

WHITE PAPER

Ochrona antywirusowa w urządzeniach UTM NETASQ

WPROWADZENIE

CORAZ WIĘCEJ ZAGROŻEŃ

W ciągu ostatnich kilku lat zagrożenia komputerowe rozwinęły się w szybkim tempie. Wzrosła liczba metod i sposobów infekcji komputera, a przy tym złożoność złośliwego oprogramowania.

Zmianie uległa przede wszystkim intencja osób tworzących wirusy. Twórcy złośliwych aplikacji coraz rzadziej są pasjonatami i zapaleńcami oczekującymi uznania i podziwu. Obecnie za atakami (z sieci) stoją cybernetyczni przestępcy, którzy czerpią poważne zyski ze swojej działalności.

Efektym konfrontacji cyberprzestępców z producentami zabezpieczeń IT jest rozwój różnorodnych metod ochrony stosowanej w systemach zabezpieczających komputery i sieci.

Nowoczesna ochrona przed zagrożeniami musi uwzględniać dużą liczbę wirusów, ich złożoność i różnorodność. Nowoczesne systemy ochrony muszą przewidywać ich pojawienie się oraz szybko je neutralizować. Dzisiaj to warunek konieczny skutecznego rozwiązania.

Obecnie na rynku IT dostępne są rozwiązania bezpieczeństwa o zróżnicowanej możliwości uzyskania zintegrowanej ochrony przed wirusami.

W niniejszym dokumencie zaprezentujemy różne sposoby, metody i techniki ochrony antywirusowej, po to, aby ułatwić klientowi zrozumienie branży bezpieczeństwa IT i w efekcie dokonanie świadomego i trafnego wyboru rozwiązania dla swojej firmy.

ATAKI DLA ZYSKU

Charakter zagrożeń dla komputerów stacjonarnych znacząco zmienił się na przestrzeni lat. Dziś wielość sposobów wymiany informacji daje zagrożeniom znacznie większą możliwość rozprzestrzeniania się. Już mało kto pamięta o wirusach przenoszonych jedynie na dyskietkach. W czasie gdy rozwijały się nowe metody komunikacji (Internet, poczta e-mail czy ogólnie określana komunikacja szerokopasmowa), zmieniały się również zagrożenia dla użytkowników. Ich rozwój nastąpił w dwóch wymiarach:

- wzrostu liczby metod infekowania,

- wzrostu złożoności złośliwych programów jak i samej ich liczby.

Wirusy nie tylko rozpowszechniają się przez wiadomości e-mail i strony internetowe, lecz wykorzystują również zainfekowane stacje robocze do atakowania hostów z nimi połączonych. Powszechne staje się wykorzystywanie sieci zainfekowanych komputerów, sterowanych bez wiedzy użytkowników tzw. botnetów. Taka sieć stoi za atakami, które początkowo stosowały protokół IRC, by szybko przejść na poziom HTTP. Teraz stosują one techniki, które pozwalają im na zmianę zarówno nazwy wyświetlanej domeny jak i adresu IP, co czyni je coraz trudniejszymi do wykrycia.

W tym samym czasie wzrosła również liczba rodzajów ataków. Zbiór typów zagrożeń, obejmujący robaki i wirusy, rozszerzył się i obejmuje teraz także konie trojańskie i zagrożenia typu trapdoor czy oprogramowanie spyware. Szpiegowskie programy pozwalają na uzyskiwanie informacji o tym, jak użytkownicy korzystają z zainfekowanych stacji roboczych lub uruchamianie ataków wirusów na konkretne cele (np. ataki typu Dos [denial of service] lub spam).

Użytkownicy rozsyłający złośliwe aplikacje za cel postawili sobie zysk ze swojej działalności. Nie wystarczające jest już zdobycie rozgłosu. Obecnie to profesjonalne grupy przestępcze istniejące w sieci. Przeraza myśl, że cyberprzestępcy zajmują się m. in.

- sprzedaż odpowiedzi na sondaże przeprowadzane wśród Internautów celem generowania reklam skierowanych do konkretnych użytkowników,
- sterowaniem komputerem bez wiedzy użytkownika,
- nielegalną kontrolą niektórych kont bankowych klientów,
- przeprowadzaniem ataków typu DoS, paraliżujących i blokujących dostęp do witryn firmowych.

