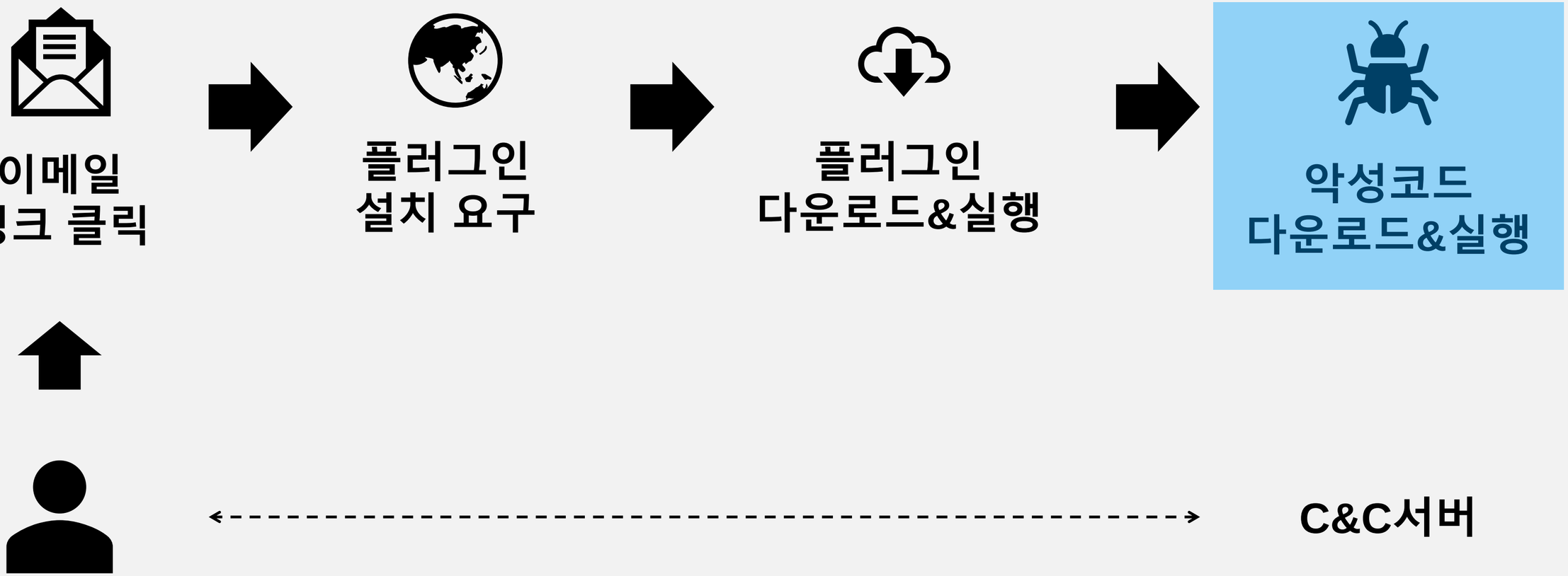
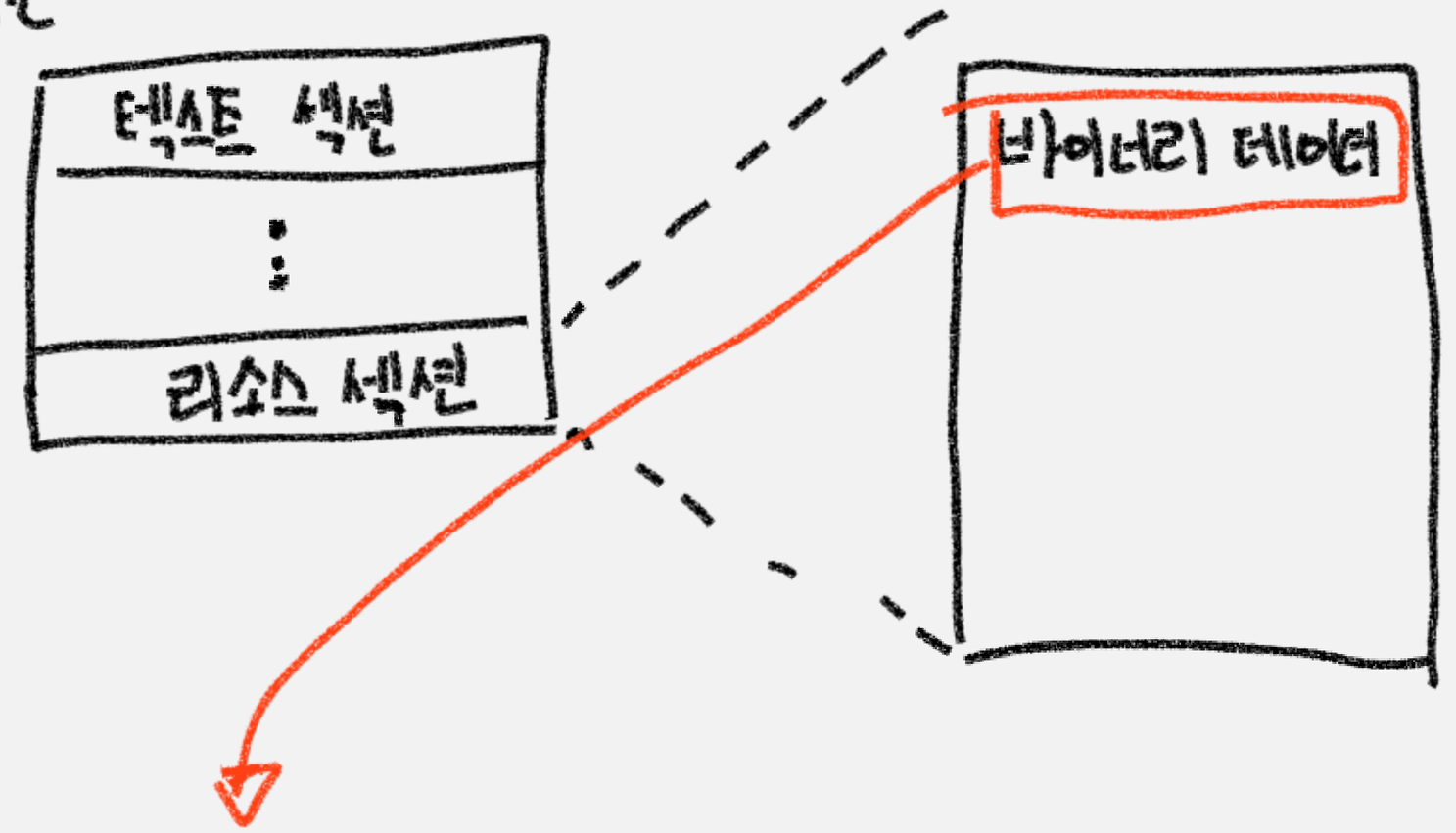
