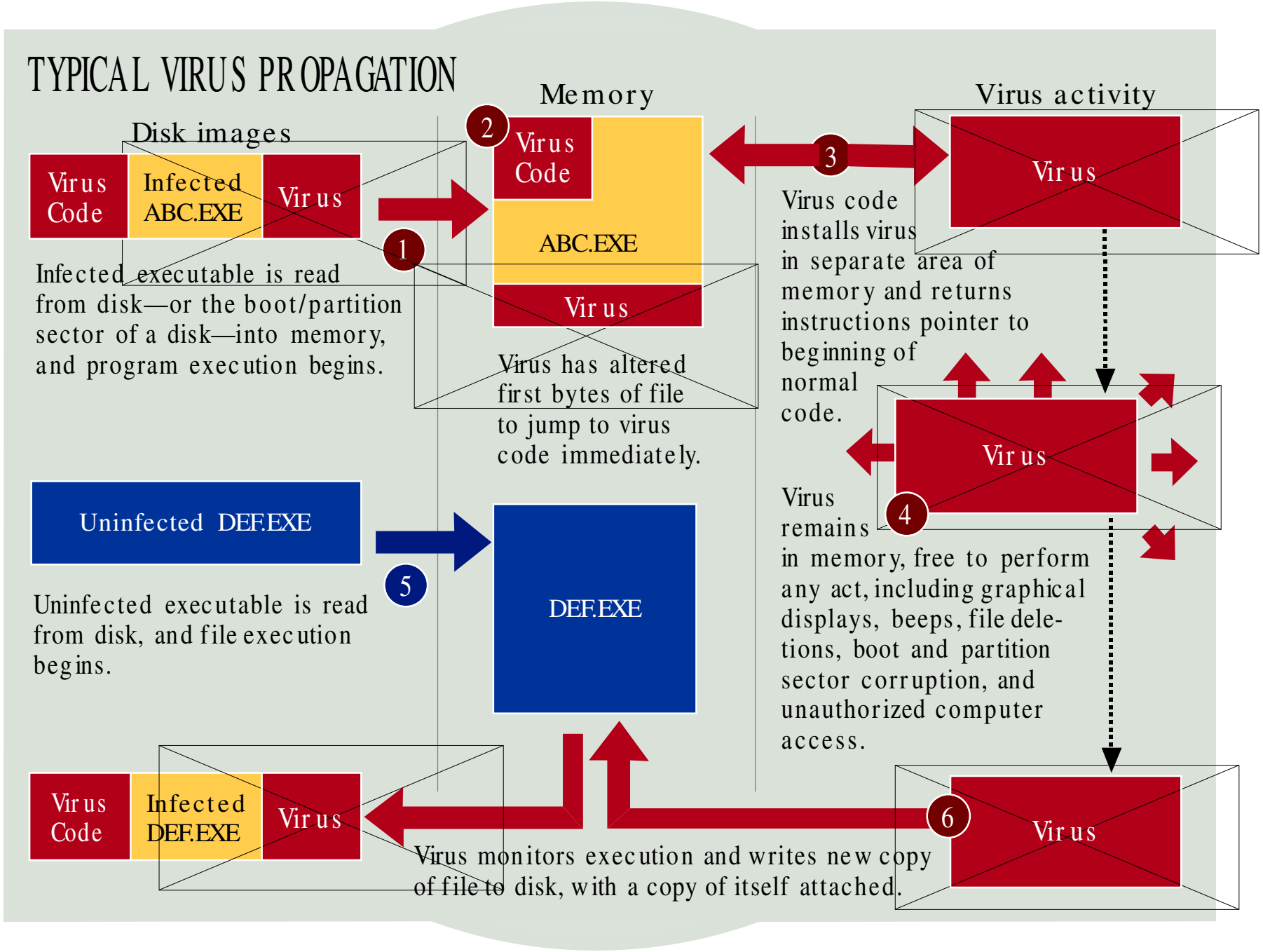
TYPICAL VIRUS PROPAGATION
Disk images
Virus Code
Infected ABC.EXE
Virus
Infected executable is read from disk—or the boot/partition sector of a disk—into memory, and program execution begins.
1
Memory
2
Virus Code
ABC.EXE
Virus
Virus has altered first bytes of file to jump to virus code immediately.
3
Virus activity
Virus
Virus code installs virus in separate area of memory and returns instructions pointer to beginning of normal code.
Virus
4
Virus remains in memory, free to perform any act, including graphical displays, beeps, file deletions, boot and partition sector corruption, and unauthorized computer access.
Uninfected DEF.EXE
5
Uninfected executable is read from disk, and file execution begins.
DEF.EXE
Virus Code
Infected DEF.EXE
Virus
6
Virus
Virus monitors execution and writes new copy of file to disk, with a copy of itself attached.