Identifiable par signature (antivirus classique)	Détection difficile : comportement variable ou polymorphe
Peut être neutralisé par un correctif système	Peut fonctionner sur plusieurs plateformes (Windows, Linux, Android)
Requiert une analyse comportementale (EDR/XDR) pour être détecté	Agit sans créer de fichier sur le disque
Fait partie d’une campagne coordonnée (Advanced Persistent Threat ou APT)	