적의 약점: 실행 불변 특징 (Execution Invariants)

실행 불변 특징(Invariant)이란, 악성코드가 변종/난독화에도 불구하고 **핵심 기능을 수행하기 위해 어쩔 수 없이 메모리에 남기는 고유한 코드나 데이터 패턴**을 의미합니다. 이는 공격자가 쉽게 바꿀 수 없는 알고리즘의 지문과 같습니다.

Amadey

메모리에서 발견되는 32글자 길이의 고정 HEX 복호화 키, 개발 경로 문자열 \Amadey\Release\Amadey.pdb

RedLine Stealer

브라우저 DB 경로 cookies.sqlite나 기능명 ChromeGetRoamingName, DownloadAndExecuteUpdate 같은 문자열

FormBook

프로세스 인젝션을 위해 필수적인 API 호출 순서 (e.g., VirtualAllocEx → WriteProcessMemory → ResumeThread)