Wirusy

1 Co to jest wirus komputerowy?

Wirusy komputerowe (mikroby) to „złośliwe” programy, które są zdolne do kopiowania i rozprzestrzeniania się w systemach komputerowych i sieciach w sposób niekontrolowany i wykonywania zaprogramowanych wcześniej procedur.

Operacje wykonywane przez wirusy komputerowe są bardzo różne: od zabawnych komunikatów wyświetlanych na ekranie do uszkodzenia fizycznego komputera.

Wirus komputerowy jest programem, który powiela się przez zarażanie zbiorów wykonywalnych, jednostek alokacji plików lub sektora startowego dyskietki lub dysku twardego. Od niedawna nosicielem może być także szablon dokumentów stworzonych za pomocą aplikacji wchodzących w skład pakietów biurowych, wyposażonych w język makr (najczęściej MS Office). Na niebezpieczeństwo narażeni są wszyscy, którzy w dowolnej formie przenoszą dane między komputerami. Źródłem infekcji może być plik skopiowany ze strony WWW, dołączony do poczty elektronicznej albo wiadomości zamieszczonej na liście dyskusyjnej czy też przeniesiony z innego komputera za pośrednictwem dyskietki. Znane są przypadki, gdy producent oprogramowania prawdopodobnie nieświadomie rozpowszechniał

swój produkt na oryginalnie zapakowanych, a jednocześnie zawirusowanych dyskietkach lub płytach CD-ROM. Natomiast w czasach, gdy do dystrybucji oprogramowania masowo wykorzystywano dyskietki, zdarzało się, że po zwrocie oprogramowania przez klienta przepakowany (i zarażony) towar trafiał w ręce innego nabywcy. Nikt nie sprawdzał, czy w międzyczasie nie doszło do zarażenia plików na dyskietkach instalacyjnych.

2 Historia wirusów

Autorstwo pojęcia "wirus komputerowy" przypisuje się dr Fredowi Cohenowi - specjaliście od zabezpieczeń. 3 listopada 1983 r. podczas seminarium na temat bezpieczeństwa Cohen po raz pierwszy przedstawił teoretyczne zasady działania wirusów komputerowych. Kilka dni później, po uzyskaniu zgody uczelni, pokazał pierwszego działającego wirusa komputerowego - efekt swoich eksperymentów. Uruchomiono go na komputerze Vax działającym pod kontrolą systemu Unix. W 1984 r. podczas pracy na Uniwersytecie Południowej Kalifornii Cohen podał definicję wirusa jako "programu, który infekuje inne programy, modyfikując je tak, aby zawierały i wykonywały jego własny kod". Analogia do świata przyrody jest oczywista i bardzo trafna. Kilka lat później powstało pojęcie "robaka" (ang. worm) - programu równie destrukcyjnego co wirus.

Nowoczesne wirusy nie powstały jednak w Stanach Zjednoczonych. Uprzedzili ich programiści z Pakistanu, który podobnie jak Indie ma niezwykle zdolnych programistów. W 1986 r. dwaj bracia prowadzących małą firmę Brain Computers zajmującą się produkcję oprogramowania analizowali tzw. sektor startowy (boot sektor) dyskietki komputerowej zawierającej system operacyjny MS-DOS. Zawiera on procedurę, której celem jest wprowadzenie do pamięci i uruchomienie systemu operacyjnego. Czynność ta wykonywana jest przy każdym uruchomieniu komputera. Pakistańczycy wpadli na pomysł umieszczenia w sektorze startowym programu, który powielałby się w każdym nowo napotkanym sektorze startowym. W ten sposób wirus Brain (nazwa pochodziła od nazwy firmy) po każdym uruchomieniu komputera przenoszony był do pamięci, po czym nagrywał się w sektorach startowych wszystkich dyskietek wkładanych do stacji dysków. Dzieło Pakistańczyków błyskawicznie rozprzestrzeniło się po całym świecie, zarażając najwięcej komputerów w Stanach Zjednoczonych. Cel, jaki przyświecał twórcom zarówno wirusów Apple i Brain, można by uznać za światły. Ich autorzy chcieli odwieść użytkowników komputerów od powszechnej wówczas praktyki kopiowania oprogramowania. To właśnie dzięki kopiowaniu programów wirusy rozprzestrzeniały się tak szybko.

Po pojawieniu się Brain po raz pierwszy zwrócono uwagę na zagrożenie, jakim są wirusy komputerowe. Powstały pierwsze programy antywirusowe, w firmach wprowadzono po raz pierwszy procedury, których celem była ochrona komputerów przed zarażeniem. Aby je obejść, twórcy wirusów wymyślili zupełnie nowy typ - tzw. konia trojańskiego. Metoda jest prosta i, co ciekawe, do dziś stosowana z doskonałym skutkiem. Autor konia trojańskiego zachęca właściciela komputera, by sam znalazł i uruchomił program zawierający wirusa. Jak to zrobić? Wystarczy umieścić mikroba w popularnym programie, takim, który wiele osób chciałoby mieć w swoim komputerze. Na pierwszy rzut oka program jest nieszkodliwy, wręcz pożyteczny, choć w rzeczywistości realizuje zadania postawione mu przez swego autora - pozwala na przykład przejąć kontrolę nad komputerem ofiary.

Po raz pierwszy metodę konia trojańskiego zastosowano, umieszczając wirusa w edytorze tekstów PC-Write. Wczesne wirusy właściwie nie powodowały dużych szkód, a jeżeli już, to dlatego, że często były dziełem pomysłowych, aczkolwiek dość nieudolnych programistów. Tak jest zresztą do dziś - autorzy wirusów często popełniają szkolne błędy - twierdzi Andre Post z Symanteca. To dlatego szkodliwa działalność komputerowych wirusów

często objawia się w sposób przez autora niezamierzony, np. zawieszeniem komputera albo uszkodzeniem struktury plików na dyskietce.

W 1987 r. studenci uniwersytetu Leigh zaczęli zgłaszać dość dziwne problemy. Twierdzili, że z ich dyskietek znikały pliki. Na początku informatycy uniwersyteccy bagatelizowali problem, twierdząc, że najprawdopodobniej studenci sami niechcący kasowali pliki. Wkrótce okazało się, że winę ponosił wirus nazwany później Leigh. Był to pierwszy wirus, który rozprzestrzeniał się nie w sektorach startowych dyskietek, ale infekował pliki komputerowe nagrane na dyskietce. Kod wirusa Leigh dołączał się do pliku command.com (jeden z kluczowych plików MS-DOS) i starał się przenosić na wszystkie inne dyskietki zawierające ten plik. Fakt, że atakował tylko jeden rodzaj pliku, oraz w sumie dość wczesne wykrycie go spowodowało, że Leigh nie wydostał się poza dyskietki i komputery uniwersytetu.

Wkrótce potem powstał wirus o nazwie Jerusalem (zwanym też Israeli), który po raz pierwszy wykryto w komputerach Izraelskiego Ministerstwa Obrony. Uznawany jest za jednego z najbardziej udanych wirusów. Jego autor może być dumny, bo nie tylko udało mu się opracować zupełnie nowy rodzaj wirusa, ale również zachęcić innych do tworzenia jego mutacji. Leigh zarażał tylko jeden plik: command.com, tymczasem Jerusalem atakował wszystkie napotkane pliki programów (z końcówkami .com i .exe). Autor wirusa wykazał się nie lada pomysłowością. Jego kod po uruchomieniu programu, w którym się znajdował, umieszczany był w pamięci komputera, skąd zarażał inne pliki. Dzięki temu wirus prowadził swoją destrukcyjną działalność nawet, jeśli użytkownik przestał używać zarażonego programu. Jeruzalem zasłynął również jako pierwszy wirus zawierający tzw. bombę logiczną. Sprawdzał on aktualną datę i jeśli był to 13 dzień miesiąca i piątek, kasował znajdujące się na twardym dysku pliki z programami. Dokładna analiza kodu wirusa pokazała, że pierwszym dniem, w którym miał zadziałać, był 13 maja 1988 r. - 50. rocznica powstania państwa Izrael. Biorąc to pod uwagę, oraz fakt, że wirusem zainfekowano komputery Ministerstwa Obrony Izraela, można przypuścić, że wirusa stworzył programista palestyński. Początek lat 90. to okres, w którym wybuchła swoista wojna pomiędzy twórcami wirusów a producentami programów antywirusowych. Programy antywirusowe, podobnie jak same wirusy, były stosunkowo proste - ich zadaniem było sprawdzenie, czy w pamięci albo plikach na twardym dysku nie ma specyficznych kodów identycznych z tymi, jakie zawierają wirusy. Zadaniem autorów programów antywirusowych była jak najszybsza analiza kodu wirusa i przygotowanie tzw. sygnatury (charakterystycznych dla wirusa ciągów znaków) oraz szczepionki - programu, który usuwał złoczyńcę. W 1991 r. wszystko uległo zmianie. Amerykański naukowiec Mark Washburn opracował na podstawie znanego wirusa o nazwie Vienna metodę ukrywania kodu programu. Tak powstała idea wirusów polimorficznych, czyli takich, których kod jest zaszyfrowany, a na dodatek każda kolejna kopia różni się od pierwowzoru. Pomysł Washburna oraz kod stworzonego przez niego wirusa były i są nadal dostępne w Internecie. Sam autor stworzony przez siebie kod wirusa początkowo udostępnił tylko i wyłącznie autorom programów antywirusowych. Mimo tajemnicy, na pierwszego wirusa polimorficznego nie trzeba było długo czekać. Jeszcze w tym samym 1991 r. komputery na całym świecie zaatakowane zostały przez pochodzącego ze Szwajcarii Tecquille. Na początku lat 90. środowisko twórców udanych wirusów było dość hermetyczne. Autorów rzeczywiście działających i groźnych programów można było policzyć na palcach dwóch rąk. Wielką "zasługę" w rozpowszechnieniu wiedzy o tworzeniu wirusów zawdzięczamy pierwszemu BBS-owi (pierwowzór Internetu oparty na komputerach z modemami) o wirusach, który powstał w Bułgarii. Korzystający z niego twórcy wirusów wymieniali się pomysłami i dyskutowali nad skutecznymi metodami tworzenia wirusów oraz oszukiwania programów antywirusowych. Na efekty nie trzeba było długo czekać. Wkrótce pojawił się jeden z najgroźniejszych wirusów - Dark Avenger, nazwany tak od pseudonimu

nieznanego dotąd z imienia i nazwiska bułgarskiego programisty. Opracował on również pierwszy program do tworzenia wirusów, Dark Avenger Mutation Engine, który zamieniał dowolnego wirusa w jego postać polimorficzną - niełatwą do wykrycia w ówczesnych czasach. Wkrótce tworzenie wirusów stało się bajecznie łatwe za sprawą Virus Creation Kit - programu, który pozwala nawet dziecku, stworzyć niebezpieczny program. Wystarczy z menu wybrać rodzaj wirusa, określić, co ma robić i wskazać program, do którego nasze dzieło ma być dołączone. Po kilku minutach wirus jest gotowy. Obydwa programy spowodowały, że wirusy zaczęły pojawiać się jak grzyby po deszczu. Na szczęście szybko opracowano metodę wykrywania programów tworzonych przy użyciu takich narzędzi i dziś każdy program antywirusowy radzi sobie z nimi bez żadnego problemu.