Ataki przeprowadzane przez organizacje przestępcze są coraz liczniejsze oraz coraz poważniejsze w skutkach.

Częstsze ataki wymuszają stosowanie coraz skuteczniejszych zabezpieczeń antywirusowych na komputerach osobistych. Skaner antywirusowy musi nadążać za wzrostem liczby typów zagrożeń i zachowywać równowagę między bezpieczeństwem a wydajnością pracy.

KILKA TERMINÓW

Przedstawione pojęcia obejmują podstawowe pojęcia najczęściej stosowane w odniesieniu do złośliwych aplikacji.

Wirus: to popularne określenie złośliwego programu, który dopisuje się do pliku wykonywalnego innego programu zmieniając lub blokując jego działanie. Wirusy nie mogą się same rozprzestrzeniać.

Wirusy polimorficzne i metamorficzne: wirusy, które kodują swoje sygnatury inaczej dla każdego zainfekowanego pliku. Są trudniejsze do wykrycia przez skanery antywirusowe, ponieważ sygnatura każdego z nich jest inna.

Robak: złośliwy program, który replikuje się sam, używając do tego celu np. wiadomości e-mail, komunikatorów internetowych. Robaki mogą wyłączać ochronę komputerów lub nawet instalować oprogramowanie w celu dodania zainfekowanego hosta do sieci komputerów zombie (botnet).

Konie trojańskie: aplikacje, które przedostają się na komputer, często udając przydatne oprogramowanie instalowane przez nieświadomych użytkowników. Po zainstalowaniu konie trojańskie wyszukują poufne informacje o użytkowniku (np. dane logowania do bankowości elektronicznej) celem przesłania ich dalej bez jego wiedzy.

Botnet: sieć zainfekowanych komputerów, sterowanych zdalnie bez wiedzy użytkownika przez twórcę złośliwego programu. Ten typ zagrożenia używany jest często do ataków przeprowadzanych na skalę masową (kampanie spamowe czy DoS).

OCHRONA ANTYWIRUSOWA

SYGNATURY I HEURYSTYKA

Podstawę rozwiązań antywirusowych stanowi serce silnika antywirusowego, czyli baza sygnatur wirusów, czyli lista wszystkich zagrożeń rozpoznawanych przez nie. Fakt, że stale pojawiają się nowe zagrożenia, zmusił producentów programów antywirusowych do wprowadzenia do oferty rozwiązań proaktywnych, opartych na analizie heurystycznej. Pozwala to na walkę z nowymi wirusami i to jeszcze zanim baza sygnatur wirusów zostanie zaktualizowana.

BAZA NIE WYSTARCZY

Sygnatura to fragment kodu z jakiego składa się złośliwy program. Skaner w silnikach antywirusowych sprawdza obecność złośliwego kodu. Rosnąca liczba wirusów powoduje konieczność stałego poszerzania baz sygnatur, pomimo postępu w opracowywaniu algorytmów, które służą do wykrywania wielu wirusów za pomocą jednej sygnatury generycznej.

Skuteczność silnika antywirusowego można mierzyć nie tylko wielkością jego bazy sygnatur wirusów, lecz także częstotliwością aktualizacji tej bazy oraz umiejętnością skanowania proaktywnego. Technika ta jest jednak dziś niewystarczająca.

SAMODZIELNA ANALIZA

W celu generycznego wykrywania wirusów nieobecnych w bazach programów antywirusowych opracowano techniki analizy heurystycznej, które sprawdzają kod źródłowy plików, makr lub plików wykonywalnych w celu wykrycia różnego rodzaju złośliwego oprogramowania.

W skanerze takim stosowane są dwa odrębne typy analizy – analiza statyczna i dynamiczna.

Statyczna analiza heurystyczna opiera się na użyciu małych sygnatur charakterystycznych dla większości wirusów, zwanych „podejrzanyimi komendami”.

Choć metoda ta jest łatwa w zastosowaniu i pozwala na szybkie wykrywanie zagrożeń,

niestety wykazuje się niskim współczynnikiem wykrywalności nowo powstałych wirusów.

Dynamiczna analiza heurystyczna korzysta z wirtualnych systemów zwanych „sandbox”. Podejrzany program jest uruchamiany w środowisku wirtualnym oraz badany pod kątem nietypowych zachowań.

