WIRUSY KOMPUTEROWE

1. WIRUS TO...

Wirus komputerowy (ang.Virus) jest to program posiadający zdolność samodzielnego powielania się i przenoszenia się na inne komputery. Terminem „wirus” często niesłusznie określa się wszystkie destrukcyjne programy np. konie trojańskie, które są ukrytymi w programach kodami, sprawiającymi, że programy takie po uruchomieniu komputera realizują oprócz swoich funkcji także różne nieprzyjemne dla użytkownika działania jak np. zawieszenie systemu operacyjnego, usuwanie plików czy też wyświetlanie na ekranie różnych komunikatów. Wirus jest dość podobny do zwyczajnej grypy, która atakuje ludzi. Wirusy doczepiają się do plików. Drogą przenoszenia mogą być wszelkiego rodzaju nośniki danych oraz media komunikacyjne. Dawniej wirus uruchamiany był przez uruchomienie zainfekowanego programu. Obecnie wirus niejednokrotnie nie wymaga uruchomienia przez ofiarę zainfekowanego pliku - oprogramowanie komputera, mające za zadanie jak najbardziej ułatwić życie użytkownikowi, automatycznie uruchamia pliki i wykonuje różnorakie zadania. Do zarażenia dochodzi przeważnie podczas kopiowania. Wirusy komputerowe są bardzo zróżnicowane pod względem działania - począwszy od "nieszkodliwych" wirusów samopowielających się, poprzez wirusy infekujące pliki, do wirusów niszczących pliki, a nawet całe zawartości dysków twardych.

Pierwsze wirusy komputerowe dla IBM PC pojawiły się już w 1986 r., ale jeszcze dwa lata później wiele postaci świata informatycznego wątpiło w ich istnienie. Peter Norton (wg „Patologii wirusów komputerowych” Davida Ferbrache’a) nazwał wirusy komputerowe wielkomiejskim mitem i porównał ich istnienie z historiami o krokodylach w kanałach Nowego Jorku. Ta opinia dość dobrze oddaje stan wiedzy na temat wirusów w środowisku komputerowym u progu lat dziewięćdziesiątych. Sytuacja zmieniła się dopiero kilka lat później, po odkryciu wykreowanego przez media na pierwszą gwiazdę przemysłu informatycznego, wirusa Michael Angelo. Dzięki nagłośnieniu jego istnienia i masowej akcji ostrzegawczej Michael Angelo wywarł pozytywny wpływ i uświadomił milionom użytkowników komputerów na całym świecie grożące im (oraz ich danym) niebezpieczeństwo.
W ciągu minionych kilku lat zainteresowanie wirusami komputerowymi znacznie spadło. Wielu użytkowników oswoiło się z możliwością infekcji i nauczyło się minimalizować jej skutki. Niestety, w dalszym ciągu liczne grono osób korzystających z komputerów, co gorsza również na stanowiskach kierowniczych, nie zdaje sobie sprawy z potencjalnego zagrożenia. Pod względem działania wirusy komputerowe przypominają swoje biologiczne pierwowzory. Zamiast ludzkiego organizmu, infekują dysk (dyskietkę) lub program, umieszczając w nich swój kod. Główne zadanie wirusa komputerowego polega na jak najszerszym rozpowszechnieniu się, a nie „szkodzeniu”, jak mylnie sądzi wielu użytkowników. Niszczenie danych na dysku, wyświetlanie informacji na ekranie, blokowanie systemu i nienormalne zachowanie się komputera to drugorzędne cele wirusów komputerowych. Wynika to z prostej zasady: pozostając dłużej w ukryciu, mogą wygenerować większą liczbę potomków. Pierwszym krokiem na drodze do zabezpieczenia się przed wirusami jest poznanie zasad ich działania, w szczególności metod „rozmnażania”. Każdy wirus związany jest z konkretnym systemem operacyjnym lub programem. Pierwsze z nich nazywamy systemowymi a drugie aplikacyjnymi.

