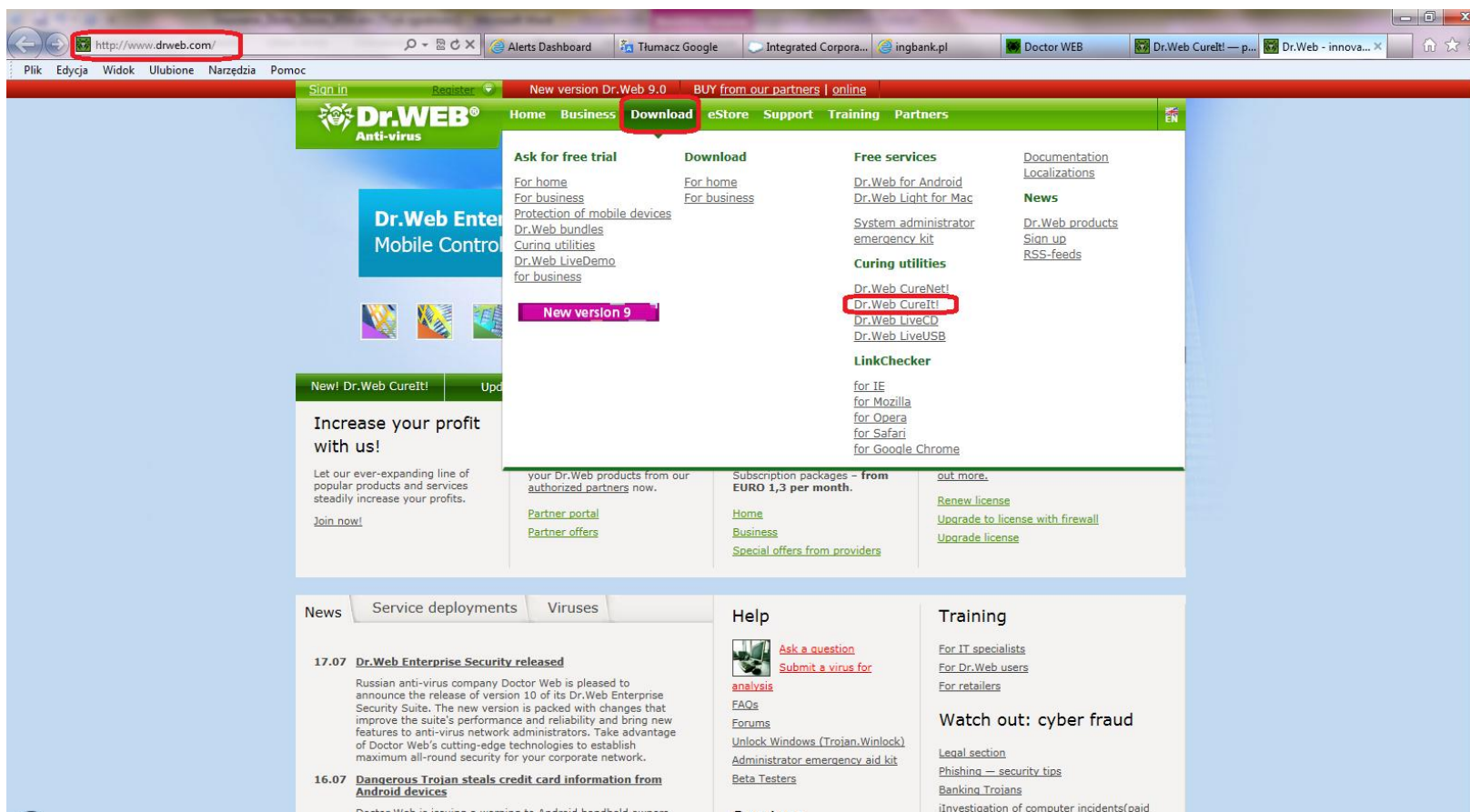


Usuwanie Trojana Zbot/Zeus/Panda

Skąd pobrać program Dr.Web CureIt?

