Charakterystyka wirusów komputerowych a poprawność działania oprogramowania

Tomasz Prauzner
Instytut Edukacji Technicznej, Wyższa Szkoła Pedagogiczna w Częstochowie

Paweł Ptak
Politechnika Częstochowska, Wydział Elektryczny, Instytut Elektroniki i Systemów Sterowania
Zakład Metrologii i Elektroniki, 42-200 Częstochowa
al. Armii Krajowej 17, tel. (034) 325 08 72, ptak@el.pcz.czest.pl

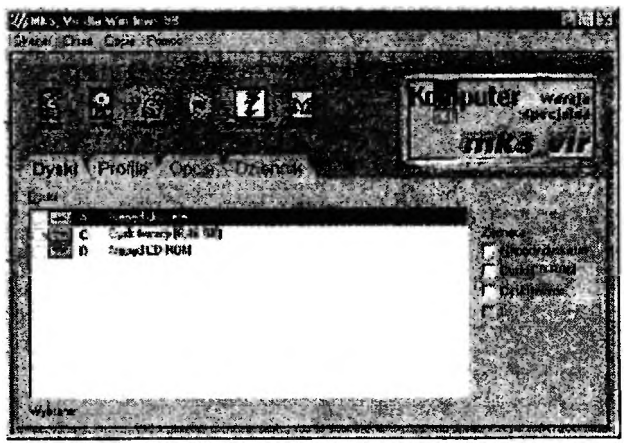
Abstract. A brief characterization of the most often encountered types of computer viruses is presented, pointing to the variety of ways viruses may operate and to the variety of ways they can be fought. The crucial information on viruses concerns the locations in the computer system where they can reside and reproduce. Besides, the main routes of infecting computer systems and the main forms of active viruses are discussed. The basic functions of viruses and phases which can be distinguished in their operation are also described. All the above mentioned points provide a basis for a detailed classification of viruses, which is presented at the end of the paper and followed by some concluding remarks.

I. WSTĘP

Niejednokrotnie każdy gościł na swoim komputerze nowego współużytkownika naszego systemu informatycznego. O ile na temat wirusów komputerowych można znaleźć wiele publikacji i wzmianek na dany temat, o tyle danych recenzji jest studiowana przez nas pobieżnie, aż do pewnego momentu. Moment ten jest najczęściej dla nas dużym zaskoczeniem i nadchodzi zazwyczaj w najmniej pożądanym czasie. Pojawienie się niepokojących objawów w zachowaniu stabilnej pracy systemu komputerowego jest dla nas najczęściej sygnałem do sięgnięcia do pierwszej pomocy w postaci programu antywirusowego. Wydaje się, iż użycie danego programu diagnostycznego jest jedynym lekarstwem w danej chwili. Czy rzeczywiście taki tok rozumowania jest poprawny, to zależy od wielu czynników.

Po pierwsze, najlepszym rozwiązaniem, aby nasz system był wolny od niepokojących gości, jest skrupulatna profilaktyka polegająca na tym, aby oprogramowanie antywirusowe było zainstalowane na naszym komputerze przed pojawieniem się wirusa. Profilaktyka ta jest o tyle ważna, iż jej skuteczność zależy od ciągłej aktualizacji bazy danych powstających nowych wirusów. Zadanie to mogą spełniać przede wszystkim programy w wersji pełnej i zarejestrowanej. Wersje „demo" zazwyczaj szybko tracą swoje zalety (rys. 1).

Po drugie, jeśli jesteśmy pewni, iż przyczyną problemów może być wirus komputerowy, powinniśmy jak najszybciej zareagować i zaopatrzyć się w najaktualniejszą wersję oprogramowania. Tylko taka wersja umożliwi nam wyłapanie wszystkich zainfekowanych plików i ich wyleczenie. Często w książkach czytamy, iż należy wykonywać kopie naszych dokumentów na innych nośnikach danych. Jest to rozwiązanie jak najbardziej godne uwagi. Wiele wirusów działa niestety nieodwracalnie negatywnie na nasze zbiory danych. Jedynym rozwiązaniem jest oczywiście wykonywać jak najczęściej kopie naszych dokumentów.