Ta technika pomimo, że wymaga większych zasobów pamięci, gwarantuje wyższą wykrywalność.

KRYPTOANALIZA I KLUCZE

Wirusy polimorficzne i metamorficzne nie mają sygnatur, gdyż nie mają stałych fragmentów kodu, które pozwoliłyby na ich identyfikację. Dlatego też nie są wykrywane za pomocą analizy opartej na sygnaturach.

Struktura wirusa polimorficznego ulega modyfikacjom w trakcie replikacji. Użycie sygnatur do wykrywania tych wirusów, jest zatem bezcelowe, dlatego konieczne jest zastosowanie odrębnych techniki wykrywania tych wirusów.

Maska zredukowana wykorzystując silnik antywirusowy w strukturze zaszyfrowanego wirusa wyszukuje klucz dekodujący i przelicza ponownie kod źródłowy. Technika ta po ujawnieniu kodu stosuje analizę sygnatur.

Kryptoanaliza znanego tekstu jawnego wykorzystuje pierwotny kod źródłowy wirusa jak również znany zaszyfrowany kod (bądź przynajmniej podejrzany kod, który przypomina zaszyfrowaną strukturę wirusa). Pozwala to na rekonstrukcję kluczy i algorytmu w celu rozszyfrowania zaszyfrowanej części struktury wirusa. Technika ta, oparta na równaniach, jest trudna w zastosowaniu. Przypomina ona klasyczne kryptograficzne techniki rozszyfrowywania tekstu bez znajomości klucza do szyfru. Są jednak dwie zasadnicze różnice: większość potrzebnych danych jest znana, a czas na rozszyfrowanie jest ograniczony.

Istnieją także inne techniki wykrywania wirusów polimorficznych, jednak są one porównywalne z dynamiczną analizą heurystyczną.

METODY ZAAWANSOWANE

Silniki antywirusowe w programach antywirusowych najnowszej generacji muszą stosować w połączeniu z podstawowymi technikami różne środki pozwalające na zwiększenie wskaźnika wykrywalności wirusów. Spośród nich można przedstawić następujące:

- obliczanie sum kontrolnych,

- wykrywanie generyczne,
- analiza obiektów złożonych.

Obliczanie sum kontrolnych całego pliku w oparciu o lokalizację ciągu i jego wartość pozwala na ograniczenie problemów związanych z rozmiarem baz danych i błędną klasyfikacją programów jako wirusów. Zamiast szukać sygnatury metoda ta porównuje sumy kontrolne plików.

Wykrywanie generyczne polega na identyfikacji kilku wirusów przy użyciu jednej sygnatury. Zauważono, że skuteczne zagrożenia są często kopiowane i używane ponownie. Metoda generyczna polega więc na stworzeniu sygnatury, która może wykryć wszystkie zagrożenia należące do tej samej rodziny.

Analiza obiektów złożonych polega na wykrywaniu wirusów w złożonych plikach (archiwa, pliki tekstowe, wiadomości e-mail i bazy danych). Ten typ analizy jest podstawą dla silników antywirusowych, jako że zagrożenia mogą się znajdować w dowolnej części złożonego pliku. Nietrudno wyobrazić sobie złośliwy program skompresowany programem UPX a następnie dodany do archiwum zip i włączony do pliku CAB.

Silnik antywirusowy musi zatem współpracować z kilkoma wersjami programów służących do kompresji i archiwizacji.

ANTYWIRUS SIECIOWY

KOMPLETNA OCHRONA

Rozwój nowych zagrożeń wymusił na dostawcach rozwiązań bezpieczeństwa IT rozstrzygnięcie kwestii konfliktu pomiędzy maksymalizacją bezpieczeństwa a wydajnością pracy. Urządzenie UTM firmy NETASQ jest propozycją dla tych, którzy chcą otrzymać maksymalną ochronę przy jednoczesnym minimalnym obciążeniu sieci.

Celem urządzenia wielofunkcyjnego jest zintegrowanie takich elementów jak:

- firewall,
- system wykrywania i blokowania ataków IDS/IPS,
- zapewnienie bezpiecznego połączenia VPN,
- autoryzacja użytkowników,
- skanera wnętrza sieci SEISMO,
- ochrona antywirusowej,
- ochrona antyspamowej,
- filtrowanie URL,
- monitoring sieci w czasie rzeczywistym,
- generowania raportów.