Powstanie wirusów polimorficznych i narzędzi do ich tworzenia oraz olbrzymia ilość tzw. fałszywych alarmów zwróciły uwagę mediów. Pierwszym nagłośnionym przez gazety na całym świecie przypadkiem pojawienia się wirusa był Michelangelo. Media na całym świecie (w tym również "Gazeta Wyborcza") ostrzegały przed wirusem, który miał zaatakować 6 marca 1992 r. Przewidywano, że uszkodzonych może zostać około 5 mln komputerów (w rzeczywistości zarażonych wirusem zostało "ledwie" kilka tysięcy), podawano recepty jak się przed nim ustrzec, producenci programów antywirusowych sprzedawali ogromne ilości programów, które wykrywały i usuwały intruza. Ten ostatni fakt stał się zapewne źródłem do dziś powtarzanej plotki, że autorzy i producenci programów antywirusowych to jedne i te same osoby. Najpierw tworzą wirusy, a następnie szczepionki, które je usuwają. Co prawda nikomu jeszcze nie udało się dowieść tego związku, ale dmuchając na zimne, wielu producentów, np. Symantec, wprowadziło zasady, jakich muszą przestrzegać ich pracownicy. Przede wszystkim nie wolno im mieć absolutnie żadnych kontaktów z twórcami wirusów. Pracownikiem takiej firmy nie może zostać też były autor wirusów - choćby nie wiadomo jak był zdolny.

Pierwsze wirusy zagrażały właściwie wyłącznie posiadaczom komputerów z systemem DOS. W 1992 r. po raz pierwszy spadła liczba komputerów zainfekowanych wirusami działającymi w tym systemie operacyjnym. Jednocześnie powoli pojawiły się nowe. Był to efekt ekspansji Windows 3.1 - pierwszej popularnej wersji flagowego produktu Microsoft. Jednak prawdziwa eksplozja wirusów nowej generacji nastąpiła po premierze Windows 95 w sierpniu 1995 r. Już na przełomie 1995/96 pojawił się Boza - pierwszy wirus korzystający z nowego systemu plików zastosowanego właśnie w Windows 95. Choć wprawdzie nowe okienka sprawiły, że zniknęło wiele rodzajów wirusów, np. atakujące sektor startowy, to jednak pojawienie się nowego systemu operacyjnego i możliwości nowych programów, głównie Worda i Excela, spowodowały, że autorzy wirusów ochoczo przystąpili do pracy.

Wirusy komputerowe potrzebują, podobnie jak ich biologiczni kuzyni, środowiska, w którym mogą się rozmnażać. Im większe środowisko, tym oczywiście lepiej. W miarę jak rosła popularność czołowych programów Microsoftu, rosło też zainteresowanie nimi autorów wirusów. Wchodzące w skład pakietu Office programy mają bardzo przydatną funkcję - język makropoleceń, który pozwala zautomatyzować pewne czynności. Ów język makropoleceń jest na tyle elastyczny, że pozwala na stworzenie wirusa. Palmę pierwszeństwa dzierżą dwa mikroby: Concept i Laroux. Wirusy "makro" są początkiem zupełnie innej, o wiele niebezpieczniejszej generacji wirusów. Przez lata 90. powstawały coraz bardziej wyrafinowane pomysły, jak przeniknąć przez w miarę szczelną zaporę programów antywirusowych. Ponieważ wzrosła świadomość zagrożenia, jakie stanowią programy nieznanego pochodzenia, autorzy musieli wymyślić inne formy rozprzestrzeniania wirusów. Zaostrzenie się konkurencji na rynku oprogramowania zmusiło wiele firm do coraz częstszego uaktualniania swoich programów i wyposażania ich w nowe funkcje. Takie programy, jak Outlook, nie mówiąc już o Excelu czy Wordzie, posiadają możliwości znacznie przekraczające potrzeby przeciętnego użytkownika. W tej pogoni programiści często tworzyli

buble, albo niechcący niezbyt dobrze zabezpieczali programy. Klasycznym przykładem jest Microsoft Outlook oraz jego skromniejsza, ale dołączana do każdej kopii Windows wersja Outlook Express. Jednym z wynalazków Microsoftu szybko wykorzystanym przez autorów wirusów jest automatyczny podgląd treści listu. Dzięki autopodglądowi e-mail otwierał się automatycznie, nie dając użytkownikowi szans na usunięcie listu przed otwarciem. Funkcja ta przysłużyła się rozpowszechnieniu nowej metody rozsyłania, głównie makro wirusów, pocztą elektroniczną. Jeden z pierwszych zaczął działać w piątek 24 marca 1999 r. Posiadacze kont poczty elektronicznej na całym świecie otrzymali list z załączonym do niego dokumentem Worda. Nie uruchamiał się on sam jak późniejsze wirusy, trzeba było otworzyć dokument. Otwarcie dokumentu było równoznaczne z zainfekowaniem swój komputera wirusem o nazwie Melissa. Ukryty program pobierał adresy pierwszych 50 osób z naszej książki teleadresowej i wysłał do nich mail z dokumentem, w którym znajdował się kod wirusa. W ten sposób Melissa błyskawicznie rozprzestrzeniła się na całym świecie.

Pod koniec lat 90. w Internecie hakerska grupa o nazwie Cult of the Dead Cow (Kult zdechłej krowy) udostępniła pakiet Back Oriffice, przy pomocy którego możliwe jest zdalne zarządzanie komputerem. Składał się on z niewielkiego serwera oraz programu, dzięki któremu z dowolnego miejsca na świecie można połączyć się i pracować na włączonym np. w pracy pececie. W rzeczywistości szybko okazało się, że BO jest klasycznym koniem trojańskim, który pozwalał hakerom wykorzystywać komputer do słynnych ataków DoS (Denial of Service). Ataki polegają na tym, że atakowany serwer stron WWW dostaje tak dużo żądań wyświetlenia strony, aż przestaje działać. W ten właśnie sposób grupa hakerów zablokowała kilka znanych serwisów internetowych, m.in. Yahoo! czy Amazon. W tym czasie, kiedy strony znanych serwisów padały pod atakiem DOS, pojawił się inny groźny wirus: I Love You. Rozprzestrzeniany poprzez pocztę e-mail skutecznie zablokował tysiące serwerów pocztowych na całym świecie.

Przyszłość w robakach internetowych 3 listopada 1988 r. zapamiętali chyba wszyscy ówcześni administratorzy sieci komputerowych w Stanach Zjednoczonych. Gdy przyszli rano do pracy, okazało się, że serwery i sieci, którymi się opiekują, są przeciążone, i to do tego stopnia, że tylko niektórym udało się nawet zalogować. Jednocześnie w pokojach administratorów rozdzwoniły się telefony wściekłych użytkowników. Sprawcą całego zamieszania był robak o nazwie Internet Worm. Stworzył go w ramach eksperymentu młody student Robert Morris - nawiasem mówiąc - syn jednego z wykładowców uniwersyteckich, a później specjalistów CIA. Program Morrisa rzeczywiście pełzał jak robak, zarażając błyskawicznie wszystkie komputery, do których mógł dotrzeć. Całe nieszczęście polegało na tym, że Morris wcale nie chciał zrobić nic złego, ale z powodu błędu w programie jego twórca stracił nad nim zupełnie kontrolę. W ciągu kilku godzin Internet Worm zaraził praktycznie wszystkie podłączone do Internetu amerykańskie komputery. Przez prawie dwa dni, po raz pierwszy i na razie ostatni, Internet praktycznie przestał działać w Stanach Zjednoczonych, bo komputery nie robiły nic innego, tylko przesyłały między sobą listy z wirusem. Robert Morris został skazany na trzy lata ograniczenia wolności i kilkadziesiąt tysięcy dolarów grzywny.

Koncepcja robaków internetowych, których główną cechą jest to, że potrafią infekować inne komputery bez pomocy człowieka, czyli mniej lub bardziej świadomego uruchomienia programu, odżyła pod koniec lat 90. Niestety, teraz przeżywa swój renesans, a przykładem jest kilka naprawdę groźnych robali, takich jak Nimda i Code Red .Fakty mówią same za siebie - Nimda w ciągu jednego tylko dnia zaatakował ponad 2,2 mln serwerów i komputerów na całym świecie. Jeden dzień działania robaka kosztował zaatakowane firmy ponad 500 mln dol. - tyle trzeba było wydać na usunięcie go z komputerów i odtworzenie danych. Według specjalistów Symanteca Nimda i Code Red są robakami nowej generacji, a ich autorzy dość dokładnie przeanalizowali dotychczasowe metody działania robaków i wirusów.