Liczba wirusów w ciągu ostatnich lat szybko rośnie. Przyczynia się do tego powstawanie mutacji istniejących „wirusów” i stosowanie kilku form rozmnażania przez jeden wirus. Z tego powodu mówi się o rodzinach wirusów, które się ciągle na nowo szyfrują, a kolejne egzemplarze „szkodnika” nie przypominają swoich przodków.
W ciągu ostatnich lat pracowano nad mechanizmami ukrycia wirusów. W ten sposób powstały wirusy typu stealth. „Tajniacy” dostarczają skanerowi danych w oryginalnej („niezarażonej”) postaci, a wykrycie ich staje się możliwe dopiero po restarcie systemu z wolnej od wirusów dyskietki.
W 1988 r. jeden z robaków doprowadził nawet do załamania komputera sieci Internet. Zdecydowana większość wirusów została napisana dla systemu DOS i nie działa w innych środowiskach. Nie dotyczy to jednak Windows 95 (a raczej MS-DOS-a 7.0), który stwarza sprzyjające warunki dla niemałej części „szkodników”. OS/2 Warp i Windows NT nie należą do ścisłego kręgu zainteresowań twórców wirusów, wynika to po części ze skutecznych mechanizmów bezpieczeństwa tych systemów. Osoby, które zetknęły się już z wirusami komputerowymi, wiedzą, że nie ma z nimi żartów. Nawet (pozornie) nieszkodliwe okazynie niszczące danych - zwiększają awaryjność systemu komputerowego, ponieważ sama ich obecność w pamięci może blokować niektóre operacje programu lub wywoływać przypadkowe działania.
Wirusy stwarzają i stwarzać będą w przyszłości potencjalne zagrożenie, od którego nie ma ucieczki. Użytkownik może w dużym stopniu zminimalizować ryzyko zarażenia, ale w praktyce zawsze może liczyć na wizytę „nieproszonego gościa”. Jedynym sposobem 100% bezpieczeństwa pozostaje chyba odcięcie się od świata zewnętrznego.

2. PODZIAŁ ZE WZGLĘDU NA SPOSÓB INFEKCJI

- ***Wirusy pasożytnicze (plikowe)***

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.

- ***Wirusy towarzyszące***

Wirusy tego typu są najczęściej pisane w językach wysokiego poziomu. Atakują one pliki, a ich działanie opiera się na hierarchii stosowanej w DOS podczas uruchamiania programów. W momencie uruchamiania programu, w przypadku nie podania rozszerzenia urachamianego pliku, najpierw poszukiwany jest plik o rozszerzeniu COM, potem EXE, a na końcu BAT. W przypadku wykorzystywania interpretatora poleceń DOS dochodzą jeszcze pliki BTM, poszukiwane podczas uruchamiania programu przed plikami BAT.

- ***Bomby logiczne***

Bomba Logiczna 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.

- ***Robaki internetowe***

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.

- ***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 różnych językach i w róży sposób. 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 sposób. Trzeba szyfrować również procedurę szyfrującą, bowiem 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. 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.

- ***Wirusy plików wsadowych***

Wirusy plików wsadowych wykorzystujące do transportu pliki BAT, istnieją od dość dawna, pomimo raczej ubogiego zestawu środków, jakimi dysponuje ich potencjalny twórca. Może wydawać się to niedorzeczne, lecz często potrafią infekować nie tylko pliki BAT, ale także pliki COM, EXE czy sektor tablicy partycji. Po uruchomieniu zainfekowanego pliku wsadowego tworzony jest plik uruchamialny COM lub EXE, zawierający właściwy kod infekujący pliki BAT. Po utworzeniu jest on wykonywany, a następnie kasowany. Ze względu na to, iż procesor nie rozróżnia kodu i danych, można, poprzez sprytną manipulację, utworzyć plik, który będzie mógł się wykonać zarówno jako typowy plik BAT, jak i plik COM.

- ***Makrowirusy, wirusy makrosów.***

Tego typu wirusy to jeden z najnowszych pomysłów. Makrowirusy na zarażają programów uruchamialnych, lecz pliki zawierające definicje makr. Najpopularniejsze obiekty infekcji to pliki DOC, XLS oraz SAM. Do mnożenia się makrowirusy wykorzystują funkcje zawarte w językach makr, wbudowanych w dane aplikacje, np. Word Basic w Microsoft Word lub Visual Basic for Applications w programie Microsoft Excel.

- ***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 się on wówczas resztę swojego kodu, który się tam nie zmieścił i prawdziwy sektor. Jeśli mamy zainfekowany dysk twardy, to by go wyleczyć trzeba uruchomić komputer z dyskietki systemowej i uruchomić dobry program antywirusowy.

