하나의 패턴, 여러 개의 표적: 악성코드 패밀리 간 메모리 수렴성

서로 다른 악성코드들도 결국 메모리상에서는 유사한 형태나 동작(수렴성)을 보입니다.
이는 각 패밀리가 수행하는 고유한 악성 행위가 공통된 기술적 흔적을 남기기 때문입니다.

Amadey (Loader)

Invariant

문자열 복호화 루틴, C2 통신 스레드 생성 코드.

RedLine (Stealer)

Invariant

브라우저 프로파일, 암호화폐 지갑 관련 평문 문자열.

FormBook (Injector)

Invariant

다층 암호화 후 최종 단계의 프로세스 인젝션 API 호출 시퀀스.

SmokeLoader (Loader)

Invariant

`explorer.exe` 등 정상 프로세스에 인젝션된 비정상 코드 영역.