Nimda atakuje wyłącznie serwery działające pod kontrolą Microsoft Internet Information Server, w których administrator nie zainstalował jednej z poprawek bezpieczeństwa programu. Po przejęciu kontroli nad serwerem Nimda działa jak klasyczny robak i próbuje z zaatakowanego serwera wyszukiwać kolejne ofiary. Potrafi również rozprzestrzeniać się, wykorzystując do tego celu pocztę elektroniczną. Kod wirusa zawiera nawet własny serwer pocztowy umożliwiający wysłanie e-maila z nieistniejącego konta pocztowego.

Równie niebezpieczny jest Code Red. Robak umożliwia przeprowadzenie z zainfekowanego komputera ataku typu DoS na wybrany przez autora serwer. W przeciwieństwie do innych rezyduje w pamięci komputera i dlatego początkowo programy antywirusowe nie potrafiły go wykryć. Nie powodował również jak Nimda żadnych zakłóceń w pracy IIS - twierdzą specjaliści z Symanteca.Według Erica Chiena z europejskiego oddziału Symanteca największym zagrożeniem będą właśnie "bledned threats" - robaki internetowe wyposażone w wiele innych funkcji, jak Nimda czy Code Red. Dziś atakują one właściwie tylko serwery i komputery podłączone do Internetu, ale jutro - przewidują w Symantecu - zagrożone będą wszystkie urządzenia w jakikolwiek sposób podłączone do sieci.

3 Rodzaje wirusów

Podziałów wirusów komputerowych jest bardzo dużo. Od strony użytkownika komputera, najważniejsze wydają się podziały ze względu na:

- sposób przenoszenia wirusa
- działanie podejmowane przez wirusa po zainfekowaniu systemu operacyjnego.

Ze względu na sposób przenoszenia można wyróżnić następujące rodzaje wirusów:

- wirusy przenoszące się za pomocą nośników: dyskietki, CD-ROM-y, dyski twarde.
- wirusy doklejające się do programów wykonywalnych: programy systemowe, narzędziowe, czy nawet komercyjne aplikacje.
- wirusy przenoszące się poprzez sieć komputerową: aplety Java, wirusy atakujące usługi sieciowe czy też najbardziej rozpowszechnione robaki internetowe przenoszone przez pocztę elektroniczną.

Ze względu na działania podejmowane po infekcji rozróżniamy:

- niegroźne wirusy wyświetlające zabawne lub dowcipne informacje na ekranie komputera,
- wirusy niszczące informacje zawarte w dokumentach użytkownika i same dokumenty,
- wirusy niszczące wszelkie informacje zawarte na dysku (w tym system operacyjny),
- wirusy powodujące wykasowanie procedur BIOS-u komputera,
- wirusy powodujące uszkodzenie sprzętu komputerowego.

Łagodne wirusy poprzestają jedynie na bezobjawowym replikowaniu się. Inne, wyświetlają na ekranie komunikaty tekstowe lub efekty graficzne. Bardziej złośliwe zawierają procedury destrukcyjne - np. kasowanie plików na dysku twardym. Najniebezpieczniejsze potrafią nie tylko pozbawić użytkownika danych, ale także uszkodzić płytę główna komputera. W czasach, gdy Internet był jeszcze mało dostępy, a dominującym systemem operacyjnym był DOS, typowa infekcja wirusowa zaczynała się od włożenia zainfekowanej dyskietki do stacji dysków i uruchomienia pliku, który był nosicielem mikroba. Wirus instalował się w pamięci RAM i infekował kolejne pliki na dysku twardym i dyskietkach.

Mógł też umieścić własny kod w sektorze rozruchowym dysku twardego (tzw.bootsector), dzięki temu jedna z pierwszych czynności, jakie wykonywał system operacyjny po włączeniu komputera, było uaktywnienie wirusa. Na tym etapie użytkownik zwykle nie zauważał żadnych niepokojących objawów, zresztą jedynym, który mógłby zauważyć, była niewielka zmiana wielkości zakażonych plików, spowodowana dołączeniem do nich kodu wirusa. Bardziej widoczne objawy infekcji pojawiały się najczęściej dopiero w momencie uaktywnienia się procedur destrukcyjnych. Gdyby jednak destrukcja następowała bezpośrednio po zakażeniu, szanse wirusa na powielanie i rozprzestrzenianie swego kodu "genetycznego" byłyby marne. Dlatego złośliwa część kodu zwykle uaktywniała się z pewnym opóźnieniem, np. w Wigilię Bożego Narodzenia. Od momentu zarażenia do wystąpienia objawów mogło, więc minąć wiele miesięcy, podczas których komputer był bezobjawowym nosicielem i czynnym źródłem zakażenia. Wirus komputerowy składa się z dwóch podstawowych części: głowy (jądra) i ogona (ciała). Za głowę uznaje się tę jego część, która uzyskuje sterowanie przebiegiem wykonania programu i służy do samo powielania się. W najprostszym przypadku jest to jedyna część wirusa. Ogon jest opcjonalna częścią i ma za zadanie realizację określonych funkcji (np. wyświetlenie komunikatu czy usunięcie pliku).

3.1 Metody przenoszenia wirusów

3.1.1 Wirusy sektora startowego dysku

Wirusy sektora startowego dysku (wirusy boot sektora, ang. boot sector viruses), to wirusy, których nosicielem jest sektor startowy nośnika danych, takiego jak dysk twardy (MBR - Master Boot Record) czy dyskietka (Boot sector).

Dyski są podzielone na sektory. Pierwszy sektor jest zwany właśnie boot sectorem i w jego skład wchodzi Master Boot Record (MBR). Na początku tego sektora jest zlokalizowany malutki program a na końcu informacje o partycji i tablicy partycji. Ten program wykorzystuje te informacje by określić, która partycja jest bootowalna i z której zastartować. Podczas uruchomiania komputera BIOS odczytuje i egzekwuje właśnie ten pierwszy sektor dyskietki/dysku twardego ładując do pamięci potrzebne informacje z MBR. I dopiero po tym procesie następuje załadowanie systemu plików (FAT/NTFS...). Należy mieć świadomość, że każda sformatowana dyskietka, nawet nie zawierająca plików systemowych, posiada boot sektor, a więc jako taka może zawierać wirusa.

Jest to jeden z najgorszych rodzajów wirusów, który dewastuje boot recorda. Tego typu wirusów nie niszczy nawet format! Dlaczego? Właśnie dlatego, że ukrywają się w 1-szym sektorze dysku i podczas uruchamiania komputera są ładowane przez BIOS do pamięci PRZED załadowaniem systemu plików. To daje im kontrolę nad wszystkim. Gdy już umiejscowią się, tam gdzie było zaplanowane infekują boot sektory każdej dyskietki, która została uruchomiona na komputerze!

Wirusy tego typu transportują się poprzez dyskietki. Pliki na dyskietkach nie są szkodliwe, ale oryginalny boot record dyskietki został zastąpiony przez wirusa. I jeśli nieświadomy użytkownik umieści taką zakażoną dyskietkę w swoim napędzie i zrestartuje komputer wirus się aktywuje umieszczając swoją kopię w obszarze MBR dysku twardego i wykazując gotowość do zarażania kolejnych dyskietek nie zabezpieczonych przed ponownym zapisem. Bardzo rzadkim przypadkiem jest zakażenie przez ściągnięte pliki exe niemniej nie jest to niemożliwe.

W innym przypadku wirus przenosi kod inicjujący system z sektora startowego w inny obszar dysku i zajmuje jego miejsce, co powoduje jego załadowanie jeszcze przed (!) startem systemu, a więc także przed uruchomieniem jakiegokolwiek oprogramowania antywirusowego. Działanie tego typu umożliwia wirusom przejęcie kontroli nad oprogramowaniem przeznaczona do ich zwalczania.

Naprawić zakażony dysk można używając komendy programu *fdisk*:
fdisk /MBR

Nie zawsze jednak takie działanie okazuje się skuteczne i najbezpieczniejszą metodą jest wykorzystanie oprogramowania antywirusowego w kombinacji z czystą, nie zainfekowaną dyskietką startową. Ta dyskietka jest potrzebna by zastartować komputer ze źródła zewnętrznego "na czysto" (do pamięci załaduje się czyściutki boot record dyskietki). Oczywiście są też narzędzia, których można użyć bezpośrednio spod Windows gdyż mają one wbudowane specjalne mechanizmy zabijania wirusa w pamięci. Dyskietki startowe muszą być utworzone na komputerze NIE zainfekowanym i muszą być zabezpieczone przed ponownym zapisem! Startujemy z nie zakażonej czystej dyskietki zabezpieczonej przed zapisem lub bootowalnego CD Antywirusa i usuwamy stosownym narzędziem.

Należy mieć świadomość ze Boot Sector znajduje się na każdej sformatowanej dyskietce, także w przypadku, gdy nie zawiera ona żadnych plików systemowych. Wobec tego czysta dyskietka znajdująca się w napędzie podczas uruchamiania systemu może być przyczyna kłopotów, nawet jeżeli zobaczymy na ekranie tylko komunikat: "Non-System disk or disk error".

3.1.2 Wirusy plikowe

Wirusy plikowe (ang. file viruses), ten rodzaj wirusów jest najszerzej rozprzestrzeniony na świecie i najczęściej spotykany. Wirusy tego rodzaju wykorzystują swoje ofiary do transportu modyfikując ich strukturę wewnętrzną. Często pliki używane do transportu przez wirusy pasożytnicze są trwale niszczone, a jedynym ratunkiem jest użycie szczepionki lub kopii zapasowych, ponieważ zarażane pliki z reguły nie są przez wirusa leczone.

Każdy wirus przed dokonaniem szkód najpierw ulega replikacji. Rozwój technik przenoszenia wirusów wiąże się z wynajdywaniem nowych nosicieli. Początkowo na atak wirusów tego typu narażone były tylko pliki wykonywalne (*.exe, .com) oraz wsadowe (*.bat). Rozwój technologii wirusów powiększył grono zagrożonych plików o zbiory zawierające fragmenty kodu, biblioteki, sterowniki urządzeń (*.bin, *.dll, *.drv, *.lib, *.obj, *.ovl, *.sys, *.vxd).

