교묘한 적: 정적 탐지를 무력화하는 Amadey

정적 탐지는 디스크 상의 파일 서명을 분석하지만, Amadey와 같은 최신 악성코드는 이를 쉽게 우회합니다.

- **핵심 우회 기법**: Amadey는 페이로드 내 주요 문자열을 **2중으로 인코딩(사용자 정의 인코딩 + Base64)**하여 정적 분석을 극도로 어렵게 만듭니다.
- **결과**: 패커(packer)나 암호화로 감싸진 변종 악성코드는 기존의 파일 해시나 문자열 서명 기반 탐지를 무력화시킵니다. 이는 MaaS(Malware-as-a-Service) 형태로 빠르게 유포되는 Amadey 변종 탐지에 치명적인 약점입니다.