Zastosowanie oprogramowania antywirusowego pozwala na eliminację zagrożeń przychodzących z zewnątrz sieci, co bezpośrednio wpływa na bezpieczeństwo antywirusowe całej sieci wewnętrznej. Wirusy oraz szkodliwe programy są skutecznie neutralizowane bezpośrednio na urządzeniu NETASQ. Zapobiega to rozprzestrzenianiu się wirusów wewnątrz sieci. Nie zapewnia jednak ochrony w przypadku zagrożeń pochodzących np. z dysków przenośnych oraz nośników wymiennych, ponieważ skanowanie antywirusowe realizowane jest w ramach komunikacji sieciowej.

Niezależnie od tych ograniczeń rozwiązania wybrane przez dostawcę urządzeń wielofunkcyjnych muszą spełniać pewne kryteria wyszczególnione przez niezależny zespół badawczy. Niemniej wprowadzenie silnika antywirusowego w ograniczonym środowisku urządzenia sieciowego może oznaczać konieczność pewnych kompromisów, co w szczególności dotyczy zamkniętej bazy sygnatur (WildList).

ZALETY ROZWIĄZAŃ ZINTEGROWANYCH

Główną zaletą urządzeń wielofunkcyjnych jest połączenie kilku systemów bezpieczeństwa, które w znaczący sposób zwiększają poziom zabezpieczenia danej sieci.

Są również inne zalety takich rozwiązań, między innymi:

- ograniczenie ruchu sieciowego poprzez eliminację zagrożeń, co bezpośrednio wpływa na zmniejszenie kosztów utrzymania łączy oraz koszty stosowania alternatywnych zabezpieczeń,
- rozwiązanie typu Plug & Play: nie ma konieczności instalacji dodatkowych aplikacji na stacjach roboczych,
- zwiększenie poziomu bezpieczeństwa oraz podniesienie wydajności pracy stacji roboczych.

Ochrona zintegrowana pozwala na blokowanie zagrożeń w urządzeniu NETASQ, zapobiegając w ten sposób ich rozprzestrzenianiu się na potencjalnie narażone stacje robocze. W połączeniu z dodatkowo zainstalowanym programem antywirusowym na stacjach roboczych daje to podwójne zabezpieczenie i zapewnia optymalną ochronę.

Gwarancja rezydentnego sieciowego skanowania antywirusowego jest ważna, gdyż użytkownicy zwykle wyłączają programy antywirusowe zainstalowane na swoich komputerach. Zastosowanie skanera antywirusowego w zintegrowanym urządzeniu umożliwia skanowanie całego ruchu w sieci i zapewnia pełną scentralizowaną ochronę stacji roboczych.

KRYTERIA WYBORU ROZWIĄZANIA

Przy wyborze rozwiązania do ochrony antywirusowej, czy jest to ochrona na poziomie sieci czy też aplikacji, pomocna jest analiza kluczowych cech takiego rozwiązania. Niezależne testy, badające skuteczność aplikacji antywirusowych, opierają swoją ocenę na kluczowych parametrach danego programu. Wyznacznikami skuteczności rozwiązania są:

- współczynnik wykrywalności znanych wirusów,
- współczynnik wykrywalności wirusów polimorficznych,
- czas aktualizacji bazy sygnatur (czas reakcji),
- szybkość skanowania (wydajność pracy),
- wykrywanie proaktywne,
- współczynnik fałszywych alarmów (false positive).

Współczynnik wykrywalności znanych wirusów jest jednym z najistotniejszych kryteriów przy pomiarze skuteczności programu antywirusowego, ponieważ rozwiązania służące do wykrywania tych wirusów stanowią podstawę takich programów.

Test taki porównuje liczbę wykrytych przez skaner znanych wirusów z ogólną liczbą istniejących wirusów znajdujących się w bazie. Pozwala to zarówno na sprawdzenie, czy baza wirusów jest aktualna, jak i pomiar skuteczności danego programu.

Współczynnik wykrywalności wirusów polimorficznych pokazuje zdolność

programu antywirusowego do stosowania sygnatur generycznych, co zapewnia wykrycie mutacji wirusów przy jednoczesnej optymalizacji rozmiaru bazy sygnatur.