Infekcja następuje poprzez dopisanie kodu wirusa do pliku nosiciela. Załadowanie zainfekowanego pliku do pamięci jest równoznaczne z uaktywnieniem wirusa. Wiele wirusów nie niszczy zaatakowanego pliku, dzięki czemu może po aktywacji wykonać program nosiciela, tak że użytkownik niczego nie podejrzewa.

Wirusy pasożytnicze można podzielić ze względu na zajmowane przez nie miejsce w zainfekowanych plikach na:

Wirusy **nadpisujące** (ang. Overwrite infectors), lokujące się na początku pliku, często prowadzące do nieodwracalnych zmian, ponieważ z reguły nie zapamiętują zawartości pliku przed zainfekowaniem**.**

Wirusy lokujące się na **końcu pliku** (ang. End of file infectors), jest to najbardziej rozpowszechniona odmiana wirusów, modyfikują one pewne ustalone struktury na początku pliku tak, aby wskazywały na wirusa, po czym dopisują się na końcu pliku.

Wirusy **nagłówkowe** (ang. Header infectors), lokują się w nagłówku plików EXE przeznaczonych dla DOSa.

Wirusy lokujące się w pliku w miejscu gdzie jest jakiś **wolny obszar** (wypełniony ciągiem zer), który można nadpisać nie niszcząc pliku (ang. Cave infectors).

Wirusy lokujące się w **dowolnym miejscu pliku** (ang. Surface infectors), występują dość rzadko, co jest pewnie wynikiem tego, że trzeba posiadać duże umiejętności, aby je napisać.

3.1.3 Wirus towarzyszący

Najprostsza forma wirusa w sensie sposobu zadomowienia się w systemie jest wirus towarzyszący. Jego działanie opiera się na DOS-owskiej kolejności uruchamiania plików o tej samej nazwie. Jeśli podana zostanie nazwa zbioru bez podania rozszerzenia, wówczas system szuka najpierw pliku z rozszerzeniem.COM, następnie .EXE a na końcu .BAT . Wirus towarzyszący odszukuje plik .EXE lub .BAT, dla którego nie istnieje zbiór z ta sama nazwa, ale z innym rozszerzeniem .COM, po czym tworzy zainfekowanego .COM-a. Próba załadowania programu bez podania rozszerzenia zakończy się wczytaniem wirusa. Także w tym przypadku właściwy plik może zostać uruchomiony dla niepoznaki w dalszej kolejności. "Okienkowa" wersja wirusa towarzyszącego podmienia jedna z systemowych bibliotek DLL, autentyczna zapisując pod zmieniona nazwa. Odwołanie się do funkcji z podstawionej biblioteki najpierw uaktywnia wirusa, a dopiero potem wywołuje żądaną funkcję z oryginalnego DLLa.

3.1.4 Wirusy FAT

Wirusy FAT (wirusy tablicy alokacji plików, link/FAT viruses): do replikacji wirusy mogą także wykorzystywać Jednostki Alokacji Plików (JAP), na jakie tablica FAT dzieli DOS-ową partycję dysku twardego. W celu uzyskania dostępu do pliku DOS odszukuje w FAT numer jego pierwszej jednostki alokacji, po czym kolejno (zgodnie z FAT) wczytuje wszystkie jednostki zajmowane przez plik.

Wirusy atakujące JAP zmienia wartość pierwszej JA jednego lub wielu plików na numer wskazujący JA kodu wirusa. Wczytanie takiego pliku powoduje uruchomienie wirusa, który w dalszej kolejności może, ale nie musi, załadować właściwy program (w tym celu musi zapamiętać oryginalny numer jego pierwszej JAP).

3.1.5 Makrowirusy

Najmłodszą rodziną wirusów są tzw. makrowirusy, które pojawiły się jako skutek uboczny rozszerzenia możliwości pakietów biurowych, takich jak Microsoft Office, a także Lotus SmartSuite oraz Corel WordPerfect Suite językiem pozwalającym na tworzenie makr. Języki Word Basic, a potem Visual Basic for Applications wywodzące się jeszcze od prostego Basica, mają na tyle duże możliwości, ze pozwalają na stworzenie wirusa. Dzięki temu twórcy wirusów zostali wyposażeni w nowe łatwe narzędzie. Napisanie wirusa nie wymaga już zaawansowanej znajomości assemblera, ponieważ można posłużyć się językiem wysokiego poziomu(Turbo Pascal, C, VBfA). Najczęściej spotykane makrowirusy MS Worda wykorzystują fakt, że szablony dokumentów mogą zawierać makra. Zazwyczaj wirus uaktywnia się w chwili otwarcia zainfekowanego szablonu w środowisku aplikacji MS Word, następnie zaraża zdrowe zbiory z rozszerzeniem .doc i zapisuje je jako szablony, ponieważ dokumenty nie mogą zawierać makr. W ostatnim kroku jedno lub kilka automatycznie wykonywanych makr np. AutoOpen, FileSaveAs, zostaje zastąpionych kodem wirusa. Co prawda, standardowo szablony używają rozszerzenia .DOT w odróżnieniu od .DOC zarezerwowanego dla dokumentów. Nie ma jednak przeszkody, aby szablon również miał rozszerzenie .DOC i udawał dokument. Następnym razem użytkownik otwierając plik , nie zdaje sobie sprawy ze faktycznie jest to zainfekowany szablon. Łakomym kaskiem dla makrowirusa jest szablon NORMAL.DOT zawierający makra globalne. Po jego zarażeniu wirus może uaktywniać się wraz z każdym uruchomieniem Worda i przenosi się na wszystkie tworzone lub otwierane dokumenty. Znany jest także wirus o nazwie

WORDMACRO.NUCLEAR, który oprócz zarażania dokumentów Worda potrafi umieścić w pamięci rezydentnego wirusa Ph33r atakującego pliki .COM i .EXE. Przysługę wirusowi może oddać przeglądarka internetowa, która po załadowaniu pliku .DOC z serwisu WWW automatycznie uruchamia Worda w celu otwarcia dokumentu, ryzykując przy tym infekcje. Po pojawieniu się makrowirusów Worda było tylko kwestia czasu stworzenie ich klonów, atakujących w ten sam sposób dokumenty Exela i Accessa, a także aplikacji wchodzących w skład pakietów biurowych firm Corel i Lotus. Ponadto istnieją już wirusy mające zdolność infekowania dowolnego dokumentu z pakietu Microsoft Office.

3.2 Działania wirusów

Aby wirus przetrwał i jednocześnie zainfekował jak największa liczbę komputerów, jego obecność musi pozostać niezauważona możliwie jak najdłużej. Siłą rzeczy, najczęściej skutkiem jego działalności jest tylko nieodczuwalne nadszarpnięcie zasobów komputera w postaci "kradzieży" kilkuset bajtów pamięci operacyjnej i niewielkiej ilości miejsca na dysku. Czasem wystarcza to do obniżenia stabilności systemu. Kariera mikrobów siejących spustoszenie jest zazwyczaj bardzo krótka, ponieważ wykrywane są szybko, zanim się jeszcze nadmiernie rozprzestrzenia. Prawdziwym problemem są wirusy, które replikują się przez długi czas niezauważone, a ich nieprzyjemne skutki ujawniają się dopiero w określonych okolicznościach.

Za prawdziwa plagę należy uznać wirusy wychodzące spod rak mniej wprawnych programistów. Często nieudolnie napisane powodują niezamierzone skutki uboczne w wyniku błędów w kodzie źródłowym. Łatwo je wykrywać i unieszkodliwić, ale jeśli już dojdzie do infekcji, to rzadko udaje się naprawić zarażone pliki. Tak naprawdę do tworzenia wirusów nie jest potrzebna żadna wiedza, jeżeli wykorzysta się do tego jeden z generatorów wirusów, których wiele znaleźć można w Internecie. Ich obsługa sprowadza się do wyboru funkcji udostępnianych w menu. Czasem można wpisać tylko tekst, wypisywany przez wirusa na ekranie jako rezultat infekcji, ale niektóre generatory pozwalają określić rodzaj zarażonych plików i dołączyć własne procedury. Na szczęście stworzone w ten sposób wirusy są zwykle na tyle charakterystyczne, że skanery antywirusowe dają sobie z nimi radę bez większego problemu.

Zasada działania wirusów uzależniona jest od inwencji twórców. Możemy w nich wyróżnić trzy podstawowe fazy. Pierwsza faza występuje zawsze, natomiast moment wykonania dwóch pozostałych jest dowolny.

Faza 1 – aktywacja: jest to uruchomienie głowy wirusa. W przypadku wirusów sektora startowego polega na uruchomieniu komputera z zarażonego nośnika, natomiast w przypadku wirusów plikowych jest to uruchomienie zainfekowanego programu. Faza ta jest obligatoryjna i po jej zakończeniu wirus może zakończyć swoja działalność.

Faza 2 – destrukcja: polega na dokonaniu zniszczeń w systemie (np. usunięcie plików). Jest to najniebezpieczniejsza cześć działalności wirusa. Faza ta jest opcjonalna, a niektóre wirusy na tym etapie kończą swoje działanie.

Faza 3 – ujawnienie: polega na poinformowaniu użytkownika o obecności niechcianego programu (np. odegranie melodyjki czy wyświetlenie komunikatu). Faza ta jest opcjonalna.

Główne symptomy wniknięcia wirusa do systemu są następujące:

- Uruchamianie niektórych programów jest znacznie wolniejsze.

- Niektóre pliki (w szczególności te, które są uruchamiane) zwiększają swój rozmiar.
- Nowe pliki nieznanego pochodzenia pojawiły się w komputerze.
- Ilość wolnej pamięci RAM zmniejszyła się z nieznanych powodów.
- Występują nieoczekiwane komunikaty lub dźwięki.
- System staje się niestabilny.
- System nagle się resetuje.

