Directory viruses

Science, Computer Science

There are many ways to sabotage a computer. Some malicious programs create software that automatically replicates itself and spreads throughout a computer's file system to destroy it later. One of these virus types is called the Directory Virus. From its name itself, one can know that it attacks the directory and file system of a computer. The computer uses a large file that contains information about its subdirectories and files. It includes information such as the starting cluster, the name, the time and date it was created or modified, attributes such as being read-only, and other information.

Every time a file needs to be accessed, it searches for the directory entry and the starting cluster, an index to the File Allocation Table or FAT. All the other cluster addresses are in the FAT. So a Directory Virus infects clusters and allocates it in the FAT. It then targets other clusters and infects other files. The destructive code is usually with executable files such as the ones ending with . EXE or . COM. The location or paths to the computer's files will then be changed by the Directory Virus so that it can infect other files.

This will be done transparently, without the user's knowledge, until the original files will be impossible to find. Eventually, the user's files become useless (Spam Laws, 2009). In May 1991, the DIR II virus was discovered first in Bulgaria. It is also known as Creeping Death and was written by the same programmers who coded the DIR, MG and Shake viruses. At that time, it was considered to be unique since directory viruses were still unknown. It changed directory entries only and did not change the files (Hypponen, 2010).

It was eventually followed by variants such as the DIR III and DIR BYWAY viruses. The BYWAY virus appeared first in mid 1995 in Venezuala, but was possibly authored by a Chinese programmer named Wai Chan since the code is signed “ By Wai Chan” (PR Newswire, 1995). It is similar to the DIR IIfamilyof viruses but alters the technique slightly by modifying directories and cross linking executable files to point to a file named CHKLISTx. MSx, containing the viral code (Paris, 2010).

The BYWAY virus has an interesting story since it reveals that people from different countries often disguise themselves using other countries. The Chinese search engine, Baidu, for example was attacked by malware that showed an Iranian flag, but Baidu doubts that it was Iranian. They believe that it was American hackers who did it. In the same way, the BYWAY virus claims that it was authored by Wai Chan on August 1994. And then when the virus is triggered, it pops out a message saying, “ Trabajemos Todos Por Venezuela” which means, “ We are all working for Venezuela."

It also playsmusicsimultaneously, mimicking the Venezuelan national anthem. But it is likely that the real author is neither Venezuelan nor Chinese since crooks are not likely to leave their calling cards at the scene of the crime. It is also possible to remove the virus without using disinfecting software. Simply rename all . COM and . EXE files with non-executable extensions. The virus will automatically correct the FAT. Then reboot using a clean boot disk to remove the virus in memory, and rename everything back to its executable extensions.

Do this for all hard disk partitions and the virus will be removed. Unfortunately, because viruses are popularly known to wreak havoc on computers, there is an urban myth propagating in the world that every time a PC doesn't work properly, it is always caused by a virus (Rutter, 1999). However, the fact is that not all PC problems are caused by viruses. There may be manufacturer bugs in the software or incompatibility issues with the hardware or software. Or the computer may simply be malfunctioning like any other electronic device that eventually fails.