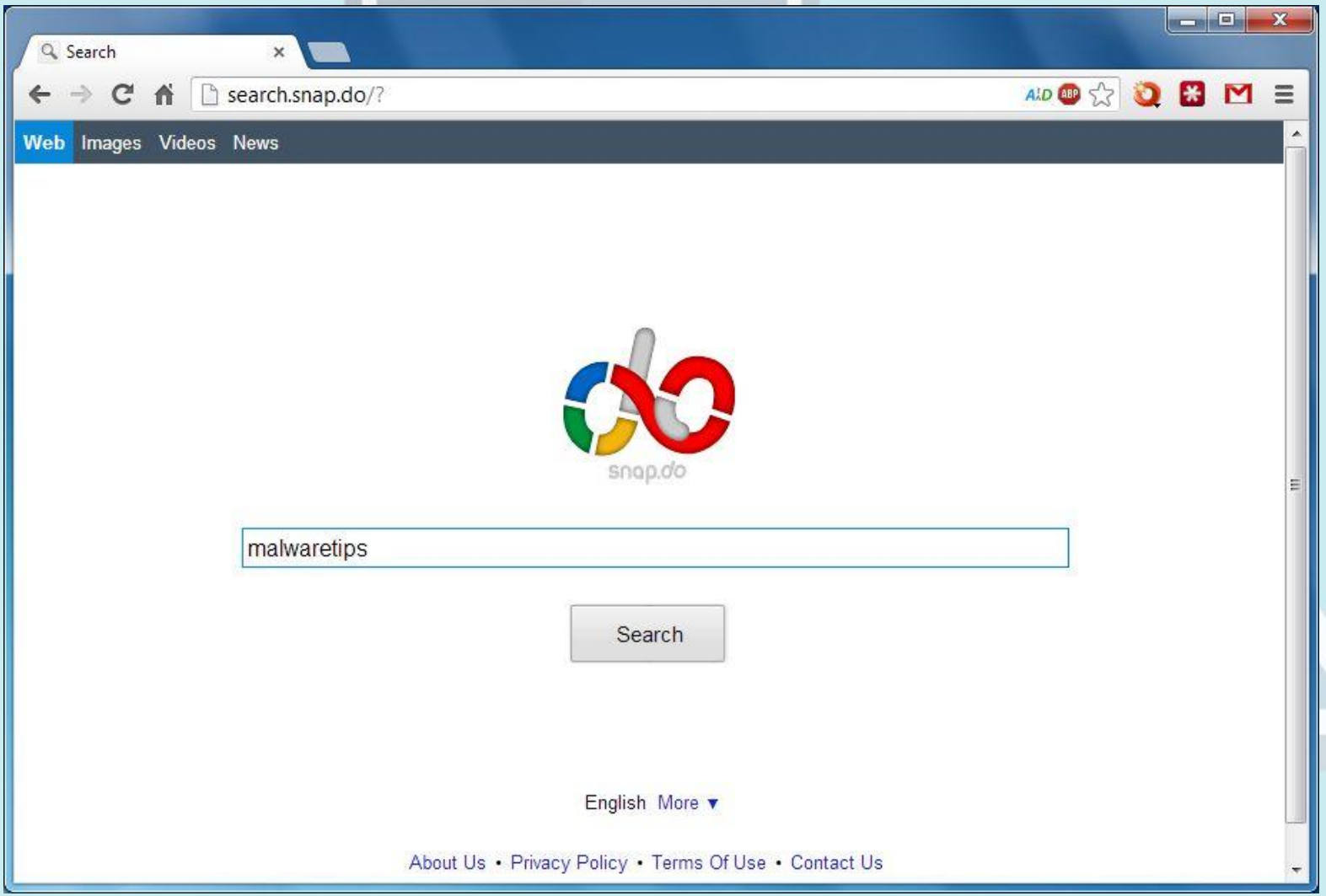
tb.ask.com


http://home.tb.ask.com/index.jhtml?n=77DE8857&p2=^ZX^yyyyyy^YYA^r
Ask Home Page
malwaretips.com
Search
RADIORAGE
Hot 103 Jamz (K
Music Videos
Music News
Play Music
More
Choose Text Size:
A
A
A
A
malwaretips.com
Search
Quick links to your favorite sites:
Modify Tab Settings | Help | Privacy Policy | Settings
TM, ® + © 2013 Ask.com

search.babylon.com



search.snap.do



3. Dziwne komunikaty

Zwykle bywają dopiero początkiem problemów.

W trakcie przeglądania stron możemy natknąć się na złośliwy kod lub specjalne reklamy, które mają nas nastraszyć.

Prawdziwe kłopoty zaczną się jeśli klikniemy na reklamę i pobierzemy fałszywy program antywirusowy.

