Zespół Szkół im. Adama Wodziczki w Mosinie

Roman Zalewski

Mariusz Bocian

Szkodniki komputerowe i zagrożenia w sieci

Mosina 2005/2006

Praca wykonana podczas zajęć
przedmiotu: przetwarzanie informacji
w II klasie liceum profilowanego
o profilu zarządzanie informacja
pod kierownictwem p. Pawła Zawieji.
Nauczyciel konsultant p. Paweł Zawieja.

Spis treści

3 Rozdział:

Wstęp

Na stronie internetowej znanego czasopisma komputerowego Chip, można przeczytać, że w roku 2004 liczba zidentyfikowanych w Internecie wirusów wzrosła o ponad 50% w porównaniu z rokiem 2003. W ubiegłym roku znaleziono ponad 100 tysięcy robaków, gwałtownie wzrosła także liczba ataków przy użyciu tzw. phishingu (wyłudzanie informacji finansowych i haseł), które na dzień dzisiejszy stanowią ponad 30% wszystkich ataków. Wiele komputerów zostało przejętych przez hakerów i wykorzystanych do przeprowadzania kolejnych ataków. Specjaliści uważają, że jedną z największych zmian, jakie zaszły w roku 2004, jest fakt, iż twórcy wirusów, które bardzo szybko rozprzestrzeniają się po sieci i czynią duże szkody, to bardzo młodzi ludzie. Pomimo tego, że dla nich jest to zabawa, rośnie liczba przestępstw kryminalnych dokonywanych przy użyciu wirusów. Najpopularniejsze z nich to przestępstwa finansowe. Jednocześnie w roku 2004 odniesiono więcej niż w poprzednich latach sukcesów w walce z cyberprzestępcami. Aresztowano kilku z nich i zamknięto strony WWW, na których handlowano skradzionymi numerami kart kredytowych. Każdy użytkownik komputera na pewno słyszał, lub, co gorsza osobiście miał do czynienia z wirusem. Jednak niewielu z nich zna zasadę ich działania, gdyż w tej dziedzinie, tak jak w wielu innych dziedzinach naszego życia, panują ustalone stereotypy. Są one wynikiem zarówno braku wiedzy przeciętnego użytkownika, jak i dezinformacji, lub raczej braku poprawnych i pożytecznych informacji, ze strony mediów i producentów oprogramowania antywirusowego. Choć trudno w to uwierzyć, infekcjom mogą ulegać również komputery. Wirusy komputerowe, tak jak grypa przykuwająca ludzi do łóżka, potrafią bardzo skutecznie sparaliżować nawet najlepsze komputery powodując, że ich właściciele mają czasem spore problemy z ich usunięciem. Liczba wirusów jest trudna do oszacowania, można przyjąć, że jest ich od kilku do kilkunastu tysięcy. Te mniej groźne są jedynie uciążliwe, inne jednak mogą doprowadzić nawet do utraty danych. W ostatnim czasie, kiedy większość ludzi na stałe przyłączona jest do Internetu, gdzie coraz bardziej popularne stały się programy peer-to-peer, zaczęliśmy masowo korzystać z komunikatorów, nawet, jeśli nie jesteśmy bezpośrednio zagrożeni, to jest wielce prawdopodobne, że wymienimy się zarażonymi danymi z takimi osobami.

Bakcyla w e-mailu możemy otrzymać każdego dnia, fragmenty kodu uruchamiającego złośliwe skrypty możemy spotkać oglądając strony WWW. Niniejsza

praca ma na celu omówienie problematyki wirusów i wyprostowanie wszelkich błędnych opinii na ich temat, opisuje, w jaki sposób możemy zwiększyć nasze bezpieczeństwo w Internecie, co zrobić, aby komputer był jak najmniej narażony na ataki, czego należy unikać poruszając się po sieci. W pierwszym rozdziale przedstawiono ogólne pojęcia zagrożeń, które można napotkać w sieci, jak również, w jaki sposób komputer może ulec infekcji, a także przybliżono historię robaków oraz wirusów komputerowych. Rozdział drugi przedstawia rodzaje wirusów, ich podział ze względu na sposób działania po uruchomieniu. Omówiono kilka z najpopularniejszych w ostatnim miesiącu robaków, które pojawiły się w Internecie. W rozdziale trzecim zostały opisane metody zwalczania szkodliwego oprogramowania, budowa i działanie programów antywirusowych, oraz inne metody ochrony przed dostępem nieupoważnionych osób do komputera.

1 Rozdział:
Podstawowe informacje

Bezpieczeństwo danych w Internecie spędza sen z powiek specjalistom i przeciętnym użytkownikom. Każdy z nas może niespodziewanie stać się ofiarą ataku hakera lub programu zakłócającego poprawną prace komputera. Należy, zatem pilnować, aby elektroniczna furtka do naszych danych była stale zamknięta.

1.1 Zagrożenia w sieci

Pierwsze włamania w Polsce miały charakter czysto „poznawczy". Młodzi ludzie (w większości studenci różnych uczelni, którzy mieli dostęp do sieci) często usiłowali dostać się do innego komputera podłączonego do sieci po to, aby udowodnić sobie, że są w stanie złamać te zabezpieczenia. Sęk w tym, że wówczas zabezpieczeń tych nie było zbyt wiele. Dziś trudno już w to uwierzyć, ale były to czasy bez WWW (wtedy najpopularniejsze tego typu usługi to gopher i WAIS), większość serwerów unixowych miała hasła zaszyfrowane, przechowywane bezpośrednio w /etc/password i każdy użytkownik mógł sobie taki plik password skopiować. Nietrudno też było o jakiekolwiek „exploidy". Często jedynymi, dostępnymi źródłami informacji użytecznych dla hakerów były zagraniczne grupy newsowe lub serwery FTP, zawierające ostrzeżenia o błędach w systemach operacyjnych i oprogramowaniu (np. ftp.cert.org). Internet komercyjny w zasadzie wówczas w Polsce nie istniał, tak więc firmy komercyjne nie były jeszcze zainte-

resowane tematyką bezpieczeństwa sieci lokalnych podłączonych do Internetu. Podstawowym narzędziem używanym przez ówczesnych hakerów był zwykły kompilator C dostępny w systemie i gotowe narzędzia podobne w działaniu do Cracka (np. legendarny już Killer Cracker), czyli programy, służące do znajdywania haseł użytkowników tzw. metodą słownikową. Można wyróżnić dwie podstawowe pobudki, którymi kierowali się ówcześni polscy hakerzy. Pierwsza z nich to - rzecz jasna - wspomniana już czysta ciekawość i chęć udowodnienia sobie, że jest się „lepszym" niż administrator, któremu nie udało się uratować swojego systemu przed „atakiem". Drugim powodem działania hakerów była bardzo słaba dostępność sieci. Wielu ówczesnych pasjonatów informatyki, najczęściej jeszcze niebędących studentami, nie miało praktycznie ani szans, ani nawet podstaw ku temu, by znaleźć się w tym elitarnym klubie - sieci Internet. Tacy ludzie podejmowali często desperackie dość próby uzyskania dostępu do Internetu za pośrednictwem nielicznych miejsc, dzięki którym do sieci można było dostać się przy użyciu zwykłego modemu i telefonu. Sytuacja taka utrzymywała się praktycznie aż do 1994 roku, a gdzieniegdzie nawet do 1995 r. Wtedy to właśnie zaczęły coraz wyraźniej pojawiać się zwiastuny nowej epoki w dziejach polskiego Internetu. Coraz częściej słychać było hasło „Internet komercyjny". Na rynku pojawili się pierwsi, komercyjni dostawcy usług internetowych. Na początku ich oferta nadal nie była atrakcyjna dla pasjonatów, tym bardziej, że w tamtych czasach nawet prywatny dostawca usług internetowych musiał być podłączony do NASK-u (Naukowo-Akademickiej Sieci Komputerowej),a to bynajmniej nie powodowało obniżenia cen. NASK bardzo wytrwale pilnował swojego monopolu w tej dziedzinie. Z punktu widzenia rozwoju społeczeństwa informacyjnego, taka sytuacja była niewłaściwa - a w pewien sposób kryminogenna. Haker traktowany był często przez rówieśników jak bohater - ktoś, kto przełamuje znienawidzony monopol. Dziś możemy śmiało powiedzieć, że 99,9% ówczesnych włamań można zakwalifikować do kategorii czysto sportowych, niemających żadnego innego podłoża niż chęć wykazania się lub po prostu dostania się do globalnej sieci w celu korzystania z wielu jej usług. W miarę rozwoju sieci i powolnego powstawania Internetu komercyjnego zaczęły pojawiać się (przynajmniej teoretycznie) nowe zagrożenia. Wprawdzie nadal w polskim Internecie nie mieliśmy ani istotnych serwerów rządowych, ani tym bardziej militarnych, nie było też banków i dużych przedsiębiorstw. Co najwyżej niektórzy przedstawiciele tych instytucji posiadali słono

opłacane konta poczty elektronicznej, ale one nie interesowało polskich hakerów. W sieci bark było innych instytucji niż akademickie, nie było, więc w polskim Internecie głośnych włamań dokonywanych przez hakerów, takich, o jakich od dawna słyszało się w krajach tzw. Zachodu. Pierwsze, naprawdę głośne włamanie w historii polskiego Internetu miało miejsce w noc sylwestrową, 31 grudnia 1995 roku. Dotyczyło ono wielu komputerów centralnego węzła sieci NASK w Warszawie, a uwieńczone zostało modyfikacją strony głównej WWW tej instytucji. Haker - występujący pod pseudonimem „Gumiś" - zaprotestował w ten sposób przeciwko słynnemu już, nowemu cennikowi usług NASK, w którym wprowadzono zasadę opłaty za ruch w miejsce używanej powszechnie w Internecie stałej odpłatności za przepustowość łącza. Włamanie to miało duże znaczenie, ponieważ zbiegło się w czasie z początkiem intensyfikacji rozwoju Internetu komercyjnego w Polsce. Wiele odpowiedzialnych osób wreszcie zaczęło zastanawiać się poważnie nad zagadnieniem bezpieczeństwa samej sieci i danych przesyłanych za jej pośrednictwem. Z drugiej jednak strony na przełomie lat 1995/96 było jeszcze za wcześnie na zauważalną reakcję na rynku informatycznym. NASK wprowadziła dodatkowe systemy zabezpieczeń, aby uniemożliwić w przyszłości powtórny atak hackerów. World Wide Web (ogólnoświatowa pajęczyna) ułatwiła osobom zainteresowanym docieranie do najróżniejszych informacji zgromadzonych w sieci, w tym do informacji o błędach w systemach operacyjnych i rozmaitych metodach stosowanych w celu przełamywania zabezpieczeń. Upowszechniły się nowe metody ataków sieciowych (spoofing, sniffing), pojawiły się możliwości wykorzystywania nowych, znacznie trudniejszych do wykrycia błędów w oprogramowaniu (np. słynna możliwość wykonywania rozmaitych fragmentów kodu maszynowego instalowanego w segmencie stosu za pośrednictwem licznych błędów należących do kategorii „buffer overflow").Na efekty zwiększonej dostępności Internetu oraz pojawienia się szybkich i łatwych metod pozyskiwania informacji nie trzeba było długo czekać. Rok 1997 to rok głośnych włamań w polskim Internecie. Zaczęło się w nocy z 3 na 4 maja 1997 roku włamaniem na serwer WWW Biura Informacyjnego Rządu, kiedy to dwaj szesnastoletni chłopcy przy użyciu gotowych przepisów (tzw. exploidów), pozyskanych za pośrednictwem Internetu, zdobyli uprawnienia niezbędne do zmodyfikowania strony głównej WWW wspomnianej instytucji. Obaj chłopcy nie byli nawet uznawani przez swoich rówieśników za prawdziwych hackerów. Jak sami przy-

