Internet Crime

The Internet provides a wide variety of opportunities for communication and development, but unfortunately it also has its dark side. Crackers, or black-hat hackers, are computer criminals who use technology to perform a variety of crimes: virus propagation, fraud, intellectual property theft, etc.

Internet-based crimes include scam, e-mail fraud to obtain money or valuables, and phishing, bank fraud, to get banking information such as passwords of internet bank accounts or credit card details. Both crimes use e-mails or websites that look like those of real organizations.

Crackers are a new type of criminals. Due to its anonymity, the Internet also provides the right environment for on-line harassment or abuse, mainly in chat rooms or newsgroups. Piracy, the illegal copying and distribution of copyrighted software, information, music and video files, is widespread. But by far the most common type of crime involves malware.

Malware is software created to damage or alter the computer data or its operations.

Viruses are programs that spread by attaching themselves to executable files or documents. When the infected program is run, the virus propagates to other files or programs on the computer.

There are many types of viruses:

1) O*verwrite Virus.* Overwrite viruses are very dangerous. They simply delete the data (partially or completely) and replace the old code with their own. They replace the file content without changing its size. It is easy to detect as the original program stops working. Once the file gets infected, it can’t be restored and you will end up losing all data. It can affect any file. Examples: Way, Loveletter. Protection: The only way to get rid of this virus is to delete all the infected files, so it’s better to keep your antivirus program updated.

2) *Polymorphic Virus.* The polymorphic virus encodes themselves using different encryption keys and algorithms each time they infect a program or create a copy of itself. Because of different encryption keys, it becomes very difficult for the antivirus software to find them. In other words, it is a self-encrypted virus which is designed to avoid detection by scanners. It can affect any file. Examples: Whale, Simile. Protection: Install advanced, high-end antivirus software.

3) *Memory Resident Virus.* These viruses live in RAM and get activated whenever you switch on the computer. They affect all files currently running on the desktop. Basically, it allocates memory and runs its own code when any program is executed. It can affect any file running on PC and files that are being copied or renamed. Examples: Randex, Meve, CMJ. Protection: Install strong antivirus software.

4) *Companion Virus.* Unlike traditional viruses, they do not modify the existing file. It creates a copy of a file with a different extension which runs in parallel with the actual program. For example, if there is a file named abc.exe, this virus will create another hidden file named abc.com. And when the system calls a file ‘abc’, the .com (higher priority extension) runs before the .exe extension. It can perform malicious steps such as deleting the original files. Can affect: All .exe files. Examples: Stator, Terrax.1096. Protection: Install reliable antivirus software and avoid downloading attachments of unsolicited emails.

5) *Macro Virus.* There are a few software such as a word processor that allows a macro program to embed in documents. This virus is written in the macro language, so it may run automatically when the document is opened and it can easily spread to other files too. It depends on the application rather than the operating system. They are generally hidden in documents that are more likely shared via email. It can affect: .mdb, .PPS, .Doc, .XLs files. Examples: Bablas, Concept and Melissa virus. Protection: Disable macros and don’t open emails from unknown sources. Alternatively, you can install modern antivirus software that can detect macro virus easily.

Logic Bombs. They are not a virus but inherently malicious like worms and viruses. It is a piece of code intentionally inserted (hidden) into a software tool. This code is executed after certain criteria are met.