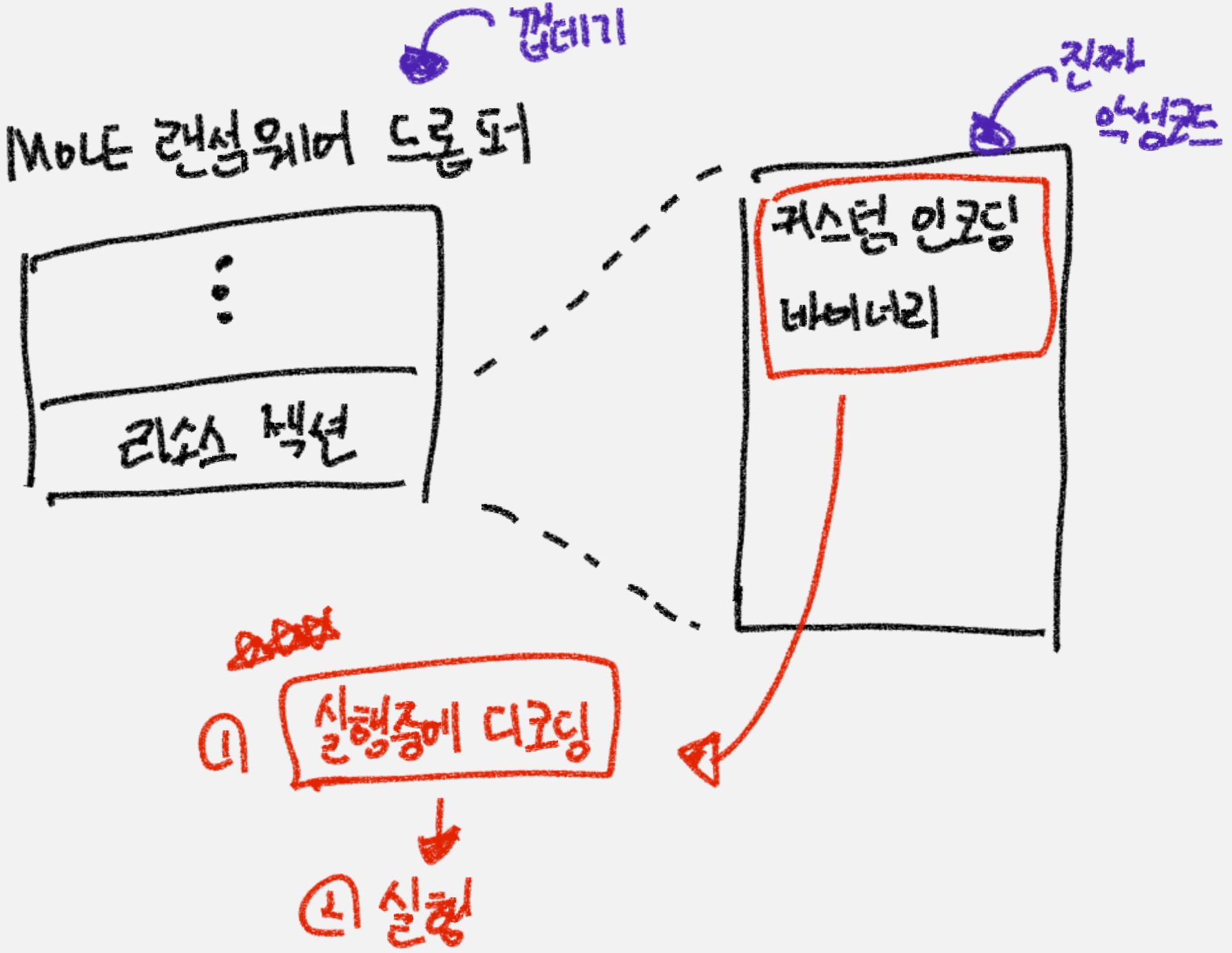
랜섬웨어 감염 과정 요약

