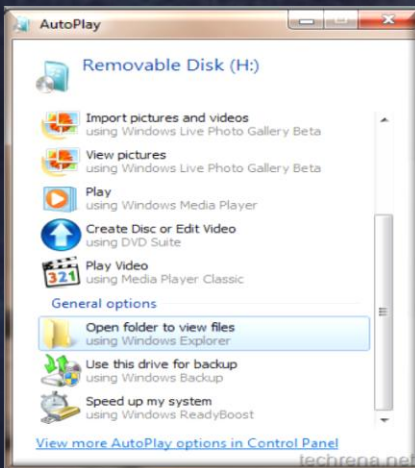


Autorun worm

Autorun worms are malicious programs that take advantage of the Windows AutoRun feature. They execute automatically when the device on which they are stored is plugged into a computer.



Autorun worms are commonly distributed on USB drives, automatically infecting computers as soon as the USB is plugged in. AutoPlay is a similar technology to AutoRun. It is initiated on removable media, prompting users to choose to listen to music with the default media player, or to open the disk in Windows Explorer. Attackers have similarly exploited AutoPlay, most famously via the Conficker worm.

On patched and newer operating systems, Microsoft has set AutoRun to off by default. As a result, autorun worms should pose less of a threat in the future.

Disable it!!