Rys. 1. Program antywirusowy Marka Sella MkS-Vir

Ze względu na sposoby działania programy antywirusowe można podzielić na następujące rodzaje:

- Programy monitorujące, czyli programy śledzące aktywność uruchamianych na komputerze programów (kontrolują one tylko programy załadowane do pamięci operacyjnej).
- Programy obliczające sumy kontrolne wszystkich programów zapisanych w plikach na dyskach twardych.
- Programy skanujące, czyli programy polujące na określone wirusy i potrafiące je unieszkodliwiać bez zniszczenia programu będącego nosicielem wirusa.

Poniżej przedstawiono krótką charakterystykę najczęściej występujących grup wirusów komputerowych mając na celu pokazanie różnorodności ich działania i sposobów profilaktyki.

II. DEFINICJA WIRUSA KOMPUTEROWEGO

Wirus komputerowy to program, który - tak jak prawdziwy wirus - przyłącza się do innych programów

i jest wraz z nimi przenoszony pomiędzy komputerami. W taki sposób rozprzestrzenia się, infekując nowe programy. W sieciach pojawiły się również tzw. robaki, infekujące kolejne systemy komputerowe. "Robaki" rozmnażają się i przemieszczają same. W latach sześćdziesiątych powstały pierwsze wirusy zwane królikami. Były to programy powielające się i zapełniające system. Obecnie znamy setki odmian i rodzajów wirusów. Mogą one powodować różnorodne szkody: zmieniać lub uszkadzać dane, zakłócać komunikację, wyświetlać komunikaty, przechwytywać informacje, spowalniać pracę systemu, zmieniać ustawienia komputera

Wirus komputerowy jest programem, który instaluje się na komputerze zazwyczaj bez wiedzy ani przyzwolenia jego użytkownika i powoduje niepożądane skutki, groźne zarówno dla pracy samej maszyny, jak też dla danych w niej zawartych. Podobnie jak wirusy znane w biologii dotykają ludzi, tak też wirusy komputerowe są zakaźne, tzn. wędrują z jednej maszyny na drugą.

Powiela się on poprzez zarażanie zbiorów wykonywalnych, jednostek alokacji plików lub sektora startowego nośnika danych (HDD, FDD) oraz dokumentów stworzonych za pomocą pakietów biurowych, takich jak MS Office.

III. Podstawowe wiadomości o wirusach

Miejsca w systemie komputerowym, które mogą być narażone na rozmnażanie wirusów to:

- programy typu EXE, COM,
- pliki z rozszerzeniem OVL, BIN, SYS,
- biblioteki DLL,
- pliki systemowe COMMAND.COM, IBMBIO.COM, IBMDOS.COM,
- tablica partycji dysku stałego,
- boot - sektor dysku lub dyskietki,
- tablica partycji dysku twardego FAT,
- sektory zaznaczone jako uszkodzone tzw. bad sectors,
- zagubione klastery tzw. lost clusters,
- dokumenty programu WORD FOR WINDOWS,
- pisanie makropoleceń może być inspirujące dla autorów wirusów,
- skoroszyty programu EXCEL FOR WINDOWS,
- bazy danych programu ACCESS FOR WINDOWS,
- inne miejsca wymyślone przez komputerowych „terrorystów".

W 99% zakażenie następuje dwoma drogami:

- poprzez dyskietkę, CD-ROM lub dysk wymienny zawierające nielegalne oprogramowanie, dokumenty wytworzone w Microsoft Office czy też programy demonstracyjne, które przechodzą z jednego komputera do drugiego,
- poprzez jakikolwiek kanał łączności: sieć komputerową, modem czy też - ostatnio coraz częściej - przez Internet.

Wirusy komputerowe aktywne mogą pojawiać się pod dwoma postaciami:

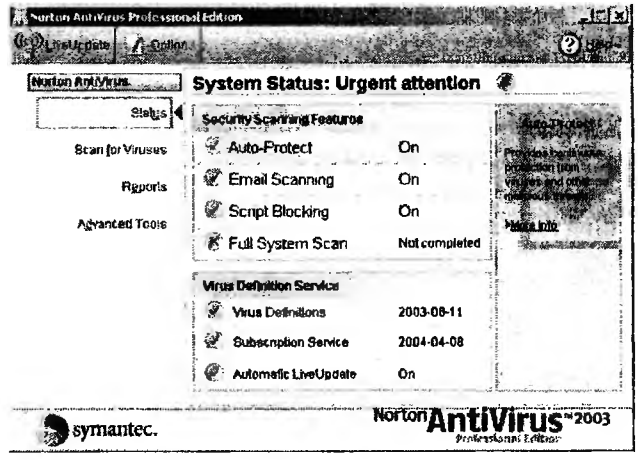
- W pierwszym przypadku powodują one zakażenie, gdy znajdą odpowiedni ku temu moment; w międzyczasie pozostają rezydentne w pamięci komputera.
- W drugim, wirus rozpoczyna swą niszczycielską robotę odpalony zazwyczaj przez jakieś określone zdarzenie (jakąś datę, ilość razy zainicjowania systemu, itp.).