znali w wywiadzie udzielonym dziennikarzom telewizyjnych „Wiadomości” - byli początkującymi użytkownikami Internetu, którzy interesowali się siecią od sześciu miesięcy. Sprawa szybko została nagłośniona przez media. Dla nas - specjalistów, zajmujących się bezpieczeństwem - wesołym akcentem w tej sprawie było oświadczenie ówczesnej pani rzecznik prasowej rządu, która stwierdziła w wystąpieniu, iż poufne dane rządowe są bezpieczne, ponieważ są przechowywane na przenośnych komputerach niepodłączonych do sieci, konkretnie, na komputerach PC klasy notebook. Stwierdzenie to dowodziło ignorancji osób odpowiedzialnych za istotne dane państwowe. Równie szokujący był fakt, iż serwer informacyjny Rządu RP był całkowicie niezabezpieczony przed próbami ataku hackerów. Zapewne wielu użytkowników Internetu nie zdawało sobie sprawy z faktu, iż jest to jedynie przysłowiowy „wierzchołek góry lodowej”. Stosunkowo szybko miało się okazać, że wyrosło nowe pokolenie hakerów, którzy potrafią skutecznie zaatakować nawet na pierwszy rzut oka dobrze zabezpieczone serwery internetowe. 8 sierpnia 1997 roku hakerzy zaatakowali największy serwer FTP w Polsce - słynny SunSite zlokalizowany w ICM (Interdyscyplinarnym Centrum Modelowania Matematycznego i Komputerowego). Hakerom udało się zdobyć uprawnienia wystarczające do modyfikowania plików udostępnianych za pośrednictwem anonymous FTP. Tym razem podłożyli oni tzw. konia trojańskiego, modyfikując udostępniane na serwerze źródła popularnego programu SSH (ang. Secure Shell), tak, aby liczby pierwsze wykorzystywane przez algorytm kodowania transmisji SSH były wysyłane na odpowiednie konto pocztowe bez wiedzy użytkownika programu. Na szczęście, administratorzy SunSite szybko zorientowali się w sytuacji i po krótkiej przerwie udostępnili swój niezwykle popularny serwer użytkownikom Internetu. Niemniej sieć ICM należy do najlepiej strzeżonych w Polsce sieci naukowych. Włamanie to było, więc dla wszystkich poważnym ostrzeżeniem. Na kolejne, głośne włamanie musieliśmy czekać do jesieni, a konkretnie do nocy z 25 na 26 października 1997 roku. Wtedy to hakerzy, podpisujący się „Gumisie”, nawiedzili serwer WWW NASK, a hasło „Gumisie wróciły!” szybko zyskało popularność. Tym razem strony WWW NASK znowu zmieniły swoją zawartość, tyle tylko, że oprócz grafik przedstawiających rzeczone Gumisie oraz tekstów prezentujących opinię hakerów, dotyczącą działalności NASK, na stronie WWW opisującej zasoby sieciowe w Polsce pojawiła się mapka Polski z naniesionymi wieloma miastami. Kliknięcie na którekolwiek z zaznaczonych miast powodowa-

ło wyświetlenie pliku tekstowego w formacie charakterystycznym dla unixowego /etc/password, prezentującego bazę użytkowników z wybranego serwera internetowego, znajdującego się w danym mieście. Plik zawierał zazwyczaj zakodowane, aktualne hasła. Szybko w polskiej sieci pojawiły się kopie tych zmodyfikowanych przez hakerów stron. Kierownictwo NASK - bardzo zdenerwowane opublikowaniem tych stron - rozpoczęło akcję, mającą na celu usuwanie z widocznych miejsc w sieci stron spreparowanych przez „Gumisie". Niemniej, przy odrobinie wysiłku można nadal znaleźć ich kopie w Internecie na różnych serwerach WWW. Należy pamiętać, że po pierwszym włamaniu na serwer WWW, NASK wprowadził specjalne procedury zabezpieczające swoją sieć przed ponownym atakiem hakerów - niestety, i znów udało się im je złamać.

1.2 Historia wirusów

Rok 1998 zdecydowanie powinien być określany jako rok technologicznego ataku hakerów na światową siec komputerową Internet. Ich celem okazały się główne aplikacje internetowe, czyli przeglądarki i oraz programy do obsługi poczty elektronicznej. Jednak wszyscy musieli być świadomi, że dzień taki nadejdzie, gdyż Intenet jest przysłowiowym „łakomym kąskiem" dla piszących wirusy i nie mogli oni pozostać wobec niego bierni. Praktycznie wszystkie znane podziemne grupy hakerskie w mniejszym lub większym stopniu badały zdolność aplikacji internetowych do przenoszenia wirusów i starały się wykorzystać te możliwości by zaatakować Internet. Stare wirusy DOS'owe odeszły w zapomnienie, celem nowoczesnych hakerów stał się WIRUS, który może się bezproblemowo rozprzestrzeniać przez Internet, infekować lokalne sieci, zdalne stacje robocze oraz domowe komputery. Niestety twórcy wirusów odnieśli na tym polu duże sukcesy. W ciągu dwóch ostatnich lat (1997 i 1998) pojawiło się wiele nowych wirusów, które używają Internetu do rozprowadzania swych kopii poprzez pocztę elektroniczną. Większość z nich to makrowirusy, które używają standardowych funkcji systemu Windows by dostać się do zainstalowanych klientów poczty elektronicznej, stworzyć załącznik ze swoją kopią oraz rozesłać wiadomość z tym załącznikiem do przypadkowo wybranych adresatów. Systemy nieostrożnych użytkowników, którzy otrzymują taką wiadomość i otwierają załącznik poprzez Word'a lub Excel'a (w zależności o typu wirusa) zostają zainfekowane a wirus kontynuuje swoje powielanie, lecz juz z innego adresu. Dla przykładu makrowirus Word'a

„ShareFun” wysyła zainfekowany załącznik używając programu MS-Mail; makrowirus Word’a 97 „Antimarc” używa do powielania siebie programu Outlook Express; wirus z platformy Windows 3.xx „RedTeam” przenika do bazy danych Outbox programu Eudora mail i umieszcza w niej zainfekowany plik *.exe; makrowirus Word’a „Innuendo” używa uniwersalnych metod, które pozwalają na przesłanie zainfekowanej wiadomości poprzez dowolny program pocztowy; wirus platformy Windows „Parvo” by dostać się do zasobów Internetu używa funkcji Windows API. (Zobacz opisy wirusów w encyklopedii wirusów AVP www.avpve.pl, www.avp.ch). Druga połowa 1998 roku przyniosła kontynuację ataków na aplikacje internetowe. Tym razem obróciły się one także przeciwko przeglądarkom internetowym. Celem pierwszego ataku był bardzo mocno promowany język Java, szeroko używany podczas tworzenia witryn internetowych. W sierpniu roku 1998 pewien nieznany „pisarz” wirusów wypuścił pierwszy wirus infekujący aplikacje napisane w Javie. Kolejna aplikacją, które uległa atakom był język skryptów Windows - programy napisane w Visual Basic Script również często używane do „kolorowania” stron WWW. W listopadzie tego samego roku pojawił się pierwszy wirus atakujący bezpośrednio strony HTML, które są głównym i niezbędnym elementem wszystkich serwisów sieciowych. Jak widać wszystkie główne aplikacje internetowe zostały zaatakowane i co gorsza atak ten był skuteczny. Jednak pomimo tego wszelkie znane wirusy, które starają się rozprzestrzeniać poprzez Internet nie są tak groźne jak można by sobie to wyobrazić. Możliwość zaistnienia niebezpieczeństwa ze strony takich wirusów jest natury czysto teoretycznej: są one bądź „dobrze widoczne”, (jeśli są dołączone w postaci załączników do przesyłki), bądź „niepracujące” - wszystkie popularne przeglądarki internetowe posiadają wewnętrzne moduły bezpieczeństwa, które natychmiast odrzucają wszelkie wirusopodobne akcje lub ostrzegają o nich użytkownika.

1.3 Dialer - to wyspecjalizowany rodzaj programu komputerowego do łączenia się z Internetem za pomocą modemu. Niekiedy program tego rodzaju instalowany w jego komputerze bez wiedzy i zgody użytkownika jest wykorzystywany do nawiązywania połączenia z siecią.

1.4 Koń trojański (trojan) - program, który nadużywa zaufania użytkownika wykonując bez jego wiedzy dodatkowe, szkodliwe czynności. Składa się z serwe-

ra i klienta. Serwerem jest plik, który wbrew woli użytkownika jest instalowany w systemie(szczególnie w systemie operacyjnym Microsoft Windows). Klient pozwala włamywaczowi przejąć kontrolę nad maszyną, co jest nielegalne.

1.5 Robak - Główną różnicą między wirusem, a robakiem jest to, że, podczas gdy wirus potrzebuje nosiciela – jakiegoś pliku wykonalnego, który modyfikuje doczepiając do niego swój kod wykonywalny, to robak jest pod tym względem samodzielny a rozprzestrzenia się we wszystkich sieciach podłączonych do zarażonego komputera poprzez wykorzystanie luk w systemie operacyjnym oraz naiwność użytkownika.