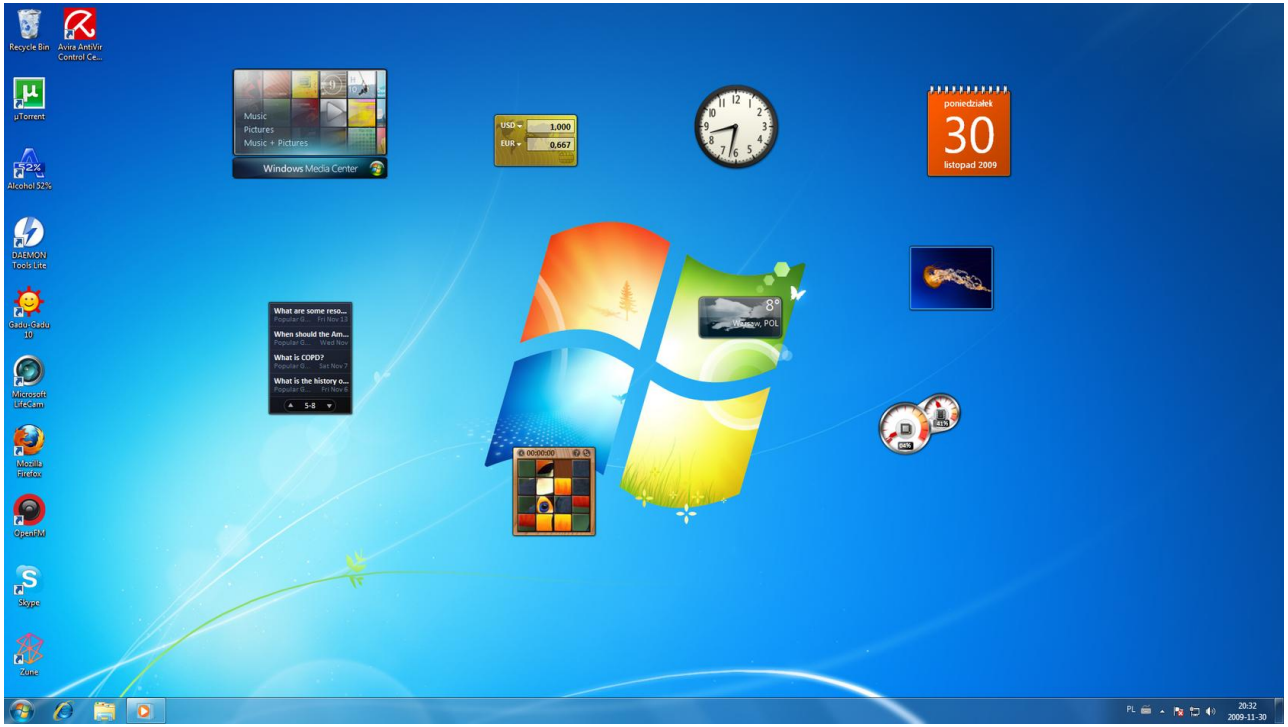
Zagrożenie wirusem typu spyware

Czasem błąd jest mniej zauważalny

4. Nowe ikony na pulpicie

Czasem na pulpicie może pojawić się coś nowego.

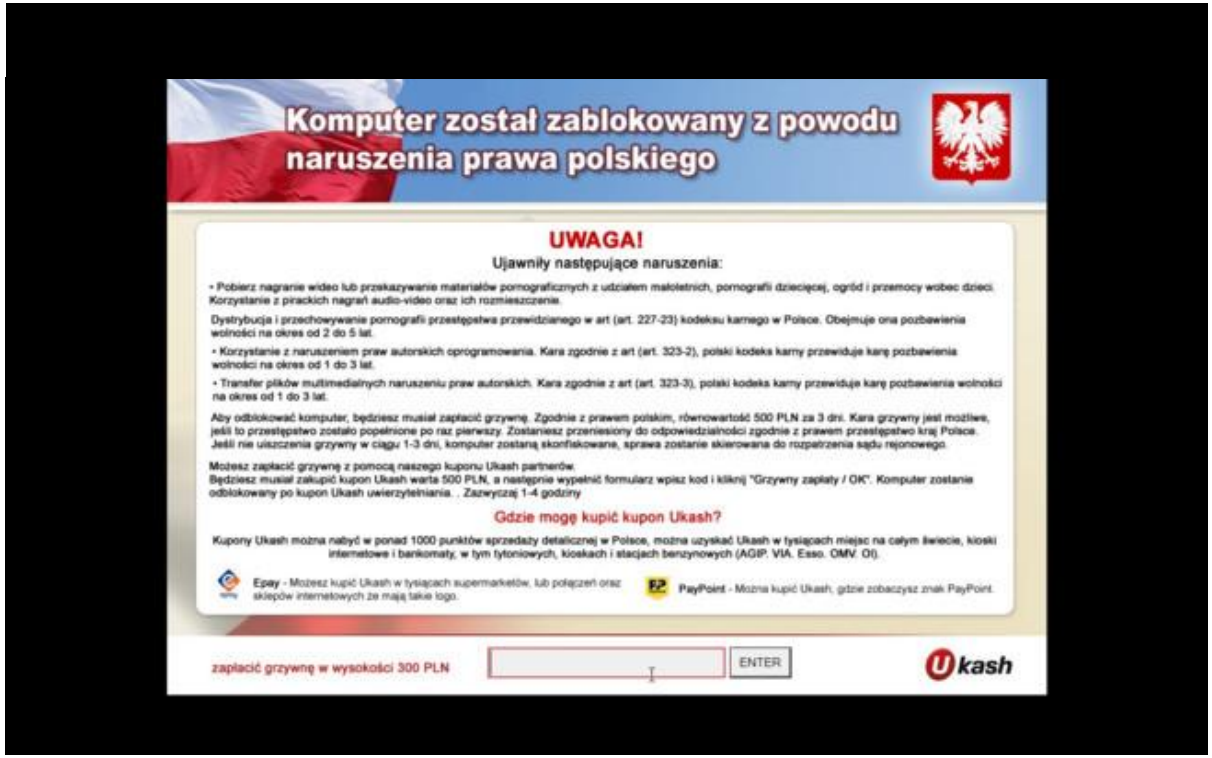
Być może na pulpicie pojawiły się nowe ikony lub elementy graficzne. Warto się zainteresować, czy to przypadkiem nie jest wirus.



5. Zablokowany komputer

Niektóre wirusy blokują nam komputer.

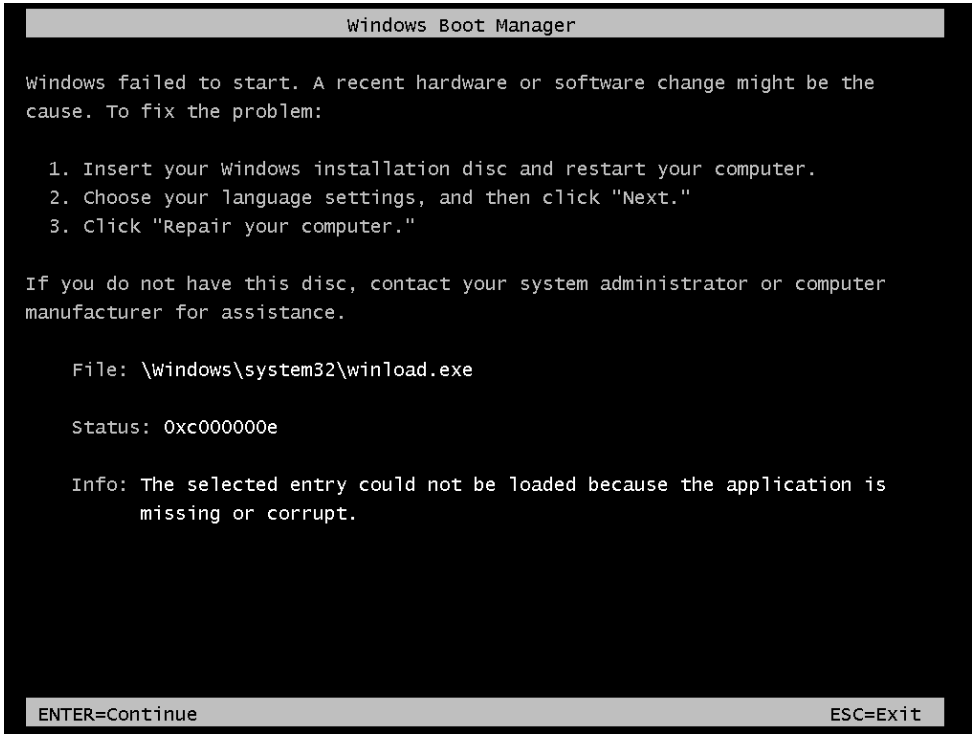
Jeśli nie możemy zalogować się do swojego konta, czy nie mamy dostępu do pulpitu, to wyraźny znak, że mamy kłopot z infekcją.



