Good example of computer security: malicious code essay

Law, Security

Malicious code refers to the term used to describe the code in any part of any software having potential threat to damage the system. Whenever some malicious code infects the system and system show irregular behavior, those saved Backups are being run in order to restore the previously saved safe state of the system before the malicious code was active. In this way, the malicious code is automatically detected and thrown out of the system. Backups are common tools for defense against any malicious code. Backups are basically copies of files that exist in the form of “ Shadow Files” and Windows keep it in order to perform a safe " Restore System" and revert the system to the state it has been behaving previously (Cohen, 1994; McMains, 2008).

On-line backups are used to replace the dataset with an image of it when it was last trusted. Although this mechanism is effective in all cases but it does carry few limitations and one among those is the doubling of space for each covered data set. In addition, sufficient data sets redundancy for compression can reduce space problem and make it more effective. Thus, on-line backups are normally implemented by compressing the original executable files along with the on-line backups such that they require only ½ of the space what the original executable file required. On-line backups are often guarded by other protection techniques to make it more effective like cryptography and so forth. Such protection techniques make the backups more strong and effective against virus attack and help in restoring the clean system image (Cohen, 1992).

Unfortunately in personal computers, the bootstrap process in not normally secure and viruses are succeeded in bypassing the integrity shell

implementations. But this can be overcome by using roll back techniques to “ SnapShot” system memory at bootup and thus it performs the complete replacement of system state with the previously known safe state from previous bootstrap. Thus, this mechanism of backup is capable of removing any memory resident corruptions automatically. But SnapShot mechanism must also be protected from any serious attack but due to its strong management of control; this mechanism is strongly effective against viruses and restores system to its original stable state more quickly. This has been found effective against all PC based bootstrap modifying viruses and has been proved very effective against viruses than online backups. Backups in any form are the first choice to prevent system from losing its original form and keep the system cleans (Cohen, 1992).

References

Cohen, F. B. (1992), “ Defense-In-Depth against Computer Viruses”, Computers & Security, 11(6), 563–579.

Cohen, F. B (1994), “ A Short Course on Computer Viruses”, Retrieved from http://www. goodreads. com/book/show/4748447-a-short-course-on-computer-viruses

McMains, W. (2008), “ Backup: System Protection and Deleting Shadow Copies”, Retrieved from http://www. imagingtips. com/othertips/organizing/0920shadow. shtml