1. Skąd mogę wiedzieć, czy mój komputer jest zainfekowany?

Istnieje zespół charakterystycznych objawów możliwej infekcji, jak ogólne spowolnienie pracy, "tajemnicze zniknięcia" plików i informacji, nieprawidłowe funkcjonowanie urządzeń peryferyjnych, stałe wysyłanie danych podczas bezczynności etc. Jednak nie wszystkie wirusy dają o sobie znać już w chwili infekcji, ale czekają na spełnienie określonych warunków na przykład wystąpienia konkretnej daty, czy uruchomienie programu, by się aktywować.

Najprostszym, niestety nie zawsze skutecznym sposobem sprawdzenia, czy doszło do infekcji jest przeskanowanie całego systemu za pomocą programu antywirusowego.

{jcomments on}

2. Co mogę zrobić, aby ochronić się przed wirusami?

Obecnie głównym źródłem infekcji jest sieć Internet i sieci komputerowe. Dzieje się tak z powodu możliwości bardzo szybkiej wymiany informacji, jakie stwarzają sieci (e-mail, przeglądanie stron WWW, pobieranie plików, czaty, grupy dyskusyjne, sieci peer-to-peer etc). Tradycyjne źródła infekcji takie jak płyty CD, dyskietki itp. mają obecnie drugorzędne znaczenie.

Najlepszym rozwiązaniem, które pozwoli uniknąć infekcji jest instalacja dobrego programu antywirusowego z codzienną, najlepiej automatyczną aktualizacją bazy danych wirusów i łatwo dostępną, kompetentną pomocą techniczną. Koniecznie należy też na bieżąco pobierać wszystkie zalecane aktualizacje systemu operacyjnego, przeglądarki internetowej, czy programu pocztowego. Jeśli podłączysz swój komputer do Internetu, nie wyposażając go wcześniej w specjalistyczne oprogramowanie, a zainstalowane programy nie będą "załatane", możesz spodziewać się, że wirus wkradnie się do Twojego komputera w ciągu 20 pierwszych minut od połączenia. Istnieją bowiem pewne typy wirusów, które mogą zainfekować komputer bez konieczności uruchamiania załącznika, ale podczas otwierania wiadomości email, gdyż szkodnik uruchamia się automatycznie w tzw. okienku "atopodglądu". Inne uruchamiają się automatycznie podczas przeglądania zainfekowanych stron WWW lub bezpośrednio przez otwarte porty na komputerze podłączonym do sieci. Jest jednak to możliwe jedynie wówczas, gdy użytkownik nie pobiera krytycznych aktualizacji systemu operacyjnego, przeglądarki internetowej, czy programu pocztowego.

Zaleca się również pogłębianie swojej wiedzy o tym, w jaki sposób wirusy rozprzestrzeniają się i infekują komputery. Pozwoli to uniknąć ryzykownych zachowań takich jak: otwieranie e-maili z nieznanych źródeł, otwieranie podejrzanych plików i stron WWW, groźnych załączników, pobieranie plików z niepewnych stron internetowych.

3. Jak mogę odróżnić hoax (fałszywy alarm) od prawdziwego wirusa?

Najlepiej korzystać z programu antywirusowego. Hoaxy nie są wirusami i nie wykonują żadnych destrukcyjnych działań na komputerze. Hoax to wiadomość informująca o wirusie (nie istniejącym), którego nie mogą zlokalizować programy antywirusowe - zwykle są to złośliwe żarty. Oprócz hoaxów istnieje jeszcze grupa programów określanych jako jokes, które symulują destrukcyjne działania, a w rzeczywistości nie wyrządzają żadnych szkód.

Jeśli otrzymasz hoaxa zastosuj się do poniższych instrukcji:
Nie zwracaj żadnej uwagi na treść wiadomości.
Nie przesyłaj tej wiadomości do nikogo.
Nie wykonuj żadnych instrukcji zawartych w tej wiadomości (kasowanie wskazanych w treści plików może doprowadzić do uszkodzenia systemu).
Usuń tę wiadomość.
Warto także skontaktować się z nadawcą i poinformować go, że alarm jest fałszywy.
W razie wątpliwości zanim cokolwiek zrobisz, zadzwoń na PogotoVie AntyVirusowe.

4. Co może zrobić wirus?

Wbrew obiegowej opinii, wirusy nie mogą bezpośrednio uszkodzić sprzętu komputerowego (CD_ROM, dyskietki, dyski, etc.). Również nie mogą, zarazić dysków zabezpieczonych przed zapisem (np. płyty CD - w trybie "tylko do odczytu") lub urządzeń w pobliżu komputera np. kart kredytowych.

A jednak efekty działania wirusów mogą być bardzo poważne, od całkowitego zniszczenia wszystkich informacji zapisanych w komputerze, do uruchamiania małych, dokuczliwych programów z niewielkimi lub w ogóle bez efektów destrukcyjnych. Inne programy z grupy złośliwych kodów (malware) mogą śledzić nasze zachowanie umożliwić kradzież danych (adresów e-mail, haseł do kont bankowych), włamanie na komputer, a nawet nabić nasz rachunek telefoniczny przekierowując połączenie modemowe na dodatkowo płatne numery. Szczególnie złośliwym działaniem jest wykorzystanie zainfekowanego komputera jako tzw. Zombie do przeprowadzenia ataku hakerskiego na określoną witrynę internetową. Dzieje się to bez świadomości ofiary, która staje się pierwszym podejrzanym.

Niebezpieczeństwo, jakie stwarza wirus wiąże się z dwoma rodzajami jego działań: szkodami, jakie wyrządzają w komputerze i prędkością rozprzestrzeniania się. Stąd groźniejszym wirusem jest ten, który oprócz uszkadzania danych szybko rozprzestrzenia się przez Internet niż ten, który np. usuwa dane, ale nie potrafi się powielać. Wiele wirusów pozbawionych procedur destrukcyjnych potrafi narobić wiele zamieszania przez sam proces rozprzestrzeniania się.

5. Co powinienem zrobić, gdy dostanę podejrzany e-mail?

To bardzo proste: nie otwierać go. Następnie przeskanować go dobrym zaktualizowanym programem antywirusowym i bez żalu pozwolić mu go skasować. W razie wątpliwości zanim cokolwiek zrobisz zadzwoń na PogotoVie AntyVirusowe.

Najczęściej wirus pojawia się na komputerze ofiary jako coś - całkowicie darmowego i wyjątkowego, bowiem w normalnej sytuacji kosztowałoby b. dużo (np. darmowe oprogramowanie, pliki mp3, czy bezpłatny dostęp do komercyjnych witryn, najczęściej pornograficznych...).

Jeśli więc w Twojej skrzynce pocztowej niespodziewanie znajdziesz coś:
1. wyjątkowego
2. darmowego
3. w dodatku czujesz, że musisz to mieć

UWAGA - istnieje duże prawdopodobieństwo, że do Twojego komputera próbuje zakraść się niebezpieczny wirus. Oczywiście, jest możliwe, że naprawdę Ci się poszczęściło, ale w 99 przypadkach na 100 - przykro nam, dostałeś wirusa.

Nie ufaj nikomu. To, że ufasz danej osobie, nie oznacza, że powinieneś również ufać plikowi, który do niej należy.

źródło>>>