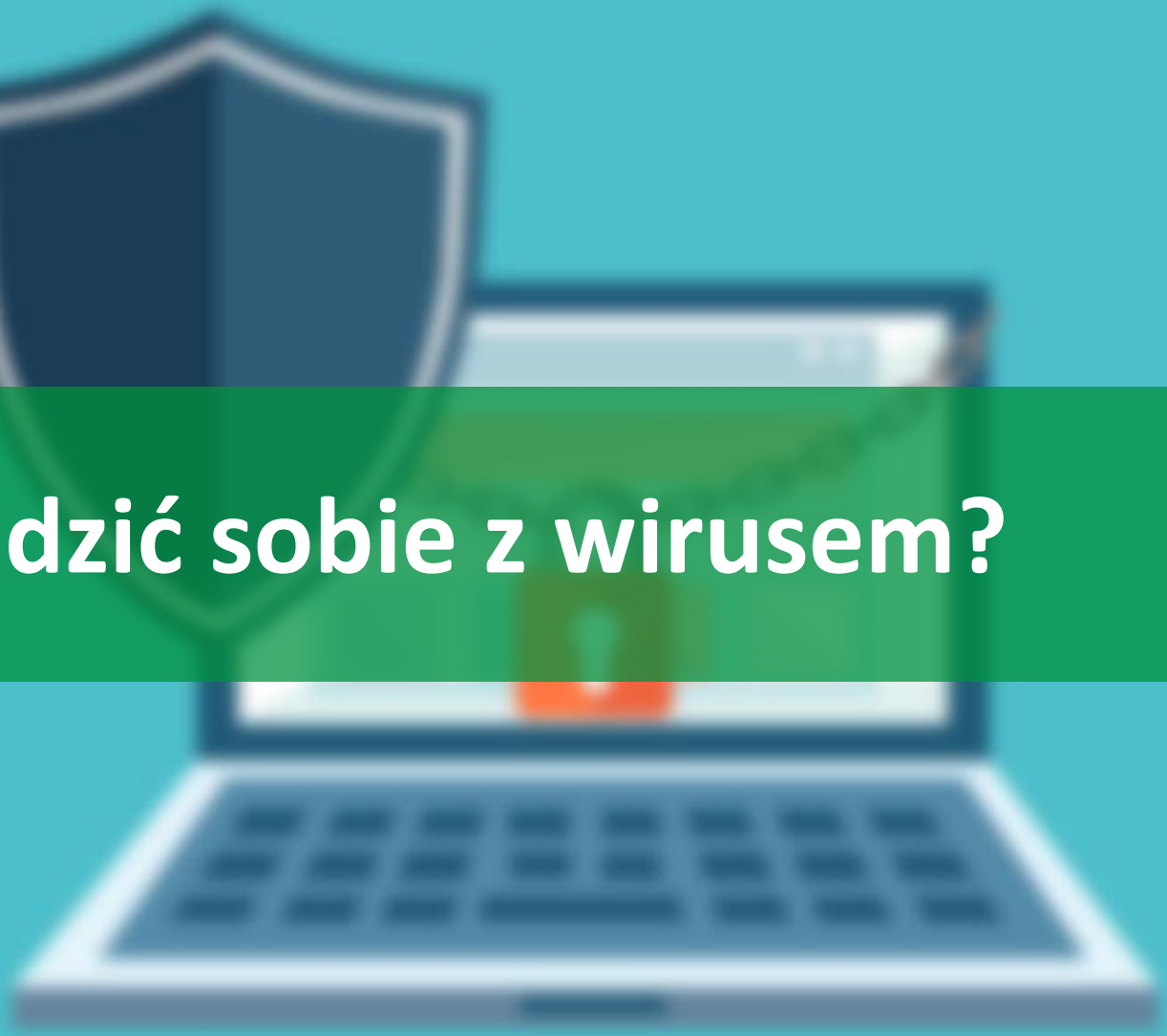
6. Komputer się nie włącza

Tego objawu nie da się przeoczyć.

Jeśli komputer się nie uruchamia to może być to wirus lub wiele innych czynników od uszkodzeń systemu, bo usterki mechaniczne.



Jak poradzić sobie z wirusem?