3.2.1 Bomby logiczne

Bomba może pozostać w ukryciu przez długi czas, swoje działanie ukazuje w określonym odpowiednimi warunkami czasie (najczęściej zależne od aktualnej daty lub liczby poprzednich wywołań programu). Kod może być ukryty w dowolnym miejscu programu zawierającego bombę, więc należy ostrożnie obchodzić się z aplikacjami pochodzenia nieznanego. Bomba logiczna może badać, którzy użytkownicy są zalogowani lub, jakie programy są w danej chwili używane w systemie. Raz zaktywizowana, bomba logiczna może doprowadzić do zniszczenia lub zmiany danych, spowodować zawieszenie urządzenia lub w jakiś inny sposób uszkodzić system.

Co pewien czas media ostrzegają przed wyjątkowo destrukcyjnym wirusem, który uaktywni się w chwili wybicia ustalonej godziny. Jak do tej pory takie alarmy wzbudzały tylko przerażenie wśród słabiej wyedukowanych jednostek społeczności informatycznej i zwiększały nakład czasopism branżowych.

3.2.2 Fałszywki

Fałszywki (ang. haoxy), to inaczej ostrzeżenia przed nieistniejącymi wirusami. Cecha charakterystyczna fałszywego ostrzeżenia jest prośba o przesłanie go do możliwie dużej liczby osób - rzekomo w trosce o ich bezpieczeństwo. Początkujący Internauci, rozsyłają fałszywe alarmy, do kogo się tylko da, co pozwala hoaxom krążyć po Internecie całymi miesiącami, w milionach egzemplarzy, doprowadzając do wściekłości osoby, które otrzymują je po raz n-ty. Pamiętajmy by nie rozsyłać fałszywych alarmów! Jeśli trafi do nas ostrzeżenie, wystarczy wejść na stronę dowolnego producenta programów antywirusowych i sprawdzić tam, czy nie jest to hoax. Wygodnym rozwiązaniem jest zaprenumerowanie e-mailowego biuletynu na temat wirusów. Godny polecenia jest polskojęzyczny biuletyn MKS-a. Raz na parę dni do naszej poczty e-mailowej trafi wiarygodny raport o nowych wirusach oraz zbliżających się datach uaktywnienia się niebezpiecznych mikrobów atakujących z opóźnieniem. Autorzy biuletynu bezlitośnie demaskują też krążące po sieci hoaxy!

Możemy również otrzymać emaila z wiadomością, że plik o podanej nazwie jest wirusem i można się go pozbyć jedynie poprzez usunięcie tego pliku. W rzeczywistości plik nie jest wirusem i może być nawet częścią systemu operacyjnego, a jego usunięcie może spowodować nieprzewidziane skutki. Użytkownik najczęściej zastosuje się do wskazówek zawartych w otrzymanej wiadomości i w dobrej wierze rozpowszechni ja dalej (w przypadku maili spowoduje to niepotrzebny wzrost generowanego w sieci ruchu). Oprócz wywołania zamieszania fałszywki mogą również przyczynić się do poniesienia szkód (np. otrzymanie wiadomości o awarii serwera i prośbie o wysłanie hasła do konta na podany adres). Walczyć z takimi fałszywymi alarmami jest szczególnie trudno gdyż nigdy nie ma 100% pewności czy są one prawdziwe czy nie. Najlepiej jest mieć ograniczone zaufanie do podejrzanych i pochodzących z niepewnych źródeł wiadomości i sprawdzać ich wiarygodnosć w serwisach antywirusowych.

3.2.3 Konie trojańskie

Koń trojański nie jest wirusem komputerowym, ale ze względu na swoje działanie często bywa z nim utożsamiany. Uruchamiany wykonuje niby normalna pracę, wynikającą z przeznaczenia programu, lecz dodatkowo, niejako w tle, od razu po uruchomieniu wykonuje jakieś niezauważalne dla użytkownika operacje (niszczy, kasuje, zamazuje dane na dysku, może również wykradać hasła i przesyłać je do autora trojana lub brutalnie sformatować dysk). Konie najczęściej przenoszą się w plikach udających nowe, popularne programy kompresujące (np.: ZIP, ARJ, RAR) lub też udają programy narzędziowe do obsługi dysków. Może ukrywać się również np. w pożytecznym (na pozór) oprogramowaniu, jak np. program antywirusowy czy przeglądarka plików graficznych. Jak widzimy konie trojańskie znajdują się właśnie w takich programach i dlatego też użytkownik sam je sobie instaluje i korzysta z nich, nieświadomy tego, co może go spotkać. Można powiedzieć, że trojan to - zwykły program, który został zmieniony poprzez wstawienie miedzy jego linijki niechcianego kodu i właśnie ten kawałek kodu spełnia nie znane użytkownikowi funkcje.

Większość nowych trojanów posiada opcje, dzięki którym zostaniemy powiadomiony e-mailem o tym, że ofiara uruchomiła serwer (zarażony plik) na swoim komputerze. Otrzymamy też numer IP ofiary oraz inne informacje. Oczywiście możemy zdefiniować adres e-mailowy, na który mają być przysyłane te informacje. Prawie każdy nowszy trojan pozwala na manipulowanie plikami na komputerze ofiary. Użytkownik może przeglądać, kasować, przenosić, wysyłać, ściągać, uruchamiać pliki na cudzym komputerze. Trojony mają wiele więcej niebezpiecznych opcji. Uruchamia się je odpowiednim przyciskiem za pomocą, którego można przykładowo sformatować dysk twardy ofiary. Inna niebezpieczna funkcja to możliwość uruchomienia serwera FTP na dysku ofiary i otworzenia portów, co pozwoli wszystkim innym użytkownikom sieci na ściąganie, wgrywanie czy uruchamianie plików z komputera ofiary. Posiadają też mniej złośliwe opcje, takie jak ukrycie wskaźnika myszy, przejęcie kontroli nad myszka, restart Windows, wyświetlenie rysunku itp. Nie są one szkodliwe, ale mogą przeszkadzać użytkownikom w normalnej pracy. Uruchomienie zarażonego pliku powoduje otworzenie specyficznego portu i nasłuchiwanie na połączenie z zewnątrz.

Trojan może używać protokołu TCP lub UPD. Jeśli już połączymy się z IP ofiary możemy wtedy robić z jego komputerem, co tylko chcemy, pozwala na to serwer, który ofiara uruchomiła na swoim komputerze. Coraz więcej trojanów uruchamia się ponownie przy każdym restarcie Windows lub wyłączeniu komputera. Modyfikują pliki win.ini lub system.ini, dzięki czemu trojan może się uruchamiać po każdym załadowaniu Windows, większość trojanów modyfikuje jednak rejestr, aby uzyskać ten efekt. Trojan to bardzo niebezpieczna zabawka. Ktoś może dowiedzieć się wielu rzeczy o Nas.

3.2.4 Robaki

Robaki (ang. worms) to programy, które podobnie jak wirusy mogą zawierać procedury destrukcyjne i z łatwością mogą zniszczyć dane zgromadzone na dysku twardym. Robaki są najbardziej popularne w sieciach, gdzie maja do dyspozycji protokoły transmisji sieciowej, dzięki którym mogą przemieszczać się po całej sieci. Do prawidłowego funkcjonowania nie potrzebują nosiciela (wytwarzając swoje dokładne kopie). Rozmnażają się samoistnie i w sposób ciągły, powodując w bardzo krótkim czasie wyczerpanie zasobów systemu. Wirusy tego typu są zdolne w bardzo krótkim czasie sparaliżować nawet dość rozległa sieć komputerowa. Są uruchamiane przez nasza nieostrożność, bądź niewiedzę. Po uruchomieniu wykorzystują np. adresy osób z książki adresowej programu pocztowego i wysyłają do nich swoje kopie.

3.2.5 Bakterie

Bakterie (ang. bactery), zwane także królikami (ang. rabbits), to programy, które w zasadzie nie niszczą plików. Ich jedynym celem jest samokopiowanie. Typowy program w rodzaju bakterii może nie robić nic więcej niż jednoczesne uruchomienie dwóch swoich kopii w systemach wieloprogramowych lub stworzenie dwóch nowych plików, z których każdy jest kopia oryginalnego pliku źródłowego bakterii. Oba programy mogą następnie skopiować się podwójnie itd. Bakterie reprodukują się wykładniczo, zabierając ostatecznie cała moc obliczeniowa procesora, pamięć lub wolny obszar pamięci dyskowej, uniemożliwiając użytkownikowi dostęp do tych zasobów. Ten rodzaj ataku jest jedna z najstarszych form zaprogramowanych zagrożeń. Użytkownicy niektórych z najwcześniejszych urządzeniach wieloprocesorowych używali tych programów w celu zawieszenia pracy danego urządzenia lub po prostu by zobaczyć, co się stanie. Na taka formę ataku są szczególnie narażone urządzenia nie posiadające ograniczeń wykorzystania zasobów i ograniczeń w stosunku do użytkowników.

3.3 Wirusy polimorficzne i wirusy typu stealth

W zasadzie wszystkie wymienione wcześniej wirusy mogą, choć nie muszą, należeć do tej grupy. Ich powstanie związane jest z postępem w dziedzinie wykrywania wirusów. W pierwszych latach obecności wirusów każdy miał swoją sygnaturę (charakterystyczny tylko dla siebie ciąg bajtów). Sytuacja zmieniła się, gdy Bułgar o pseudonimie Dark Avenger opracował metodę pozwalającą tworzyć wirusy samomutujące się, czyli wirusy polimorficzne. Nie mają one stałej sygnatury, ponieważ ich kod zmienia się samoczynnie przy każdej infekcji.

Wirusy polimorficzne są trudne do wykrycia, ponieważ ich różne próbki nie wyglądają tak samo. Często dwie próbki tego samego wirusa polimorficznego nie mają ze sobą nic wspólnego. Ten polimorfizm może być osiągnięty poprzez zakodowanie ciała wirusa lub przy użyciu różnych dekoderów.