Czas aktualizacji bazy sygnatur to czas reakcji na nowego wirusa. Masowy wzrost liczby wirusów oraz pojawiające się nowe metody rozprzestrzeniania się wirusów wymagają szybkiej reakcji. Testy badają częstotliwość aktualizacji bazy sygnatur wirusów danego programu. Częstsze i szybsze aktualizacje oznaczają lepszą ochronę.

Szybkość skanowania jest dla programu antywirusowego jedną z najważniejszych cech. Stosowane metody detekcji zagrożeń nie powinny prowadzić do zauważalnego zwolnienia działania sieci, w przeciwnym razie istnieje ryzyko, że zostaną wyłączone.

Skanowanie proaktywne oznacza reakcję programu na nowego wirusa bez konieczności aktualizacji bazy sygnatur wirusów. Nazywane jest to ochroną dnia zerowego (ang. zero-day protection). Kryterium to pokazuje skuteczność technik analizy heurystycznej danego programu antywirusowego.

Współczynnik fałszywych alarmów (false positive) to kryterium ważne przy ocenie jakości silnika antywirusowego. Błędne wskazanie wirusa w niezainfekowanym pliku może mieć poważny wpływ na funkcjonowanie firmy (brak możliwości przesyłania ważnych dokumentów).

Oprócz tego wybór programu antywirusowego uzależniony jest od jego umiejętności **wykrywania zagrożeń w plikach skompresowanych**. Przed rozpoczęciem skanowania konieczna jest dekompresja pliku. Skuteczność w tym zakresie jest mierzona liczbą poziomów kompresji, z którymi dany program współpracuje (skompresowany plik może zawierać kilka innych skompresowanych plików).

BAZA AKTUALNYCH WIRUSÓW (WILDLIST)

Bezpieczeństwo infrastruktury wymaga często znalezienia kompromisu między oferowanymi sposobami ochrony a różnymi związanymi z nimi ograniczeniami. Niektóre sieciowe rozwiązania antywirusowe korzystają z ograniczonej bazy sygnatur, co wynika z chęci optymalizacji jej rozmiarów ale również poprawy wydajności pracy aplikacji. Metoda ta opiera się na aktualizowanej raz w miesiącu bazie sygnatur wirusów aktualizowanej przez Wild List Organization (www.wildlist.org). Organizacja ta oferuje bazę sygnatur wirusów i złośliwego oprogramowania ocenionych jako za „aktywne”. Aby program został uznany za „aktywny” musi pojawić się co najmniej kilka doniesień o jego istnieniu a także można ocenić go jako szeroko rozpowszechniony. Niektóre a w szczególności nowo powstałe wirusy mogą się zatem na niej nie znajdować, a inne mogą zostać z niej usunięte kiedy zmniejszy się zasięg ich wpływów.

Metoda ta ma jednak istotne wady:

- Po pierwsze, miesięczne odstępy w aktualizacji listy sprawiają, że pojawia się niebezpieczna przerwa między pojawieniem się wirusa a jego faktycznym wykryciem przez bazę sygnatur wirusów. W związku z ciągłym rozwojem zagrożeń takie rozwiązanie jest ryzykowne. Sytuację tę można by zmienić poprzez częstsza aktualizację bazy sygnatur.

- Co więcej, jako że stale pojawiają się nowe wirusy (w roku 2008 było ich średnio 30 000 miesięcznie), rozmiar tej bazy sygnatur (ok. 25 000) nie może nadążyć za rozwojem zagrożeń w inny sposób niż przez częste aktualizacje.

Dlatego też stosowanie ograniczonej bazy sygnatur poświęca kwestię bezpieczeństwa na rzecz wydajności. Kompromis ten wymaga kontroli nad sygnaturami znajdującymi się w bazie poprzez stałe jej aktualizowanie, dzięki czemu może być porównywalna z typową bazą (ok. 500 000 sygnatur).

Podsumowując, choć producenci rozwiązań antywirusowych i niezależne organizacje testujące korzystają z zamkniętej bazy sygnatur, jej stosowanie jest kontrowersyjne. Co potwierdza również w swojej prezentacji Av-Test z Konferencji Virus Bulletin 2007 „WildList nie żyje, niech żyje WildList”.