Po pierwsze musimy go wykryć

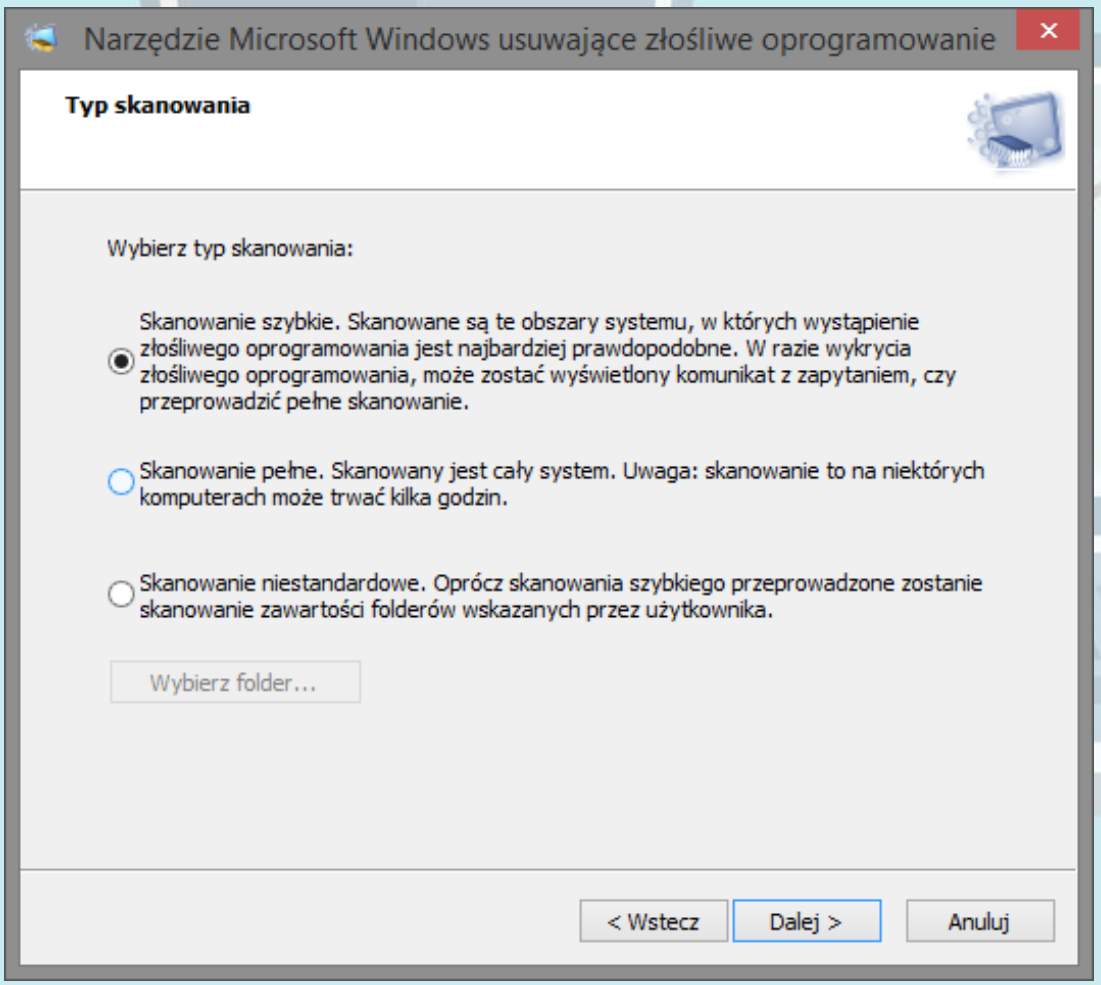
Ciężko walczyć z przeciwnikiem którego nie znamy.

Podstawowe narzędzia do walki z wirusami mamy wbudowane w system. Są do wcześniej wspomniany **Windows Defender** oraz **Narzędzie do usuwania złośliwego oprogramowania**.

Zaczynamy od **Narzędzie do usuwania złośliwego oprogramowani**, czyli uruchamiamy mrt.exe (Malicious Removal Tool). Możemy przeprowadzić szybkie skanowanie, trwa około 5 minut. Jeśli coś wykryje wykonujemy pełny skan, który może zająć już ponad godzinę.

MRT w akcji

Start > Uruchom > mrt.exe lub Start > Wyszukaj > mrt.exe



Co dalej?

MRT nic nie wykryło, a problem jest nadal.

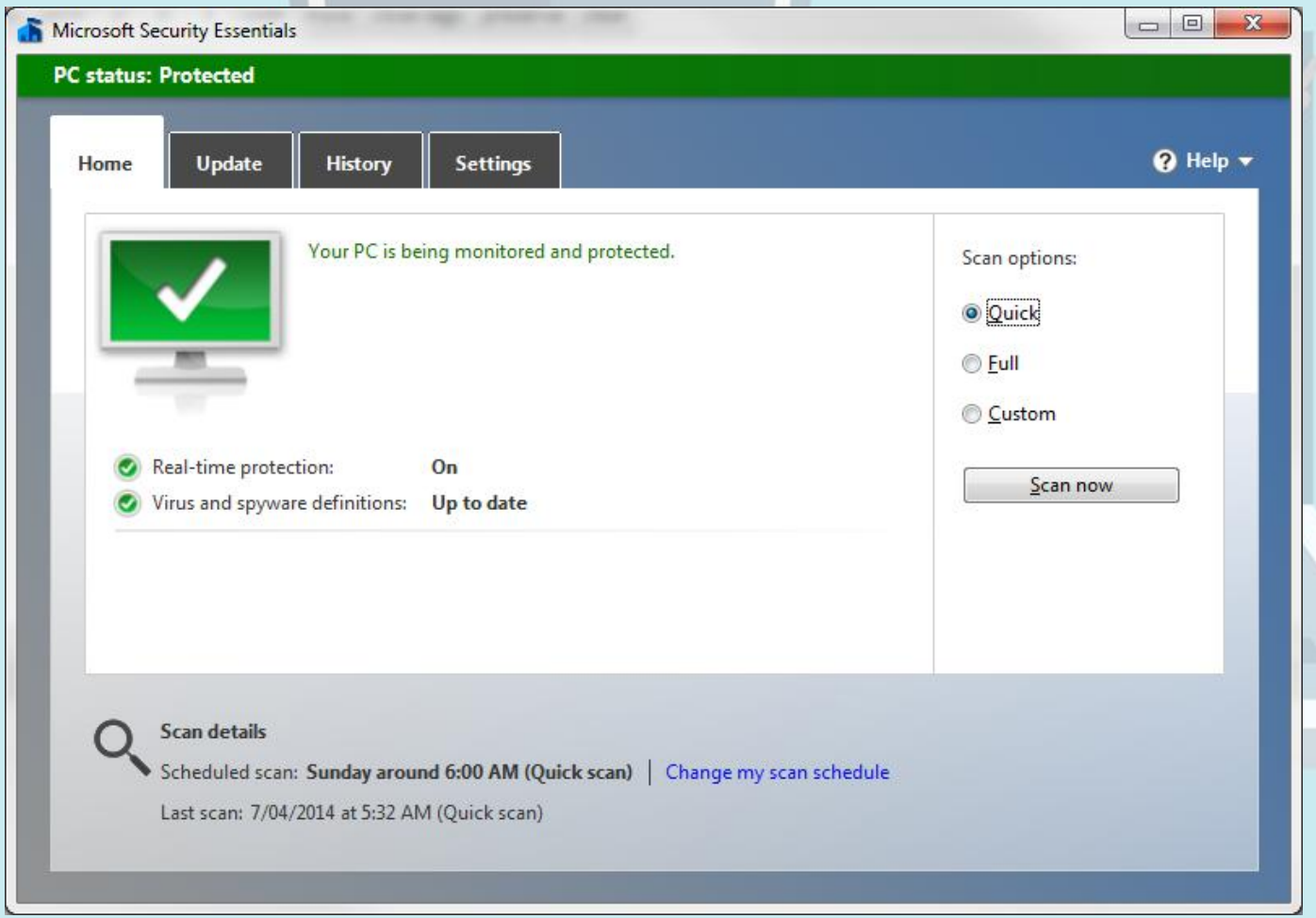
Po drugie uruchamiamy Windows Defender lub inny program antywirusowy jaki mamy zainstalowany i wybieramy „szybkie skanowani”.

