

Wirusy, konie trojańskie i inne zagrożenia

Wirusy komputerowe to specjalne, samopowielające się programy, które wyrządzają szkodę na zainfekowanym komputerze. Niszczą one zawartość dysku twardego (programy, pliki), usuwają z niego wybrane pliki (np. te dokumenty, z których korzystamy najczęściej) lub powiększają rozmiary plików, destabilizując i spowalniając pracę systemu operacyjnego. Mogą również uszkodzić system operacyjny lub sformatować dysk twardy.

Odmiany złośliwego oprogramowania

1. **Robaki komputerowe** są podobne do wirusów, jednak rozprzestrzeniają się nie poprzez doklejanie kodu do innych programów, lecz poprzez sieci komputerowe (pocztę elektroniczną, komunikatory, serwisy społecznościowe).
2. **Trojany (konie trojańskie)** to programy pełniące z pozoru funkcję użytkową lub rozrywkową, a w rzeczywistości czyniące szkody. Rozsyłane są zwykle za pomocą poczty elektronicznej. Konie trojańskie mogą usunąć dane, a niektóre z nich przekazują kontrolę nad komputerem w niepowołane ręce. Ktoś może w ten sposób uzyskać dostęp do danych zapisanych na naszym komputerze, np. do haseł, numerów kart kredytowych itp. Nazwa tego rodzaju programów nawiązuje do mitologicznego konia trojańskiego.
3. **Spyware** (z ang. spy - szpiegować) to określenie programów wykradających z komputera różnego rodzaju dane (pliki, hasła dostępu, historię odwiedzanych stron).
4. **Botnet** to grupa komputerów z zainstalowanym złośliwym oprogramowaniem (liczba komputerów w największych botnetach to kilka milionów) i kontrolowanych przez jedną osobę (grupę przestępczą). Można go wykorzystać np. do wysyłania spamu, ataków na serwery, operacji prania brudnych pieniędzy itp. Komputery wchodzące w skład botnetu nazywa się czasami **komputerami zombie**.
5. **Keylogger** (z ang. key - klawisz, log - zapisać) to specjalny program, który funkcjonuje w systemie w niezauważalny sposób (np. nie widać go na pasku zadań). Przechwytuje i gromadzi informacje o wszystkich naciśniętych klawiszach. Ponieważ klawiatury używa się m.in. do wprowadzania haseł, osoba kontrolująca keylogger może wykorzystać przechwycone dane na przykład do uzyskania dostępu do kont użytkownika w serwisach internetowych - w tym do kont bankowych.
6. **Ransomware** (z ang. ransom - okup) to złośliwe oprogramowanie, które po infekcji szyfruje pliki użytkownika na dysku twardym i dyskach zewnętrznych. Odzyskanie zawartości plików jest możliwe po zapłaceniu przestępcom pewnej kwoty, stanowiącej okup.