- ***Hybrydowe***

Wirusy Hybrydowe łączą wirusy sektora ładowania z wirusem pasożytniczym (plikowym). Daje to największe możliwości replikacji a jednocześnie utrudnia leczenie zainfekowanego systemu. Wykorzystują kombinacje różnych metod. Możliwy jest przykład, gdy wirus jest nie rezydentny a po uzyskaniu kontroli pozostawia w pamięci rezydentny fragment swego kodu

- ***Inicjujące***

Inicjujące (sektora ładowania) - zmieniają zawartość albo głównego sektora ładowania (ang. master boot sector) , albo sektora ładowania DOS'a, zależnie od wirusa i dysku , zwykle zastępując właściwą zawartość swoją własną wersją. Oryginalna wersja modyfikowanego sektora jest na ogół przechowywana w innym miejscu dysku tak, żeby wersja wirusowa była wykonywana jako pierwsza. Zwykle ładuje ona pozostałą część kodu wirusa do pamięci, poprzedzając wykonanie oryginalnej wersji sektora ładowania. W ten sposób wirus rezyduje na stałe w pamięci dopóki komputer jest włączony. Wirusy sektora ładowania są rozpowszechniane przez fizyczną wymianę każdego nośnika, który może być wykorzystany do uruchomienia systemu operacyjnego. Komputer zostaje zainfekowany wirusem sektora ładowania tylko wtedy , gdy użytkownik zainicjuje działanie systemu z zainfekowanego dysku. Całkowicie bezpieczne jest włożenie zainfekowanej dyskietki do kieszeni napędu i skopiowanie z niej danych.

Konie trojańskie

Koń trojański nie jest wirusem komputerowym, ale ze względu na swoje działanie często bywa z nim utożsamiany. Zasada działania konia trojańskiego jest banalnie prosta. Uruchomiony, 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 twardym). Konie trojańskie najczęściej przenoszą się w plikach udających nowe, popularne programy kompresujące (np. PKZIP, ARJ, RAR) lub też udają programy narzędziowe do obsługi dysków.

PODZIAŁ ZE WZGLĘDU NA SPOSÓB PRZENOSZENIA:

- ✓ wirusy przenoszące się za pomocą nośników: np. dysków twardych, dyskietek
- ✓ wirusy doczepiające się do programów wykonywalnych: np. programy systemowe, komercyjne aplikacje,
- ✓ Wirusy, które przenoszą się przez sieć komputerową : np. wirusy atakujące usługi sieciowe, rozpowszechnione robaki internetowe przenoszone przez pocztę elektroniczną,

PODZIAŁ ZE WZGLĘDU NA SPOSÓB DZIAŁANIA PO URUCHOMIENIU:

- ✓ *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.

- ✓ *Rezydentne*

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.

- ✓ *Szybkie infektory*

Przejmują wszystkie możliwe funkcję systemu DOS, używane do obsługi plików i zarażają wszystko, co się im nawinie w maksymalnie krótkim czasie, co powoduje po okresie bardzo szybkiej ekspansji wirusa w danym systemie następuje jego pasywacja (wirus nie może znaleźć już żadnego pliku do infekcji). Duża aktywność szybkiego infektora będzie na pewno łatwo zauważalna dla użytkownika.

- ✓ *Wolne infektory*

Wirusy tego typu są bardzie wyrafinowane. Ich głównym celem jest jak najdłuższe pozostanie w zainfekowanym systemie. Wirusy te używają najczęściej wolnych, kilku stopniowych zmiennych procedur szyfrujących i technik Stealth (ukrywanie swojego kodu). Są to wirusy bardzo trudne do wykrycia i usunięcia, nawet przez bardzo zaawansowane programy antywirusowe.

PODZIAŁ ZE WZLĘDU NA DZIAŁANIE PODEJMOWANE PRZEZ WIRUSA PO ZAINFEKOWANIU SYSTEMU OPERACYJNEGO:

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

3. JAK SIĘ PRZED NIMI ZABEZPIECZAC:

Program antywirusowy jest obecnie niezbędnym dodatkiem do systemu dla każdego użytkownika komputera. Nie zawsze działają one skutecznie bez aktualnych bibliotek antywirusowych, dlatego ważne jest, aby dbać o ich uaktualnianie.
Na stronie mojego systemu operacyjnego można znaleźć listę wszystkich niezbędnych poprawek do naszego systemu, które pozwolą na zatrzymanie wirusów korzystających z błędów systemu i oprogramowania poczty klienta. Nie uruchamianie załączników na pewno uchroni nas przed wieloma wirusami. Kopiowanie plików z Internetu również naraża nas na

niebezpieczeństwo. Znane są przypadki, że nawet na stronach znanych, dużych firm znajdowały się pliki zainfekowane wirusem. Drogą infekcji są też różnego rodzaju nośniki - począwszy od dyskietek, płyt, pamięci zewnętrznych po dyski twarde przynoszone przez znajomych. Tu najczęściej musimy uruchomić zainfekowany plik, aby zainfekować nasz system. Ważną rzeczą jest posiadanie rozwiązania na sytuacje awaryjne. Takim rozwiązaniem jest dyskietka startowa ze skanerem antywirusowym.

Programy antywirusowe - sprawdzają programy i dane na dysku oraz na dyskietkach i jeśli znajdą wirusy, starają się je zniszczyć. Aby zwalczyć nowo powstałe wirusy, programy antywirusowe muszą być często uaktualniane.

Profilaktyka antywirusowa:

a) używaj legalnie zakupionego oprogramowania,
b) nie korzystaj z dyskietek kolegi bez sprawdzenia ich,
c) zabezpieczaj dyskietki, na których nie będziesz niczego zapisywać,
d) sporządzaj kopie zapasowe dyskietek z danymi i bardzo ważnymi programami,
e) kopie zapasowe przechowuj w bezpiecznym miejscu,
f) unikaj pożyczania swoich dyskietek,
g) swoją nie zabezpieczoną dyskietkę używaną na innym komputerze uważaj za potencjalnie zawirusowaną i dlatego przed ponownym użyciem koniecznie ją sprawdź,
h) okresowo zaopatruj się w bezpłatną wersję demonstracyjną programu MKS-VIR

4. JAK SIĘ ROZPRZESTRZENIAJĄ?

Wiele bardzo groźnych wirusów przenosiło się głównie za pośrednictwem załączników do poczty e-mail — plików wysyłanych wraz z wiadomością e-mail. Z reguły można stwierdzić, czy wiadomość zawiera załącznik, gdyż obok niej jest wyświetlana ikona spinacza do papieru reprezentująca załącznik, a w wiadomości znajduje się nazwa załącznika. Jeśli więc nadejdzie od kogoś wiadomość z niezrozumiałą treścią lub z nieoczekiwanym załącznikiem, należy najpierw się skontaktować z nadawcą i potwierdzić zawartość załącznika przed otwarciem go.
Inne wirusy mogą się rozprzestrzeniać za pośrednictwem programów pobieranych z Internetu lub z zainfekowanych dysków komputerowych pożyczanych od przyjaciół czy nawet zakupionych w sklepie. Są to rzadsze sposoby infekcji. Większość osób doprowadza do infekcji, otwierając nieznane załączniki wiadomości e-mail.
Kolejną drogą infekcji są różnego rodzaju nośniki - począwszy od dyskietek, płyt, pamięci zewnętrznych po dyski twarde przynoszone przez znajomych.

5. PRZYKŁADY WIRUSÓW:

Babybear jest robakiem internetowym, którego działanie polega na rozsyłaniu własnych kopii za pomocą poczty elektronicznej oraz na uszkadzaniu instalacji programu Norton AntiVIrus.

Fizzer jest robakiem internetowym, którego działanie polega na rozsyłaniu własnych kopii za pomocą poczty elektronicznej oraz udostępnianiu dostępu do komputera ofiary za pośrednictwem IRCa i KaZaA.

Opasoft jest robakiem, którego działanie polega na rozprzestrzenianiu się w sieci lokalnej, a także w sieci internet poprzez udostępnione dyski twarde oraz pobieraniu uaktualnień z internetu. Robak wykorzystuje zupełnie nową metodę rozprzestrzeniania się, poprzez wykorzystanie błędów w oprogramowaniu Microsoft Windows.

6. PRZYKŁADY PROGRAMÓW ANTYWIRUSOWYCH:

Avast
Mks_Vir
Norton Antyvirus
Dr. Web
Kaspersky AntiVirus
NOD32
Symantec
McAfee
F-Secure
Norton System WOrks
Panda Software
Norman
Sophos
Trend Micro Inc.
RAV AntiVirus
Norton Internet Security

Bibliografia:

1. Nieograniczone zasoby sieci zwaną Internet .
2. „Wirusy komputerowe. Leczenie i profilaktyka”
3. CHIP (różne numery)