Możemy też wybrać dodatkowe skanowanie uruchomionych aplikacji lub sektora rozruchowego.

Standardowo, jeśli wykryto zagrożenie to usuwamy zainfekowane pliki i ponawiamy skanowanie tym razem z opcją „skanowanie standardowe” lub „skanowanie pełne”.

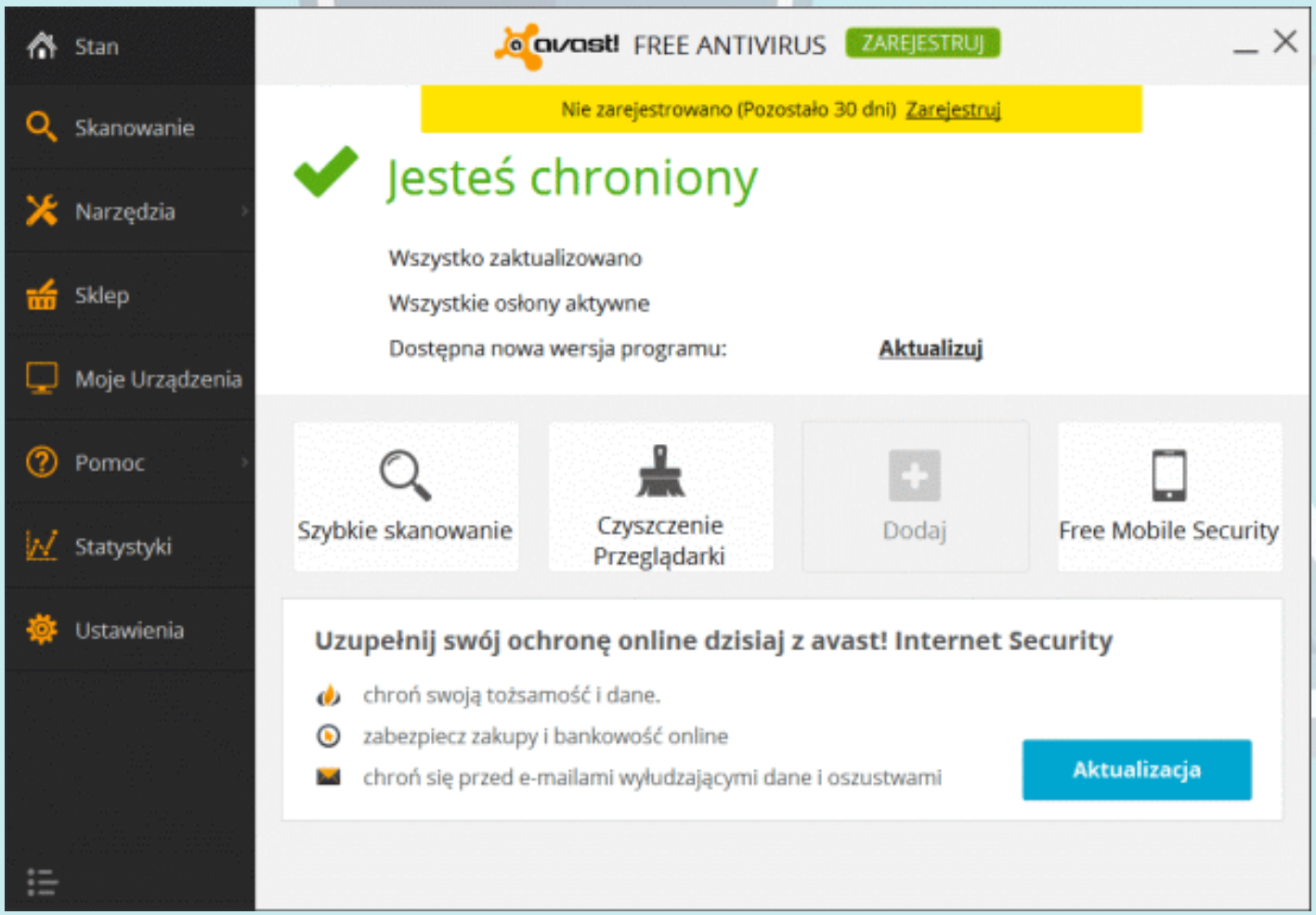
Windows Defender

Skanowanie za pomocą Microsoft Security Essentials



