사냥의 시작: YARA를 이용한 불변 특징 탐지

- YARA는 텍스트/바이너리 패턴을 정의하여 악성코드 군을 식별하는 강력한 도구입니다.
- 파일뿐만 아니라, 실행 중인 프로세스 메모리나 메모리 덤프를 직접 스캔하여 난독화 너머의 실제 페이로드를 탐지할 수 있습니다.
- 해시 매칭과 달리 일반화된 패턴을 사용하므로, 수많은 폴리모픽 변종에 대응하는 **불변 특징(Invariant) 탐지에 최적화**되어 있습니다.

```
rule Detect_Amadey_Invariant_InMemory {
    meta:
        description = "Detects Amadey PDB path or key patterns in memory"
    strings:
        // Evidence 1: Development artifact
        $pdb = "\\Amadey\\Release\\Amadey.pdb" ascii wide ⟵ 개발 경로 문자열
        // Evidence 2: Unique code sequence
        $seq_0 = { 89 45 F4 83 7D F4 08 74 4F } ⟵ 고유 코드 실행 흐름
    condition:
        // Found in a PE file loaded in memory
        uint16(0) == 0x5A4D and any of them
}
```