Wirusy typu stealth natomiast, to wirusy, które przechwytują odwołania systemu operacyjnego do zainfekowanych plików lub sektorów dysku i zastępują dane, które byłyby widziane, jeśli pliki lub sektory nie były zainfekowane. Poprzez te działania wirusy ukrywają swoją obecność.

Stealth boot virus jest typowym przedstawicielem tej grupy wirusów, z jednym interesującym wyjątkiem. Mianowicie wirus ten tworzy swoje własne MBR, ale nie niszczy zdrowego tylko je przesuwa w inny rejon. Kiedy uruchamia się narzędzie do skanowania boot sectora w celu namierzenia wirusa, wirus "odsyła" program do prawdziwego sektora. Antywirus wierzy, iż skanuje prawdziwe MBR i nie widzi problemu, a w rzeczywistości jest skanowany zdrowy, lecz przesunięty i w związku z tym fałszywy boot record.

Wirusa takiego, antywirus może zobaczyć i usunąć tylko wtedy, gdy nie jest on aktywny w pamięci. Czyli sprowadza się to do czystego zbootowania z czystej dyskietki.

3.4 Wirusy rezydentne (ang. resident viruses)

Zasada działania tych wirusów polega na zainstalowaniu się w pamięci operacyjnej komputera i przejęciu odpowiednich odwołań do systemu w sposób podobny jak czynią to programy typu TSR (Terminate but stay Resident). Typowy wirus rezydentny po zainstalowaniu ukrywa swój kod przed programami przeglądającymi pamięć. Aktywny i jednocześnie ukryty w pamięci, ma o wiele szersze pole manewru niż wirusy nie rezydentne. Monitorowanie odpowiednich funkcji DOS i BIOS pozwala mu przy każdej dowolnej próbie dostępu na infekcje plików lub sektorów. Możliwe jest także zastosowanie techniki zaawansowanego ukrywania się w systemie (patrz opis wirusów stealth). Zawładnięcia

systemu dokonuje się poprzez przejęcie odpowiednich przerwań sprzętowych i funkcji obsługiwanych przez ogólnie dostępne przerwania programowe.

Wirusy rezydujące w pamięci przerywają swą działalność tylko, gdy użytkownik wyłączy lub zresetuje zainfekowany system. Wirusy nie rezydujące w pamięci nie infekują pamięci RAM i są aktywne tylko przez ograniczony czas. Niektóre wirusy umieszczają w pamięci RAM małe, rezydentne programy, które nie są odpowiedzialne za rozprzestrzenianie wirusa.

Ze względu na szybkość mnożenia się wirusy rezydentne dzielą się na szybkie infektory i wolne infektory.

Szybkie infektory przejmują wszystkie możliwe funkcje systemu DOS, używane do obsługi plików i zarażają wszystko, co jest możliwe, w maksymalnie krótkim czasie, co powoduje, iż po okresie bardzo szybkiej ekspansji wirusa w danym systemie następuje jego pasywacja, gdyż wirus nie może znaleźć kolejnej ofiary do zarażenia. Często pierwsza czynnością wykonywana przez wirusa jest zniszczenie w pamięci kodu zamazywanej części interpretatora poleceń, co sprawia, że przy następnym wywołaniu jakiegokolwiek polecenia z poziomu DOS plik zawierający interpretator poleceń (czyli najczęściej COMMAND,COM) zostanie ponownie uruchomiony i w efekcie natychmiast zainfekowany. Duża aktywność szybkiego infektora będzie na pewno łatwo zauważalna dla użytkownika.

Wolne infektory – ich celem w przeciwieństwie do szybkich infektorów nie jest szybka ekspansja w systemie, lecz raczej jak najdłuższe przetrwanie. Wirusy te używają najczęściej wolnych, kilkustopniowych, zmiennych procedur szyfrujących i techniki stealth. Infekują najczęściej tylko takie obiekty, które modyfikuje lub tworzy użytkownik, a więc nawet w przypadku sygnalizowania jakiejś niebezpiecznej operacji przez ewentualny program antywirusowy użytkownik będzie przekonany, iż potwierdza wykonywane przez siebie czynności. Są to wirusy bardzo trudne do wykrycia i usunięcia, nawet przez bardzo zaawansowane programy antywirusowe.

4 Jak się bronić?

Podstawową zasadą jest posiadanie dobrego pakietu antywirusowego. Pakietu, gdyż obecnie większość tego typu programów składa się z wielu modułów o różnych funkcjach. Programy antywirusowe są najsilniejszym narzędziem, jakie powstało w celu walki z wirusami. Od momentu pojawienia się pierwszego wirusa powstał cały szereg różnorodnego oprogramowania. Istniejące i ciągle rozwijające się programy ułatwiają ochronę systemu przed inwazją, szybkie jej wykrycie i w większości przypadków usunięcie skutków.

Programy antywirusowe możemy podzielić na następujące grupy funkcjonalne:

Blokery - są to jedyne programy, próbujące przeciwdziałać inwazji. Zasadą ich działania jest monitorowanie poczynań uruchamianych programów i w przypadku odkrycia "podejrzanych" operacji alarmowanie użytkownika i pozostawianie mu decyzji o dalszym działaniu. Jest to znakomita metoda, ale jak każda posiada oczywiście swoje wady. Jedną z nich jest przede wszystkim mała skuteczność, gdyż nowe wirusy bardzo często posiadają mechanizmy uniemożliwiające wyodrębnienie z nich operacji "podejrzanych". Kolejną wadą jest zajmowanie części zasobów komputera - pamięci operacyjnej oraz obciążanie w jakimś stopniu procesora. Ostatnią wadą jest to, iż programy owe mają tendencję do częstego "mylenia się", co związane jest z "fałszywym alarmem".

Programy diagnostyczno-leczące - ta grupa programów opiera się na poszukiwaniu na dysku i w pamięci znanych już wirusów i w przypadku wykrycia (na podstawie charakterystycznych sygnatur zawartych w plikach) - usuwaniu skutków infekcji. Są to programy najczęściej stosowane i chyba najbardziej przydatne w profilaktyce. Niestety są nieskuteczne w przypadku zainfekowania nieznanym wirusem bądź wtedy, gdy wirus zadziała natychmiast po zainfekowaniu komputera i dokona nieodwracalnych zniszczeń. Bardzo ważne jest także, aby skaner wykorzystywał najnowsze metody wyszukiwania, takie jak np. heurystyczna metoda wykrywania wirusów - chroni przed wirusami polimorficznymi, polega na analizie kodu pliku i symulacji jego wykonania. Pozwala na wykrycie operacji charakterystycznych dla wirusów, takich jak np. próba bezpośredniego dostępu do dysku.

Programy sprawdzające sumy kontrolne plików - istotą tej grupy programów jest zakładanie bazy danych, zwierających pewne cechy zbiorów dyskowych i newralgicznych obszarów dysków. Te programy, przez systematycznym stosowaniu, umożliwiają wykrycie źródła infekcji, a czasem odzyskanie pozornie bezpowrotnie straconych informacji. Dodatkowo oprogramowanie antywirusowe powinno umożliwiać generowanie raportów z bieżącej pracy.

Co zrobić w przypadku zarażenia wirusem?

Przede wszystkim sprawdzić na stronie producenta programu antywirusowego, czy posiadamy najnowszą bazę wirusów. Jeśli nie, należy niezwłocznie ściągnąć ją i zainstalować w komputerze.

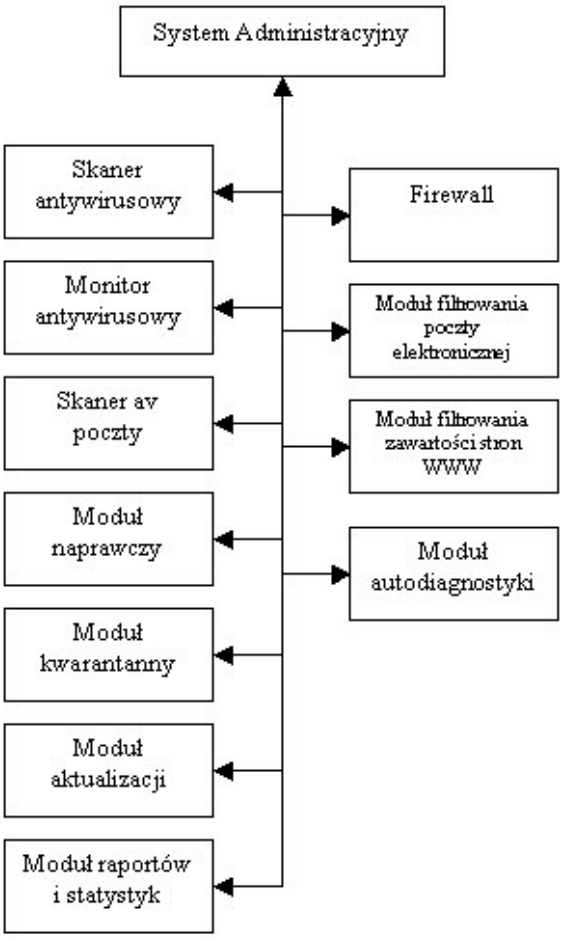
Użyć innego programu antywirusowego, jeśli mamy taką możliwość. W przypadku zarażenia robakiem internetowym rozsyłanym przez pocztę elektroniczną, należy odłączyć się od sieci komputerowej, co przerwie rozsyłanie wirusa dalej.

Przeczytać, co do tej pory wiadomo na temat tego wirusa: co robi, jak go usunąć. Tego typu informacje udostępniane są przez producentów oprogramowania antywirusowego.

5 Jak działa program antywirusowy

Praca programu antywirusowego polega na sprawdzaniu kodu wchodzącego do komputera lub takiego, który ma być za chwilę wprowadzony. Programy antywirusowe obserwują również pracę działających programów i w chwili zauważenia ich niewłaściwego zachowania podejmują działania obronne.