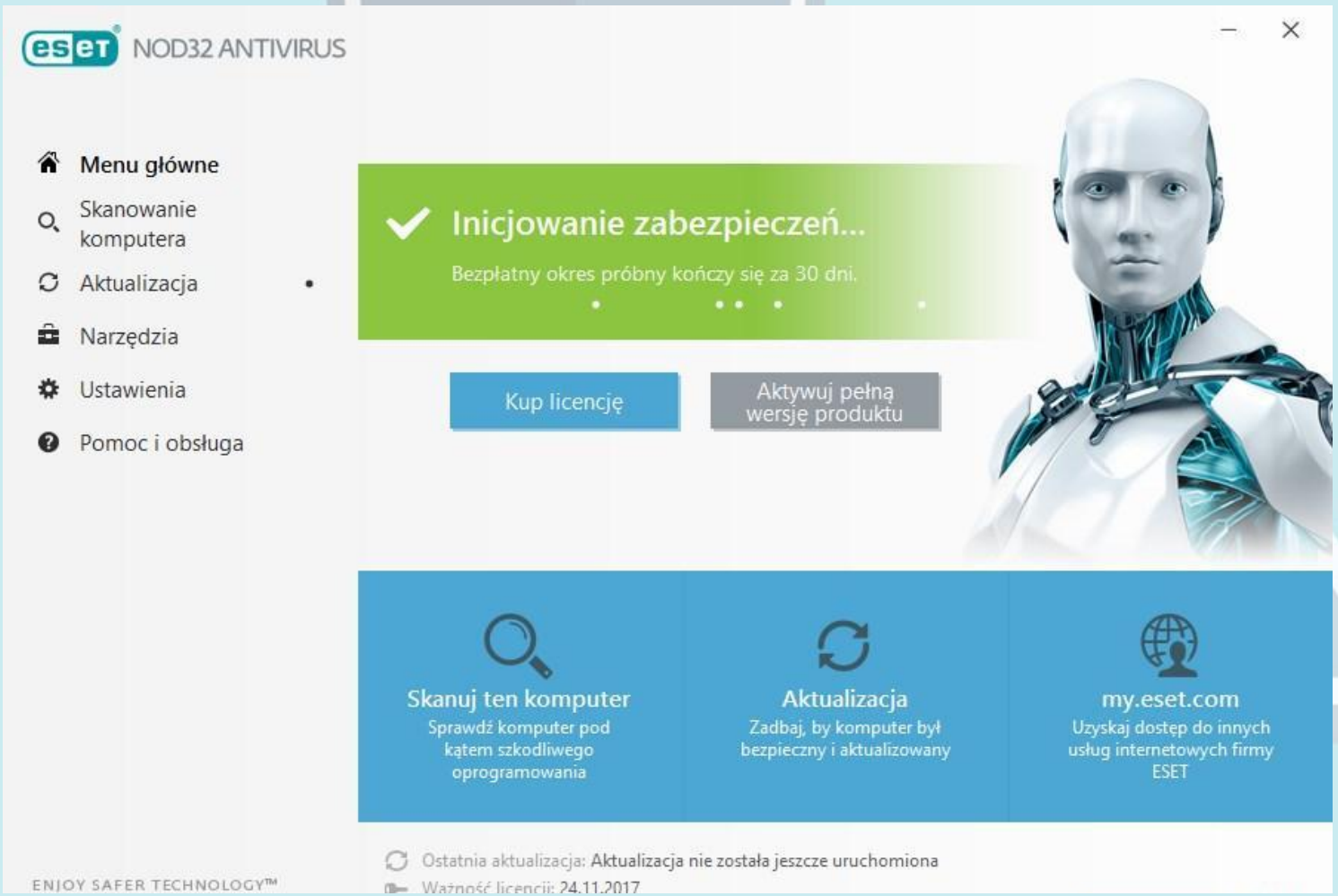
Avast! Free Antivirus

Skanowanie za pomocą Avasta!



ESET NOD32 Antivirus 11

Skanowanie za pomocą ESET-a.



A jeśli dalej mamy problem?

Możemy skorzystać ze skanera Online.

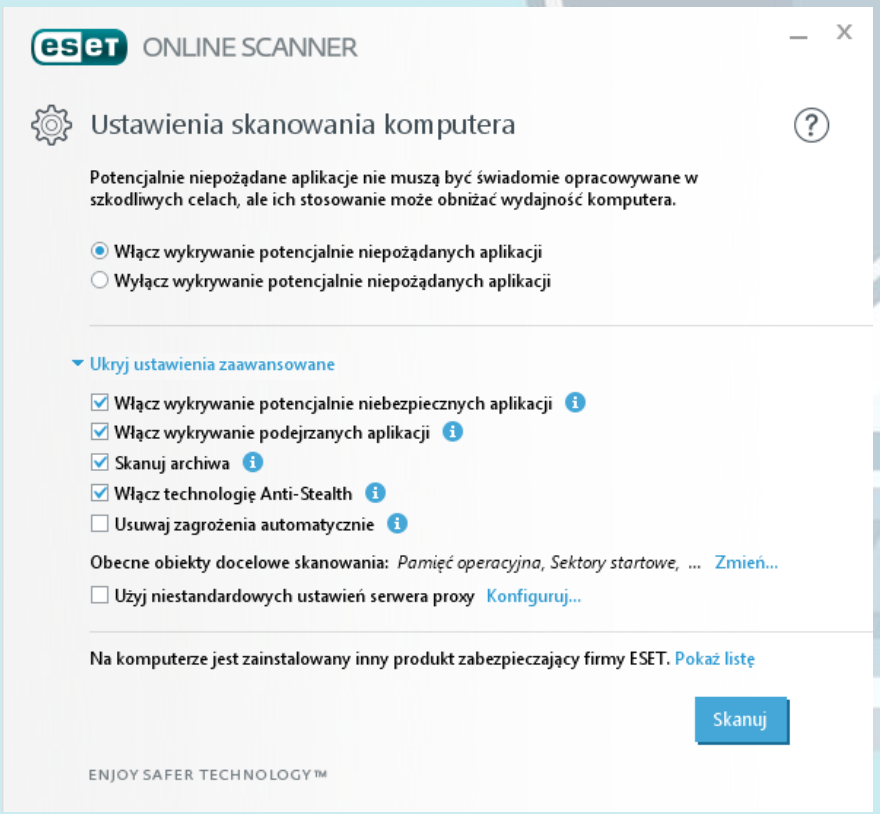
Jeżeli powyższe działania nie pomogły to zawsze można użyć zewnętrznego programu do skanowania komputera.

