Where Do Trojans Come From?

Trojans are created strictly by programmers. One does not get a Trojan through any means other than by accepting a trojaned file that was prepared by a programmer. True, it might be possible for a thousand monkeys typing 24 hours a day to ultimately create a trojan, but the statistical probability of this is negligible. Thus, a trojan begins with human intent or mens rea. Somewhere on this planet, a programmer is creating a trojan right now. That programmer knows exactly what he or she is doing, and his or her intentions are malefic (or at least, not altruistic).

The trojan author has an agenda. That agenda could be almost anything, but in the context of Internet security, a trojan will do one of two things:

Perform some function that either reveals to the programmer vital and privileged information about a system or compromises that system.

Conceal some function that either reveals to the programmer vital and privileged information about a system or compromises that system.

Some trojans do both. Additionally, there is another class of trojan that causes damage to the target (for example, one that encrypts or reformats your hard disk drive). So trojans may perform various intelligence tasks (penetrative or collective) or tasks that amount to sabotage.

One example that satisfies the sabotage-tool criteria is the PC CYBORG trojan horse. As explained in a December 19, 1989 CIAC bulletin ("Information about the PC CYBORG (AIDS) Trojan Horse"):

There recently has been considerable attention in the news media about a new trojan horse which advertises that it provides information on the AIDS virus to users of IBM PC computers and PC clones. Once it enters a system, the Trojan horse replaces AUTOEXEC.BAT, and may count the number of times the infected system has booted until a criterion number (90) is reached. At this point PC CYBORG hides directories, and scrambles (encrypts) the names of all files on drive C:. There exists more than one version of this trojan horse, and at least one version does not wait to damage drive C:, but will hide directories and scramble file names on the first boot after the trojan horse is installed.