Funkcje wirusów

W funkcjonowaniu wirusów można wyodrębnić dwie fazy:

1. fazę rozmnażania się wirusa,
2. fazę destrukcji.

Faza rozmnażania się wirusa **(I faza - tajna)** polega na umieszczeniu jego zaszyfrowanego kodu w kolejnych miejscach systemu komputerowego, a faza destrukcji polega na ujawnieniu się wirusa. To co wirus w ramach destrukcji **(II faza - jawna)** dokonuje, jest zależne od umiejętności, wiedzy, fantazji i złośliwości twórcy wirusa. Wirusy zwane końmi trojańskimi to programy, które poza wykonywaniem normalnej, na ogół pożytecznej lub rozrywkowej pracy, prowadzą działalność typową dla drugiej fazy działania wirusów, czyli destrukcję w systemie.



Rys. 2. Okno programu Norton AntiVirus

IV. Szczegółowa klasyfikacja wirusów

A. Wirusy plikowe (tzw. "zwykłe", file viruses)

Wirusy plikowe to najstarsza rodzina tych programów. Każdy wirus przed dokonaniem szkód najpierw ulega replikacji, dlatego rozwój "przemysłu" wirusowego 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).

Zasada działania:

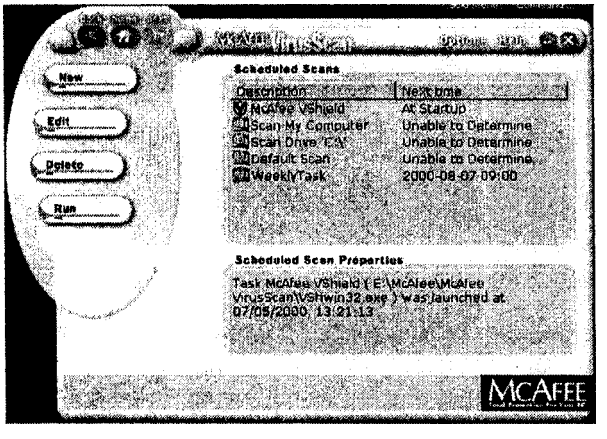
Infekcja następuje poprzez dopisanie kodu wirusa na końcu pliku (wirusy starsze) lub modyfikację jego początku i dopisanie kodu w środku lub na końcu (wirusy nowsze, atakujące niewykonywalne pliki). Załadowanie zainfekowanego pliku do pamięci jest równoznaczne z uaktywnieniem wirusa. Wiele wirusów nie niszczy zaatakowanego pliku, dzięki czemu może po aktywacji wykonać program nosiciela, tak że użytkownik niczego nie podejrzewa.

B. Wirusy sektora startowego dysku (wirusy boot sektora, boot sector viruses)

Innym nosicielem wirusa może być sektor startowy nośnika danych, takiego jak dysk twardy (MBR - Master Boot Record) czy dyskietka (Boot sector). Wirusy tego typu są szczególnie groźne. Wynika to z faktu, iż po uruchomieniu komputer próbuje wczytać system, który jest zapisany w pierwszym sektorze dysku lub dyskietki. Należy mieć świadomość, że każda sformatowana dyskietka, nawet niezawierająca plików systemowych, posiada boot sektor, a więc jako taka może zawierać wirusa.

Zasada działania:

Wirus tego typu może ulokować się w MBR i np. zniszczyć jego zawartość, uniemożliwiając tym samym dostęp do dysku. 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 przeznaczonym do ich zwalczania.



