

Przyjęło się nazywać wszystkie szkodniki wirusami, jednak w zależności od sposobu działania, rozpowszechniania i szkodliwości dzielimy je na kilka kategorii:

Robaki

Tego typu szkodliwe oprogramowanie do rozprzestrzeniania się wykorzystuje zasoby sieci. Klasa ta nazwana została robakami z powodu jej specyficznego działania przypominającego „pełzanie” z komputera na komputer przy użyciu sieci, poczty elektronicznej i innych kanałów informacyjnych. Dzięki temu tempo rozprzestrzeniania się robaków jest bardzo szybkie.

Robaki przedostają się do komputera, obliczają adresy sieciowe innych komputerów oraz wysyłają na te adresy swoje kopie. Poza adresami sieciowymi wykorzystują również dane z książki kontaktów klientów poczty. Przedstawiciele tego typu szkodliwego oprogramowania tworzą czasami pliki robocze na systemie dysków, ale nie mogą infekować zasobów komputera (z wyjątkiem pamięci operacyjnej).

Wirusy

Programy, które zarażają inne programy poprzez dodanie do nich kodu wirusa, w celu uzyskania dostępu do komputera przy uruchamianiu zainfekowanego pliku. Ta prosta definicja przedstawia podstawowe działanie wirusa - infekcję. Szybkość rozprzestrzeniania wirusów jest mniejsza niż robaków.

Trojany

Programy, które wykonują na zainfekowanych komputerach niekontrolowane przez użytkownika działania - w zależności od warunków mogą usuwać informacje z dysków, powodować stany bezczynności systemu, wykraść dane itp. Tego typu szkodliwe oprogramowanie w tradycyjnym rozumieniu nie jest wirusem (tzn. nie infekuje innych programów lub danych): trojany same z siebie nie mogą włamać się na komputer, ale są rozprzestrzeniane przez oszustów jako „pożyteczne” i niezbędne oprogramowanie. A jednak szkody spowodowane przez trojany są większe niż przez tradycyjne ataki wirusów.

Adware

Kod programu wbudowanego w oprogramowanie bez wiedzy użytkownika w celu wyświetlania reklam. Z reguły adware jest wbudowany w oprogramowanie, które jest dystrybuowane bezpłatnie. Reklama jest wyświetlana w interfejsie roboczym. Adware często gromadzi i przenosi prywatne dane użytkownika do dystrybutora tego zagrożenia.

Spyware

Jest to oprogramowanie, które pozwala na zbieranie danych na temat konkretnego użytkownika lub organizacji, która nie jest tego świadoma. Ofiara może nawet nie podejrzewać, że na jej komputerze znajduje się spyware. Z reguły celem tego szkodnika jest:

- Śledzenie działań wykonywanych na komputerze przez użytkownika.
- Gromadzenie informacji na temat zawartości dysków twardej, co często oznacza skanowanie niektórych folderów i rejestru systemu w celu utworzenia listy oprogramowania zainstalowanego na komputerze.
- Zbieranie informacji o jakości połączenia, sposobie podłączenia, prędkości modemu itp.

Riskware

To oprogramowanie nie jest wirusem, ale zawiera w sobie potencjalne zagrożenie. W niektórych warunkach obecność riskware na komputerze oznacza zagrożenie dla danych. Takimi programami mogą być te do zdalnego zarządzania, programy korzystające z połączenia Dial-Up oraz inne do łączenia ze stronami internetowymi pay-per-minute.

Żarty

Oprogramowanie, które nie wyrządza szkody na komputerze, ale wyświetla wiadomości, że szkodnik już spowodował uszkodzenie lub je spowoduje. Często ostrzega użytkownika o istniejącym niebezpieczeństwie, np. wyświetla komunikaty o formatowaniu dysku twardego (choć formatowanie nie jest wykonywane), wykrywa wirusy w nie zainfekowanych plikach itp.

Rootkity

Są to narzędzia wykorzystywane do ukrywania złośliwego działania. Ukrywane są przez złośliwe oprogramowanie, aby uniknąć wykrycia przez aplikacje antywirusowe. Rootkity mogą zmodyfikować system operacyjny oraz zmienić jego główne funkcje aby ukryć swoją obecność i działania wykonywane przez intruza na zainfekowanym komputerze.

Źródło: <https://support.kaspersky.com/pl/viruses/general/614>.