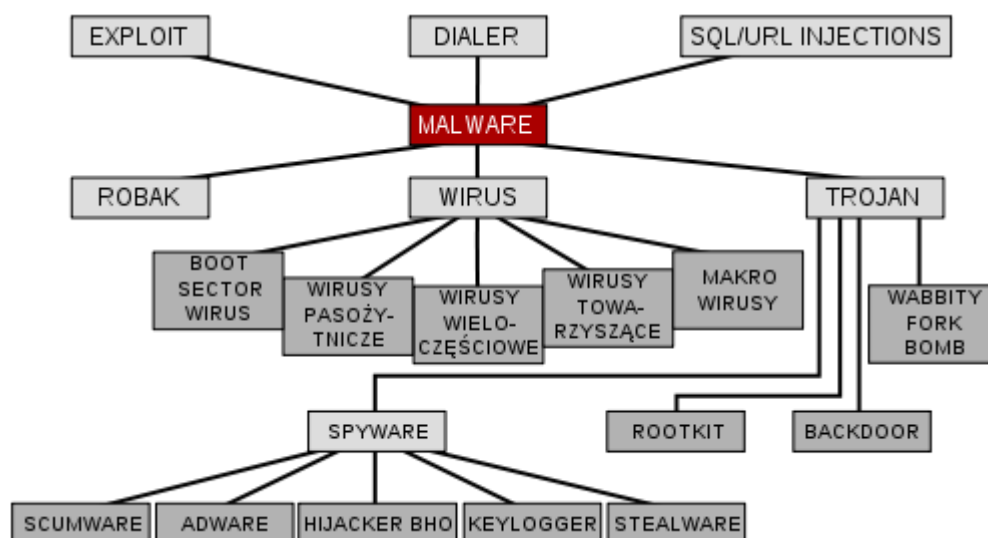


Każde oprogramowanie, które jest szkodliwe dla komputera zwane jest złośliwym, skróciła wersja z języka angielskiego – **Malware**, od malicious software - "złowrogi, złośliwy" i software.

Rodzaje szkodliwego oprogramowania



Wirus – jest on tylko jednym z złośliwego oprogramowania.

To co go charakteryzuje to fakt, że musi, jak w organizmie człowieka, posiadać nosiciela. Jest to inny program, który jest przez niego infekowany, dzięki niemu powiela się i atakuje inne programy.

Wirusy dzielimy na:

- **Makro wirusy** – makro to komenda wykonywana skrótem klawiszowym (dla przykładu standardowo CTRL + S oznacza zapis, F1 wywołuje pomoc). Wirusy atakują podstawowe funkcjonalności w komputerze zamieniając ich funkcje. W ten sposób zamiast zapisać dokument w Wordzie może okazać się, że ściągniemy plik z Internetu z kolejnym złośliwym oprogramowaniem, które wyrządzi jeszcze większe szkody.
- **Wirusy pasożytnicze** – poprzednie wirusy atakowały konkretne makro. Tym razem mamy do czynienia z wirusem, który atakuje kolejne makra, zmuszając je do zmian według jego schematu. Co ciekawe, ta metoda jest wolniejsza od ataku poszczególnych makr.
- **Wirusy towarzyszące** – atakują programy tworząc pliki wykonywalne z innym rozszerzeniem, modyfikując oryginalny plik. Gdy przychodzi żądanie uruchomienia programu (na przykład poprzez podwójny klik lewą myszką) wirus powoduje, że to zainfekowana kopia się otwiera. Z pozoru nic się nie zmienia dla użytkownika, choć w tle wirus zbiera żniwo.

- **Wirusy boot sector** – jako, że kod realizowany podczas startu komputera (z angielskiego boot właśnie) uruchamia się automatycznie ten sektor jest bardzo wrażliwy na ataki. Wirusy te potrafią wyrządzić przez to wiele szkód. By się im przeciwstawić wiele współczesnych BIOSów (zestawy podstawowych procedur komunikacji sprzętu z systemem operacyjnym) uniemożliwia jakiegokolwiek zmiany w tym sektorze poprzez oprogramowanie zewnętrzne.
- **Wirusy wieloczęściowe** – jest to dość niebezpieczny rodzaj, który atakuje na wiele sposobów, łącząc atak na boot sector, jak i na zwykłe programy, czy makra. Pierwszym tego typu wirusem był Ghostball odkryty już w 1989 roku.

Worm – robak jest programem, który sam się powiela by rozprzestrzeniać na inne komputery, najchętniej przez sieć. Nie potrzebuje żadnego innego oprogramowania by się pod nie podczepić. Najczęściej robaki nie powodują szkód poza obciążaniem łącza w celu replikacji.

Exploit – tłumaczenie samego słowa to użytek czegoś na własną korzyść, oznacza wykorzystanie luki w systemie lub tylko jednym z zainstalowanych programów (także legalnych i płatnych!) najczęściej w celu przejęcia kontroli nad naszym komputerem.

Dialer – oprogramowanie nie mające racji bytu w większości miejsc na świecie. Służy do modyfikacji numeru z jakim łączy się modem, tak byśmy płacili ogromne rachunki za telefon.