OCHRONA NETASQ

NETASQ, producent rozwiązań do zabezpieczania sieci, nigdy nie godził się na kompromisy w kwestii bezpieczeństwa, gwarantując jednocześnie optymalną wydajność pracy. System IPS, serce jego zintegrowanego systemu bezpieczeństwa, znany jest z tego, że ma jeden z najwyższych współczynników przepustowości IPS przy najlepszej ochronie typu „zero day” na rynku.

Firma NETASQ stawia na rozwiązania zintegrowane, a swoją działalność opiera na współpracy z uznanymi na rynku partnerami. Właśnie dlatego filtry URL są oparte na silniku OPTENET, a rozwiązanie antyspamowe bazuje na silniku Vaderetro.

Chcąc zagwarantować najlepszą ochronę antywirusową, firma NETASQ zdecydowała się na współpracę z jednym z liderów w tej dziedzinie na rynku. Przed podjęciem tej decyzji firma sprawdziła wszystkie rozwiązania i przeanalizowała kwestie najistotniejsze dla programów antywirusowych:

- współczynnik wykrywalności znanych wirusów,
- współczynnik wykrywalności wirusów polimorficznych,
- czas aktualizacji bazy sygnatur (czas reakcji),
- szybkość skanowania,
- wykrywanie proaktywne,
- współczynnik fałszywych alarmów (false positive).

Analiza ta skłoniła NETASQ do współpracy z firmą Kaspersky Labs. Przez lata rozwiązania

Kaspersky Labs osiągały jedne z najlepszych wyników w różnych testach porównawczych niezależnych instytucji badawczych.

Jednocześnie NETASQ we wszystkich swoich produktach oferuje wbudowaną ochronę antywirusową bazującą na skanerze Clam AV, cenionym rozwiązaniu open-source'owym.

PODSUMOWANIE

W związku z pojawieniem się nowych dróg rozprzestrzeniania się wirusów i zmianą natury ich ataków konieczne jest połączenie zaawansowanych rozwiązań do ochrony antywirusowej. W tym kontekście podejście oparte na skanowaniu sieciowym daje podwójną korzyść w postaci zmniejszenia kosztów operacyjnych i zwiększenia poziomu bezpieczeństwa dzięki gwarancji stałej, centralnie sterowanej ochrony.

W swoich zintegrowanych rozwiązaniach firma NETASQ oferuje pełen zakres ochrony sieci, firewall i filtry URL, jednocześnie nie zapomina o zapobieganiu i blokowaniu włamań oraz ochronie antywirusowej. Firma NETASQ nie ustępuje w kwestiach bezpieczeństwa i korzysta z możliwości wyboru spośród dwóch skanerów antywirusowych, opierając się na pełnych bazach sygnatur wirusów. Różne testy wykazały, że analiza oparta na liście WildList nie daje wystarczającego współczynnika wykrywalności, nawet wtedy, gdy organizacje przeprowadzające testy wybierają najnowsze wirusy. To ograniczenie w kwestii bezpieczeństwa wynika w głównej mierze z dużej liczby nowych wirusów pojawiających się co miesiąc.

O FIRMIE NETASQ

Firma NETASQ specjalizuje się w rozwiązaniach do zintegrowanego zabezpieczenia sieci. Jako główny cel firma postawiła sobie dostarczanie rozwiązań zapewniających ten sam, najwyższy poziom zabezpieczeń dla firmy niezależnie od ich wielkości.

Rozwiązania NETASQ obecne są na rynkach w blisko 50 krajach poprzez sieć autoryzowanych partnerów również w Polsce.

Urządzenia NETASQ UTM posiadają m. in. certyfikację Common Criteria EAL4+ na kluczowe funkcje urządzeń czyli firewall, system wykrywania i blokowania włamań oraz VPN.

