

**Se cache dans la
mémoire vive (fileless)**

**Masque sa présence au
système (rootkit)**

**Modifie le registre ou
crée des services
persistants**

**Change régulièrement de
signature pour échapper à
la détection
(polymorphisme)**

**Détourne des processus
système légitimes**

**Efface ses traces après
exécution**

**S'installe dans le
firmware ou le secteur
de démarrage**

