Binary planting is a general term for an attack where the attacker places (i.e., plants) a binary file containing malicious code to a local or remote file system in order for a vulnerable application to load and execute it.

There are various ways this attack can occur:

Insecure access permissions on a local directory allow a local attacker to plant the malicious binary in a trusted location. (A typical example is an application installer not properly configuring permissions on directories used to store application files.)

One application may be used for planting a malicious binary in another application’s trusted location. (An example is the Internet Explorer - Safari blended threat vulnerability)

The application searches for a binary in untrusted locations, possibly on remote file systems. (A typical example is a Windows application loading a dynamic link library from the current working directory after the latter has been set to a network shared folder.)