2 Rozdział Działanie wirusów i rodzaje ataków w sieci

2.1 Rodzaje wirusów

2.1.1 Robaki

Robak to program, którego działanie sprowadza się do tworzenia własnych duplikatów, tak, że nie atakuje on żadnych obiektów, jak to czynią wirusy. Oprócz zajmowania miejsca na dysku program ten rzadko wywołuje skutki uboczne. Podobnie jak wirusy towarzyszące, robaki są najczęściej pisane w językach wysokiego poziomu. Robaki są najbardziej popularne w sieciach, gdzie mają do dyspozycji protokoły transmisji sieciowej, dzięki którym mogą przemieszczać się po całej sieci.

2.1.2 Królik (ang. Rabbit)

Program wielokrotnie kopiujący i uruchamiający swój własny kod źródłowy celem pełnego zagarnięcia zasobów komputera (czasu procesora, pamięci operacyjnej, przestrzeni dyskowej) i doprowadzenia do upadku systemu.

2.1.3 Koń Trojański

Koń trojański nie jest wirusem komputerowym, ale ze względu na swoje działanie często bywa z nim utożsamiany. Zasada działania konia trojańskiego jest banalnie prosta. Uruchomiany, wykonuje niby to normalną pracę, bezpośrednio wynikającą z przeznaczenia programu (np. gra, demo. program użytkowy), lecz dodatkowo, niejako w tle, wykonuje jakieś niezauważalne dla użytkownika operacje, (najczęściej po prostu niszczy - kasuje lub zamazuje - dane na dysku twar-

dym). Konie trojańskie najczęściej przenoszą się w plikach udających nowe, popularne programy kompresujące (np. PKZIP, ARJ, RAR) lub też udają programy narzędziowe do obsługi dysków.

2.1.4 Bomby logiczne

O ile koń trojański wykonuje brudną robotę od razu po uruchomieniu, o tyle bomba swe destrukcyjne oblicze ukazuje tylko w określonym odpowiednimi warunkami czasie (najczęściej zależnie od aktualnej daty lub liczby poprzednich wywołań programu). Ze względu na to, iż właściwy, destrukcyjny kod może być ukryty w dowolnym miejscu programu zawierającego bombę, należy ostrożnie obchodzić się z aplikacjami, których pochodzenie jest nieznane. Mianem bomby określa się często także destrukcyjny, uruchamiany tylko po spełnieniu jakiegoś warunku, kod zawarty w wirusach.

2.1.5 Wirusy

Wirus komputerowy (łacińskie „virus” oznacza truciznę) to krótki program, który posiada zdolność samoczynnego powielania się i przenoszenia z jednego komputera na drugi bez wiedzy i poza kontrolą użytkownika. Twórcą tego terminu, funkcjonującego od 1986 r. jest Fred Cohen, który za badania nad tym zjawiskiem otrzymał doktorat w dziedzinie inżynierii elektrycznej. Wirusy tworzone są przez anonimowych programistów, najczęściej w złych zamiarach - Stephen Hawking, laureat nagrody Nobla w dziedzinie fizyki, określił je jako pierwszą formę życia stworzoną przez człowieka. Najwcześniejszy przypadek ukarania autora wirusa miał miejsce w 1995 r. - został on skazany na 18 miesięcy więzienia. Szkody wyrządzane przez wirusy różnią się w zależności od jego rodzaju, począwszy od wyświetlania na ekranie niegroźnych komunikatów, a skończywszy na uszkodzeniu bądź zniszczeniu danych i unieruchomieniu komputera. Wirusy mogą być przenoszone poprzez dyskietki, dyski optyczne oraz sieć. Terminem "wirus" bywają często określane niesłusznie wszystkie destrukcyjne programy m.in. konie trojańskie. Wirusy to programy, które maskują się podczepiając pod inne użyteczne pliki. Są to głownie pliki z rozszerzeniem; *.exe, *.doc, *.xls, *.com, również e-maile i pliki html. Wirusy głównie kopiują się w dziesiątki miejsc, ale są i takie, które czynią duże szkody. Wirus komputerowy nigdy nie powstaje samoistnie, każdy „insekt” tworzony jest przez osobę, która postawiła

sobie za cel stworzenia programu, który będzie się sam powielał w komputerach, w których się pojawi. Większość wirusów jest niegroźna, często ich celem jest np. wyświetlenie jakiegoś komunikatu na ekranie monitora. Jednak wirusy pisane przez dobrych programistów często prowadzą do nieodwracalnych szkód, np. wykradanie danych, bądź ich niszczenie, „dobre" wirusy najczęściej pisane są w asemblerze, co spowodowane jest głównie specyfiką kodu generowanego przez ten język, a zwłaszcza jego zwięzłością. Kod maszynowy programu, który z punktu widzenia użytkownika nie robi nic, w językach wysokiego poziomu (Pascal, C) zajmie od kilkuset bajtów do kilku kilobajtów, natomiast w asemblerze podobny program zajmie od jednego do czterech bajtów. Spowodowane jest to tym, iż języki wysokiego poziomu do każdego wygenerowanego przez siebie programu dodają standardowe prologi i epilogi, niewidoczne dla piszącego w danym języku programisty, które są odpowiedzialne np. za obsługę błędów. W asemblerze programista ma dużą swobodę w dostępie do pamięci czy portów, ma możliwość świadomego wpływu na kształt programu np. w zakresie używanych instrukcji. Programy tworzone w asemblerze przez wprawnych programistów są optymalne pod względem szybkości działania i długości kodu. Jedynym ograniczeniem asemblera jest fakt, iż programy napisane w tym języku nie mogą być przenoszone na komputery o innej architekturze, stąd mogą działać tylko w jednej rodzinie komputerów. Cały czas powstają nowe wirusy. Zastosowanie dobrego programu antywirusowego zapobiega zagrożeniu w 99%. Programy te muszą być aktualizowane i muszą monitorować wszystko to, co dzieje się w systemie. Skanować należy wszystko to, co przychodzi z zewnątrz począwszy, od e-maili a kończąc na płytkach pism komputerowych. Informacje o najnowszych wirusach znajdziesz m.in. www.antivirus.com/vinfo Proces infekowania polega najczęściej na odpowiedniej modyfikacji struktury pliku bądź sektora. Długość typowego wirusa waha się zazwyczaj w granicach od kilku bajtów do kilku kilobajtów, zależy to głównie od programisty piszącego wirusa oraz od języka, w którym wirus jest pisany. Efekt działania wirusa zależy od programisty oraz jego umiejętności. Celem większości wirusów jest tylko własna replikacja a widoczne efekty często spowodowane są działaniem ubocznym wynikającym z błędów. Uaktywnienie wirusa najczęściej spowodowane jest nieświadomym działaniem użytkownika, który, uruchamia zarażony program, bądź próbuje wczytać system z zarażonej dyskietki,

czy odczytuje zarażony dokument. W ten sposób użytkownik sam instaluje wirusa w używanym przez siebie komputerze.

2.1.5.1 Rezydentne

Wirusy tego typu instalują się w pamięci jako rezydentne programy usługowe TSR (ang. Terminate and Stay Resident). Przejmują jedno lub więcej przerwań i infekują, gdy spełnione są określone warunki np. uruchomienie programu.

2.1.5.2 Nie rezydentne

Są aktywne jedynie wtedy, gdy jest wykonywany zainfekowany program użytkowy. Wykonują one całkowicie swój program na tym etapie i nie pozostają w pamięci.

2.1.5.3 Wirusy plików wsadowych (ang. Batchviruses)

Wykorzystują one do transportu pliki z rozszerzeniem *.bat, są to raczej starsze wirusy. Jednak mimo raczej ubogiego zestawu środków, jakimi operują twórca, potrafią często infekować nie tylko pliki *.bat, ale często pliki *.com i *.exe czy sektor tablicy partycji. Po uruchomieniu zainfekowanego pliku wsadowego tworzony jest plik uruchamiany *.com lub *.exe (za pomocą polecenia ECHO, którego parametry są przekierowywane do pliku), zawierający właściwy kod infekujący pliki *.bat. Po tym jak zostanie stworzony i wykorzystany jest kasowany.

2.1.6 Makrowirusy (ang. Macroviruses)

Wirusy tego typu to jeden z nowszych wynalazków, nie zarażają one programów uruchamialnych, lecz pliki zawierające definicje makr. Wśród najczęściej zarażanych plików górują pliki z rozszerzeniami *.doc (pliki programu Microsoft Word), *.xls (Microsoft Excel, SAM (dokumenty AmiPro). Makrowirusy do rozprzestrzeniania się wykorzystują funkcje zawarte w językach makr, wbudowanych w różne aplikacje np. WordBasic w MS Word).

2.2 Działanie wirusów

2.2.1 Wirusy plikowe

Wirusy plikowe infekują wszystkie pliki uruchamialne. Ostatnio nawet *.doc i *.xls. Dołączane są do kodu infekowanego programu. Mogą dołączać się na jego

końcu, początku i w środku. Istnieją również wirusy plikowe, które zamazują część kodu programu uszkadzając go już nieodwracalnie. Zazwyczaj wirusy plikowe są uruchamiane przed właściwym programem, jednak istnieją i takie, które zostają uaktywnione po zakończeniu działania pierwotnego programu. Przykładem może być wirus BeTaViRiLaTiOn lub GEOv1.0 napisane w Turbo Pascal'u. Wirusów plikowych jest najwięcej, z tego względu, że są proste do napisania i szybko się rozprzestrzeniają.