Należy wejść na stronę <http://www.drweb.com/> i wybrać zakładkę „Download” i program Dr.Web CureIt



The screenshot shows the Dr.Web website interface. The browser's address bar is highlighted with a red box, containing the URL <http://www.drweb.com/>. The website's navigation menu includes 'Home', 'Business', 'Download', 'eStore', 'Support', 'Training', and 'Partners'. The 'Download' menu is expanded, showing options for 'Ask for free trial', 'Download' (with sub-links for home, business, and mobile devices), 'Free services', 'Documentation', 'Localization', 'News', 'Curing utilities', and 'LinkChecker'. The 'Dr.Web CureIt!' link under 'Curing utilities' is highlighted with a red box. Below the navigation menu, there are sections for 'New! Dr.Web CureIt!', 'Increase your profit with us!', 'Subscription packages', and 'Help'. The 'Help' section includes links for 'Ask a question', 'Submit a virus for analysis', 'FAQs', 'Forums', 'Unlock Windows (Trojan.Winlock)', 'Administrator emergency aid kit', and 'Beta Testers'. The 'Training' section includes links for 'For IT specialists', 'For Dr.Web users', and 'For retailers'. The 'Watch out: cyber fraud' section includes links for 'Legal section', 'Phishing — security tips', 'Banking Trojans', and 'Investigation of computer incidents(paid)'.

Po wybraniu tego programu następuje przejście na stronę <http://www.freedrweb.com/cureit/>
 Na podanej znajduje się dokładny opis jak przeskanować nasz komputer.

The screenshot shows the Dr.Web CureIt! website interface. At the top, there's a navigation bar with links for 'Dr.Web CureIt! Nowy!', 'Dr.Web LiveCD', 'Dr.Web LinkChecker', and 'Dr.Web dla Android Light'. Below this, there are several icons representing different features: 'Demo', 'Kup pełną wersję', 'Zestaw pierwszej pomocy administratora systemu', 'Skorzystaj dzięki naszej ofercie', 'Opinie ekspertów', 'Dla stron internetowych', and 'Fora'. The main content area is divided into several sections: 'Dr.Web CureIt! Korzyści', 'Umowa Licencyjna', 'Wersja komercyjna', 'Kup', 'Jak korzystać?', 'Dr.Web CureIt!: statystyki', 'Praca z wierszem poleceń', 'Aktualizacja', 'Obsługiwane języki', and 'Historia projektu'. A prominent warning states: 'Bezpłatne użytkowanie programu Dr.Web CureIt! do celów biznesowych jest nielegalne. Umowa licencyjna'. Below this, there's a section titled 'Czy na Twoim komputerze jest zainstalowane oprogramowanie antywirusowe, ale mimo to wątpisz w jego skuteczność?' with instructions on how to use the software. A small window at the bottom shows the Dr.Web CureIt! interface with a scan option.

Na końcu strony zamieszczona jest ikonka pozwalająca na pobranie programu.

The screenshot shows a web browser window with the URL <http://www.freedrweb.com/cureit/>. The page displays a scan result: "Skanowanie zostało zakończone" (Scanning completed) with a green checkmark and the message "Nie wykryto zagrożen" (No threats detected). It also shows "Liczba sprawdzonych obiektów: 34741" and "Czas skanowania: 00:15:41". Below this is a table with columns: Nazwa pliku, Zagrożenie, Akcja, Ścieżka. At the bottom of the scan result area, there is a banner for "Beta Dr.WEB for Android" with features like "Anti-virus", "Anti-spam", and "New! CloudChecker".

Below the scan result, there are two main buttons:

- Pobierz za darmo** (Download for free) - "Dla komputerów domowych" (For home computers). This button is highlighted with a red border.
- Zakup licencji** (Purchase license) - "Dla komputerów biurowych albo komputerów klientów" (For office computers or client computers).

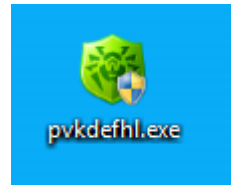
Below these buttons is a link for [Dokumentacja](#) (Documentation). At the bottom right, there is a search bar labeled "Szukaj" with a magnifying glass icon.

At the bottom left, there is a copyright notice: © Doctor Web 2003 — 2014.

