What Is a Trojan?

Before I start, I want to offer a definition of what a trojan is because these devices are often confused with other malicious code. A Trojan horse is an unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user.

A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown (and probably unwanted) by the user.

Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown (and probably unwanted) by the user.

The unauthorized functions that the trojan performs may sometimes qualify it as another type of malicious device as well. For example, certain viruses fit into this category. Such a virus can be concealed within an otherwise useful program. When this occurs, the program can be correctly referred to as both a trojan and a virus. The file that harbors such a trojan/virus has effectively been trojaned. Thus, the term trojan is sometimes used as a verb, as in "He is about to trojan that file."

Classic Internet security documents define the term in various ways. Perhaps the most well known (and oddly, the most liberal) is the definition given in RFC 1244, the Site Security Handbook:

A trojan horse program can be a program that does something useful, or merely something interesting. It always does something unexpected, like steal passwords or copy files without your knowledge.

Another definition that seems quite suitable is that given by Dr. Alan Solomon, an internationally renowned virus specialist, in his work titled All about Viruses:

A trojan is a program that does something more than the user was expecting, and that extra function is damaging. This leads to a problem in detecting trojans. Suppose I wrote a program that could infallibly detect whether another program formatted the hard disk. Then, can it say that this program is a Trojan? Obviously not if the other program was supposed to format the hard disk (like Format does, for example), then it is not a trojan. But if the user was not expecting the format, then it is a trojan. The problem is to compare what the program does with the user's expectations. You cannot determine the user's expectations for a program.