2.2.1 Wirusy pasożytnicze (ang. Parasite infectors)

W zasadzie większość znanych wirusów to wirusy pasożytnicze, które wykorzystują swoje ofiary do transportu, modyfikując ich strukturę wewnętrzną. Jedynym ratunkiem dla zainfekowanych obiektów jest użycie szczepionki lub w ostateczności kopii zapasowych, gdyż zarażone pliki z reguły nie są przez wirusa leczone. Wyjątek stanowią nieliczne wirusy wykorzystujące pliki tylko do transportu między komputerami, mające za główny cel infekcję tablicy partycji lub BOOT-sektora dysku twardego. Po zainfekowaniu któregoś z tych obiektów wirus zmienia działanie i leczy wszystkie używane pliki znajdujące się na twardym dysku, a infekuje jedynie pliki już znajdujące się na dyskietkach lub dopiero na nie kopiowane. Ze względu na miejsce zajmowane w zainfekowanych plikach wirusy pasożytnicze dzieli się na: -wirusy nadpisujące, lokujące się na początku pliku, często niezapamiętujące poprzedniej zawartości pliku, (co w efekcie nieodwracalnie niszczy plik); -wirusy lokujące się na końcu pliku, najbardziej rozpowszechniona odmiana wirusów pasożytniczych, które modyfikują pewne ustalone struktury na początku pliku tak, aby wskazywały na wirusa, po czym dopisują się na jego końcu; -wirusy nagłówkowe, likujące się w nagłówku plików *.exe przeznaczonych dla systemu DOS; wykorzystują one fakt, iż nagłówek plików *.exe jest standardowo ustawiony przez programy linkujące na wielokrotność jednego sektora (512 bajtów). Zwykle wirusy te nie przekraczają rozmiaru jednego sektora i infekują poprzez przejęcie funkcji BIOS służących do odczytu i zapisu sektorów; -wirusy lokujące się w pliku w miejscu gdzie jest jakiś pusty, niewykorzystany obszar, który można nadpisać nie niszcząc pliku; -wirusy lokujące się w dowolnym miejscu pliku, dość rzadkie, bardzo trudne do napisania; -wirusy wykorzystujące część ostatniej Jednostki Alokacji Pliku JAP, korzystające z faktu, iż plik rzadko zajmuje dokładnie wielokrotność jednej JAP. Ten rodzaj wirusów jest

najszerzej rozprzestrzeniony na świecie i najczęściej spotykany, wykorzystują swoje ofiary do transportu modyfikując ich strukturę wewnętrzną. Często pliki używane do transportu przez wirusy pasożytnicze są trwale niszczone, jedynym ratunkiem jest użycie szczepionki lub kopii zapasowych, ponieważ zarażane pliki z reguły nie są przez wirusa leczone. Wyjątkiem są wirusy, których celem jest infekcja tablicy partycji lub BOOT sektora dysku twardego, wtedy pliki używane są tylko do transportu. Taki wirus po zainfekowaniu tablicy partycji lub BOOT sektora, leczy pliki znajdujące się na twardym dysku, których użył do transportu, a infekuje jedynie te znajdujące się na dyskietkach lub na nie kopiowane. 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.

a. 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.

b. Wirusy nagłówkowe (ang. Header infectors), lokują się w nagłówku plików *.exe przeznaczonych dla DOS'a, wykorzystują one fakt, ze nagłówek plików *.exe jest standardowo ustawiony przez programy linkujące na wielokrotność jednego sektora (512 bajtów). Wirusy te zwykle nie przekraczają rozmiaru jednego sektora i infekują przez przejęcie funkcji BIOS, które służą do odczytu i zapisu sektorów (02,03/13).

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

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

e. Wirusy wykorzystujące część ostatniej jednostki alokacji pliku JAP (ang. Slack space infectors), korzystają one z tego, że plik rzadko zajmuje dokładnie wielokrotność jednej Jednostki Alokacji Pliku (JAP).

2.2.2 Wirusy towarzyszące (ang. Companion infectors)

Wirusy te pisane są najczęściej w językach wysokiego poziomu (C, Pascal). Atakują one pliki a ich działanie opiera się na hierarchii systemu DOS podczas uruchamiania programów. Oznacza to, że w przypadku uruchamiania jakiegoś programu bez podania rozszerzenia, najpierw poszukiwany jest plik o rozszerzeniu *.com, później *.exe a na końcu *.bat (W przypadku wykorzystania interpretatora poleceń 4DOS dochodzą jeszcze pliki BTM, które będą poszukiwane przed plikami *.bat).

Przykład:

1 Jeżeli w jednym katalogu istnieją trzy pliki:

a) prog.bat
b) prog.com
c) prog.exe

To jako pierwszy będzie uruchamiany plik z rozszerzeniem *.com, później *.exe a na końcu *.bat.

Plik prog.com będzie się uruchamiać ilekroć podamy nazwę PROG bez rozszerzenia lub z rozszerzeniem *.com. Plik PROG.EXE można w tym wypadku uruchomić wyłącznie poprzez podanie jego pełnej nazwy, bądź tez poprzez uprzednie usunięcie pliku PROG.COM z danego katalogu. Uruchomienie pliku *.bat wymaga albo usunięcie dwóch wcześniej wymienionych plików z katalogu, bądź wpisanie nazwy pliku z rozszerzeniem *.bat. Jak widać wirus ma kilka możliwości, aby zainfekować uruchamiany program.

Istnieje plik *.com: nie można zastosować infekcji

Istnieje plik *.exe: można utworzyć plik o takiej samej nazwie, o rozszerzeniu *.com który będzie zawierał wirusa.

Istnieje plik *.bat: można utworzyć plik o takiej samej nazwie, o rozszerzeniu *.com lub *.exe, który będzie zawierał wirusa.

Następna próba uruchomienia tak zarażonego programu spowoduje najpierw uruchomienie podszywającego się pod program wirusa, a dopiero on, po zakończeniu pracy, przekaże sterowanie do programu macierzystego, najczęściej poprzez wywołanie programu interpretatora poleceń z parametrem: /C NazwaPlikuOfiary.

Ciekawym „udoskonaleniem” techniki opisanej powyżej, jest sposób infekcji stosowany przez wirusy towarzyszące, które wykorzystują zmienną środowisko-

wą PATH (ang. Path companion infectors). Zmienna ta określa listę katalogów przeszukiwanych przez DOS'a podczas uruchamiania programu. Wirus korzystający z tej techniki tworzy plik, który zawiera kod wirusa w innym katalogu, znajdującym się w zmiennej środowiskowej PATH przed katalogiem, w którym znajduje się zarażana ofiara. W takim wypadku infekcję można zastosować dla dowolnego pliku z *.com, *.exe, *.bat, ponieważ kolejność uruchamiania zależna jest przede wszystkim od zawartości zmiennej. Przykładowo:

PATH = C:\,C:\DOS;C:\Windows, a w katalogu C:\DOS umieścimy plik WIN.BAT, to podczas kolejnego wywołania systemu WINDOWS (przez uruchomienie programu

C:\WINDOWS\WIN.COM bez podawania ścieżki, czyli najczęściej WIN) z katalogu innego niż

C:\WINDOWS, system uruchomi najpierw plik C:\DOS\WIN.BAT, a ten dopiero uruchomi właściwy program

C:\WINDOWS\WIN.COM.

2.3 Techniki tworzenia wirusów:

2.3.1 Wirusy wielopostaciowe

Od dawna twórcy wirusów marzyli, aby ich „dzieła" były niewykrywalne przez skanery antywirusowe. Rozwiązanie było proste: wczesne skanery antywirusowe posługiwały się próbką (łańcuchem bajtów charakterystycznych) ze złapanego i przeanalizowanego wirusa. Taki skaner przeszukując plik porównywał jego strukturę ze składowanymi w swojej bazie próbkami. W razie wykrycia podobieństwa wszczynany był alarm. Wystarczyło stworzyć wirusa, z którego nie można było pobrać próbki. Aby było to możliwe, wirus po każdym swoim powieleniu powinien wyglądać inaczej. Początkowo wprowadzono procedury szyfrujące kod wirusa za pomocą stałego lub zmiennego klucza. Ta procedura zawsze wyglądała jednakowo i z niej można było wyznaczyć bajty charakterystyczne. Następnie programiści poszli dalej. Aby „zamydlić oczy" skanerowi wprowadzono do kodu procedury deszyfrującej dodatkowych, nieistotnych dla algorytmu instrukcji, zmienianych podczas każdej infekcji. W odpowiedzi na to autorzy skanerów antywirusowych wprowadzili do swoich próbek tzw. znaki zastępcze (np. bajt ignorowany, przyjmujący dowolną wartość). Kolejnym ruchem autorów wirusów było utworzenie algorytmów generujących od kilkudziesięciu do nawet 1 miliarda

różnych postaci procedury deszyfrującej. Przy procedurach, które generują małą ilość wariantów możliwe jest wykrywanie przez zapisanie w bazie skanera wszystkich możliwych do wygenerowania ciągów. Jednak przy dzisiejszych możliwościach autorów i ich wirusów ta metoda wykrywania nie zdaje egzaminu. Autorzy nowoczesnych wirusów stosują metody: zastępowania i przestawiania instrukcji procedury deszyfrującej, mieszania instrukcji właściwego kodu procedury z instrukcjami „jałowymi" np. NOP (nic nie rób) oraz rozsiewania kodu procedury deszyfrującej w kodzie nosiciela. Metoda szyfrowania polimorficznego jest również stosowana dla kodu wirusa rezydującego w pamięci komputera. Utrudnia to jego identyfikacje i obezwładnienie.

2.3.2 Wirusy utajnione (ang. Stealth)

Jedną z metod uczynienia wirusa niewykrywalnym jest jego utajnienie. Na ogół kod wirusa jest widoczny w kodzie zarażonego programu. Możemy się o tym przekonać oglądając zarażony program np. edytorem binarnym. Metoda utajniania polega na podsuwaniu programom czytającym zarażony plik, obrazu jego sprzed infekcji. Wirus wykorzystujący technikę STEALTH przechwytuje odpowiednie przerwania i na żądanie odczytu odkaża nosiciela (wirusy plikowe) lub podsuwa oryginalny kod ze swojej przechowalni (wirusy dyskowe). W przypadku wirusów plikowych plik odkażony po zamknięciu jest ponownie infekowany. Wirusy dyskowe ukrywają swój kod na dysku również w inny sposób. Formatują sobie dodatkową ścieżkę, na której umieszczają swój kod. Do tak spreparowanej ścieżki system operacyjny nie ma dostępu i kod wirusa nie jest narażony na wykrycie. Wirusy typu STEALTH przekłamują odczyty rozmiaru pliku, odejmując od oryginalnego rozmiaru wielkość wirusa. Użytkownik komputera nie zauważy wiec faktu powiększenia się rozmiarów zbiorów na skutek infekcji. Aby ukryć fakt rezydowania w pamięci komputera wirusy typu STEALTH podsuwają programom oryginalne adresy wektorów przerwań oraz ukrywają zajęte przez siebie bloki pamięci oznaczając je najczęściej jako nieprzydzielone.

