hat portscanning is, and what TrashScan can do about it.

When a hacker wants to use an innocent computer as an intermediary to conceal the origin of an attack, or simply wants to break into or otherwise damage a computer through the network, the first step taken is to find weaknesses that can be exploited.   One convenient way to do this is by portscanning.

Portscanning involves trying to connect to various ports ("channels") on the target computer, in order to discover any servers that might be running. This usually is not a problem on a Macintosh computer, but other platforms such as Linux may have servers running that the administrator is not aware of.   Nevertheless, since portscanning is often a preliminary step in an attack, detecting it can be a good way to stop the attack before it can begin in earnest.

TrashScan works by listening for connections on various randomly-chosen ports.   If someone is conducting an extensive portscan on your computer, odds are good they will eventually connect to one of TrashScan's "hot" ports.   This intrusion will alert you and the scanner that scanning has been detected.   Odds are further increased by having dedicated listeners for particularly attractive ports (those used for HTTP, FTP, or TELNET servers).

When you're alerted to a scan detection, you can ignore it, or contact your ISP and provide them with information from the TrashScan log.   This procedure will be covered in greater detail later.