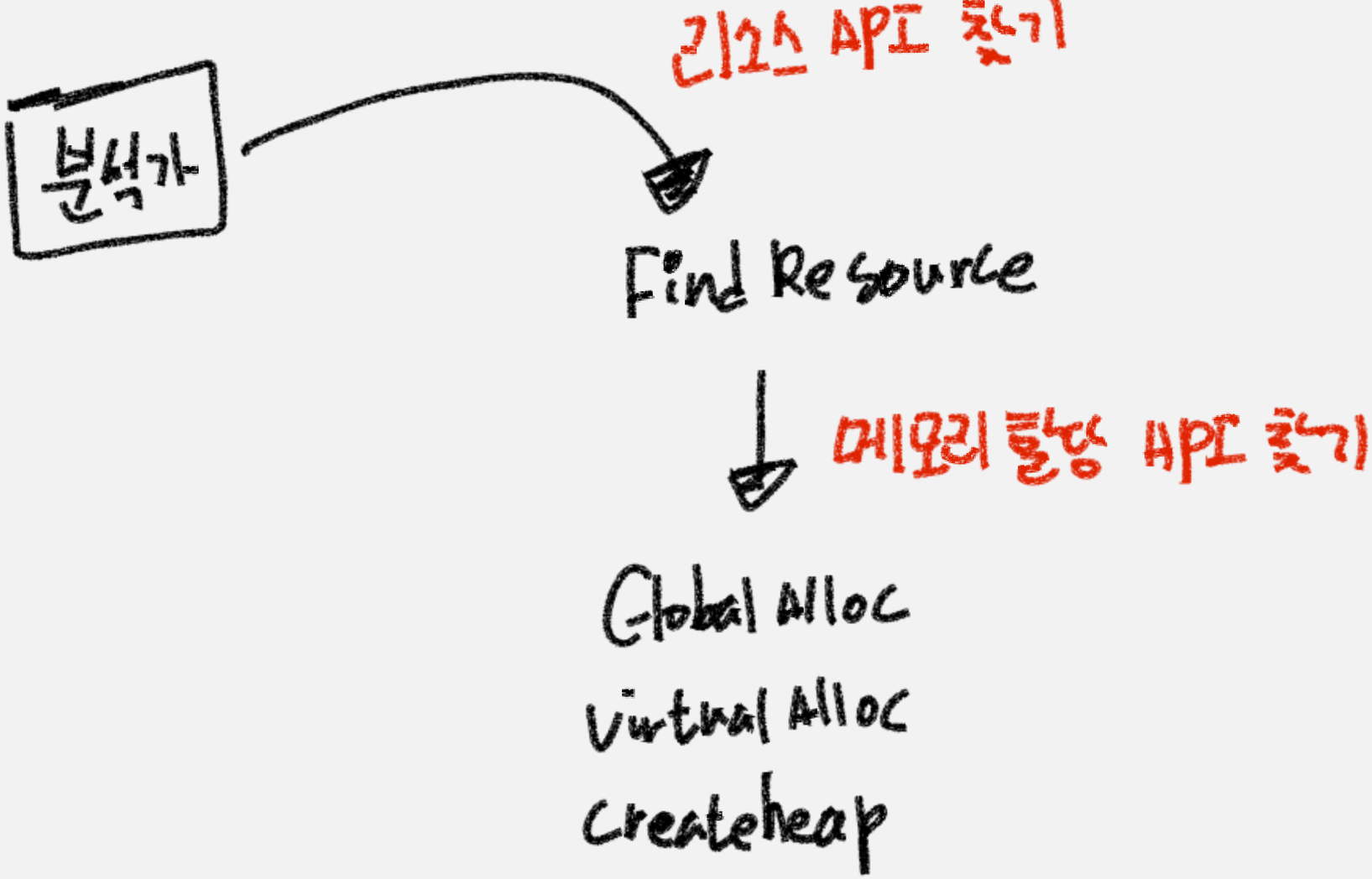


PE 섹션



① 아이콘
② 폰트
③ 악성코드


컴파일
진짜 액션코드
MoLe 랜섬웨어 드롭퍼
리소스 섹션
커스텀 인코딩
네버네리
실행중에 디코딩
실행


분석가
리소스 API 찾기
Find Resource
메모리 할당 API 찾기
GlobalAlloc
VirtualAlloc
CreateHeap