At the bottom center, there is a paragraph of text: "Doctor Web to rosyjski dostawca rozwiązań z zakresu bezpieczeństwa informatycznego. Oprogramowanie antywirusowe Dr.Web jest rozwijane od 1992 r. Doctor Web – lider rosyjskiego rynku usług w dziedzinie bezpieczeństwa informatycznego – był pierwszym dostawcą, który zaoferował w Rosji ochronę antywirusową w formie usługi. Firma oferuje również sprawdzone rozwiązania antywirusowe i antyspamowe dla firm, urzędów i do użytku prywatnego. Mamy solidne doświadczenie w dziedzinie wykrywania szkodliwych programów oraz przestrzegamy wszystkich międzynarodowych standardów bezpieczeństwa. Doctor Web otrzymał wiele certyfikatów i nagród. Zadowoleni klienci na całym świecie to najlepszy dowód zaufania, jakie pokładają oni w nasze produkty."

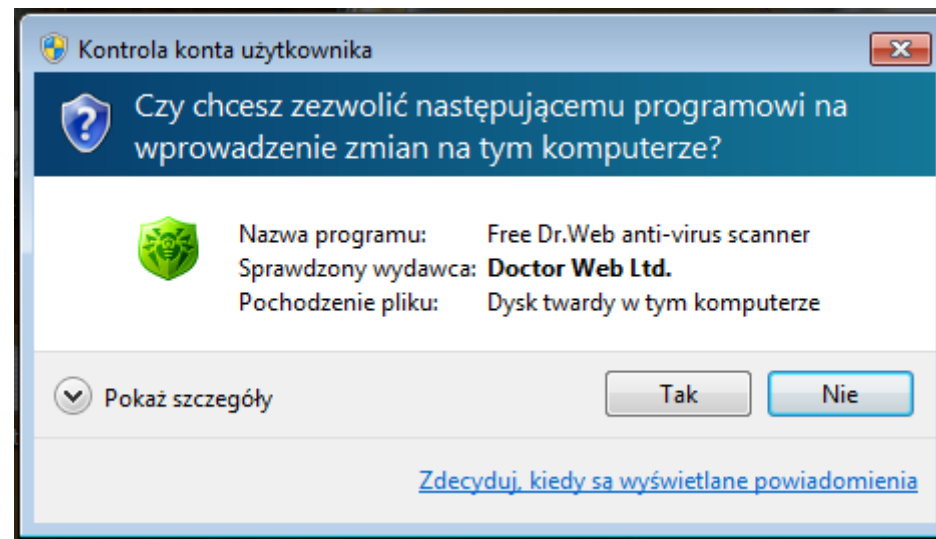
At the bottom right, there is a section titled "Więcej zasobów WWW:" (More WWW resources) with links to www.drweb.com (official company website) and www.av-desk.com (Dr.Web AV-Desk website).

Po zaakceptowaniu umowy licencyjnej należy zapisać pobrany plik (np. na pulpicie). Nazwa programu może być różna. Poniżej przykład



Jak zainstalować program i usunąć Trojana?

Program nie wymaga tradycyjnej instalacji. Wystarczy dwukrotnie nacisnąć lewy przycisk myszki na ikonie pobranego programu Aby rozpocząć skanowanie komputera. Żeby skorzystać z wersji darmowej należy zgodzić się na udział w poprawie jakości oprogramowania.



Nazwa Trojana może być różna w zależności od firmy antywirusowej. Dr. Web Trojana Zbot nazywał **Trojan.PWS.Panda.xxx** gdzie **xxx** może przyjmować różne wartości w zależności od wersji Trojana np.: 31,102,106, 368, 5676, ...

Dr.Web CureIt! Skanowanie szybkie

Dr.Web CureIt! sprawdza komputer...