2.3.3 Wirusy opancerzone (ang. Armory)

Dobry wirus musi nie tylko się ukrywać, ale również musi być odporny na jego analizę. Aby zapobiec deassemblacji kodu wirusa, autorzy wstawiają do jego kodu wiele pojedynczych bajtów dobranych w taki sposób, aby przy próbie przetłu-

maczenia go występowały przekłamania. Procesor wykonujący rozkazy kodu wirusa w jednoznaczny sposób „wie”, jakie rozkazy pobrał i ma wykonać, lecz program tłumaczący ten kod w mniejszym lub większym stopniu nie jest w stanie zinterpretować instrukcji, które zostały obstawione „lewymi bajtami”. Inną metodą analizy kodu wirusa jest jego śledzenie pod kontroli programu śledzącego (ang. debugger). W tym trybie kod wirusa jest wykonywany krok po kroku. Aby to było możliwe debugger wstawia w kodzie śledzonym specjalne bajty tzw. punkty zatrzymania (ang. breakpoint). Jest kilka metod, aby utrudnić taka analizę. Pierwszą metoda jest usuwanie z kodu wirusa punktów zatrzymania. Aby w praktyce to zadziałało wirus musi być już aktywny w pamięci. Z częstotliwością np. 18 razy na sekundę skanuje swój kod i sprawdza czy nie uległ modyfikacji, jeżeli tak to odtwarza zmienione bajty na podstawie sum kontrolnych. Taki wirus potrafi też np. restartować komputer, jeżeli wykryje uruchomiony program śledzący. Inna metoda polega na użyciu instrukcji "zabójczych" dla programu śledzącego np. wywołanie przerwań, które on wykorzystuje, operacje na stosie. Kolejna metoda to wykorzystanie mechanizmu procesora polegającego na przyjmowaniu nowych rozkazów, podczas gdy rozkazy wcześniej pobrane są wykonywane. Zasada jest prosta: instrukcja poprzedzająca modyfikuje instrukcje następną. Gdyby wykonać ten kod z pełną prędkością procesora, czyli bez śledzenia to modyfikacja ta nie doszłaby do skutku. Powodem tego jest to, że modyfikacja odbyłaby się w pamięci operacyjnej komputera a nie w buforze procesora. Natomiast pod nadzorem programu śledzącego bufor procesora jest odświeżany po każdej instrukcji śledzonego programu wiec taka modyfikacja zostanie „dostrzeżona” przez procesor. W ten sposób wirus może obronić się przed wścibskimi programistami lub amatorami dłubania w cudzych programach.

2.3.4 Wirusy Boot sector'a

Wirusy tego typu zmieniają zawartość sektora głównego dysku (boot sector'a) lub sektora ładowania. Zamiast prawdziwego kodu zapisują tam część samego siebie, a dobrą kopię zapisują zazwyczaj w innym miejscu. Takie wirusy uaktywniają się tylko podczas startu z zarażonego dysku. Kiedy „ruszymy” z takiego nośnika wirus znajdujący się tam zostaje uaktywniony. Wczytuje on wówczas resztę swojego kodu, który się tam nie zmieścił i prawdziwy sektor. Jeśli mamy zainfe-

kowany dysk twardy, to by go wyleczyć trzeba uruchomić komputer z dyskietki systemowej i uruchomić dobry program antywirusowy.

2.3.5 Hybrydowe

Wirusy hybrydowe, są to wirusy, które łączą w sobie różne typy wirusów. Wirusów tych jest bardzo wiele. Rozprzestrzeniają się one bardzo szybko. Najczęstsze łączenie typów to: wirus plikowy i boot sektora.

2.3.6 Polimorficzne

Wirusy tego typu są najgroźniejsze, gdyż najtrudniej jest je wykryć. Twórcy wirusów, by utrudnić życie programistom piszącym programy antywirusowe zaczęli szyfrować swoje dzieła. Szyfrowane są one w różny sposób, np. przez XOR - owanie. Każda kopia wirusa jest, więc inna, ale nie do końca, gdyż procedura szyfrująca jest zawsze taka sama i po niej skanery rozpoznają wirusa. Jest na to jeden lek. Trzeba szyfrować również procedurę szyfrującą, ale jak? Otóż zobaczmy na kody instrukcji: Wszystkie one wykonują to samo zadanie. Zerują rejestr AX. Istnieje jeszcze wiele innych instrukcji, które wykonują to samo zadanie, a mają inne kody, np. INC można zastąpić przez ADD, itp. W ten właśnie sposób działają wirusy polimorficzne. Procedura szyfrująca wirusa za każdym razem jest inna, mimo, że wykonuje to samo zadanie. W ten sposób może mieć kilkaset różnych postaci i dlatego skanery się po prostu gubią. Ten typ wirusa może zmieniać swoją sygnaturę lub procedurę operacyjną przy każdej próbie infekcji, przez co staje się on trudniejszy do wykrycia przez oprogramowanie antywirusowe. Na przykład wirus Bugbear rozprzestrzenia się za pośrednictwem załączników wiadomości e-mail i sieci lokalnych, ale pozostaje trudny do wykrycia dzięki swojej polimorficznej naturze. Inne wirusy, takie jak Sobig, które nie są polimorficzne, mogą nie zostać wykryte przez nie zaktualizowane oprogramowanie antywirusowe, ponieważ występują w kilku odmianach. Kiedy użytkownik otwiera zainfekowany załącznik, wirusy te zwykle kopiują się do folderu systemowego Windows, a następnie modyfikują zawartość rejestru tak, aby zostały uruchomione automatycznie przy ponownym uruchomieniu systemu. Następnie pobierają książkę adresową z oprogramowania obsługującego pocztę elektroniczną użytkownika i wysyłają swoje kopie pod każdy adres znaleziony na liście kontaktów. W wiadomościach tych podawane jest fałszywe nazwisko nadawcy, co utrudnia wykry-

cie prawdziwego źródła wiadomości. Temat wiadomości i tytuł załączonego pliku mogą być różne i często są przypadkowe. Ogólnie należy zachować ostrożność w przypadku wiadomości, których tytuły wyglądają na zbyt piękne, aby mogły być prawdziwe, np. „Your Gift" (Twój prezent), „£150 Free Bonus!" (Darmowy bonus 150 funtów) czy „Amazing!" (Niesamowite!). Trzeba też podejrzliwie traktować wiadomości wyglądające jak zwykłe wiadomości e-mail, zapytania i/lub biuletyny, ponieważ np. wirus BugBear potrafi się maskować w taki sposób. Pliki załączników często mają podwójne rozszerzenie i występują w formatach plików *.exe, *.scr lub *.pif. Ponadto wirusy te często instalują konie trojańskie lub programy rejestrujące naciskane przez użytkownika klawisze, które wysyłają te informacje do autora wirusa. W ten sposób wpisywane przez użytkownika hasła i numery kart kredytowych mogą być przesyłane do hakerów.

2.4 Generatory wirusów

Są to programy, które umożliwiają stworzenie wirusa bez znajomości systemu i mechanizmów wykorzystywanych przez wirusy. Niestety te „narzędzia" dostępne są w Internecie praktycznie dla każdego. Korzystając z gotowych modułów w asemblerze można utworzyć wirusa o zadanych parametrach, które można najczęściej wybrać za pomocą zwykłego menu, więc praktycznie może to zrobić nawet „zielony" użytkownik. Można określić zakres obiektów infekowanych, rodzaj efektów „specjalnych". Oprócz kodu wynikowego wirusa, (czyli gotowego do uruchomienia) generatory tworzą zazwyczaj również dobrze opisane źródła w asemblerze, co umożliwia zainteresowanym nauką pisania wirusów douczanie się.

3 Rozdział:
Ochrona przed wirusami i robakami.

W 1997 roku miało miejsce wiele włamań i innych ataków sieciowych o mniejszym znaczeniu. Wprawdzie, w świetle informacji, jakie obecnie można zdobyć w Polsce, komercyjna przestępczość komputerowa nie jest jeszcze w naszym kraju dużym problemem. Tym niemniej z analizy sytuacji wynika, że w dużej mierze polski Internet komercyjny nie jest przygotowany na odpieranie ataków hakerów. Podobnie jak na całym świecie, i w Polsce coraz więcej firm i instytucji podłącza się do światowej infostrady, jaką jest Internet. Niestety, jedynie niewielki procent tych przedsiębiorstw widzi realnie potrzebę zapewnienia swoim

sieciom lokalnym należytego poziomu bezpieczeństwa. Przedsiębiorstwa, których kierownictwo pragnie rozwiązać te zagadnienie na odpowiednim poziomie, najczęściej trafiają na różne problemy. Do najważniejszych z nich należą:

a. Brak fachowej kadry,

b. Mała dostępność wiarygodnych źródeł informacji o zagrożeniach i możliwości skutecznego przeciwdziałania,

c. Brak kompleksowej wizji systemu bezpieczeństwa.

Chcielibyśmy na moment zatrzymać przy tych punktach. Niestety, nadal w Polsce trudność sprawia znalezienie odpowiedniej osoby na stanowisko administratora sieci. Zatrudnienie etatowego specjalisty od bezpieczeństwa jest rzeczą jeszcze bardziej skomplikowaną. Dlatego też firmy i instytucje, których istotne dane opracowywane i przechowywane są w systemach informatycznych oraz przesyłane za pośrednictwem sieci komputerowych (w tym także za pośrednictwem Internetu), powinny częściej niż obecnie korzystać z pomocy fachowców, którzy zajmują się profesjonalnie tematyką szeroko pojmowanego bezpieczeństwa danych. Osobom, które dotychczas nie zetknęły się z zagadnieniami bezpieczeństwa danych, często sprawia trudność wyobrażenie mnogości zagrożeń, na jakie we współczesnych warunkach narażony jest system informatyczny przedsiębiorstwa. Tworząc mechanizmy bezpieczeństwa w przedsiębiorstwie, należy wziąć pod uwagę jedynie rozwiązania kompleksowe, zapewniające maksimum bezpieczeństwa, jakie można uzyskać w zamian za przeznaczone na ten cel fundusze. Należy pamiętać o jednoczesnym stosowaniu wielu systemów zabezpieczeń, pracujących na wielu płaszczyznach, począwszy od zapewnienia fizycznego bezpieczeństwa sieci i pracujących w niej komputerów, poprzez instalację odpowiednio dobranego przez specjalistów oprogramowania, na kompleksowo opracowanej polityce bezpieczeństwa i odpowiednim przeszkoleniu pracowników skończywszy. Opracowując system bezpieczeństwa, należy zawsze pamiętać o tym, aby zastosowane środki były adekwatne do ważności chronionych zasobów. W przeciwnym razie może łatwo popełnić błąd, polegający na nieuzasadnionym stosowaniu bardzo drogich rozwiązań w miejscu, gdzie użycie tego typu środków jest ekonomicznie niecelowe. Ważne jest też zwrócenie uwagi zarówno na zagrożenia zewnętrzne, jak i wewnętrzne. Niezbędnym, a często zupełnie pomijanym w polskich przedsiębiorstwach elementem systemu bezpieczeństwa jest odpowiednio skonstruowana polityka bezpieczeństwa, precyzyjnie określająca zarówno proce-

dury postępowania w poszczególnych sytuacjach, związanych z wykonywaniem przez pracowników różnych czynności zawodowych, jak i procedury postępowania w sytuacjach zagrożenia. Bardzo ważne jest dokładne określenie praw i obowiązków wszystkich użytkowników systemu informatycznego z administratorami systemów komputerowych i członkami kierownictwa włącznie.