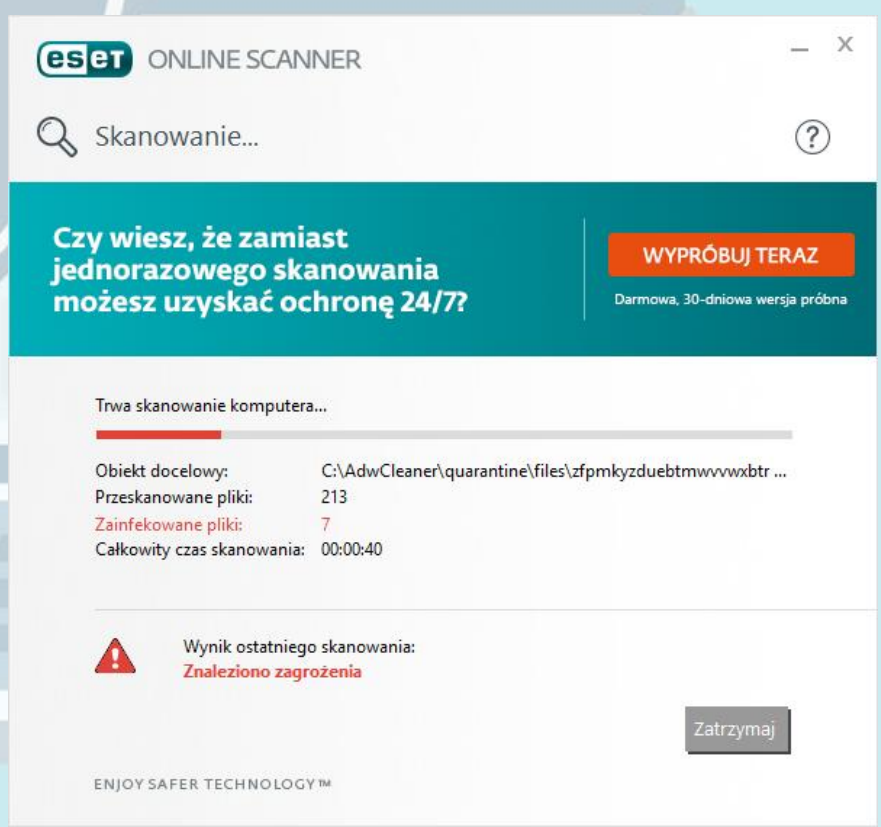
Polecam ESET Online Scanner, jest to bardzo skuteczny skaner, który nie wymaga instalacji ani konfiguracji. Do tego jest darmowy.

Wystarczy go pobrać ze strony ESET.pl > Pobierz > Dodatkowe narzędzia. Czerwony przycisk „Skanuj teraz”. Dla ułatwienia – kliknij, aby pobrać

ESET Online Scanner

Ustawiamy skanowanie według poniższego wzoru.





Szkodliwe i niepotrzebne programy

Programy typu crapware

Czy wszystkie programy są potrzebne?

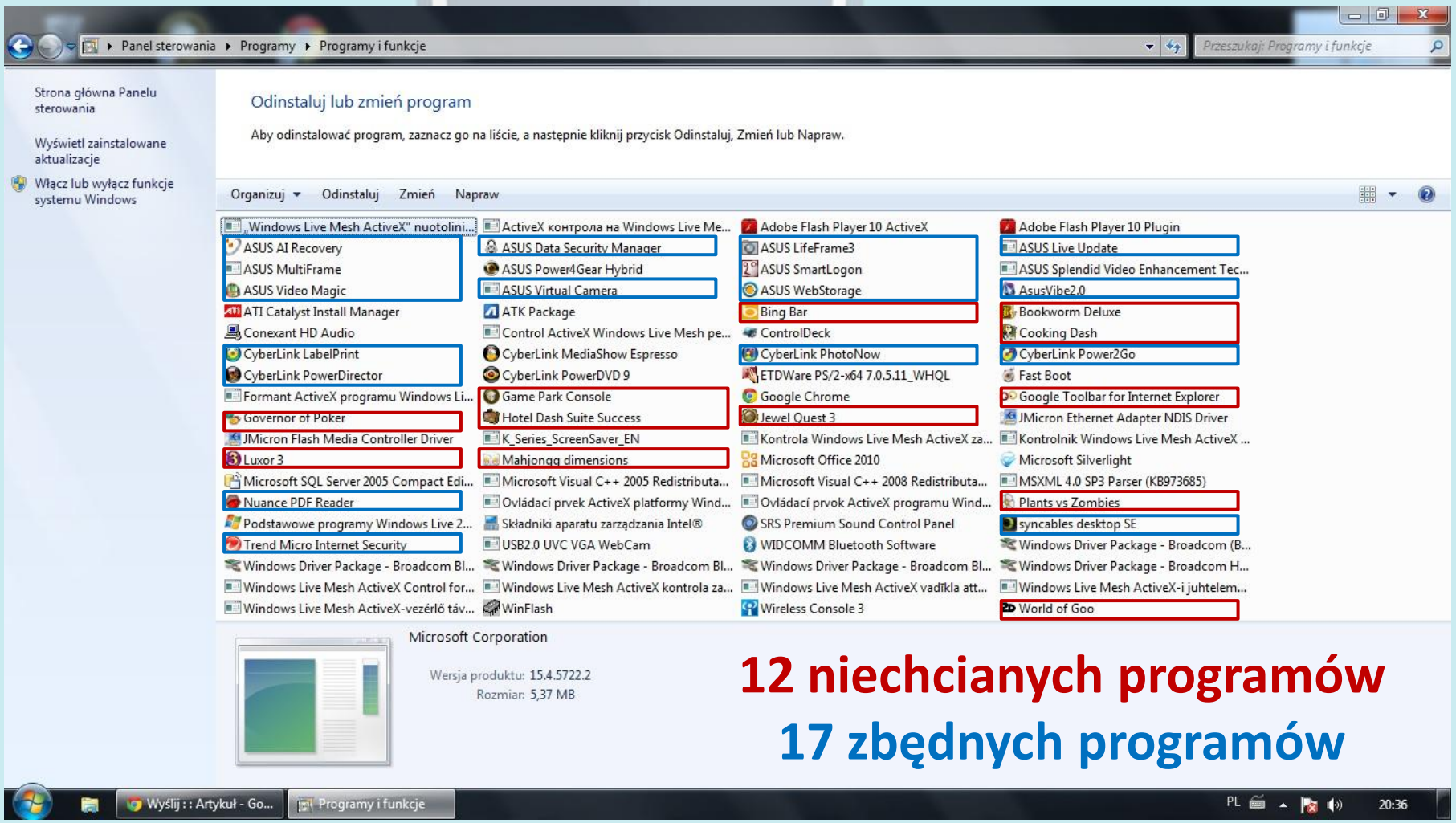
Może się zdarzyć tak, że na naszym komputerze pojawią się programy nie do końca potrzebne, albo wręcz szkodliwe i zaśmiecające nasz dysk.