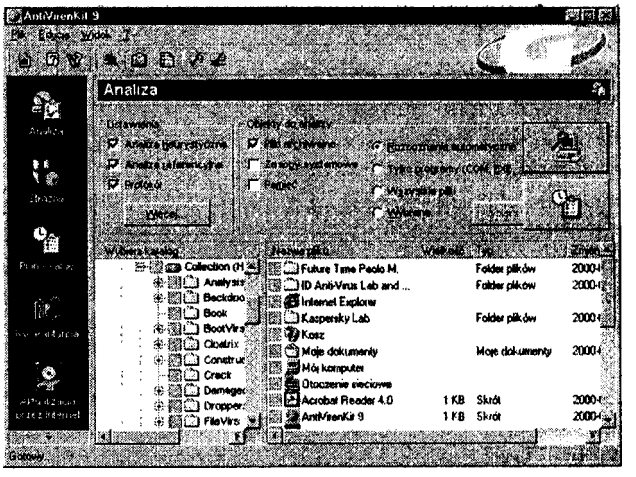
Rys. 3. Okno programu antywirusowego MCAFEE

C. 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.

Zasada działania:

Wirusy atakujące JAP zmieniają 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).



Rys. 4. Przykładowy ekran programu AntiVirenKit

D. Makrowirusy

Makrowirusy należą do najmłodszej rodziny wirusów. Ich powstanie związane jest z wprowadzeniem do pakietów biurowych (np. MS Office, Lotus SmartSuite czy Corel WordPerfect) języków pozwalających na tworzenie makr, takich jak np. Visual Basic for Applications (VBA).

Zasada działania:

Większość makrowirusów Worda wykorzystuje fakt, że szablony dokumentów mogą zawierać makra. Wirus uaktywnia się w chwili otwarcia zainfekowanego dokumentu, po czym zaraża zdrowe zbiory z rozszerzeniem *.doc i zapisuje je jako szablony (dokumenty nie mogą zawierać makr). W ostatnim kroku jedno lub kilka automatycznie wykonywanych makr zostaje zastąpionych kodem wirusa.

E. Wirusy typu stealth i wirusy polimorficzne (stealth & polymorphic viruses)

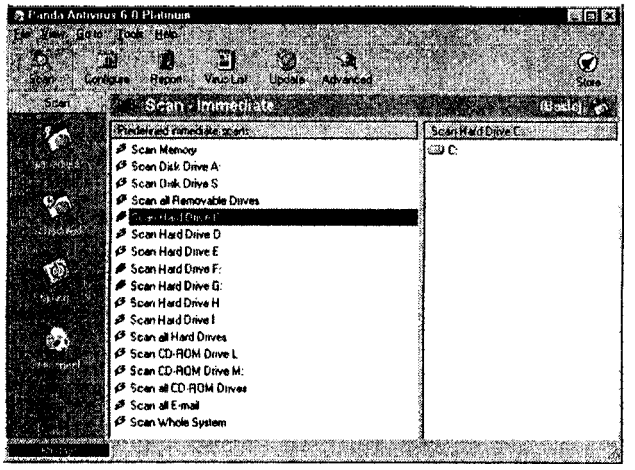
W zasadzie wszystkie wymienione wcześniej wirusy mogą (choć nie muszą) należeć do tej grupy. Ich powstanie związane jest z postępem w dziedzinie ich wykrywania. W pierwszych latach obecności wirusów każdy miał swoją sygnaturę (charakterystyczny tylko dla siebie ciąg bajtów). Sytuacja zmieniła się, gdy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

Wirusy polimorficzne nie mają stałej sygnatury, ponieważ ich kod zmienia się samoczynnie przy każdej infekcji. Wirusy stealth są to wirusy, które podczas próby dostępu do zarażonego pliku lub sektora dysku przez program antywirusowy potrafią "w locie", chwilowo naprawić uszkodzone dane i zatuszować swą obecność.

V. Wirusy rozprzestrzeniające się przez e-mail

Robaki internetowe nowej generacji rozprzestrzeniają się automatycznie za pośrednictwem poczty e-mail.

Po pierwsze wirusy te używają programu do obsługi poczty elektronicznej, tak by on sam rozesłał zainfekowaną wiadomość. W prawie wszystkich przypadkach technika ta dotyczy programu Outlook, gdyż jest on najpopularniejszym klientem poczty, co zwiększa szansę na skuteczne rozprzestrzenianie się wirusa. Dobre oprogramowanie antywirusowe również pozwala skutecznie chronić przed tego typu niebezpieczeństwem. Nowoczesne heurystyczne metody skanowania pozwalają unieszkodliwić nawet nieznane dotychczas wirusy. Robaki internetowe pisane pod kątem Outlooka są tworzone zwykle przy użyciu Visual Basica, stosunkowo prostego języka programowania, który zawiera wbudowane funkcje do obsługi Outlooka.