3.1 Budowa i działanie programów antywirusowych

Jednym z zagrożeń dla danych przechowywanych i przetwarzanych w systemach komputerowych są programy złośliwe, które mogą dostać się do nich wraz z pożądanymi danymi. Ochronę przed tym zagrożeniem stanowi obserwacja kodu, który jest wprowadzany do systemu oraz działań, jakie podejmuje. Oprogramowanie spełniające powyższe funkcje nosi nazwę oprogramowania antywirusowego. Jego praca 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. Budowa programu antywirusowego

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 oferuje następujące funkcje:

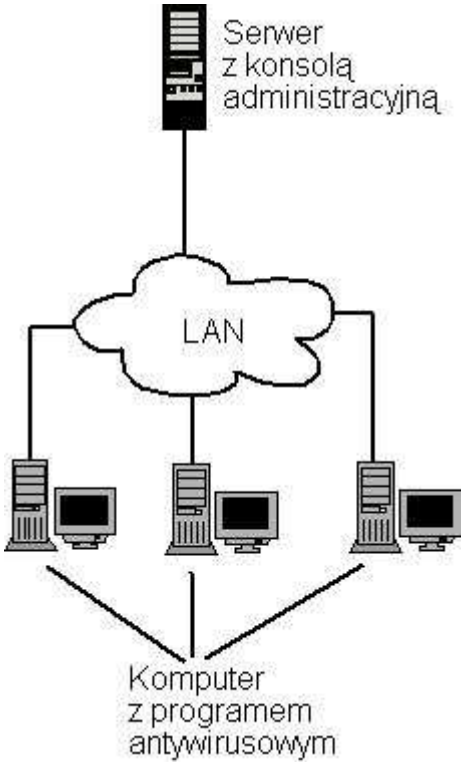
a) Automatyczna i ręczna aktualizacja baz sygnatur wirusów i oprogramowania,
b) Harmonogram zadań,
c) Skanowanie na żądanie wybranych napędów, katalogów i plików,
d) Raporty i statystyki z działania programu,
e) Włączanie i wyłączanie oraz konfiguracja monitora antywirusowego,
f) Włączanie i wyłączanie oraz konfiguracja zasad filtrowania poczty elektronicznej,
g) 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:

a) Konfiguracja dodatkowych usług świadczonych przez producenta,
b) 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 (rysunek 2). 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 niedostępne; użytkownik otrzymuje tylko informacje o decyzji odnośnie do zainfekowanego pliku, jaką podjął administrator.



Rysunek 2. Administracja programami antywirusowymi w środowisku sieciowym

3.1.1 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. 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 de-

kodowanie plików używających słabych algorytmów kodujących i sprawdzanie czy w skanowanych obiektach nie zaszły zmiany.

3.1.2 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:

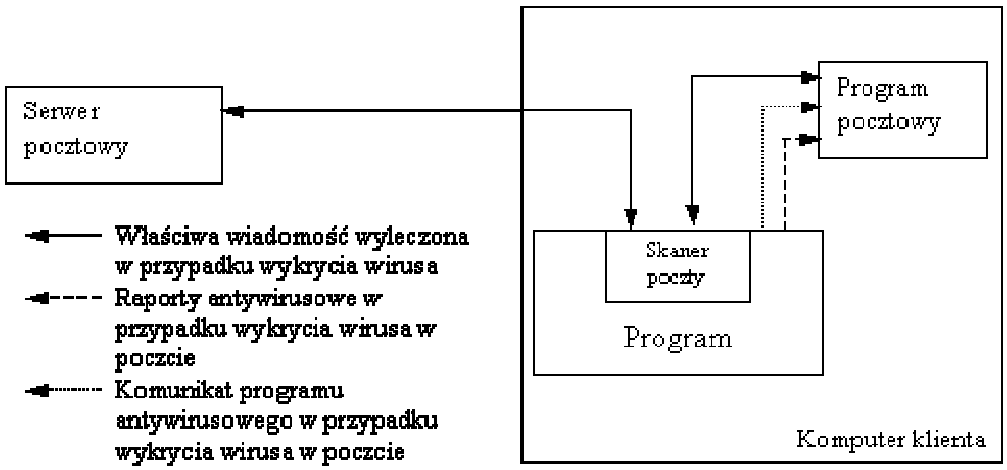
a. Programów rezydentnych systemu DOS (TSR),
b. Sterowników 16- i 32-bitowe VxD systemu Windows (sterowniki urządzeń wirtualnych),
c. Usług systemowych w systemach Windows NT/2000/XP,
d. Paneli sterowania w komputerach Macintosh,
e. Procesów- demonów w systemach UNIX/LINUX.

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.

3.1.3 Skaner poczty elektronicznej

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



Rysunek 3. Ogólna idea działania programu antywirusowego ze skanerem poczty elektronicznej.

Zadaniem Skanera poczty jest odebranie wiadomości od serwera pocztowego lub klienta poczty, przetestowanie jej i zdecydowanie o jej dalszym losie, rysunek 3.

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.

a)

b)

```
##########################################################################
Ostrzeżenie programu Panda Antivirus Platinum:

Plik Undelivered Mail: User unknown byl zainfekowany wirusem Exploit/iFrame i został wyleczony.
##########################################################################
```

Rysunek 4. Przykładowa informacja generowana przez program antywirusowy w przypadku wykrycia zakażonej poczty, wiadomość a) jest wyświetlana na ekranie komputera, b) - dołączana do wiadomości

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.

3.1.4 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:

a) Sumy kontrolne,
b) Heurystyki,
c) 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. Obecnie najczęściej tworzone są jako narzędzia usuwające konkretne wirusy, na przykład Beagle, Bagtrans.

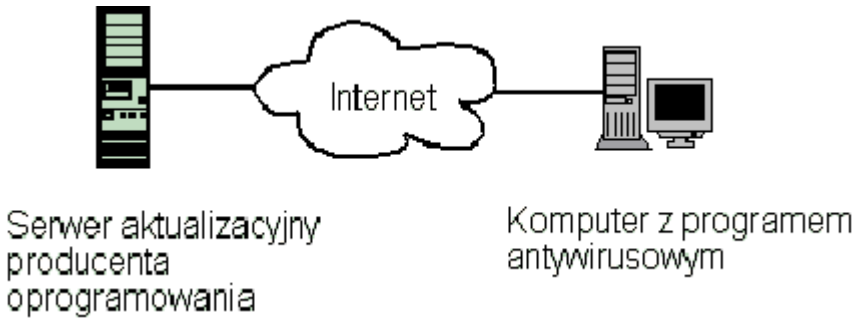
3.1.5 Moduł kwarantanny

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.

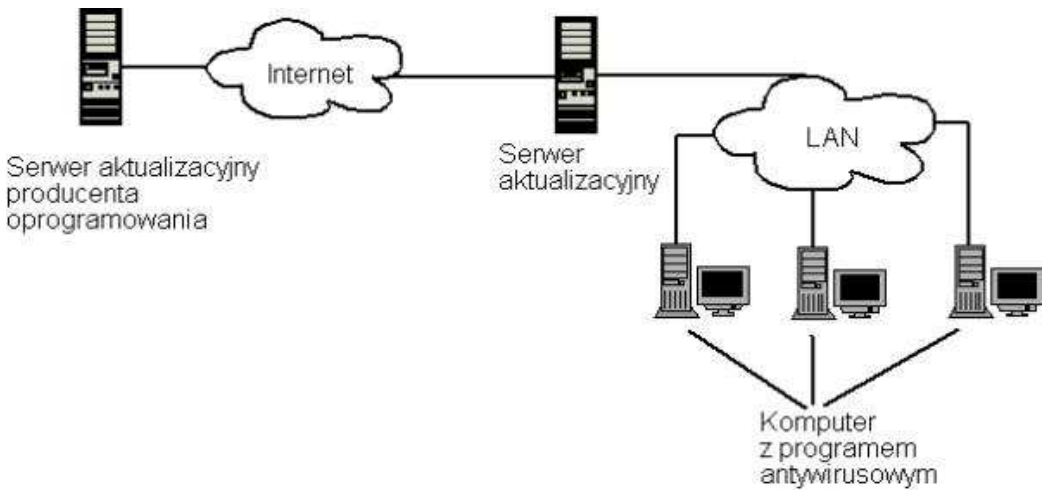
3.1.6 Moduł aktualizacji

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 tygo-

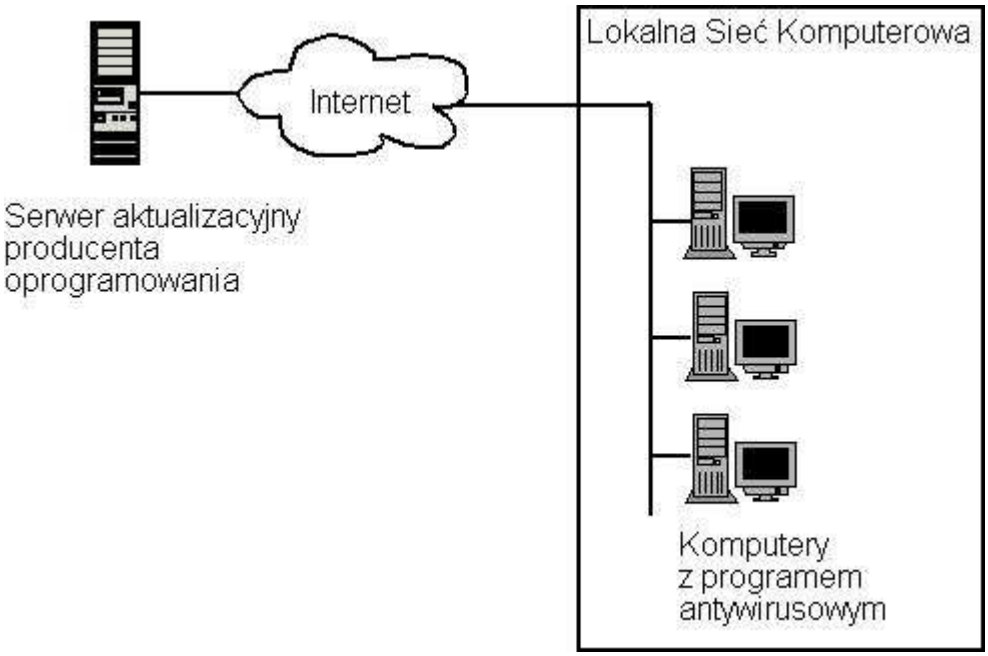
dnia, na przykład zawsze w piątek o 20:00.W zależności od konfiguracji środowiska pracy (jedno stanowisko komputerowe lub komputer pracujący w sieci lokalnej) można zastosować różne strategie aktualizacji. I tak, w przypadku jednego komputera możliwy jest tylko scenariusz aktualizacji bezpośredniej z 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.



