S’exécute automatiquement au démarrage du système

Attend une date ou un événement précis pour s’activer (bombe logique)

Communique avec un serveur de commande et contrôle (C2)

Lance des processus cachés ou planifiés

Exploite des outils légitimes du système (PowerShell, WMI…)

Utilise un faux message d’erreur pour tromper l’utilisateur

Installe une porte dérobée (backdoor)