SQL / URL injections – właściwie należałoby napisać ogólnie o „wstrzykiwaniu” fragmentu kodu do już istniejących programów, ale te dwa przypadki są najbardziej popularne. Technika polega na zmianie wykonywanych poleceń podczas działania aplikacji bądź poprzez uruchamianie dodatkowych linków. Linki te mogą zawierać reklamy, czy strony, z których niejednokrotnie złapiemy jeszcze więcej chorób.

Trojan – zwany koniem trojańskim, jest dokładnie tym co znamy z lekcji historii. Pod użyteczną aplikacją bądź ważnym archiwum (na przykład zip, rar) kryje się złośliwe oprogramowanie, otwiera on tylne drzwi do komputera, z których chętnie korzysta jego twórca by go przejąć.

Trojany dzielą się na:

- **Wabbit / Fork bomb** – ten trojan powoduje samoreplikację aż do wyczerpania zasobów komputera. Takie działanie powoduje kompletne zablokowanie komputera. Pierwsza nazwa

wzięła się od królkia Bugsa, gdyż oryginalnie był to Rabbit virus związany z tym w jakim tempie króliki powiększają swą rodzinę.

- **Backdoor** – jeśli nie znaleziono luki w naszym systemie, zawsze można nam podesłać tego trojana by otworzyć sobie drzwi do naszego komputera. Często całymi miesiącami możemy nie być świadomi, iż używa się nas do nielegalnej działalności w sieci jako tak zwane zombie PC.
- **Rootkit** – to zestaw narzędzi umożliwiający podszywanie się pod administratora systemu i nadawanie niepożądanemu użytkownikowi uprawnień do działań w naszym komputerze, na które nigdy sami byśmy się nie zgodzili. Nazwa wzięła się od słów Root – określenie administratora w systemach typu Unix oraz kit – zestaw.

Spyware Oprogramowanie szpiegujące (ang. spyware) – to w skrócie oprogramowanie, które ma za zadanie zbierać o nas informacje i przysyłać je, bez naszej wiedzy, do twórcy.

Spyware'y dzielą się na:

- **Scumware** – to ogólnie każde oprogramowanie, konkretnie, pobrane z Internetu (w przeciwieństwie do malware, które możemy zdobyć w dowolny sposób) bez naszej wiedzy. Np. są to nielegalne pliki Cookie, które magazynują nasze preferencje w sieci.
- **Adware** – to chyba jeden z najczęstszych złośliwych programów jaki spotyka każdego użytkownika Internetu. Często instaluje się bez naszej wiedzy i ciężko go usunąć. Wyświetla dodatkowe reklamy, które niejednokrotnie nie chcą się zamknąć.
- **Hijacker BHO** – w większości przypadków są to narzędzia instalujące bez wiedzy użytkownika dodatki do przeglądarek, złośliwe Toolbary i wyszukiwarki. Np. instalujące wygaszacze ekranu i paski w przeglądarkach, Dodatkowo często umożliwiają przejęcie komputera.
- **Keylogger** – bardzo niebezpieczne oprogramowanie odczytujące wszystko co piszecie na klawiaturze i wysyłające to w świat. Dzięki niemu można w łatwy sposób uzyskać dane logowania chociażby do waszego konta bankowego.
- **Stealware** – pod tym pojęciem kryje się wszystko, co bez naszej wiedzy wysyła do osób trzecich nasze dane, informacje czy pieniądze z kont bankowych, do których uzyskano dostęp.

Inne szkodliwe złośliwe oprogramowanie to:

fałszywe alarmy dotyczące rzekomo nowych i groźnych wirusów (ang. hoaxes), to także rzekome wykrycie zainfekowanego pliku, które powodują programy antywirusowe z wysokim poziomem

skanowania heurystycznego żarty komputerowe, robione najczęściej nieświadomym początkującym użytkownikom komputerów.

Generatory wirusów - istnieje wiele programów umożliwiających stworzenie własnego wirusa, nawet bez znajomości systemu czy mechanizmów wykorzystywanych przez wirusy. Można je bez problemu znaleźć w Internecie. Korzystają one z gotowych modułów w assemblerze i umożliwiają stworzenie wirusa o zadanych parametrach wybieranych zwykle przy pomocy przyjaznego użytkownikowi menu. Można w nim określić zakres infekowanych obiektów oraz rodzaj efektów które ma on wywoływać. Oprócz kodu wynikowego wirusa, generatory tworzą także źródła w assemblerze, co umożliwia zainteresowanemu pisaniem wirusów użytkownikowi dokończanie się w tej dziedzinie.

Fałszywe antywirusy

Według raportu opublikowanego przez firmę Google, nawet 15% całego złośliwego oprogramowania w Sieci to fałszywe antywirusy.

Ransomware (ang. ransomware - zbitka wyrazowa powstała ze słów ransom "okup" i software "oprogramowanie") – rodzaj szkodliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.

Potrafią podmienić stronę którą oglądasz (najczęściej strony bankowe) i wyświetlają komunikaty ostrzegawcze o blokadzie strony i wyludzają pieniądze w zamian za dostęp.