Rys. 5. Przykład programu antywirusowego skanującego pocztę elektroniczna e-mail

Drugą powszechnie wykorzystywaną metodą rozsyłania kodu wirusa jest bezpośrednie korzystanie z protokołu obsługi poczty Simple Mail Transfer Protocol (SMTP). W tym przypadku wirus może działać skutecznie niezależnie od rodzaju klienta pocztowego. Technika ta jest stosunkowo prosta. Nawiązywane jest połączenie przez SMTP z serwerem poczty, który umożliwia rozsyłanie listów bez weryfikacji nadawcy i jego dalsze wykorzystanie, by rozprzestrzenić wirusa. Wymagane jest połączenie z Internetem i wysłanie odpowiednich komend przez port 25 TCP/IP. Można wykorzystać domyślny serwer SMTP albo jeden z listy zaszytej w kodzie wirusa. Bardzo często, jeżeli serwer na to pozwoli, ukrywane są adresy IP komputerów współuczestniczących w całym procederze czy też fałszowana jest domena, z której przesyłka pochodzi. Sprawia to, że e-mail przenoszący infekcję jest niemal całkowicie anonimowy. Autorzy wirusów skłaniają się więc w stronę bardziej ogólnego podejścia opisanego powyżej. W rezultacie ci wszyscy użytkownicy, którzy używali mniej popularnych programów pocztowych (Pegasusa, Eudory i innych) jako gwarancji bezpieczeństwa są w błędzie. Ryzyko jest zmniejszone, ale wciąż pozostaje nie wyeliminowane. Jedynym rozwiązaniem umożliwiającym ochronę przed wszelkiego rodzaju robakami internetowymi jest instalacja oprogramowania antywirusowego na różnych poziomach sieci komputerowych. Pierwszym punktem obrony powinno być połączenie z Internetem, przez które tak czy inaczej wszystkie e-maile muszą przejść. Instalacja systemu blokującego niebezpieczny kod w tym miejscu ochroni sieć lokalną, jej serwery i stacje robocze przed niebezpieczeństwem z zewnątrz. Wewnętrzny przepływ wiadomości również musi być chroniony, tak na poziomie serwerów, jak i pojedynczych stacji roboczych, gdyż wirusy mogą również rozprzestrzeniać się w strukturach lokalnych.

IV. Wnioski

Jak widzimy, różnorodność wirusów jest olbrzymia. Każdy z nich ma określone cele do spełnienia, lecz najczęściej destrukcyjne. Czasami są to niegroźne „psikusy", ale najczęściej ich obecność sprawia nam naprawdę poważne problemy. Dlatego też obecnie należy unikać nielegalnych źródeł zdobywania programów drogą „koleżeńską", polegającą najczęściej na wymianie oprogramowania z różnych źródeł, należy zainstalować program antywirusowy, który cały czas czuwa i wychwytuje wszelkie zagrożenia podczas pracy oraz co wydaje się najrozsądniejsze – wykonywać kopie własnych prac, dając tym samym nam olbrzymi komfort pracy.

Literatura

[1] Dudek A., Nie tylko wirusy, Helion Wydawnictwo S. A. Gliwice, 1998.

[2] Błaszczyk A., Wirusy, Wydawnictwo RM, 2002.

[3] Zawadzki W., Wirusy komputerowe, Leczenie i profilaktyka, Helion, 1991.

[4] Harley D., Slade R., Gattiker U. E., Wirusy - Cała prawda, Translator, 2003.

[5] Wang W., Internet, hakerzy, wirusy..., ReadMe, 2001.

Streszczenie. Przedstawiono krótką charakterystykę najczęściej występujących grup wirusów komputerowych mającą na celu ukazanie różnorodności w sposobie działania i sposobie zapobiegania. Zaprezentowano podstawowe wiadomości o wirusach, a także miejsca w systemie komputerowym, które mogą być narażone na rozmnażanie wirusów. Omówiono drogi zakażeń systemów informatycznych oraz postacie wirusów komputerowych aktywnych. W artykule podano również podstawowe funkcje wirusów oraz fazy, jakie możemy wyodrębnić w funkcjonowaniu wirusów. Na koniec przedstawiono szczegółową klasyfikację wirusów.