Godzina uruchomienia: 11:37:21 Sprawdzane obiekty: 1979
 Pozostało czasu: 00:05:53 Wykryte zagrożenia: 1
 Obiekt: C:\Windows\system32\d3d10core.dll

<input checked="" type="checkbox"/>	Nazwa pliku	Zagrożenie	Akcja	Ścieżka
<input checked="" type="checkbox"/>	igba.exe	Trojan.PWS.Panda.56...	Wylecz	\Device\HarddiskVolume2\Users\test\AppData\Local\Temp\Kiuxe\igba.exe

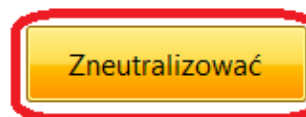
Gdy program wykryje Trojana poprosi o zgodę na Zneutralizowanie wykrytego zagrożenia. Należy wybrać akcję Usuń. Pliki z Trojanem mogą różnie się nazywać i znajdować się w innym miejscu niż na przedstawionym rysunku.



Dr.Web CureIt! wykrył zagrożenia.

Zalecamy natychmiast zneutralizować wykryte zagrożenia. Dr.Web CureIt! przeprowadzi działania zgodnie z ustawieniami.

Wykryte zagrożenia: 1
Zneutralizowane zagrożenia: 0
Czas skanowania: 00:32:34
[Otwórz raport](#)



<input checked="" type="checkbox"/>	Nazwa pliku	Zagrożenie	Akcja	Ścieżka
<input checked="" type="checkbox"/>	igba.exe	Trojan.PWS.Panda.56...	Usuń	\Device\HarddiskVolume2\Users\test\AppData\Local\Temp\Kiuxe\igba.exe

Dodatkowo należy także skorzystać z drugiego programu przeznaczonego wyłącznie do wykrywania i usuwania Trojana Zbot. Programem tym jest ZbotKiller.exe firmy Kaspersky.

Skąd pobrać program ZbotKiller?

Plik należy pobrać ze strony firmy Kaspersky <http://support.kaspersky.com/pl/viruses/utility#zbotkiller>.

Można pobrać plik w formie zarchiwizowanej (plik wymaga rozpakowania) lub plik gotowy do uruchomienia.

Plik można zapisać na pulpicie.

Program możemy uruchomić poprzez dwukrotne naciśnięcie lewym przyciskiem myszki na ikonie programu „ZBotKiller.exe”. Wtedy program uruchamiany jest bez dodatkowych parametrów lub poprzez tryb tekstowy, gdzie możemy uruchomić program z dodatkowymi parametrami (na przykład tworząc log z wykonanego skanowania).

Program nie tylko usuwa Trojana, ale również pliki i procesy wykorzystywane przez Trojana.
Poniżej efekt skanowania Programem ZBotKiller.exe.

```

C:\Documents and Settings\Administrator\Pulpit\ZBotKiller.exe
Trojan-Spy.Win32.ZBot removing tool by Yury Parshin, Kaspersky Lab 2009
version 1.1 Mar 5 2009 12:17:31
Scanning Threads ...
Infected thread was killed in process winlogon.exe with PID 664
Infected thread was killed in process winlogon.exe with PID 664
Infected thread was killed in process svchost.exe with PID 880
Infected thread was killed in process svchost.exe with PID 880
Infected thread was killed in process svchost.exe with PID 880
Infected thread was killed in process svchost.exe with PID 880
Infected thread was killed in process svchost.exe with PID 880
Infected thread was killed in process svchost.exe with PID 880
Infected thread was killed in process svchost.exe with PID 880
Infected thread was killed in process svchost.exe with PID 880
Scanning Files ...
C:\WINDOWS\system32\twext.exe infected by Trojan-Spy.Win32.ZBot...deleted
C:\WINDOWS\system32\twain_32\local.ds infected by Trojan-Spy.Win32.ZBot...delete
d
C:\WINDOWS\system32\twain_32\user.ds infected by Trojan-Spy.Win32.ZBot...deleted
C:\Documents and Settings\LocalService\Dane aplikacji\twain_32\user.ds infected
by Trojan-Spy.Win32.ZBot...deleted
C:\Documents and Settings\NetworkService\Dane aplikacji\twain_32\user.ds infecte
d by Trojan-Spy.Win32.ZBot...deleted
Scanning Hooks ...
Scanning Mutexes ...
Evil mutex _7F4523E5_ killed
Evil mutex _64AD0625_ killed

Completed
Infected files: 5
Infected threads: 10
Hooked imports: 191
Killed mutexes: 2
Cured files: 5
Fixed registry keys: 1

Press any key to close utility...
  
```

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