Programy antywirusowe składają się z wyspecjalizowanych bloków funkcjonalnych, które współpracują ze sobą zarządzane przez **system administracyjny** (Rysunek 1).



Rysunek 1

Na rysunku 1 przedstawione są moduły stanowiące elementy składowe programów antywirusowych. Elementy znajdujące się po lewej stronie rysunku stanowią składowe "tradycyjnych" programów antywirusowych, natomiast elementy znajdujące się po prawej stronie pojawiły się w wyniku wzrostu zagrożenia komputerów osobistych, w szczególności po podłączeniu ich do Internetu.

Modułowa budowa programów antywirusowych umożliwia tworzenie narzędzi przeznaczonych do specjalizowanych zadań. Osiąga się w ten sposób zwiększenie skuteczności i efektywności pracy przy jednoczesnym zminimalizowaniu zapotrzebowania na zasoby systemu. Przykładem może być tworzenie oddzielnie **monitora antywirusowego** i **skanera poczty elektronicznej**. W momencie, gdy nie odbieramy bądź nie wysyłamy poczty **skaner pocztowy** może pozostać dezaktywowany natomiast, gdy zaczynamy wykonywać którąś z tych czynności jest on automatycznie uruchamiany.

Głównym składnikiem odpowiedzialnym za pracę programu jako całości jest **system administracyjny** - z nim użytkownik ma kontakt zarówno podczas konfiguracji programu, jak i decydując o losach podejrzanych plików. System ten stanowi interfejs pośredniczący pomiędzy użytkownikiem a pozostałymi częściami programu oraz zapewnia wymianę informacji pomiędzy poszczególnymi jego modułami.

System administracyjny może oferować następujące funkcje:

- automatyczna i ręczna aktualizacja baz sygnatur wirusów i oprogramowania,
- harmonogram zadań,

- skanowanie na żądanie wybranych napędów, katalogów i plików,
- raporty i statystyki z działania programu,
- włączanie i wyłączanie oraz konfiguracja monitora antywirusowego,
- włączanie i wyłączanie oraz konfiguracja zasad filtrowania poczty elektronicznej,
- włączanie i wyłączanie oraz konfiguracja zasad filtrowania zawartości stron internetowych,
- pomoc do programu - może być off-line (jej źródła znajdują się na komputerze użytkownika) i on-line (dostępna w sieci Internet).

Dodatkowo w systemie administracyjnym, w zależności od programu, mogą się znaleźć następujące opcje:

- konfiguracja dodatkowych usług świadczonych przez producenta,
- przesyłanie informacji lub podejrzanego pliku do laboratorium producenta.

W przypadku wdrożenia sieciowych rozwiązań antywirusowych administracja programami na poszczególnych komputerach w sieci może odbywać się z jednego centralnego miejsca w sieci - serwera administracyjnego. Pozwala to zredukować koszty zarządzania oprogramowaniem antywirusowym, jak również przeprowadzać czynności administracyjne bez konieczności przerywania pracy użytkownikowi. W rozwiązaniach sieciowych oprogramowanie instalowane na komputerach-klientach umożliwia użytkownikowi jedynie wybór skanowania na żądanie wybranych plików, folderów i dysków. Pozostałe możliwości programu są dla niego niedostępne; użytkownik otrzymuje tylko informacje o decyzji odnośnie do zainfekowanego pliku, jaką podjął administrator.

5.1 Skaner antywirusowy

Skaner antywirusowy, zwany również "skanerem na żądanie", sprawdza na żądanie wskazane pliki, foldery, lub dyski. Skanery mogą być uruchamiane również automatycznie o wcześniej zaplanowanych porach, poprzez odpowiednią konfigurację funkcji harmonogramu. Możliwe jest również wywoływanie skanowania w czasie, gdy system nie wykonuje innych zadań.

Skanery antywirusowe przyglądają się plikom zapisanym w systemie i szukają sygnatur znanych wirusów, które są charakterystycznym ciągiem bitów dla danego programu złośliwego. Poniżej zostały przedstawione przykładowe sygnatury:

B8 ED FE CD 21 A3 03 01 0E 8F 06 6F 01 BA	sygnatura wirusa Atomie 1.0
5D 83 ED 03 E8 15 00 EB 27 90 E8 OF 00 B4	sygnatura wirusa Ethernity
BE 30 01 8B 16 17 01 B9 35 01 2E 31 14 83	sygnatura wirusa Human Greed
5D 81 ED 03 01 EB 1B 90 B8 24 35 CD 21	sygnatura wirusa OLG

Jeżeli zostanie znaleziony podejrzany plik, skaner przekazuje informację o znalezieniu wirusa do systemu administracyjnego, który pozwala podjąć użytkownikowi decyzję, co zrobić z podejrzanym plikiem. W przypadku korzystania z rozwiązań korporacyjnych, decyzje o dalszym losie pliku może zależeć od administratora systemu, natomiast użytkownik zostanie jedynie o niej poinformowany.

Skanery antywirusowe mogą również posługiwać się bardziej złożonymi metodami wykrywania wirusów niż wyszukiwanie sygnatur. Do metod tych możemy zaliczyć: analizę heurystyczną, skanowanie rekurencyjne zarchiwizowanych plików, wykrywanie wirusów makr i polimorficznych, przeprowadzanie leczenia zainfekowanych obiektów oraz dekodowanie plików używających słabych algorytmów kodujących i sprawdzanie czy w skanowanych obiektach nie zaszły zmiany.

5.2 Monitor antywirusowy

Praca **monitora antywirusowego** polega na skanowaniu obiektów podczas każdego dostępu i monitorowaniu działania systemu. W przypadku wykrycia infekcji lub niepożądanych działań monitor blokuje dostęp do podejrzanego obiektu i jego działanie, informując o tym użytkownika. Ten ostatni podejmuje wówczas decyzję o leczeniu pliku, jego usunięciu lub przeniesieniu do kwarantanny. Niektóre programy jedynie trwale blokują dostęp do pliku, informując użytkownika o wykrytym wirusie, a decyzję odnośnie do jego dalszego losu podejmuje administrator.

Z uwagi na sposób działania *Monitor* musi przez cały czas rezydować w tle. Wymusza to implementacje monitorów jako:

- programów rezydentnych systemu DOS (TSR),
- sterowników 16- i 32-bitowe VxD systemu Windows (sterowniki urządzeń wirtualnych),
- usług systemowych w systemach Windows NT/2000/XP,
- paneli sterowania w komputerach Macintosh,
- procesów-demonów w systemach UNIX/LINUX.

Skanery rezydentne często korzystają z tej samej bazy wirusów, co skaner działający na żądanie, w zasadzie wykrywając te same wirusy. Jednak ograniczone pod tym względem są skanery rezydentne systemu DOS, ze względu na ograniczone zasoby sprzętowe (ograniczona ilość dostępnej pamięci). Ponadto skanery TSR systemu DOS w większości nie wykrywają makro wirusów (ze względu na brak możliwości uruchomienia wielu z nich w tym systemie) oraz mają trudności z wykrywaniem wirusów polimorficznych.

Ograniczenia dotyczące metod, jakimi posługują się monitory antywirusowe w stosunku do skanerów, powodowane są kompromisem pomiędzy skutecznością a zajętością zasobów systemu. Monitory działają podczas codziennej pracy użytkownika na komputerze, dlatego też nie mogą absorbować nadmiernie zasobów systemowych. Duża zajętość systemu przez monitor skutkowałaby wydłużonym czasem oczekiwania użytkownika na realizację jego zadań. To - z kolei - implikuje chęć wyłączania zabezpieczeń, a tym samym całkowitą rezygnację z ochrony antywirusowej.

Istotną techniką pracy monitorów antywirusowych jest obserwacja pracy systemu. Praca narzędzia wykorzystującego tę technikę polega na rezydowaniu w pamięci w celu śledzenia działających procesów i wypatrywania ich możliwych szkodliwych działań. W momencie wykrycia próby wykonania szkodliwej operacji, monitory blokują jej działanie i informują o tym użytkownika. Ten musi określić czy zaobserwowane działanie jest prawidłowe, czy też nie. Zależnie od podjętej decyzji monitor pozwala na wykonanie operacji lub blokuje ją.

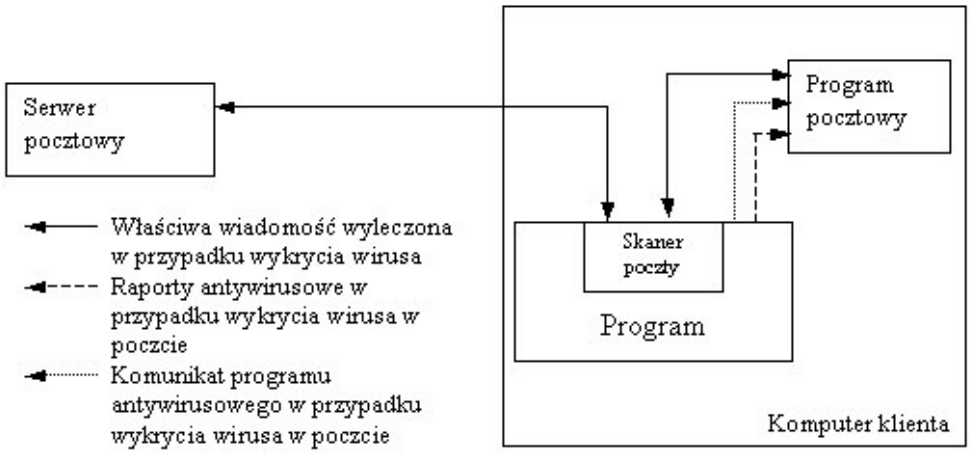
Programy stosujące tą metodę nie potrzebują bazy danych sygnatur wirusów i mogą wykrywać nie zidentyfikowane wcześniej programy złośliwe. Ponadto nie wymagają tak częstych uaktualnień jak skanery znanych wirusów oraz mogą pracować we wcześniej zainfekowanych systemach.