Rysunek 5. Aktualizacja programu antywirusowego przez samodzielny komputer

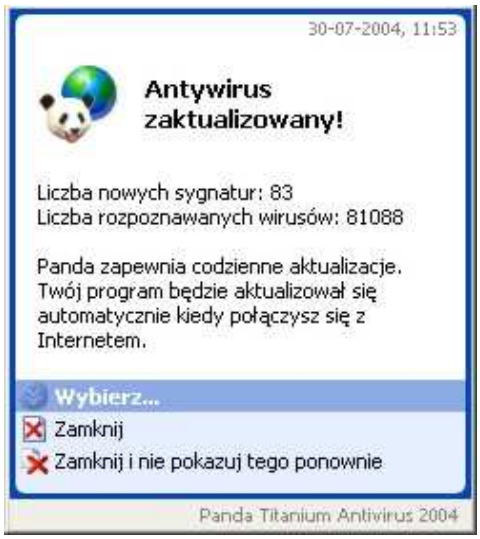


Rysunek 6. Strategia aktualizacji z wykorzystaniem serwera aktualizacji



Rysunek 7. Aktualizacja programu antywirusowego przez komputery pracujące w sieci lokalnej - scenariusz: każdy komputer pobiera aktualizację samodzielnie.

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.



Rysunek 8. Komunikat o zakończeniu aktualizacji generowany przez program

3.1.7 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.

Rysunek 9. Statystyka skanowania podawana przez program Panda Titanium Antyvirus 2004

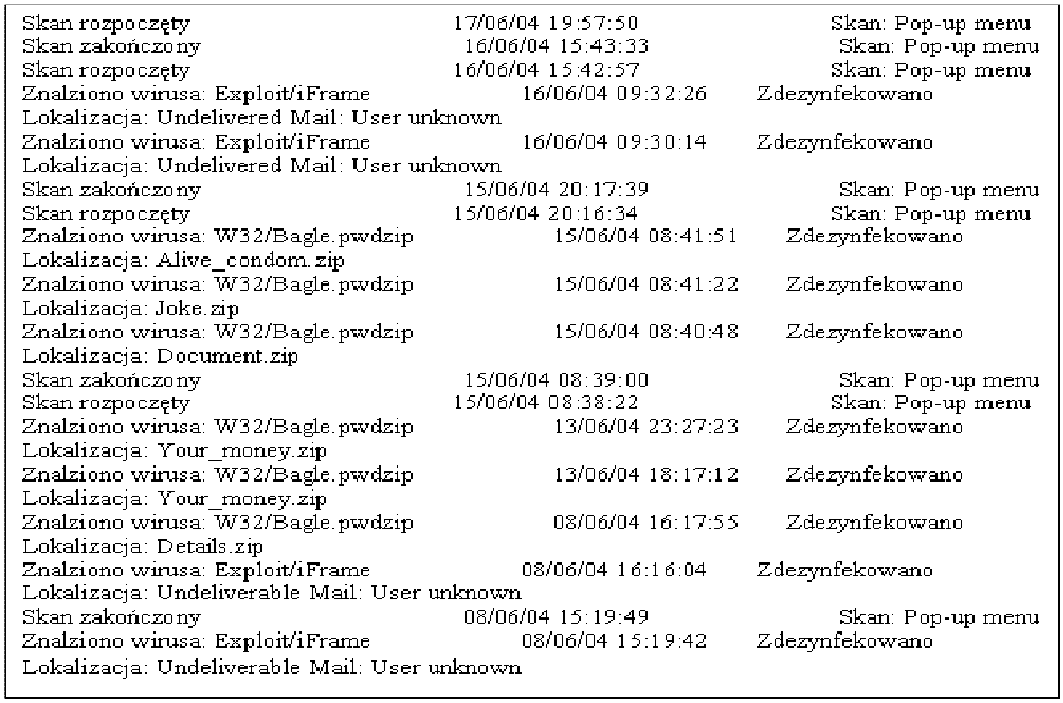
Przykładowy raport pokazany na rysunku 10 podaje informacje o pracy programu uporządkowane w kolumny zawierające informacje (patrząc od lewej) o:

a) Zdarzeniu, kiedy ono się zaczęło i skończyło oraz nazwę wykrytego wirusa.
b) Dacie, kiedy dane zdarzenie zaistniało w postaci dnia i godziny,
c) Informacje dodatkowe, czyli podaje elementy, jakie zostały poddane skanowaniu (napędy, katalogi i nazwy plików),
d) Wynik działania wykonanego przez program na każdym z plików.

3.1.8 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.

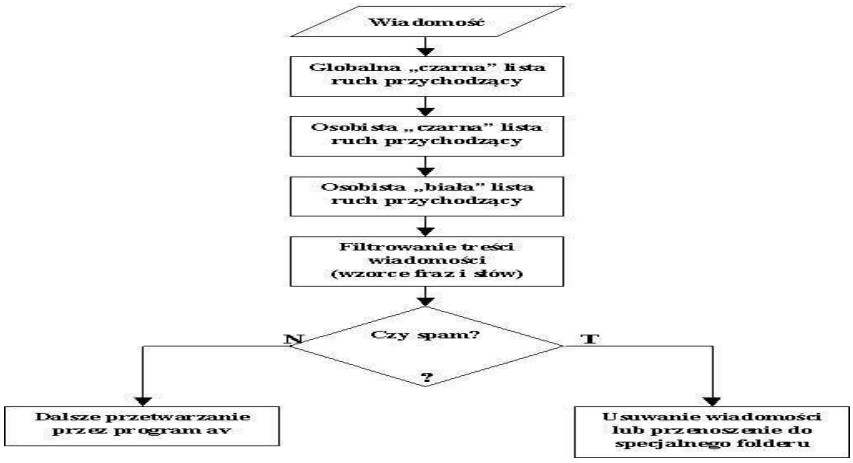


Skan rozpoczęty	17/06/04 19:57:50	Skan: Pop-up menu
Skan zakończony	16/06/04 15:43:33	Skan: Pop-up menu
Skan rozpoczęty	16/06/04 15:42:57	Skan: Pop-up menu
Znalziono wirusa: Exploit/iFrame	16/06/04 09:32:26	Zdezynfekowano
Lokalizacja: Undelivered Mail: User unknown		
Znalziono wirusa: Exploit/iFrame	16/06/04 09:30:14	Zdezynfekowano
Lokalizacja: Undelivered Mail: User unknown		
Skan zakończony	15/06/04 20:17:39	Skan: Pop-up menu
Skan rozpoczęty	15/06/04 20:16:34	Skan: Pop-up menu
Znalziono wirusa: W32/Bagle.pwdzip	15/06/04 08:41:51	Zdezynfekowano
Lokalizacja: Alive_condom.zip		
Znalziono wirusa: W32/Bagle.pwdzip	15/06/04 08:41:22	Zdezynfekowano
Lokalizacja: Joke.zip		
Znalziono wirusa: W32/Bagle.pwdzip	15/06/04 08:40:48	Zdezynfekowano
Lokalizacja: Document.zip		
Skan zakończony	15/06/04 08:39:00	Skan: Pop-up menu
Skan rozpoczęty	15/06/04 08:38:22	Skan: Pop-up menu
Znalziono wirusa: W32/Bagle.pwdzip	13/06/04 23:27:23	Zdezynfekowano
Lokalizacja: Your_money.zip		
Znalziono wirusa: W32/Bagle.pwdzip	13/06/04 18:17:12	Zdezynfekowano
Lokalizacja: Your_money.zip		
Znalziono wirusa: W32/Bagle.pwdzip	08/06/04 16:17:55	Zdezynfekowano
Lokalizacja: Details.zip		
Znalziono wirusa: Exploit/iFrame	08/06/04 16:16:04	Zdezynfekowano
Lokalizacja: Undeliverable Mail: User unknown		
Skan zakończony	08/06/04 15:19:49	Skan: Pop-up menu
Znalziono wirusa: Exploit/iFrame	08/06/04 15:19:42	Zdezynfekowano
Lokalizacja: Undeliverable Mail: User unknown		

Rysunek 10. Przykładowy raport generowany przez program antywirusowy Panda Titanium 2004

3.1.9 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.



Rysunek 11. Schemat filtrowania poczty elektronicznej

Schemat z rysunku 11 obrazuje działanie filtra, w którym wiadomości są najpierw sprawdzane pod kątem występowania nadawców na listach znanych nadawców spamu (RBL), a następnie na stworzonej przez użytkownika „osobistej" liście spamerów. Kolejnym krokiem jest sprawdzenie, czy nadawca widnieje na „osobistej" białej liście, czyli liście osób, od których poczta jest zawsze uznawana za „dobrą", bez względu na wynik działania innych metod klasyfikacji. Ostatnim etapem oceny jest filtrowanie treści wiadomości z użyciem wzorców fraz i słów zawartych w słowniku spamu. Po przejściu tego etapu wiadomość jest oceniana na podstawie wyniku wszystkich poprzednich operacji, do dalszego sprawdzania przez program antywirusowy przechodzi tylko poczta nieuznana za spam. Natomiast wiadomości zaklasyfikowane jako spam są usuwane lub przenoszone do osobnego folderu, gdzie w dowolnym momencie można je przeglądać.

3.1.10 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.

3.1.11 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.