Crapware, to grupa programów niechcianych przez użytkowników lub preinstalowanych przez producentów sprzętu.

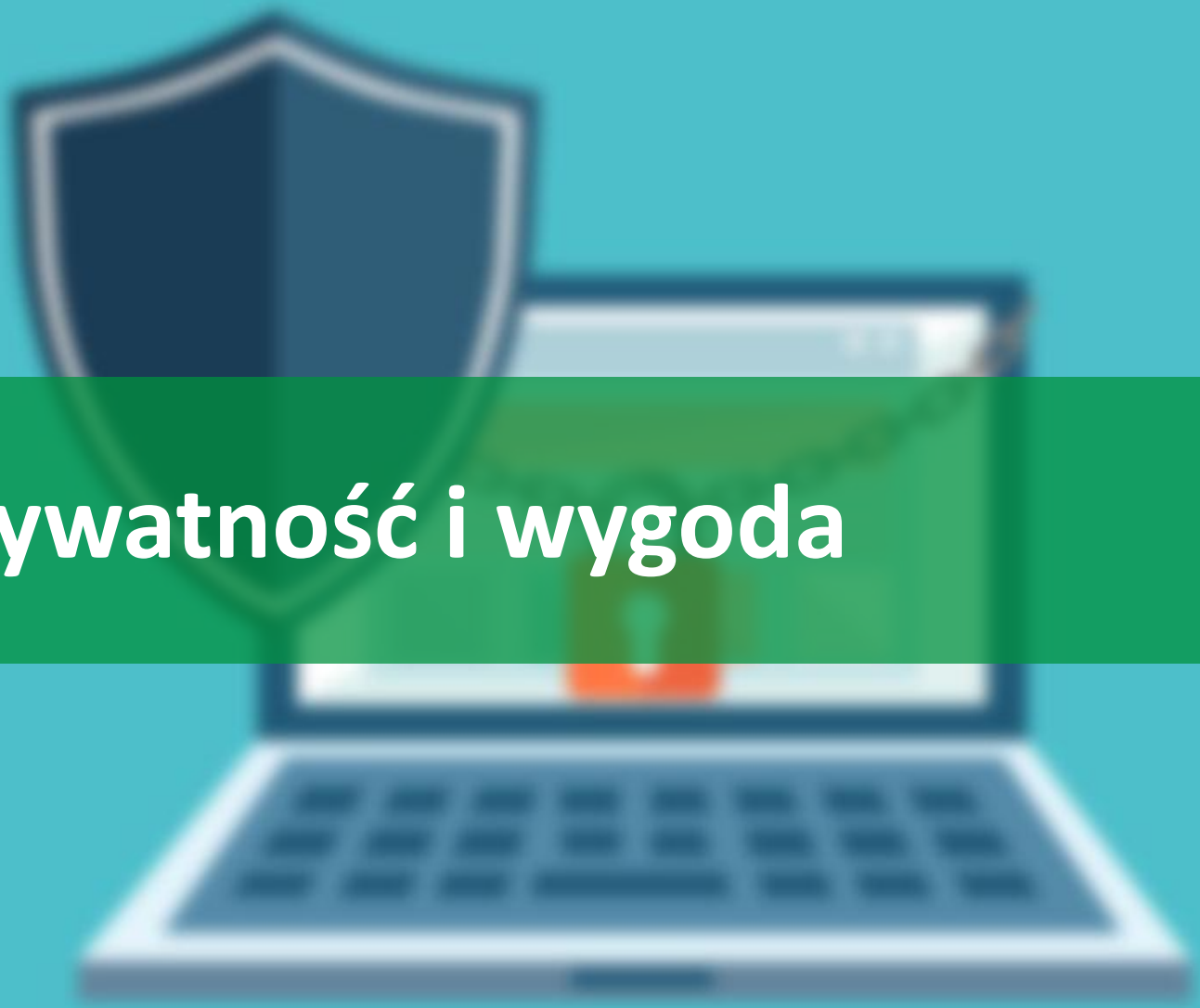
Takimi programami są np. narzędzia użytkowe dodawane przez producentów laptopów, gry, wersje demonstracyjne programów biurowych itp.

Zainstalowane programy

Panel sterowania > Programy > Programy i funkcje



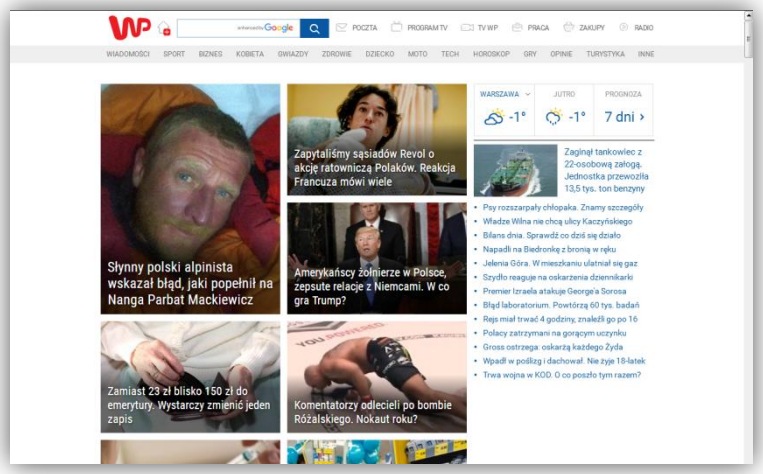
Prywatność i wygoda



Wszechobecne reklamy

Czy da się przeglądać Internet bez reklam?

Korzystając ze strona WWW zawsze musimy oglądać setki reklam, filmików i innej niechcianej treści. Co ciekawe reklamy takie są tworzone w oparciu o dane, które pochodzą z mediów społecznościowych i innych portali. Na szczęście da się coś na to poradzić.



uBlock Origin

Czyli sposób na reklamy

Blokowanie uciążliwych reklam w przeglądarkach.

Dla Chrome – Pobierz

Dla Firefox – Pobierz

Dla Opera – Pobierz

Przyspiesza wczytywanie stron, sprawia, że są bardziej czytelne.


DZIĘKUJĘ ZA UWAGĘ
I DO ZOBACZENIA
ZA TYDZIEŃ
KONIEC