ZAŁĄCZNIK – DEFINICJE

- **Adware:** program komputerowy oparty na wyświetlaniu reklam na komputerze użytkownika. Część adware jest względnie nieszkodliwa i wyświetla jedynie reklamy darmowych produktów. Jednakże niektóre firmy sprzedają targetowane kampanie promocyjne oparte na programach instalowanych bez wiedzy użytkownika. Istnieją również programy, które wyszukują dane wrażliwe użytkownika, w szczególności informacje o jego sposobie korzystania z Internetu.
- **Backdoor:** termin ten odnosi się do złośliwego oprogramowania, które w chwili uruchomienia na zainfekowanym komputerze otwiera kanały komunikacyjne z zewnętrznymi sieciami. Twórca złośliwego programu może połączyć się w ten sposób i zdalnie kontrolować zainfekowany host. Najczęściej backdoor instalowany jest przez wirusa, robaka lub konia trojańskiego. Tego typu programów używać można do wyszukiwania na zainfekowanym komputerze wrażliwych danych (loginy i hasła, adresy e-mail). A sam host może być częścią sieci botnet, a także zostać wykorzystany w kampaniach spamowych.
- **Bomba logiczna:** program komputerowy zaprojektowany, by w chwili określonego zdarzenia rozpocząć szkodliwą dla systemu działalność. Zdarzeniem tym może być upływanie jakiegoś terminu, zmiana konkretnych danych lub brak wiadomości od autora programu. Ten typ zagrożenia zwykle umieszczany jest w systemie przez nieuczciwych pracowników i jest aktywowany, gdy odchodzą oni z firmy.
- **Bot:** patrz – Robot
- **Greyware:** złośliwe oprogramowanie, które wymaga zainstalowania jak też odinstalowania przez samego użytkownika, dlatego stanowi niewielkie ryzyko. Termin ten obejmuje również inne rodzaje złośliwego oprogramowania, takie jak spyware'y i adware'y. Ten typ zagrożenia pogarsza wydajność pracy zainfekowanego komputera. Może ono również przeprowadzać niechciane działania jak otwieranie okien, zbieranie informacji o zwyczajach użytkownika, a nawet wystawiać komputer na potencjalny atak przez eksponowanie jego słabych punktów.
- **Malware:** patrz – złośliwe oprogramowanie
- **Makrowirusy:** wirusy zaprogramowane z wykorzystaniem języka używanego do tworzenia makr w pakiecie programów biurowych Windows. Wirus rozprzestrzenia się we wszystkich dokumentach stworzonych przy pomocy tego modelu makr. Luki związane z makrowirusami zostały usunięte w MS Office 2000.
- **Pharming:** technika phishingu wykorzystująca dane wrażliwe na serwerach nazw domen. Choć użytkownik podaje właściwą nazwę domeny w przeglądarce, w wyniku podrobienia adresu IP serwera www, trafia na fałszywą stronę.

- **Phishing:** to zjawisko polegające na wysyłaniu fałszywych wiadomości e-mail mających na celu wyłudzenie poufnych danych (login i hasło do konta bankowego lub portali społecznościowych). W e-mailu podawany jest link do strony, gdzie użytkownik powinien podać wszystkie dane osobowe. Po przechwyceniu takich danych autorzy mają do konta ofiary. Wysyłane wiadomości najczęściej podszywają się pod banki lub inne godne zaufania instytucje.
- **Riskware:** oprogramowanie, które jako takie nie jest złośliwe, ale jego zastosowanie może prowadzić do przeniknięcia na komputer złośliwego oprogramowania. Przykładem potencjalnie niebezpiecznego programu może być klient komunikatora internetowego.
- **Robot:** program komputerowy, automatycznie wykonujący określone zadania, używany w sieciach zombie zwanych botnetami. Bot, instalowany zwykle przez robaka lub konia trojańskiego, uruchamia tzw. backdoor, przez który administrator takiej sieci, może zdalnie kontrolować hosta.
- **Rootkit:** metoda pozwalająca na ukrycie przed użytkownikiem działających programów lub procesów. Złośliwe oprogramowanie, które ma na celu przejęcie kontroli nad systemem, często korzysta z tej metody, by ukryć swoją obecność i działanie. Ten typ zagrożenia może funkcjonować na różnych poziomach zainfekowanego systemu. Od warstwy aplikacji (modyfikacja konfiguracji programu, by zapobiec wyświetlaniu informacji), przez jądro systemu operacyjnego (przejęcie funkcji, dodanie sterowników), rootkity mogą sięgać najniższych warstw i uruchamiać się przed systemem operacyjnym, czyniąc ich wykrycie jeszcze trudniejszym.
- **Złośliwe oprogramowanie:** termin używany dawniej w odniesieniu do koni trojańskich i wirusów. Obecnie termin „malware” stosowany jest do określania każdego oprogramowania działającego bez wiedzy użytkownika.