3.2 Programy antywirusowe.

Historia z zainfekowaniem w 1986 r. kilkudziesięciu uniwersyteckich komputerów wirusem Worm Toma Morrisona uznawana jest oficjalnie za pierwszy przypadek rozpowszechnienia wirusa przez Internet. Niestety, ewolucja złośliwych programów nie zatrzymała się wówczas w miejscu. Wraz z udoskonalaniem oprogramowania zabezpieczającego także wirusy stają się coraz bardziej podstępne i niebezpieczne, a to oznacza, że bez nowego, sprawnie działającego i przede wszystkim regularnie aktualizowanego programu antywirusowego nie mamy, co liczyć, że nie dosięgnie nas jakiś mikrob. Program antywirusowy XXI wieku musi być narzędziem, które będzie w stanie radzić sobie nie tylko z bieżącymi zagrożeniami, ale także spełniać wiele innych funkcji. Bardzo ważnym walorem jest np. możliwość monitorowania poczty elektronicznej. Ryzyko zainfekowania komputera tą drogą jest bardzo duże. Kolejna sprawa to wykrywanie i usuwanie koni trojańskich, hoaksów (fałszywych alarmów), podejrzanych apletów, kontrolek ActiveX, dialerów... - lista ta z roku na rok wydłuża się podwyższając poprzeczkę producentom oprogramowania antywirusowego, ale też zapewniając im pracę i chleb na długie lata. Dlatego, mimo rosnących wymagań programów antywirusowych wciąż przybywa, nie ma, więc kłopotu w wybraniem dla siebie najbardziej optymalnego rozwiązania.

3.2.1 Norton antywirus

Skorzystaj z ochrony zapewnianej przez cieszący się największym zaufaniem na świecie program antywirusowy, automatycznie zabezpieczający komputer przed wirusami, robakami i oprogramowaniem typu „spyware”.

- Umożliwia pobieranie aktualizacji zabezpieczeń przez 12 miesięcy i korzystanie z nowych funkcji produktu przez cały rok. Następnie można wykupić kolejne roczne subskrypcje.
- Umożliwia bezpieczne korzystanie z komputera, zapewniając wykrywanie i automatyczne usuwanie wirusów, koni trojańskich i robaków.
- Pozwala na przeglądanie stron internetowych bez ryzyka obserwacji przez niebezpieczne oprogramowanie typu „spyware" lub niepożądane programy typu „adware", przejęcia kontroli nad komputerem czy przekierowania do witryn pobierania aplikacji szpiegowskich.
- Zapewnia odpowiednią ochronę w przypadku pojawienia się nowych wirusów dzięki automatycznemu aktualizowaniu systemu zabezpieczeń.
- Umożliwia bezpieczne otwieranie załączników przesyłanych za pośrednictwem poczty e-mail oraz komunikatorów internetowych, zapewniając przeszukiwanie ich pod kątem występowania zagrożeń.
- Pozwala na tworzenie i udostępnianie plików bez jakichkolwiek ograniczeń, ponieważ nawet skompresowane pliki są skanowane w poszukiwaniu wirusów.
- Automatycznie usuwa wirusy, konie trojańskie i robaki.
- Wykrywa i eliminuje niebezpieczne oprogramowanie typu „spyware", programy śledzące wprowadzane na klawiaturze znaki i inne niepożądane oprogramowanie monitorujące.
- Zapobiega przejmowaniu przez aplikacje typu „spyware" kontroli nad stroną główną ustawioną w przeglądarce internetowej i przekierowywaniu do witryn pobierania tego typu programów.
- Sprawdza załączniki do przychodzących i wychodzących wiadomości e-mail pod kątem obecności wirusów.
- Automatycznie skanuje załączniki do przychodzących wiadomości przesyłanych przez komunikatory internetowe w poszukiwaniu zagrożeń.
- Sprawdza skompresowane pliki archiwalne pod kątem wirusów.
- Blokuje niebezpieczne robaki internetowe, chroniąc system przed zainfekowaniem.
- Automatycznie pobiera aktualizacje w celu ochrony przed nowymi zagrożeniami.
- Automatycznie wykonuje skanowanie w poszukiwaniu wirusów po pobraniu aktualizacji.

- Korzysta z inteligentnych technologii w celu wykrywania nowych robaków i innych zagrożeń, nie czekając na aktualizacje oraz Przygotowuje system do instalacji, oczyszczając go z wirusów.
- Wymagania systemowe
- Windows® XP Home Edition/Professional
- Procesor 300 MHz lub szybszy
- 256 MB pamięci RAM
- 150 MB wolnego miejsca na dysku twardym
- Windows 2000 Pro z dodatkiem SP3 lub nowszym
- Procesor 300 MHz lub szybszy
- 128 MB pamięci RAM
- 150 MB wolnego miejsca na dysku twardym
- Wymagania dotyczące wszystkich instalacji
- Napęd DVD lub CD-ROM
- Microsoft® Internet Explorer, wersja 5.5 lub nowsza (zalecana wersja 6.0)
- Obsługa skanowania poczty elektronicznej dla standardowych programów pocztowych
- Obsługiwane komunikatory internetowe
- AOL® Instant Messenger, wersja 4.7 lub nowsza
- Yahoo!® Instant Messenger, wersja 5.0 lub nowsza
- MSN® Messenger, wersja 4.6, 4.7, 6.0 lub nowsza

3.2.2 NOD 32

3.2.2.1 Serwery pocztowe

Skanowany jest cały ruch pocztowy z i do serwerów: calisto, novci1, novci2, antares i capella. W przypadku znalezienia wirusa przez moduł skanujący, email zawierający wirusa zostanie przeniesiony do kwarantanny. Nasz system nie powiadamia nadawcy ani adresata o znalezieniu wirusa. Funkcja ta została wyłączona, ponieważ, powoduje ona więcej konfuzji i problemów niż pierwotnie zakładano. Wynika to z faktu, że wirusy, podszywając się pod inne osoby, używają fałszywych adresów pocztowych i powiadomienia trafiają do niewinnych osób.

3.2.2.2 Serwery plików

Serwery plików obsługujące laboratoria dydaktyczne Centrum Informatyki (sale: 213, 202B, 203B oraz CI1) i składające się na domenę GALAKTYKA wyposażone są w oprogramowanie antywirusowe, pliki przetwarzane przez serwer są skanowane i w przypadku wykrycia wirusa leczone. W przypadku, gdy leczenie się nie powiedzie lub nie jest możliwe plik jest kasowany.

3.2.2.3 Stacje robocze

- Stacje robocze, czyli wszystkie komputery, które nie są serwerami, zostały wyposażone w oprogramowanie antywirusowe, składające się z:
- modułu rezydentnego AMON - skanujacego w locie pliki ładowane do pamięci komputera,
- modułu internetowego IMON - skanujacego w locie pocztę oraz kod skryptów na stronach internetowych
- modułu skanowania na żądanie NOD32 - skanującego pliki na dyskach twardych oraz wymiennych, takich jak stacje dyskietek, stacje CD-ROM, pen drive, dyski mapowane przez sieć
- modułu pocztowego EMON (opcjonalnie) - skanującego repozytoria pocztowe (PST) w programach opartych na MS Exchange: Outlook 95/97/2000/XP i nowsze.

Programy na stacjach roboczych nie wymagają żadnego nadzoru ze strony użytkownika: aktualizują się co godzinę, mają zabezpieczone hasłem konfiguracje, które są zarządzane centralnie z serwera tzw. kopii dystrybucyjnej.

3.2.3 MKS_VIR

3.2.3.1 Monitor antywirusowy

Monitor antywirusowy jest rezydentnym modułem, który na bieżąco kontroluje uruchamianie i zapisywanie plików w systemie oraz na innych nośnikach (np. dyskietce).

3.2.3.2 Skaner dyskowy

Skaner jest wygodnym narzędziem do sprawdzania wszystkich zasobów komputera pod kątem istnienia zagrożenia. Program może być w prosty sposób skonfigurowany tak by odpowiadał indywidualnym potrzebom użytkownika.

3.2.3.2 Skaner poczty elektronicznej ArcaMail

Skaner poczty elektronicznej jest programem, który w interaktywny sposób skanuje odbierane i wysyłane listy elektroniczne. Może on współpracować z każdym programem pocztowym działającym w oparciu o protokoły POP3 i SMTP.

ArcaMail korzysta z wewnętrznego sterownika systemowego. To rozwiązanie gwarantuje wysoką efektywność skanowania (niewielkie obciążenie systemu) i eliminuje potrzebę zmiany konfiguracji programu pocztowego. ArcaMail został zaprojektowany tak, by stanowić część systemu operacyjnego.

3.2.3.3 Moduł automatycznej aktualizacji

ArcaVir Update jest narzędziem służącym do automatycznej lub ręcznej aktualizacji programu poprzez sieć.

3.2.3.4 Firewall

Firewall zawarty w pakiecie ArcaVir stanowi kolejną warstwę w systemie zabezpieczeń komputera. W dobie internetu firewall jest niezbędnym elementem ochrony komputera, zwiększającym poziom bezpieczeństwa oraz chroniącym dane przed hakerami. ArcaVir Firewall został zaprojektowany tak, by był łatwy w użyciu nawet dla niedoświadczonych użytkowników, jednocześnie posiadając wiele możliwości konfiguracyjnych, które docenią zaawansowani użytkownicy.

3.2.3.5 Monitor rejestru

Monitor rejestru jest aplikacją, która cały czas kontroluje zmiany w newralgicznych obszarach rejestru systemu Windows.Zalety pakietu ArcaVir:
Efektywność działania - zarówno skaner jak i monitor pakietu nie obciążają zbytnio systemu.

Umiejętność usuwania wirusów bez niszczenia zainfekowanych plików.
Ciągłe aktualizacje zapewniają ochronę przed nowopowstałymi zagrożeniami wkrótce po ich ujawnieniu się.

Blokowanie wirusów przy odbieraniu poczty elektronicznej, kopiowaniu plików, uruchamianiu dyskietek i płyt CD.

Bezpłatne wsparcie techniczne dla licencjonowanych użytkowników

Bibliografia

1. http://stasiekjasinski.webpark.pl/historia.htm „Początki Hakerstwa”
2. http://www.cyber.com.pl/archiwum/11/29.shtml „numer 3/98: O bezpieczeństwie sieci słów kilka...”, „Podłoże konfliktu”
3. Wirusy, robaki.
4. http://pl.wikipedia.org/wiki/Strona_g%C5%82%C3%B3wna
5. Piotr Jerzy Durka „Komputer, Internet- cyfrowa rewolucja” wyd. nauk. PWN
6. Hakerzy – Czasopismo komputerowe „Chip”

Wykaz rysunków