Natomiast do wad tej metody walki z wirusami zaliczamy dużą absorpcję uwagi użytkownika, który musi - ze względu na małą różnicę pomiędzy działaniami szkodliwymi a pożądanymi - potwierdzać prawidłowość różnych działań. W momencie wykrycia

prawdziwego szkodliwego programu to użytkownik musi podjąć decyzję, co zrobić. Kolejną wadą jest możliwość ominięcia tak działających zabezpieczeń przez wirusy używające procedur niskopoziomowych zamiast standardowych wywołań systemowych. Jednak niektóre monitory działań mogą wyszukiwać programy przeprowadzające niskopoziomowe działania na sprzęcie z pominięciem standardowych wywołań systemowych.

5.3 Skaner poczty elektronicznej

Skaner poczty elektronicznej jest częścią programu antywirusowego instalowaną pomiędzy serwerem, a klientem pocztowym, co umożliwia sprawdzanie poczty przychodzącej i wychodzącej.



Rysunek 2

Zadaniem skanera poczty jest odebranie wiadomości od serwera pocztowego lub klienta poczty, przetestowanie jej i zdecydowanie o jej dalszym losie (rysunek 2). W zależności od możliwości i konfiguracji skanowane mogą być wyodrębnione załączniki z wiadomości, bądź też całe wiadomości. Jednak, w tym drugim przypadku, moduł skanujący pocztę musi mieć możliwość skanowania pocztowych formatów tekstowych. Natomiast, gdy program potrafi wyodrębniać załączniki z wiadomości, w razie wykrycia jego infekcji może go wyleczyć lub usunąć, a do klienta pocztowego dociera - już bezpieczna - wiadomość. W takim przypadku program antywirusowy informuje o przebiegu operacji. Jeśli zainfekowana poczta była wysyłana z chronionego komputera, przesyłka taka jest blokowana, a o wykryciu infekcji użytkownik informowany jest stosownym komunikatem. Podobnie wygląda sposób postępowania, gdy program pocztowy operuje na wiadomości w pocztowym formacie tekstowym.

Natomiast, gdy nie zostanie wykryta infekcja, program antywirusowy przekaże wiadomość dalej; w przypadku poczty wychodzącej - do serwera pocztowego, a w przypadku poczty przychodzącej - do klienta pocztowego.

5.4 Moduł naprawczy

Moduł naprawczy, to część programu antywirusowego odpowiedzialna za usunięcie złośliwego programu z pliku oraz przywrócenie go do stanu sprzed infekcji. Niestety niektóre skutki infekcji lub działania wirusa mogą być nieodwracalne, a inne, takie jak zmiany w rejestrze, chociaż są odwracalne - to zwykle nie są poprawiane. Ostatnio można zauważyć tendencję wśród producentów narzędzi antywirusowych do oferowania specjalizowanych narzędzi do usuwania konkretnych, głęboko zagnieżdżonych, wirusów (na przykład Sasser A, Blaster).

Narzędzia dezynfekujące mogą wykorzystywać:

- sumy kontrolne,
- heurystyki,
- bazy z informacjami o zmianach dokonywanych przez wirusy.

W przypadku wykorzystania sum kontrolnych musimy mieć pewność, że wyliczanie sum kontrolnych nastąpiło w momencie, gdy pliki nie były zainfekowane. Spowodowane to jest tym, że wyliczenie sum kontrolnych dla zainfekowanych plików, powoduje przeoczenie faktu infekcji.

Detektory heurystyczne wykorzystują algorytmy starające się przywrócić oryginalną zawartość obiektów. W swej działalności nie wykorzystują baz znanych wirusów.

Natomiast dezynfektory wykorzystujące bazy danych znanych wirusów potrafią precyzyjnie usunąć programy złośliwe.

5.5 Moduł kwarantanny

Zadaniem tego modułu jest, bezpieczne dla systemu, przechowywanie obiektów zainfekowanych lub podejrzanych o infekcję. Mechanizmy zaimplementowane w **module kwarantanny** uniemożliwiają uruchomienie takiego pliku oraz blokują dostęp do niego wszystkim użytkownikom i programom poza programem antywirusowym.

5.6 Moduł aktualizacji

Moduł ten pozwala na pobieranie uaktualnień baz sygnatur wirusów. Pobieranie najczęściej odbywa się metodą przyrostową, co oznacza, że bazy sygnatur wirusów na serwerze producenta porównywana jest z bazą na komputerze klienta i ściągane są tylko brakujące definicje wirusów. Metoda ta pozwala zmniejszyć obciążenie łącza zarówno serwera z aktualizacjami, jak i łącza klienta. Funkcja umożliwia również aktualizację plików programu antywirusowego.

Programy antywirusowe wyposażone są w funkcję automatycznego pobierania aktualizacji. Przebiega ona następująco: program, co pewien (określony) czas sprawdza czy na serwerze aktualizacyjnym pojawiły się nowe elementy do pobrania. Jeśli tak, ściąga je i informuje użytkownika o aktualizacji (powiadamianie można wyłączyć).

W **module aktualizacyjnym** dostępna jest opcja wyłączająca automatyczną aktualizację. W tym momencie możliwe jest ręczne przeprowadzanie aktualizacji na życzenie, bądź ustalenie harmonogramu aktualizacji bez udziału użytkownika. Opcja ta pozwala wybrać dowolną porę dnia i dowolny dzień tygodnia, w którym będzie dokonywana aktualizacja bez udziału użytkownika. Można również wybrać cykliczne wykonywanie aktualizacji o określonej porze w danym dniu tygodnia, na przykład zawsze w piątek o 20.00.

W zależności od konfiguracji środowiska pracy (jedno stanowisko komputerowe lub komputer pracujący w sieci lokalnej) można zastosować różne strategie aktualizacji. I tak, w przypadku jednego komputera możliwy jest tylko scenariusz aktualizacji bezpośredniej z serwera z uaktualnieniami do programu (nowe definicje wirusów, pliki programu). Natomiast w przypadku komputerów pracujących w lokalnej sieci komputerowej możliwy jest scenariusz taki jak dla pojedynczego komputera, czyli każdy z komputerów łączy się bezpośrednio z serwerem aktualizacyjnym producenta lub pobieranie aktualizacji za pośrednictwem dedykowanego serwera do pobierania aktualizacji.

W przypadku zastosowania strategii aktualizacyjnej za pośrednictwem serwera, wszystkie aktualizacje są najpierw przez niego ściągane, a dopiero stamtąd (co wymaga akceptacji administratora) dystrybuowane do komputerów klienckich. Strategia ta pozwala zmniejszyć obciążenie łącza, poprzez które sieć lokalna jest połączona z Internetem oraz zmniejszyć obciążenie serwera aktualizacyjnego producenta oprogramowania. Ponadto

administrator może decydować, jakie poprawki i w jakich porach będą instalowane na komputerach w jego sieci.

5.7 Moduł raportów i statystyk

Moduł ten podaje raporty o incydentach, wykrytych wirusach oraz działaniu automatycznej ochrony. Ponadto generuje statystyki po zakończeniu skanowania na żądanie. Przykładową statystykę generowaną przez program Panda Titanium Antyvirus przedstawia rysunek 9.

Statystyka generowana po zakończonym skanowaniu podaje, co zostało przeskanowane i w jakiej ilości, oraz informację o obiektach zainfekowanych, wyleczonych i którym zmieniono nazwy.

5.8 Firewall

Zapora ogniowa w swej podstawowej konfiguracji sprawdza skąd pochodzi pakiet, jakiego jest typu i dokąd jest kierowany, a następnie na podstawie tych danych podejmuje decyzję o jego przesłaniu lub odrzuceniu. Zapory ogniowe działające na wyższym poziomie sprawdzają typ pakietu, a następnie przeprowadzają dodatkową jego analizę i negocjacje w imieniu użytkownika. Zapory działające w ten sposób nazywane są usługą proxy. Zapora ogniowa może jednocześnie świadczyć usługi filtru pakietów i serwera proxy.

5.9 Moduł filtrowania zawartości poczty elektronicznej

Funkcja filtrowania zawartości poczty elektronicznej ma za zadanie wyeliminować niechciane wiadomości, określane jako spam. W tym celu sprawdza zawartość pól: "Od", "Nadawca X", "Nadawca" w nagłówku wiadomości. Jeżeli wartości tych pól znajdują się na liście znanych nadawców spamu (RBL), wiadomość zostaje odrzucona. Kolejna metodą jest odrzucanie wiadomości w oparciu o adres IP nadawcy. Inna metoda polega na analizie treści listu przy wykorzystaniu słownika spamu, w którym każde słowo ma statystyczną wagę odzwierciedlającą częstość występowania w spamie. Wyszukiwanie tych słów i sumowanie ich wskaźników pozwala uzyskać minimalny poziom błędnej klasyfikacji wiadomości jako spam.

5.10 Moduł filtrowania zawartości stron internetowych

Moduł ten pozwala na sprawdzanie zawartości strony www pod kątem występowania na niej słów uznanych za niepożądane przez nas i w przypadku ich wystąpienia blokuje do niej dostęp. Możemy również wspomóc się listami "zakazanych" stron internetowych, prowadzonymi przez niezależne organizacje. Istnieje też opcja zabraniająca wyświetlania pewnych elementów strony, na przykład grafiki, bądź stron znajdujących się pod konkretnymi adresami.

Wykorzystanie tej funkcji pozwala kontrolować wydajność pracowników, poprzez zablokowanie niewłaściwego wykorzystania Internetu. Możemy w ten sposób ograniczyć, na przykład dostęp do prywatnych kont e-mail dostępnych przez www, wirtualnych sklepów lub stron o treściach pornograficznych.

5.11 Autodiagnostyka

Ponieważ program antywirusowy sam może stać się celem ataku (na przykład w celu uniemożliwienia mu skutecznej pracy), posiada funkcję pozwalającą zdiagnozować swój stan. W przypadku wykrycia nieprawidłowości może poinformować o tym użytkownika, zakończyć swoje działanie, lub zastąpić uszkodzone pliki dobrymi z wykonanej wcześniej kopii.